ORACLE

# Using Oracle Site Guard to manage Disaster Recovery for OCI PaaS Systems

Using Oracle Site Guard for SOA Cloud Service DR, SOA Market Place DR and WebLogic for OCI DR

March 2021 | Version 2

## PURPOSE STATEMENT

This document provides a description, a summary of requirements, and the setup procedure for using Oracle Site Guard to manage switchover and failover in a Paas Disaster Recovery. The steps described in this whitepaper apply to SOA Cloud Service, SOA Market Place and WebLogic for OCI Disaster Recovery environments that are based on the Oracle best practices. This paper is oriented to a technical audience having knowledge of Enterprise Manager, Site Guard, Oracle Cloud, Oracle WebLogic, Oracle Database, and Oracle Data Guard.

## DISCLAIMER



## REVISION HISTORY

The following revisions have been made to this white paper:

| Date | Revision | Comments |
|---|---|---|
| June 2020 | 1 | Initial publication |
| March 2021 | 2 | Small fixes |
| | | |

# TABLE OF CONTENTS

# 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.

This protection is also required for the systems deployed in the Cloud, like the PaaS services. Oracle's Maximum Availability Architecture (Oracle MAA) provides disaster recovery solutions for several PaaS services like SOA Cloud Service, SOA on Market Place and WebLogic for OCI, that are published in MAA Best Practices for the Oracle Cloud. The disaster recovery architecture solution for these PaaS services is based in an active-passive topology: there is one system in one region with primary role and a secondary system in another region with the standby role. The switchover is a planned procedure that changes the roles between these two sites: the primary sites 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 role change.

These steps can be performed manually 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 PaaS Disaster Recovery environments 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 Cloud Control, Oracle Cloud Infrastructure, Oracle Weblogic Server, Oracle Database, Data Guard and Oracle Database backup and recovery.

# ORACLE SITE GUARD FOR PAAS 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 Fusion Middleware, Oracle Fusion Applications, and Oracle Databases. 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 in a WebLogic Market Place DR environment.

Oracle Site Guard can be used to coordinate the switchovers for PaaS Disaster Recovery scenarios that follow the MAA best practices described in the following whitepapers available in MAA Best Practices for the Oracle Cloud web:

- SOA Cloud Service Disaster Recovery on OCI
- SOA on OCI Market Place Disaster Recovery
- Oracle WebLogic Server for Oracle Cloud Infrastructure Disaster Recovery

A sample Paas Cloud Disaster Recovery with Site Guard topology is shown below:

