Automating Disaster Recovery using Oracle Site Guard for Oracle Exalogic

WITH ORACLE EXADATA DATABASE MACHINE

Oracle Maximum Availability Architecture White Paper
July 2013

Maximum
Availability
Architecture

Oracle Best Practices For High Availability

Executive Overview

Oracle Maximum Availability Architecture (MAA) [1] is the Oracle best practices blueprint for implementing Oracle high availability technologies. Maximum Availability Architecture is one of the key requirements for any Oracle Fusion Middleware enterprise deployment. Oracle Fusion Middleware includes an extensive set of high availability features such as: process death detection and restart, server clustering, server migration, clusterware integration, GridLink, load balancing, failover, backup and recovery, rolling upgrades, and rolling configuration changes, which protect an Enterprise Deployment from unplanned down time and minimize planned downtime.

Additionally, enterprise deployments need protection from unforeseen disasters and natural calamities. The typical protection solution involves setting up a standby site at a geographically different location than the primary site. The standby site may have equal or fewer services and resources compared to the primary site. Application data, metadata, configuration data, and security data are replicated to the standby site on a periodic or continual basis. The standby site is normally in a passive mode; it is started when the primary site is not available. This deployment model is sometimes referred to as an active/passive model.

The Oracle Fusion Middleware Disaster Recovery solution uses storage replication technology for disaster protection of middle tier components while Oracle Data Guard provides disaster protection for the Oracle databases that are part of Oracle Fusion Middleware deployments. Disaster Recovery operations are typically time consuming, manual, and prone to errors. Oracle Site Guard, a part of Oracle Enterprise Manager, will help you build, manage and execute reliable Disaster Recovery plans. It helps meet the Recovery Time Objective (RTO) through the automation of Disaster Recovery procedures and reduces costs by achieving predictable and timely results for recovery of a production environment.

The Oracle Site Guard Disaster Recovery Solution for the Oracle Exalogic machine and Oracle Exadata Database machine builds upon these well-established disaster protection solutions for Oracle Fusion Middleware and Oracle databases. While this paper describes the Oracle Site Guard Disaster Recovery solution for Oracle Exalogic and Oracle Exadata Database machine deployments, the principles described here also apply to deployments on an Oracle Exalogic machine with an Oracle Database, and to standalone deployments on an Oracle Exalogic machine.

Introduction

Oracle Exalogic Elastic Cloud is an integrated hardware and software system designed to provide a complete platform for a wide range of application types and widely varied workloads. Oracle Exalogic is intended for large-scale, performance-sensitive, mission-critical application deployments. It combines Oracle Fusion Middleware software and industry-standard Sun hardware to enable a high degree of isolation between concurrently deployed applications, which have varied security, reliability, and performance requirements.

The Oracle Exalogic Elastic Cloud consists of Sun Fire Servers as compute nodes, a Sun ZFS Storage appliance, and required InfiniBand and Ethernet networking components. The Sun ZFS Storage appliance combines multi-protocol connectivity, data services for business continuity, and ease of management into a single appliance. The appliance supports NFS, Internet Small Computer System Interface (iSCSI), and InfiniBand (IB) for data access. The appliance also supports Network Data Management Protocol (NDMP) for backing up and restoring the data.

The Sun ZFS Storage appliance can be configured with dual controllers (also referred to as server heads) operating as an active-passive cluster. The storage disks in the Sun ZFS Storage appliance are allocated to a single storage pool, and this storage pool is assigned to one of the storage controllers. Applications deployed on the Oracle Exalogic machine access the storage using the NFSv4 protocol over the InfiniBand network.

The Oracle Exadata Database machine is an easy to deploy solution for hosting the Oracle Database, which delivers the highest levels of database performance available. The Exadata Database machine is a "cloud in a box" composed of Database Servers, Oracle Exadata Storage Servers, an InfiniBand fabric for storage networking, and all the other components required for hosting an Oracle Database.

The Oracle Exadata Database machine provides an optimal solution for all database workloads, ranging from scan-intensive data warehouse applications to highly concurrent online transaction processing (OLTP) applications. With its combination of smart Oracle Exadata Storage Server Software, complete and intelligent Oracle Database software, and the latest industry-standard hardware components, Oracle Exadata Database machine delivers extreme performance in a highly-available, highly-secure environment.

Oracle Site Guard, a part of Oracle Enterprise Manager, provides flexible and seamless orchestration of switchovers and failovers between disaster recovery sites, thereby minimizing downtime for enterprise deployments. The disaster recovery automation features in Oracle Site Guard eliminate the need for human intervention and prevent human-induced errors in the switchover or failover process. Oracle Site Guard is flexible and easily integrates with various platforms including Oracle Exalogic and Exadata.

While many variations in disaster recovery topologies are possible, Oracle strongly recommends using a topology similar to the one described in this paper, i.e., an Exalogic and Exadata machine pair is recommended for both sites, even though they may vary in configuration and capacity. The topology described in this paper is designed to maintain SLAs through ease of management, maintenance, and automated disaster recovery operations.

The goal of this technical paper is to provide:

- Oracle Fusion Middleware Disaster Recovery architecture and strategy for deployments on Oracle Exalogic with Oracle Exadata Database machine.
- Detailed deployment and configuration steps for a Oracle Site Guard-driven disaster recovery solution for Oracle Fusion Middleware running on Exalogic with Exadata.
- Best practices for the Oracle Fusion Middleware Disaster Recovery solution with Exalogic and Exadata.

This paper describes the use of Oracle Site Guard to provide disaster recovery in an Oracle engineered systems deployment, however, the concepts presented herein can be adapted for use in other Oracle-supported deployments, such as:

- Oracle applications deployed on Exalogic machines that do not use a database.
- Oracle applications deployed on Exalogic machines that use an Oracle database not deployed on Oracle Exadata.
- Oracle applications deployed on Exalogic machines that use an Oracle database with storage and replication from an approved third-party vendor.

At the time of release of this paper, Oracle Site Guard can be used to protect any site which has a middle-tier deployment consisting of Oracle Fusion Middleware, Oracle Process Manager and Notification Server (OPMN) components, and Oracle Weblogic server components. This includes Oracle Fusion Middleware 11.x product suites, including: Oracle SOA Suite, Oracle WebCenter Portal, Oracle WebCenter Content, Oracle Business Intelligence, and Oracle Identity Management. Oracle Site Guard can also protect Oracle Fusion Applications and Oracle Weblogic-based custom applications. For the database tier, Oracle Site Guard is certified to work with all Oracle Database 11.x versions.

Audience

This document is intended for Oracle Fusion Middleware architects and administrators, storage-system administrators, Oracle database administrators and technical sales personnel. It is assumed that the reader is familiar with Oracle Exalogic Elastic Cloud, Oracle Exadata Database machine, Oracle Fusion Middleware components, Oracle Database concepts, Oracle Data Guard and Broker, Oracle Enterprise Manager, and Oracle Site Guard. For additional details, refer to the documents listed in the References section.

Oracle Fusion Middleware Disaster Recovery Strategy

Oracle Fusion Middleware product binaries, configuration and applications are deployed to the Oracle home and domain home directories. The Oracle Fusion Middleware home directories and the domain directories are stored on shared storage. The metadata and the run-time data are stored in a database repository.

The Oracle Fusion Middleware Disaster Recovery strategy facilitates data protection as follows:

- The remote replication feature of the Sun ZFS Storage appliance protects the middleware product binaries, configurations, metadata files and application data that reside on the file system.
- Oracle Data Guard and Oracle Data Guard Broker protects the Oracle Database. This database contains Oracle Fusion Middleware Repository data, as well as customer data.

The clients access the primary site during normal operation. During disaster recovery, clients access the standby site. The change is almost seamless from the client's perspective since the entire Fusion Middleware infrastructure along with the mount points and host names are configured identically at the primary and standby sites.

Disaster Recovery Considerations and Terminology

This section provides considerations for and defines the terminology for Disaster Recovery.

Site Symmetry

Site Symmetry has to do with whether the primary and standby sites are exact or partial replicas of each other. Irrespective of the site symmetry used, Oracle strongly recommends deploying Exalogic machines at both sites.

Symmetric Site

An Oracle Fusion Middleware Disaster Recovery configuration that is completely identical across all tiers on the primary site and standby site is called a **symmetric** site.

A site can be **completely symmetric** or **partially symmetric**.

In a completely symmetric site the primary site and standby site are identical in all respects. That is, they have identical Exalogic and Exadata hardware, load balancers, middleware instances, applications and databases. The same port numbers are used for both sites.

In a partially symmetric site the primary site and standby site are identical in topology but not hardware. That is, they have the same number of middleware instances, applications and databases on each site but the Exalogic and Exadata hardware is not identical.

For example, the primary site could have a full rack of Exalogic and Exadata, whereas the standby site may have a half rack of Exalogic and Exadata. This would create a partially symmetric disaster recovery topology.

The disaster recovery site configuration in this paper is symmetric, in terms of both, hardware and topology. Oracle strongly recommends having at least a partially symmetric configuration when planning for disaster recovery.

Asymmetric Site

An **asymmetric** topology is a disaster recovery configuration that is different across tiers at the primary site and standby site.

In an asymmetric topology, the standby site has fewer resources than the primary site. Typically, the standby site in an asymmetric topology still deploys Exalogic and Exadata racks, but may have fewer hosts, load balancers, Fusion Middleware instances, and applications than the primary site.

The number of database instances on the standby site must match those at the primary site, but they can be Non-RAC database instances.

Many of the concepts for setting up a symmetric topology are also valid for setting up an asymmetric topology.

It is important to ensure that an asymmetric standby site has sufficient resources to provide adequate performance when it assumes the primary role.

Please refer to the Oracle Fusion Middleware Disaster Recovery Guide for the steps to setup an asymmetric site.

Storage Considerations and Terminology

This section provides an overview of the terminology and storage concepts for the Sun ZFS Storage appliance. This appliance is a part of every Oracle Exalogic machine.

Storage Pool

The storage pool (similar to a volume group or aggregate) is created over a set of physical disks. File systems are then created over the storage pool. The storage pool is configured with a RAID layout such as mirrored, RAID-Z (single parity), or RAID-Z2 (dual parity).

In an Exalogic machine, all the physical hard disks are mirrored and allocated to a single storage pool. This is the default configuration for an Exalogic machine

Projects

All file systems and LUNs are grouped into projects. A project can be considered a **consistency group**. A project defines a common administrative control point for managing shares. All shares within a project can share common settings, and quotas can be enforced at the project level in addition to the share level. Projects can also be used solely for grouping logically related shares together, so that their common attributes (such as accumulated space) can be accessed from a single point.

Shares

Shares are file systems and LUNs that are exported over supported data protocols to clients of the appliance. Exported file systems can be accessed over NFS. The project/share is a unique identifier for a share within a pool. Different projects can contain shares with the same name, but a single project cannot contain shares with the same name.

Oracle strongly recommends that the compute nodes from an Exalogic machine access the shares/projects over NFSv4. The NFS shares are mounted using IPoIB (IP over InfiniBand).

ZFS Replication

ZFS replication is a method where two storage systems are replicated with a lag, such as a write is considered complete as soon as local storage acknowledges it. The remote storage is usually updated with a small lag. This has the advantage of being able to process writes much faster at the primary location, because the system does not have to wait for data to be saved at the replication site. This is usually implemented using snapshots; a snapshot of the current state of the master system is replicated to the secondary storage system. Depending on the configuration used, the process is repeated as soon as the snapshot is replicated, or it is triggered at certain times.

The main advantage of this technique is that it allows for replication over far larger distances, because the link between the storage systems can have a lower bandwidth (not every write has to be replicated; only the state of the system at certain points in time), and higher latency (because writes don’t need to be confirmed at both sites at once). The disadvantage is that in case of a failure on the primary system, data loss is guaranteed. The secondary system will always be missing data that has been written to the master. Performance is greatly increased, but if local storage is lost, the remote storage is not guaranteed to have a current copy of the data and most recent data may be lost.

The Sun ZFS Storage appliance in the Exalogic machine supports snapshot-based replication of projects and shares from a source appliance to any number of target appliances. The replication includes both data and metadata. The replication for a project or share can be configured to use one of three modes: scheduled, on-demand or continuous.

Scheduled Replication

In this mode, the user can define a schedule for automatic replication. If a schedule is established, then the replication occurs at the defined interval. The interval can be every half-hour, hour, day, week, or month. This mode is preferred in situations where replication during off-peak time is preferred or where backup is scheduled at the target site at specific time.

On-demand Replication

In this mode, also called as a manual mode, the replication occurs only when the user requests. This is the default mode when the scheduled mode is chosen but no schedule is defined.

Continuous Replication

In this mode, the replication process happens continuously without any user intervention. As soon as the package successfully arrives at the target, the subsequent replication process automatically begins. This mode is deployed where the target site is expected to be almost in sync with the source.

Project Level Replication vs. Share Level Replication

The Sun ZFS Storage appliance in the Exalogic machine allows remote replication to be configured at the project, as well as the share level.

By default, the shares in a project inherit the configuration of the parent project. Inheriting the configuration means that the share is replicated on the same schedule, to the same target, and with the same options as its parent project. It also means that the share is replicated in the same stream using the same project-level snapshots as other shares inheriting the project's configuration. This is important for applications that require data consistency among multiple shares.

Overriding the configuration means that the shares are not replicated with any project-level actions, though it may be replicated with its own share-level actions that include the project. It is not possible to override part of the project's replication configuration and inherit the rest.

More precisely, the replication configuration of a project and its shares define some number of replication groups, each of which is replicated with a single stream using snapshots taken simultaneously. All groups contain the project itself (which essentially just includes its properties). One project-level group includes all shares inheriting the replication configuration of the parent project. Any shares which override the project's configuration form a new group consisting of only the project and shares themselves.

While it is appropriate to choose project or share level replication across different projects, Oracle strongly recommends that project-level and share-level replication be avoided within the same project because it can lead to unexpected results (particularly when reversing the direction of replication).

For the deployment used in this paper, all replication is configured at the project level. No share-level replication is used.

Storage Replication Channel

A storage replication channel is a network channel that is dedicated specifically to replication traffic between the Sun ZFS Storage appliances at the primary site and the standby site.

The Sun ZFS Storage appliance within Exalogic has four 1 Gigabit Ethernet ports (igb0, igb1, igb2 and igb3). In the current configuration two ports (igb0 and igb1) are used for managing the Sun ZFS Storage appliance.

Oracle recommends creating the replication channel by connecting the unused ports (igb2 and igb3) to the corporate network in your datacenter and creating a bonded interface using IP network MultiPathing (IPMP). This bonded interface is dedicated for replication traffic and provides high availability for the storage replication channel.

Oracle strongly recommends:

- Connecting port igb2 to the embedded Cisco Catalyst switch in the Exalogic machine
- Connecting port igb3 directly to a corporate network drop in your data center.
- Connecting the ports to two different switches (this provides switch level high availability).
- Configuring the two switches, to which the ports are connected, on the same VLAN.
- Disabling the management options on the two ports used for replication. This ensures the separation of the replication traffic from the management traffic. This is also an Oracle Security best practices recommendation.

Host Names

Host names play a key role in any topology. In a disaster recovery topology, the hostnames used for wiring intra component and inter component communications, need to be same. Typically, the site where Oracle Fusion Middleware is first installed, dictates the hostname used. The standby site instantiated subsequently should be configured to resolve these hostnames to the standby site's (local) IP addresses. Therefore, it is important to plan the host names for the primary site and standby site. It is also very important that the configuration at all levels use hostnames, and not IP addresses.

This paper assumes that a symmetric disaster recovery site is being set up, where the primary site and standby site have the same number of hosts. Each host at the primary site has a peer host at the standby site. The peer hosts are configured the same. For example, hosts at one site use the same port numbers as their counterparts at the other site.

When configuring each component, use hostname-based configuration instead of IP-based configuration, unless the component requires you to use IP-based configuration. For example, if you are configuring the listen address of an Oracle Fusion Middleware component to a specific IP address such as 192.168.10.33, use the host name wlsvhn1.mycompany.com, which resolves to 192.168.10.33.

It is recommended that DNS be deployed for hostname resolution. In the absence of DNS, aliases in the /etc/hosts file may be used.

Other Site Services

There may be other services, such as Network Information Service (NIS), or Lightweight Directory Access Protocol (LDAP), that are deployed and used at the primary site. Ensure that the same services are also available at the standby site.

Oracle Data Guard

Oracle Data Guard is Oracle's disaster recovery solution prescribed by the Maximum Availability Architecture (MAA) to protect mission critical databases residing on Exadata Database machine. Data Guard is also used to maintain availability should any outage unexpectedly impact the primary database and to minimize downtime during planned maintenance. Data Guard provides a comprehensive set of services that create, maintain, manage, and monitor one or more standby databases to enable primary Oracle databases to survive disasters and data corruptions. Data Guard maintains these standby databases as copies of the primary database. Then, if the primary database becomes unavailable because of a planned or an unplanned outage, Data Guard can switch any standby database to the primary role, minimizing the downtime associated with the outage. Data Guard can be used with traditional backup, restoration, and cluster techniques to provide a high level of data protection and data availability.

Oracle Active Data Guard

Oracle Active Data Guard, an option built on the infrastructure of Oracle Data Guard, allows a physical standby database to be opened read-only while changes are applied to it from the primary database. This enables read-only applications to use the physical standby with minimal latency between the data on the standby database and that on the primary database, even while processing very high transaction volumes at the primary database. This is sometimes referred to as real-time query.

An Oracle Active Data Guard standby database is used for automatic repair of data corruption detected by the primary database, transparent to the application. In the event of an unplanned outage on the primary database, high availability is maintained by quickly failing over to the standby database. An Active Data Guard standby database can also be used to off-load fast incremental backups from the primary database because it is a block-for-block physical replica of the primary.

Data Guard Protection Modes

Data Guard provides different protection modes depending on the user's requirements. The deployment in this paper uses the Maximum Performance mode, however as long as Data Guard is deployed using one of the available modes, the protection mode used has no direct bearing on Site Guard's disaster recovery operations. A brief description of the available Data Guard protection modes follows.

Maximum Availability

This protection mode provides the highest level of data protection that is possible without compromising the availability of a primary database. Transactions do not commit until all redo data needed to recover those transactions has been written to the online redo log and to the standby redo log on at least one synchronized standby database. If the primary database cannot write its redo stream to at least one synchronized standby database, it operates as if it were in maximum performance mode to preserve primary database availability until it is again able to write its redo stream to a synchronized standby database.

This mode ensures that no data loss occurs if the primary database fails, but only if a second fault does not prevent a complete set of redo-data from being sent from the primary database to at least one standby database.

Maximum Performance

This protection mode provides the highest level of data protection that is possible without affecting the performance of a primary database. This is accomplished by allowing transactions to commit as soon as all redo data generated by those transactions has been written to the online log. Redo data is also written to one or more standby databases, but this is done asynchronously with respect to transaction commitment, so primary database performance is unaffected by delays in writing redo data to the standby database(s).

This protection mode offers slightly less data protection than maximum availability mode and has minimal impact on primary database performance.

This is the default protection mode for a database.

Maximum Protection

This protection mode ensures that no data loss occurs if the primary database fails. To provide this level of protection, the redo data needed to recover a transaction must be written to both the online redo log and to the standby redo log on at least one synchronized standby database before the transaction commits. To ensure that data loss cannot occur, the primary database shuts down, rather than continuing to process transactions, if it cannot write its redo stream to at least one synchronized standby database.

Because this data protection mode prioritizes data protection over primary database availability, Oracle recommends that a minimum of two standby databases be used to protect a primary database that runs in maximum protection mode to prevent a single standby database failure from causing the primary database to shut down.

Oracle Data Guard Broker

Oracle Data Guard broker is a distributed management framework that automates and centralizes the creation, maintenance, and monitoring of Data Guard configurations. The following list describes some of the operations the broker automates and simplifies:

- Creating Data Guard configurations that incorporate a primary database, a new or existing (physical, logical, or snapshot) standby database, redo transport services, and log apply services, where any of the databases could be Oracle Real Application Clusters (RAC) databases.
- Adding additional new or existing (physical, snapshot, logical, RAC or non-RAC) standby databases to an existing Data Guard configuration, for a total of one primary database, and from 1 to 9 standby databases in the same configuration.
- Managing an entire Data Guard configuration, including all databases, redo transport services, and log apply services, through a client connection to any database in the configuration.
- Managing the protection mode for the broker configuration.
- Invoking switchover or failover with a single command to initiate and control complex role changes across all databases in the configuration.
- Configuring failover to occur automatically upon loss of the primary database, increasing availability without manual intervention.
- Monitoring the status of the entire configuration, capturing diagnostic information, reporting statistics such as the redo apply rate and the redo generation rate, and detecting problems quickly with centralized monitoring, testing, and performance tools.

All management operations can be performed locally or remotely through the broker's easy-to-use interfaces: the Data Guard management pages in Oracle Enterprise Manager, which is the broker's graphical user interface (GUI), and the Data Guard command-line interface called DGMGRL. These interfaces simplify the configuration and management of a Data Guard configuration.

Deploying Data Guard broker with Data Guard is essential before Oracle Site Guard can be used for disaster recovery.

Oracle Enterprise Manager

Oracle Enterprise Manager is Oracle's integrated enterprise information technology (IT) management platform. It provides the management infrastructure using which the Oracle Site Guard plug-in provides disaster recovery services.

Since Enterprise Manager is critical for managing disaster recovery operations, Oracle strongly recommends the following for the Enterprise Manager deployment:

- Ensure that Enterprise Manager is not deployed on the Exalogic machines at either the primary or standby sites. Doing so makes it vulnerable to the outages that it is intended to detect and protect from.
- Implement high availability and disaster recovery plans for protecting the Enterprise Manager deployment. Maintain these plans separate from the disaster recovery plans for the production environment.

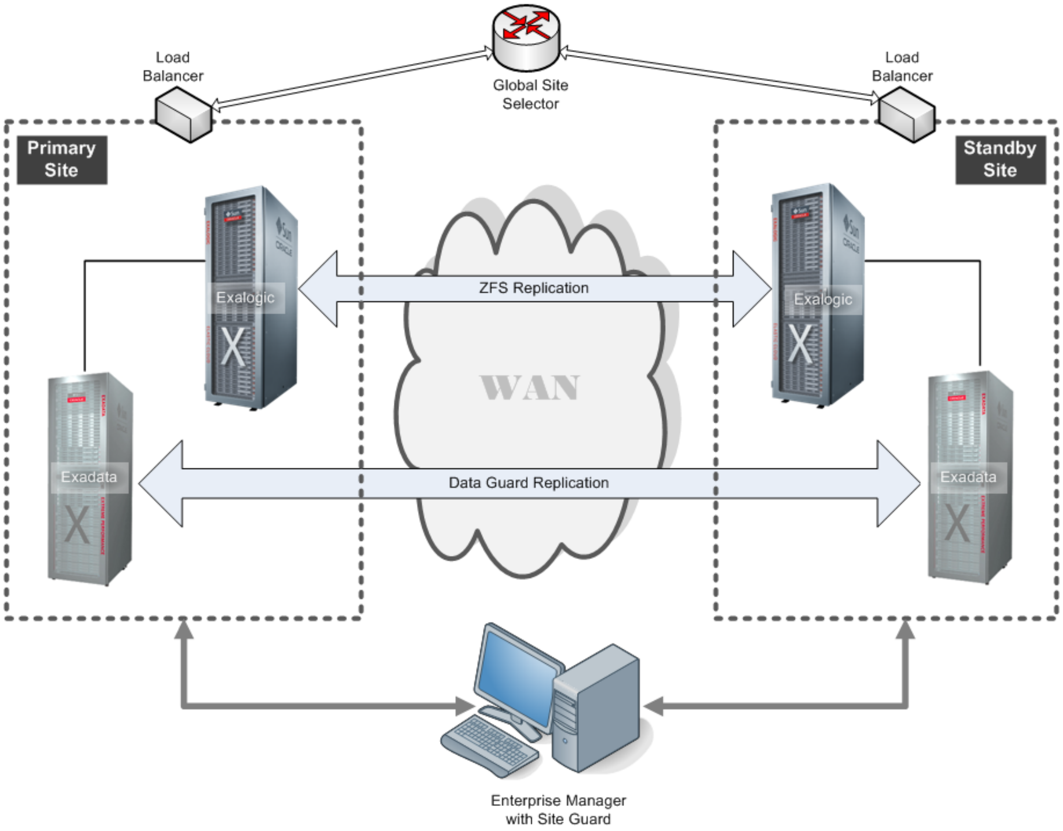
Disaster Recovery Architecture

The topology described in the **Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intelligence** was used as the reference architecture in this paper. This reference architecture was then adapted for deployment on Exalogic and Exadata machines using the guidelines provided in the **Oracle Fusion Middleware Exalogic Enterprise Deployment Guide**; and finally adapted for Oracle Site Guard-based disaster recovery using the guidelines in the **Oracle Fusion Middleware Disaster Recovery Guide,** and the **Oracle Enterprise Manager Cloud Control Lifecycle Management Administrator's Guide**.

