



Oracle Application Disaster Recovery Using Site Guard



On Oracle Private Cloud
Appliance and Exadata
Database Machine

January 2021 | Version 1.0
Copyright © 2021, Oracle and/or its affiliates
Public

PURPOSE STATEMENT

This document provides a description, a summary of requirements, and the setup procedure for Oracle Site Guard to manage Application-level switchover and failover of Oracle applications such as EBS, Siebel and Peoplesoft. The steps described in this whitepaper apply to hardware configurations where Oracle Private Cloud Appliance hosts the application tier and Oracle Exadata hosts the Oracle Database tier. This paper is oriented to a technical audience having knowledge of Oracle Enterprise Manager, Oracle Site Guard, Oracle Private Cloud Appliance, Oracle ZFS Storage Appliance, Oracle Database, and Oracle Data Guard.

DISCLAIMER

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

TABLE OF CONTENTS

Purpose Statement	1
Disclaimer	1
Introduction	4
ORACLE Site Guard for APPLICATION-LEVEL Disaster Recovery	5
Initial Setup	5
Special Considerations for ZFS Storage Role Reversal	6
Enterprise Manager Cloud Control Setup	6
1. Create an administrator account for Site Guard Administration	7
Network Setup	8
1. Hostnames setup	8
2. Security	8
Agent Installation	8
Discover Database Targets	8
Site Guard Configuration	9
2. Create named credentials	9
3. Configuring preferred credentials	10
4. Defining Primary and Standby Site Systems in EM	10
5. Defining Site Roles	11
6. Credential associations	11
7. Configuring required scripts	11
8. Configuring apply and transport lag thresholds (optional)	15
9. Creating switchover and failover operation plans	15
Performing a Switchover with Site Guard	18
Performing a Failover with Site Guard	19
Conclusion	19
APPENDIX A: Install EM Agent AND DISCOVER TARGETS	20
Install EM Agent Using Agent Deploy Method	20
1. Get the agent software	20
2. Install the agent	20
Target Discovery	22
1. Promoting automatically discovered targets	22
2. Discover ASM targets	22
3. Discover Database targets	23
4. Target Host preparation	24
Appendix B. PeopleSOFT DISASTER RECOVERY USING SITE GUARD	26
Site Guard Configuration	26
1. Create named credentials	26
2. Configuring preferred credentials	27
3. Defining Primary and Standby Site Systems in EM	27
4. Defining Site Roles	28
5. Credential associations	28
6. Configuring required scripts	28
7. Configuring apply and transport lag thresholds (optional)	31
8. Creating switchover and failover operation plans	31
Appendix C. SIEBEL DISASTER RECOVERY USING SITE GUARD	34
Site Guard Configuration	34
1. Create named credentials	34

2.	Configuring preferred credentials	35
3.	Defining Primary and Standby Site Systems in EM	35
4.	Defining Site Roles	36
5.	Credential associations	36
6.	Configuring required scripts	36
7.	Configuring apply and transport lag thresholds (optional)	39
8.	Creating switchover and failover operation plans	39

APPENDIX D. How to setup a service host for Site Guard use	42
---	-----------

INTRODUCTION

Oracle's Maximum Availability Architecture (Oracle MAA) is the best practices blueprint for data protection and availability of Oracle products (Database, Fusion Middleware, Applications) deployed on on-premises, private, public or hybrid clouds. Implementing Oracle Maximum Availability Architecture best practices is one of the key requirements for any Oracle deployment: any critical system needs protection from unforeseen disasters and natural calamities.

Oracle's Maximum Availability Architecture (Oracle MAA) Application-Level disaster recovery solutions are based on an active-passive topology: there is one system in one site with primary role and a secondary system in another site with the standby role. The switchover is a planned procedure that changes the roles between these two sites: the primary site becomes the standby and the secondary takes the primary role. This role change happens also during a failover procedure. The failover procedure is usually an unplanned event that must be performed when the primary is unavailable. Both procedures consist of various steps to stop/start different components and perform the database and ZFS role change. These steps can be performed manually as described in the MAA application disaster recovery white papers or you can configure Oracle Site Guard to orchestrate the full stack switchover steps. This document explains how to achieve this. It includes detailed steps to configure Site Guard for the Application-Level Disaster Recovery environment and how to manage the switchover/failover using Site Guard operation plans.

This paper is intended for a technical audience having knowledge of Oracle Enterprise Manager, Oracle Site Guard, Oracle Private Cloud Appliance, Oracle ZFS Storage Appliance, Oracle Exadata, Oracle Database and Oracle DataGuard.

ORACLE SITE GUARD FOR APPLICATION-LEVEL DISASTER RECOVERY

[Oracle Site Guard](#) is a disaster-recovery (DR) solution that enables administrators to automate complete site switchover or failover. It orchestrates the coordinated failover of Oracle Applications, Oracle Databases and Oracle ZFS Storage. It is also extensible to include other data center software components. Oracle Site Guards offers the following benefits:

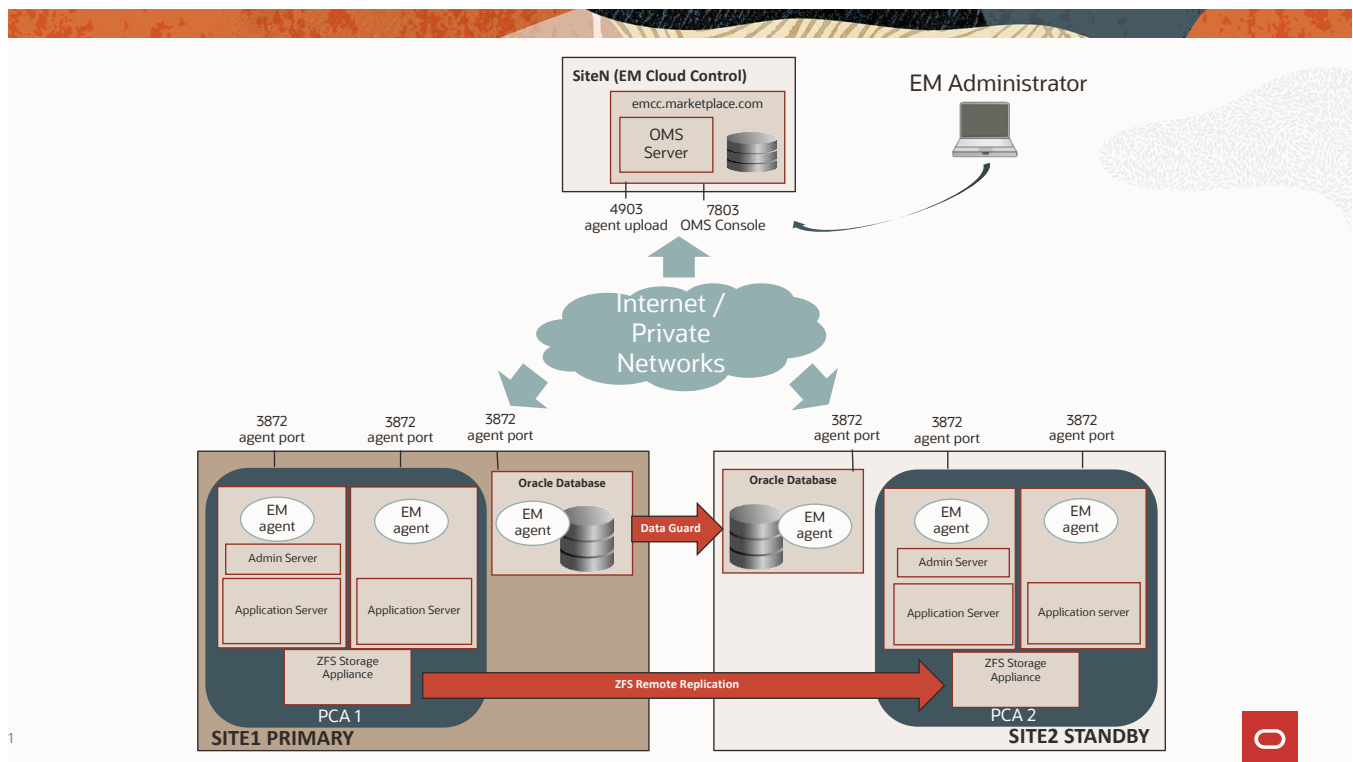
- Fully automate disaster recovery operations and launch them with a single click
- Minimizes disaster-recovery time
- Reduces human errors
- Flexible and customizable
- Eliminates the need for special skills
- Use a single pane of glass to manage disaster recovery
- Assure disaster recovery readiness using on-demand or scheduled disaster recovery drills

Oracle Site Guard is included in Enterprise Manager Cloud Control Fusion Middleware Plugin. Enterprise Manager Cloud Control Management Server and Agent deployment is required to use Oracle Site Guard.

Oracle Site Guard can be used to orchestrate the switchovers for Oracle Application Disaster Recovery scenarios that follow the MAA best practices described in the following whitepapers:

- PeopleSoft Maximum Availability Architecture on Private Cloud Appliance and Exadata
- EBS Maximum Availability Architecture on Private Cloud Appliance and Exadata
- Siebel Maximum Availability Architecture on Private Cloud Appliance and Exadata

A sample Oracle Application Disaster Recovery with Site Guard topology is shown below:



Notice that a single EM installation like the one described in this document can be used to orchestrate and manage multiple Disaster Protection systems. Oracle strongly recommends that Enterprise Manager be deployed at a third site that is not vulnerable to outages that may affect the primary or standby sites.

INITIAL SETUP

The following steps are required to accomplish this setup:

- **Enterprise Manager Cloud Control Setup**
Install and configure the EM Cloud Control Oracle Management Server. The Enterprise Manager Cloud Control Server can be located in the same site of one of the systems or in a different site. However, Oracle strongly

recommends that Enterprise Manager be deployed at a third site that is not vulnerable to outages that may affect the primary or standby sites.

- **Network Setup**
Create the required network rules to allow the communications between targets and Oracle Enterprise Manager's management server (OMS).
- **Agent Installation**
Install Enterprise Manager Cloud Control Agents in the Oracle Application VM and Database environment hosts.
- **Target Discovery**
Discover the targets that will be managed by the Site Guard (Application Tier Hosts, Databases, etc.)
- **Site Guard Configuration**
Configure Site Guard (sites, credentials, scripts, plans, etc.) to orchestrate the switchover and failover in the Oracle Application DR environment.

It is expected that the required Enterprise Manager Cloud Control licenses with Oracle Site Guard are used. Basic technical background on Enterprise Manager Cloud Control concepts and administration is assumed for completing the setup. Refer to the next sections for details on each one of the steps.

Special Considerations for ZFS Storage Role Reversal

All of the Application Tier shared file systems are stored on a ZFS Storage Appliance. If Oracle Private Cloud Appliance is prior to X8 an external ZFS Storage Appliance must be used. If the Oracle Private Cloud appliance is X8 or later the internal ZFS Storage Appliance may be used. When Application Tier data is stored on the internal ZFS Storage Array, Oracle Advanced Customer Services should be engaged to configure the necessary external interfaces required to support ZFS remote replication.

The file systems are exported from ZFS and are mounted with NFS by all mid tier servers. Specific shared file systems are replicated to the secondary disaster recovery site using ZFS remote replication.

A Host must be selected that allows Oracle Site Guard to execute scripts that perform ZFS Storage role reversal. The host must be an Enterprise Manager target. An Enterprise Manager agent must be installed on the host.

- The host must have network access to the ZFS Storage Appliances used by the Oracle Private Cloud Appliances at the Primary and Standby sites.

If the shared filesystems are stored on Oracle Private Cloud Appliance X8 internal ZFS Storage Array a management node can be configured as a bastion/service host and an EM agent installed on it to provide direct access to the internal ZFS Storage Array.

There are at least four ways to deploy this bastion/service host:

- The bastion/service host could be the management node itself. The drawback to this deployment is that the Site Guard software components and dependencies can be lost during periodic upgrade or maintenance, requiring re-installation.
- The bastion/service host could be an Oracle VM guest deployed in Oracle Private Cloud Appliance and managed by Oracle VM Manager. This deployment requires the addition of a management network to the bastion Oracle VM guest. See *How to Create Service Virtual Machines on the Private Cloud Appliance by using Internal Networks (Doc ID 2017593.1)*.
- The bastion/service host could be a separate server independent of the Oracle Private Cloud Appliance. Typically, it is in a separate rack with a cable connecting it to the Oracle Private Cloud Appliance's internal Oracle Switch ES1-24.
- The bastion/service host could be an Oracle VM guest deployed on an Oracle VM Server independent of Oracle Private Cloud Appliance. Like the previous deployment, the physical server is in a separate rack with a cable connecting it to the Oracle Private Cloud Appliance's internal Oracle Switch ES1-24.

Another option is to add a Host Network to the Oracle Private Cloud Appliance. This would be a custom network configured to provide connectivity to Oracle VM servers from the public network. See the *Network Customization* section of the *Oracle® Private Cloud Appliance Administrator's Guide* for more information.

See [Appendix D](#) for an example on how to setup a service host guest VM for Site Guard use.

The internal ZFS Storage Appliance administration shell can only be accessed via the Oracle Private Cloud Appliance internal network. Site Guard's ZFS role reversal script (`zfs_storage_role_reversal.sh`) requires an entry in `.ssh/config` of the bastion host user running the EM agent to provide access:

```
Host pca3zfs.cloud.osc.oracle.com <--- remote replication FQDN
HostName 192.168.4.100      <--- internal ZFS Storage Array VIP
User root                   <--- root user
```

Enterprise Manager Cloud Control Setup

If you already have an Enterprise Manager Cloud Control installed and configured, you can skip this step and continue with the rest of the sections (network setup, agent installation, Site Guard configuration).

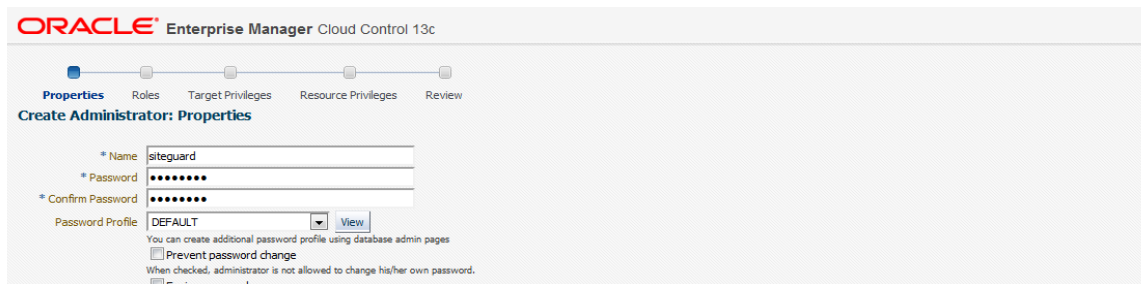
If you do not have an Enterprise Manager Cloud Control, you can follow the steps in [Oracle Enterprise Manager Cloud Control Installation and Configuration](#) to create and configure an Enterprise Manager.

1. Create an administrator account for Site Guard Administration

It is best practice to create a separate administrator account so only authorized systems administrators have the ability to trigger site transitions. Create Site Guard administrator accounts using SYSMAN, the default administrator account, or an administrator account with like privileges.