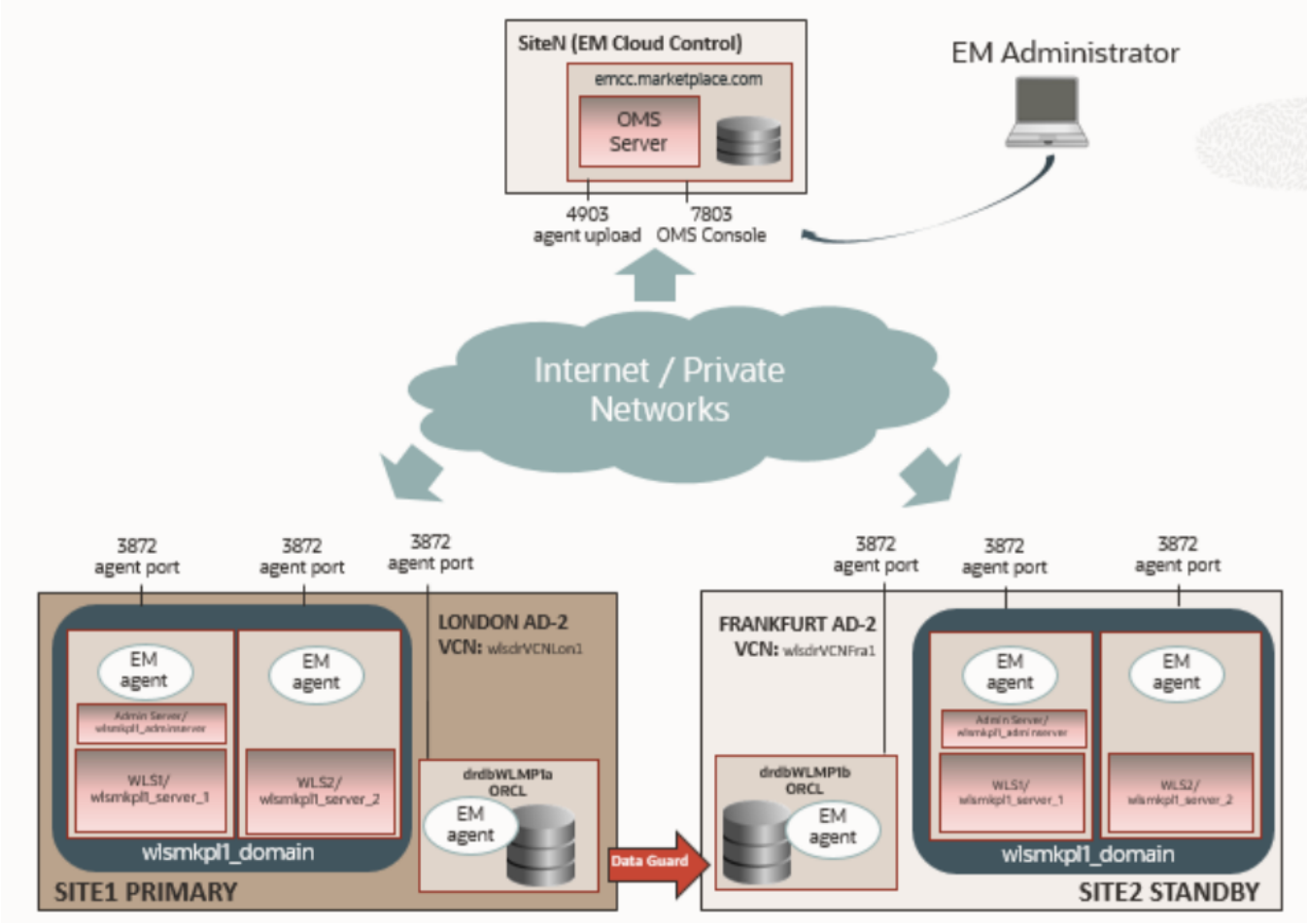


Figure 1 Using Site Guard to manage switchover in Paas DR

**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 in Cloud. The Enterprise Manager Cloud Control Server can be located in the same region of one of the PaaS systems or in a different region. 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 PaaS DR environment hosts.
- **Target Discovery**
  Discover the targets that will be managed by the Site Guard (WebLogic Domains, Databases, etc.)
- **Site Guard Configuration**
  Configure Site Guard (sites, credentials, scripts, plans, etc.) to orchestrate the switchover and failover in the PaaS 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.

## 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 Setting Up Oracle Enterprise Manager 13.3 on Oracle Cloud Infrastructure in order to create and configure an EM in your cloud tenancy based on a Market Place EM image. This Marketplace Image contains pre-configured Oracle Enterprise Manager (13.3 PG) with co-located Oracle Database (19.3). As a result, an EM host will be created with name "emcc.marketplace.com". This hostname is used in following sections to refer to the OMS hostname.

## 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 cloud datacenters, and the 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 WebLogic Cloud DR targets will communicate each other via their public IPs. Oracle recommends using hostnames associated to the public IPs of the cloud 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.

Private names for the hosts are given by cloud infrastructure, but the public names must be defined/customized in each case. For example:

| SITE | PRIVATE NAME | PUBLIC NAME (DEFINED BY CUSTOMER) | PUBLIC IP |
|---|---|---|---|
| **SiteN** | emcc.marketplace.com | emcc.marketplace.com | 111.111.111.100 |
| **Site1** | wlsmkpl1-wls-0.site1cloudinternaldomain.com | wlsmkpl1-wls-0-public.site1.example.com | 111.111.111.11 |

| | | | |
|---|---|---|---|
| | wlsmkpl1-wls-1.site1cloudinternaldomain.com | wlsmkpl1-wls-1-public.site1.example.com | 111.111.111.12 |
| | drdbwlmp1a.site1cloudinternaldomain.com | drdbwlmp1a-public.site1.example.com | 111.111.111.13 |
| **Site2** | wlsmkpl1-wls-0.site2cloudinternaldomain.com | wlsmkpl1-wls-0-public.site2.example.com | 222.222.222.11 |
| | wlsmkpl1-wls-1.site2cloudinternaldomain.com | wlsmkpl1-wls-1-public.site2.example.com | 222.222.222.12 |
| | drdbwlmp1b.site2cloudinternaldomain.com | drdbwlmp1b-public.site2.example.com | 222.222.222.13 |

This is an example of the /etc/hosts file entries that would be set in OMS host and in each monitored host when they are communicating using public IPs:

```
#########################################################################
# OMS host public IP (this entry only required to be added to the monitored hosts. In the OMS is already set and should not be changed)
111.111.111.100      emcc.marketplace.com
#########################################################################
# Public names for cloud monitored hosts
#########################################################################
# SITE 1 (these entries only required in SITE1 hosts and OMS host)
111.111.111.11       wlsmkpl1-wls-0-public.site1.example.com
111.111.111.12       wlsmkpl1-wls-1-public.site1.example.com
111.111.111.13       drdbwlmp1a-public.site1.example.com

# SITE 2 (these entries only required in SITE2 hosts and OMS host)
222.222.222.11       wlsmkpl1-wls-0-public.site2.example.com
222.222.222.12       wlsmkpl1-wls-1-public.site2.example.com
222.222.222.13       drdbwlmp1b-public.site2.example.com
```

In scenarios when the communication between OMS and monitored hosts is possible using **private** networks (through a Dynamic Routing Gateway[1]), the OMS and monitored hosts **can use the appropriate internal IPs/names instead** of the public IP/names to communicate with each other. In that case, the /etc/hosts files of the OMS should contain the internal IPs and internal names of the hosts.

## 2. Security Rules

Oracle Management Servers needs to communicate with the agents in the monitored hosts, and the agents connect to OMS server to upload the monitoring data. For discovering FMW targets, the OMS needs to be able to communicate with the Administration Server of the WebLogic domains, and for database monitoring, OMS needs to 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 encryption[2]). The following communications are required between the OMS and the monitored targets:

| SOURCE | DESTINATION | PROTOCOL |
|---|---|---|
| **Any Monitored Host** | OMS Upload port (4903) | HTTPS |
| **OMS host** | Any monitored host agent port (3872) | HTTPS |
| **OMS host** | Any target database listener port (1521) | SQL (with Network Encryption) |
| **OMS host** | Any monitored host ssh port (22) | SSH (for agent software transfer) |

[1] Refer to the Dynamic Routing Gateways for details on the network configuration.