An Enterprise deployment is a reference configuration that is designed to support large-scale, mission-critical business software applications and is an Oracle best practices blueprint based on proven Oracle high-availability and security technologies and recommendations for Oracle Exalogic.

Overview of Topology

The figure below shows an overview of the topology that is deployed and tested for this paper.



The primary and standby sites each consist of:

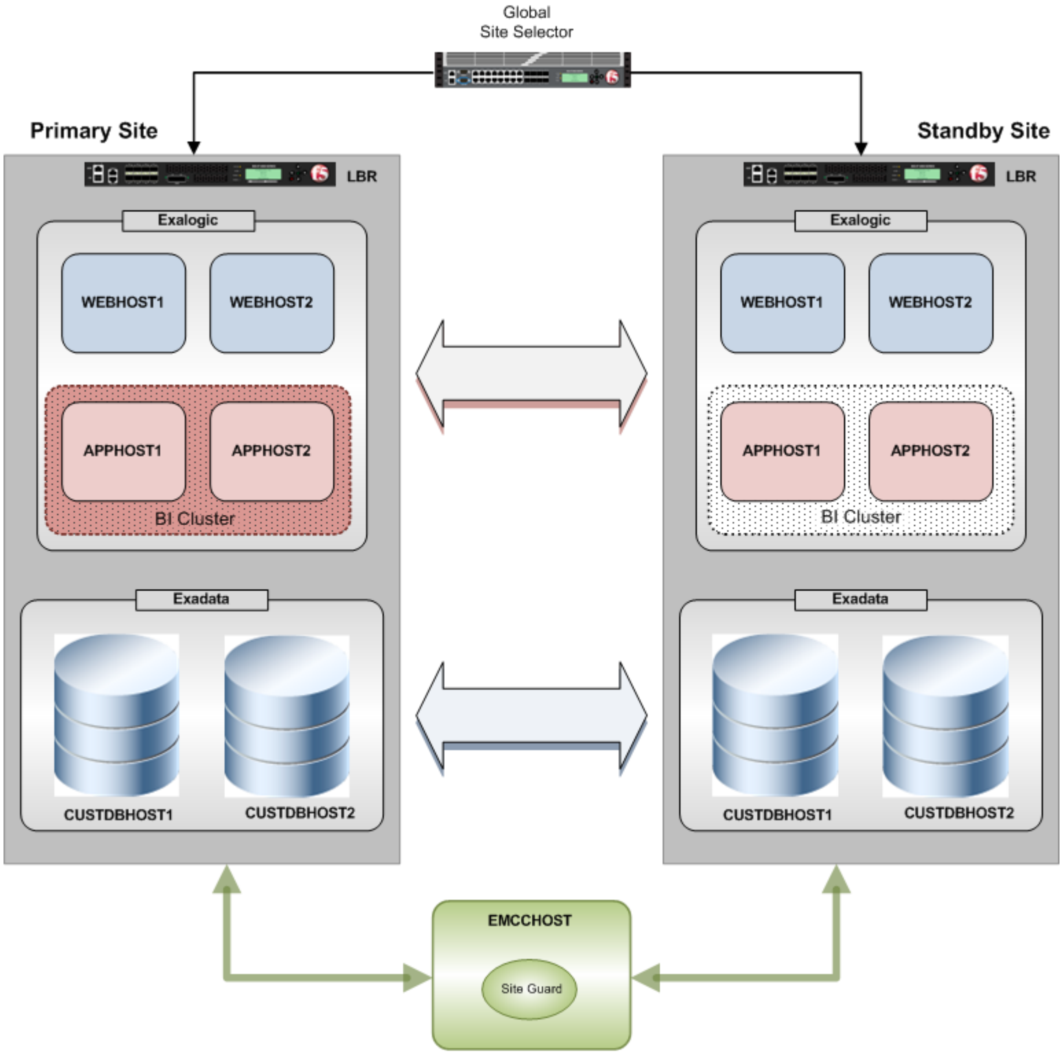
1. Two Oracle HTTP Servers running on Oracle Exalogic. (webhost1, webhost2)
2. One Oracle Weblogic Administration Server running on Oracle Exalogic. (apphost1)
3. Two Oracle Weblogic Managed Servers and OPMN-managed components running on Oracle Exalogic. (apphost1, apphost2).
4. One two node Oracle RAC database running on an Oracle Exadata Database machine for application data. (custdbhost1, custdbhost2)
5. The binaries and configuration files for the Oracle HTTP Server and Oracle Weblogic Server were installed on the shared storage in the Exalogic machine.

In addition to the site-specific hosts above, there is one stand-alone server (emcchost) running Oracle Enterprise Manager Cloud Control with Oracle Site Guard plug-in that is used to co-manage both sites.

In the deployment used in this paper, all the hosts running on Exalogic (namely, webhosts and apphosts) were vServers (virtual machines); however, these hosts could also be deployed on physical servers in the Exalogic machine.

Oracle Traffic Director (OTD) may also be deployed instead of, or in addition to Oracle HTTP Server. Oracle Site Guard scripts for switchover of Oracle Traffic Director components, are provided in the Appendix.

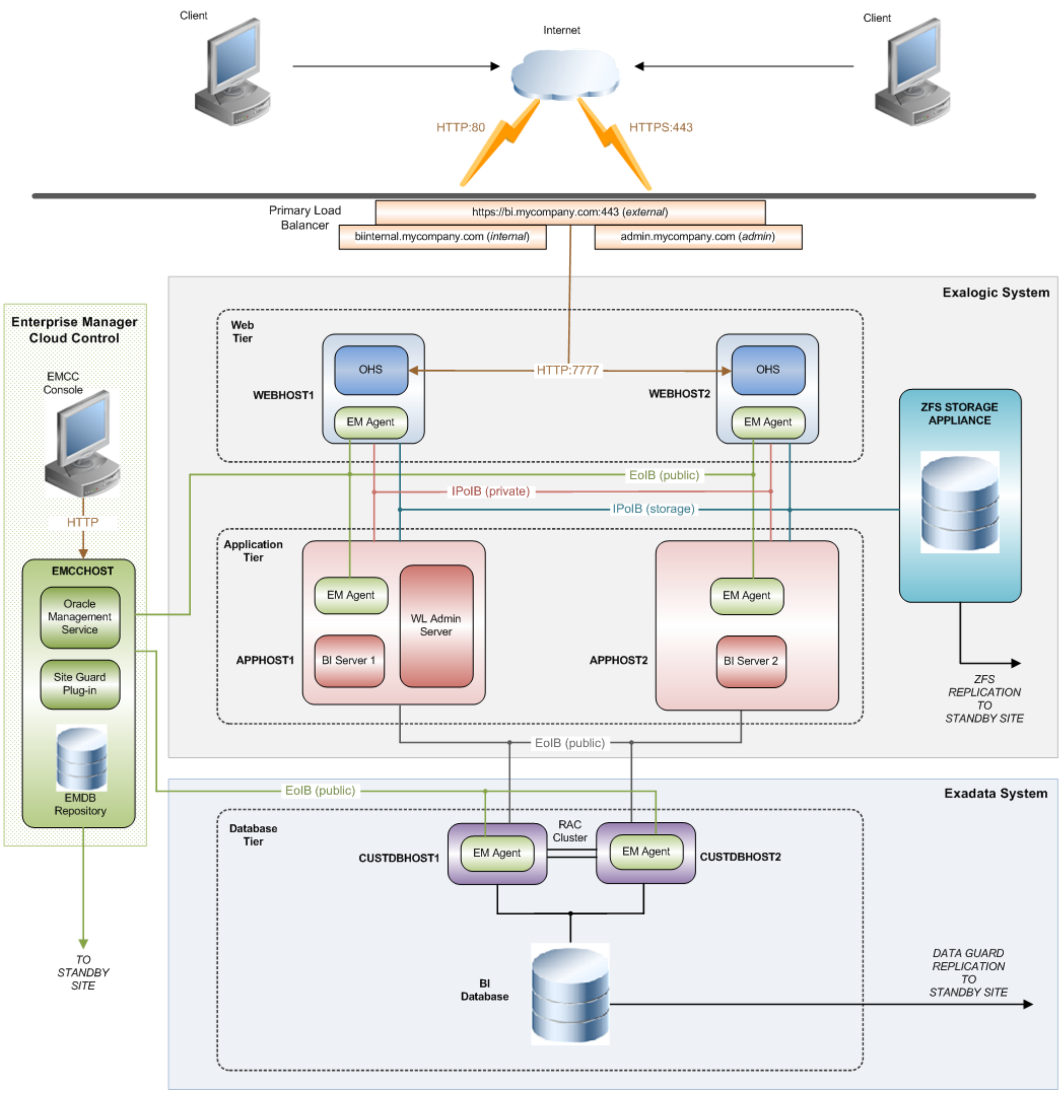
The diagram below shows how the hosts are deployed at each site.



Detailed Site Topology

The figure below shows additional details in the topology at the primary site. The standby site topology is not depicted because it is a symmetrical mirror image of the primary site topology (with the exception of Enterprise Manager Cloud Control, which co-manages both sites).

Although the recommended best-practice is to connect the Exalogic and Exadata systems using InfiniBand and leverage the higher performance available through the Infiniband fabric, this particular deployment used Ethernet-over-InfiniBand (EoIB) communications between the Exalogic and Exadata systems.



Hardware

Oracle Exalogic Elastic Cloud X2-2 and X3-2

For this deployment, an Oracle Exalogic X2-2 machine is used for the Primary site, and an Oracle Exalogic X3-2 machine is used for the Standby site. At both sites, the Web and Application servers are provisioned as vServers from a Virtual Data Center (vDC) hosted on the Exalogic machines. Each vServer has interfaces on the following networks:

1. A public (Ethernet-over-Infiniband) network used for data center connectivity.
2. A private (InfiniBand-based) network used for communication with other Web and Application vServers hosted in the Exalogic machine.
3. A private (InfiniBand-based) network used for access to the ZFS storage appliance in the Exalogic machine

Oracle Exadata X3-2

At each site, the database is deployed in an Exadata quarter-rack configuration with each deployment consisting of two database servers (compute nodes) and three storage servers (cell nodes). The Exadata database and storage servers are configured to communicate over the Exadata machine's internal InfiniBand fabric.

Oracle Enterprise Manager

For this paper, Oracle Enterprise Manager is deployed at a third site on a virtual server running Oracle Linux Server 6.2. The Oracle Enterprise Manager Plug-in for Oracle Fusion Middleware is installed. This plug-in suite includes the Oracle Site Guard Plug-in.

The Oracle Enterprise Management Agent is installed on all the monitored hosts at the primary and standby sites. This includes webhosts, apphosts, and dbhosts. The Management Agent is installed on each host from the Enterprise Manager GUI. Refer to the **Oracle Enterprise Manager Cloud Control Basic Installation Guide** in the Oracle Enterprise Manager Cloud Control Documentation Library for details on installing the Management Agent.

Web Hosts

Primary Site

VSERVER HOST NAME	PUBLIC EOIB IP ADDRESS	SERVER IPOIB IP ADDRESS	STORAGE IPOIB IP ADDRESS	COMMENT
elprimwebvm1.mycompany.com	10.133.49.15	192.168.0.33	10.196.32.48	Primary webhost1

elprimwebvm2.mycompany.com	10.133.49.16	192.168.0.34	10.196.32.49	Primary webhost2

Standby Site

VSERVER HOST NAME	PUBLIC EOIB IP ADDRESS	SERVER IPOIB IP ADDRESS	STORAGE IPOIB IP ADDRESS	COMMENT
elstbywebvm1.mycompany.com	10.133.235.17	192.168.0.22	172.27.8.222	Standby webhost1
elstbywebvm2.mycompany.com	10.133.235.18	192.168.0.20	172.27.8.223	Standby webhost2

Application Hosts

Primary Site

VSERVER HOST NAME	PUBLIC EOIB IP ADDRESS	SERVER IPOIB IP ADDRESS	STORAGE IPOIB IP ADDRESS	SERVER IPOIB HOST NAME (ALIAS)	COMMENT
elprimappvm1.mycompany.com	10.133.49.17	192.168.0.35	10.196.32.29	elprimappvm1-priv	Primary apphost1
elprimappvm2.mycompany.com	10.133.49.18	192.168.0.36	10.196.32.28	elprimappvm2-priv	Primary apphost2

Standby Site

VSERVER HOST NAME	PUBLIC EOIB IP ADDRESS	SERVER IPOIB IP ADDRESS	STORAGE IPOIB IP ADDRESS	SERVER IPOIB HOST NAME (ALIAS)	COMMENT
elstbyappvm1.mycompany.com	10.133.235.19	192.168.0.23	172.27.7.52	elstbyappvm1-priv	Standby apphost1
elstbyappvm2.mycompany.com	10.133.235.20	192.168.0.14	172.27.7.51	elstbyappvm2-priv	Standby apphost2

Sun ZFS Storage 7320 Appliance

Primary Site

STORAGE NODE HOST NAME	PUBLIC EOIB IP ADDRESS	STORAGE IPOIB IP ADDRESS (VIRTUAL)	STORAGE IPOIB HOST NAME (ALIAS)	COMMENT
elprimstor1.mycompany.com	10.133.41.68	10.196.32.5	elprimstor-ib	Active-Passive cluster
elprimstor2.mycompany.com	10.133.41.69			

Standby Site

STORAGE NODE HOST NAME	PUBLIC EOIB IP ADDRESS	STORAGE IPOIB IP ADDRESS (VIRTUAL)	STORAGE IPOIB HOST NAME (ALIAS)	COMMENT
elstbystor1.mycompany.com	10.133.47.68	172.27.0.5	elstbystor-ib	Active-Passive cluster
elstbystor2.mycompany.com	10.133.47.69			

Oracle Exadata Database Machine X2-2

Primary Site

COMPUTE NODE NAME	PUBLIC EOIB IP ADDRESS	SERVER IPOIB IP ADDRESS	SERVER IPOIB HOST NAME (ALIAS)
edprimdb1.mycompany.com	10.133.40.73	192.168.10.102	edprimdb1-priv
edprimdb2.mycompany.com	10.133.40.74	192.168.10.103	edprimdb2-priv
edprimcel1.mycompany.com	10.133.40.82	192.168.10.111	edprimcel1-priv
edprimcel2.mycompany.com	10.133.40.83	192.168.10.112	edprimcel2-priv
edprimcel3.mycompany.com	10.133.40.84	192.168.10.113	edprimcel3-priv

Standby Site

COMPUTE NODE NAME	PUBLIC EOIB IP ADDRESS	SERVER IPOIB IP ADDRESS	SERVER IPOIB HOST NAME (ALIAS)
edstbydb1.mycompany.com	10.133.40.25	192.168.40.25	edstbydb1-priv
edstbydb2.mycompany.com	10.133.40.26	192.168.40.26	edstbydb2-priv

edstbycel1.mycompany.com	10.133.40.36	192.168.40.36	edstbycel1-priv
edstbycel2.mycompany.com	10.133.40.37	192.168.40.37	edstbycel2-priv
edstbycel3.mycompany.com	10.133.40.38	192.168.40.38	edstbycel3-priv

Software

The following products were used to test the deployment in this paper. No additional patches were required.

- Oracle HTTP Server 11.1.1.7
- Oracle WebLogic Server 10.3.6
- Oracle Business Intelligence 11.1.1.7
- Oracle Database Enterprise Edition 11.2.0.3
- Oracle Enterprise Manager Cloud Control 12.1.0.3
- Oracle Enterprise Manager Plug-in for Oracle Fusion Middleware 12.1.0.4 (this includes the Oracle Site Guard Plug-in).

Network

Virtual IP Addresses - Private InfiniBand Network

Primary Site

VIRTUAL HOST NAME	SERVER IPOIB IP ADDRESS	COMMENT
adminvhn.mycompany.com	192.168.0.40	Admin Server Listen Address
apphost1vhn1.mycompany.com	192.168.0.41	Managed Server 1 Listen Address
apphost2vhn1.mycompany.com	192.168.0.42	Managed Server 2 Listen Address
edprimdb1-ibvip.mycompany.com	192.168.10.102	Database Host1 VIP on InfiniBand Network
edprimdb2-ibvip.mycompany.com	192.168.10.103	Database Host2 VIP on InfiniBand Network

Standby Site

VIRTUAL HOST NAME	SERVER IPOIB IP ADDRESS	COMMENT
adminvhn.mycompany.com	192.168.0.43	Admin Server Listen Address
apphost1vhn1.mycompany.com	192.168.0.44	Managed Server 1 Listen Address
apphost2vhn1.mycompany.com	192.168.0.45	Managed Server 2 Listen Address
edstbydb1-ibvip.mycompany.com	192.168.40.25	Database Host1 VIP on InfiniBand Network
edstbydb1-ibvip.mycompany.com	192.168.40.26	Database Host2 VIP on InfiniBand Network

Virtual IP Addresses - Client Access Network

Primary Site

VIRTUAL HOST NAME	CLIENT ACCESS IP ADDRESS	COMMENT
edprimdb1-vip.mycompany.com	10.133.56.69	Primary Database Host1 VIP
edprimdb2-vip.mycompany.com	10.133.56.70	Primary Database Host2 VIP
edprimdb-scan.mycompany.com	10.133.56.78 10.133.56.79 10.133.56.80	Primary Database SCAN address

Standby Site

VIRTUAL HOST NAME	CLIENT ACCESS IP ADDRESS	COMMENT
edstbydb1-vip.mycompany.com	10.133.56.42	Standby Database Host1 VIP
edstbydb2-vip.mycompany.com	10.133.56.43	Standby Database Host2 VIP
edstbydb-scan.mycompany.com	10.133.56.53 10.133.56.54 10.133.56.55	Standby Database SCAN address

Storage Replication Channel

Primary Site

HOST NAME	IP ADDRESS	COMMENT
elprimrepl.mycompany.com	10.133.57.148	Primary Site Replication Channel

Standby Site

HOST NAME	IP ADDRESS	COMMENT
elstbyrepl.mycompany.com	10.133.47.109	Standby Site Replication Channel

Load Balancers

The following virtual IP addresses are configured on the load balancer for this paper

VIRTUAL HOST NAME	IP ADDRESS	COMMET
bi.mycompany.com	144.25.145.19	VIP for External Client Traffic
biinternal.mycompany.com	144.25.145.20	VIP for Internal Client Traffic
admin.mycompany.com	144.25.145.9	VIP for WLS Administration Traffic

Prerequisites

Storage Configuration

The storage layout used in this paper differs slightly from the one recommended in the Oracle Exalogic Enterprise Deployment Guide. Depending on the Oracle Fusion Middleware Components, the applications, the access policies, the replication groups and other requirements, alternative layouts are possible as well.

Web Tier

1. Create a Project for the Oracle HTTP server product binaries and configuration. For example: **OHS**. All shares in the project inherit the properties from the parent project.
2. In this project, create two shares for each webhost: one for the Oracle Home containing product binaries, and the other for Oracle Instance.

Application Tier

1. Create a Project for the Oracle product binaries in the application tier. For example: **MW_Binaries**. The shares in this project inherit properties from the parent project.
    a. Create two different shares (e.g., **mw_home1** and **mw_home2**), under this project. Each of the shares will be used for a Middleware Home that contains product binaries.
    b. Using two different shares for redundant Middleware Homes is a MAA best practice recommendation and provides, Maximum Availability, zero downtime rolling patching and upgrades and isolates failures on the shares.
    c. Additional servers (when scaling out or up) of the same type can use either one of these two locations without requiring more installations.
2. Create a second Project for the configuration files and data. For example: **Configuration**. The shares in this project inherit properties from the parent project.
    a. Create a share for the Administration Server domain home. (e.g., **aserver**)
    b. For each managed server, create a separate share (e.g., **mserver*N***)
    c. Create a share for the BI cluster information (e.g., **bi_cluster**)
    d. For each BI instance, create a separate share (e.g., **biinstance*N***)

Creating Projects and Shares on the Shared Storage

Primary Site

Project Name: MW_Binaries

PROPERTY NAME	PROPERTY VALUE	COMMENTS
Quota	100 GB	Quota for the Project, including snapshots. The quota should be allocated based on your requirements
Mount Point	/export/binaries	
All other settings	Default	
Share Name	mw_home1	• Share mount point: /export/binaries/mw_home1 • Mounted on apphost1 • Contains Oracle Fusion Middleware binaries
Share Name	mw_home2	• Share mount point: /export/binaries/mw_home2 • Mounted on apphost2 • Contains Oracle Fusion Middleware binaries

Project Name: Configuration

PROPERTY NAME	PROPERTY VALUE	COMMENTS
Quota	500 GB	Quota for the Project, including snapshots. The quota should be allocated based on your requirements
Mount Point	/export/config	
All other settings	Default	
Share Name	bi_cluster	• Share mount point: /export/config/bi_domain/bi_cluster • Mounted on apphost1, apphost2 • Shared location for BI cluster data, such as JMS and Transaction Log persistent stores
Share Name	aserver	• Share mount point: /export/config/bi_domain/aserver • Mounted on apphost1 (or on apphost2 on a failover) • Contains the domain configuration for the WebLogic Admin Server
Share Name	mserver1	• Share mount point: /export/config/bi_domain/mserver1 • Mounted on apphost1 • Mount point for domain configuration for WebLogic Managed 1
Share Name	mserver2	• Share mount point: /export/config/bi_domain/mserver2 • Mounted on apphost2 • Mount point for domain configuration WebLogic Managed Server 2
Share Name	biinstance1	• Share mount point: /export/config/instances/biinstance1

		• Mounted on apphost1 • Mount point for instance data for bi_server1
Share Name	biinstance2	• Share mount point: /export/config/instances/biinstance2 • Mounted on apphost2 • Mount point for instance data for bi_server2

Project Name: OHS

PROPERTY NAME	PROPERTY VALUE	COMMENTS
Quota	200 GB	Quota for the Project, including snapshots
Mount Point	/export/ohs	
All other settings	Default	
Share Name	admin1	• Share mount point: /export/ohs/admin1 • Mounted on webhost1 • Contains Oracle HTTP instance configuration
Share Name	admin2	• Share mount point: /export/ohs/admin2 • Mounted on webhost2 • Contains Oracle HTTP Server instance configuration
Share Name	fmw1	• Share mount point: /export/ohs/fmw1 • Mounted on webhost1 • Contains Oracle HTTP Server binaries
Share Name	fmw2	• Share mount point: /export/ohs/fmw2 • Mounted on webhost2 • Contains Oracle HTTP Server binaries

Configuring the Storage Replication Channel

A **storage replication channel** is a network channel that is dedicated specifically to replication traffic between the Sun ZFS Storage 7320 appliance at the primary site and the standby site. The storage replication channel must be configured at both the primary site and standby site before configuring remote replication.

