Oracle® Site Guard
Administrator's Guide

13c Release 4
F32444-01
June 2020

Oracle Site Guard Administrator's Guide, 13c Release 4

F32444-01

Copyright © 2020, 2020, Oracle and/or its affiliates.

Primary Author: Oracle Corporation

Contributors: Enterprise Manager Cloud Control Development Teams, Quality Assurance Teams, Customer Support Teams, and Product Management Teams.

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

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

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

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or “commercial computer software documentation” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government’s use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

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

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

Intel and Intel Inside 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, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

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

Contents

Preface

Audience xi
Documentation Accessibility xi
Related Documents xi
Conventions xii

1 Introduction to Oracle Site Guard

What is Oracle Site Guard 1-1
Benefits of Oracle Site Guard 1-1
What's New in this Guide 1-2
- What's New in Release 13.3.1.0.0 1-2
- What’s New in Release 13.2.2.0.0 1-2
- What’s New in Release 13.2.0.1.0 1-2
- What's New in Release 13.1.1.0.0 1-3

2 Introduction to Oracle Site Guard

Representation of a Site in Enterprise Manager Cloud Control Console 2-1
Oracle Site Guard Features 2-3
- Extensibility 2-3
  - Types of Scripts for Extensibility 2-3
  - Sequence of Script Execution 2-5
  - Configuring Script Paths 2-7
- Prechecks and Health Checks 2-9
  - Prechecks 2-9
  - Health Checks 2-9
  - Customizing Prechecks and Health Checks 2-10
  - Lag Checks 2-10
- Storage Integration 2-11
  - Oracle Sun ZFS 2-11
  - NetApp MetroCluster 2-11
  - Integrating Other Storage Types 2-12

Mount and Unmount Scripts 2-12
Standby Site Validation 2-12
Creating Execution Groups 2-13
Monitoring Executions and Managing Errors 2-14
Customizing Operations 2-14
Monitoring Executions 2-15
Operation Error Modes 2-15
Retrying Failed Operations 2-16
Suspending and Resuming Operations 2-16
Credential Management 2-16
Oracle Enterprise Manager Credential Management Framework 2-16
Oracle Site Guard Credential Configuration 2-16
Role-Based Access Control 2-17
Software Library Integration 2-17
Custom Credentials for Script Execution 2-17
Passing Credentials as Script Parameters 2-18
Oracle Site Guard Workflows 2-18
Switchover Workflow 2-19
Failover Workflow 2-20
Start Workflow 2-21
Stop Workflow 2-22
Open for Validation Workflow 2-22
Revert to Standby Workflow 2-23

3 Installing and Preparing Oracle Site Guard

Installing Oracle Site Guard 3-1
Preparing Oracle Site Guard for Operation 3-2
Discovering Targets on the Primary and the Standby Sites 3-2
Creating Oracle Site Guard Administrator Users 3-2
Creating an Oracle Site Guard Administrator User with Enterprise Manager Cloud Control Console 3-3
Creating an Oracle Site Guard Administrator User with Enterprise Manager Command-Line Interface 3-4
Creating Primary and Standby Sites 3-4
Creating a Generic System with Enterprise Manager Cloud Control Console 3-4
Creating a Generic System with Enterprise Manager Command-Line Interface 3-5
Creating Credentials 3-6
Creating Named Credentials 3-7
Creating Preferred Credentials 3-9
Granting Credential Privileges to Oracle Site Guard Administrator Users 3-10

Granting Credential Privileges with Enterprise Manager Cloud Control Console 3-11
Configuring Software Library Storage Location 3-11
Configuring Software Library Storage Location with Enterprise Manager Cloud Control Console 3-11
Configuring Software Library Storage Location with Enterprise Manager Command-Line Interface 3-12
Verifying Database and Data Guard Configurations 3-13

4 Configuring Oracle Site Guard

Overview 4-1
Configuring Sites 4-2
Configuring Sites with Enterprise Manager Cloud Control Console 4-2
Configuring Sites with EMCLI Commands 4-3
Configuring Site Properties with EMCLI Commands 4-3
Updating Site Configuration 4-4
Updating Site Configuration with Enterprise Manager Cloud Control Console 4-4
Updating Site Configuration with EMCLI Commands 4-5
Creating Credential Associations 4-6
Creating Named or Preferred Credential Associations 4-6
Creating Named or Preferred Credential Associations with Enterprise Manager Cloud Control Console 4-7
Creating Named or Preferred Credential Associations with EMCLI Commands 4-8
Configuring Scripts 4-9
Configuring Custom Precheck Scripts, Pre Scripts, Post Scripts, Global Pre Scripts, and Global Post Scripts 4-10
Configuring Custom Precheck Scripts, Pre Scripts, Post Scripts, Global Pre Scripts, and Global Post Scripts with Enterprise Manager Cloud Control Console 4-11
Configuring Custom Precheck Scripts, Pre Scripts, Post Scripts, Global Pre Scripts, and Global Post Scripts with EMCLI Commands 4-13
Configuring Mount and Unmount Scripts 4-15
mount_umount.sh 4-16
Configuring Storage Scripts 4-21
zfs_storage_role_reversal.sh 4-22
Configuring Storage Scripts with Enterprise Manager Cloud Control Console 4-25
Configuring Storage Scripts with EMCLI Commands 4-27
Configuring Credentials as Parameters for Scripts 4-29
Adding Credential Parameters to a Script 4-29
Deleting Credential Parameters with a Script 4-30
Getting Credential Parameters for a Script 4-30
Cloning a Script with Existing Scripts 4-31

Configuring Auxiliary Hosts 4-31
Adding an Auxiliary Host with EMCLI Commands 4-32
Deleting an Auxiliary Host with EMCLI Commands 4-32
Listing Auxiliary Targets with EMCLI Commands 4-33
Configuring Database Lag Checks with EMCLI Commands 4-33
Configuring Database Lag Checks with EMCLI Commands 4-34
Updating Threshold Value for Database Lag with EMCLI Commands 4-34
Deleting Threshold Value for Database Lag with EMCLI Commands 4-35
Listing Database Lag Thresholds with EMCLI Commands 4-35

5 Performing Oracle Site Guard Operations

Overview 5-1
Managing Operation Plans 5-2
Creating Operation Plans 5-2
Creating an Operation Plan with Enterprise Manager Cloud Control Console 5-3
Creating an Operation Plan with EMCLI Commands 5-4
Creating New Operation Plans with Existing Plans 5-5
Editing and Updating Operation Plans 5-5
Editing and Updating Operation Plans with Enterprise Manager Cloud Control Console 5-6
Editing and Updating Operation Plans with EMCLI Commands 5-7
Adding and Deleting Operation Plan Tags with EMCLI Commands 5-9
Deleting an Operation Plan 5-9
Deleting an Operation Plan with Enterprise Manager Cloud Control Console 5-10
Deleting an Operation Plan with EMCLI Commands 5-10
Running Prechecks 5-11
Running Precheck Utility with Enterprise Manager Cloud Control Console 5-11
Running Precheck Utility with EMCLI Commands 5-12
Scheduling and Stopping Health Checks 5-12
Scheduling a Health Check with Enterprise Manager Cloud Control Console 5-13
Scheduling a Health Check with EMCLI Commands 5-13
Stopping a Health Check with Enterprise Manager Cloud Control Console 5-16
Stopping a Health Check with EMCLI Commands 5-16
Executing Oracle Site Guard Operation Plans 5-17
Executing Oracle Site Guard Operation Plan with Enterprise Manager Cloud Control Console 5-17
Executing Oracle Site Guard Operation Plan with EMCLI Command 5-18
Monitoring Oracle Site Guard Operations 5-18
Monitoring an Operation Plan with Enterprise Manager Cloud Control Console 5-19
Viewing an Operation Activity 5-19
Suspending, Resuming, or Stopping an Operation 5-21

Monitoring an Operation Plan with EMCLI Commands 5-21
Managing Execution Errors 5-22
Manually Reversing Site Roles 5-23
Manually Reversing Site Roles with Enterprise Manager Cloud Control Console 5-24
Manually Reversing Site Roles with EMCLI Commands 5-24