[2] Setting Up Oracle Enterprise Manager 13.3 on Oracle Cloud Infrastructure

| | | |
|---|---|---|
| **Internet (or the CIDR of the administrators users' network)** | OMS console port (7803) | HTTPS |

However, some of these communications are not allowed by default. To enable them, security rules are required. Follow the steps in the next points to create them.

**a) Security Rules in OMS' side**

Create the network rules to allow communication **from targets to OMS:**

- Login to the OCI Console
- Navigate to Networking > Virtual Cloud Networks > click on the Virtual Cloud Network of the OMS.
- Click in the security list where you want to add the rule under **Security Lists**.
- **Add Ingress Rule** (stateful) to allow traffic **from Any monitored host to OMS upload port:**
  - Source CIDR: Monitored hosts network CIDR[3]. Example: 111.111.111.0/24
  - IP Protocol: TCP
  - Source Port Range: All
  - Destination Port Range: 4903

  Repeat this for each monitored host's network.
- **Add Ingress Rule** (stateful) to allow traffic **from Internet (or from specific network) to OMS console port:**
  - Source CIDR: Use 0.0.0.0/0 to allow access to all or specify a custom network CIDR.
  - IP Protocol: TCP
  - Source Port Range: All
  - Destination Port Range: 7803

**b) Security Rules in targets' side**

Create the network rules to allow communication **from OMS to host targets:**

- Login to the OCI Console
- Navigate to Networking > Virtual Cloud Networks > click on the Virtual Cloud Network of the targets in Site1.
- Click in the security list where you want to add the rule under **Security Lists**.
- **Add Ingress Rule** (stateful) to allow traffic **from OSM host to the agent port of the monitored hosts:**
  - Source CIDR: OMS IP in CIDR format[4]. Example: 111.111.111.100/32
  - IP Protocol: TCP
  - Source Port Range: All
  - Destination Port Range: 3872
- **Add Ingress Rule** (stateful) to allow traffic **from OMS host to the db listener** port of monitored db hosts:
  - Source CIDR: OMS IP in CIDR format[5]. Example: 111.111.111.100/32
  - IP Protocol: TCP
  - Source Port Range: All
  - Destination Port Range: 1521

Repeat for the Virtual Cloud Network of the targets in Site2.

**c) IP tables in DB hosts**

In addition to OCI network security rules, the following iptables rule need may be needed in the target DB systems:

- Connect via ssh to the DB system host.
- Log in as opc and then sudo to the root user.
- Save a copy of iptables as a backup. If necessary, you can restore the original file by using the command iptables-restore < /tmp/iptables.orig.

```
[root@drdbwlmp1a ~]# iptables-save > /tmp/iptables.orig
```

[3] Use public network CIDR when OMS and targets communicate via internet, use private network CIDR when the communication via private IPs is possible.

[4] Use OMS public IP CIDR when OMS and targets communicate via internet, use OMS private IP CIDR when the communication via private IPs is possible

[5] Use OMS public IP CIDR when OMS and targets communicate via internet, use OMS private IP CIDR when the communication via private IPs is possible

- Add a rule to iptables **to allow inbound traffic on the EM agent**, as shown in the following sample.

```
[root@drdbwlmp1a ~]# iptables -I INPUT 8 -p tcp -m state --state NEW -m tcp --dport 3872 -j ACCEPT -m comment --comment "Required for EM agent port"
```

- Make sure the rule was added.

```
[root@drdbwlmp1a ~]# service iptables status
```

- Save the updated file to /etc/sysconfig/iptables.

```
[root@drdbwlmp1a ~]# service iptables save
```

- The change takes effect immediately and will remain in effect when the node is rebooted.

Using the previous example, this is a summary example of the security rules created:

| SITE | RULE TYPE | SOURCE CIDR | PROTOCOL | SOURCE PORT | DESTINATION PORT RANGE |
|---|---|---|---|---|---|
| **SiteN (OMS)** | Ingress Rule | Site1 Network CIDR<br>Example: 111.111.111.0/24 | TCP | All | 4903<br>(Upload port) |
| **SiteN (OMS)** | Ingress Rule | Site2 Network CIDR<br>Example: 22.222.222.0/24 | TCP | All | 4903<br>(upload port) |
| **SiteN (OMS)** | Ingress Rule | Administrator's Network CIDR<br>(0.0.0.0/o to allow Access to Internet) | TCP | All | 7803<br>(OMS Console Port) |
| **Site1 and Site2** | Ingress Rule | OMS IP in CIDR format.<br>Example: 111.111.111.100/32 | TCP | All | 3872<br>(agent port) |
| **Site1 and Site2** | Ingress Rule | OMS IP in CIDR format.<br>Example: 111.111.111.100/32 | TCP | All | 1521<br>(db listener port) |

*NOTE: access to the ssh port (22) is assumed to be already open from OMS to hosts. If not, add the pertinent rules to allow traffic from OMS IP to those ports in the same way as above.*

# Agents Installation

Enterprise Manager Cloud Control Agent must be installed in all the hosts of the PaaS DR environment.

## 1. 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 cloud machine. This is oracle group in midtier hosts (weblogic or soa hosts) and oinstall group in DB hosts.