For details on how to configure the storage replication channel, follow the instructions in the **Sun ZFS Storage System Administration Guide**.

Configuring Remote Replication Targets

The Sun ZFS Storage 7320 appliance supports replication of projects and shares from a source appliance to a number of target appliances manually, on a schedule, or continuously. The replication includes both data and metadata. This is typically one-time setup that can be through the GUI or the CLI.

This section details the steps on configuring the remote replication targets using the GUI. Follow the steps below to configure the storage replication channel. All these steps must be completed at both the primary site and the standby sites

1. Open the GUI for the storage appliance.
2. Navigate to **Configuration → Service** to bring up the Services screen
3. Under the **Data Services** table, click on the **Remote Replication** link to bring up the **Remote Replication** Screen
4. Setup the replication target as follows: Click the **+** next to the **Targets** table to bring up the **Add Replication Target** screen. Enter the following details:
    a. **Name**: Enter the name for the target. For example: **dr-repl-channel**
    b. **Hostname**: Enter the IP address for the Target appliance. This is the IP address of the storage replication channel. For example: 10.133.47.109**.**

       Note:

       - On the primary site, provide the IP address of the storage replication channel of the standby site as the target.
       - On the standby site, provide the IP address of the storage replication channel of the primary site as the target

    c. **Root Password**: Enter the root password for the target appliance.
    d. Click **Add** to add the replication target

At this point the replication configuration has been set up between the targets.

Host Setup

Hostnames and Aliases

In a disaster recovery topology, the primary site host names must resolve to the IP addresses of the corresponding peer systems at the standby site. For the Exalogic topology used in this paper, this aliasing is only required for the private InfiniBand network. This can be set up by creating aliases for hostnames in the /etc/hosts file. Create hostname aliases for all the hosts on the primary and standby sites by creating the entries shown in the table below

Web Tier

Primary Site: Web Host Alias

IP ADDRESS	NETWORK NAME	HOSTNAME ALIAS
10.133.49.15	elprimwebvm1.mycompany.com	webhost1.mycompany.com
10.133.49.16	elprimwebvm2.mycompany.com	webhost2.mycompany.com

Standby Site: Web Host Alias

IP ADDRESS	NETWORK NAME	HOSTNAME ALIAS
10.133.235.17	elstbywebvm1.mycompany.com	webhost1.mycompany.com
10.133.235.18	elstbywebvm2.mycompany.com	webhost2.mycompany.com

Application Tier

Primary Site: Hostname Aliases

IP ADDRESS	NETWORK NAME	HOSTNAME ALIAS
10.133.49.17	elprimappvm1.mycompany.com	None
10.133.49.18	elprimappvm2.mycompany.com	None
192.168.0.35	elprimappvm1-priv.mycompany.com	apphost1.mycompany.com
192.168.0.36	elprimappvm2-priv mycompany.com	apphost1.mycompany.com

Primary Site: InfiniBand Network VIPs

INFINIBAND IP ADDRESS	VIRTUAL HOST NAME	HOSTNAME ALIAS
192.168.0.40	adminvhn.mycompany.com	None
192.168.0.41	apphost1vhn1.mycompany.com	None
192.168.0.42	apphost2vhn1.mycompany.com	None

Standby Site: Hostname Aliases

IP ADDRESS	NETWORK NAME	HOSTNAME ALIAS
10.133.235.19	elstbyappvm1.mycompany.com	None
10.133.235.20	elstbyappvm2.mycompany.com	None
192.168.0.23	elstbyappvm1-priv.mycompany.com	apphost1.mycompany.com
192.168.0.14	elstbyappvm2-priv mycompany.com	apphost1.mycompany.com

Standby Site: InfiniBand Network VIPs

INFINIBAND IP ADDRESS	VIRTUAL HOST NAME	HOSTNAME ALIAS
192.168.0.43	adminvhn.mycompany.com	None
192.168.0.44	apphost1vhn1.mycompany.com	None
192.168.0.45	apphost2vhn1.mycompany.com	None

Database Tier

Primary Site: InfiniBand Network Database VIPs

INFINIBAND IP ADDRESS	VIRTUAL HOST NAME	HOSTNAME ALIAS
192.168.10.102	edprimdb1-ibvip.mycompany.com	None
192.168.10.103	edprimdb2-ibvip.mycompany.com	None

Standby Site: InfiniBand Network Database VIPs

INFINIBAND IP ADDRESS	VIRTUAL HOST NAME	HOSTNAME ALIAS
192.168.40.25	edstbydb1-ibvip.mycompany.com	None
192.168.40.26	edstbydb1-ibvip.mycompany.com	None

Mount Points

Web Tier

Primary Site

HOSTNAME	APPLIANCE MOUNT POINT	HOST MOUNT POINT	COMMENT
elprimwebvm1	elprimstor-ib1:/export/ohs/admin1	/u01/app/oracle/admin	OHS Instance Data
	elprimstor-ib1:/export/ohs/fmw1	/u01/app/oracle/product/fmw	OHS Binaries
elprimwebvm2	elprimstor-ib1:/export/ohs/admin2	/u01/app/oracle/admin	OHS Instance Data
	elprimstor-ib1:/export/ohs/fmw2	/u01/app/oracle/product/fmw	OHS Binaries

Standby Site

HOSTNAME	APPLIANCE MOUNT POINT	HOST MOUNT POINT	COMMENT
elstbywebvm1	elstbystor-ib1:/export/ohs/admin1	/u01/app/oracle/admin	OHS Instance Data
	elstbystor-ib1:/export/ohs/fmw1	/u01/app/oracle/product/fmw	OHS Binaries
elstbywebvm2	elstbystor-ib1:/export/ohs/admin2	/u01/app/oracle/admin	OHS Instance Data
	elstbystor-ib1:/export/ohs/fmw2	/u01/app/oracle/product/fmw	OHS Binaries

Application Tier

Primary Site

HOSTNAME	APPLIANCE MOUNT POINT	HOST MOUNT POINT	COMMENT
elprimappvm1	elprimstor-ib1: /export/binaries/mw_home1	/u01/app/oracle/product/fmw	MW Home
	elprimstor-ib1: /export/config/bi_domain/bi_cluster	/u01/app/oracle/admin/bi_domain/bi_cluster	BI Cluster Data
	elprimstor-ib1: /export/admin/bi_domain/aserver	/u01/app/oracle/admin/bi_domain/aserver	Admin Server (only mounted on one apphost at a time)
	elprimstor-ib1: /export/admin/bi_domain/mserver1	/u01/app/oracle/admin/bi_domain/mserver	Managed Server
	elprimstor-ib1: /export/admin/instances/biinstance1	/u01/app/oracle/admin/instances/instance1	BI Instance
elprimappvm2	elprimstor-ib1: /export/binaries/mw_home2	/u01/app/oracle/product/fmw	MW Home
	elprimstor-ib1: /export/config/bi_domain/bi_cluster	/u01/app/oracle/admin/bi_domain/bi_cluster	BI Cluster Data
	elprimstor-ib1: /export/admin/bi_domain/aserver	/u01/app/oracle/admin/bi_domain/aserver	Admin Server (only mounted on one apphost at a time)
	elprimstor-ib1: /export/admin/bi_domain/mserver2	/u01/app/oracle/admin/bi_domain/mserver	Managed Server
	elprimstor-ib1: /export/admin/instances/biinstance2	/u01/app/oracle/admin/instances/instance1	BI Instance

Standby Site

HOSTNAME	APPLIANCE MOUNT POINT	HOST MOUNT POINT	COMMENT
elstbyappvm1	elstbystor-ib1: /export/binaries/mw_home1	/u01/app/oracle/product/fmw	MW Home
	elstbystor-ib1: /export/config/bi_domain/bi_cluster	/u01/app/oracle/admin/bi_domain/bi_cluster	BI Cluster Data
	elstbystor-ib1: /export/exsg/admin/bi_domain/aserver	/u01/app/oracle/admin/bi_domain/aserver	Admin Server (only mounted on one apphost at a time)
	elstbystor-ib1: /export/exsg/admin/bi_domain/mserver1	/u01/app/oracle/admin/bi_domain/mserver	Managed Server
	elstbystor-ib1: /export/exsg/admin/instances/biinstance1	/u01/app/oracle/admin/instances/instance1	BI Instance
elstbyappvm2	elstbystor-ib1: /export/binaries/mw_home2	/u01/app/oracle/product/fmw	MW Home
	elstbystor-ib1: /export/config/bi_domain/bi_cluster	/u01/app/oracle/admin/bi_domain/bi_cluster	BI Cluster Data
	elstbystor-ib1: /export/exsg/admin/bi_domain/aserver	/u01/app/oracle/admin/bi_domain/aserver	Admin Server (only mounted on one apphost at a time)
	elstbystor-ib1: /export/exsg/admin/bi_domain/mserver2	/u01/app/oracle/admin/bi_domain/mserver	Managed Server
	elstbystor-ib1: /export/exsg/admin/instances/biinstance2	/u01/app/oracle/admin/instances/instance1	BI Instance

Client Access Network Configuration

The client access network connects the compute nodes in an Exalogic machine to the existing corporate network through the Sun Network QDR InfiniBand Gateway Switch. The Sun Network QDR InfiniBand Gateway Switches are connected to a 10 Gigabit Network switch to provide the Ethernet over InfiniBand (EoIB) connectivity.

Ensure that the client access network has been configured. Refer to the **Oracle Fusion Middleware Exalogic Machine Owner's Guide** for the configuring the Client Access Network.

Cabling the Exalogic and Exadata Database Machines over InfiniBand

Ensure that the Exalogic machine and the Exadata Database machine on each site are connected to each other over InfiniBand. Refer to the **Oracle Exalogic Multirack Cabling Guide** for the procedure to connect an Exalogic machine with an Exadata Database machine.

Setup and Configuration Flow

The steps below provide the recommended setup and configuration flow for a two-site disaster recovery deployment protected by Oracle Site Guard. This is the configuration process that was used for the deployment in this paper.

1. Set up the primary site as described in the Primary Site Deployment section. Ensure that the primary site is functional.

2. Deploy Oracle Enterprise Manager with Oracle Site Guard as described in the Oracle Enterprise Manager and Site Guard section.

3. Using the instructions in Oracle Site Guard Pre-requisites for Each Site:

    a. Discover targets on the primary site as described in the ***Discover Targets*** section.

    b. Create a generic system for the primary site as described in the ***Create a Generic System*** section.

    Steps 3-a. and 3-b. above are optional but recommended. Discovering targets and adding them to a generic system facilitates monitoring of the primary site using Oracle Enterprise Manager.

Note: At this point the primary site will be functional and monitored by Oracle Enterprise Manager. The remaining steps below relate to setting up a standby site and configuring disaster recovery operations. This can be accomplished at a later date, and without impacting operations at the primary site.

4. Instantiate and validate the standby site as described in Standby Site Deployment and Validation. Ensure that the standby site is functional and testable, but isolated (not accessible to production traffic). This allows for operations at the standby site without impacting operations at the primary site.

5. For the standby site, perform the four steps given in the Oracle Site Guard Pre-requisites for Each Site section. These steps are:

    a. Discover targets for standby site.

    b. Create a generic system for the standby site.

    c. Create and associate credentials for the standby site.

    d. Create and associate pre/post and storage scripts for the standby site.

6. Using Oracle Enterprise Manager, create Oracle Site Guard operations for starting and stopping the standby site. These “Start Site” and “Stop Site” operations will be used for

fire drill tests at the standby site to validate that the site can be brought up/down successfully.

Refer to the ***Using Oracle Site Guard*** section in the **Oracle Enterprise Manager Lifecycle Management Administrator's Guide** in the Oracle Enterprise Manager Cloud Control Documentation Library, and the Configuring Oracle Site Guard Operations for Disaster Recovery section of this document, for instructions on creating Oracle Site Guard operations.

Important: Before moving on to the next step, verify that running any fire drill tests at the standby site will not inadvertently affect operations at the primary site. For example, actions executed in custom Pre or Post scripts at the standby site could affect the primary site.

7. Using the "Start Site" and "Stop Site" operations created in the previous step, verify that Oracle Site Guard can successfully start and stop operations at the standby site. Note: these start and stop operations only bring up/down the web and application tiers. The Oracle RAC Database at the standby site must be manually started and stopped as required.

8. Stop the standby site as described in Stop the Standby Site after Validation.

9. For the primary site, perform the four steps given in the Oracle Site Guard Pre-requisites for Each Site section. These steps are:

    a. Discover targets for the primary site.

    b. Create a generic system for the primary site.

    Note: Steps 9-a. and 9-b. are required only if they were not performed earlier after the primary site was set up.

    c. Create and associate credentials for the primary site.

    d. Create and associate pre/post and storage scripts for the primary site.

10. Configure and pair the primary and standby sites as described in the ***Configure Sites*** section of Oracle Site Guard Pre-requisites for All Sites. This will change the standby site's role to *standby*. Note: this role change will invalidate the Site Guard start/stop operations created earlier for the standby site.

11. Configure the software library as described in the ***Configure Software Library*** section of Oracle Site Guard Pre-requisites for All Sites.

12. Configure Oracle Site Guard operations for disaster recovery, such as Site Switchover and Site Failover, as described in Configuring Oracle Site Guard Operations for Disaster Recovery.

13. Execute and monitor Oracle Site Guard disaster recovery operations as described in Disaster Recovery Operations.

Site Deployment and Configuration

Primary Site Deployment

When setting up the primary site, the database tier is set up first and the Business Intelligence schemas are populated before setting up the web and applications tiers.

Database Tier

For this paper the customer database is running on an Exadata Database machine in a Quarter Rack configuration. The high level steps for configuring the database tier are given below.

1. Follow the **Oracle Exadata Database Machine Owners Guide** to setup the Exadata Database machine. The Oracle Exadata Storage Server and Oracle Exadata Database Machine Documentation can be found on the Exadata Storage cell under the `/opt/oracle/cell/doc` directory
2. Ensure that Exalogic machine and the Exadata Database machine have been physically cabled as described in the **Oracle Exalogic Machine Multirack Cabling Guide**
3. Ensure that the private InfiniBand networks on the Exalogic machine and the Exadata Database machine are configured to be on the same subnet. Refer to the **Oracle Exalogic Owners Guide** and the **Oracle Exadata Database Machine Owners Guide** for the steps to accomplish this task.
4. Follow the **Oracle Exalogic Enterprise Deployment Guide** to enable the SDP protocol and to configure an additional listener on the InfiniBand network.
5. Ensure that all database traffic from the Exalogic machine to the Exadata Database machine is configured to use the private InfiniBand network. Due to hardware limitations, this is not implemented for the deployment used in this paper.
6. Create a role-based service for the database using *svrctl* and assign the database role as Primary to the service. The Data Guard broker will coordinate with Oracle Clusterware (CRS) to properly fail over role-based services to a new primary database after a Data Guard failover has occurred.
7. Create BI schemas as described in the **Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intelligence.**

Web Tier

The web tier on the primary site consists of two hosts called webhost1 and webhost2. Both hosts are running Oracle HTTP Server. These two webhosts are front ended by a load balancer configured to load balance traffic between webhost1 and webhost2.

Follow the **Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intelligence** to install and configure the Oracle HTTP Server. The high level steps to configure the web tier are below:

1. Ensure that the /etc/hosts file is setup properly on webhost1 and webhost2
2. Ensure that the mount points are properly configured on webhost1 and webhost2
3. On webhost1, install the Oracle HTTP Server binaries to the /u01/app/oracle/product/fmw directory.
4. Specify /u01/app/oracle/admin/web1 on webhost1 (or web2 on webhost2) as the directory for the Instance Home Location.

Application Tier

The application tier on the primary site consists of two hosts, apphost1 and apphost2. Both hosts are running Oracle WebLogic Server.

For this paper, the enterprise topology described in the **Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intelligence** is deployed as one WebLogic Admin Server and two Weblogic Managed Servers running on apphost1 and apphost2.

The table below provides a summary:

HOSTNAME	WEBLOGIC SERVER NAME	CLUSTER NAME	WEBLOGIC SERVER LISTEN ADDRESS
apphost1	Admin Server	None	adminvhn.mycompany.com
	Managed server (bi_server1)	bi_cluster	apphost1vhn1.mycompany.com
apphost2	Managed server (bi_server2)	bi_cluster	apphost2vhn1.mycompany.com

Follow the deployment steps provided in **Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intelligence** to:

1. Install Oracle Weblogic Server and Oracle Business Intelligence binaries
2. Configure an Oracle WebLogic Admin Server and Managed Server on apphost1.
3. Install and configure Oracle Business Intelligence on the first Managed server running on apphost1.
4. Scale out the Business Intelligence deployment to a second Managed Server on apphost2.

At this point the Primary site instantiation should be complete and the Primary site should be operational.

If the Oracle Enterprise Manager and Site Guard deployment that will be used to manage this site is already functional, a target discovery of the Oracle Fusion Middleware farm components and Oracle RAC database instances may be performed at this stage. For details on how to discover targets, refer to the ***Using Oracle Site Guard*** section in the **Oracle Enterprise Manager Lifecycle Management Administrator's Guide** in the Oracle Enterprise Manager Cloud Control Documentation Library, and to the Preparing to Configure Oracle Site Guard for Disaster Recovery section of this document.

Configuring Replication for the Projects and Shares

Replication must be configured on the Sun ZFS Storage 7320 appliance at the primary site before instantiating the standby site. The product binaries and configuration installed/configured on the primary site will then be replicated to the standby site when the primary site storage is replicated to the standby site storage. This avoids the need to perform installation and configuration at the standby site.

Replication can be configured either at the project level or at the share level, however for the deployment used in this paper (and other similar deployments), Oracle strongly recommends that replication be set up at the project level. It is also recommended, that snapshot replication be enabled during configuration.

Follow the steps below to configure replication between the primary site and the standby site.

1. From the GUI, navigate to **Shares → Projects** screen and choose a project or share, then click the Replication.
2. Create a **Replication Target** as follows: Click **+** next to the Actions Table to bring up the **Add Replication Target** screen. Provide the following details.
   a. Choose the target system from the drop-down. Note that only the targets added under the **Services → Remote replication →Targets** are listed in the drop-down. For example: **dr-repl-channel**
   b. Select the name of the pool, by default in the Exalogic machine, there is only one pool
   c. Select the mode of replication. **Scheduled or Continuous**. Oracle recommends selecting the replication mode based on your requirements and the data in the project/share. Refer to the **Oracle MAA Best Practices for Disaster Recovery** section for guidelines
   d. If using the **Scheduled** replication mode, click **+** next to the **Schedule table** to create a schedule.

e. If the replication happens within a data center protected by a firewall, SSL can be disabled to enhance performance.

f. The bandwidth used for replication can be limited based on individual requirements.

g. If snapshots are taken at the source for the replication project or share, the user can choose to include replicating the snapshots.

3. For this paper, **Scheduled** replication is configured as shown in the table below:

PROJECT NAME	SHARE NAME	REPLICATION LEVEL	REPLICATION TYPE	SCHEDULE
OHS	admin1	Project	Scheduled	Every 30 minutes
	admin2			
	fmw1			
	fmw2			
MW_Binaries	mw_home1	Project	Scheduled	Every 30 minutes
	mw_home2			
Configuration	aserver	Project	Scheduled	Every 30 minutes
	bi_cluster			
	mserver1			
	mserver2			
	instance1			
	instance2			

4. If the target is added with Continuous mode of replication, the replication starts immediately.

5. If the Scheduled mode of replication is chosen, then it is recommended to perform a manual update one time if the schedule is expected to occur sometime in the future. This will enable a copy of the binaries and the configuration to be available at the standby site in case the primary site fails before the first scheduled replication occurs.

6. Validate that the replication between the primary site and the standby is configured. To validate that the packages are being received or have already been received. Use the GUI and navigate to **Shares** → **Projects** at the left side frame and then click **Replica**. This will list all the packages that are being received or have been received from primary site.

7. Validate that all the replicas between the primary and standby sites are being replicated as expected. To do this using the GUI: for each replica, click on the replica's name in

the **Projects** frame on the left, and then click on **Replication** in the upper right. Inspect the *Last Sync*, *Last Attempt*, and *Status* attributes.

Standby Site Deployment and Validation

The standby site can be deployed and partially validated without affecting operations at the primary site. No installation and configuration for Oracle Fusion Middleware components is required at the standby site. When the primary site storage is replicated to the standby site storage, the Oracle Fusion Middleware product binaries and configuration installed and configured on the primary site will be replicated at the standby site.

However, software installation and configuration **is required** for the database on the Exadata Database machine at the standby site.

Database Tier

The database tier on the standby site consists of two hosts called custdbhost1 and custdbhost2, running an Oracle database.

For this paper the standby customer database is running on an Exadata Database machine in a Quarter Rack configuration. The high level steps to configure the database tier on the standby site are below:

1. Follow the Oracle Exadata Database Machine Owners Guide to setup the Exadata Database machine.

2. Ensure that Exalogic machine and the Exadata Database machine have been physically cabled as described in the **Oracle Exalogic Machine Multirack Cabling Guide**.

3. Ensure that the private InfiniBand networks on the Exalogic machine and Exadata Database machine are configured to be on the same subnet. Refer to the **Oracle Exalogic Owners Guide** and the **Oracle Exadata Database machine Owners Guide** for the steps to accomplish this task.

4. Follow the **Oracle Exalogic Enterprise Deployment Guide** to enable the SDP protocol and to configure an additional listener on the InfiniBand network.

5. Ensure that all database traffic from the Exalogic machine to the Exadata Database machine is configured to use the private InfiniBand network. Due to hardware limitations, this is not implemented for the deployment used in this paper.

6. Create a role-based service for the database using *svrctl* and assign the database role as Standby to the service. The Data Guard broker will coordinate with Oracle Clusterware (CRS) to properly fail over role-based services to a new primary database after a Data Guard failover has occurred.

Data Guard and Broker Setup

1. The database on the standby site can be setup as a physical standby or a logical standby database. For this paper, the database on the standby site is setup as a physical standby database.
2. Oracle Active Data Guard is not configured for this setup.
3. Oracle Active Data Guard can be configured if custom applications in your topology are designed to leverage the Oracle Active Data Guard technology.
4. The steps for setting up Oracle Data Guard are not covered in this paper. Follow the **Oracle Data Guard Concepts and Administration Guide** and the **Oracle Data Guard Broker Guide** to configure Data Guard and Data Guard Broker between the databases on the primary site and the standby site.
5. For Oracle Data Guard best practices for the Exadata Database machine, please refer to the white paper titled **Oracle Data Guard: Disaster Recovery Best Practices for Exadata Database Machine**.

Initial Storage Snapshot and Clones

To create the initial ZFS storage snapshot of the product binaries and configuration on the standby site, perform a manual replication of the Projects.

1. The manual update must be initiated from the ZFS storage appliance on the primary site. This can be done through the GUI or the CLI.
2. Open the GUI and navigate to the **Shares → Projects** and then click on **Replication** to bring up the Replication screen.
3. Click on the Manual replication icon next to the target to start the Manual update. The status of the update can be viewed under the status column.

On the standby site, validate that the packages have been received. Use the GUI and navigate to **Shares →Projects** at the left side frame and then click **Replica**. This will list all the packages that are being received or have been received from primary site.

Under the Replication Tab for each project, click on the '+' icon to create a clone from the most recently received project snapshot. These newly created clones will be used as local projects at the standby site.