6 Troubleshooting Oracle Site Guard

Operation Plan Issues 6-1
Targets Not Discovered in Operation Plan Workflow 6-1
Oracle WebLogic Server Managed Server Target Not Identified 6-2
Manual Intervention Needed for Hung Operation Step 6-2
OPMN Managed System Components Not Discovered In Operation-Plan Workflow 6-3
Oracle RAC Database Not Discovered in Operation Plan 6-3
Operation Step Failure When Target is Accessed with Sudo Privileges 6-3
Error While Creating Operation Plan Indicating Credential Association Not Configured 6-4
Inability to Associate Credentials for Targets Added to a Site 6-4
Error While Deleting Or Updating Operation Plans 6-4
Error Indicating Inability to Create Scalar Value While Creating Operation Plan 6-5
Error While Creating Operation Plan Indicating Missing Node Manager Credentials 6-5
Error Indicating Inability to Stage SWLIB Artifacts Due To Insufficient Disk Space on Target Host 6-6
Operation Plan Fails Because of Inability to Copy WLS Utility Script to Domain Directory 6-6
Switchover and Failover Operation Issues 6-7
Oracle WebLogic Administration Server Not Starting After Switchover or Failover Operation 6-7
Oracle WebLogic Administration Server not Restarting After Switchover or Failover Operation 6-8
Host Not Available During Switchover or Failover Operation 6-8
Switchover or Failover Operation Fails When Oracle RAC Database Not Available 6-8
Precheck and Healthcheck Issues 6-9
Prechecks Failures 6-9
Prechecks Hang When Oracle Management Agent Is Not Available 6-9
Healthchecks Can Not Be Retried or Resumed 6-9
Oracle WebLogic Server Issues 6-10
Node Manager Fails to Restart 6-10
Node Manager Start/Stop Fails Due to Missing Properties File 6-11
Oracle WebLogic Server Managed Server Fails to Start 6-11

Oracle Site Guard Does Not Include Oracle WebLogic Server Instances That Are Migrated to a Different Host 6-11
Error While Creating Operation Plan 6-12
Oracle Site Guard Fails To Access Node Manager 6-12
Unable to Associate Distinct Credentials for Node Manager 6-13
Oracle WebLogic Server Password Updates and Site Guard Credentials 6-13
Oracle Enterprise Manager Cannot Manage Domain Components 6-13
Database Issues 6-14
Prechecks for Database Switchover and Failover Operations Fail 6-14
Databases Protected by Data Guard Included in the Incorrect Operation Plan Category 6-14
Database Inaccessible When Opening a Site for Standby Validation 6-15
Open For Validation plan operation fails with ORA-16692 error 6-15
Storage Issues 6-15
ZFS Storage Appliance Log in Failure 6-16
Storage Role Reversal Operation Failure 6-16
Storage Role Reversal Operation Failure 6-16
ZFS Storage Role Reversal Fails During Operation Plan Execution 6-17
Remote Replication Targets List Multiple Appliances With The Same Name 6-17
ZFS Storage Role Reversal Failure 6-17

7 Oracle Site Guard Command Line Interface

add_operation_plan_tags 7-1
add_site_properties 7-2
add_siteguard_aux_hosts 7-2
add_siteguard_script_credential_params 7-3
add_siteguard_script_hosts 7-4
configure_siteguard_lag 7-4
create_operation_plan 7-5
create_siteguard_configuration 7-6
create_siteguard_credential_association 7-7
create_siteguard_script 7-8
delete_operation_plan 7-11
delete_operation_plan_tags 7-11
delete_site_properties 7-12
delete_siteguard_aux_host 7-12
delete_siteguard_configuration 7-13
delete_siteguard_credential_association 7-14
delete_siteguard_lag 7-15
delete_siteguard_script 7-16
delete_siteguard_script_credential_params 7-16

delete_siteguard_script_hosts 7-17
get_operation_plan_details 7-18
get_operation_plans 7-18
get_site_properties 7-19
get_siteguard_aux_hosts 7-20
get_siteguard_configuration 7-21
get_siteguard_credential_association 7-21
get_siteguard_health_checks 7-22
get_siteguard_lag 7-23
get_siteguard_script_credential_params 7-24
get_siteguard_script_hosts 7-24
get_siteguard_scripts 7-25
get_siteguard_supported_targets 7-26
run_prechecks 7-26
schedule_siteguard_health_checks 7-27
stop_siteguard_health_checks 7-29
submit_operation_plan 7-29
update_operation_plan 7-31
update_site_properties 7-32
update_siteguard_configuration 7-32
update_siteguard_credential_association 7-34
update_siteguard_lag 7-35
update_siteguard_script 7-36

8 Upgrading or Downgrading Oracle Site Guard

Upgrading Oracle Site Guard 8-1
Downgrading Oracle Site Guard 8-2

A Passing Credentials as Parameters

Passing Credentials as Parameters A-1
extract_credentials_sample_script.sh A-1
extract_credentials_sample_script.py A-2
extract_credentials_sample_script.pl A-4

B Bundled Scripts

Bundled Scripts B-1
Oracle Virtual Machine (OVM) DR Script — siteguard_ovm_control.py B-1
WebLogic Server Control Script – wls_control_wrapper.pl B-6
Node Manager Control Script – nm_control_wrapper.pl B-8

Database Control Script - db_control_wrapper.pl B-10
ZFS Storage Script - zfs_storage_role_reversal.sh B-11
ZFS Analysis Script - zfs_analysis.sh B-12

C Oracle Site Guard Terminology

Preface

The Oracle Site Guard guide introduces you to the Oracle Fusion Middleware Disaster Recovery solution offered by Oracle Enterprise Manager Cloud Control (Cloud Control), and describes in detail how you can use the product to manage sites to manage your data center.

Audience

This guide is primarily meant for administrators who want to use Oracle Site Guard features offered by Cloud Control to meet their Oracle Fusion Middleware disaster-recovery needs. As an administrator, you can either be a Designer, who performs the role of a system administrator and does critical data center operations, or an Operator, who runs the default as well as custom deployment procedures, patch plans, and patch templates to manage the enterprise configuration.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For more information, see the following documents:

- *Oracle Fusion Middleware Disaster Recovery Guide*
- *Oracle Fusion Middleware High Availability Guide*
- *Automating Disaster Recovery Using Oracle Site Guard for Oracle Exalogic*
- *Oracle Enterprise Manager Lifecycle Management Administrator's Guide*
- *Oracle Enterprise Manager Command Line Interface Guide*
- *Oracle VM 3: Getting Started with Disaster Recovery*

Conventions

The following text conventions are used in this document:

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

1

Introduction to Oracle Site Guard

In this section, you learn about Oracle Site Guard and its benefits.

This chapter includes the following sections:

- Representation of a Site in Enterprise Manager Cloud Control Console
- Oracle Site Guard Features
- Oracle Site Guard Workflows

What is Oracle Site Guard

Oracle Site Guard is a disaster recovery solution that enables administrators to automate complete site switchover and failover.

Oracle Site Guard 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 Guard integrates with underlying replication mechanisms that synchronize primary and standby environments and protect mission critical data. It comes with a built-in support for Oracle Data Guard for Oracle database, and Oracle Sun ZFS. Oracle Site Guard can also support other storage replication technologies.

Benefits of Oracle Site Guard

In this section, you learn about the benefits of the Oracle Site Guard.

Oracle Site Guard offers the following benefits:

- Minimizes disaster recovery time

  Oracle Site Guard operates at the site level, and therefore eliminates the need to tediously perform manual disaster recovery for individual site components like applications, middleware, databases, and so on. The traffic of an entire production site can be redirected to a standby site in a single operation.

- Reduces human errors

  Disaster recovery involves a complicated orchestration of many precise, interdependent procedures. Oracle Site Guard automates and sequences these procedures to provide fast and seamless disaster recovery operations across sites without any human interaction.

- Flexible and customizable

  Oracle Site Guard can be adapted for use in any enterprise deployment by customizing and tuning disaster recovery plans. Oracle Site Guard provides mechanisms for customizing operations and handling errors.

- Eliminates the need for special skills

Oracle Site Guard operators and administrators do not require any special skills or domain expertise in areas like databases, applications, and storage replication. Oracle Site Guard can continuously monitor disaster recovery readiness and it can do this without disrupting the production site.

What's New in this Guide

In this section, you learn about Oracle Guard Site features introduced in this and previous releases.

The following sections describe the main features introduced in 13.3.1.0.0 and previous Oracle Site Guard releases:

- What's New in Release 13.3.1.0.0
- **What's New in Release 13.2.2.0.0**
- What's New in Release 13.2.0.1.0
- What's New in Release 13.1.1.0.0

What's New in Release 13.3.1.0.0

The following new features are available with Oracle Site Guard release 13.3.1.0.0:

- Database Disaster Recovery Enhancements

  Option to configure Database Failover to ignore non-fatal Data Guard warnings

- Create Site Properties

  Create user-defined name/value pairs to associate with one or more Site Guard sites. Site Properties provide a method to filter out and identify a subset of Site Guard sites. Site Properties is an EMCLI-only feature

- ZFS Disaster Recovery Enhancements

  It is no longer required to specify a ZFS lag value during Site Guard configuration storage script creation.