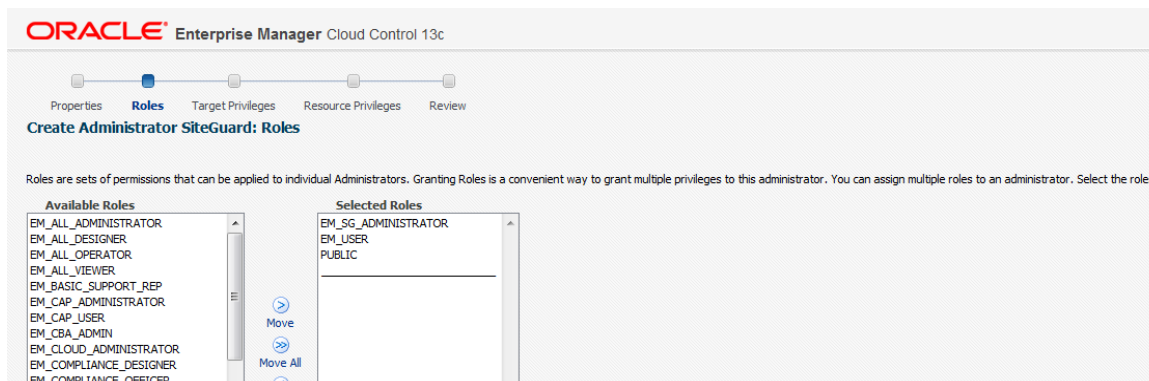
a) Create Account

Super Administrator access is not required for the Site Guard account.



b) Add Roles to Siteguard Account

This is the minimum needed to create a valid account, but the operating standards for your data center may require other privileges and resources not covered in this document. Please consult your organization's standard operating procedures for more requirements specific to your data center.



Please ensure the Site Guard administrator has the following roles:

- EM_SG_ADMINISTRATOR: Site Guard Administrator
- EM_USER: Role has privilege to access Enterprise Manager Application
- PUBLIC: The role granted to all administrators. This role can be customized at site level to group privileges that need to be granted to all administrators

Network Setup

1. Hostnames setup

Enterprise Manager hostname and its monitored hosts must be mutually resolvable. Primary and Standby sites are typically located in different datacenters, and Enterprise Manager Cloud Control OMS can be located in one of them or in another different datacenter.

When there is no internal communication between the datacenters, Enterprise Manager Cloud Control OMS and Host DR targets will communicate each other via their public IPs. Oracle recommends using hostnames associated to the public IPs of the hosts. This can be done by registering them in a DNS server or by configuring the name resolution in the `/etc/hosts` file of the OMS and target hosts.

2. Security

Oracle Management Servers need to communicate with the agents in the monitored hosts, and the agents connect to OMS server to upload the monitoring data. For database monitoring, OMS must be able to connect to the target database. All this traffic is encrypted given that secured protocols are used (HTTPS, t3s and SQL*NET with network encryption¹). The following communications are required between the OMS and the monitored targets:

SOURCE	DESTINATION	PROTOCOL
Any Monitored Host	OMS Upload port (usually 4903)	HTTPS
OMS host	Any monitored host agent port (3872)	HTTPS
OMS host	Any target database listener port	SQL (with Network Encryption)
OMS host	Any monitored host ssh port (22)	SSH (for agent software transfer)
Internet(*)	OMS console port (usually 7803)	HTTPS

Agent Installation

Enterprise Manager Cloud Control Agent must be installed on all application tier and DB hosts in the DR environment. Refer to [Installing Oracle Management Agents](#) in the [Enterprise Manager Cloud Control Basic Installation Guide](#). Upon completion the application tier and DB hosts will be discovered as Host Targets. No further discovery is required for the application tiers. The next step is to discover Database Targets on the discovered DB Host targets

Discover Database Targets

Site Guard requires that the application databases be discovered as Database Targets. Refer to [Discovering and Adding Database Targets](#) in the [Enterprise Manager Cloud Control Administrator's Guide](#).

NOTE: Refer to [Appendix A](#) for a detailed example of installing agents and discovering targets using the Agent Deployment method.

Site Guard Configuration

The steps described in this section are based on the [Site Guard Administrator's Guide for Enterprise Manager Cloud Control version 13.4](#). Oracle E-Business Suite (EBS) will be used as the example application. Refer to [Appendix B](#) for Peoplesoft and [Appendix C](#) for Siebel.

1. Create named credentials

You must create named credentials for the targets associated with Oracle Site Guard for application tier hosts, db hosts Oracle Databases. This table summarizes the named credentials required for managing EBS application-level DR with Oracle Site Guard:

CREDENTIAL NAME	AUTHENTICATION TARGET TYPE	CREDENTIAL TYPE	CREDENTIAL SCOPE	TARGET USERNAME	DESCRIPTION
EBS_APPLMGR_CRED	Host	Host Credential	Global	applmgr	App Tier User Credentials
EBS_ROOT_CRED	Host	Host Credential	Global	root	App Tier Root Credentials
EXADATA_ORACLE_CRED	Host	Host Credential	Global	oracle	Oracle User Credentials
EXADATA_DB_SYS_CRED	Database Instance	Database Credential	Global	sys as sysdba	SYSDBA Credentials

NOTE: Credentials are the same for the primary and standby app tier and db hosts so using global credentials instead of targeted credentials simplifies the configuration.

a) Create EBS Application Named Credentials

To create the credentials described in the table above:

- Login to Enterprise Manager Cloud Control console
- Navigate to Setup > Security > Named Credentials.
- Click Create, and create the named credentials as described in the table
- Test and Save.
- Repeat the same to create all and any other additional credentials you need for the host.

This table summarizes the named credentials for managing ZFS storage role reversal:

CREDENTIAL NAME	AUTHENTICATION TARGET TYPE	CREDENTIAL TYPE	CREDENTIAL SCOPE	TARGET USERNAME	DESCRIPTION
SITE1_ZFS_CRED	Host	Host Credential	Global	root	ZFS Root Credentials
SITE2_ZFS_CRED	Host	Host Credential	Global	root	ZFS Root Credentials
SITE1_BASTION_HOST_CRED	Host	Host Credential	Global	oracle	EM Agent User Credentials
SITE2_BASTION_HOST_CRED	Host	Host Credential	Global	oracle	EM Agent User Credentials

b) Create ZFS Named Credentials

To create the credentials described in the table:

- Login to Enterprise Manager Cloud Control console
- Navigate to Setup > Security > Named Credentials.
- Click Create, and create the named credentials as described in the table
- Save.

- A warning will be displayed asking you to confirm saving without testing the connection, Select OK
- The ZFS Storage Arrays are not Discovered Host Targets, so you will not be able to test the connection.

c) Create Bastion Host Named Credentials

To create the credentials described in the table:

- Login to Enterprise Manager Cloud Control console
- Navigate to Setup > Security > Named Credentials.
- Click Create, and create the named credentials as described in the table
- Test and Save.

2. Configuring preferred credentials (optional)

Once the named credentials have been created, they can be assigned to the targets as the preferred credentials. This approach is recommended to simplify the Site Guard configuration. Follow these steps to configure the preferred credentials for a target:

- Login to Enterprise Manager Cloud Control console
- Navigate to Setup > Security > Preferred Credentials
- Select a target type (Database Instance, Hosts, etc.), and click “Manage Preferred Credentials”.
- Set the preferred credentials for each target credential, by clicking each row, “Set” and selecting the appropriate named credential created in the previous step.
- Do this for the following targets:
 - **Primary and Standby Database Instances** (at minimum, sysdba credentials, database hosts credentials)
 - **Primary and Standby App Tier Hosts**
 - **Primary and Standby Bastion Hosts**

3. Defining Primary and Standby Site Systems in EM

A disaster recovery site managed by Oracle Site Guard is modeled as a Generic System target type in Oracle Enterprise Manager. Follow these steps to create the Generic System that models the Primary (active) site, EBS_SITE1:

NOTE: In the rest of the steps EBS_SITE1 will be the Primary site and EBS_SITE2 will be the Standby site.

- Login to Enterprise Manager Cloud Control console
- Go to Targets > Systems
- Click Add > Generic System
- Generic System: General Screen
- Enter a Name for the System. For example: EBS_SITE1.
- You can optionally add system properties (Department, Line of Business, Location, etc.)
- Add members to the system. For the primary site add:
 - The **primary EBS Host Targets**
 - The **primary Database Instance Target**
 - The **primary PCA Bastion Host Target**
 - The **standby PCA Bastion Host Target**

NOTE: Do NOT add the database system itself. The Data Guard system that is part of will be added and it will include primary and standby databases.

- Click Next
- Generic System: Define Associations.** You can leave defaults and click Next.
- Generic System: Availability Criteria.** You can add database as key member and click Next.
- Generic System: Charts Screen.** You can leave defaults and click Finish.

Repeat same steps to create the standby site system, EBS_SITE2, using the standby targets.

4. Defining Site Roles

Once a disaster recovery site managed by Oracle Site Guard has been modeled as a Generic System target in Oracle Enterprise Manager, you designate it as a primary site or a standby site. This is done following these steps:

- Login to Enterprise Manager Cloud Control console, go to **Targets > Systems**
- Click on the name of the **primary** site system, EBS_SITE1.
- On the system's home page, from the Generic System menu, select **Site Guard > Configure**.
- On the **General** tab, click **Create**
- On the **General** tab, in the **Standby System(s)** section, click **Add**.
- Choose the **standby** system, EBS_SITE2, and click **Select**.
- Click **Save** and **OK** to confirm the action. Site Guard saves the standby system configuration.
- Verify that the roles have been assigned:
In the primary Site system, EBS_SITE1, in Oracle Site Guard Configuration, General Tab, you must see:
Current Role Primary
In the secondary Site system, EBS_SITE2, in Oracle Site Guard Configuration, General Tab, you must see:
Current Role Standby

5. Credential associations

Credentials are associated with targets and used by Oracle Site Guard operation plans when they are executed. These associations must be configured for primary and standby systems:

- Login to Enterprise Manager Cloud Control console.
- From the Targets menu, click **Systems**
- On the Systems page, click the name of the system for which you want to configure credential associations.
- On the system's home page, from the Generic System menu, select **Site Guard > Configure**.
- Click the Credentials tab. Now associate the different types of credentials
- Normal Host Credentials** section, click **Add**, select **All** and check **Preferred**, Normal Host Credentials. Click **Save**.
- Privileged Host Credentials** are required for the app tier hosts. Privileged credentials are used to execute scripts that mount and unmount NFS filesystems.
- SYSDBA Database Credentials** section, click **Add**, select **All** and **Preferred**, "SYSDBA Database Credentials". Click **Save**

Repeat the same for the standby system.

6. Configuring required scripts

Oracle Site Guard provides a mechanism for you to configure scripts for managing disaster recovery operations. The scripts for EBS disaster recovery can be found in the EBS Maximum Availability Architecture on Private Cloud Appliance and Exadata whitepaper. Different kind of scripts can be defined for Site Guard:

SCRIPT TYPE	SCRIPT PATH	OPERATION	ROLE	TARGET HOST
Pre Script	Following scripts will be run as pre-scripts: <ul style="list-style-type: none">/home/applmgr/EBSRoleChange/EBS_stopServices.sh	Switchover	Primary	All Primary App Tier Hosts
Post Scripts	Following scripts will be run as post-scripts: <ul style="list-style-type: none">/home/applmgr/EBSRoleChange/EBS_cleanUpStates.sh/home/applmgr/EBSRoleChange/set_webentry_prodURL_to_f5_LB.sh/home/applmgr/EBSRoleChange/EBS_autoconfig.sh/home/applmgr/EBSRoleChange/EBS_startWLSAdminServer.sh/home/applmgr/EBSRoleChange/EBS_startServices.sh	Switchover/ Failover	Standby	All Standby App Tier Hosts
Switchover Mount Unmount	Unmount EBS application NFS filesystem on primary: sh mount_umount.sh -o umount -f <nfs mount point>	Switchover	Primary	All Primary App Tier Hosts

Storage Scripts	Example: sh mount_umount.sh -o umount -f '/u02'			
	Mount EBS application NFS filesystem on standby: sh mount_umount.sh -o mount -f <nfs mount point> Example: sh mount_umount.sh -o mount -f '/u02'	Switchover/ Failover	Standby	All Standby App Tier Hosts
Switchover Role Reversal Storage Scripts	<p>Note: The source appliance is the ZFS Storage Appliance at the Primary Site and the target appliance is the ZFS Storage Appliance at the Standby Site. All of the scripts are entered at the Standby Site (EBS_Site2).</p> <pre>sh zfs_storage_role_reversal.sh --target_appliance <target remote replication FQDN> --source_appliance <source remote replication FQDN> --project_name <ZFS Project Name> --target_pool_name <Target Pool Name> --source_pool_name <Source Pool Name> --is_sync_needed N --continue_on_sync_failure Y --sync_timeout 1800 --operation_type opc_switchover --sub_operation_type get_action</pre> <pre>sh zfs_storage_role_reversal.sh --target_appliance <target remote replication FQDN> --source_appliance <source remote replication FQDN> --project_name <ZFS Project Name> --target_pool_name <Target Pool Name> --source_pool_name <Source Pool Name> --is_sync_needed N --continue_on_sync_failure Y --sync_timeout 1800 --operation_type opc_switchover --sub_operation_type get_source</pre> <pre>sh zfs_storage_role_reversal.sh --target_appliance <target remote replication FQDN> --source_appliance <source remote replication FQDN> --project_name <ZFS Project Name> --target_pool_name <Target Pool Name> --source_pool_name <Source Pool Name> --is_sync_needed N --continue_on_sync_failure Y --sync_timeout 1800 --operation_type opc_switchover --sub_operation_type get_replication_properties</pre> <pre>sh zfs_storage_role_reversal.sh --target_appliance <target remote replication FQDN> --source_appliance <source remote replication FQDN> --project_name <ZFS Project Name> --target_pool_name <Target Pool Name> --source_pool_name <Source Pool Name> --is_sync_needed N --continue_on_sync_failure Y --sync_timeout 1800 --operation_type opc_switchover --sub_operation_type role_reverse</pre>	Switchover	Standby	Primary Bastion Host Standby Bastion Host Primary Bastion Host Standby Bastion Host
Example Switchover Role Reversal Storage Scripts	<pre>sh zfs_storage_role_reversal.sh --target_appliance pca1zfs.cloud.osc.oracle.com --source_appliance pca3zfs.cloud.osc.oracle.com --project_name MAA_EBS --target_pool_name Pool01 --source_pool_name OVCA_POOL --is_sync_needed N --continue_on_sync_failure Y --sync_timeout 1800 --operation_type opc_switchover --sub_operation_type get_action</pre> <pre>sh zfs_storage_role_reversal.sh --target_appliance pca1zfs.cloud.osc.oracle.com --source_appliance pca3zfs.cloud.osc.oracle.com --project_name MAA_EBS --target_pool_name Pool01 --source_pool_name OVCA_POOL --is_sync_needed N --continue_on_sync_failure Y --sync_timeout 1800 --operation_type opc_switchover --sub_operation_type get_source</pre> <pre>sh zfs_storage_role_reversal.sh --target_appliance pca1zfs.cloud.osc.oracle.com --source_appliance pca3zfs.cloud.osc.oracle.com --project_name MAA_EBS --target_pool_name Pool01 --source_pool_name OVCA_POOL --is_sync_needed N --continue_on_sync_failure Y --sync_timeout 1800 --operation_type opc_switchover --sub_operation_type get_replication_properties</pre> <pre>sh zfs_storage_role_reversal.sh --target_appliance pca1zfs.cloud.osc.oracle.com --source_appliance pca3zfs.cloud.osc.oracle.com</pre>			pca3bastion pca1bastion pca3bastion pca1bastion

```
--project_name MAA_EBS --target_pool_name Pool01 --source_pool_name
OVCA_POOL --is_sync_needed N --continue_on_sync_failure Y --
sync_timeout 1800 --operation_type opc_switchover --sub_operation_type
role_reverse
```