Web Tier

The web tier at the standby site consists of two hosts called webhost1 and webhost2. Both hosts are running Oracle HTTP Server. These two webhosts are front ended by a load balancer configured to load balance traffic between webhost1 and webhost2. Ensure that the /etc/hosts file is setup properly on webhost1 and webhost2.

Application Tier

The application tier on the standby site consists of two hosts called apphost1 and apphost2. Both hosts are running the Oracle WebLogic Server. The application tier at the standby site has the same number of hosts as the primary site. Ensure that the /etc/hosts file is setup properly on apphost1 and apphost2.

Follow these steps to instantiate and validate the standby site:

1. On the ZFS storage appliance at standby site, create clone projects from the Replicas synced from primary site, while leaving the on-going replication of the projects intact. Ensure that the cloned projects are writable.
2. Convert the physical standby database to a snapshot standby database using the following steps
    a. Stop Redo Apply, if it is active.
    b. Ensure that the stand-by database is mounted, but not open.
    c. Ensure that a fast recovery area has been configured. It is not necessary for flashback database to be enabled.
    d. Issue the following SQL statement to perform the conversion.

    ```
    SQL> ALTER DATABASE CONVERT TO SNAPSHOT STANDBY;
    ```

   Note: A snapshot standby database cannot be the target of a switchover or failover. A snapshot standby database must first be converted back into a physical standby database before performing a role transition. For additional details on Snapshot standby databases, refer to the Oracle Data Guard Documentation.
3. Bring the standby database online by issuing the following SQL statement.

   ```
   SQL> ALTER DATABASE OPEN;
   ```

4. On the standby site's apphosts and webhosts, mount the shares from the cloned ZFS projects. Use identical mount points and attributes that were used at the primary site.
5. On the standby site apphosts, manually start the processes for the application server instances. This includes Weblogic admin server, Weblogic managed servers, and OPMN components.
6. On the standby site webhosts, manually start the processes for OHS instances.
7. Validate that the standby site is functional.

The level of validation that can occur at the standby site is partial. It is limited by that fact that the site is not accessible to client traffic, and does not involve exercising all the devices, software, and configuration that a fully operational production site will exercise.

Stop the Standby Site after Validation

After standby site operations have been validated and other activities (such as creating Oracle Enterprise Manager and Site Guard configurations for the site) have been completed, follow these steps to stop the standby site:

1. On the standby site webhosts, manually stop the processes for OHS instances.
2. On the standby site apphosts, manually stop the processes for the application server instances. This includes Weblogic admin server, Weblogic managed servers, and OPMN components.
3. On the standby site's apphosts and webhosts, unmount the shares from the cloned ZFS projects.
4. On the ZFS appliance, explicitly delete all the cloned projects that were created using Replicas from the primary site.
5. Ensure that ZFS replication from the primary site to standby site is functioning as expected.
6. Convert the snapshot standby database to a physical standby database, and bring the database back to a mounted but unopened state. Issue the following SQL statement to perform the conversion.

   ```
   SQL> ALTER DATABASE CONVERT TO PHYSICAL STANDBY;
   ```

   Note: during the period that the standby database is functioning as snapshot standby, redo log shipping continues from the primary site to the standby site however the redo logs are not applied to the standby database. Once the standby database is converted back to a physical standby, the redo logs are applied.
7. Ensure that Data Guard database replication from the primary site to standby site is functioning as expected.

Oracle Site Guard Configuration

Oracle Enterprise Manager and Site Guard

This paper focuses on using the Oracle Site Guard functionality in Oracle Enterprise Manager Cloud Control to configure and automate the disaster recovery process. Before beginning the disaster recovery configuration process using Oracle Site Guard:

- Ensure that Oracle Enterprise Manager Cloud Control is installed and configured as described in the **Oracle Enterprise Manager Cloud Control Basic Installation Guide**.
- Install the Oracle Fusion Middleware Plug-in for Oracle Enterprise Manager. This plug-in suite includes Oracle Site Guard plug-in.
- Install the Oracle Enterprise Manager Management Agents on all servers in the Enterprise Deployment, as described in the **Oracle Enterprise Manager Cloud Control Basic Installation Guide**.
- Ensure that the directory locations where the Management Agents are installed on each server are not replicated to the other site.

Preparing to Configure Oracle Site Guard for Disaster Recovery

Before configuring Oracle Site Guard to automate the disaster recovery process, ensure that all the pre-requisites in this section have been completed.

For additional details on executing each of these steps, refer to the ***Using Oracle Site Guard*** section in the **Oracle Enterprise Manager Lifecycle Management Administrator's Guide** in the Oracle Enterprise Manager Cloud Control Documentation Library.

Note: In the following examples, the label *Site A* is used for the site that will initially be configured as the primary site, and the label *Site B* is used for the initial standby site. These labels are transient in nature (because these are symmetric sites) and over time either site could end up assuming the primary or standby roles.

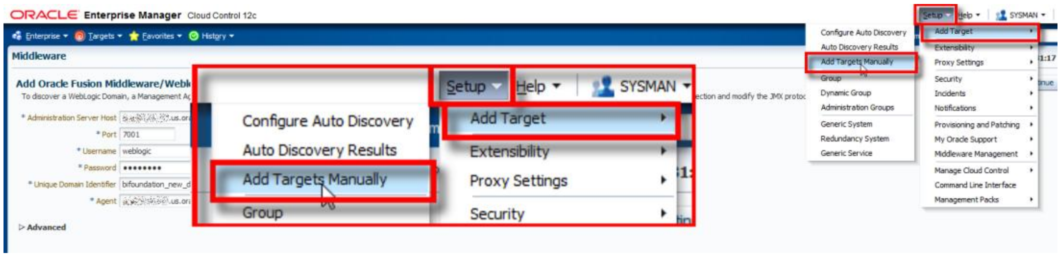
Oracle Site Guard Pre-requisites for Each Site

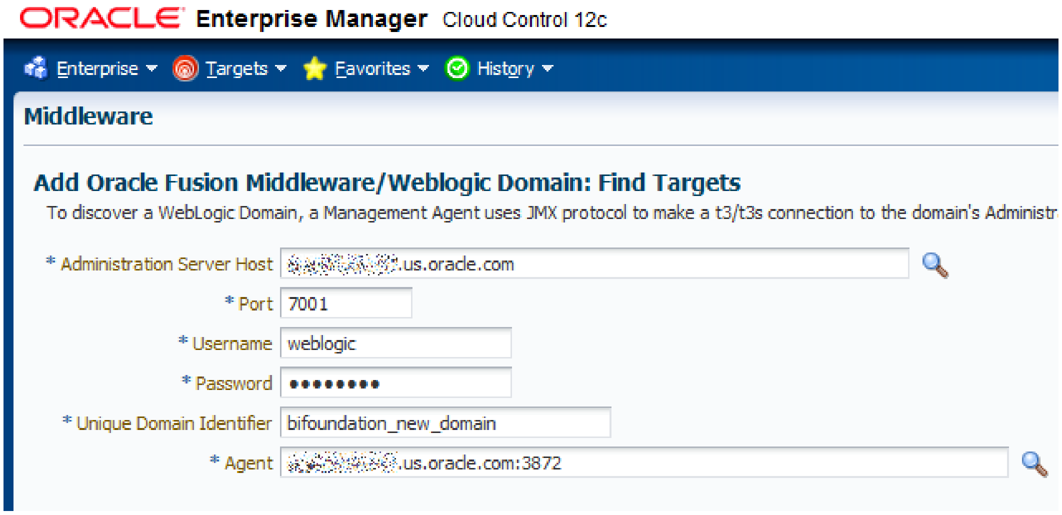
Follow the four steps described below to configure pre-requisites for the primary site. Then, perform a manual switchover to the standby site and repeat the same procedures for the standby site.

1. **Discover Targets**. Perform a discovery of all targets in the Oracle Middleware Fusion farm (the Oracle Business Intelligence Enterprise Deployment). This includes all components of the Fusion Middleware Instance, including the Oracle RAC Database.

In this deployment, target discovery is performed using the Enterprise Management Agent as a proxy to discover WebLogic and BI components on apphost nodes, because the node and the Management agent have access to the public EoIB network, but the WebLogic administration server is not accessible over the public EoIB network.

The example below demonstrates target discovery at the primary site.



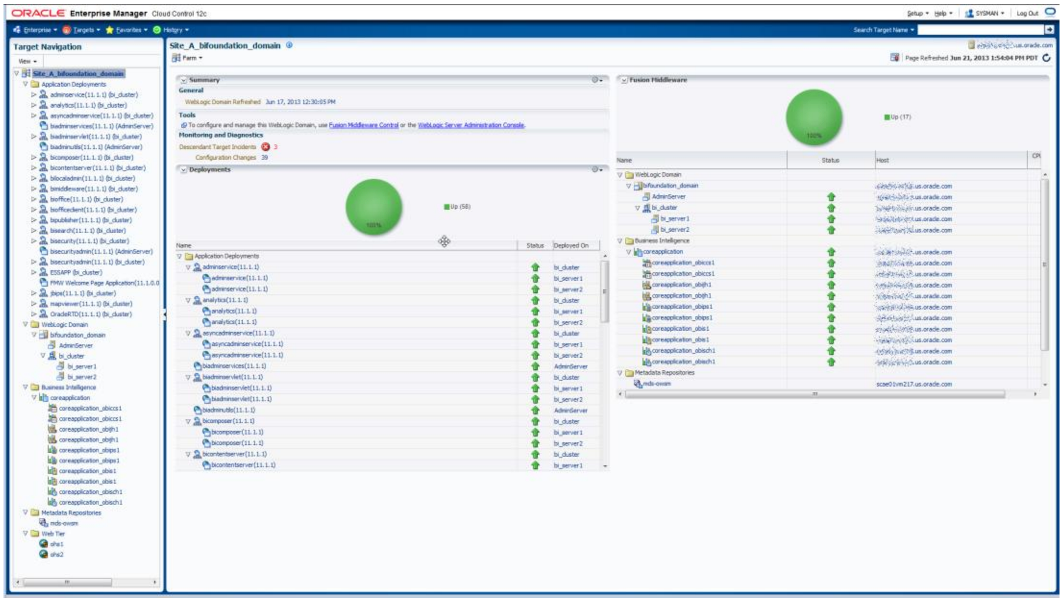


Add Oracle Fusion Middleware/Weblogic Domain: Find Targets

To discover a WebLogic Domain, a Management Agent uses JMX protocol to make a t3/t3s connection to the domain's Administr

* Administration Server Host [redacted].us.oracle.com
* Port 7001
* Username weblogic
* Password ••••••••
* Unique Domain Identifier bifoundation_new_domain
* Agent [redacted].us.oracle.com:3872

The example below shows the different components in an Oracle Fusion Middleware Instance, after discovery is complete.


ORACLE Enterprise Manager Cloud Control 12c
Setup ▾ Help ▾ SYSMAN ▾ Log Out
Enterprise ▾ Targets ▾ Favorites ▾ History ▾
Search Target Name ▾
View ▾
Farm ▾
100%
Up (58)
100%
Up (17)

Target Navigation

- Site_A_bifoundation_domain
  - Application Deployments
    - adminservice(11.1.1) (bi_cluster)
    - analytics(11.1.1) (bi_cluster)
    - asyncadminservice(11.1.1) (bi_cluster)
    - biadminservices(11.1.1) (AdminServer)
    - biadminservlet(11.1.1) (bi_cluster)
    - biadminutils(11.1.1) (AdminServer)
    - bicomposer(11.1.1) (bi_cluster)
    - bicontentserver(11.1.1) (bi_cluster)
    - bilocaladmin(11.1.1) (bi_cluster)
    - bimiddleware(11.1.1) (bi_cluster)
    - bioffice(11.1.1) (bi_cluster)
    - bioffceclient(11.1.1) (bi_cluster)
    - bipublisher(11.1.1) (bi_cluster)
    - bisearch(11.1.1) (bi_cluster)
    - bisecurity(11.1.1) (bi_cluster)
    - bisecurityadmin(11.1.1) (AdminServer)
    - bisecurityadmin(11.1.1) (bi_cluster)
    - ESSAPP (bi_cluster)
    - FMW Welcome Page Application(11.1.0.0
    - jbips(11.1.1) (bi_cluster)
    - mapviewer(11.1.1) (bi_cluster)
    - OracleRTD(11.1.1) (bi_cluster)
  - WebLogic Domain
    - bifoundation_domain
      - AdminServer
      - bi_cluster
        - bi_server1
        - bi_server2
  - Business Intelligence
    - coreapplication
      - coreapplication_obiccs1
      - coreapplication_obiccs1
      - coreapplication_obijh1
      - coreapplication_obijh1
      - coreapplication_obips1
      - coreapplication_obips1
      - coreapplication_obis1
      - coreapplication_obis1
      - coreapplication_obisch1
      - coreapplication_obisch1
  - Metadata Repositories
    - mds-owsm
  - Web Tier
    - ohs1
    - ohs2

Site_A_bifoundation_domain

[redacted].us.oracle.com

Page Refreshed **Jun 21, 2013 1:54:04 PM PDT**

Summary

General

WebLogic Domain Refreshed Jun 17, 2013 12:30:05 PM

Tools

To configure and manage this WebLogic Domain, use Fusion Middleware Control or the WebLogic Server Administration Console.

Monitoring and Diagnostics

Descendant Target Incidents 3

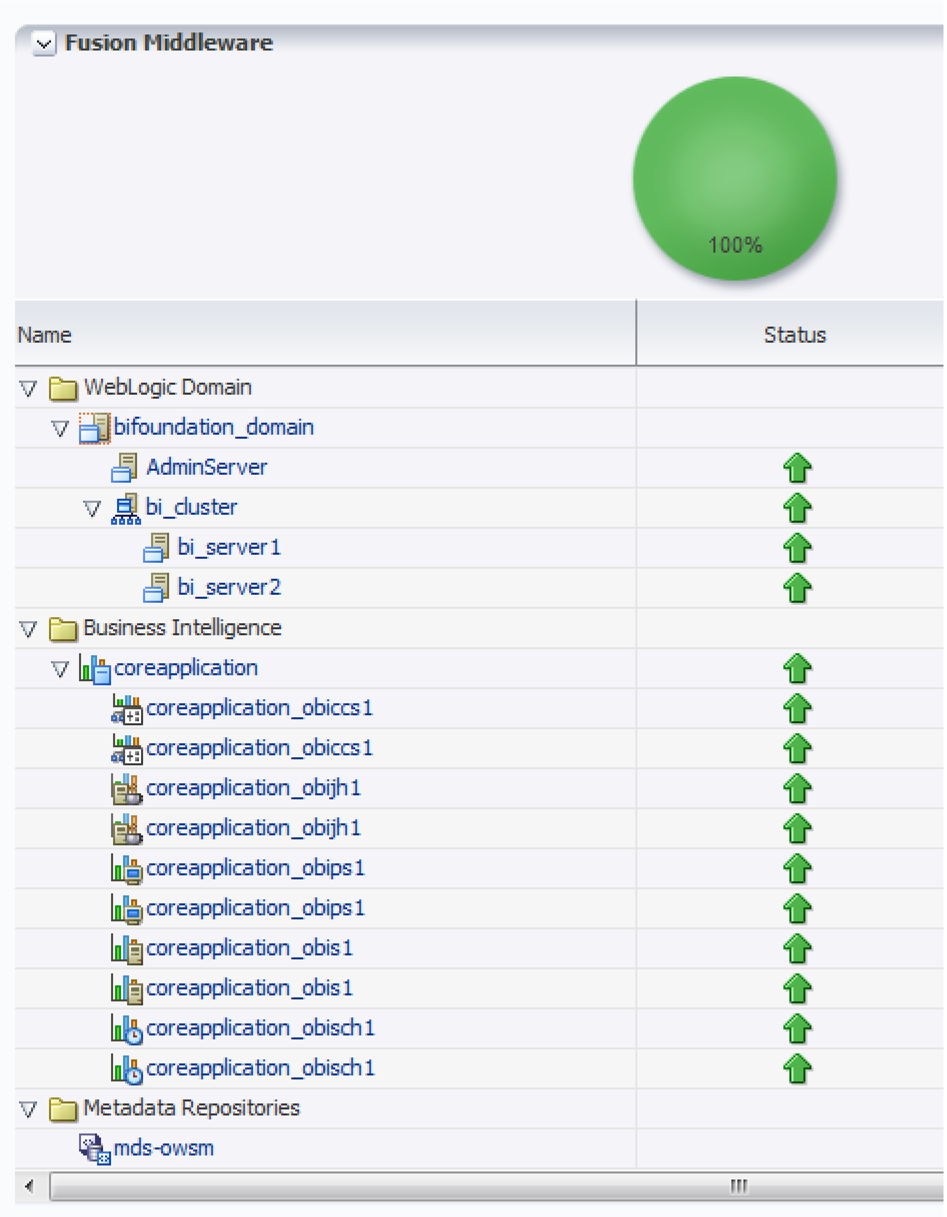
Configuration Changes 39

Deployments

Name	Status	Deployed On
Application Deployments		
adminservice(11.1.1)	⬆	bi_cluster
adminservice(11.1.1)	⬆	bi_server1
adminservice(11.1.1)	⬆	bi_server2
analytics(11.1.1)	⬆	bi_cluster
analytics(11.1.1)	⬆	bi_server1
analytics(11.1.1)	⬆	bi_server2
asyncadminservice(11.1.1)	⬆	bi_cluster
asyncadminservice(11.1.1)	⬆	bi_server1
asyncadminservice(11.1.1)	⬆	bi_server2
biadminservices(11.1.1)	⬆	AdminServer
biadminservlet(11.1.1)	⬆	bi_cluster
biadminservlet(11.1.1)	⬆	bi_server1
biadminservlet(11.1.1)	⬆	bi_server2
biadminutils(11.1.1)	⬆	AdminServer
bicomposer(11.1.1)	⬆	bi_cluster
bicomposer(11.1.1)	⬆	bi_server1
bicomposer(11.1.1)	⬆	bi_server2
bicontentserver(11.1.1)	⬆	bi_cluster
bicontentserver(11.1.1)	⬆	bi_server1

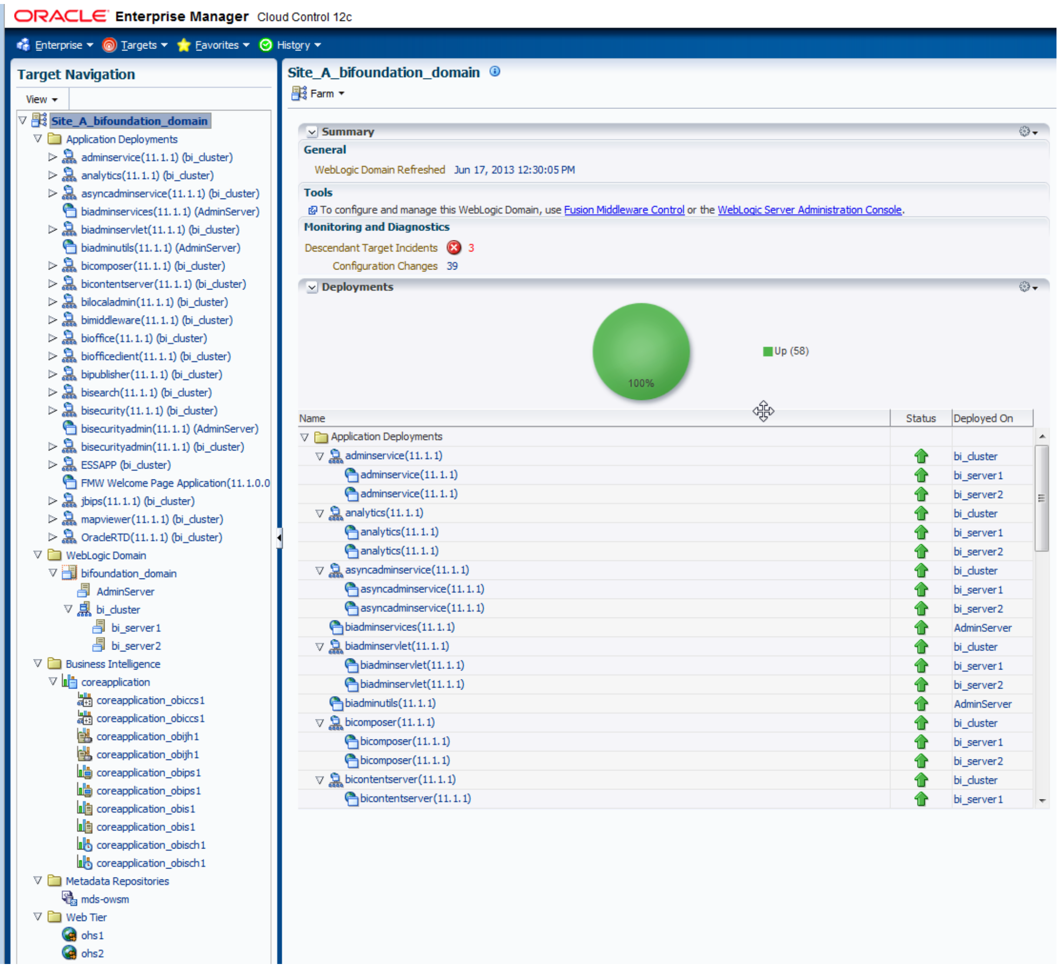
Fusion Middleware

Name	Status	Host	CPU
WebLogic Domain			
bifoundation_domain		[redacted].us.oracle.com	
AdminServer	⬆	[redacted].us.oracle.com	
bi_cluster	⬆	[redacted].us.oracle.com	
bi_server1	⬆	[redacted].us.oracle.com	
bi_server2	⬆	[redacted].us.oracle.com	
Business Intelligence			
coreapplication	⬆	[redacted].us.oracle.com	
coreapplication_obiccs1	⬆	[redacted].us.oracle.com	
coreapplication_obiccs1	⬆	[redacted].us.oracle.com	
coreapplication_obijh1	⬆	[redacted].us.oracle.com	
coreapplication_obijh1	⬆	[redacted].us.oracle.com	
coreapplication_obips1	⬆	[redacted].us.oracle.com	
coreapplication_obips1	⬆	[redacted].us.oracle.com	
coreapplication_obis1	⬆	[redacted].us.oracle.com	
coreapplication_obis1	⬆	[redacted].us.oracle.com	
coreapplication_obisch1	⬆	[redacted].us.oracle.com	
coreapplication_obisch1	⬆	[redacted].us.oracle.com	
Metadata Repositories			
mds-owsm		scae01vm217.us.oracle.com	



Fusion Middleware

Name	Status
WebLogic Domain	
bifoundation_domain	
AdminServer	⇧
bi_cluster	⇧
bi_server1	⇧
bi_server2	⇧
Business Intelligence	
coreapplication	⇧
coreapplication_obiccs1	⇧
coreapplication_obiccs1	⇧
coreapplication_obijh1	⇧
coreapplication_obijh1	⇧
coreapplication_obips1	⇧
coreapplication_obips1	⇧
coreapplication_obis1	⇧
coreapplication_obis1	⇧
coreapplication_obisch1	⇧
coreapplication_obisch1	⇧
Metadata Repositories	
mds-owsm	



- Site_A_bifoundation_domain
  - Application Deployments
    - adminservice(11.1.1) (bi_cluster)
    - analytics(11.1.1) (bi_cluster)
    - asyncadminservice(11.1.1) (bi_cluster)
    - biadminservices(11.1.1) (AdminServer)
    - biadminservlet(11.1.1) (bi_cluster)
    - biadminutils(11.1.1) (AdminServer)
    - bicomposer(11.1.1) (bi_cluster)
    - bicontentserver(11.1.1) (bi_cluster)
    - bilocaladmin(11.1.1) (bi_cluster)
    - bimiddleware(11.1.1) (bi_cluster)
    - bioffice(11.1.1) (bi_cluster)
    - biofficeclient(11.1.1) (bi_cluster)
    - bipublisher(11.1.1) (bi_cluster)
    - bisearch(11.1.1) (bi_cluster)
    - bisecurity(11.1.1) (bi_cluster)
    - bisecurityadmin(11.1.1) (AdminServer)
    - bisecurityadmin(11.1.1) (bi_cluster)
    - ESSAPP (bi_cluster)
    - FMW Welcome Page Application(11.1.0.0
    - jbips(11.1.1) (bi_cluster)
    - mapviewer(11.1.1) (bi_cluster)
    - OracleRTD(11.1.1) (bi_cluster)
  - WebLogic Domain
    - bifoundation_domain
      - AdminServer
      - bi_cluster
        - bi_server1
        - bi_server2
  - Business Intelligence
    - coreapplication
      - coreapplication_obiccs1
      - coreapplication_obiccs1
      - coreapplication_obijh1
      - coreapplication_obijh1
      - coreapplication_obips1
      - coreapplication_obips1
      - coreapplication_obis1
      - coreapplication_obis1
      - coreapplication_obisch1
      - coreapplication_obisch1
  - Metadata Repositories
    - mds-owsm
  - Web Tier
    - ohs1
    - ohs2

Site_A_bifoundation_domain

Summary

General

WebLogic Domain Refreshed Jun 17, 2013 12:30:05 PM

Tools

To configure and manage this WebLogic Domain, use Fusion Middleware Control or the WebLogic Server Administration Console.