What's New in Release 13.2.2.0.0

The following new features are available with Oracle Site Guard release 13.2.2.0.0:

- Oracle Virtual Machine CLI (OVMCLI) DR Script (siteguard_ovmcli_control.py) for performing disaster recovery for OVM 3.2 environments, such as Oracle Private Cloud Appliance (PCA).
- Site Guard ZFS utility script (sg_zfs_utility.sh) for cleaning up and reconfiguring ZFS replication in a multi-site DR configuration.
- Get Site Guard Health Check reports using the new EMCLI command "get_siteguard_health_check_report".
- Filter health check notifications so that you are only notified when problems occur.

What's New in Release 13.2.0.1.0

The following new features are available with Oracle Site Guard release 13.2.0.1.0:

- Oracle Virtual Machine (OVM) DR Script – siteguard_ovm_control.py

- WebLogic Server Control Script – wls_control_wrapper.pl

What's New in Release 13.1.1.0.0

The following new features are available with Oracle Site Guard release 13.1.1.0:

- Standby Site Validation

  Convert your Standby site to a fully functional site in order to validate and test the site in preparation for a disaster recovery event. Increase your confidence in your disaster recovery plans and procedures.

- Create Execution Groups

  Create execution groups to customize the sequence in which you want to handle targets in your operation plan. Execution groups contain targets which are handled in parallel within the group. Use this feature to orchestrate the parallel and serial aspects of your disaster recovery plan.

- Customize Step-level Timeouts for Operation Plans

  Customize the timeout for each step in an operation plan based on the needs of your DR environment.

- Database Disaster Recovery Enhancements
  - Enable diagnostic tracing at the Data Guard level for database switchover and failover.
  - Configure immediate failover of databases at the Data Guard level.
  - Ignore warnings and force a database failover.

- Support for Multi-Tenant Databases

  Protect multi-tenant databases in your enterprise.

- ZFS Disaster Recovery Enhancements

  Configure ZFS disaster recovery to use ZFS public or singleton interfaces instead of private interfaces. Leverage ZFS clustering to provide a more resilient disaster recovery plan.

- Detect and Analyze ZFS Replication Lags

  Use bundled scripts to analyze lags in ZFS replication configurations before and during execution of disaster recovery plans.

- Assign Tags to Operation Plans

  Assign one or more tags to operation plans and use combinations of these tags to filter and display your operation plans. Use this feature to search, organize, and catalog, your operation plans.

- Invoke Database and Storage Disaster Recovery Scripts During Any Phase of Operation

  Customize your operation plan by invoking database and storage disaster recovery scripts during the Pre or Post phases of your plan.

- Support for NetApp MetroCluster Storage Deployments

  For details, see MOS note in *Oracle Site Guard Feature For NetApp MetroCluster (Doc ID 1964220) at https://support.oracle.com*.

2

Introduction to Oracle Site Guard

In this section, you learn about Oracle Site Guard and its benefits.

This chapter includes the following sections:

- Representation of a Site in Enterprise Manager Cloud Control Console
- Oracle Site Guard Features
- Oracle Site Guard Workflows

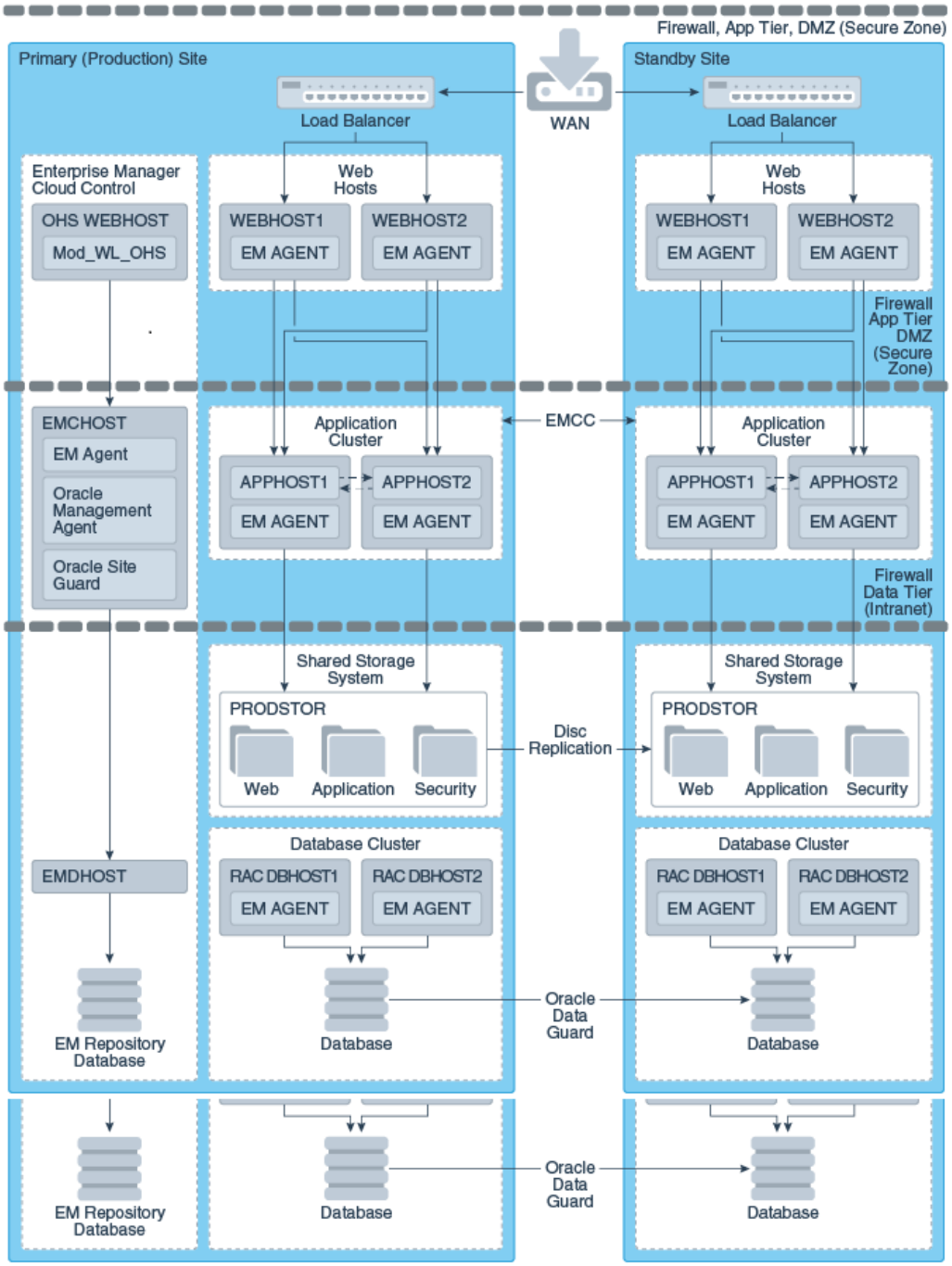
Representation of a Site in Enterprise Manager Cloud Control Console

A site is a logical grouping of software components and associated hardware that run one or more user applications.

A site could consist, for example, of a collection of servers (hosts) that are used to deploy Oracle Fusion Middleware instances, Oracle Fusion Application instances, Oracle databases, along with the associated storage for these software components. Oracle Site Guard uses the Enterprise Manager Cloud Control generic system target to represent a site. Every site, whether primary or standby, is represented as a **Generic System**, which is a collection of other target types, such as Oracle Database and Oracle Fusion Middleware Domain. Oracle Site Guard only supports Enterprise Manager deployments where both primary and standby sites are managed by the same Enterprise Manager Cloud Control deployment.

The following picture illustrates the main portions of an Oracle Fusion Middleware Disaster Recovery topology managed by the same Enterprise Manager Cloud Control deployment.

Figure 2-1 Primary (Production) and Standby Site for Oracle Fusion Middleware Disaster Recovery Topology Managed by Enterprise Manager Cloud Control



The main aspects of an Oracle Fusion Middleware Disaster Recovery topology are as follows:

- A single Enterprise Manager Cloud Control monitors the primary site and the standby site.