For midtier 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 Midtier hosts: /u01/agent13c (note this is under / volume)[6]
<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@drdbwlmp1a]# chown emcadm:oinstall <AGENT_BASE_DIR>
```

[6] As a good practice in the midtier hosts, you can configure and attach an OCI block volume instead of using the root volume. Check Oracle documentation about block volumes in OCI documentation Overview of Block Volume

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

```
[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. Example:

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

## 2. Get the agent software

"AgentDeploy" method will be used for this. 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/
```

## 3. 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@drdbwlmp1a tmp]$ mkdir agent_image
[emcadm@drdbwlmp1a tmp]$ cp 13.3.0.0.0_AgentCore_226.zip agent_image
[emcadm@drdbwlmp1a tmp]$ cd agent_image
[emcadm@drdbwlmp1a 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=drdbwlmp1a.site1cloudinternaldomain.com
LOCALPORT=3872 AGENT_PORT=3872 ORACLE_HOSTNAME=drdbwlmp1a-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: emcc.marketplace.com |
| 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:<br>`[root@ wlsmkpl1-wls-0]# hostname –fqdn`<br>`wlsmkpl1-wls-0.site1cloudinternaldomain.com` |
| 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. OMS will use this to communicate with this agent. Must either the public IP of the host, or a public name resolvable to that public IP.<br>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 (FQDN of the hostname).<br>**TIP:** Use hostnames instead of IPs is recommended.<br>**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.<br>**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:

a) Login in OMS Console
b) Go to Setup > Add Target > Configure Auto Discovery
c) See "**Target on Hosts**". Select a host and click in "**Discover now**"
d) Then go to Setup > Add Target > Auto Discovery Results
e) See "Targets on Hosts"
f) 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:

a) 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>;
```

b) In the **Auto Discovery Results** in OMS Console, select the discovered "Cluster ASM" target in and click "Promote".
c) 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".
d) 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.
e) Click **Next** and then **Save**

## 3. Discover Database targets

To promote or discover a database target:

a) 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;
```

b) 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 dbnsmp user:

```
sqlplus / as sysdba
SQL> grant sysdba to dbsnmp 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

c) 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.

d) 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 dbsnmp. |
| Role | select "SYSDBA" |
| select "SYSDBA" | enter the password for the dbsnmp |

e) 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. Discover WebLogic Domains targets

WebLogic domains and its associated targets need to be manually discovered.

*NOTE: the admin server and the agents in the target domain needs to be up and running for discovering the domain.*

a) Login in OMS Console
b) Go to Setup > **Add Targets Manually**
c) In "Add Non-Host Target Using Guided Process" click in "Add Using Guided Process"
d) Select "**Oracle Fusion Middleware/WebLogic Domain**" and click "Add.."
e) Provide the following details:

| | |
|---|---|
| Administrator Server Host | Set it to the hostname of the WebLogic admin server host. It is recommended to provide here **the private name**, because this **is accessed by the local EM agent that runs in the WLS Admin host** and not from OMS host. If you provide here the public name or IP of the WLS Admin host be sure it is reachable from the agent that runs in the host. |
| Port | The WLS Admin server t3s port. In OCI, it is typically 9072. |
| Username/Password | weblogic/<weblogic_password> |

| | |
|---|---|
| Node Manager Username/Password | weblogic/<weblogic_password> |
| Unique Domain Identified | This is an identifier used **to differentiate WebLogic domains with the same name**s that are discovered in the same Enterprise Manager. **This is very important in WebLogic Disaster Recovery** environments because the WebLogic domain name is the same for the primary and standby. So use this to identify the site of each domain.<br>For example:<br>Use Site1 when discovering the WebLogic domain in Site1<br>Use Site2 when discovering the WebLogic domain in Site2 |
| Agent | Select **the agent of the host where WLS Admin server is running** |
| Discover Application versions | Not relevant for Site Guard, can be checked or not |

f) Click in Advance and:

| | |
|---|---|
| JMX Protocol | Use t3s. |
| Discover Down Servers | Check |
| Enable Automatic Refresh | Check |

g) Leave the rest of the properties by default (empty), and click Continue

h) In the "**Assign Agents**" screen, review carefully that the agent and host assigned to each target is the correct (especially for the second managed server). By default, each target should be assigned to the local agent that is on the same host as the target. In case they are not assigned to the proper agent or host, use "Change Hostname" or "Assign Agent" to correct any mismatch.

i) Once finished, go to Targets > Middleware to verify that the WebLogic domain has been discovered.

j) Repeat to discover the standby WebLogic domain. At least, admin server needs to be up, but to make sure everything is correctly discovered by the EM, it is recommended to run the discovery of the standby domain while it is up (admin and managed servers). To do this, you can convert the standby database to snapshot standby, then start the standby domain servers, and make the discovery. After this, stop the standby domain and convert the standby db in physical standby again.

# Site Guard Configuration

The steps described in this section are based on the Site Guard Administrator's Guide for Enterprise Manager Cloud Control version 13.3. Refer to the documentation for more details.

## 1. Creating named credentials

You must create named credentials for the targets associated with Oracle Site Guard: for mid-tier and db hosts, Oracle Node Managers, Oracle Weblogic Servers and Oracle Databases. This table summarizes the minimum named credentials required for managing WebLogic Cloud DR with Oracle Site Guard:

| CREDENTIAL NAME | AUTHENTICATION TARGET TYPE | CREDENTIAL TYPE | TARGET TYPE | TARGET | TARGET USERNAME |
|---|---|---|---|---|---|
| **WLSDR_SITE1_DB_HOST_ORACLE** | Host | SSH Key Cred. | Host | Site1 DB host | opc (with sudo to oracle) |
| **WLSDR_SITE2_DB_HOST_ORACLE** | Host | SSH Key Cred. | Host | Site2 db host | opc (with sudo to oracle) |
| **WLSDR_SITE1_WLS_HOSTS_ORACLE** | Host | SSH Key Cred. | n/a (global) | n/a (global) | opc (with sudo to oracle) |
| **WLSDR_SITE2_WLS_HOSTS_ORACLE** | Host | SSH Key Cred. | n/a (global) | n/a (global) | opc (with sudo to oracle) |
| **WLSDR_DOMAIN_NODEM** | Oracle WebLogic Domain | Node Manager Cred. | n/a (global) | n/a (global) | weblogic |
| **WLSDR_DOMAIN_WEBLOGIC** | Oracle WebLogic Domain | WebLogic Admin Cred. | n/a (global) | n/a (global) | weblogic |
| **WLSDR_ADMIN_WEBLOGIC** | Oracle WebLogic Server | Oracle WebLogic Cred. | n/a (global) | n/a (global) | weblogic |
| **WLSDR_SITE1_DB_SYS** | Database Instance | Database Cred. | Database Instance | Primary Database | sys as sysdba |
| **WLSDR_SITE2_DB_SYS** | Database Instance | Database Cred. | Database Instance | Standby Database | sys as sysdba |
| **(OPTIONAL) *ANY_AUX*_HOST_*USER***<br>**Samples:**<br>**OMS_HOST_ROOT**<br>**OMS_HOST_ORACLE** | Host | SSH Key Cred. | Host | | Any required user for executing scripts in an auxiliary host. Sample: opc (with sudo to root) for OMS host |

*NOTE: Node Manager Credentials, WebLogic Administrator Credentials and Oracle WebLogic credentials are the same for the primary and standby WebLogic domain (they must be the same in a WebLogic Cloud DR environment), so using global credentials instead of targeted credentials simplifies the configuration.*

In Cloud, the SSH authentication is done using SSH keys. SSH key **with passphrases are NOT currently supported in Enterprise Manager**. In case that the SSH keys used by your cloud instances use passphrase, you need to add to them a SSH key that does not use a passphrase. Refer to the Cloud Documentation Oracle Cloud Infrastructure Documentation >

Managing Key Pairs on Linux Instances to add a new SSH key. More than one SSH key can be configured for a cloud instance.

**a) Configure Privilege Delegation**

Only the opc user can login directly in OCI hosts. It has sudo privileges so it can sudo to any user (oracle, root). Enterprise Manager needs to perform task as oracle user in the hosts. To allow this, privilege delegation feature must be configured in the targets:

- Login in Enterprise Manager OMS Console
- Go to Setup > Security > Privilege Delegation Setting
- Select the host you want to configure and click "Edit"
- Select **Sudo**, and enter this for sudo command: "/usr/bin/sudo -i -u %RUNAS% %COMMAND%" (the "-i" option is required to load env variables from oracle's .bashrc)
- Click Save

Repeat for all the hosts in primary and standby sites, and for the OMS host (it will be configured later as an auxiliary host for executing some post-scripts).

**b) Create Names Credentials**

To create the credentials described in the table XXX:

- In OMS console, 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 or for any other auxiliary host.

## 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:

a) Login in EM, go to Setup > Security > Preferred Credentials
b) Select a target type (Database Instance, hosts, WebLogic Domain, etc.), and click "Manage Preferred Credentials".
c) Set the preferred credentials for each target credential, by clicking each row, "Set" and selecting the appropriate named credential created in the previous step.
d) Do this for the following targets:
   - **Primary and Standby Database Instances** (at minimum, sysdba credentials, database hosts credentials)
   - **Primary and Standby WebLogic Domain** (target type "Oracle WebLoigc Domain", credentials: weblogic administrator credentials, hosts credentials)
   - **Primary and Standby Admin Servers** (target type "Oracle WebLogic Server", credentials: Oracle WebLogic Administration Credentials, Host Credentials)
   - **Primary and Standby hosts**. Target type Host. Normally, only "Normal Host credentials" are required to manage DR.
   - **Any other aux host**. OMS host will be configured later as an example auxiliary host for running some post scripts. Set normal and privilege preferred credentials for this host.

## 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 a Generic System for the Site 1:

a) Login in EM OMS Console
b) Go to Targets > Systems
c) Click Add > Generic System
d) Generic System: General Screen
e) Enter a Name for the System. For example: SITE1_wlsdr.
f) You can optionally add system properties (Department, Line of Business, Location, etc.)
g) Add members to the system. For the primary site add:
   The **primary WebLogic Domain target**
   The **primary Database Instance target**

It is NOT REQUIRED to add explicitly any other components like hosts, node managers, etc.

*NOTE: do NOT add the Database System target itself. The Data Guard system that is part of will be added and it will include primary and standby databases.*

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

Repeat same steps to create the standby site system (example: SITE2_wlsdr).

## 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:

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

## 5. Configuring auxiliary hosts

You can configure one or more hosts managed by Oracle Enterprise Manager as an auxiliary host to a site. These hosts are not part of the system but are used to run Pre Scripts, Post Scripts, or Storage Scripts on a site. To add an auxiliary host to a system:

```
emcli add_siteguard_aux_hosts  -system_name="system_name"  -host_name="host_name"
```

The following auxiliary hosts are required for a PaaS DR Site Guard configuration:

**a) Auxiliary hosts for running the WLS Domain config replica script in the other site**

This is required when you are propagating configuration changes between primary and standby using an script (*dbfscopy.sh or config_replica.sh* in most recent versions), as explained in the appropriate DR whitepaper in MAA OTN page.