Monitoring and Diagnostics

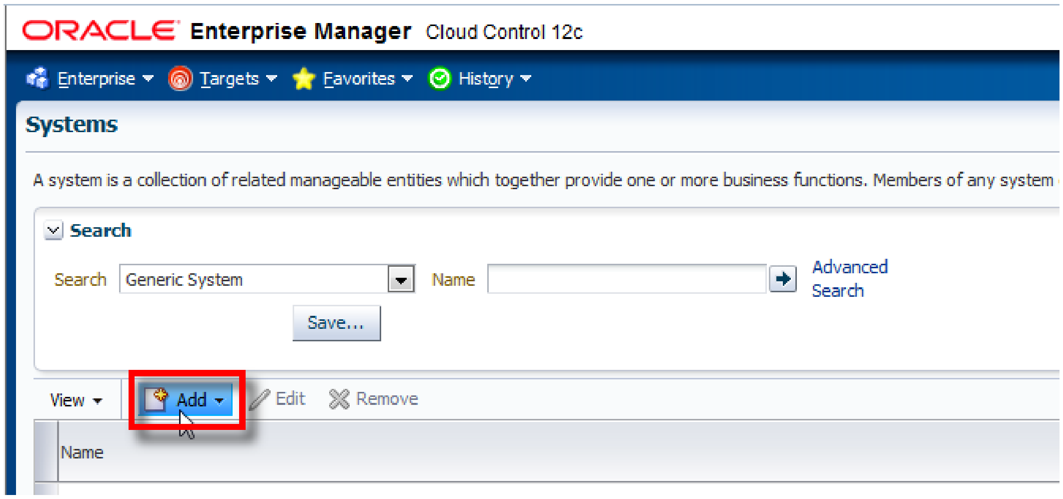
Descendant Target Incidents ✕ 3

Configuration Changes 39

Deployments

Name	Status	Deployed On
Application Deployments		
adminservice(11.1.1)	⬆	bi_cluster
adminservice(11.1.1)	⬆	bi_server1
adminservice(11.1.1)	⬆	bi_server2
analytics(11.1.1)	⬆	bi_cluster
analytics(11.1.1)	⬆	bi_server1
analytics(11.1.1)	⬆	bi_server2
asyncadminservice(11.1.1)	⬆	bi_cluster
asyncadminservice(11.1.1)	⬆	bi_server1
asyncadminservice(11.1.1)	⬆	bi_server2
biadminservices(11.1.1)	⬆	AdminServer
biadminservlet(11.1.1)	⬆	bi_cluster
biadminservlet(11.1.1)	⬆	bi_server1
biadminservlet(11.1.1)	⬆	bi_server2
biadminutils(11.1.1)	⬆	AdminServer
bicomposer(11.1.1)	⬆	bi_cluster
bicomposer(11.1.1)	⬆	bi_server1
bicomposer(11.1.1)	⬆	bi_server2
bicontentserver(11.1.1)	⬆	bi_cluster
bicontentserver(11.1.1)	⬆	bi_server1

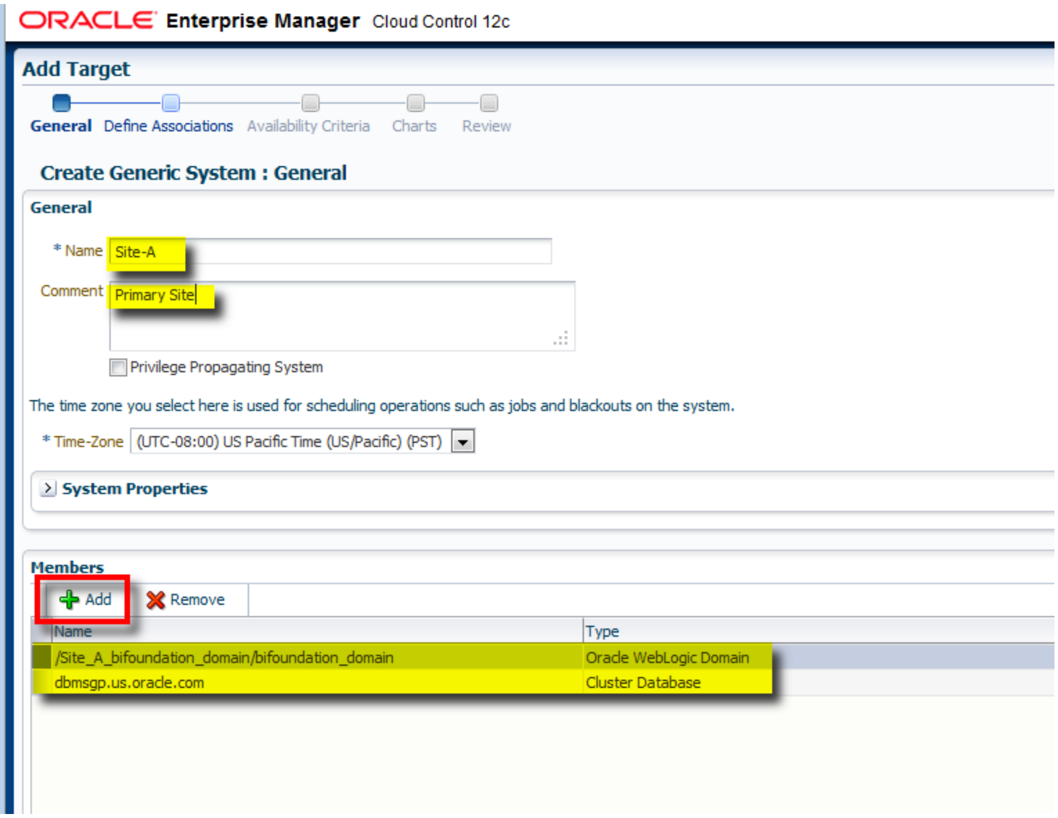
2. **Create a Generic System**. Create a generic system to collectively represent the discovered Oracle Fusion Middleware farm which comprises all the targets that will be protected by the Oracle Site Guard Disaster Recovery configuration (this configuration will be created in the next section). The example below shows the Oracle Fusion Middleware farm, and the Oracle RAC Database being added as members of the Generic system.



A system is a collection of related manageable entities which together provide one or more business functions. Members of any system

Search: Generic System

Name:



Create Generic System : General

General

* Name: Site-A

Comment: Primary Site

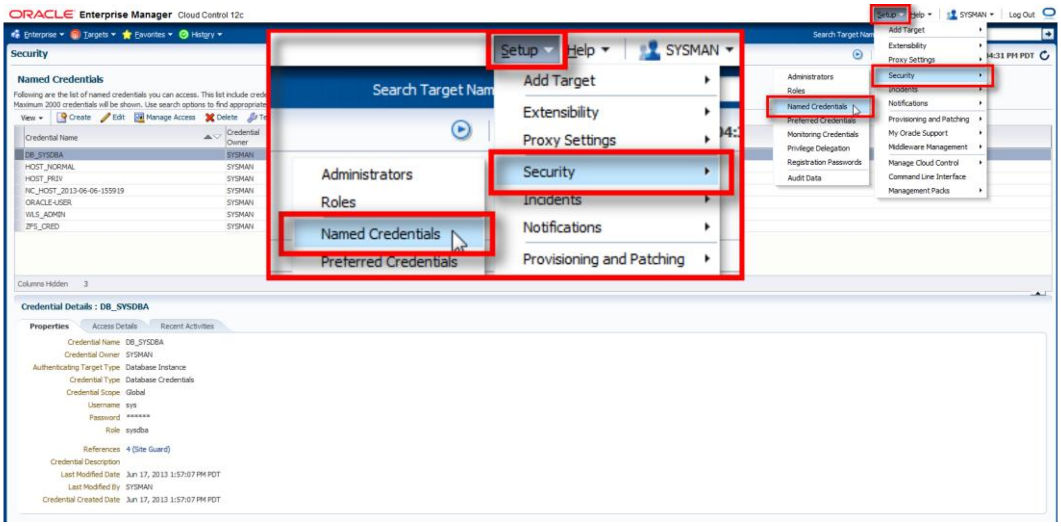
□ Privilege Propagating System

The time zone you select here is used for scheduling operations such as jobs and blackouts on the system.

* Time-Zone: (UTC-08:00) US Pacific Time (US/Pacific) (PST)

Name	Type
/Site_A_bifoundation_domain/bifoundation_domain	Oracle WebLogic Domain
dbmsgp.us.oracle.com	Cluster Database

3. **Configure Credentials**. Set up named credentials for various entities in the Oracle Middleware Fusion farm and Oracle RAC database that must be accessed and managed during disaster recovery operations.



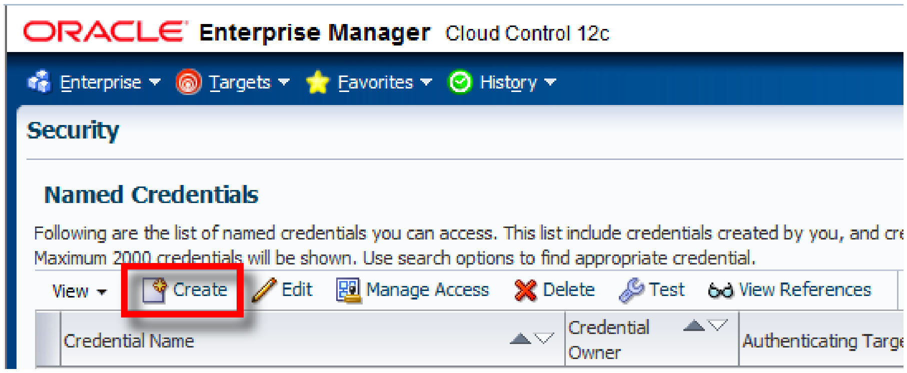
Named Credentials

Following are the list of named credentials you can access. This list include cred
Maximum 2000 credentials will be shown. Use search options to find appropriate

Credential Name	Credential Owner
DB_SYSDBA	SYSMAN
HOST_NORMAL	SYSMAN
HOST_PRIV	SYSMAN
NC_HOST_2013-06-06-155919	SYSMAN
ORACLE-USER	SYSMAN
WLS_ADMIN	SYSMAN
ZFS_CRED	SYSMAN

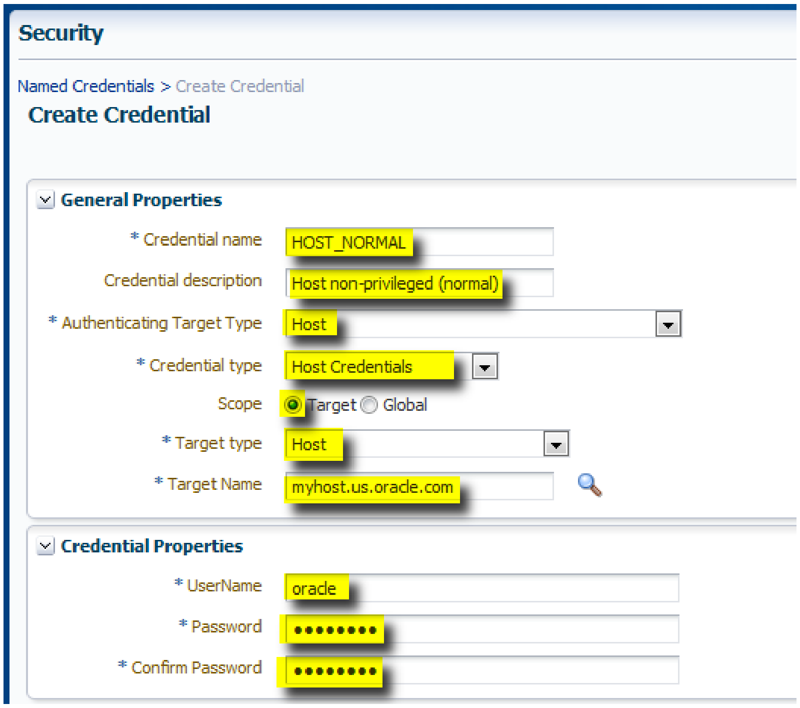
Credential Details : DB_SYSDBA

Credential Name DB_SYSDBA
Credential Owner SYSMAN
Authenticating Target Type Database Instance
Credential Type Database Credentials
Credential Scope Global
Username sys
Password ******
Role sysdba
References 4 (Site Guard)
Credential Description
Last Modified Date Jun 17, 2013 1:57:07 PM PDT
Last Modified By SYSMAN
Credential Created Date Jun 17, 2013 1:57:07 PM PDT



Named Credentials

Following are the list of named credentials you can access. This list include credentials created by you, and cre
Maximum 2000 credentials will be shown. Use search options to find appropriate credential.



Security

Named Credentials > Create Credential

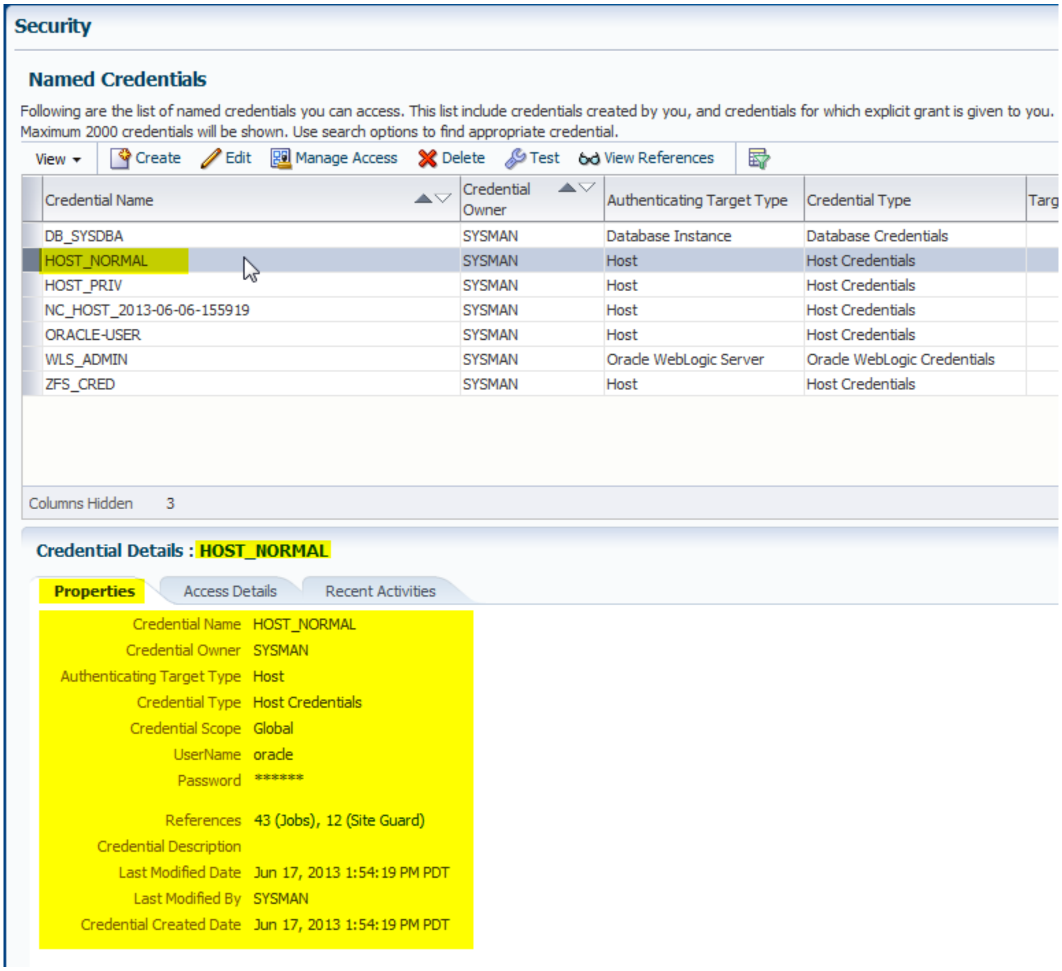
Create Credential

General Properties

* Credential name	HOST_NORMAL
Credential description	Host non-privileged (normal)
* Authenticating Target Type	Host
* Credential type	Host Credentials
Scope	● Target ○ Global
* Target type	Host
* Target Name	myhost.us.oracle.com

Credential Properties

* UserName	oracle
* Password	●●●●●●●●
* Confirm Password	●●●●●●●●



Named Credentials

Following are the list of named credentials you can access. This list include credentials created by you, and credentials for which explicit grant is given to you. Maximum 2000 credentials will be shown. Use search options to find appropriate credential.

Credential Name	Credential Owner	Authenticating Target Type	Credential Type	Targ
DB_SYSDBA	SYSMAN	Database Instance	Database Credentials	
HOST_NORMAL	SYSMAN	Host	Host Credentials	
HOST_PRIV	SYSMAN	Host	Host Credentials	
NC_HOST_2013-06-06-155919	SYSMAN	Host	Host Credentials	
ORACLE-USER	SYSMAN	Host	Host Credentials	
WLS_ADMIN	SYSMAN	Oracle WebLogic Server	Oracle WebLogic Credentials	
ZFS_CRED	SYSMAN	Host	Host Credentials	

Columns Hidden 3

Credential Details : HOST_NORMAL

Credential Name	HOST_NORMAL
Credential Owner	SYSMAN
Authenticating Target Type	Host
Credential Type	Host Credentials
Credential Scope	Global
UserName	oracle
Password	******
References	43 (Jobs), 12 (Site Guard)
Credential Description	
Last Modified Date	Jun 17, 2013 1:54:19 PM PDT
Last Modified By	SYSMAN
Credential Created Date	Jun 17, 2013 1:54:19 PM PDT

The table below summarizes the credentials that were set up for the deployment in this paper.

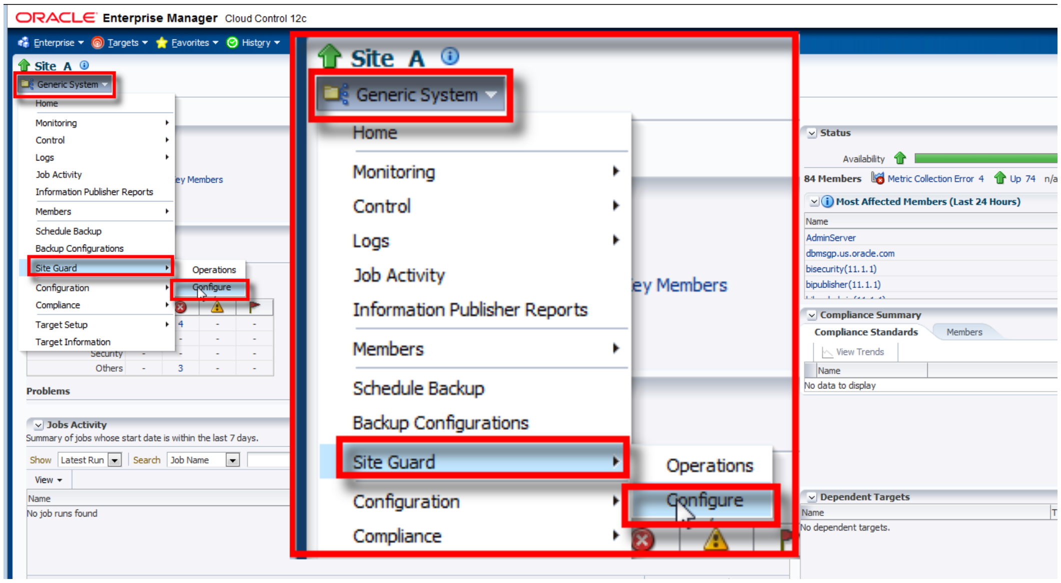
CREDENTIAL NAME	TARGET TYPE	NOTES
DB_SYSDBA	Database Instance	Oracle Database sysdba credentials
HOST_NORMAL	Host	Non-privileged host credentials (e.g., oracle)
HOST_PRIV	Host	Privileged host credentials (e.g., root)
WLS_ADMIN	Oracle WebLogic Server	WebLogic Admin Credentials
ZFS_CRED	Host	ZFS Appliance Admin Credentials

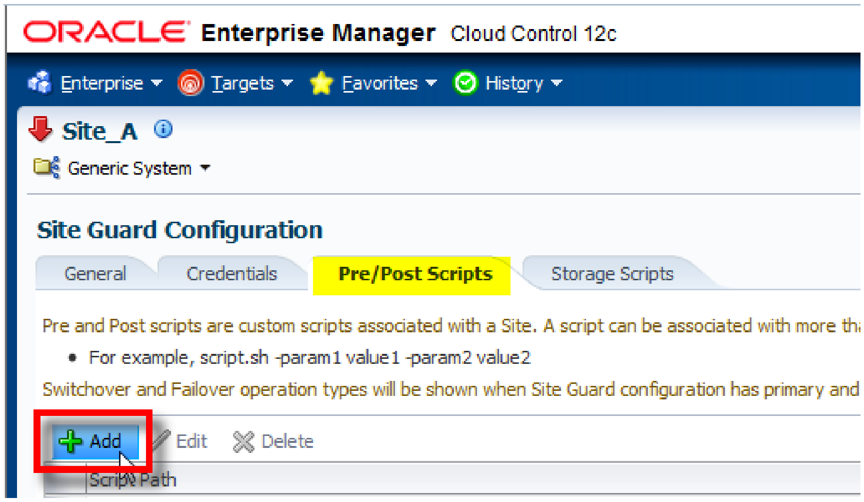
4. **Create Scripts**. There are two types of scripts that are created here.

   a. Custom Pre and Post scripts for handling application-specific events or conditions at the site you are configuring. For example, the deployment in this paper uses custom scripts to mount (or un-mount) all the NFS shares from the OHS and Application servers, before (or after) all the services have been started (or stopped). These Pre scripts are executed before initiating a switchover.

   b. Scripts that handle storage-specific actions, such as performing a replication role-reversal before switchover or failover of the application and web tiers. The storage-specific scripts used in this deployment come bundled with Oracle Site Guard. A description of the bundled scripts used is provided in the Appendix.

After the two types of scripts have been created, they must be associated with the generic system (the Site) created earlier. This is shown in the examples below.