Failover Role Reversal Storage Scripts

Note: The source appliance is the ZFS Storage Appliance at the Primary Site and the target appliance is the ZFS Storage Appliance at the Standby Site. The scripts execute on a bastion host configured on the Standby PCA.

```
sh zfs_storage_role_reversal.sh --target_appliance <target remote replication FQDN> --source_appliance <source remote replication FQDN> --project_name <ZFS Project Name> --target_pool_name <Target Pool Name> --source_pool_name <Source Pool Name> --is_sync_needed N --continue_on_sync_failure Y --sync_timeout 1800 --operation_type _opc_failover --sub_operation_type get_source
```

```
sh zfs_storage_role_reversal.sh --target_appliance <target remote replication FQDN> --source_appliance <source remote replication FQDN> --project_name <ZFS Project Name> --target_pool_name <Target Pool Name> --source_pool_name <Source Pool Name> --is_sync_needed N --continue_on_sync_failure Y --sync_timeout 1800 --operation_type _opc_failover --sub_operation_type role_reverse
```

Failover

Standby

Standby
PCA
Bastion
Host

Example
Failover
Role
Reversal
Storage
Scripts

```
sh zfs_storage_role_reversal.sh --target_appliance
pca1zfs.cloud.osc.oracle.com --source_appliance pca3zfs.cloud.osc.oracle.com
--project_name MAA_EBS --target_pool_name Pool01 --source_pool_name
OVCA_POOL --is_sync_needed N --continue_on_sync_failure Y --
sync_timeout 1800 --operation_type opc_failover --sub_operation_type
get_source

sh zfs_storage_role_reversal.sh --target_appliance
pca1zfs.cloud.osc.oracle.com --source_appliance pca3zfs.cloud.osc.oracle.com
--project_name MAA_EBS --target_pool_name Pool01 --source_pool_name
OVCA_POOL --is_sync_needed N --continue_on_sync_failure Y --
sync_timeout 1800 --operation_type opc_failover --sub_operation_type
role_reverse
```

pca1bastionpca1bastion

- Login to Enterprise Manager Cloud Control console, go to **Targets > Systems**
- Right-click the **EBS_SITE1** System
- Navigate to **Site Guard > Configure**
- Click the **Pre/Post** scripts tab
- Add **Pre-Scripts** to **EBS_SITE1** system:
 - Add Pre-scripts as described in the Pre-Scripts section of the table
- Add **Post-Scripts** to **EBS_SITE1** system:
 - Add Switchover Post-scripts as describe in the table
 - Add Failover Post-scripts as described in the Post Scripts section of the table

- Click the Storage Scripts tab
- Add the Switchover Storage Unmount Script

- a. Click Add
 - b. Click the Search icon (eyeglass) to the right of the Software Library Path edit box
 - c. Enter: 'Role Reverse Storage Scripts'
 - d. Select 'Role Reverse Storage Scripts' row with type 'Component'
 - e. Click Select
 - f. Insert "sh mount_umount.sh -o umount -f '/u02'" into Script Path
 - g. Select all app tier Target Hosts (do not select any non-app tier hosts)
 - h. Select 'Unmount' Script Type
 - i. Select 'Switchover' Operation Type
 - j. Expand Advanced Options and Select 'All Hosts'
 - k. Click Save
- c) Add the Switchover Storage Mount Script
 - a. Select Storage Unmount Script you just created
 - b. Click Add Like
 - c. Insert "sh mount_umount.sh -o mount -f '/u02'" into Script Path
 - d. Select all app tier Target Hosts (do not select any non-app tier hosts)
 - e. Select 'Mount' Script Type
 - f. Select 'Switchover' Operation Type
 - g. Expand Advanced Options and Select 'All Hosts'
 - h. Click Save
- d) Add the Failover Storage Mount Script:
 - a. Select Storage Mount Script you just created
 - b. Click Add Like
 - c. Insert "sh mount_umount.sh -o mount -f '/u02'" into Script Path
 - d. Select all app tier Target Hosts (do not select any non-app tier hosts)
 - e. Select 'Mount' Script Type
 - f. Select 'Failover' Operation Type
 - g. Expand Advanced Options and Select 'All Hosts'
 - h. Click Save
- e) Add the four Switchover ZFS Storage Role Reversal scripts
 - a. Click Add
 - b. Click the Search icon (eyeglass) to the right of the Software Library Path edit box
 - c. Enter: 'Role Reverse Storage Scripts'
 - d. Select 'Role Reverse Storage Scripts' row with type 'Component'
 - e. Click Select
 - f. Insert the `zfs_role_reversal.sh` switchover example from the table. Substitue your deployments source and target remote replication FQDNs, ZFS project name and source and target Pool Names.
 - g. Select the PCA Bastion Host Target
 - h. Select 'Storage-Switchover' Script Type
 - i. Select 'Switchover' Operation Type
 - j. Expand Advanced Options to add credentials to connect to ZFS Storage in this order:
 - i. Move the Primary PCA ZFS credential ('SITE1_ZFS_CRED') from Available Value to Selected Value
 - ii. Move the Standby PCA ZFS credential ('SITE2_ZFS_CRED') from Available Value to Selected Value
 - k. Click Save
- f) Add the two Failover ZFS Storage Role Reversal scripts
 - a. Click Add
 - b. Click the Search icon (eyeglass) to the right of the Software Library Path edit box
 - c. Enter: 'Role Reverse Storage Scripts'
 - d. Select 'Role Reverse Storage Scripts' row with type 'Component'
 - e. Click Select
 - f. Insert the `zfs_role_reversal.sh` failover example from the table. Substitue your deployments source and target remote replication FQDNs, ZFS project name and source and target Pool Names.
 - g. Select the PCA Bastion Host Target
 - h. Select 'Storage-Failover' Script Type
 - i. Select 'Failover' Operation Type
 - j. Expand Advanced Options to add credentials to connect to ZFS Storage in this order:
 - i. Move the Primary PCA ZFS credential ('SITE1_ZFS_CRED') from Available Value to Selected Value
 - ii. Move the Standby PCA ZFS credential ('SITE2_ZFS_CRED') from Available Value to Selected Value

- k. Click Save

To configure the EBS DR scripts for EBS_Site2:

- g) Login to Enterprise Manager Cloud Control console, go to Targets > Systems
- h) Right-click the EBS_SITE2 System
- i) Navigate to Site Guard > Configure
- j) Click the Pre/Post scripts tab
- k) Add **Pre-Scripts** to **EBS_SITE2** system:
 - Add Pre-scripts as describe in the Pre-Scripts section of the table
- l) Add **Post-Scripts** to **EBS_SITE2** system:
 - Add Switchover Post-scripts as describe in the table
 - Add Failover Post-scripts as described in the Post Scripts section of the table

To configure the Storage Scripts for EBS_SITE2 repeat the steps described for configuring the Storage Scripts for EBS_SITE1. The source and target parameters will be the reverse of what you specified for EBS_SITE1.

7. Configuring apply and transport lag thresholds (optional)

Site Guard verifies the apply and transport lag of the Data Guard during the prechecks and the switchover. By default, if the value is different than zero, the precheck fails and the switchover is not performed. You can define a threshold value to allow a few seconds so the check is more permissive. This step is optional. Example to set the thresholds to 10 seconds:

- a) Connect via SSH to the OMS host
- b) Login to emcli:

```
[oracle@emcc bin]$ cd $EM_HOME/middleware/bin
[oracle@emcc bin]$ ./emcli login -username=sysman
```

- c) Set the threshold to 10 seconds in both sites:

```
[oracle@emcc]$ ./emcli configure_siteguard_lag -system_name=EBS_SITE1 -property_name=apply_lag -value=10
[oracle@emcc]$ ./emcli configure_siteguard_lag -system_name=EBS_SITE2 -property_name=apply_lag -value=10
[oracle@emcc]$ ./emcli configure_siteguard_lag -system_name=EBS_SITE1 -property_name=transport_lag -value=10
[oracle@emcc]$ ./emcli configure_siteguard_lag -system_name=EBS_SITE2 -property_name=transport_lag -value=10
```

8. Creating switchover and failover operation plans

An operation plan describes the flow of execution that Oracle Site Guard performs in a disaster recovery operation. It consists of (ordered) actions that can be executed serially or in parallel. Oracle Site Guard creates a default version of the operation plan based on the site topology and the Oracle Site Guard configuration. You can use this default operation plan or customize it depending on your configuration.

The following operations plans are recommended for EBS DR:

PLAN	DESCRIPTION
EBS_SITE1_TO_SITE2_SWITCHOVER	Switchover from Site1 to Site2 where Site1 is the primary system and Site2 is the standby system. This is a planned transition where Site1 is gracefully shutdown prior to transition to Site2.
EBS_SITE2_TO_SITE1_SWITCHOVER	Switchover from Site2 to Site1 when Site2 is the primary system and Site1 is the standby system. This is a planned transition where Site2 is gracefully shutdown prior to transition to Site1.
EBS_SITE1_TO_SITE2_FAILOVER	Failover from Site1 to Site2 when Site1 is the primary system and Site2 is the standby system. A failover occurs as a result of an unplanned event when the primary site becomes unavailable.

EBS_SITE2_TO_SITE1_FAILOVER

Switchover from Site2 to Site1 when Site2 is the primary system and Site1 is the standby system. A failover occurs as a result of an unplanned event when the primary site becomes unavailable.

NOTE: To successfully execute a Site Guard operation plan the state of Site Guard configuration, Data Guard configuration and ZFS remote replication must be consistent. That is, if EBS_SITE1 generic system is the primary system in the Site Guard Configuration the Database Target associated with EBS_SITE1 must be the primary database in the Data Guard configuration and the ZFS project, not the replication package, must reside on the ZFS Storage Array attached to the PCA hosting the primary application tier hosts.

a) Create EBS_SITE1_TO_SITE2_SWITCHOVER

Operation plan for performing a switchover from EBS_SITE1 to EBS_SITE2.

- Login to Enterprise Manager Cloud Control console, go to **Target > Systems**
- Click in **EBS_Site1 System > Site Guard > Operations**.
- Click Create.
- Enter a name for the plan. Example: **EBS_SITE1_TO_SITE2_SWITCHOVER**
- Select Operation Type: Switchover
- Select the other site (EBS_SITE2) as the standby system
- Click Save
- The created plan will need to be customized. Edit the Post-Script steps to group scripts that can be executed in parallel and modify the order of execution:
 - Click Edit
 - In the Edit Operation Plan pane, select Detach
 - Use Move Up/Move Down to move the scripts into the correct execution order
 - Modify the Execution Group for steps executing the same scripts into the same Execution Group. This results in the scripts executing in parallel.
 - The resulting Execution Groups and order of execution (see example screen shot below):
 - /home/applmgr/EBSRoleChange/EBS_cleanUpStates.sh (Execution Group 1)
 - /home/applmgr/EBSRoleChange/set_webentry_prodURL_to_f5_LB.sh (Execution Group 2)
 - /home/applmgr/EBSRoleChange/EBS_autoconfig.sh (Execution Group 3)
 - /home/applmgr/EBSRoleChange/EBS_startWLSAdminServer.sh (Execution Group 4)
 - /home/applmgr/EBSRoleChange/EBS_startServices.sh (Execution Group 5)
 - Save the changes

Target Name	Target Host	Operation Type	Error Mode	Execution Mode	Execution Group	Run Mode
Pre-Scripts				Parallel		
/home/applmgr/EBSRoleChange/EBS_stopServices.sh	pca1vm55.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled
/home/applmgr/EBSRoleChange/EBS_stopServices.sh	pca1vm56.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled
Storage Unmount Scripts				Parallel		
sh mount_umount.sh -o umount -f /u02 (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca1vm55.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled
sh mount_umount.sh -o umount -f /u02 (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca1vm56.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled
Storage Scripts				Parallel		
sh zfs_storage_role_reversal.sh --target_appliance pca3zfs.cloud.osc.oracle.com --source_appliance pca1zfs.cloud.osc.oracle.com --project_name MAA_EBS --target_pc	pca3bst.cloud.osc.oracle.com	Run Storage Script	Stop on Error		1	Enabled
Database Instances				Parallel		
EBS_CDB_phv3xd_EBSCDB1	exa14-01.us.osc.oracle.com	Switchover Database	Stop on Error		1	Enabled
Storage Mount Scripts				Parallel		
sh mount_umount.sh -o mount -f /u02 (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca3vm55.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled
sh mount_umount.sh -o mount -f /u02 (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca3vm56.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled
Post-Scripts				Parallel		
/home/applmgr/EBSRoleChange/EBS_cleanUpStates.sh	pca3vm55.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled
/home/applmgr/EBSRoleChange/EBS_cleanUpStates.sh	pca3vm56.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled
/home/applmgr/EBSRoleChange/set_webentry_prodURL_to_f5_LB.sh	pca3vm55.cloud.osc.oracle.com	Run Script	Stop on Error		2	Enabled
/home/applmgr/EBSRoleChange/set_webentry_prodURL_to_f5_LB.sh	pca3vm56.cloud.osc.oracle.com	Run Script	Stop on Error		2	Enabled
/home/applmgr/EBSRoleChange/EBS_autoconfig.sh	pca3vm55.cloud.osc.oracle.com	Run Script	Stop on Error		3	Enabled
/home/applmgr/EBSRoleChange/EBS_autoconfig.sh	pca3vm56.cloud.osc.oracle.com	Run Script	Stop on Error		3	Enabled
/home/applmgr/EBSRoleChange/EBS_startWLSAdminServer.sh	pca3vm55.cloud.osc.oracle.com	Run Script	Stop on Error		4	Enabled
/home/applmgr/EBSRoleChange/EBS_startServices.sh	pca3vm55.cloud.osc.oracle.com	Run Script	Stop on Error		5	Enabled
/home/applmgr/EBSRoleChange/EBS_startServices.sh	pca3vm56.cloud.osc.oracle.com	Run Script	Stop on Error		5	Enabled

b) Create EBS_SITE1_TO_SITE2_FAILOVER

Operation plan for performing a failover from EBS_SITE1 to EBS_SITE 2. A failover is an unplanned event when the primary site becomes unavailable.

- Login to Enterprise Manager Cloud Control console, go to **Target > Systems**
- Click in **Site1 System > Site Guard > Operations**.
- Click Create.
- Enter a name for the plan. Example: EBS_SITE1_TO_SITE2_FAILOVER
- Select Operation Type: Failover
- Select the other site (EBS_SITE2) as the standby system
- Click Save
- The created plan will need to be customized. Edit the Post-Script steps to group scripts that can be executed in parallel and modify the order of execution:
 - Click Edit
 - In the Edit Operation Plan pane, select Detach
 - Use Move Up/Move Down to move the scripts into the correct execution order
 - Modify the Execution Group for steps executing the same scripts into the same Execution Group. This results in the scripts executing in parallel.
 - The resulting Execution Groups and order of execution (see example screen shot above):
 - /home/applmgr/EBSRoleChange/EBS_cleanUpStates.sh (Execution Group 1)
 - /home/applmgr/EBSRoleChange/set_webentry_prodURL_to_f5_LB.sh (Execution Group 2)
 - /home/applmgr/EBSRoleChange/EBS_autoconfig.sh (Execution Group 3)
 - /home/applmgr/EBSRoleChange/EBS_startWLSAdminServer.sh (Execution Group 4)
 - /home/applmgr/EBSRoleChange/EBS_startServices.sh (Execution Group 5)
- Save the changes.

c) Create EBS_SITE2_TO_SITE1_SWITCHOVER

Follow the same steps than in the previous but in EBS_SITE2 system. Select the EBS_SITE1 as the standby.

d) Create EBS_SITE2_TO_SITE1_FAILOVER

Follow the same steps than in the previous but in EBS_SITE2 system. Select the EBS_SITE1 as the standby.