- Oracle Management Agent (EM Agent) is installed on local (non-replicated) storage on all hosts on the primary site and the standby site.

  For example:

  – Web Tier managed system components (`WEBHOST1` and `WEBHOST2`)

  – Oracle Fusion Middleware Applications (`APPHOST1` and `APPHOST2`)

  – Oracle RAC Database (`RAC DBHOST1` and `RAC DBHOST2`)

  Oracle Management Agent (EM Agent) is one of the core components of Enterprise Manager Cloud Control that enables you to convert an unmanaged host to a managed host in the Enterprise Manager system. The Management Agent works in conjunction with Enterprise Manager plug-ins to manage the targets running on that managed host.

Oracle Site Guard Features

Oracle Site Guard offerings include extensibility, storage integration, monitoring execution, and credentials managing.

Oracle Site Guard main features include the following:

Extensibility

Oracle Site Guard allows extending the built-in disaster recovery functionality by allowing you to insert custom scripts at specific points in the operation workflow.

Extensibility provides a mechanism to perform customized, site-specific, and operation-specific activities during a disaster recovery operation.

Any number of scripts can be configured for extensibility. The time and manner in which these user-defined scripts are executed and the sequence in which they are executed can be configured by selecting the script type.

This section contains the following topics:

Types of Scripts for Extensibility

Oracle Site Guard offers several kind of scripts with which you can extend its functionality.

To customize and extend Oracle Site Guard functionality, use any of the following scripts:

- **Custom Precheck Scripts**
- **Pre Scripts**
- **Post Scripts**
- **Global Pre Scripts**
- **Global Post Scripts**
- **Mount/Unmount Scripts**
- **Storage Scripts**

Custom Precheck Scripts

These scripts are provided by the user. They are used to perform user-defined activities during the Precheck or Health Check phase that occurs before an operation plan executes. Custom Precheck Scripts are executed as part of a Precheck or Health Check.

Pre Scripts

These scripts are provided by the user. They are used to perform user-defined activities at the beginning of site-specific operations in an operation plan. Pre Scripts are executed before Oracle Site Guard performs any target-related operations at a site.

Post Scripts

These scripts are provided by the user. They are used to perform user-defined activities at the end of site-specific operations in an operation plan. Post scripts are executed after Oracle Site Guard performs any target-related operation at a site.

Global Pre Scripts

These scripts are provided by the user. They are used to perform user-defined operation-specific activities at the beginning of an operation plan. Global Pre Scripts are executed before Oracle Site Guard begins any operation at the first site (usually the primary site).

Global Post Scripts

These scripts are provided by the user. They are used to perform user-defined operation-specific activities at the end of an operation plan. Global Post Scripts are executed after Oracle Site Guard has completed performing operations on the last site (usually a standby site).

Mount/Unmount Scripts

These scripts are bundled with Oracle Site Guard, but you can also define your own scripts. They are used to perform mount and un-mount operations on file systems during an operation. Unmount scripts are executed after all services and applications have been stopped at the primary site. Mount scripts are executed before any services or applications are started at the standby site.

Storage Scripts

These scripts are bundled with Oracle Site Guard, but you can also define your own storage scripts. They are used to perform storage role-reversal activities for Oracle Sun ZFS Appliance during a disaster-recovery operation. Storage Switchover scripts are executed during a switchover operation and they execute at the standby site before any mount scripts are executed. Storage Failover scripts are executed during a failover operation and they execute at the standby site before any mount scripts are executed.

Table 2-1 provides an overview of the various types of scripts used when you set up sites with Oracle Site Guard.

Figure 2-2 and Figure 2-3 provide a visual representation of the source of the scripts and their functions.

Table 2-1 Types of Scripts Used by Oracle Site Guard

Type of Script	Provided by the User? (Custom Scripts)	Provided with Oracle Site Guard? (Bundled Scripts)
Custom Precheck Script	Yes (optional)	No
Pre Script, Post Script, Global Pre Script, Global Post Script	Yes (optional)	No
Mount and Unmount Scripts	Yes (optional)	Yes.; must be configured by user.
Storage Switchover and Storage Failover Scripts	Yes (optional)	Yes; only for Oracle Sun ZFS and NetApp MetroCluster. To be configured by user.)

Figure 2-2 Oracle Site Guard Scripts: What They Do

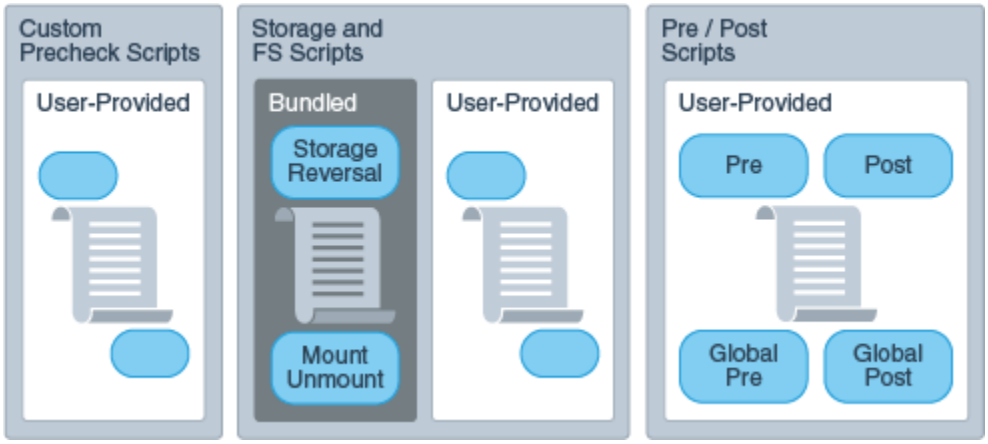
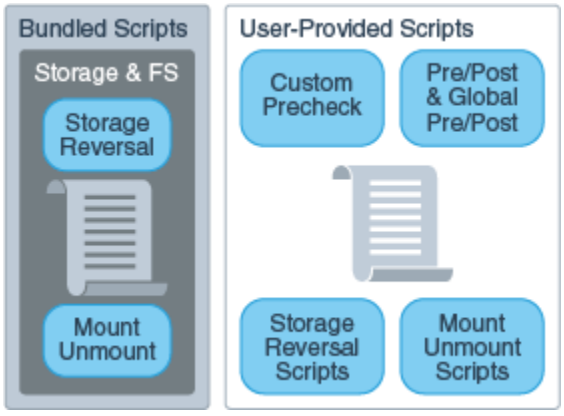


Figure 2-3 Oracle Site Guard Scripts: Who Provides Them



Sequence of Script Execution

The executing workflow of an Oracle Site Guard operation varies according to the operation carried out: switchover, failover, or start and stop.

Figure 2-4, Figure 2-5, and Figure 2-6 show the sequence in which Oracle Site Guard executes user-defined scripts in different kinds of operations.

Figure 2-4 Executing Sequence of Scripts for Switchover Operation

Figure 2-5 Execution Sequence of Scripts for Failover Operation

> **Note:**
>
> The optional scripts that are executed at the Primary site during a failover, are the same as that executed at the Primary site during a switchover operation. The scripts at the primary site are only executed as part of the failover operation if the user chooses to stop the Primary site during the failover.

Figure 2-6 Execution Sequence of Scripts for Start or Stop Operation

> **Note:**
>
> Custom Precheck scripts are scheduled to run on the Primary site for a Failover operation. But, since the Primary site might be inaccessible or non-operational, these scripts are set to run with a Continue on Error mode.

Configuring Script Paths

Configure the path of your user-defined scripts with the appropriate format according to the script type and runtime behavior.

Oracle Site Guard determines the location (path) of the script using the configuration path and type of script you provide. Table 2-2 illustrates how to configure various types of scripts, the corresponding script path that the user needs to specify, and the component that is extracted and used by Oracle Site Guard. Only the script path formats listed in the following tables are supported.