Site Guard Configuration

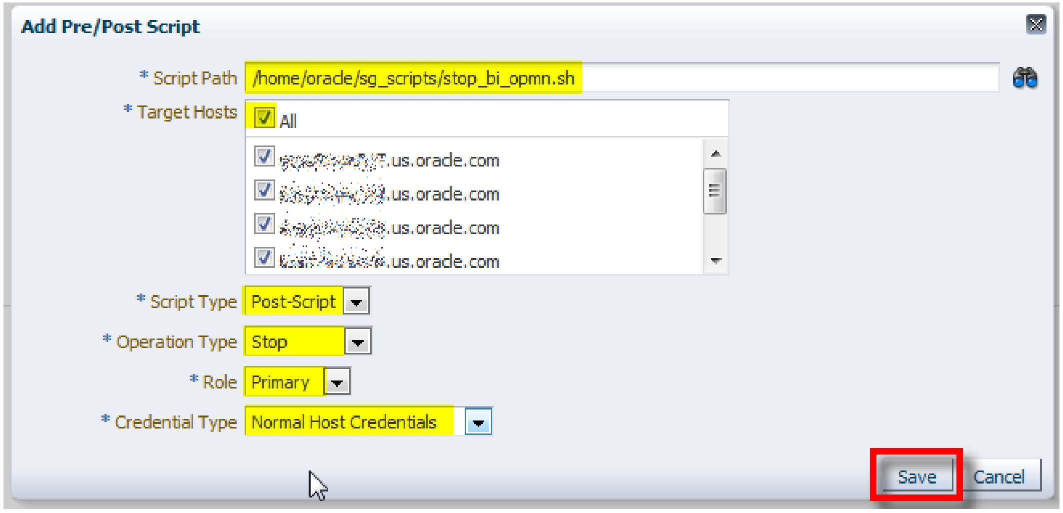
General | Credentials | Pre/Post Scripts | Storage Scripts

Pre and Post scripts are custom scripts associated with a Site. A script can be associated with more th

- For example, script.sh -param1 value1 -param2 value2

Switchover and Failover operation types will be shown when Site Guard configuration has primary and

Script Path



Add Pre/Post Script

* Script Path: /home/oracle/sg_scripts/stop_bi_opmn.sh

* Target Hosts: ☑ All

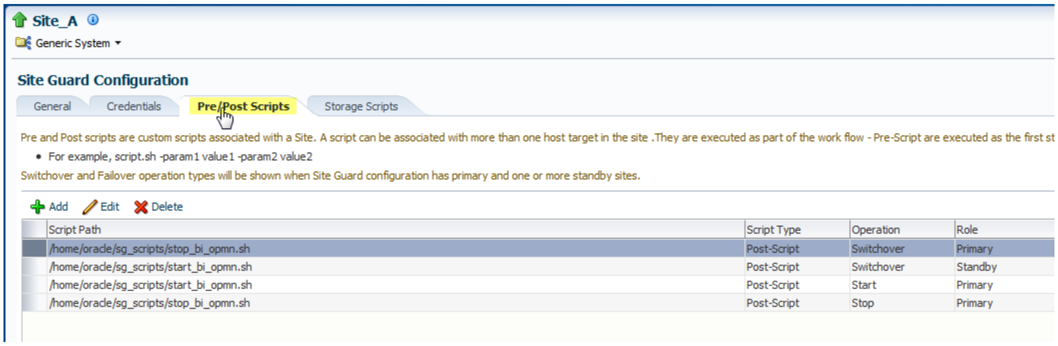
- ☑ [redacted].us.oracle.com
- ☑ [redacted].us.oracle.com
- ☑ [redacted].us.oracle.com
- ☑ [redacted].us.oracle.com

* Script Type: Post-Script

* Operation Type: Stop

* Role: Primary

* Credential Type: Normal Host Credentials



Site Guard Configuration

General | Credentials | Pre/Post Scripts | Storage Scripts

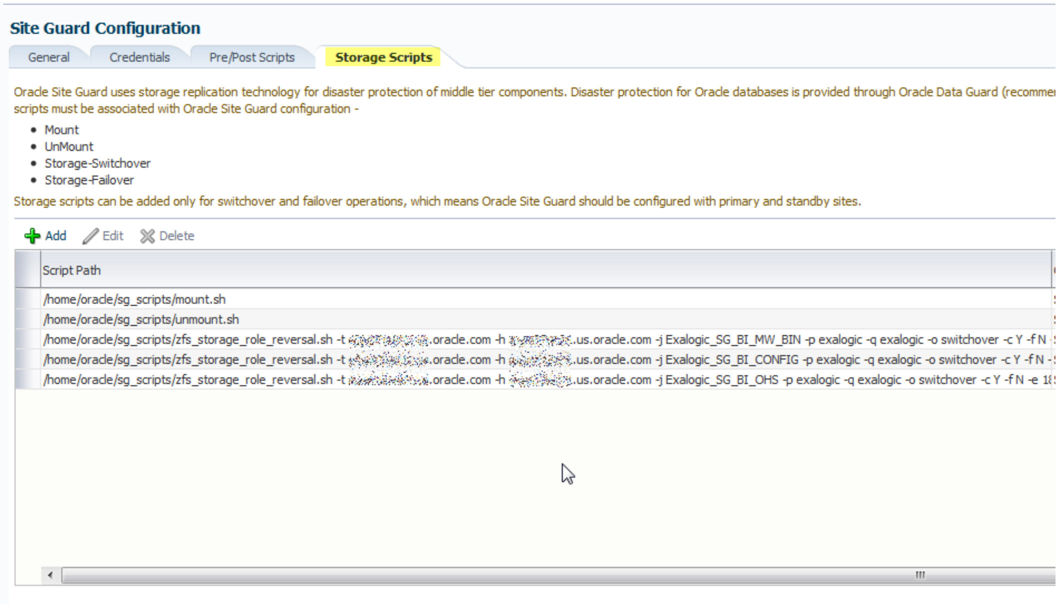
Pre and Post scripts are custom scripts associated with a Site. A script can be associated with more than one host target in the site .They are executed as part of the work flow - Pre-Script are executed as the first st

- For example, script.sh -param1 value1 -param2 value2

Switchover and Failover operation types will be shown when Site Guard configuration has primary and one or more standby sites.

Script Path	Script Type	Operation	Role
/home/oracle/sg_scripts/stop_bi_opmn.sh	Post-Script	Switchover	Primary
/home/oracle/sg_scripts/start_bi_opmn.sh	Post-Script	Switchover	Standby
/home/oracle/sg_scripts/start_bi_opmn.sh	Post-Script	Start	Primary
/home/oracle/sg_scripts/stop_bi_opmn.sh	Post-Script	Stop	Primary

In the storage scripts configuration shown below, note the addition of the *zfs_storage_role_reversal.sh* script three times with appropriate parameters – once for each ZFS project being replicated.



Site Guard Configuration

Oracle Site Guard uses storage replication technology for disaster protection of middle tier components. Disaster protection for Oracle databases is provided through Oracle Data Guard (recomme
scripts must be associated with Oracle Site Guard configuration -

- Mount
- UnMount
- Storage-Switchover
- Storage-Failover

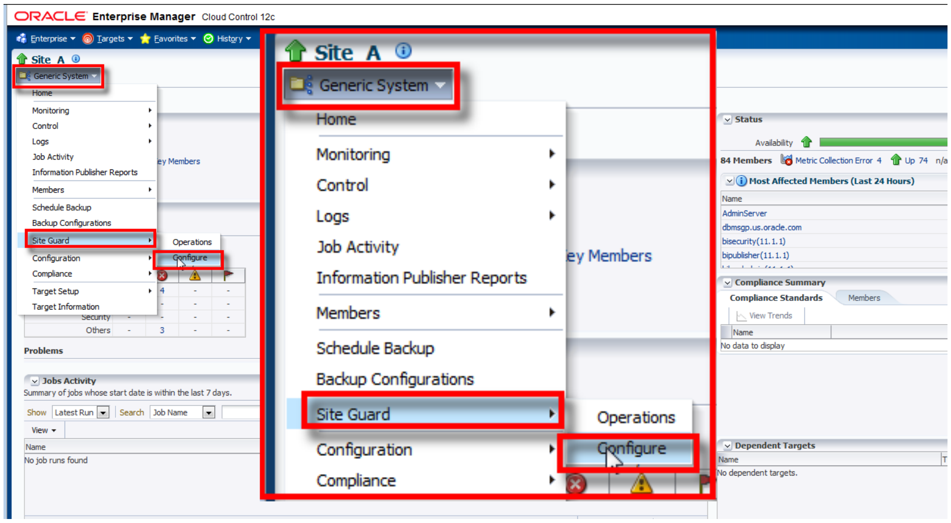
Storage scripts can be added only for switchover and failover operations, which means Oracle Site Guard should be configured with primary and standby sites.

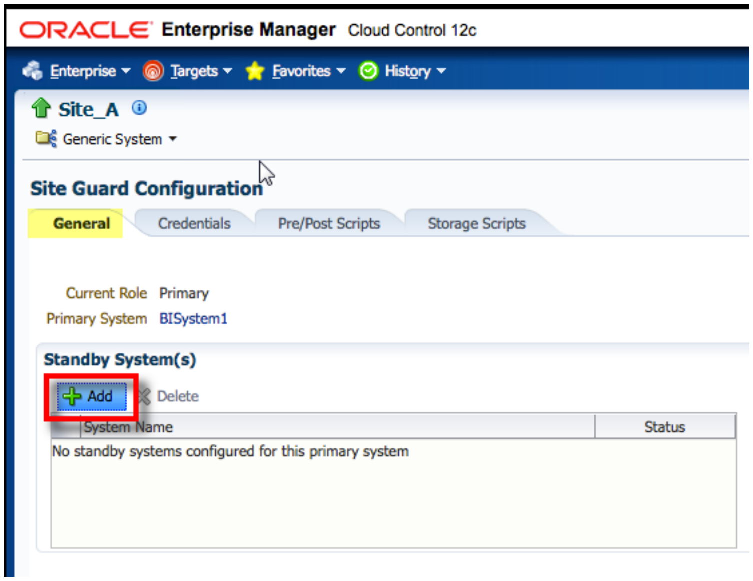
Script Path
/home/oracle/sg_scripts/mount.sh
/home/oracle/sg_scripts/unmount.sh
/home/oracle/sg_scripts/zfs_storage_role_reversal.sh -t [redacted].oracle.com -h [redacted].us.oracle.com -j Exalogic_SG_BI_MW_BIN -p exalogic -q exalogic -o switchover -c Y -f N
/home/oracle/sg_scripts/zfs_storage_role_reversal.sh -t [redacted].oracle.com -h [redacted].us.oracle.com -j Exalogic_SG_BI_CONFIG -p exalogic -q exalogic -o switchover -c Y -f N -
/home/oracle/sg_scripts/zfs_storage_role_reversal.sh -t [redacted].oracle.com -h [redacted].us.oracle.com -j Exalogic_SG_BI_OHS -p exalogic -q exalogic -o switchover -c Y -f N -e 1

Oracle Site Guard Pre-requisites for All Sites

After the pre-requisite configuration steps described above have been completed for each site, perform the configuration described in the following two steps only once, since these procedures are common both sites. This will finish the pre-requisite setup process.

1. **Configure Sites**. This step identifies the Primary and Standby sites. The example below shows this configuration process. It presumes that Site A is currently active (the Primary) and Site B is not active (the Standby).

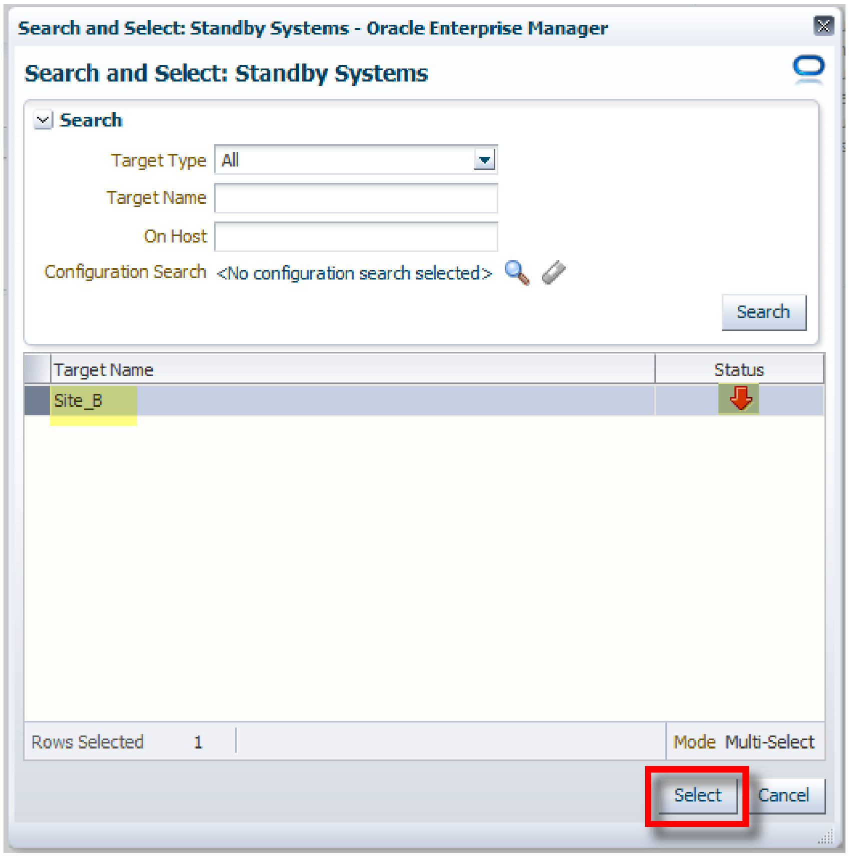




Current Role Primary

Primary System BISystem1

No standby systems configured for this primary system



Search and Select: Standby Systems - Oracle Enterprise Manager

Search and Select: Standby Systems

Search

Target Type: All

Target Name

On Host

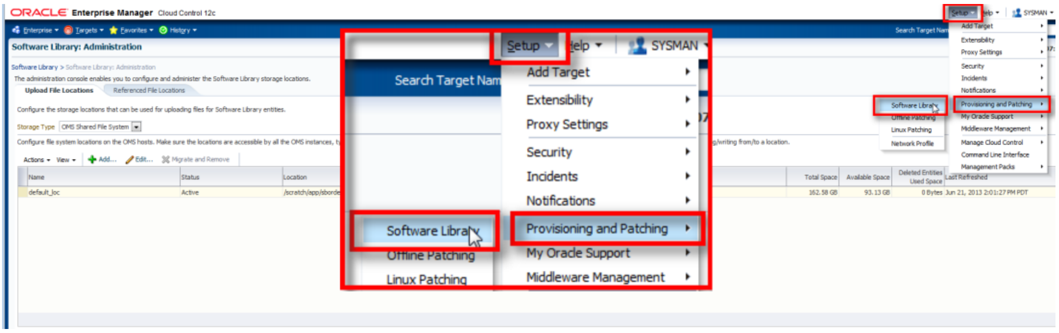
Configuration Search: <No configuration search selected>

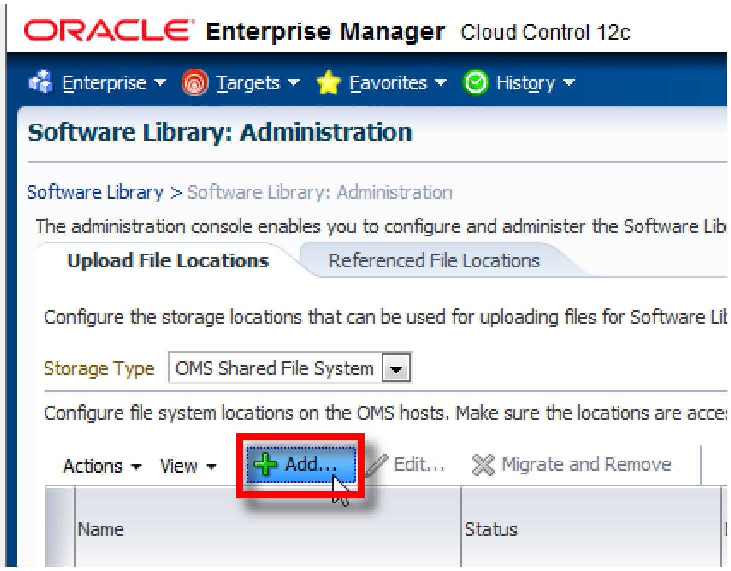
Target Name	Status
Site_B	⬇

Rows Selected 1

Mode Multi-Select

2. **Configure Software Library**. Set up the Software Library location which contains scripts to be used by Oracle Site Guard when executing the disaster recovery action plan. For this paper the location specified is `$ORACLE_BASE/emcc/swlib` on the EMCCHOST node.





Software Library: Administration

Software Library > Software Library: Administration

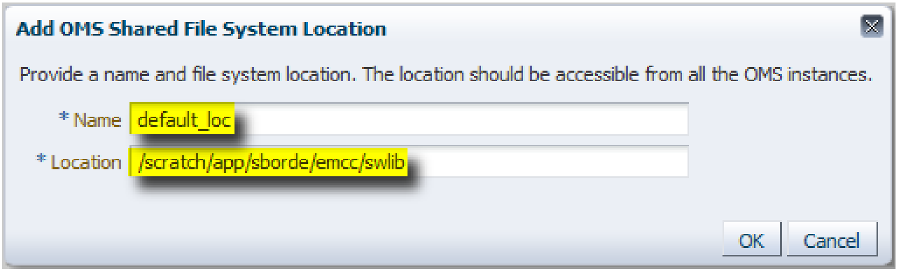
The administration console enables you to configure and administer the Software Lib

Upload File Locations | Referenced File Locations

Configure the storage locations that can be used for uploading files for Software Lil

Storage Type: OMS Shared File System

Configure file system locations on the OMS hosts. Make sure the locations are acce:



Add OMS Shared File System Location

Provide a name and file system location. The location should be accessible from all the OMS instances.

* Name: default_loc

* Location: /scratch/app/sborde/emcc/swlib

Configuring Oracle Site Guard Operations for Disaster Recovery

After setting up the pre-requisites described in the previous section, Oracle Site Guard operations can now be configured for Disaster Recovery operations.

Configuring Oracle Site Guard Disaster Recovery operations requires that an ***operation plan*** be created for each kind of operation that Oracle Site Guard must execute. An operation plan is a pre-defined execution flow containing an ordered sequence of steps, with additional attributes that define how these steps will be executed.

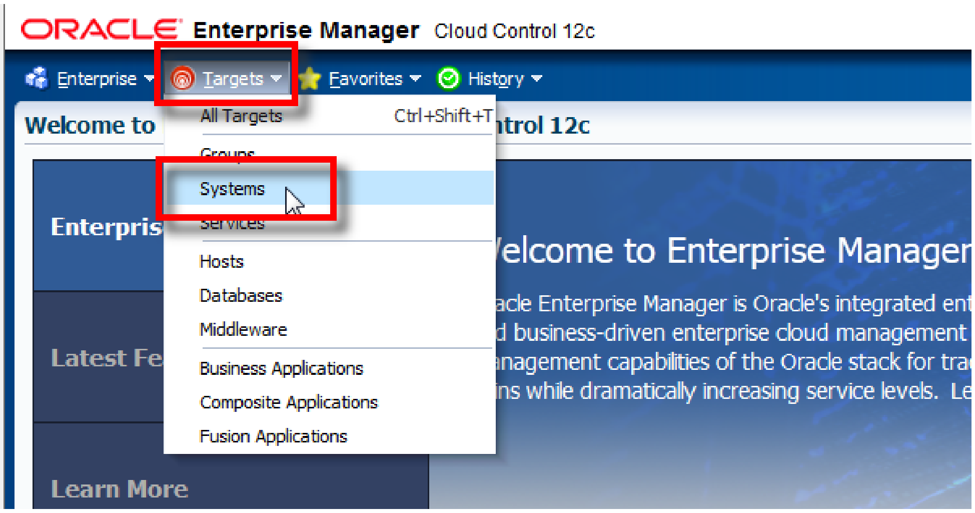
The table below shows the Oracle Site Guard operations tested in this paper.

SITE GUARD OPERATION NAME	DESCRIPTION
Stop-Site-A	Bring down the application and database at the primary site
Start-Site-B	Bring up the application and database at the standby site
Switchover-to-Site-B	Switch over operations from primary to standby site

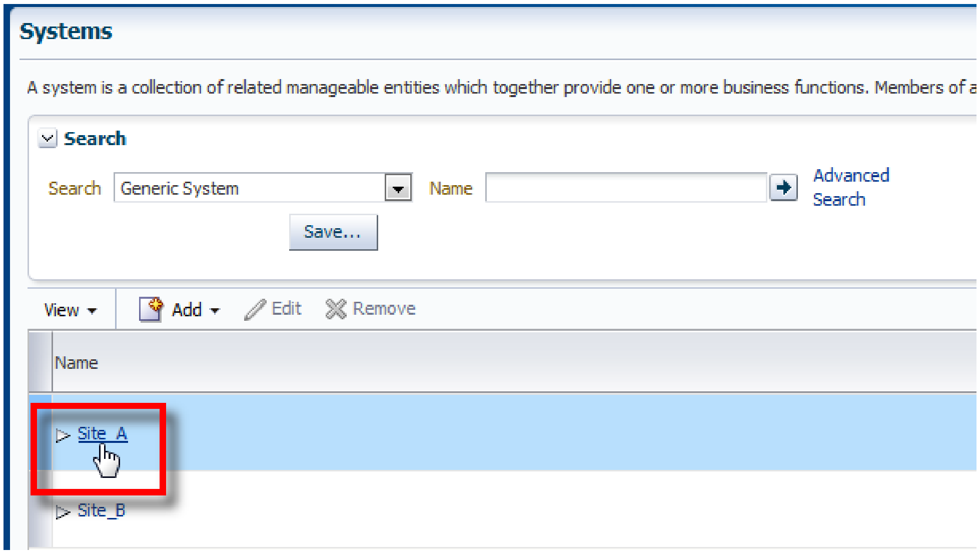
Switchback-to-Site-A	Switch operations back to primary site from standby site
Failover-to-Site-B	Fail over operations from primary to standby site
Fallback-to-Site-A	Fail over operations back to primary site from standby site

The following example shows the creation of an Operation Plan for switching over from Site A to B. Other operations plans will follow a similar configuration flow.

Begin by clicking on the **Targets** menu and navigating to the **Systems** page.

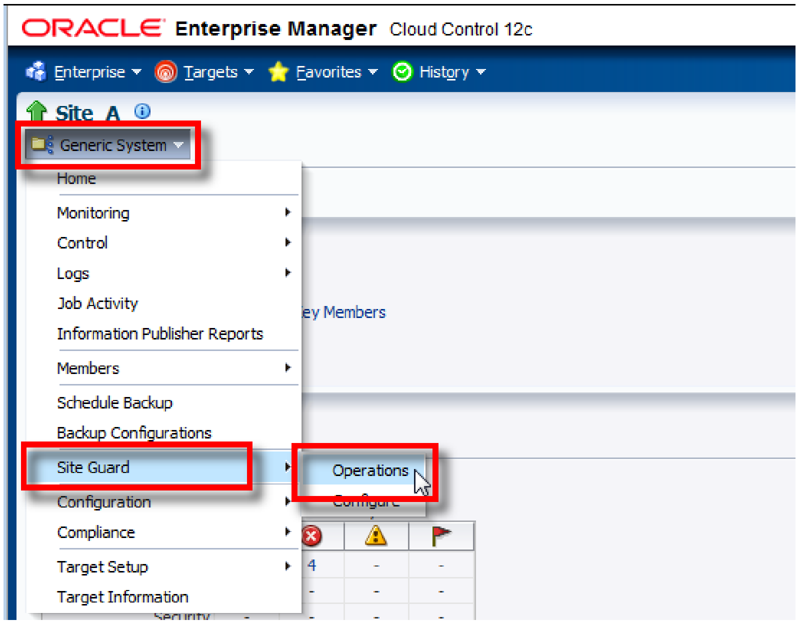

ORACLE Enterprise Manager Cloud Control 12c
Enterprise
Targets
Favorites
History
All Targets
Ctrl+Shift+T
Groups
Systems
Services
Hosts
Databases
Middleware
Business Applications
Composite Applications
Fusion Applications
Welcome to
trol 12c
Enterpris
Latest Fe
Learn More
elcome to Enterprise Manager
acle Enterprise Manager is Oracle's integrated ent
d business-driven enterprise cloud management
anagement capabilities of the Oracle stack for tra
ns while dramatically increasing service levels. Le

On the Systems page, click on **Site A**.