PERFORMING A SWITCHOVER WITH SITE GUARD

Once the operations plans are created you can perform the switchover of the complete DR Site with Site Guard. To execute a switchover operation using OMS Console:

- a) Login to Enterprise Manager Cloud Control console, go to **Target > Systems**
- b) Click the current primary Site System
- c) Go to **Site Guard > Operations**
- d) Select the operation plan you want to execute.
- e) Click "Execute Operation"

Alternatively, the operation plans can be submitted using EMCLI:

- a) SSH to OMS host with user oracle (or to other host that has EM CLI installed)
- b) Login to emcli

```
[oracle@emcc bin]$ cd $EM_HOME/middleware/bin  
[oracle@emcc bin]$ ./emcli login -username=sysman
```

- c) Submit the operation plan

```
emcli submit_operation_plan -name="name_of_operation_plan"
```

Site Guard will orchestrate all the steps defined in the switchover plan per the following:

- Oracle Site Guard executes precheck steps: it checks the agent status in the involved hosts, checks if any targets have been added or deleted from the generic systems, runs Oracle Data Guard Broker prechecks to ascertain whether the Database is ready for role reversal and runs Storage prechecks to ascertain whether the ZFS project is ready for role reversal.
- Oracle Site Guard executes the Pre-Scripts on the Primary system
- Oracle Site Guard performs the database switchover from primary database to standby database using Data Guard broker.
- Oracle Site Guard performs the ZFS role reversal from the Primary ZFS Storage Array to the Standby ZFS Storage Array.
- Oracle Site Guard executes the Post-Scripts on the Standby System.
- If everything is successful, the roles of the sites are updated in the Site Guard metadata schema.
- The progress of the operation plan can be monitored in the Enterprise Manager Cloud Control console, in **System > Site Guard > Operations > Operation Activities**. Details of each steps are provided (timing, actions, result, etc.) and any failed step can be retried.
- Once finished, the sites' role change can be verified using the **System > Site Guard > Configure > General** screen

PERFORMING A FAILOVER WITH SITE GUARD

You can perform a failover using Site Guard as explained in the previous section, by executing the failover operation plan with Enterprise Manager Cloud Control console or EMCLI. Site Guard will orchestrate the steps for the Application DR failover:

- Oracle Site Guard executes precheck steps: it checks the agent status in the involved hosts and runs Oracle Data Guard Broker prechecks.
- No Pre-Scripts are executed. A failover is an unplanned event that happens when the primary site becomes unavailable so configuration synchronization is not expected.
- Oracle Site Guard performs the database failover from primary database to standby database using Data Guard broker.
- Oracle Site Guard performs the ZFS failover from the Primary ZFS Storage Array to the Standby ZFS Storage Array.
- Oracle Site Guard executes the Post-Scripts on the Standby System.
- If everything is successful, the roles of the sites are updated in the Site Guard metadata schema.

After a failover operation, the pertinent actions need to be performed to bring the original primary site back to a healthy status: solve the problem that forced the failover, reinstantiate the database, etc. Then a switchback can be performed with Site Guard.

CONCLUSION

Enterprise Manager Cloud Control Site Guard can be used to manage switchovers and failovers for Application DR systems like EBS, PeopleSoft and Siebel. The setup requires some initial steps described in this document, but once it is configured, the full stack switchover can be completely performed by the Site Guard just with a few clicks. This greatly simplifies the disaster recovery administration: it minimizes disaster-recovery time, reduces human errors, and eliminates the need for special skills. In addition, it is flexible and customizable so the customer can adapt it to include other particular steps that are specific to their environment.

APPENDIX A: INSTALL EM AGENT AND DISCOVER TARGETS

Install EM Agent Using Agent Deploy Method

1. Get the agent software

In this method, you must use EM CLI to download the Management Agent software onto the remote destination host before executing the script to install the Management Agent. You can either choose to use EM CLI from the OMS host, or from the remote destination host. If you choose to use EM CLI from the OMS host, you must transfer the downloaded Management Agent software to the remote destination host before executing the script to install the Management Agent. This method supports many additional parameters, and is ideal for a customized Management Agent install.

Use `emcli` in the OMS host to download the agent software and then copy it to the target host:

- a) Login to `emcli` in the OMS host (`MIDDLEWARE_HOME` is `/u01/app/em13c/middleware`):

```
[oracle@emcc bin]$ cd $MIDDLEWARE_HOME/bin
[oracle@emcc bin]$ ./emcli login -username=sysman
```

- b) Verify the available software and get the agent image for the Linux x86-64 platform:

```
[oracle@emcc bin]$ ./emcli get_supported_platforms
-----
Version = 13.3.0.0.0
Platform = Linux x86-64
-----
Platforms list displayed successfully.

[oracle@emcc bin]$ ./emcli get_agentimage -destination=/tmp/agent_image -platform="Linux x86-64" -version=13.3.0.0.0
..
Downloading /tmp/agent_image/13.3.0.0.0_AgentCore_226.zip
Agent Image Download completed successfully.
```

- c) Copy it to each remote host where the agent will be install using `scp`, for example:

```
[oracle@emcc ~]$ scp -i <public_ssh_key>.ppk /tmp/agent_image/13.3.0.0.0_AgentCore_226.zip opc@<monitored-host-name>:/tmp/
```

2. Install the agent

In the host where the agent is going to be installed:

- a) Verify that the agent user (example `emcadm`) can read the agent software zip.
- b) Unzip the software with the agent user (`emcadm`) in a temporal folder. Example, `/tmp/agent_image`

```
[emcadm@drdbw1mp1a tmp]$ mkdir agent_image
[emcadm@drdbw1mp1a tmp]$ cp 13.3.0.0.0_AgentCore_226.zip agent_image
[emcadm@drdbw1mp1a tmp]$ cd agent_image
[emcadm@drdbw1mp1a agent_image]$ unzip 13.3.0.0.0_AgentCore_226.zip
```

- c) In the folder where the agent is unzipped, install it using `agenDeploy.sh` with the agent user (`emcadm`). Example:

```
./agentDeploy.sh AGENT_BASE_DIR=/u01/agent13c OMS_HOST=emcc.marketplace.com EM_UPLOAD_PORT=4903
AGENT_REGISTRATION_PASSWORD=welcome1 LOCALHOST=drdbw1mp1a.site1cloudinternaldomain.com LOCALPORT=3872
AGENT_PORT=3872 ORACLE_HOSTNAME=drdbw1mp1a-public-site1.example.com ALLOW_IPADDRESS=TRUE
START_AGENT=true
```

Where:

AGENT_BASE_DIR	The folder where the agent will be installed
OMS_HOST	The name to connect to the OMS. In this example: <code>emcc.marketplace.com</code>
EM_UPLOAD_PORT	The upload port of the OMS. Typically 4903
AGENT_REGISTRATION_PASSWORD	The agent registration password

LOCALHOST	FQDN of the hostname where the agent is being installed (the private name). Example: <pre>[root@wlsmkpl1-wls-0]# hostname -fqdn wlsmkpl1-wls-0.site1cloudinternaldomain.com</pre>
LOCALPORT/AGENT_PORT	The port where the agent will listen. Example: 3872
ORACLE_HOSTNAME	When the communication between OMS and targets is via internet, this is the PUBLIC name of the monitored host that OMS will use to communicate with this agent. Must either be the public IP of the host, or a public name resolvable to that public IP. When the communication between OMS and targets is done via private networks (i.e.: DRG is used), this is the PRIVATE name of the monitored host. TIP: Use hostnames instead of IPs is recommended. IMPORTANT: Write this name in lowercase. Using uppercase in the public name can cause errors validating the agent certificate.
ALLOW_IPADDRESS	Enter TRUE if you want to specify an IP address for ORACLE_HOSTNAME. If ALLOW_IPADDRESS is set to FALSE, a prerequisite check fails when you specify an IP address for ORACLE_HOSTNAME while installing a Management Agent. Not required is using hostnames. TIP: Using names instead of IPs is recommended.
START_AGENT	When set to true, agent will be started after the installation.

- d) Once the installation has finished successfully, execute the root script as root user:

```
<AGENT_BASE_DIR>/agent_13.3.0.0.0/root.sh
```

NOTE: In case the agent installation hangs in the step "Waiting for agent targets to get promoted..." and finally returns an error, follow these steps to solve the issue:

```
- as root, run the <AGENT_BASE_DIR>/agent_13.3.0.0.0/root.sh  
- as emcadm start agent and retry the internal target addition:  
/u01/agent13c/agent_inst/bin/emctl start agent  
/u01/agent13c/agent_inst/bin/emctl config agent addinternaltargets
```

- e) Verify the status with `<AGENT_BASE_DIR>/agent_13.3.0.0.0/bin/emctl status agent`
Agent URL should show the public hostname of the host (when OMS and target are communicated via public IPs), or private hostname (when OMS and target are communicate internally).
Verify that the **Local Agent URL** is using the private hostname
Verify that the **Repository URL** points to the OMS name

```
[emcadm@wlsmkpl1-wls-0 bin]$ ./emctl status agent  
Oracle Enterprise Manager Cloud Control 13c Release 3  
Copyright (c) 1996, 2018 Oracle Corporation. All rights reserved.  
-----  
Agent Version      : 13.3.0.0.0  
OMS Version        : 13.3.0.0.0  
Protocol Version   : 12.1.0.1.0  
Agent Home         : /u01/agent13c/agent_inst  
Agent Log Directory : /u01/agent13c/agent_inst/sysman/log  
Agent Binaries     : /u01/agent13c/agent_13.3.0.0.0  
Core JAR Location  : /u01/agent13c/agent_13.3.0.0.0/jlib  
Agent Process ID   : 16917  
Parent Process ID  : 16880  
Agent URL          : https://wlsmkpl1-wls-0-public.site1.example.com:3872/emd/main/  
Local Agent URL in NAT : https://wlsmkpl1-wls-0.wlsdrvcnlon1ad2.wlsdrvcnlon1.oraclevcn.com:3872/emd/main/  
Repository URL     : https://emcc.marketplace.com:4903/empbs/upload  
Started at         : 2020-02-25 10:02:28  
Started by user    : emcadm
```

...

Agent is Running and Ready

- f) Verify that the agent upload runs ok:

```
[emcadm@wlsmkpl1-wls-0 bin]$ cd <AGENT_BASE_DIR>/agent_inst/bin
[emcadm@wlsmkpl1-wls-0 bin]$ ./emctl upload agent
Oracle Enterprise Manager Cloud Control 13c Release 3
Copyright (c) 1996, 2018 Oracle Corporation. All rights reserved.
-----
EMD upload completed successfully
```

- g) Restart agent to verify that everything is properly configured:

```
[emcadm@maa4-wls-1 bin]$ ./emctl stop agent
Oracle Enterprise Manager Cloud Control 13c Release 3
Copyright (c) 1996, 2018 Oracle Corporation. All rights reserved.
Stopping agent ... stopped.
[emcadm@maa4-wls-1 bin]$ ./emctl start agent
Oracle Enterprise Manager Cloud Control 13c Release 3
Copyright (c) 1996, 2018 Oracle Corporation. All rights reserved.
Starting agent ..... started.
```

- h) Login in the OMS Console https://<oms_public_ip>:7803/em , go to Targets > Hosts and verify that the host is registered.

NOTE: If there is any error and the agent needs to be reinstalled, it can be de-installed using this (execute it in a folder outside the agent base dir). Write it in a single line:

```
<AGENT_BASE_DIR>/agent_13.3.0.0.0/perl/bin/perl <AGENT_BASE_DIR>/agent_13.3.0.0.0/sysman/install/AgentDeinstall.pl -agentHome
<AGENT_BASE_DIR>/agent_13.3.0.0.0
```

If any target of the agent was registered in the OMS, it must be deleted also by decommissioning the agent. See: “EM 13C: How to Deinstall the Enterprise Manager 13c Cloud Control Agent (Doc ID 2095678.1)”

Target Discovery

Primary and standby WebLogic domains and databases must be discovered in EM. The procedure to discover and promote the targets running on an Oracle Cloud host is the same as the procedure to discover and promote targets running on any normal host in the on-premises environment.

1. Promoting automatically discovered targets

Some targets are automatically discovered, and just required to be promoted. This is typically the process for Oracle Database home, Oracle Grid Infrastructure home, Oracle High Availability Service and Cluster. To promote automatically discovered these targets:

- Login in OMS Console
- Go to Setup > Add Target > Configure Auto Discovery
- See “**Target on Hosts**”. Select a host and click in “**Discover now**”
- Then go to Setup > Add Target > Auto Discovery Results
- See “Targets on Hosts”
- Review the auto discovered targets, click in one of them and click in Promote.

Databases and ASM instances and cluster can be also automatically discovered. To promote them, see the following points.

2. Discover ASM targets

ASM instances are normally automatically discovered. Follow these steps to complete the discovery:

- ASSNMP user is typically used to monitor the ASM databases. The customer needs to change the password of the ASSNMP user. Do the following in any target DB host using ASM (primary and secondary):
 - Login in the DB host as opc user and sudo to user grid.

- Connect to the ASM instance as sysadm and Reset the password for the user ASMSNMP:
- Reset the password for the user ASMSNMP

```
sqlplus " / as sysasm"
sql> alter user asmsnmp identified by <new password>;
```

- In the **Auto Discovery Results** in OMS Console, select the discovered “Cluster ASM” target in and click “Promote”.
- In the **Results** screen, select the Cluster ASM target and click on “Configure”:
 - In **General** tab, set the Monitor username to ASMSNMP and set the password.
 - In **Instances** tab, ensure that “Listener Machine Name” it is set to the hostname that the OMS uses to connect to this host target. OMS needs to connect to the database. Use the proper machine host name (public or private) depending on your network topology.
 - Click “**Test Connection**” to verify that the connection is successful and then click “Save”.
- Back in the **Results** screen, verify that the ASM listener is also selected. Leave default values for the listener. ASM listener target is monitored by the local agent and the private machine name can be used.
- Click **Next** and then **Save**

3. Discover Database targets

To promote or discover a database target:

- The user DBSNMP is typically used to monitor the database. This user account is locked by default. Connect to the primary database as sysdba to unlock if necessary and set a password:

```
sql> ALTER USER DBSNMP ACCOUNT UNLOCK;
Sql> ALTER USER DBSNMP IDENTIFIED BY password;
```

- Paas DR databases use Data Guard. If the standby database is open (Active Data Guard), the DBSNMP user will be able to login with normal role. If standby database is mounted (not Active Data Guard), the user DBSNMP needs SYSDBA privilege to login to the database.