Table 2-2 Script Paths in Enterprise Manager Software Library

Script Type	User Configured Path	Script Path Extracted by Oracle Site Guard

Shell script	`sh swlib_script.sh`
	`sh ./swlib_script.sh`
	`sh ./swlib_script.sh -`
	`sh ./swlib_script.sh -option1 -option2`
	`/home/bash swlib_script.sh`
	`/home/bash swlib_script.sh -a param1 -b param2`
		`swlib_script.sh`

Perl script	`perl swlib_script.pl`
	`perl swlib_script.pl -a param1 -b param2`
	`/home/perl swlib_script.pl`
	`/home/perl swlib_script.pl -a param1 -b param2`
		`swlib_script.pl`

Python script	`python swlib_script.py`
	`python swlib_script.py -a param1 -b param2`
	`/home/python swlib_script.py`
	`/home/python swlib_script.py -a param1 -b param2`
		`swlib_script.py`

Table 2-3 Script Paths in Custom Scripts

Script Type	User Configured Path	Script Path Extracted by Oracle Site Guard

Shell script	`sh /home/oracle/custom_script.sh`
	`/home/oracle/custom_script.sh`
	`/home/bash /home/oracle/custom_script.sh`
	`/home/bash /home/oracle/custom_script.sh -a param1 -b param2`
	`/home/bash /home/oracle/custom_script`
	`/home/oracle/custom_script`
		`/home/oracle/custom_script.sh`
		`/home/oracle/custom_script`

Perl script	`perl /home/oracle/custom_script.pl` `/home/perl /home/oracle/custom_script.pl -a param1 -b param2`	`/home/oracle/custom_script.pl`
Python script	`/home/python /home/oracle/custom_script.py` `/home/python /home/oracle/custom_script.py -a param1 -b param2`	`/home/oracle/custom_script.py`

Prechecks and Health Checks

Ensure that the standby site is ready to perform the production role before initiating any disaster recovery operation by running prechecks and health checks.

The success of a disaster recovery plan depends on how accurately the plan represents the environment it is supposed to protect. Topology changes and configuration drift in the protected site can cause the disaster-recovery operation plan to lose synchronization with the environment, and can render the plan partially or completely ineffective. Frequently, this divergence, between the disaster-recovery plan and the environment being protected, is not discovered until an actual disaster-recovery attempt is in progress.

Oracle Site Guard provides a solution to this problem offering precheck and health checks:

Prechecks

A Precheck is an on-demand, automated procedure that assesses the disaster recovery readiness of a site.

A Precheck can be executed by itself (stand-alone mode) to check if a selected operation plan will succeed. It can also be invoked before an operation plan is executed. In the latter case, if the Precheck fails, the operation plan is not executed. Prechecks invoked before an operation plan are optional and can be skipped if desired.

Health Checks

A Health Check is a precheck that is scheduled to run periodically to provide an ongoing assessment of disaster recovery readiness.

A health check must be configured for a specified operation plan and must have a user-specified schedule associated with it. For example, you might set up a health check associated with the `Switchover to Standby Site` plan to run every Wednesday and Saturday at 12:30 am to monitor the fidelity of that operation plan on an ongoing basis. You can also choose to be notified of health check results through e-mail.

Each configured operation plan can have an associated health check, and health checks for different plans execute independent of each other. You can stop health checks for an operation plan at any time

Oracle Site Guard performs the following checks during Prechecks and Health Checks:

- Checks whether all the hosts involved in the planned disaster recovery operation are reachable. During this check, Oracle Site Guard logs into each host using the credentials configured for that host. This ensures that the host is reachable and can be accessed for executing directives and scripts.
- Checks whether the primary and standby databases are configured correctly and Data Guard protection is functioning correctly. This check verifies the following:
  - The primary and standby database names are correct.
  - The database login credentials are correct.

  - Data Guard broker is ready to switchover the database.
  - Database Flashback status is set to **ON**.
  - Data Guard Redo and Transport Lags are within the limits specified by the user.
- Checks whether the ZFS storage replication is functioning correctly. This check verifies the following:
  - The replication lags are within the limits specified by the user.
  - The source and destination ZFS appliances are reachable.
  - The login credentials are valid.
  - The replication action is configured correctly.
- Checks whether user scripts are configured correctly by verifying whether each configured user script is found at the correct location.
- Checks whether replicated file systems can be mounted during a switchover or failover. To confirm this, the check verifies that the file system mount points exist and can be accessed for mount operations.
- Checks whether the Data Guard and ZFS replication lag checks are within the bounds specified by the user.

> **Note:**
>
> An associated Precheck is automatically created for every operation plan that is created. However, a health check must be explicitly scheduled for an operation plan.

Customizing Prechecks and Health Checks

You can customize built-in Prechecks and Health Checks by adding custom (user-defined) scripts that execute in any of those operations.

This allows you to enhance Oracle Site Guard Prechecks and Health Checks by inserting prechecks for third-party components that need to be included in the disaster recovery workflow. Custom precheck scripts function the same way that built-in Prechecks. If a custom precheck script detects an anomaly and returns an error, that precheck step is regarded as failed and, depending on how the script is configured (for example, if the script execution step is configured with the attribute **Stop on Error**), the disaster recovery operation may be aborted.

Lag Checks

The efficiency and timeliness of the data replication between the primary and standby sites depend on many factors, including network bandwidth, congestion, latency, storage appliance load, amount of replicated data, and so on.

Disaster Recovery configurations typically include one or more storage appliances and data stores that are used for data storage by the application and database tiers. To make this data available at the standby site in the event of disaster recovery, these data stores are replicated from the primary to standby site using either continuous or periodic replication. To perform a successful site switchover or failover, Oracle

Site Guard must also perform storage role reversal as part of the disaster recovery process.

It is not uncommon for a certain amount of lag to be present between the source data at the primary site and the replicated data at the standby site. Oracle Site Guard provides a mechanism to configure the amount of replication lag that is permissible before a disaster recovery operation can begin execution. During the Precheck phase of a disaster recovery operation, Oracle Site Guard checks the current replication lag. If the lag exceeds the user-specified threshold, Oracle Site Guard does not execute the disaster recovery operation.

You can configure the following lag check parameters:

Database Lag Check

This parameter specifies the permissible lag for Redo Apply and Redo Transport which is managed by Oracle Data Guard.

ZFS Lag Check

By default Site Guard will determine the proper lag value for application-tier storage replication which is managed by ZFS. Alternatively, the ZFS lag check parameter can be used to specify a permissible lag value.

Storage Integration

During a disaster recovery, the storage replication direction must be reversed and storage appliances must be reconfigured before applications can be migrated to a standby site.

Managing storage operations is an essential part of a disaster recovery. Oracle Site Guard offers storage management and integration options for various storage technologies.

The following sections describe the Oracle Site Guard storage integration options:

Oracle Sun ZFS

Oracle Site Guard provides a built-in script to orchestrate Oracle Sun ZFS storage role reversals.

If you are deploying Oracle Sun ZFS storage appliances, you can use the bundled storage management `zfs_storage_role_reversal.sh` script to orchestrate Oracle Sun ZFS storage role reversal as part of Oracle Site Guard disaster recovery operations.

NetApp MetroCluster

Oracle Site Guard provides a built-in script to orchestrate NetApp MetroCluster storage role reversals.

If you have deployed a NetApp MetroCluster Disaster Recovery configuration, you can use the bundled NetApp storage management `siteguard_netapp_control.sh` script to orchestrate NetApp MetroCluster storage role reversal as part of Oracle Site Guard disaster recovery operations. For details, see MOS note titled *Oracle Site Guard Feature For NetApp MetroCluster (Doc ID 1964220) at https://support.oracle.com*.

Integrating Other Storage Types

Oracle Site Guard offers integration with storage technologies by allowing you to incorporate your own custom storage management scripts into Oracle Site Guard operation plans.

You can implement storage role reversal for third-party storage technologies by invoking your own custom storage management scripts during the storage script execution phase of the operation plan execution.

Mount and Unmount Scripts

Oracle Site Guard provides a built-in script to mount and unmont file systems and allows you to use custom scripts to manage file systems.

In addition to integrating with storage technologies, Oracle Site Guard allows you to incorporate your own scripts to manage file systems. For example, during a switchover operation, file systems that are used by a multi-tier application are unmounted at the primary site after the application is stopped; and replicated versions of those file systems are then mounted at the standby site before the application is started. These unmount and mount operations for application servers at the primary and standby sites can be orchestrated using the built-in mechanism for integrating scripts. Oracle Site Guard provides the `mount_umount.sh` script for file system mount and unmount operations. Alternately, you can define your own custom script to be invoked at appropriate points in the operation plan.

Standby Site Validation

Standby Site Validation allows you to convert your standby site into a fully functional site, so you can test and validate standby sites.

In a normal Site Guard disaster recovery configuration, the standby site is offline and unavailable for business operations.

To open a standby site for validation, configure and execute a *Open for Validation* type of operation plan for the site. After testing and validation are complete, you can revert the site back to a standby role by configuring and executing a *Revert to Standby* type of operation plan.