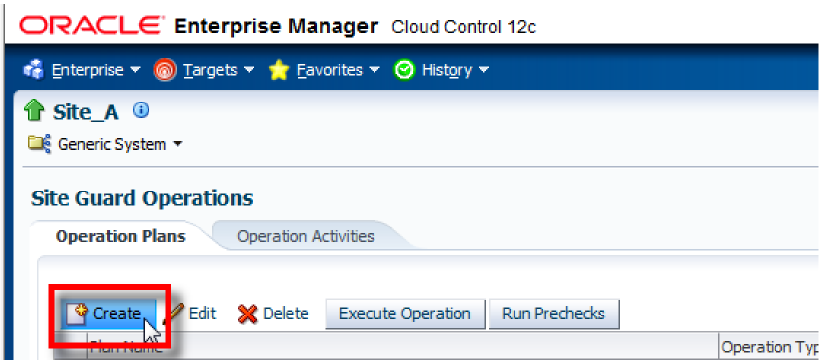

Systems

A system is a collection of related manageable entities which together provide one or more business functions. Members of a

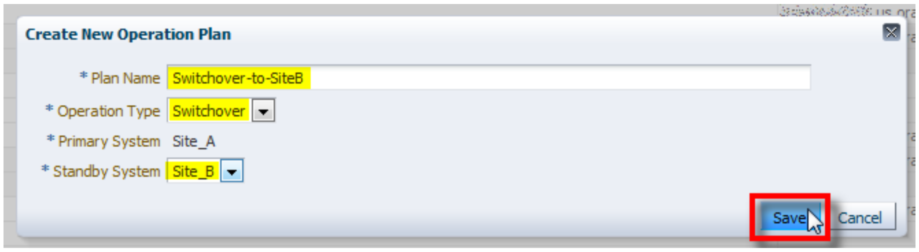
On the page for Site A, click on **Generic System**, and navigate to the **Site Guard → Operations** menu entry.



On the Site Guard Operations page, click on **Create** to begin creating a new Operation Plan.



When the desired *Operation Type* is selected in the *Create New Operation Plan* dialog, Oracle Site Guard will assemble the appropriate sequence of steps required to execute that operation plan for all the components comprising the generic system (Site A).

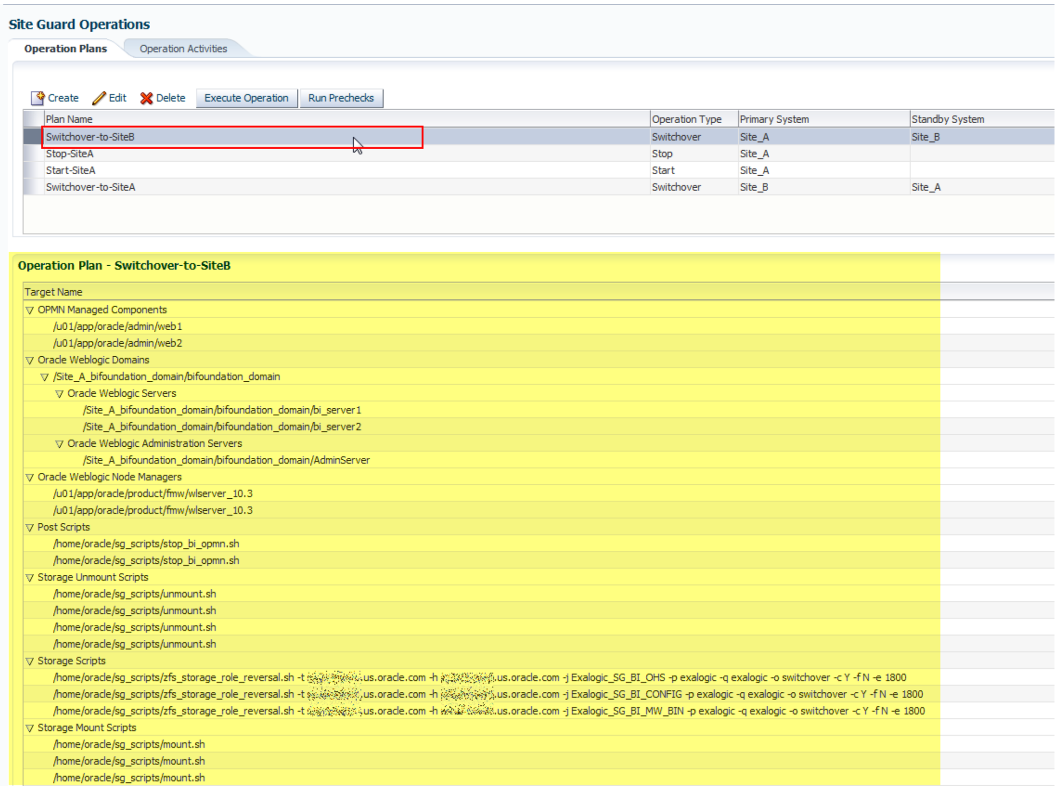


Create New Operation Plan

* Plan Name	Switchover-to-SiteB
* Operation Type	Switchover
* Primary System	Site_A
* Standby System	Site_B

Finally, selecting the newly created operation **Switchover-to-SiteB** will show all the steps in the operation plan with additional information on:

- The Target Host that the step applies to.
- The Operation Type that the step entails.
- The Error Mode for that step (Stop on Error, Continue, etc.)
- The Execution Mode (Serial, Parallel, etc.)



Site Guard Operations

Plan Name	Operation Type	Primary System	Standby System
Switchover-to-SiteB	Switchover	Site_A	Site_B
Stop-SiteA	Stop	Site_A	
Start-SiteA	Start	Site_A	
Switchover-to-SiteA	Switchover	Site_B	Site_A

Operation Plan - Switchover-to-SiteB

```
Target Name
▽ OPMN Managed Components
    /u01/app/oracle/admin/web1
    /u01/app/oracle/admin/web2
▽ Oracle Weblogic Domains
  ▽ /Site_A_bifoundation_domain/bifoundation_domain
    ▽ Oracle Weblogic Servers
        /Site_A_bifoundation_domain/bifoundation_domain/bi_server1
        /Site_A_bifoundation_domain/bifoundation_domain/bi_server2
    ▽ Oracle Weblogic Administration Servers
        /Site_A_bifoundation_domain/bifoundation_domain/AdminServer
▽ Oracle Weblogic Node Managers
    /u01/app/oracle/product/fmw/wlserver_10.3
    /u01/app/oracle/product/fmw/wlserver_10.3
▽ Post Scripts
    /home/oracle/sg_scripts/stop_bi_opmn.sh
    /home/oracle/sg_scripts/stop_bi_opmn.sh
▽ Storage Unmount Scripts
    /home/oracle/sg_scripts/unmount.sh
    /home/oracle/sg_scripts/unmount.sh
    /home/oracle/sg_scripts/unmount.sh
    /home/oracle/sg_scripts/unmount.sh
▽ Storage Scripts
    /home/oracle/sg_scripts/zfs_storage_role_reversal.sh -t [redacted].us.oracle.com -h [redacted].us.oracle.com -j Exalogic_SG_BI_OHS -p exalogic -q exalogic -o switchover -c Y -f N -e 1800
    /home/oracle/sg_scripts/zfs_storage_role_reversal.sh -t [redacted].us.oracle.com -h [redacted].us.oracle.com -j Exalogic_SG_BI_CONFIG -p exalogic -q exalogic -o switchover -c Y -f N -e 1800
    /home/oracle/sg_scripts/zfs_storage_role_reversal.sh -t [redacted].us.oracle.com -h [redacted].us.oracle.com -j Exalogic_SG_BI_MW_BIN -p exalogic -q exalogic -o switchover -c Y -f N -e 1800
▽ Storage Mount Scripts
    /home/oracle/sg_scripts/mount.sh
    /home/oracle/sg_scripts/mount.sh
    /home/oracle/sg_scripts/mount.sh
```

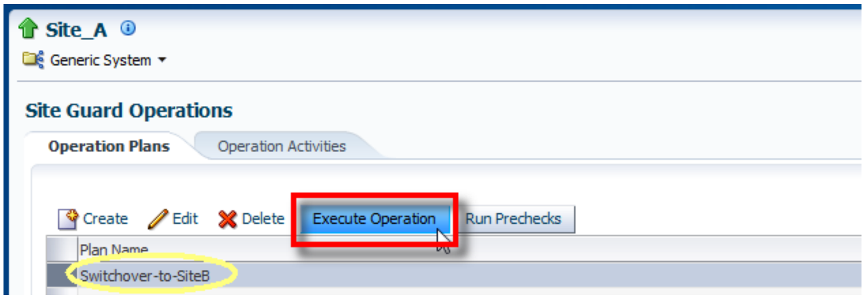
Similarly, an Operation Plan for failing over to Site B (**Failover-to-Site-B**) can be created for failover operations.

Disaster Recovery Operations

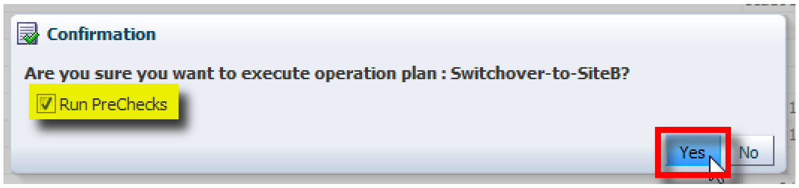
After one or more operation plans have been created, these operation plans can now be executed. The examples below demonstrate the execution of switchover and failover operations from Site A (primary) to Site B (standby).

Switch Over to Site B

The switchover operation is initiated by navigating to the page for the generic system Site A, and executing the configured operation plan named **Switchover-to-SiteB**.



In the confirmation dialog, ensure that *Run PreChecks* is selected as this will verify that many of the pre-conditions required for a successful switchover, are satisfied.


Confirmation

Are you sure you want to execute operation plan : Switchover-to-SiteB?

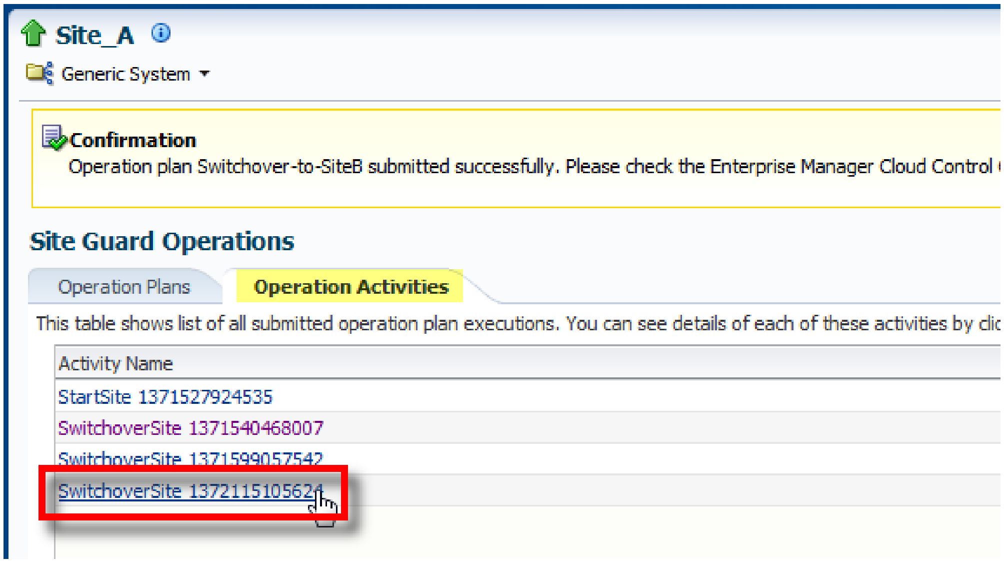
☑ Run PreChecks

Some of the checks performed when *Run PreChecks* is enabled, are:

- Checks whether the Fusion Middleware Farms running on the primary site are down, before performing a switchover operation.
- Checks the Enterprise Management Agent status on all hosts involved in the operation.
- Checks if any new targets were added to the generic system after the operation plan is created.
- Checks whether all targets involved in the operation plan exist in the Enterprise Manager repository.

- Detects if any targets were moved out or deleted from the generic system after the operation plan is created.
- Asserts the existence of all configured scripts (pre/post/mount/unmount/storage role reversal) on their respective target hosts.
- Runs Oracle Data Guard Broker prechecks to determine whether the Database is ready for role reversal (during switchover or failover operations)
- Performs Database Role Checks

After the switchover operation plan has started execution, details of its progress can be viewed by navigating to the Operation Activities tab, and clicking on the corresponding activity link as shown below.



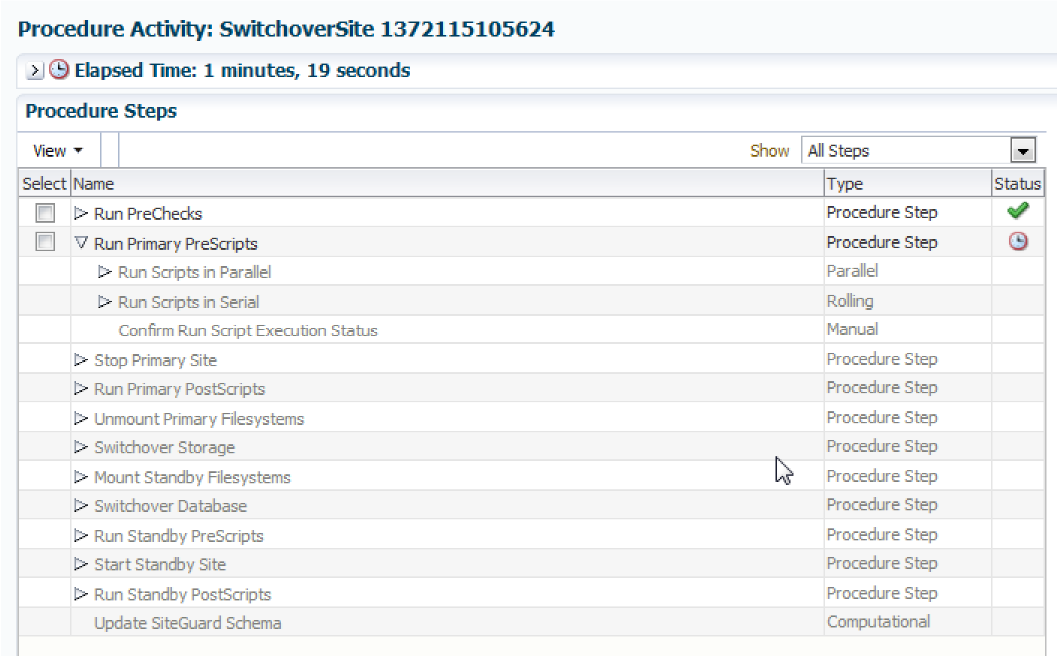
Confirmation

Operation plan Switchover-to-SiteB submitted successfully. Please check the Enterprise Manager Cloud Control

Site Guard Operations

This table shows list of all submitted operation plan executions. You can see details of each of these activities by clic

Activity Name
StartSite 1371527924535
SwitchoverSite 1371540468007
SwitchoverSite 1371599057542
SwitchoverSite 1372115105624



Procedure Activity: SwitchoverSite 1372115105624

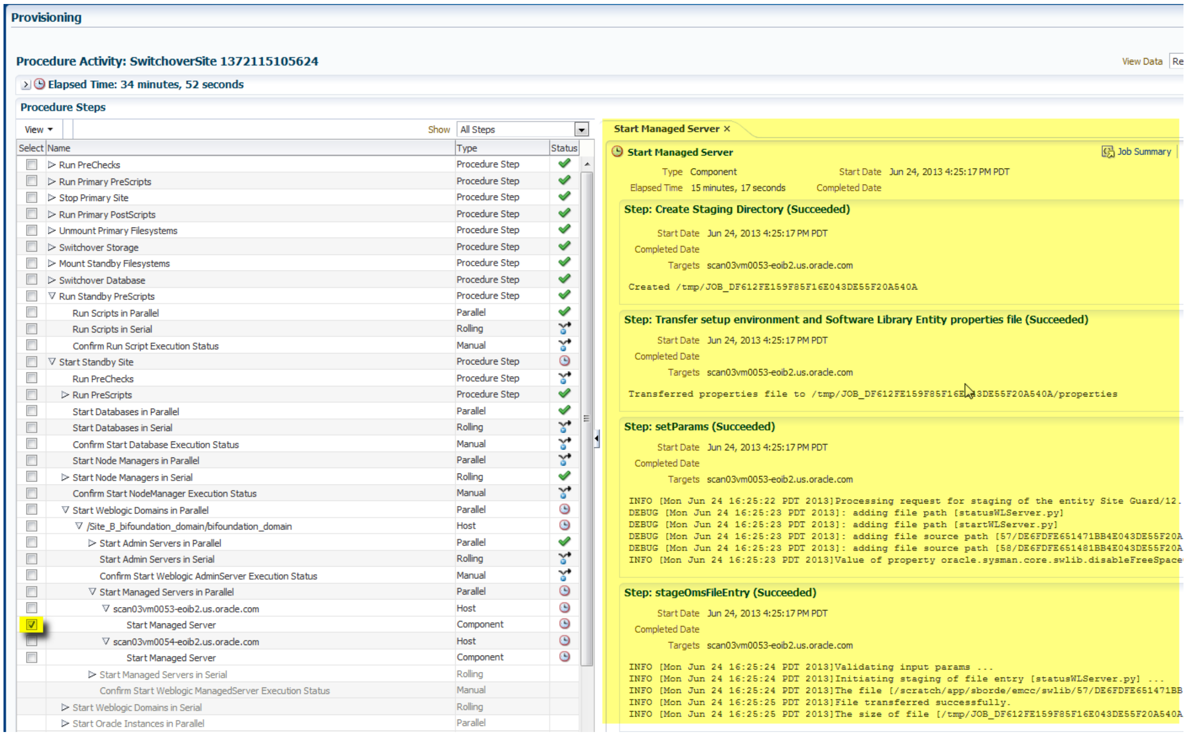
Elapsed Time: 1 minutes, 19 seconds

Procedure Steps

All Steps

Select	Name	Type	Status
□	▷ Run PreChecks	Procedure Step	✓
□	▽ Run Primary PreScripts	Procedure Step	🕒
	▷ Run Scripts in Parallel	Parallel	
	▷ Run Scripts in Serial	Rolling	
	Confirm Run Script Execution Status	Manual	
	▷ Stop Primary Site	Procedure Step	
	▷ Run Primary PostScripts	Procedure Step	
	▷ Unmount Primary Filesystems	Procedure Step	
	▷ Switchover Storage	Procedure Step	
	▷ Mount Standby Filesystems	Procedure Step	
	▷ Switchover Database	Procedure Step	
	▷ Run Standby PreScripts	Procedure Step	
	▷ Start Standby Site	Procedure Step	
	▷ Run Standby PostScripts	Procedure Step	
	Update SiteGuard Schema	Computational	

The Procedure Activity window can be refreshed automatically or manually to view the current progress of the operation plan. Each high-level step can be further inspected in detail by drilling down the hierarchy and selecting a constituent step. A green check mark (or a skipped symbol) appears in the *Status* column after a step is completed.



Provisioning

Procedure Activity: SwitchoverSite 1372115105624

Elapsed Time: 34 minutes, 52 seconds

Procedure Steps

All Steps

Select	Name	Type	Status
□	▷ Run PreChecks	Procedure Step	✓
□	▷ Run Primary PreScripts	Procedure Step	✓
□	▷ Stop Primary Site	Procedure Step	✓
□	▷ Run Primary PostScripts	Procedure Step	✓
□	▷ Unmount Primary Filesystems	Procedure Step	✓
□	▷ Switchover Storage	Procedure Step	✓
□	▷ Mount Standby Filesystems	Procedure Step	✓
□	▷ Switchover Database	Procedure Step	✓
□	▽ Run Standby PreScripts	Procedure Step	✓
□	Run Scripts in Parallel	Parallel	✓
□	Run Scripts in Serial	Rolling	⑂
□	Confirm Run Script Execution Status	Manual	⑂
□	▽ Start Standby Site	Procedure Step	◷
□	Run PreChecks	Procedure Step	⑂
□	▷ Run PreScripts	Procedure Step	✓
□	Start Databases in Parallel	Parallel	✓
□	Start Databases in Serial	Rolling	⑂
□	Confirm Start Database Execution Status	Manual	⑂
□	Start Node Managers in Parallel	Parallel	⑂
□	▷ Start Node Managers in Serial	Rolling	✓
□	Confirm Start NodeManager Execution Status	Manual	⑂
□	▽ Start Weblogic Domains in Parallel	Parallel	◷
□	▽ /Site_B_bifoundation_domain/bifoundation_domain	Host	◷
□	▷ Start Admin Servers in Parallel	Parallel	✓
□	Start Admin Servers in Serial	Rolling	⑂
□	Confirm Start Weblogic AdminServer Execution Status	Manual	⑂
□	▽ Start Managed Servers in Parallel	Parallel	◷
□	▽ scan03vm0053-eoib2.us.oracle.com	Host	◷
☑	Start Managed Server	Component	◷
□	▽ scan03vm0054-eoib2.us.oracle.com	Host	◷
□	Start Managed Server	Component	◷
	▷ Start Managed Servers in Serial	Rolling	
	Confirm Start Weblogic ManagedServer Execution Status	Manual	
	▷ Start Weblogic Domains in Serial	Rolling	
	▷ Start Oracle Instances in Parallel	Parallel	

Start Managed Server ×

Start Managed Server

Type Component
Start Date Jun 24, 2013 4:25:17 PM PDT
Elapsed Time 15 minutes, 17 seconds
Completed Date

Step: Create Staging Directory (Succeeded)

Start Date Jun 24, 2013 4:25:17 PM PDT
Completed Date
Targets scan03vm0053-eoib2.us.oracle.com

```
Created /tmp/JOB_DF612FE159F85F16E043DE55F20A540A
```

Step: Transfer setup environment and Software Library Entity properties file (Succeeded)

Start Date Jun 24, 2013 4:25:17 PM PDT
Completed Date
Targets scan03vm0053-eoib2.us.oracle.com

```
Transferred properties file to /tmp/JOB_DF612FE159F85F16E043DE55F20A540A/properties
```

Step: setParams (Succeeded)

Start Date Jun 24, 2013 4:25:17 PM PDT
Completed Date
Targets scan03vm0053-eoib2.us.oracle.com

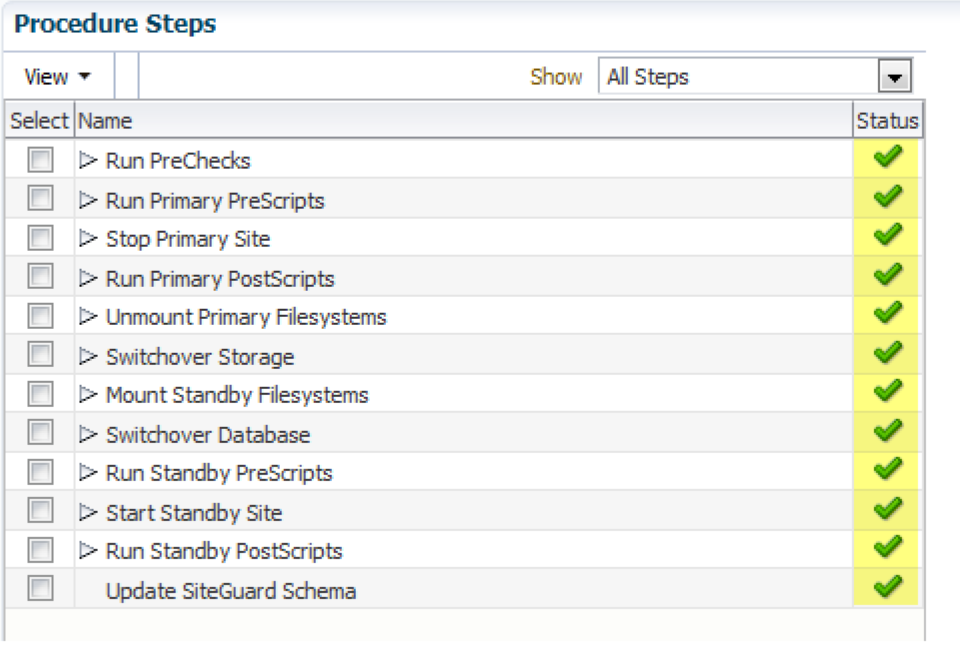
```
INFO [Mon Jun 24 16:25:22 PDT 2013]Processing request for staging of the entity Site Guard/12.
DEBUG [Mon Jun 24 16:25:23 PDT 2013]: adding file path [statusWLServer.py]
DEBUG [Mon Jun 24 16:25:23 PDT 2013]: adding file path [startWLServer.py]
DEBUG [Mon Jun 24 16:25:23 PDT 2013]: adding file source path [57/DE6FDFE651471BB4E043DE55F20A
DEBUG [Mon Jun 24 16:25:23 PDT 2013]: adding file source path [58/DE6FDFE651481BB4E043DE55F20A
INFO [Mon Jun 24 16:25:23 PDT 2013]Value of property oracle.sysman.core.swlib.disableFreeSpace
```

Step: stageOmsFileEntry (Succeeded)

Start Date Jun 24, 2013 4:25:17 PM PDT
Completed Date
Targets scan03vm0053-eoib2.us.oracle.com

```
INFO [Mon Jun 24 16:25:24 PDT 2013]Validating input params ...
INFO [Mon Jun 24 16:25:24 PDT 2013]Initiating staging of file entry [statusWLServer.py] ...
INFO [Mon Jun 24 16:25:24 PDT 2013]The file [/scratch/app/sborde/emcc/swlib/57/DE6FDFE651471BB
INFO [Mon Jun 24 16:25:25 PDT 2013]File transferred successfully.
INFO [Mon Jun 24 16:25:25 PDT 2013]The size of file [/tmp/JOB_DF612FE159F85F16E043DE55F20A540A
```

The switchover is complete when all the steps in the Operation Plan indicate a completed status.