- Run below SQL to check if DBSNMP user having SYSDBA privilege:

```
SQL> select username, sysdba from v$pwfile_users where username='DBSNMP';
```

- If above SQL does not return any rows, this means SYSDBA privilege not granted to DBSNMP user. Login in primary DB system and connect to primary database as sysdba and grant sysdba to dbnmp user:

```
sqlplus / as sysdba
SQL> grant sysdba to dbnmp container=all
```

- For database versions before 12.2, copy the password file from primary host to standby host. The default location of the password file is \$ORACLE_HOME/dbs/orapw\$ORACLE_SID
- Discover the database if it was not automatically discovered:
 - Login in **OMS Console** https://<oms_public_ip>:7803/em
 - Go to **Setup > Add Targets Manually**
 - In “**Add Non-Host Target Using Guided Process**” click in “**Add Using Guided Process**”
 - Select “**Oracle Database, Listener and Automatic Storage Manage**” and click “Add..”
 - In the “**Database Discover: Search Criteria**” screen, select the public name of the host running the database
 - If the database is not found, verify that there is and entry for it in /etc/oratab and retry.
 - Once the Database has been discovered (either automatically or manually), select it in the **Results** screen and click in “**Configure**”. Update with the following:

Listener Machine Name	Ensure it is set to the db hostname that the OMS uses to connect to this host target. Use the proper machine hostname (public or private) depending on your network topology.
Monitor Username	Enter the name of the database user that will be used to monitor it from OMS. Typically dbnmp.
Role	select “SYSDBA”
select “SYSDBA”	enter the password for the dbnmp

- Click the “**Test Connection**” and verify that it is successful.

- f) Click **Save**.
- g) Back in the “**Database Discovery: Results**” page, verify that the listener is also selected. Leave default values for the listener. Listener is monitored by the local agent and the private machine name is used.
- h) Click **Next**
- i) In the “**Database Discovery: Review**”, click Save
- j) Once finished, you can go to Targets > Databases to verify that the database has been discovered.

NOTE: if duplicated targets are discovered, (for example, LISTENER and LISTENER0, or ASM_1, etc), select the first and ignore the duplicated.

4. Target Host preparation

Perform the following steps to prepare the target host for the agent installation.

a) Create user and group

A dedicated user can be used to install and run the agent software, in order to isolate processes, environment variables, etc. from the monitored software. Create the user (for example: emcadm) in the host where the agent will be installed, and add it to the group of the user that is running the software in the host. This is oracle group in app hosts and oinstall group in DB hosts.

For app hosts, software group is oracle:

```
[root@host]# useradd -g oracle emcadm
```

For DB hosts, software group is oinstall (oracle group does not exist):

```
[root@host]# useradd -g oinstall emcadm
```

NOTE: specific user for the agent is not mandatory. User “oracle” can also be used for installing and running the agent. The steps in this documentation use a specific agent user (emcadm), in order to identify any step requirement/action needed when the user running the agent is different than the user running the monitored software.

b) Verify communication to OMS

Verify that the target host is able to resolve the Enterprise Manager OMS hostname and its own public name (when public names are used). This should be already configured as described in the previous section [Network Setup](#). Use nc to verify that Enterprise Manager OMS upload port is reachable. Use the appropriate OMS IP (public or private) for your environment:

```
$ nc -v -w 5 -z <oms_ip> 4903
Connection to <oms_ip> 4903 port [tcp/*] succeeded!
```

c) Create Agent Home base folder

The agent home base folder has some requirements, especially important when Privilege Delegation Provider is used (which will be used for the credentials). See Agent Base Directory Requirements in the “Installing Oracle Management Agent in Silent Mode” chapter of the Enterprise Manager Cloud Control documentation.

The following folders are suggested for the agent home base in the storage volumes that are already mounted in the hosts:

For DB hosts: /u01/agent13c (under /u01 volume)

For App tier hosts: /u01/agent13c (note this is under / volume)

<AGENT_BASE_DIR> will be used to refer to the agent base folder.

- Create the folders, with user root:

```
[root@wlsmkpl1-wls-0~]# mkdir -p <AGENT_BASE_DIR>
```

- Change the ownership of that folder to the user and group that will run the agent
In mid-tier hosts:

```
[root@wlsmkpl1-wls-0~]# chown emcadm:oracle <AGENT_BASE_DIR>
```

In DB hosts:

```
[root@drdbwlp1a]# chown emcadm:oinstall <AGENT_BASE_DIR>
```

- Add read and execute permissions to the group and others to the folder and to the parent folders also. This is also required for Privilege Delegation:

```
[root@wlsmkpl1-wls-0]# chmod go+rx /u01/agent13c  
[root@wlsmkpl1-wls-0]# chmod go+rx /u01
```

d) Review other requirements

The complete list of the requirements for the agent is in *Table 6-1 Prerequisites for Installing Oracle Management Agent in Silent Mode* in the “[Installing Oracle Management Agent in Silent Mode](#)” chapter of the *Enterprise Manager Cloud Control documentation*. It is expected that DB hosts meet those requirements, and no additional actions are required. In mid-tier hosts, there are some operating system packages that are required by the agent and are not installed by default. If they are not installed, the agent installer will provide the following message:

```
Check complete: Passed
```

```
=====
Performing check for Packages_agent
Are the required packages installed on the current operating system?
Checking for make-3.82-21; found make-1:3.82-23.el7-x86_64. Passed
Checking for binutils-2.23; found binutils-2.27-34.base.0.1.el7-x86_64. Passed
Checking for gcc-4.8.2-16; Not found. Failed <<<<
Checking for libaio-0.3.109-12; found libaio-0.3.109-13.el7-x86_64. Passed
Checking for glibc-common-2.17-55; found glibc-common-2.17-292.0.1.el7-x86_64. Passed
Checking for libstdc++-4.8.2-16; found libstdc++-4.8.5-39.0.3.el7-x86_64. Passed
Checking for sysstat-10.1.5-4; found sysstat-10.1.5-17.el7-x86_64. Passed
Check complete. The overall result of this check is: Failed <<<<
```

Install the missing package with root user:

```
[root@wlsmkpl1-wls-0]# yum install gcc
```

APPENDIX B. PEOPLESOFT DISASTER RECOVERY USING SITE GUARD

Site Guard Configuration

The steps described in this section are based on the [Site Guard Administrator's Guide for Enterprise Manager Cloud Control version 13.4](#). This Appendix contains only those steps specific to configuring Site Guard for PeopleSoft switchover/failover. Refer to the main body of the white paper for steps that are not PeopleSoft specific

1. Create named credentials

You must create named credentials for the targets associated with Oracle Site Guard for application tier hosts, db hosts Oracle Databases. This table summarizes the named credentials required for managing PeopleSoft application-level DR with Oracle Site Guard:

CREDENTIAL NAME	AUTHENTICATION TARGET TYPE	CREDENTIAL TYPE	CREDENTIAL SCOPE	TARGET USERNAME	DESCRIPTION
PSOFT_ORACLE_CRED	Host	Host Credential	Global	oracle_psft	App Tier User Credentials
PSOFT_ROOT_CRED	Host	Host Credential	Global	root	App Tier Root Credentials
EXADATA_ORACLE_CRED	Host	Host Credential	Global	oracle	Oracle User Credentials
EXADATA_DB_SYS_CRED	Database Instance	Database Credential	Global	sys as sysdba	SYSDBA Credentials

NOTE: Credentials are the same for the primary and standby app tier and db hosts so using global credentials instead of targeted credentials simplifies the configuration.

d) Create PeopleSoft Application Named Credentials

To create the credentials described in the table above:

- Login to Enterprise Manager Cloud Control console
- Navigate to Setup > Security > Named Credentials.
- Click Create, and create the named credentials as described in the table
- Test and Save.
- Repeat the same to create all and any other additional credentials you need for the host.

This table summarizes the named credentials for managing ZFS storage role reversal:

CREDENTIAL NAME	AUTHENTICATION TARGET TYPE	CREDENTIAL TYPE	CREDENTIAL SCOPE	TARGET USERNAME	DESCRIPTION
SITE1_ZFS_CRED	Host	Host Credential	Global	root	ZFS Root Credentials
SITE2_ZFS_CRED	Host	Host Credential	Global	root	ZFS Root Credentials
SITE1_BASTION_HOST_CRED	Host	Host Credential	Global	oracle	EM Agent User Credentials
SITE2_BASTION_HOST_CRED	Host	Host Credential	Global	oracle	EM Agent User Credentials

e) Create ZFS Named Credentials

To create the credentials described in the table:

- Login to Enterprise Manager Cloud Control console
- Navigate to Setup > Security > Named Credentials.

- Click Create, and create the named credentials as described in the table
- Save.
 - A warning will be displayed asking you to confirm saving without testing the connection, Select OK
 - The ZFS Storage Arrays are not Discovered Host Targets, so you will not be able to test the connection.

f) Create Bastion Host Named Credentials

To create the credentials described in the table:

- Login to Enterprise Manager Cloud Control console
- Navigate to Setup > Security > Named Credentials.
- Click Create, and create the named credentials as described in the table
- Test and Save.

2. Configuring preferred credentials

Once the named credentials have been created, they can be assigned to the targets as the preferred credentials. This approach is recommended to simplify the Site Guard configuration. Follow these steps to configure the preferred credentials for a target:

- Login to Enterprise Manager Cloud Control console
- Navigate to Setup > Security > Preferred Credentials
- Select a target type (Database Instance, Hosts, etc.), and click “Manage Preferred Credentials”.
- Set the preferred credentials for each target credential, by clicking each row, “Set” and selecting the appropriate named credential created in the previous step.
- Do this for the following targets:
 - **Primary and Standby Database Instances** (at minimum, sysdba credentials, database hosts credentials)
 - **Primary and Standby App Tier Hosts**
 - **Primary and Standby Bastion Hosts**

3. Defining Primary and Standby Site Systems in EM

A disaster recovery site managed by Oracle Site Guard is modeled as a Generic System target type in Oracle Enterprise Manager. Follow these steps to create the Generic System that models the Primary (active) site, PSOFT_SITE1:

NOTE: In the rest of the steps PSOFT_SITE1 will be the Primary site and PSOFT_SITE2 will be the Standby site.

- Login to Enterprise Manager Cloud Control console
- Go to Targets > Systems
- Click Add > Generic System
- Generic System: General Screen
- Enter a Name for the System. For example: PSOFT_SITE1.
- You can optionally add system properties (Department, Line of Business, Location, etc.)
- Add members to the system. For the primary site add:
 - The **primary PeopleSoft Host Targets**
 - The **primary Database Instance Target**
 - The primary **PCA Bastion Host Target**
 - The standby **PCA Bastion Host Target**

NOTE: Do NOT add the database system itself. The Data Guard system that is part of will be added and it will include primary and standby databases.

- Click Next
- Generic System: Define Associations.** You can leave defaults and click Next.
- Generic System: Availability Criteria.** You can add database as key member and click Next.
- Generic System: Charts Screen.** You can leave defaults and click Finish.

Repeat same steps to create the standby site system, PSOFT_SITE2.

4. Defining Site Roles

Once a disaster recovery site managed by Oracle Site Guard has been modeled as a Generic System target in Oracle Enterprise Manager, then you designate it as a primary site or a standby site. This is done following these steps:

- i) Login to Enterprise Manager Cloud Control console, go to Targets > Systems
- j) Click on the name of the **primary** site system, PSOFT_SITE1.
- k) On the system's home page, from the Generic System menu, select **Site Guard > Configure**.
- l) On the **General** tab, click **Create**
- m) On the **General** tab, in the **Standby System(s)** section, click Add.
- n) Choose the **standby** system, PSOFT_SITE2, and click **Select**.
- o) Click **Save** and **OK** to confirm the action. Site Guard saves the standby system configuration.
- p) Verify that the roles have been assigned:
In the primary Site system, PSOFT_SITE1, in Oracle Site Guard Configuration, General Tab, you must see:
Current Role Primary
In the secondary Site system, PSOFT_SITE2, in Oracle Site Guard Configuration, General Tab, you must see:
Current Role Standby

5. Credential associations

Credentials are associated with targets and used by Oracle Site Guard operation plans when they are executed. These associations must be configured for primary and standby systems:

- i) Login to Enterprise Manager Cloud Control console.
- j) From the Targets menu, click **Systems**
- k) On the Systems page, click the name of the system for which you want to configure credential associations.
- l) On the system's home page, from the Generic System menu, select Site Guard > Configure.
- m) Click the Credentials tab. Now associate the different types of credentials
- n) **Normal Host Credentials** section, click Add, select **All** and check **Preferred**, Normal Host Credentials. Click Save.
- o) **Privileged Host Credentials** are required for the app tier hosts. Privileged credential are used to execute scripts that mount and unmount nfs filesystems.
- p) **SYSDBA Database Credentials** section, click Add, select **All** and **Preferred**, "SYSDBA Database Credentials". Click Save

Repeat the same for the standby system.

6. Configuring required scripts

Oracle Site Guard provides a mechanism for you to configure scripts for managing disaster recovery operations. The scripts for PeopleSoft disaster recovery can be found in section 11.4.7 Application and PIA Webserver Scripts in the PeopleSoft Maximum Availability Architecture whitepaper. Different kind of scripts can be defined for Site Guard:

SCRIPT TYPE	SCRIPT PATH	OPERATION	ROLE	TARGET HOST
Pre Script	Following scripts will be run as pre scripts: <ul style="list-style-type: none">• /home/oracle_psft/PSFTRoleChange/stopAPP.sh• /home/oracle_psft/PSFTRoleChange/stopPS.sh• /home/oracle_psft/PSFTRoleChange/stopRMIregistry.sh• /home/oracle_psft/PSFTRoleChange/stopWLS.sh	Switchover	Primary	All Primary App Tier Hosts
Post Scripts	Following scripts will be run as post scripts: <ul style="list-style-type: none">• /home/oracle_psft/PSFTRoleChange/startWLS.sh• /home/oracle_psft/PSFTRoleChange/startPS.sh• /home/oracle_psft/PSFTRoleChange/startAPP.sh	Switchover/ Failover	Standby	All Standby App Tier Hosts
Storage Scripts	Unmount EBS application NFS filesystem on primary: sh mount_umount.sh -o umount -f <nfs mount point>	Switchover	Primary	All Primary App Tier Hosts

Example: sh mount_umount.sh -o umount -f '/u01'			
Mount EBS application NFS filesystem on standby: sh mount_umount.sh -o mount -f <nfs mount point> Example: sh mount_umount.sh -o mount -f '/u01'	Switchover/ Failover	Standby	All Standby App Tier Hosts
Perform ZFS Role Reversal on switchover: sh zfs_storage_role_reversal.sh --target_appliance <target remote replication FQDN> --source_appliance <source remote replication FQDN> --project_name <ZFS Project Name> --target_pool_name <Target Pool Name> --source_pool_name <Source Pool Name> --is_sync_needed N --continue_on_sync_failure Y --sync_timeout 1800 --operation_type switchover Example: sh zfs_storage_role_reversal.sh --target_appliance pca1zfs.cloud.osc.oracle.com --source_appliance pca3zfs.cloud.osc.oracle.com --project_name MAA_PS --target_pool_name Pool01 --source_pool_name OVCA_POOL --is_sync_needed N --continue_on_sync_failure Y --sync_timeout 1800 --operation_type switchover	Switchover	Standby	Standby PCA Bastion Host
Perform ZFS Role Reversal on failover: sh zfs_storage_role_reversal.sh --target_appliance <target remote replication FQDN> --source_appliance <source remote replication FQDN> --project_name <ZFS Project Name> --target_pool_name <Target Pool Name> --source_pool_name <Source Pool Name> --is_sync_needed N --continue_on_sync_failure Y --sync_timeout 1800 --operation_type failover Example: sh zfs_storage_role_reversal.sh --target_appliance pca1zfs.cloud.osc.oracle.com --source_appliance pca3zfs.cloud.osc.oracle.com --project_name MAA_PS --target_pool_name Pool01 --source_pool_name OVCA_POOL --is_sync_needed N --continue_on_sync_failure Y --sync_timeout 1800 --operation_type failover Note: The source appliance is the ZFS Storage Appliance at the Primary Site and the target appliance is the ZFS Storage Appliance at the Standby Site. The scripts execute on a bastion host configured on the Standby PCA.	Failover	Standby	Standby PCA Bastion Host