When opening a standby site for validation, Oracle Site Guard:

- Converts the standby database from a physical standby database to a snapshot standby database. In this mode, the Data Guard redo logs are still shipped from the primary to the standby, but the logs are not applied to the standby database. The accumulated redo logs are applied after the database converts back to a physical standby database (after executing a Revert to Standby operation in Oracle Site Guard).
- Clones ZFS replicated projects that are part of this Site Guard configuration to create a readable and writable copy of the replicated project. The file systems in this cloned project are then mounted for use by applications at the standby site. While the cloned project is being read to or written from by applications at the standby site, the ZFS replication from the primary site to the standby site (that was originally configured) continues with no interruptions. When the opened for validation standby site is closed with a Revert to Standby operation, the cloned

file systems are un-mounted and the ZFS clones that were created as part of the Open for Validation operation are destroyed.

- Executes all configured Global Prescripts and Global Postscripts, Prescripts and Postscripts, and Custom Precheck Scripts as they would be in any other operation plan.

When a standby site is opened for validation, the Recovery Point Objective (RPO) remains unaffected because database redo transport and ZFS storage replication continue uninterrupted as configured. No transaction data at the primary site is lost. However, the Recovery Time Objective (RTO) is affected because the standby site is not immediately available to accept an incoming switchover or failover. The standby site must first be reverted back to a (normal) Standby mode before the primary site can switchover or failover to the standby site.

The ability to open a standby site in validation mode offers the following benefits:

- It increases your confidence that the disaster recovery configuration is correct and provides a way to verify that the standby site can become operational and meets your expectations.
- It increases resource utilization by using standby sites for testing patches, validating new configurations, and generating analytics and reports.

> **Caution:**
>
> Note the following important points regarding a standby site opened for validation:
>
> - *A standby site that is opened for validation is not available as a disaster recovery site. It must be reverted back to a standby role (with Revert to Standby) before it can accept an incoming switchover or failover from the primary site.*
> - *A standby site that is opened for validation must not be used for production activities (customer traffic) because any transactions that occur in the site will be discarded when the site reverts to a standby site.*
> - When a physical standby has a RedoRoutes property assigned to the primary database, it must be specified as (LOCAL : ...) in the rule. If not, Data Guard broker will not allow the conversion to a snapshot standby and the operation will fail with the ORA-16692 error. Refer to Oracle Database documentation for details on configuring RedoRoutes with the LOCAL primary database value.

Creating Execution Groups

An Execution Group allows you to customize the step sequence of executions (within common functional areas) when those executions run in parallel.

Site Guard operation plans consist of separate buckets for handling a common functional areas or target types when the plan executes; for example, all database instances for a site will be in a single bucket. Each of these buckets typically consists of one or more steps which process the target type or functionality for which that

bucket is intended. Additionally, the *Execution Mode* of a bucket specifies whether the steps in a bucket should be executed in *Serial* or *Parallel*.

For example, a typical operation plan will contain separate buckets that contain all the steps for each of the following functional areas in a site:

- Shutting down all Oracle WebLogic Server domains
- Switching over all databases
- Executing all the Pre Scripts
- Executing all the Mount or Unmount scripts

Execution Groups allow you to define a precise orchestration sequence within a bucket. For example, operation plan steps that are in Execution Group 3 will all execute in parallel only after all the steps in Execution Group 2 have finished execution. Similarly, Site Guard will ensure that all the operation plan steps in Execution Group 3 finish executing before any steps in Execution Group 4 are started. This allows you to place each operation plan step in a given bucket in a specific group in order to determine when that operation plan step will be executed.

When you create an operation plan, Site Guard initially marks the Execution Mode for each bucket as Parallel, and will place all the steps in the bucket in Execution Group 1. However, you can edit the operation plan and customize the Execution Group for each step to determine its execution sequence.

> **Note:**
>
> *If a bucket has an Execution Mode of Serial, then Execution Groups become irrelevant because all the steps in that bucket will be executed sequentially. This is the equivalent of putting each step in its own execution group. Site Guard allows you to edit the operation plan and re-order the sequence of steps in a Serial execution bucket.*
>
> *When viewing or editing plans in the Site Guard UI, the Execution Group column is hidden by default*.
>
> *Custom pre checks can be placed into execution groups, however regular pre checks cannot and will always execute in parallel.*

Monitoring Executions and Managing Errors

In this section, you learn how to customize, execute, and monitor execution plans with Oracle Site Guard.

When you execute an Oracle Site Guard operation plan, you can customize the plan before you execute it, monitor the execution of the plan, manage any errors you encounter during plan execution, and retry plan execution after making changes.

This section contains the following topics:

Customizing Operations

Learn how to customize Oracle Site Guard operations according to your environment.

Oracle Site Guard operation plans can be customized according to the characteristics of your environment. Specifically, you can customize any operation step by:

- Specifying whether the step should be enabled or disabled for execution (disabled steps are skipped during execution).
- Moving the step to another point in the execution sequence (for example, changing the order of managed servers to be brought up within a domain group).
- Specifying how errors for the step are to be handled (that is, stop or continue operation execution when an error is encountered).
- Specifying whether the steps of a given group are to be executed serially or in parallel (for example, start up all the managed servers at the same time, or start one managed server at the time).

Monitoring Executions

You can monitor operation results in the Procedure Activity page of Oracle Enterprise Manager Cloud Control Console.

Oracle Site Guard disaster recovery operations execute as Oracle Enterprise Manager Deployment Procedures. The procedure activity screen for an Oracle Site Guard operation displays each operation plan as a hierarchy of steps with a graphical icon showing the result of each step as it is executed. A check mark is displayed if the step succeeds, or a cross is displayed if the step fails. The icon, , indicates that the step was skipped and not configured for execution. This mechanism provides a visual summary of the operation plan progress.

When viewed in the Operation Activity page, the execution details for each operation plan or precheck are organized as a hierarchy of top-level steps with consequent sub-steps. Initially, only the top-level steps are visible to the user. The consequent sub-steps are collapsed and hidden within each top-level step. However, each top-level step in the operation activity can be further inspected in detail by clicking on the step to expand it, and navigating down into the hierarchy to select a constituent sub-step. The execution log for each sub-step can also be examined for additional details. This hierarchical organization of operation activity allows you to examine the results of the operation plan at any desired level of detail.

Operation Error Modes

Each step in an Oracle Site Guard operation plan has an error mode an associated with it, which you can configure.

This error mode defines how Oracle Site Guard handles any error that is encountered during the execution of that step.

The following error modes are available:

Stop on Error

This mode specifies that Oracle Site Guard should stop executing the operation plan if it encounters an error while executing the current step.

Continue on Error

This mode specifies that Oracle Site Guard should continue with the execution of the next step if it encounters an error while executing the current step.

Retrying Failed Operations

If Oracle Site Guard stops execution because of an error encountered during an operation, you can resolve the issue that caused the error and retry the operation.

Oracle Site Guard resumes execution of the failed operation at the step where the failure occurred. You can also ignore the failed step, by clicking **remove**, and retry the operation. In this case, Oracle Site Guard will ignore the failed step, and resume execution of the operation plan starting with the step immediately following the failed step.

Suspending and Resuming Operations

You can suspend an in-progress Oracle Site Guard operation or resume a suspended operation, at any point in time.

When resuming a suspended operation, Oracle Site Guard will resume execution of the operation at the point where it was suspended. Additionally, you can also stop an operation that is currently in progress.

> **Note:**
>
> Stopped operations cannot be resumed.

Credential Management

Learn how to manage credentials used in Oracle Site Guard.

This section includes the following topics:

- Oracle Enterprise Manager Credential Management Framework
- Oracle Site Guard Credential Configuration

Oracle Enterprise Manager Credential Management Framework

Oracle Enterprise Manager provides the Credential Management Framework that you can use to manage identities and to ensure that the access to Oracle Enterprise Manager targets is authorized and authenticated.

Typically, you can set up Named Credentials in Enterprise Manager before configuring Oracle Site Guard to use these credentials. After the credentials are configured, Oracle Site Guard uses them to access all managed targets at protected sites.

Depending on the topology of the site, Oracle Site Guard may need to use Named Credentials for different targets such as hosts, Oracle Database instances, WebLogic Servers, and other target types. For information about setting up credentials in Enterprise Manager, see Setting Up Credentials.

Oracle Site Guard Credential Configuration

Learn how to use credentials in Oracle Site Guard operations.