This script runs first in primary mid-tier host1, to synchronize changes from primary WebLogic domain configuration to the staging filesystem (dbfs or FSS). Then it runs in standby mid-tier host2, and synchronizes changes from the staging filesystem (dbfs or FSS) to the standby WebLogic domain config. It is recommended to schedule this at some intervals. But it is also good practice to run the script before any switchover operation when possible, to ensure that configuration in the new standby is up-to-date. The execution of this script can be included in the Site Guard plans.

To modeling this in Site Guard, it is required to define the Site2 mid-tier host1 as an auxiliary host for Site1, and define Site1 mid-tier host1 as an auxiliary host for Site2. Perform the following steps:

- Login in Enterprise Manager host and login in emcli:

```
[oracle@emcc bin]$ cd /u01/app/em13c/middleware

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

- Use emcli to add **the Site 2 mid-tier host1** as **an auxiliary host for Site1**. Use the hostname as it is registered in the EM. Example:

```
[oracle@emcc bin]$ ./emcli add_siteguard_aux_hosts -system_name="SITE1_wlsdr"  -host_name="wlsmkpl1-wls-0-public.site2.example.com"

Auxiliary host(s) added to system SITE1_wlsdr
```

- Use emcli to add **the Site 1 mid-tier host1 as an auxiliary host for Site2**. Use the hostname as it is registered in the EM. Example:

```
[oracle@emcc bin]$ ./emcli add_siteguard_aux_hosts -system_name="SITE2_wlsdr"  -host_name="wlsmkpl1-wls-0-public.site1.example.com"

Auxiliary host(s) added to system SITE2_wlsdr
```

**b) Auxiliary host for running DNS or /etc/hosts change**

The public name used by application consumers (defined as the frontend in the WebLogic domains) must always point to the public IP used by the frontend Load Balancer (LBR, OTD, etc.) in the site that has the primary role. So, at the end of each switchover, it is required to perform a DNS push or alter the file host resolution to point that address to the public IP used by LBR in the new primary site.

*NOTE: The name resolution does not change for mid-tier hosts: they always point to its own LBR. The change must be effective for application clients.*

You can use the Site Guard to run a custom script that performs a change in the /etc/hosts file or push a change in the DNS server. The host or hosts where the script will run must be discovered in the Enterprise Manager and added as auxiliary hosts to the systems.

As an example in this document, the EM host (i.e.: emcc.marketplace.com) will run scripts that perform frontend name IP changes in its own /etc/host file, so it is added as auxiliary host to the sites:

```
[oracle@emcc bin]$ ./emcli add_siteguard_aux_hosts -system_name="SITE1_wlsdr" -host_name="emcc.marketplace.com"
Auxiliary host(s) added to system SITE1_wlsdr

[oracle@emcc bin]$ ./emcli add_siteguard_aux_hosts -system_name="SITE2_wlsdr" -host_name="emcc.marketplace.com"
Auxiliary host(s) added to system SITE2_wlsdr
```

## 6. 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:

a) Login to Enterprise Manager
b) From the Targets menu, click **Systems**
c) On the Systems page, click the name of the system for which you want to configure credential associations.
d) On the system's home page, from the Generic System menu, **select Site Guard > Configure**.
e) Click the **Credentials** tab. Now associate the different types of credentials
f) **Normal Host Credentials** section, click **Add**, select **All** and check **Preferred > Normal Host Credentials**. Click Save.
g) **Privileged Host Credentials** are not required for the WLS and DB hosts, because Site Guard scripts are executed with oracle user. However, privileged credential may be required for auxiliary hosts that run scripts with root user (example, to update the /etc/hosts file). If this is the case, add the privileged host credential to that auxiliary host (EM host is used as an example auxiliary host in this approach).
h) **Oracle Node Manager Credentials** section, click Add, select **All** and **NAMED**. Select the NodeManager credential created before. Example: WLSDR_DOMAIN_NODEM. Click Save
i) **WebLogic Administration Credentials** section, click Add, select **All** and **Preferred**. Click Save
j) **SYSDBA Database Credentials** section, click Add, select **All** and **Preferred, "SYSDBA Database Credentials"**. Click Save

Repeat the same for the standby system.

## 7. Configuring required scripts

Oracle Site Guard provides a mechanism for you to configure scripts for managing disaster recovery operations. Different kind of scripts can be defined for Site Guard:

| SITEGUARD SCRIPTS | DETAILS |
|---|---|
| **PreCheck, Mount and unmount or Storage** | Not required for WLS and SOA Paas DR |
| **Pre Scripts** | The scripts that perform the WLS Domain config synchronization can be run as pre scripts.<br>Example:<br>/u01/install/config_replica.sh in mid-tier host 1 of Site1, run as oracle.<br>/u01/install/config_replica.sh in mid-tier host 1 of Site2, run as oracle.<br><br>(also named "dbfscopy.sh in previous versions) |
| **Post Scripts** | Following scripts will run as post scripts in this example:<br>• **Post script that update the frontend virtual hostname IP in the /etc/hosts** of a host after a switchover/failover. This would change the frontend ip in the host where the script runs, which in this example this will run in the EM host. Example:<br><br>/root/scripts/change_frontend_ip_from_SITE1_to_SITE2.sh[7]<br>/root/scripts/change_frontend_ip_from_SITE2_to_SITE1.sh<br>• **Post script that update the frontend virtual hostname IP in DNS** after a switchover/failover. For scenarios where DNS is used for the external frontend resolution (Oracle Cloud DNS, commercial DNS, etc.) appropriate API can be used to push the change. An example that push this change in an Oracle Cloud DNS can be found here.<br>• **Post script to check am App url** after the complete switchover/failover, to verify that the switchover has been successful. Sample script can be found in:<br>check-sample-url.zip for WLS (sample-app url)<br>check-soainfra.zip for SOA (soa-infra url) |

To configure the Pre-Scripts for Paas DR:

a) Login in EM, and go to Targets > Systems
b) Click the System where you want to configure the scripts
c) Click Site Guard > Configure > Pre/Post scripts tab
d) Add **Pre Scripts** to **Site1** system:
   - Insert the Script Path to the script that makes the WLS config replica.
     Example: /u01/install/config_replica.sh (or /u01/install/dbfscopy.sh)
   - Select Script Type: Global-PreScript
   - Select Operation: Switchover
   - Select as targets the Site1 midtier host1 and the Site2 midtier host1 (which is an aux host for this site).
   - Select the normal preferred credentials for the hosts.

*NOTE: By default the dbfscopy.sh prompts for the sysdba password. Customer can customize it to take the password as an argument in order to be executed from Oracle Site Guard. Comment the lines that prompt for the password and define the password variable with its value directly in the script (use double quotes for the value).*

e) Add **Pre Scripts** to **Site2** system:
   - Insert the path to the script that makes the WLS config replica.
     Example: /u01/install/config_replica.sh (or /u01/install/dbfscopy.sh)

[7] Sample script change_frontend_ip_from_SITE1_to_SITE2.sh:

```
# Script to change /etc/hosts file entry mywebapp.mycompany.com ip (entry must exist in the /etc/host file)
# from SITE1 LBR IP: 111.111.111.10
# to SITE2 LBR IP: 222.222.222.20
sed -i 's/111.111.111.10/222.222.222.20/g' /etc/hosts
```

- Select Script Type: Global-PreScript
- Select Operation: Switchover
- Select Role: Primary
- Select as targets the Site2 mid-tier host1 and the Site 1 mid-tier host1 (which is an aux host for this site).
- Select the normal preferred credentials for the hosts.

To configure the Post-Scripts for Paas DR:

a) Add **Post Scripts** to **Site1** system, to be executed **post the switchover from Site2 to Site1**:
   - Insert the path to the script that changes the dns **name to the Site 1 LBR public IP.** Example: /root/scripts/change_frontend_ip_from_SITE2_to_SITE1.sh
   - Select **Script Type**: Global-PostScript (it will be executed at the end of the operation plan when switching to Site1)
   - Select **Operation**: Switchover
   - Select the aux host where host file is updated, **OMS host in this case**.
   - In Advanced, select the **privileged** preferred credential for the host (only root can modify hosts file).

b) To create the same post script for the failover operation from Site2 to Site1.
   - Select the post script created in previous step and click on "Add Like"
   - Change operation to "Failover"
   - Click Save

c) Add **Post Scripts** to **Site2** system, to be executed post the switchover from Site1 to Site2:
   - Insert the path to the script that changes the name to the Site2 LBR public IP. Example: /root/scripts/change_frontend_ip_from_SITE1_to_SITE2.sh
   - Select **Script Type:** Global-PostScript (it will be executed at the end of the operation plan when switching to Site2)
   - Select **Operation**: Switchover.
   - Select the aux host where host file is updated, **OMS host in this case**.
   - Select the **privileged** preferred credential for the host (only root can modify hosts file)

d) To create the same post script for the failover from Site1 to Site2.
   - Select the post script created in previous step and click on "Add Like"
   - Change operation to "Failover"
   - Click Save

e) Repeat to add any other post-script (for example, the sample app url verification script).

## 8. Configuring apply and transport lag thresholds

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. 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=SITE1_wlsdr -property_name=apply_lag -value=10
[oracle@emcc]$ ./emcli configure_siteguard_lag -system_name=SITE2_wlsdr -property_name=apply_lag -value=10

[oracle@emcc]$ ./emcli configure_siteguard_lag -system_name=SITE1_wlsdr -property_name=transport_lag -value=10
[oracle@emcc]$ ./emcli configure_siteguard_lag -system_name=SITE2_wlsdr -property_name=transport_lag -value=10
```

## 9. 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 PaaS DR:

| PLAN | DESCRIPTION |
|---|---|

| | |
|---|---|
| **SWITCHOVER_SITE1_TO_SITE2_WITH_SYNC** | Switchover from Site1 to Site2, that also performs a WLS config synchronization based on the WLS domain config replica script (*config_replica.sh* or *dbfscopy.sh).* |
| **SWITCHOVER_SITE2_TO_SITE1_WITH_SYNC** | Switchover from Site2 to Site1, that also performs a WLS config synchronization based on the WLS domain config replica script (*config_replica.sh* or *dbfscopy.sh).* |
| **SWITCHOVER_SITE1_TO_SITE2** | Switchover from Site1 to Site2, without WLS domain config sync (RTO is reduced) |
| **SWITCHOVER_SITE2_TO_SITE1** | Switchover from Site1 to Site2, without WLS domain config sync (RTO is reduced) |
| **FAILOVER_SITE1_TO_SITE2** | Failover from Site1 to Site2. No WLS domain config synchronization is performed, as a failover is an unplanned event when the primary site becomes unavailable. |
| **FAILOVER_SITE2_TO_SITE1** | Failover from Site2 to Site1. No WLS domain config synchronization is performed, as a failover is an unplanned event when the primary site becomes unavailable. |

#### *a)* Create SWITCHOVER_SITE1_TO_SITE2_WITH_SYNC

Operation plan for performing a switchover from SITE to SITE 2, that performs a WLS Domain config synchronization before the switchover.