To configure the PeopleSoft DR scripts for PSOFT_SITE1:

- m) Login to Enterprise Manager Cloud Control console, go to Targets > Systems
- n) Right-click the PSOFT_SITE1 System
- o) Navigate to Site Guard > Configure
- p) Click the Pre/Post scripts tab
- q) Add **Pre-Scripts** to **PSOFT_SITE1** system:
 - Add Pre-scripts as described in the Pre-Scripts section of the table
- r) Add **Post-Scripts** to **PSOFT_SITE1** system:
 - Add Switchover Post-scripts as describe in the table
 - Add Failover Post-scripts as described in the Post Scripts section of the table

To configure the Storage Scripts for PSOFT_SITE1:

- g) Click the Storage Scripts tab
- h) Add the Switchover Storage Unmount Script
 - a. Click Add
 - b. Click the eyeglass to the right of the Software Library Path edit box
 - c. Enter: 'Role Reverse Storage Scripts'
 - d. Select 'Role Reverse Storage Scripts' row with type 'Component'
 - e. Click Select
 - f. Insert "sh mount_umount.sh -o umount -f '/u01'" into Script Path

- g. Select all app tier Target Hosts (do not select any non-app tier hosts)
- h. Select 'Unmount' Script Type
- i. Select 'Switchover' Operation Type
- j. Click Save
- i) Add the Switchover Storage Mount Script
 - a. Select Storage Unmount Script you just created
 - b. Click Add Like
 - c. Insert "sh mount_umount.sh -o mount -f '/u01'" into Script Path
 - d. Select all app tier Target Hosts (do not select any non-app tier hosts)
 - e. Select 'Mount' Script Type
 - f. Select 'Switchover' Operation Type
 - g. Click Save
- j) Add the Failover Storage Mount Script:
 - a. Select Storage Mount Script you just created
 - b. Click Add Like
 - c. Insert "sh mount_umount.sh -o mount -f '/u01'" into Script Path
 - d. Select all app tier Target Hosts (do not select any non-app tier hosts)
 - e. Select 'Mount' Script Type
 - f. Select 'Failover' Operation Type
 - g. Click Save
- k) Add the Switchover ZFS Storage Role Reversal script
 - a. Click Add
 - b. Click the eyeglass to the right of the Software Library Path edit box
 - c. Enter: 'Role Reverse Storage Scripts'
 - d. Select 'Role Reverse Storage Scripts' row with type 'Component'
 - e. Click Select
 - f. Insert the zfs_role_reversal.sh switchover example from the table. Substitue your deployments source and target remote replication FQDNs, ZFS project name and source and target Pool Names.
 - g. Select the PCA Bastion Host Target
 - h. Select 'Storage-Switchover' Script Type
 - i. Select 'Switchover' Operation Type
 - j. Expand Advanced Options to add credentials to connect to ZFS Storage in this order:
 - i. Move the Primary PCA ZFS credential ('SITE1_ZFS_CRED') from Available Value to Selected Value
 - ii. Move the Standby PCA ZFS credential ('SITE2_ZFS_CRED') from Available Value to Selected Value
 - k. Click Save
- l) Add the Failover ZFS Storage Role Reversal script
 - a. Click Add
 - b. Click the eyeglass to the right of the Software Library Path edit box
 - c. Enter: 'Role Reverse Storage Scripts'
 - d. Select 'Role Reverse Storage Scripts' row with type 'Component'
 - e. Click Select
 - f. Insert the zfs_role_reversal.sh failover example from the table. Substitue your deployments source and target remote replication FQDNs, ZFS project name and source and target Pool Names.
 - g. Select the PCA Bastion Host Target
 - h. Select 'Storage-Failover' Script Type
 - i. Select 'Failover' Operation Type
 - j. Expand Advanced Options to add credentials to connect to ZFS Storage in this order:
 - i. Move the Primary PCA ZFS credential ('SITE1_ZFS_CRED') from Available Value to Selected Value
 - ii. Move the Standby PCA ZFS credential ('SITE2_ZFS_CRED') from Available Value to Selected Value
 - k. Click Save

To configure the Peoplesoft DR scripts for PSOFT_Site2:

- s) Login to Enterprise Manager Cloud Control console, go to Targets > Systems
- t) Right-click the PSOFT_SITE2 System
- u) Navigate to Site Guard > Configure
- v) Click the Pre/Post scripts tab
- w) Add **Pre-Scripts** to **PSOFT_SITE2** system:
 - Add Pre-scripts as describe in the Pre-Scripts section of the table

- x) Add **Post-Scripts** to **PSOFT_SITE2** system:
 - Add Switchover Post-scripts as describe in the table
 - Add Failover Post-scripts as described in the Post Scripts section of the table

To configure the Storage Scripts for PSOFT_SITE2 repeat the steps described for configuring the Storage Scripts for PSOFT_SITE1. The source and target parameters will be the reverse of what you specified for PSOFT_SITE1.

7. Configuring apply and transport lag thresholds (optional)

Site Guard verifies the apply and transport lag of the Data Guard during the prechecks and the switchover. By default, if the value is different than zero, the precheck fails and the switchover is not performed. You can define a threshold value to allow a few seconds so the check is more permissive. This step is optional. Example to set the thresholds to 10 seconds:

- d) Connect via SSH to the OMS host
- e) Login to emcli:

```
[oracle@emcc bin]$ cd $EM_HOME/middleware/bin
[oracle@emcc bin]$ ./emcli login -username=sysman
```

- f) Set the threshold to 10 seconds in both sites:

```
[oracle@emcc]$ ./emcli configure_siteguard_lag -system_name=PSOFT_SITE1 -property_name=apply_lag -value=10
[oracle@emcc]$ ./emcli configure_siteguard_lag -system_name=PSOFT_SITE2 -property_name=apply_lag -value=10
[oracle@emcc]$ ./emcli configure_siteguard_lag -system_name=PSOFT_SITE1 -property_name=transport_lag -value=10
[oracle@emcc]$ ./emcli configure_siteguard_lag -system_name=PSOFT_SITE2 -property_name=transport_lag -value=10
```

8. Creating switchover and failover operation plans

An operation plan describes the flow of execution that Oracle Site Guard performs in a disaster recovery operation. It consists of (ordered) actions that can be executed in series or in parallel. Oracle Site Guard creates a default version of the operation plan based on the site topology and the Oracle Site Guard configuration. You can use this default operation plan or customize it depending on your configuration.

The following operations plans are recommended for EBS DR:

PLAN	DESCRIPTION
PSOFT_SITE1_TO_SITE2_SWITCHOVER	Switchover from Site1 to Site2 where Site1 is is the primary system and Site2 is the standby system. This is a planned transition where Site1 is gracefully shutdown prior to transition to Site2.
PSOFT_SITE2_TO_SITE1_SWITCHOVER	Switchover from Site2 to Site1 when Site2 is is the primary system and Site1 is the standby system. This is a planned transition where Site2 is gracefully shutdown prior to transition to Site1.
PSOFT_SITE1_TO_SITE2_FAILOVER	Failover from Site1 to Site2 when Site1 is is the primary system and Site2 is the standby system. A failover occurs as a result of an unplanned event when the primary site becomes unavailable.
PSOFT_SITE2_TO_SITE1_FAILOVER	Switchover from Site2 to Site1 when Site2 is is the primary system and Site1 is the standby system. A failover occurs as a result of an unplanned event when the primary site becomes unavailable.

NOTE: To successfully execute a Site Guard operation plan the state of Site Guard configuration, Data Guard configuration and ZFS remote replication must be consistent. That is, if PSOFT_SITE1 generic system is the primary system in the Site Guard Configuration the Database Target associated with PSOFT_SITE1 must be the primary database in the Data Guard configuration and the ZFS project, not the replica, must reside on the ZFS Storage Array attached to the PCA hosting the primary application tier hosts.

d) Create PSOFT_SITE1_TO_SITE2_SWITCHOVER

Operation plan for performing a switchover from EBS_SITE1 to EBS_SITE 2.

- Login to Enterprise Manager Cloud Control console, go to Target > Systems
- Click in PSOFT_SITE1 System > Site Guard > Operations.
- Click Create.
- Enter a name for the plan. Example: **PSOFT_SITE1_TO_SITE2_SWITCHOVER**
- Select Operation Type: Switchover
- Select the other site (PSOFT_SITE2) as the standby system
- Click Save
- The created plan will need to be customized. Edit the Pre-Script steps to group scripts that can be executed in parallel and modify the order of execution:
 - Click Edit
 - In the Edit Operation Plan pane, select Detach
 - Use Move Up/Move Down to move the scripts into the correct execution order
 - Modify the Execution Group for steps executing the same scripts into the same Execution Group. This results in the scripts executing in parallel.
 - The resulting Execution Groups and order of execution (see example screen shot below):
 - /home/oracle_psft/PSFTRoleChange/stopAPP.sh (Execution Group 1)
 - /home/oracle_psft/PSFTRoleChange/stopPS.sh (Execution Group 2)
 - /home/oracle_psft/PSFTRoleChange/stopRMRegistry.sh (Execution Group 3)
 - /home/oracle_psft/PSFTRoleChange/stopWLS.sh (Execution Group 4)
- Edit the Post-Script steps to group scripts that can be executed in parallel and modify the order of execution:
 - Click Edit
 - In the Edit Operation Plan pane, select Detach
 - Use Move Up/Move Down to move the scripts into the correct execution order
 - Modify the Execution Group for steps executing the same scripts into the same Execution Group. This results in the scripts executing in parallel.
 - The resulting Execution Groups and order of execution (see example screen shot below):
 - /home/oracle_psft/PSFTRoleChange/startAPP.sh (Execution Group 1)
 - /home/oracle_psft/PSFTRoleChange/startPS.sh (Execution Group 2)
 - /home/oracle_psft/PSFTRoleChange/startWLS.sh (Execution Group 3)
 - Save the changes

Target Name	Target Host	Operation Type	Error Mode	Execution Mode	Execution Group	Run Mode
Pre-Scripts				Parallel		
/home/oracle_psft/PSFTRoleChange/stopAPP.sh	pca3vm52.cloud.oracle.com	Run Script	Stop on Error		1	Enabled
/home/oracle_psft/PSFTRoleChange/stopAPP.sh	pca3vm51.cloud.oracle.com	Run Script	Stop on Error		1	Enabled
/home/oracle_psft/PSFTRoleChange/stopPS.sh	pca3vm51.cloud.oracle.com	Run Script	Stop on Error		2	Enabled
/home/oracle_psft/PSFTRoleChange/stopPS.sh	pca3vm52.cloud.oracle.com	Run Script	Stop on Error		2	Enabled
/home/oracle_psft/PSFTRoleChange/stopRMRegistry.sh	pca3vm51.cloud.oracle.com	Run Script	Stop on Error		3	Enabled
/home/oracle_psft/PSFTRoleChange/stopRMRegistry.sh	pca3vm52.cloud.oracle.com	Run Script	Stop on Error		3	Enabled
/home/oracle_psft/PSFTRoleChange/stopWLS.sh	pca3vm54.cloud.oracle.com	Run Script	Stop on Error		4	Enabled
/home/oracle_psft/PSFTRoleChange/stopWLS.sh	pca3vm53.cloud.oracle.com	Run Script	Stop on Error		4	Enabled
Storage Unmount Scripts				Parallel		
sh mount_unmount.sh -o umount -f /u01 (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca3vm54.cloud.oracle.com	Run Script	Stop on Error		1	Enabled
sh mount_unmount.sh -o umount -f /u01 (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca3vm51.cloud.oracle.com	Run Script	Stop on Error		1	Enabled
sh mount_unmount.sh -o umount -f /u01 (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca3vm53.cloud.oracle.com	Run Script	Stop on Error		1	Enabled
sh mount_unmount.sh -o umount -f /u01 (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca3vm52.cloud.oracle.com	Run Script	Stop on Error		1	Enabled
Storage Scripts				Parallel		
sh zfs_storage_role_reversal.sh --target_appliance pca1zfs.cloud.oracle.com --source_appliance pca3zfs.cloud.oracle.com --project_name MAA_PS --target_poo	pca1bst.cloud.oracle.com	Run Storage Script	Stop on Error		1	Enabled
Database Instances				Parallel		
CDBHCM_osc1b_CDBHCM1	exa14-03.us.oracle.com	Switchover Database	Stop on Error		1	Enabled
Storage Mount Scripts				Parallel		
sh mount_unmount.sh -o mount -f /u01 (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca1vm54.cloud.oracle.com	Run Script	Stop on Error		1	Enabled
sh mount_unmount.sh -o mount -f /u01 (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca1vm51.cloud.oracle.com	Run Script	Stop on Error		1	Enabled
sh mount_unmount.sh -o mount -f /u01 (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca1vm52.cloud.oracle.com	Run Script	Stop on Error		1	Enabled
sh mount_unmount.sh -o mount -f /u01 (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca1vm53.cloud.oracle.com	Run Script	Stop on Error		1	Enabled
Post-Scripts				Parallel		
/home/oracle_psft/PSFTRoleChange/startAPP.sh	pca1vm51.cloud.oracle.com	Run Script	Stop on Error		1	Enabled
/home/oracle_psft/PSFTRoleChange/startAPP.sh	pca1vm52.cloud.oracle.com	Run Script	Stop on Error		1	Enabled
/home/oracle_psft/PSFTRoleChange/startPS.sh	pca1vm51.cloud.oracle.com	Run Script	Stop on Error		2	Enabled
/home/oracle_psft/PSFTRoleChange/startPS.sh	pca1vm52.cloud.oracle.com	Run Script	Stop on Error		2	Enabled
/home/oracle_psft/PSFTRoleChange/startWLS.sh	pca1vm54.cloud.oracle.com	Run Script	Stop on Error		3	Enabled
/home/oracle_psft/PSFTRoleChange/startWLS.sh	pca1vm53.cloud.oracle.com	Run Script	Stop on Error		3	Enabled

e) Create PSOFT_SITE1_TO_SITE2_FAILOVER

Operation plan for performing a failover from PSOFT_SITE1 to PSOFT_SITE 2. A failover is an unplanned event when the primary site becomes unavailable.