After the required target credentials have been configured in Enterprise Manager's Credential Management framework, you can utilize them during Oracle Site Guard's credential configuration process. Oracle Site Guard credential configuration requires that the targets that are accessed and controlled by Oracle Site Guard for disaster recovery operations have valid credentials associated with the target. For information about setting up credentials and associating them with targets, see Creating Credential Associations.

Role-Based Access Control

Oracle Site Guard offers Role-Based Access Control (RBAC) using the User Accounts framework provided by Oracle Enterprise Manager.

Oracle Enterprise Manager provides preconfigured roles for different areas or functions within Enterprise Manager. One of these administrator roles, `EM_SG_ADMINISTRATOR`, is customized for Oracle Site Guard-focused activities within Enterprise Manager. You can utilize this built-in role to create users focused on Oracle Site Guard administration tasks. Alternately, you can create your own customized roles and users that allow for greater flexibility in tuning role-based access to Oracle Site Guard functionality.

For information about setting up role-based access control, see Creating Oracle Site Guard Administrator Users.

Software Library Integration

Oracle Site Guard includes ready-to-use scripts to perform typical activities during a disaster recovery operation, such as switching over an Oracle Database, or starting or stopping an Oracle WebLogic Server.

These scripts are included as part of the Enterprise Manager Software Library, and all required scripts are automatically deployed to the applicable hosts during operation execution. However, in addition to the bundled scripts, you may require other custom scripts to be automatically deployed and executed as part of an operation. Oracle Site Guard provides a mechanism for you to upload your own custom scripts to the Enterprise Manager Software Library and to add these scripts to your operation plan when you create the plan.

An additional advantage of using scripts that are part of the Enterprise Manager Software Library is that these scripts are automatically deployed to all configured script hosts at runtime. On the other hand, user scripts that are not part of the Enterprise Manager Software Library must be manually deployed on each configured script host before the operation plan begins execution.

For more information about the various types of scripts that a user can add to the Enterprise Manager Software Library, see Extensibility.

Custom Credentials for Script Execution

You can add a set of credentials to the credential repository and configure a script to execute with these credentials.

User-defined scripts that are either externally deployed or deployed through the Software Library are typically executed using the credentials configured for the host on which the script will execute. These credentials are configured and maintained in

the Enterprise Manager credential management framework, and are referred to as the **Host Normal Credentials** or **Host Privileged Credentials**.

You can also add other sets of credentials to the credential repository and configure a script to execute with this set of credentials. This is useful in cases where the script requires credential privileges that are different from the standard (Host Normal) or privileged (Host Privileged) credentials configured for the script host. For example, a script that must be executed with a specific user ID to shut down a server process on that host.

Passing Credentials as Script Parameters

Oracle Site Guard provides a mechanism to pass credentials to a configured script.

User defined scripts frequently perform actions that require them to first authenticate with some other entity and they require one or more sets of credentials to perform this authentication. To avoid hard-coding credentials into the script or passing them insecurely as clear-text parameters to the script, Oracle Site Guard provides a mechanism to securely pass one or more sets of credentials to a configured script. These credentials are stored and maintained in a secure manner in Oracle Enterprise Manager's credential management framework. Once these credentials are configured and associated as parameters for the user script, Oracle Site Guard will encrypt and pass these credentials to the user script at execution time. The user script can then extract these credentials and use them for authentication.

For details about extracting encrypted credentials inside a user script, see Passing Credentials as Parameters.

Oracle Site Guard Workflows

Oracle Site Guard workflows (or operations) are modeled as Enterprise Manager deployment procedures.

Oracle Site Guard provides the following distinct types of workflows for disaster-recovery operations:

When there is a failure or planned outage of the primary site, Oracle Site Guard automates the following steps to enable the standby site to assume the production role in the topology:

1. Stops the services and applications running on the primary site, and unmounts the storage on the primary site.
2. Disables ongoing replication from primary site to standby site and performs role reversal.
3. Performs a failover or switchover of the Oracle Databases with Oracle Data Guard Broker.
4. Mounts the replicated storage (file systems) on the standby site.
5. Starts the services and applications on the standby site. At this point, the standby site assumes the production role.

> **Note:**
>
> If continuous storage replication is not configured, Oracle recommends that you perform a final storage replication from the primary site to the standby site, before you initiate the Site Guard operation. However, if the primary site has failed, it may not be possible to perform this final replication.

Oracle Site Guard workflows can be monitored, suspended, resumed, and stopped with Enterprise Manager's Procedure Management framework.

Switchover Workflow

This workflow transitions production activities from the primary site to a standby site.

The Switchover workflow provides the ability to perform a controlled transition of the production activity from the primary site to a standby site. Figure 2-7 shows the steps executed during a typical Switchover workflow.

> **Note:**
>
> A disaster recovery operation comprises of operations that are dependent on the topology and site configuration.

Figure 2-7 Switchover Workflow

Failover Workflow

This workflow transitions production activities to a standby site.

The Failover workflow provides the ability to perform a forced transition of production activity to a standby site. When a failover operation is launched, Oracle Site Guard assumes that the primary site is unavailable, and starts all protected applications at the standby site. Figure 2-8 shows the steps executed during a typical Failover workflow:

Figure 2-8 Failover Workflow

Start Workflow

This workflow starts activities at a production site.

The start workflow provides the ability to start activities at a production site. This workflow is typically used to bring up a site after maintenance, or to test whether the site can be started as part of testing a larger workflow such as a switchover. Figure 2-9 shows the steps executed during a typical Start workflow.

Figure 2-9 Start Workflow

Stop Workflow

This workflow stops activities at a production site.

The Stop workflow provides the ability to stop activities at a production site. This workflow is typically used to bring down a site for maintenance, or to test whether the site can be stopped as part of testing a larger workflow such as a switchover. Figure 2-10 shows the steps executed during a typical Stop workflow.

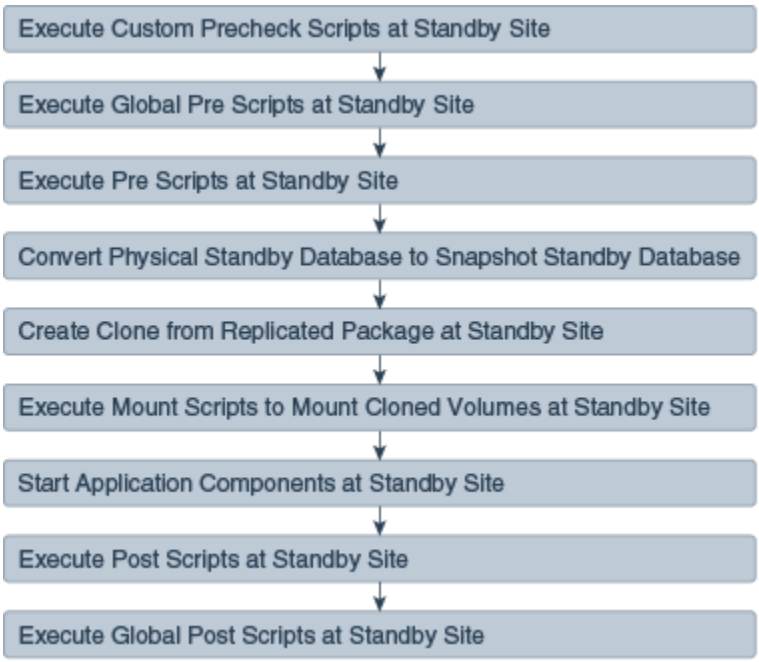
Figure 2-10 Stop Workflow

Open for Validation Workflow

This workflow converts a standby site to an operational site so that it can be tested and validated.

The Open for Validation workflow provides the ability to convert a standby site to an operational site. This workflow is typically used to convert a standby site to a functional site so that it can be tested and validated. Figure 2-11 shows the steps executed during a typical Open for Validation workflow.