- Login in EM, go to Target > Systems
- Click in Site1 System > Go to Site Guard > Operations.
- Click **Create**.
- Enter a name for the plan. Example: SWITCHOVER_SITE1_TO_SITE2_WITH_SYNC
- Select Operation Type: **Switchover**
- Select the other site (Site2) as the standby system
- Click **Save**
- The default created **plan needs to be customized**. **Edit** the plan and:
- IMPORTANT: Verify that **WLS config sync pre-scripts are run in Serial mode** (by default they run in parallel)
- IMPORTANT: verify that the **first** execution of the pre-script is in the Site that **is the original primary in this plan**. For example, when the plan is defined to switchover from Site1 to Site2, the first execution of the config_replica.sh (or *dbfscopy.sh)* must run in Site1 mid-tier host1. Move down/up if needed.
- **Disable node manager stop/start steps**. They are not required and skipping them reduces the RTO.

*NOTE: It is recommended to disable non-required start/stop steps related with components instead of deleting them. Topology Prechecks can fail when running the plan and warning "This operation plan is out of sync with current topology of the system." when the start/stop steps are deleted for some components in the system. However, there are no warnings when the start/stop steps are disabled.*[8]

- Verify that the post-script that checks the sample app url test is done after the dns or hosts file update.
- Verify that all the required steps are included and there is no step missing.
- Save the changes of the operation plan

#### b) Create SWITCHOVER_SITE2_TO_SITE1_WITH_SYNC

Follow the same steps than in the previous but in Site2 system.

Select the Site1 as the standby and verify that the pre-script *dbfscopy.sh/config_replica.sh* runs first in Site2 mid-tier host1.

#### c) Create SWITCHOVER_SITE1_TO_SITE2

8 Bug 29005772 - TOPOLOGY PRECHECKS FAIL IN SG RUN PRECHECKS WHEN SOME COMPONENT START/STOP STEPS ARE DELETED

Select the plan SWITCHOVER_SITE1_TO_SITE2_WITH_SYNC and click in “Create like”

Edit it and **delete** the Global Pre-scripts steps to skip *dbfscopy.sh/config_replica.sh* script executions.

**d) Create SWITCHOVER_SITE2_TO_SITE1**

Select SWITCHOVER_SITE2_TO_SITE1_WITH_SYNC and click in “Create like”

Edit it and **delete** the Global Pre-scripts steps to skip *dbfscopy.sh/config_replica.sh* script executions.

**e) Create FAILOVER_SITE1_TO_SITE2**

Operation plan for performing a failover from SITE1 to SITE 2. No WLS domain config synchronization is performed, because a failover is an unplanned event when the primary site becomes unavailable.

- Login in EM, go to Target > Systems
- Click in Site1 System > Go to Site Guard > Operations.
- Click Create.
- Enter a name for the plan. Example: FAILOVER_SITE1_TO_SITE2
- Select Operation Type: Failover
- Select the other site (Site2) as the standby system
- Click Save
- Select the created plan and click “Edit”. The created plan needs to be customized:
- Verify that pre-scripts for *dbfscopy.sh orconfig_replica.sh* have NOT been included in the plan.
- Disable node manager start steps. They are not required and skipping them reduces the RTO.
- Verify that the post-scripts are included in the correct order and reorder if needed (sample app check must be the last one)
- Save the changes.

**f) Create FAILOVER_SITE2_TO_SITE1**

Follow the same steps than in the previous but in Site2 system. Select the Site1 as the standby.

*NOTE: These operation plans are valid also for cases where the AdminServer is already started in the standby. The status of the Admin is checked before trying to start it and skipped the start if it is already RUNNING.*

# PERFORMING A SWITCHOVER WITH SITE GUARD

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

a) Login in EM, 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.
- It executes the pre-scripts: if the plan includes the dbfscopy.sh as defined in the previous section, it will run dbfscopy.sh in the WLS host1 of the primary site and then it will run dbfscopy.sh in the WLS host1 of the standby site to synchronize the WebLogic domain configuration.
- The WebLogic domain in the primary Site will be shutdown: first the WebLogic managed servers (in parallel) and then the WebLogic Administration Server.
- Oracle Site Guard performs the database switchover from primary database to standby database using Data Guard broker.
- Once the database switchover is done, the WebLogic domain in the standby Site is started: first the WebLogic Administration Server and then the WebLogic managed servers (in parallel).
- Any defined post-scripts will be run: to change the frontend resolution or to verify the application url status.
- 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 OMS 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 OMS Console or EMCLI. Site Guard will orchestrate the steps for the Paas 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. The script *dbfscopy.sh/config_replica.sh* is not defined for failover operations. A failover is an unplanned event that happens when the primary site becomes unavailable so configuration synchronization is not expected.
- During failover, the shutdown of the WebLogic domain in the primary Site is skipped by default, although it can be enabled manually if required).
- Oracle Site Guard performs the database failover from primary database to standby database using Data Guard broker.
- Once the database failover is completed, the WebLogic domain in the standby Site is started: first the WebLogic Administration Server and then the WebLogic managed servers in parallel.
- The post-scripts are executed to change the frontend resolution or to verify the sample app url status.
- 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 Paas DR systems like WebLogic for OCI, SOA Cloud Service or SOA Market Place. 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 radically 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 particual steps that are specific to their envornment.

## 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



WebLogic Cloud on Market Place Disaster Recovery
March, 2021