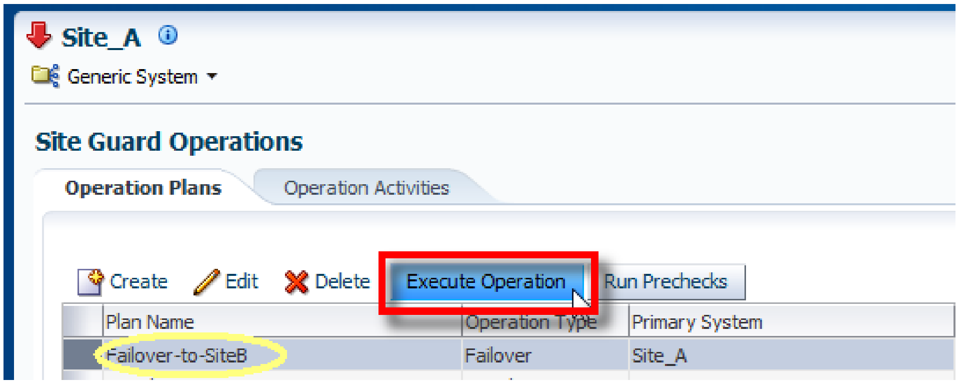
Procedure Steps

All Steps

Select	Name	Status
□	▷ Run PreChecks	✓
□	▷ Run Primary PreScripts	✓
□	▷ Stop Primary Site	✓
□	▷ Run Primary PostScripts	✓
□	▷ Unmount Primary Filesystems	✓
□	▷ Switchover Storage	✓
□	▷ Mount Standby Filesystems	✓
□	▷ Switchover Database	✓
□	▷ Run Standby PreScripts	✓
□	▷ Start Standby Site	✓
□	▷ Run Standby PostScripts	✓
□	Update SiteGuard Schema	✓

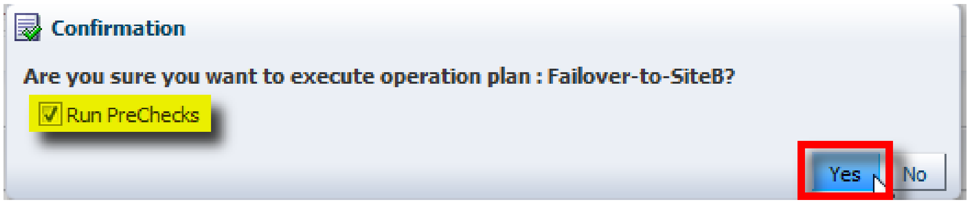
Fail Over to Site B

The failover operation is initiated by navigating to the page for the generic system Site A, and executing the configured operation plan named **Failover-to-SiteB**.



Plan Name	Operation Type	Primary System
Failover-to-SiteB	Failover	Site_A

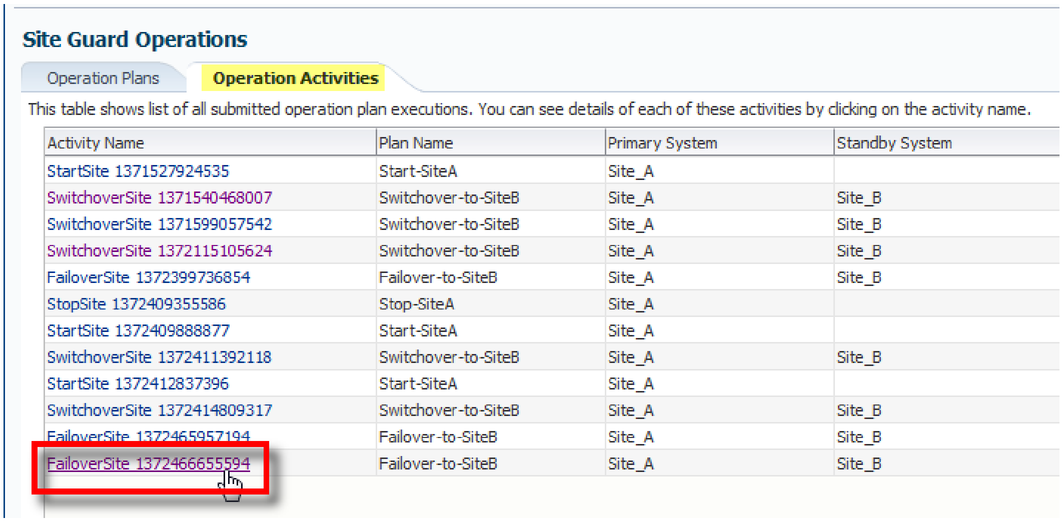
In the confirmation window, ensure that *Run PreChecks* is selected as this will verify that many of the pre-conditions required for a successful switchover, are satisfied.



Are you sure you want to execute operation plan : Failover-to-SiteB?

☑ Run PreChecks

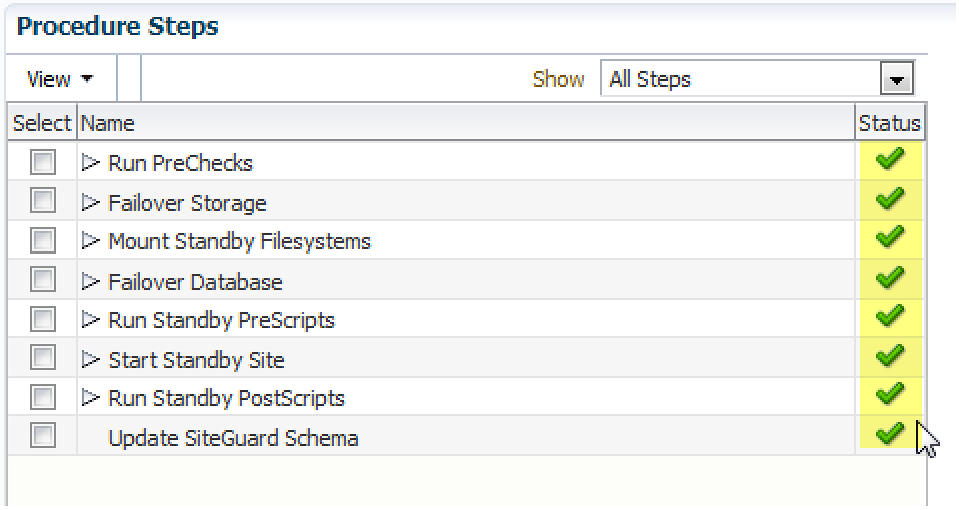
After the failover operation plan has started executing, its progress can be monitored by navigating to the Operation Activities tab and clicking on the corresponding activity link as shown below.



This table shows list of all submitted operation plan executions. You can see details of each of these activities by clicking on the activity name.

Activity Name	Plan Name	Primary System	Standby System
StartSite 1371527924535	Start-SiteA	Site_A	
SwitchoverSite 1371540468007	Switchover-to-SiteB	Site_A	Site_B
SwitchoverSite 1371599057542	Switchover-to-SiteB	Site_A	Site_B
SwitchoverSite 1372115105624	Switchover-to-SiteB	Site_A	Site_B
FailoverSite 1372399736854	Failover-to-SiteB	Site_A	Site_B
StopSite 1372409355586	Stop-SiteA	Site_A	
StartSite 1372409888877	Start-SiteA	Site_A	
SwitchoverSite 1372411392118	Switchover-to-SiteB	Site_A	Site_B
StartSite 1372412837396	Start-SiteA	Site_A	
SwitchoverSite 1372414809317	Switchover-to-SiteB	Site_A	Site_B
FailoverSite 1372465957194	Failover-to-SiteB	Site_A	Site_B
FailoverSite 1372466655594	Failover-to-SiteB	Site_A	Site_B

The failover is complete when all the steps in the Operation Plan indicate a completed status.



Select	Name	Status
☐	▷ Run PreChecks	✓
☐	▷ Failover Storage	✓
☐	▷ Mount Standby Filesystems	✓
☐	▷ Failover Database	✓
☐	▷ Run Standby PreScripts	✓
☐	▷ Start Standby Site	✓
☐	▷ Run Standby PostScripts	✓
☐	Update SiteGuard Schema	✓

Oracle MAA Best Practices for Disaster Recovery

1. It is recommended to test the standby site periodically. A good rule of thumb is to test the standby site after every major upgrade or once every quarter. This will help mitigate failures at both sites. Test the standby site by switching its role with the current primary site.
    a. Execute the site switchover operation plan to switch over the standby site to the new primary site.
    b. Once testing is complete, execute the site switchback operation plan to reverse the roles.
    c. Periodic testing validates that both the primary and standby sites are completely functional and mitigates the risk of failure at both sites. It also validates the switchover and switchback procedures.
2. Do not configure project-level and share-level replication within the same project. Configure project-level replication where possible to maintain simplicity and consistency.
3. Use the **Scheduled** replication mode for projects and shares when:
    a. Data does not change frequently.
    b. Recovery Point Objective falls within your scheduled replication window.
4. Use the **Continuous** replication mode for projects and shares when:
    a. The standby site is required to be as close as possible to the primary site.
    b. Recovery Point Objective allows for very little data loss.
    c. Data is of a critical nature.
5. Snapshots and clones can be used at the target site to offload backup, test, and development types of environment.
6. When configuring a local standby site i.e. Disaster Recovery within the data center, consider disabling SSL on the replication channel. Removing the encryption algorithm enables a higher replication throughput.
7. Always enable SSL when replication is across a wide-area-network.
8. Do not perform **rollback** operations on the projects or shares either at the primary site or at the standby site. Performing a rollback operation on the Sun ZFS Storage 7320 appliance invalidates the replication configuration. It will need to be configured again.

9. To maintain data consistency between tiers, ensure that the database and application tiers are replicated at the same time. This helps ensure that the different tiers recover to the exact point in time or as close as possible.
10. Configure Oracle Data Guard in the Managed Recovery Mode.
11. Configure Oracle Data Guard in the "Maximum Availability" data protection mode or in the "Maximum Protection" data protection mode
    a. The "Maximum Availability" data protection mode enables the highest level of data protection that is possible without compromising the availability of the primary database.
    b. The "Maximum Protection" data protection mode enables the standby database to be synchronous with the primary. This mode ensures zero data loss. This data protection mode prioritizes data protection over primary database availability.
12. It is recommended to 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.
13. The application tier and database tier on the primary site must be manually synchronized with the standby site after making configuration changes or after deploying new applications or after applying patches.
14. Oracle does not recommend synchronizing the local hard drives on the compute nodes.

Disaster Recovery Testing

The following disaster recovery operations were tested using the deployment created for this paper.

SITE GUARD OPERATION NAME	DESCRIPTION
Stop-Site-A	Bring down the application and database at the primary site
Start-Site-A	Bring up the application and database at the primary site
Switchover-to-Site-B	Switch over operations from primary to standby site
Switchback-to-Site-A	Switch operations back to primary site from standby site
Failover-to-Site-B	Fail over operations from primary to standby site

Appendix

Disaster Recovery Terminology

TERM	DEFINITION
Disaster Recovery	The ability to safeguard against natural disasters or unplanned outages at a primary site by having a recovery strategy for failing over applications and data to a geographically separate standby site.
Topology	The primary site and standby site hardware and software components that comprise an Oracle Fusion Middleware Disaster Recovery solution
Site Failover	The process of making the current standby site the new primary site after the primary site becomes unexpectedly unavailable (for example due to unplanned downtime at the primary site)
Site Switchover	The process of reversing the roles of the primary site and standby site. Switchovers are planned operations on the current primary site. During a switchover, the current standby site becomes the new primary site and the current primary site becomes the new standby.
Site Switchback	The process of reversing the roles of the new primary site (old standby) and new standby site (old primary). Switchback is applicable after a previous switchover.
Site Instantiation	The process of creating a topology at the standby site (after verifying that the primary and standby sites are valid for Oracle Fusion Middleware Disaster Recovery) and synchronizing the standby site with the primary sites so that the primary and standby sites are consistent.
Site Synchronization	The process of applying changes made to the primary site at the standby site. For example, when a new application is deployed at the primary site, you should perform synchronization so that the same application will be deployed at the standby site.
Recovery Point Objective (RPO)	Maximum age of the data you want the ability to restore in the event of a disaster. For example, if your RPO is six hours, you want to be able to restore the systems back to the state that they were in six hours ago.
Recovery Time Objective (RTO)	Time needed to recover from a disaster. This is usually determined by how long you can afford to be without your systems.

Sun ZFS Storage 7320 Terminology

OPERATION	DESCRIPTION
Source	The site being replicated from. Usually the primary site.
Target	The site being replicated to. Usually the standby site. A target can receive one or more packages from one or more Sun ZFS Storage 7320 Appliances. In this FMW infrastructure, the target site is the standby site.
Replica/Package	The replicated copy of the project at the target site. It cannot be accessed directly. In order to access the replica, it has to be cloned and the clone is accessed for read/write operations
Snapshot	Point-in-time read-only copy of the share, used for share rollbacks and creating clones.
Clone	Read-writable copy of a snapshot. One or more clones of the share are created from a snapshot.
Export Replica	Process to access the replica at the target. A new project is created. All the shares, snapshots,

	clones, and so on, are all accessible under the cloned project.
Role Reversal	The direction of the replication is reversed from source → target to target -> source for a package.

Oracle Site Guard Terminology

TERM	DEFINITION
Site	A 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.
Site Failover	The process of making the current standby site the new primary site after the primary site becomes unexpectedly unavailable (for example, due to a disaster at the primary site). This paper also uses the term "failover" to refer to a site failover.
Site Switchover	The process of reversing the roles of the primary site and standby site. Switchovers are planned operations done for periodic validation or to perform planned maintenance on the current primary site. During a switchover, the current standby site becomes the new primary site, and the current primary site becomes the new standby site. This paper also uses the term "switchover" to refer to a site switchover.
Site Guard Configuration	An Oracle Site Guard configuration contains settings such as, site creation, pre-scripts or post-scripts, storage, and credentials that are applicable to its operations.
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.
Generic System	A Generic 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 Manger, you would first create a System, that consists of the database, listener, application server, and hosts targets on which the applications run.
Operation Plan	An operation plan contains the flow of execution for a particular Oracle Site Guard operation. It defines the order in which the steps of an operation plan should be executed, in addition to other attributes, such as, serial, parallelism, and so on.
Fusion Instance	A Fusion instance target represents one or more Fusion product families, which in turn contain Fusion products and Fusion Cluster Application instances.

Storage Scripts

All the storage scripts used in this deployment come bundled with Oracle Site Guard, and were used with no modifications. The table below lists the bundled scripts used.

SCRIPT NAME	PURPOSE
zfs_storage_role_reversal.sh	Top level shell script that triggers the storage role reversal. This script invokes the other AKSH action scripts as required.

retrieve_replication_action_source.aksh	Retrieves replication action and action UUID from source appliance.
retrieve_replication_source_target.aksh	Retrieves replication source from target appliance.
validate_source.aksh	Validates that at least one sync was performed on the source appliance.
validate_target.aksh	1. Validates that at least one sync was performed on the target appliance. 2. Validates that replicated package has at least one implicit snapshot. 3. Validates that all mount points in the replicated package are unique across all the mount point on target appliance.
retrieve_replication_properties_source.aksh	Retrieves all replication properties from source appliance.
sync_project_source.aksh	Performs a sync before storage role reversal.
break_replication_source.aksh	Breaks replication before performing role reversal.
role_reverse_storage_target.aksh	Performs the actual reversal on the target appliance.

Custom Pre and Post Scripts

These are some of the additional Pre scripts that were used for the Oracle Site Guard configuration.

The Oracle Business Intelligence deployment used in this paper, requires Oracle Process Manager and Notification Server (OPMN) components to be started and stopped on each Weblogic Managed Server host. Custom Pre scripts are required to start and stop OPMN components.

start_bi_opmn.sh

This script starts all the OPMN components on an apphost node.

```
# start_bi_opmn.sh – apphost1
/u01/app/oracle/admin/instances/instance1/bin/opmnctl startall
```

stop_bi_opmn.sh

This script stops all the OPMN components on an apphost node.

```
# stop_bi_opmn.sh – apphost 1
/u01/app/oracle/admin/instances/instance1/bin/opmnctl stopall
```

mount.sh

This script mounts all the NFS shares on an apphost node.

```
# mount.sh – apphost 1
```

```
/bin/mount /u01/app/oracle/product/fmw
/bin/mount /u01/app/oracle/admin/bifoundation_domain/aserver
/bin/mount /u01/app/oracle/admin/bifoundation_domain/mserver
/bin/mount /u01/app/oracle/admin/bifoundation_domain/bi_cluster
/bin/mount /u01/app/oracle/admin/instances/instance1
```

unmount.sh

This script un-mounts all the NFS shares on an apphost node.

```
# unmount.sh – app host 1
/bin/umount -l /u01/app/oracle/product/fmw
/bin/umount -l /u01/app/oracle/admin/bifoundation_domain/aserver
/bin/umount -l /u01/app/oracle/admin/bifoundation_domain/mserver
/bin/umount -l /u01/app/oracle/admin/bifoundation_domain/bi_cluster
/bin/umount -l /u01/app/oracle/admin/instances/instance1
```

rm_wls_lockfiles.sh

This Pre script removes Weblogic server lock files. In the case of a Weblogic server crash, lock files may get left behind and they can prevent the server from re-starting.

```
# rm_wls_lockfiles.sh
# Set $ASERVER_DOMAIN_HOME to your weblogic admin server’s domain home
(e.g., /u01/app/oracle/admin/bifoundation_domain/aserver)
# Set $MSERVER_DOMAIN_HOME to your weblogic managed server’s domain home
(e.g., /u01/app/oracle/admin/bifoundation_domain/mserver)
find $ASERVER_DOMAIN_HOME –name ‘*.lok’ | xargs rm –f
find $MSERVER_DOMAIN_HOME –name ‘*.lok’ | xargs rm -f
```

Oracle Traffic Director

If Oracle Traffic Director (OTD) is deployed instead of, or in addition to Oracle HTTP Server, the Pre scripts shown below can be used for starting and stopping OTD.

The following OTD version is recommended for use with the other components deployed in this paper.

- Oracle Traffic Director 11.1.1.7

start_otd.sh

This script starts Oracle Traffic Director components.

```
# start_otd.sh
$OTD_INSTANCE/admin-server/bin/startserv
$OTD_INSTANCE/<sample_config>/bin/startserv
```

stop_otd.sh

This script stops Oracle Traffic Director components.

```
# stop_otd.sh
$OTD_INSTANCE/admin-server/bin/startserv
$OTD_INSTANCE/<sample_config>/bin/startserv
```

References

1. Oracle Maximum Availability Architecture Web site
   http://www.oracle.com/technetwork/database/features/availability/maa-090890.html

2. Oracle Fusion Middleware Disaster Recovery Guide

   http://download.oracle.com/docs/cd/E14571_01/doc.1111/e15250/toc.htm

3. Oracle Exalogic Enterprise Deployment Guide

   http://download.oracle.com/docs/cd/E18476_01/doc.220/e18479/toc.htm

4. Oracle Exalogic Multirack Cabling Guide

   http://docs.oracle.com/cd/E18476_01/doc.220/e18481/toc.htm

5. Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intelligence

   http://docs.oracle.com/cd/E28280_01/doc.1111/e15722/toc.htm

6. Oracle Exalogic Documentation Library

   http://download.oracle.com/docs/cd/E18476_01/index.htm

7. Oracle Exadata Storage Server and Oracle Exadata Database Machine Documentation

   Documentation can be found on the Exadata Storage cell in `/opt/oracle/cell/doc`

8. Oracle Data Guard: Disaster Recovery Best Practices for Exadata Database Machine

   http://www.oracle.com/technetwork/database/features/availability/maa-wp-dr-dbm-130065.pdf

9. Oracle Database 11.2 Documentation Library

   http://www.oracle.com/pls/db112/homepage

10. Oracle Database High Availability Library
    http://www.oracle.com/pls/db112/portal.portal_db?selected=14

11. Oracle Fusion Middleware High Availability Guide

    http://docs.oracle.com/cd/E14571_01/core.1111/e10106/toc.htm

12. Oracle Enterprise Manager Cloud Control Documentation Library

    http://docs.oracle.com/cd/E24628_01/index.htm

13. Using Oracle Site Guard (Oracle Enterprise Manager Lifecycle Management Administrator's Guide)

    http://docs.oracle.com/cd/E24628_01/em.121/e27046/site_guard.htm

14. Sun ZFS Storage System Administration Guide

    http://docs.oracle.com/cd/E22471_01/html/820-4167/

Automating Disaster Recovery using Oracle Site
Guard for Oracle Exalogic Database Machine
July 2013

Authors: Shekhar Borde, Lingaraj Nayak
Contributing Authors: Pradeep Bhat, Praveen
Sampath, Susan Kornberg

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200