- Login to Enterprise Manager Cloud Control console, go to Target > Systems
- Click in PSOFT1_SITE1 System > Site Guard > Operations.
- Click Create.
- Enter a name for the plan. Example: PSOFT_SITE1_TO_SITE2_FAILOVER
- Select Operation Type: Failover
- Select the other site (PSOFT_SITE2) as the standby system
- Click Save
- The created plan will need to be customized. Edit the Post-Script steps to group scripts that can be executed in parallel and modify the order of execution:
 - Click Edit
 - In the Edit Operation Plan pane, select Detach
 - Use Move Up/Move Down to move the scripts into the correct execution order
 - Modify the Execution Group for steps executing the same scripts into the same Execution Group. This results in the scripts executing in parallel.
 - The resulting Execution Groups and order of execution (see example screen shot above):
 - /home/oracle_psft/PSFTRoleChange/startAPP.sh (Execution Group 1)
 - /home/oracle_psft/PSFTRoleChange/startPS.sh (Execution Group 2)
 - /home/oracle_psft/PSFTRoleChange/startWLS.sh (Execution Group 3)
- Save the changes.

f) Create PSOFT_SITE2_TO_SITE1_SWITCHOVER

Follow the same steps than in the previous but in PSOFT_SITE2 system. Select the PSOFT_SITE1 as the standby.

d) Create PSOFT_SITE2_TO_SITE1_FAILOVER

Follow the same steps than in the previous but in PSOFT_SITE2 system. Select the PSOFT_SITE1 as the standby.

APPENDIX C. SIEBEL DISASTER RECOVERY USING SITE GUARD

Site Guard Configuration

The steps described in this section are based on the [Site Guard Administrator's Guide for Enterprise Manager Cloud Control version 13.4](#). This Appendix contains only those steps specific to configuring Site Guard for Siebel switchover/failover. Refer to the main body of the white paper for steps that are not Siebel specific.

1. Create named credentials

You must create named credentials for the targets associated with Oracle Site Guard for application tier hosts, db hosts Oracle Databases. This table summarizes the named credentials required for managing PeopleSoft application-level DR with Oracle Site Guard:

CREDENTIAL NAME	AUTHENTICATION TARGET TYPE	CREDENTIAL TYPE	CREDENTIAL SCOPE	TARGET USERNAME	DESCRIPTION
SIEBEL_ORACLE_CRED	Host	Host Credential	Global	oracle	App Tier User Credentials
SIEBEL_ROOT_CRED	Host	Host Credential	Global	root	App Tier Root Credentials
EXADATA_ORACLE_CRED	Host	Host Credential	Global	oracle	Oracle User Credentials
EXADATA_DB_SYS_CRED	Database Instance	Database Credential	Global	sys as sysdba	SYSDBA Credentials

NOTE: Credentials are the same for the primary and standby app tier and db hosts so using global credentials instead of targeted credentials simplifies the configuration.

g) Create Siebel Application Named Credentials

To create the credentials described in the table XXX:

- Login to Enterprise Manager Cloud Control console
- Navigate to Setup > Security > Named Credentials.
- Click Create, and create the named credentials as described in the table
- Test and Save.
- Repeat the same to create all and any other additional credentials you need for the host.

This table summarizes the named credentials for managing ZFS storage role reversal:

CREDENTIAL NAME	AUTHENTICATION TARGET TYPE	CREDENTIAL TYPE	CREDENTIAL SCOPE	TARGET USERNAME	DESCRIPTION
SITE1_ZFS_CRED	Host	Host Credential	Global	root	ZFS Root Credentials
SITE2_ZFS_CRED	Host	Host Credential	Global	root	ZFS Root Credentials
SITE1_BASTION_HOST_CRED	Host	Host Credential	Global	oracle	EM Agent User Credentials
SITE2_BASTION_HOST_CRED	Host	Host Credential	Global	oracle	EM Agent User Credentials

h) Create ZFS Named Credentials

To create the credentials described in the table:

- Login to Enterprise Manager Cloud Control console
- Navigate to Setup > Security > Named Credentials.

- Click Create, and create the named credentials as described in the table
- Save.
 - A warning will be displayed asking you to confirm saving without testing the connection, Select OK
 - The ZFS Storage Arrays are not Discovered Host Targets, so you will not be able to test the connection.

i) Create Bastion Host Named Credentials

To create the credentials described in the table:

- Login to Enterprise Manager Cloud Control console
- Navigate to Setup > Security > Named Credentials.
- Click Create, and create the named credentials as described in the table
- Test and Save.

2. Configuring preferred credentials

Once the named credentials have been created, they can be assigned to the targets as the preferred credentials. This approach is recommended to simplify the Site Guard configuration. Follow these steps to configure the preferred credentials for a target:

- k) Login to Enterprise Manager Cloud Control console
- l) Navigate to Setup > Security > Preferred Credentials
- m) Select a target type (Database Instance, Hosts, etc.), and click “Manage Preferred Credentials”.
- n) Set the preferred credentials for each target credential, by clicking each row, “Set” and selecting the appropriate named credential created in the previous step.
- o) Do this for the following targets:
 - **Primary and Standby Database Instances** (at minimum, sysdba credentials, database hosts credentials)
 - **Primary and Standby App Tier Hosts**
 - **Primary and Standby Bastion Hosts**

3. Defining Primary and Standby Site Systems in EM

A disaster recovery site managed by Oracle Site Guard is modeled as a Generic System target type in Oracle Enterprise Manager. Follow these steps to create the Generic System that models the Primary (active) site, SIEBEL_SITE1:

NOTE: In the rest of the steps SIEBEL_SITE1 will be the Primary site and SIEBEL_SITE2 will be the Standby site.

- w) Login to Enterprise Manager Cloud Control console
- x) Go to Targets > Systems
- y) Click Add > Generic System
- z) Generic System: General Screen
- aa) Enter a Name for the System. For example: SIEBEL_SITE1.
- bb) You can optionally add system properties (Department, Line of Business, Location, etc.)
- cc) Add members to the system. For the primary site add:
 - The **primary PeopleSoft Host Targets**
 - The **primary Database Instance Target**
 - The primary **PCA Bastion Host Target**

NOTE: Do NOT add the database system itself. The Data Guard system that is part of will be added and it will include primary and standby databases.

- dd) Click Next
- ee) **Generic System: Define Associations.** You can leave defaults and click Next.
- ff) **Generic System: Availability Criteria.** You can add database as key member and click Next.
- gg) **Generic System: Charts Screen.** You can leave defaults and click Finish.

Repeat same steps to create the standby site system, SIEBEL_SITE2.

4. Defining Site Roles

Once a disaster recovery site managed by Oracle Site Guard has been modeled as a Generic System target in Oracle Enterprise Manager, then you designate it as a primary site or a standby site. This is done following these steps:

- q) Login to Enterprise Manager Cloud Control console, go to Targets > Systems
- r) Click on the name of the **primary** site system, TT_SITE1.
- s) On the system's home page, from the Generic System menu, select **Site Guard > Configure**.
- t) On the **General** tab, click **Create**
- u) On the **General** tab, in the **Standby System(s)** section, click Add.
- v) Choose the **standby** system, SIEBEL_SITE2, and click **Select**.
- w) Click **Save** and **OK** to confirm the action. Site Guard saves the standby system configuration.
- x) Verify that the roles have been assigned:
In the primary Site system, SIEBEL_SITE1, in Oracle Site Guard Configuration, General Tab, you must see:
Current Role Primary
In the secondary Site system, SIEBEL_SITE2, in Oracle Site Guard Configuration, General Tab, you must see:
Current Role Standby

5. Credential associations

Credentials are associated with targets and used by Oracle Site Guard operation plans when they are executed. These associations must be configured for primary and standby systems:

- q) Login to Enterprise Manager Cloud Control console.
- r) From the Targets menu, click **Systems**
- s) On the Systems page, click the name of the system for which you want to configure credential associations.
- t) On the system's home page, from the Generic System menu, select Site Guard > Configure.
- u) Click the Credentials tab. Now associate the different types of credentials
- v) **Normal Host Credentials** section, click Add, select **All** and check **Preferred**, Normal Host Credentials. Click Save.
- w) **Privileged Host Credentials** are required for the app tier hosts. Privileged credential are used to execute scripts that mount and unmount nfs filesystems.
- x) **SYSDBA Database Credentials** section, click Add, select **All** and **Preferred**, "SYSDBA Database Credentials". Click Save

Repeat the same for the standby system.

6. Configuring required scripts

Oracle Site Guard provides a mechanism for you to configure scripts for managing disaster recovery operations. See Section 9.5 Switchover of the Siebel Maximum Availability Architecture on Private Cloud Appliance on Exadata for discussion on the scripts that must be developed to orchestrate Switchover and Failover using Site Guard.

SCRIPT TYPE	SCRIPT PATH	OPERATION	ROLE	TARGET HOST
Pre Script	Following scripts will be run as pre scripts (refer to xxxxx for script details): <ul style="list-style-type: none">/home/oracle/ss_down/home/oracle/gw_down/home/oracle/tomcat_down	Switchover	Primary	All Primary App Tier Hosts
Post Scripts	Following scripts will be run as post scripts (refer to xxx for script details): <ul style="list-style-type: none">/home/oracle/tomcat_up/home/oracle/gw_up/home/oracle/ss_up	Switchover/ Failover	Standby	All Standby App Tier Hosts
Storage Scripts	Unmount EBS application NFS filesystem on primary: sh mount_umount.sh -o umount -f <nfs mount point> Example: sh mount_umount.sh -o umount -f '/siebelfs'	Switchover	Primary	All Primary App Tier Hosts

<p>Mount EBS application NFS filesystem on standby:</p> <pre>sh mount_umount.sh -o mount -f <nfs mount point></pre> <p>Example: sh mount_umount.sh -o mount -f '/siebelfs'</p>	Switchover/ Failover	Standby	All Standby App Tier Hosts
<p>Perform ZFS Role Reversal on switchover:</p> <pre>sh zfs_storage_role_reversal.sh --target_appliance <target remote replication FQDN> --source_appliance <source remote replication FQDN> --project_name <ZFS Project Name> --target_pool_name <Target Pool Name> --source_pool_name <Source Pool Name> --is_sync_needed N --continue_on_sync_failure Y --sync_timeout 1800 --operation_type switchover</pre> <p>Example: sh zfs_storage_role_reversal.sh --target_appliance pca1zfs.cloud.osc.oracle.com --source_appliance pca3zfs.cloud.osc.oracle.com --project_name MAA_SiebelFS --target_pool_name Pool01 --source_pool_name OVCA_POOL --is_sync_needed N --continue_on_sync_failure Y --sync_timeout 1800 --operation_type switchover</p>	Switchover	Standby	Standby PCA Bastion Host
<p>Perform ZFS Role Reversal on failover:</p> <pre>sh zfs_storage_role_reversal.sh --target_appliance <target remote replication FQDN> --source_appliance <source remote replication FQDN> --project_name <ZFS Project Name> --target_pool_name <Target Pool Name> --source_pool_name <Source Pool Name> --is_sync_needed N --continue_on_sync_failure Y --sync_timeout 1800 --operation_type failover</pre> <p>Example: sh zfs_storage_role_reversal.sh --target_appliance pca1zfs.cloud.osc.oracle.com --source_appliance pca3zfs.cloud.osc.oracle.com --project_name MAA_SiebelFS --target_pool_name Pool01 --source_pool_name OVCA_POOL --is_sync_needed N --continue_on_sync_failure Y --sync_timeout 1800 --operation_type failover</p> <p>Note: The source appliance is the ZFS Storage Appliance at the Primary Site and the target appliance is the ZFS Storage Appliance at the Standby Site. The scripts execute on a bastion host configured on the Standby PCA.</p>	Failover	Standby	Standby PCA Bastion Host

To configure the PeopleSoft DR scripts for SIEBEL_SITE1:

- y) Login to Enterprise Manager Cloud Control console, go to Targets > Systems
- z) Right-click the SIEBEL_SITE1 System
- aa) Navigate to Site Guard > Configure
- bb) Click the Pre/Post scripts tab
- cc) Add **Pre-Scripts** to **SIEBEL_SITE1** system:
 - Add Pre-scripts as described in the Pre-Scripts section of the table
- dd) Add **Post-Scripts** to **SIEBEL_SITE1** system:
 - Add Switchover Post-scripts as describe in the table
 - Add Failover Post-scripts as described in the Post Scripts section of the table

To configure the Storage Scripts for SIEBEL_SITE1:

- m) Click the Storage Scripts tab
- n) Add the Switchover Storage Unmount Script
 - a. Click Add
 - b. Click the eyeglass to the right of the Software Library Path edit box
 - c. Enter: 'Role Reverse Storage Scripts'
 - d. Select 'Role Reverse Storage Scripts' row with type 'Component'
 - e. Click Select
 - f. Insert "sh mount_umount.sh -o umount -f '/siebelfs'" into Script Path
 - g. Select all app tier Target Hosts (do not select any non-app tier hosts)
 - h. Select 'Unmount' Script Type
 - i. Select 'Switchover' Operation Type
 - j. Click Save

- o) Add the Switchover Storage Mount Script
 - a. Select Storage Unmount Script you just created
 - b. Click Add Like
 - c. Insert "sh mount_umount.sh -o mount -f '/siebelfs'" into Script Path
 - d. Select all app tier Target Hosts (do not select any non-app tier hosts)
 - e. Select 'Mount' Script Type
 - f. Select 'Switchover' Operation Type
 - g. Click Save
- p) Add the Failover Storage Mount Script:
 - a. Select Storage Mount Script you just created
 - b. Click Add Like
 - c. Insert "sh mount_umount.sh -o mount -f '/siebelfs'" into Script Path
 - d. Select all app tier Target Hosts (do not select any non-app tier hosts)
 - e. Select 'Mount' Script Type
 - f. Select 'Failover' Operation Type
 - g. Click Save
- q) Add the Switchover ZFS Storage Role Reversal script
 - a. Click Add
 - b. Click the eyeglass to the right of the Software Library Path edit box
 - c. Enter: 'Role Reverse Storage Scripts'
 - d. Select 'Role Reverse Storage Scripts' row with type 'Component'
 - e. Click Select
 - f. Insert the `zfs_role_reversal.sh` switchover example from the table. Substitue your deployments source and target remote replication FQDNs, ZFS project name and source and target Pool Names.
 - g. Select the PCA Bastion Host Target
 - h. Select 'Storage-Switchover' Script Type
 - i. Select 'Switchover' Operation Type
 - j. Expand Advanced Options to add credentials to connect to ZFS Storage in this order:
 - i. Move the Primary PCA ZFS credential ('SITE1_ZFS_CRED') from Available Value to Selected Value
 - ii. Move the Standby PCA ZFS credential ('SITE2_ZFS_CRED') from Available Value to Selected Value
 - k. Click Save
- r) Add the Failover ZFS Storage Role Reversal script
 - a. Click Add
 - b. Click the eyeglass to the right of the Software Library Path edit box
 - c. Enter: 'Role Reverse Storage Scripts'
 - d. Select 'Role Reverse Storage Scripts' row with type 'Component'
 - e. Click Select
 - f. Insert the `zfs_role_reversal.sh` failover example from the table. Substitue your deployments source and target remote replication FQDNs, ZFS project name and source and target Pool Names.
 - g. Select the PCA Bastion Host Target
 - h. Select 'Storage-Failover' Script Type
 - i. Select 'Failover' Operation Type
 - j. Expand Advanced Options to add credentials to connect to ZFS Storage in this order:
 - i. Move the Primary PCA ZFS credential ('SITE1_ZFS_CRED') from Available Value to Selected Value
 - ii. Move the Standby PCA ZFS credential ('SITE2_ZFS_CRED') from Available Value to Selected Value
 - k. Click Save

To configure the Peoplesoft DR scripts for SIEBEL_Site2:

- ee) Login to Enterprise Manager Cloud Control console, go to Targets > Systems
- ff) Right-click the SIEBEL_SITE2 System
- gg) Navigate to Site Guard > Configure
- hh) Click the Pre/Post scripts tab
- ii) Add **Pre-Scripts** to **SIEBEL_SITE2** system:
 - Add Pre-scripts as describe in the Pre-Scripts section of the table
- jj) Add **Post-Scripts** to **SIEBEL_SITE2** system:
 - Add Switchover Post-scripts as describe in the table
 - Add Failover Post-scripts as described in the Post Scripts section of the table

To configure the Storage Scripts for SIEBEL_SITE2 repeat the steps described for configuring the Storage Scripts for SIEBEL_SITE1. The source and target parameters will be the reverse of what you specified for SIEBEL_SITE1.

7. Configuring apply and transport lag thresholds (optional)

Site Guard verifies the apply and transport lag of the Data Guard during the prechecks and the switchover. By default, if the value is different than zero, the precheck fails and the switchover is not performed. You can define a threshold value to allow a few seconds so the check is more permissive. This step is optional. Example to set the thresholds to 10 seconds:

- g) Connect via SSH to the OMS host
- h) Login to emcli:

```
[oracle@emcc bin]$ cd $EM_HOME/middleware/bin
[oracle@emcc bin]$ ./emcli login -username=sysman
```

- i) Set the threshold to 10 seconds in both sites:

```
[oracle@emcc]$ ./emcli configure_siteguard_lag -system_name=SIEBEL_SITE1 -property_name=apply_lag -value=10
[oracle@emcc]$ ./emcli configure_siteguard_lag -system_name=SIEBEL_SITE2 -property_name=apply_lag -value=10

[oracle@emcc]$ ./emcli configure_siteguard_lag -system_name=SIEBEL_SITE1 -property_name=transport_lag -value=10
[oracle@emcc]$ ./emcli configure_siteguard_lag -system_name=SIEBEL_SITE2 -property_name=transport_lag -value=10
```

8. Creating switchover and failover operation plans

An operation plan describes the flow of execution that Oracle Site Guard performs in a disaster recovery operation. It consists of (ordered) actions that can be executed in series or in parallel. Oracle Site Guard creates a default version of the operation plan based on the site topology and the Oracle Site Guard configuration. You can use this default operation plan or customize it depending on your configuration.

The following operations plans are recommended for EBS DR:

PLAN	DESCRIPTION
SIEBEL_SITE1_TO_SITE2_SWITCHOVER	Switchover from Site1 to Site2 where Site1 is the primary system and Site2 is the standby system. This is a planned transition where Site1 is gracefully shutdown prior to transition to Site2.
SIEBEL_SITE2_TO_SITE1_SWITCHOVER	Switchover from Site2 to Site1 when Site2 is the primary system and Site1 is the standby system. This is a planned transition where Site2 is gracefully shutdown prior to transition to Site1.
SIEBEL_SITE1_TO_SITE2_FAILOVER	Failover from Site1 to Site2 when Site1 is the primary system and Site2 is the standby system. A failover occurs as a result of an unplanned event when the primary site becomes unavailable.
SIEBEL_SITE2_TO_SITE1_FAILOVER	Switchover from Site2 to Site1 when Site2 is the primary system and Site1 is the standby system. A failover occurs as a result of an unplanned event when the primary site becomes unavailable.

NOTE: To successfully execute a Site Guard operation plan the state of Site Guard configuration, Data Guard configuration and ZFS remote replication must be consistent. That is, if SIEBEL_SITE1 generic system is the primary system in the Site Guard Configuration the Database Target associated with SIEBEL_SITE1 must be the primary database in the Data Guard configuration and the ZFS project, not the replica, must reside on the ZFS Storage Array attached to the PCA hosting the primary application tier hosts.

g) Create SIEBEL_SITE1_TO_SITE2_SWITCHOVER

Operation plan for performing a switchover from EBS_SITE1 to EBS_SITE 2.

- Login to Enterprise Manager Cloud Control console, go to Target > Systems
- Click in SIEBEL_SITE1 System > Site Guard > Operations.
- Click Create.
- Enter a name for the plan. Example: **SIEBEL_SITE1_TO_SITE2_SWITCHOVER**
- Select Operation Type: Switchover
- Select the other site (SIEBEL_SITE2) as the standby system
- Click Save
- The created plan will need to be customized. Edit the Pre-Script steps to group scripts that can be executed in parallel and modify the order of execution:
 - Click Edit
 - In the Edit Operation Plan pane, select Detach
 - Use Move Up/Move Down to move the scripts into the correct execution order
 - Modify the Execution Group for steps executing the same scripts into the same Execution Group. This results in the scripts executing in parallel.
 - The resulting Execution Groups and order of execution (see example screen shot below):
 - /home/oracle/ss_down (Execution Group 1)
 - /home/oracle/gw_down (Execution Group 2)
 - /home/oracle/tomcat_down (Execution Group 3)
- Edit the Post-Script steps to group scripts that can be executed in parallel and modify the order of execution:
 - Click Edit
 - In the Edit Operation Plan pane, select Detach
 - Use Move Up/Move Down to move the scripts into the correct execution order
 - Modify the Execution Group for steps executing the same scripts into the same Execution Group. This results in the scripts executing in parallel.
 - The resulting Execution Groups and order of execution (see example screen shot below):
 - /home/oracle/tomcat_up (Execution Group 1)
 - /home/oracle/gw_up (Execution Group 2)
 - /home/oracle/ss_up (Execution Group 3)
 - Save the changes

Target Name	Target Host	Operation Type	Error Mode	Execution Mode	Execution Group	Run Mode
Pre-Scripts				Parallel		
/home/oracle/ss_down	pca1vm63.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled
/home/oracle/ss_down	pca1vm62.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled
/home/oracle/gw_down	pca1vm59.cloud.osc.oracle.com	Run Script	Stop on Error		2	Enabled
/home/oracle/gw_down	pca1vm58.cloud.osc.oracle.com	Run Script	Stop on Error		2	Enabled
/home/oracle/gw_down	pca1vm57.cloud.osc.oracle.com	Run Script	Stop on Error		2	Enabled
/home/oracle/tomcat_down	pca1vm63.cloud.osc.oracle.com	Run Script	Stop on Error		3	Enabled
/home/oracle/tomcat_down	pca1vm61.cloud.osc.oracle.com	Run Script	Stop on Error		3	Enabled
/home/oracle/tomcat_down	pca1vm59.cloud.osc.oracle.com	Run Script	Stop on Error		3	Enabled
/home/oracle/tomcat_down	pca1vm60.cloud.osc.oracle.com	Run Script	Stop on Error		3	Enabled
/home/oracle/tomcat_down	pca1vm58.cloud.osc.oracle.com	Run Script	Stop on Error		3	Enabled
/home/oracle/tomcat_down	pca1vm57.cloud.osc.oracle.com	Run Script	Stop on Error		3	Enabled
/home/oracle/tomcat_down	pca1vm62.cloud.osc.oracle.com	Run Script	Stop on Error		3	Enabled
Storage Unmount Scripts				Parallel		
sh mount_umount.sh -o umount -f 'siebel's (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca1vm63.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled
sh mount_umount.sh -o umount -f 'siebel's (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca1vm61.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled
sh mount_umount.sh -o umount -f 'siebel's (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca1vm59.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled
sh mount_umount.sh -o umount -f 'siebel's (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca1vm60.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled
sh mount_umount.sh -o umount -f 'siebel's (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca1vm58.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled
sh mount_umount.sh -o umount -f 'siebel's (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca1vm57.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled
sh mount_umount.sh -o umount -f 'siebel's (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca1vm62.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled
Storage Scripts				Parallel		
sh zfs_storage_role_reversal.sh --target_appliance pca3zfs.cloud.osc.oracle.com --source_appliance pca1zfs.cloud.osc.oracle.com --project_name MAA_SiebelIFS --target	pca3bst.cloud.osc.oracle.com	Run Storage Script	Stop on Error		1	Enabled
Database Instances				Parallel		
CD811_Cluster-c1_CD8111	exa14-01.us.osc.oracle.com	Switchover Database	Stop on Error		1	Enabled
Storage Mount Scripts				Parallel		
sh mount_umount.sh -o mount -f 'siebel's (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca3vm57.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled
sh mount_umount.sh -o mount -f 'siebel's (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca3vm61.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled
sh mount_umount.sh -o mount -f 'siebel's (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca3vm60.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled
sh mount_umount.sh -o mount -f 'siebel's (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca3vm63.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled
sh mount_umount.sh -o mount -f 'siebel's (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca3vm58.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled
sh mount_umount.sh -o mount -f 'siebel's (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca3vm62.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled
sh mount_umount.sh -o mount -f 'siebel's (Software Library: Site Guard/12.1.0.2.0/all_platforms/run_script/Run Siteguard Scripts)	pca3vm59.cloud.osc.oracle.com	Run Script	Stop on Error		1	Enabled

Post-Scripts				Parallel			
/home/oracle/tomcat_up	pca3vm57.cloud.osc.oracle.com	Run Script	Stop on Error		1		Enabled
/home/oracle/tomcat_up	pca3vm61.cloud.osc.oracle.com	Run Script	Stop on Error		1		Enabled
/home/oracle/tomcat_up	pca3vm60.cloud.osc.oracle.com	Run Script	Stop on Error		1		Enabled
/home/oracle/tomcat_up	pca3vm63.cloud.osc.oracle.com	Run Script	Stop on Error		1		Enabled
/home/oracle/tomcat_up	pca3vm58.cloud.osc.oracle.com	Run Script	Stop on Error		1		Enabled
/home/oracle/tomcat_up	pca3vm62.cloud.osc.oracle.com	Run Script	Stop on Error		1		Enabled
/home/oracle/tomcat_up	pca3vm59.cloud.osc.oracle.com	Run Script	Stop on Error		1		Enabled
/home/oracle/gw_up	pca3vm57.cloud.osc.oracle.com	Run Script	Stop on Error		2		Enabled
/home/oracle/gw_up	pca3vm58.cloud.osc.oracle.com	Run Script	Stop on Error		2		Enabled
/home/oracle/gw_up	pca3vm59.cloud.osc.oracle.com	Run Script	Stop on Error		2		Enabled
/home/oracle/ss_up	pca3vm63.cloud.osc.oracle.com	Run Script	Stop on Error		3		Enabled
/home/oracle/ss_up	pca3vm62.cloud.osc.oracle.com	Run Script	Stop on Error		3		Enabled

h) Create SIEBEL_SITE1_TO_SITE2_FAILOVER

Operation plan for performing a failover from SIEBEL_SITE1 to SIEBEL_SITE 2. A failover is an unplanned event when the primary site becomes unavailable.

- Login to Enterprise Manager Cloud Control console, go to Target > Systems
- Click in SIEBEL_SITE1 System > Site Guard > Operations.
- Click Create.
- Enter a name for the plan. Example: SIEBEL_SITE1_TO_SITE2_FAILOVER
- Select Operation Type: Failover
- Select the other site (SIEBEL_SITE2) as the standby system
- Click Save
- The created plan will need to be customized. Edit the Post-Script steps to group scripts that can be executed in parallel and modify the order of execution:
 - Click Edit
 - In the Edit Operation Plan pane, select Detach
 - Use Move Up/Move Down to move the scripts into the correct execution order
 - Modify the Execution Group for steps executing the same scripts into the same Execution Group. This results in the scripts executing in parallel.
 - The resulting Execution Groups and order of execution (see example screen shot above):
 - /home/oracle/tomcat_up (Execution Group 1)
 - /home/oracle/gw_up (Execution Group 2)
 - /home/oracle/ss_up (Execution Group 3)
- Save the changes.

i) Create SIEBEL_SITE2_TO_SITE1_SWITCHOVER

Follow the same steps than in the previous but in SIEBEL_SITE2 system. Select the SIEBEL_SITE1 as the standby.

d) Create SIEBEL_SITE2_TO_SITE1_FAILOVER

Follow the same steps than in the previous but in SIEBEL_SITE2 system. Select the SIEBEL_SITE1 as the standby.

APPENDIX D. HOW TO SETUP A SERVICE HOST FOR SITE GUARD USE

These instructions will create a service host VM guest using an official Oracle 7 Linux VM assembly. If you create VM guests using an ISO image skip to step 3 after the virtual machine is created.

1. Download Oracle VM 3 Template for Oracle 7 Linux
 - 1.1. Go to Oracle Software Delivery Cloud
 - 1.2. Sign in using your Oracle account
 - 1.3. Choose 'Release' from the select list
 - 1.4. Search for 'Oracle VM 3 Templates for Oracle Linux 7'
 - 1.5. Add 'REL: Oracle VM3 Templates for Oracle 7 Linux' to the Cart
 - 1.6. Select Checkout and download the latest template
 - 1.7. Follow instructions to install the template into a Repository
2. Create a Virtual Machine
 - 2.1. From the Oracle VM Manager console click on the 'Create Virtual Machine' icon
 - 2.2. Select 'Clone from an existing VM Template'
 - 2.3. Select the Repository containing the Oracle VM 3 Template for Oracle Linux 7
 - 2.4. Select the Oracle Linux 7 VM assembly
 - 2.4.1. Example: OVM_OL7U6_x86_64_PVHVM.ova
 - 2.5. Click 'Finish'
3. Follow steps in MOS note 2017593.1 to add the 192.168.4.0 internal network to Oracle VM Manager
4. Update the service host networking
 - 4.1. Select the Virtual Machine from the Virtual Machines list
 - 4.2. Select the Edit icon
 - 4.3. Click on the Networks tab
 - 4.4. Select vm_public network for Slot 0
 - 4.5. Select 192.168.4.0 network and click 'Add VNIC' to create Slot 1
5. Complete network setup of the service host
 - 5.1. Start the Virtual Machine
 - 5.2. Open the Virtual Machine console
 - 5.3. Follow the prompts on the console to configure eth0
 - 5.4. When prompted for IP addresses for DNS, enter the 192.168.4.x name servers. You can get these from /etc/resolv.conf on one of the OVM Servers.
 - 5.5. Plumb the eth1 interface using 192.168.4.9x/24, where 9x is 90-99. The last octet must not already be in use.
6. Update to the latest Oracle 7 Linux
 - 6.1. Setup up proxy if needed
 - 6.2. Execute: yum update
 - 6.3. Execute: ol_yum_configure.sh
 - 6.4. Execute: reboot
7. After reboot log in as root and install the required Python packages:
 - 7.1. Execute: yum install bind-utils
 - 7.2. Execute: yum install oracle-epel-release-el7.x86_64
 - 7.3. Execute: yum update
 - 7.4. Execute: yum install python2-pip
 - 7.5. Execute: pip --proxy http://x.x.x.x:p install --upgrade pip
 - 7.6. Execute: pip --proxy http://x.x.x.x:p install pexpect
 - 7.7. Execute: pip --proxy http://x.x.x.x:p install requests
8. Disable iptables or add matching rules

8.1. Example: systemctl stop iptables

9. Install an EM Agent on the service host from the controlling Oracle Enterprise Manager Infrastructure

See [Installing Oracle Management Agents](#)

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.

Outside North America, find your local office at oracle.com/contact.

 blogs.oracle.com

 facebook.com/oracle

 twitter.com/oracle

Copyright © 2021, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

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

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0120

WebLogic Cloud on Market Place Disaster Recovery
March, 2021