Figure 2-11 Open for Validation Workflow

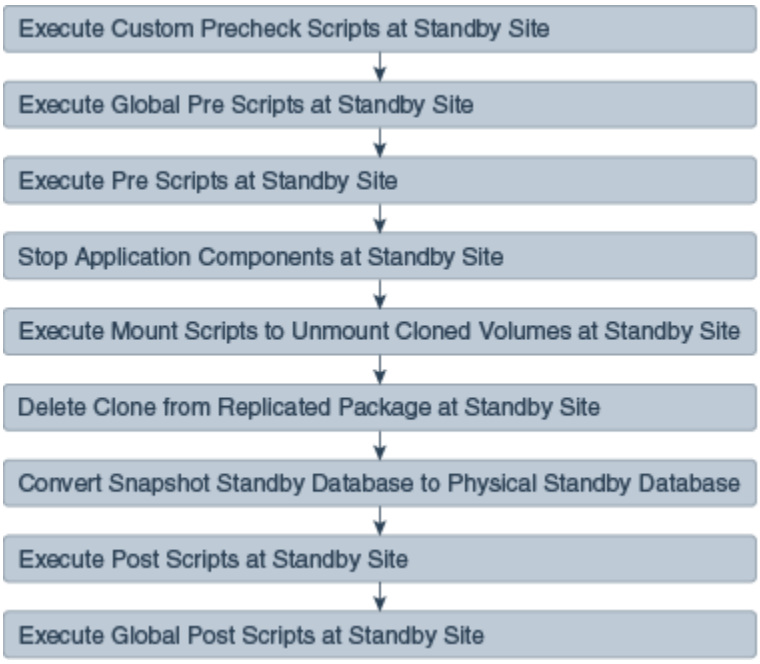


Revert to Standby Workflow

This workflow converts a site that has been opened for validation back to a standby site.

The Revert to Standby workflow provides the ability to convert a site back to a standby site after you opened the site for validation. This workflow is typically used to convert a standby site that is has been opened for validation, back to a standby site so that it can be used for disaster recovery operations such as switchover or failover. Figure 2-12 shows an example of the steps executed during a typical Revert to Standby workflow.

Figure 2-12 Revert to Standby Workflow



3

Installing and Preparing Oracle Site Guard

In this section, you learn how to install Oracle Site Guard and prepare it for operation in your Enterprise Manager Cloud Control environment.
This chapter includes the following sections:

- Installing Oracle Site Guard
- Preparing Oracle Site Guard for Operation

Installing Oracle Site Guard

Learn how to install and manage Oracle Site Guard with Enterprise Manager Command-Line Interface (EMCLI) or Oracle Enterprise Manager Cloud Control.

Oracle Site Guard is included with Enterprise Manager Cloud Control 13cR3 Fusion Middleware Plugin 13.3.1.0.0.

You can manage an Oracle Site Guard configuration EMCLI, or with Oracle Enterprise Manager Cloud Control.

To install Oracle Site Guard:

- Install Enterprise Manager Cloud Control 13c R3 Fusion Middleware Plugin 13.3.1.0.0 for your Oracle Fusion Middleware enterprise deployment. For information about installing Enterprise Manager Cloud Control 13cR3 Fusion Middleware Plugin 13.3.1.0.0, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

  > **Note:**
  >
  > Ensure that you install Oracle Management Agent (Enterprise Manager Agent) on each of the hosts managed by Enterprise Manager, as described in Installing Oracle Management Agent in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

- Install EMCLI, as described in *Oracle Enterprise Manager Command Line Interface Guide* .

  > **Note:**
  >
  > Oracle recommends that you install EM CLI in the same Oracle home where Oracle Management Service is installed. For example, `OMS_HOME/bin/emcli`.

Preparing Oracle Site Guard for Operation

Prepare Oracle Site Guard for operation.

After you have installed Oracle Site Guard, complete the following required tasks to prepare Oracle Site Guard for operation:

Discovering Targets on the Primary and the Standby Sites

To get started with Oracle Site Guard, you first discover all the targets at your primary and standby sites that Oracle Site Guard will protect.

To discover targets at the primary and standby site, complete the steps described in Discovering and Monitoring Targets in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

Discover the following target types in Oracle Enterprise Manager:

- Oracle Fusion Applications
- Oracle Fusion Middleware farm/ WebLogic Domain
- Oracle Fusion Middleware managed system components, such as Oracle HTTP Server and Oracle Internet Directory (part of the Oracle Fusion Middleware farm)
- Real Application Cluster (RAC) databases
- Single-instance database

A site should be up and running for its targets to be discovered. This means that the site would function as the production site. For a two-site deployment, the targets in the primary site should be discovered first, followed by the targets in the standby site. After you discover the targets in the primary site, you must manually perform a switchover operation, so that the standby site takes over the production role, as described in: Setting Up and Managing Disaster Recovery Sites in *Oracle® Fusion Middleware Disaster Recovery Guide*. . Then you must discover the targets in the standby site, as you did for the primary site.

> **Note:**
>
> After discovering the targets for the standby site, you can use Oracle Site Guard to switch back operations to the primary site, so that the primary site takes over the production role, as described in: Setting Up and Managing Disaster Recovery Sites in *Oracle® Fusion Middleware Disaster Recovery Guide*. You only need to switchover and switchback manually during the configuration process.

Creating Oracle Site Guard Administrator Users

Oracle recommends that you create Oracle Site Guard own users and administrators to manage disaster recovery operations.

Users who are not Enterprise Manager super users and who do not have `EM_SG_ADMINISTRATOR` role assigned, cannot access the Oracle Site Guard functionality.

Note the following privilege restrictions for Oracle Site Guard administrators and how it affects Enterprise Manager super users:

- Oracle Site Guard administrators can only view, modify and execute operation plans owned by them. An administrator cannot view, modify, or execute operation plans owned by another Oracle Site Guard administrator or super user.
- A super user can view, modify and execute operation plans owned by anyone, including all Oracle Site Guard administrators and other super users.

If these restrictions do not work in your deployment, skip the steps for creating Oracle Site Guard Administrator users and use the built-in super user roles to access Oracle Site Guard functionality.

To create one or more Oracle Site Guard Administrator users, use one of the following methods:

Creating an Oracle Site Guard Administrator User with Enterprise Manager Cloud Control Console

Learn how to create an Oracle Site Guard administrator with Enterprise Manager Cloud Control.

To create an Oracle Site Guard administrator user with Enterprise Manager Cloud Control, perform the following steps:

1. Login to Enterprise Manager as a super user.
2. From the Setup menu, select **Security**, then select **Administrators**.
3. On the Administrators page, click **Create**.
4. In the Create Administrator wizard, do the following:
   a. On the Properties page:
      1. Specify the name `SG_ADMIN`.
      2. Provide a password.
      3. Provide a password confirmation.
   b. Make changes to any other fields as appropriate, and then click **Next**.
   c. On the Roles page, select the `EM_SG_ADMINISTRATOR` role in the Available Roles pane on the left, and click **Move** to add the role to the Selected Roles pane on the right.
   d. If you discovered targets at the Primary and Standby sites as another user, assign target level privileges to the Oracle Site Guard Administrator user on the Target Privileges page.
      1. Assign **Full any Target** or **View any Target** privileges in the section **Privileges applicable to all Targets**.
      2. Alternately, assign view or full privileges for every target in the Primary and Standby sites by setting **Target Privileges**.
   e. On the Review page, review the information you have provided for the user account, and click **Finish**.

Creating an Oracle Site Guard Administrator User with Enterprise Manager Command-Line Interface

Learn how to create an Oracle Site Guard administrator with Enterprise Manager Command-Line Interface (EMCLI).

To create an Oracle Site Guard administrator, run the following EMCLI command (located at `OMS_HOME/bin/emcli`):

```
emcli create_user
       -name="SG_ADMIN"
       -password=password
       -roles="EM_SG_ADMINISTRATOR;EM_USER;PUBLIC"
```

Parameter	Description
`-name`	Enter a name for the Oracle Site Guard Administrator user.
`-password`	Enter a password for the Oracle Site Guard Administrator user.
`-roles`	The list of roles assigned to this user. Enter `EM_SG_ADMINSTRATOR;EM_USER;PUBLIC`.

For more information about the `create_user` command, see create_user.

Creating Primary and Standby Sites

Learn how to create a generic system and how to use it as a primary or secondary site.

A disaster recovery site managed by Oracle Site Guard is modeled as a Generic System target type in Oracle Enterprise Manager. You can create a generic system and then use it as a primary and standby site. Each generic system that you use, must include all targets and Oracle Fusion Middleware farms and Databases pertaining to the site that it represents.

To create a generic system, use one of the following methods:

Creating a Generic System with Enterprise Manager Cloud Control Console

Create a generic site with Enterprise Manager Cloud Control Console. You can use a generic site as a primary or secondary site.

To create a generic system with Enterprise Manager Cloud Control Console, perform the following steps:

1. Login to Enterprise Manager as a super user.
2. From the **Targets** menu, click **Systems**.
3. Click **Add** and from the drop-down menu, select **Generic System**.
4. In the **General** section, enter the name for your primary system or site.
5. Select the time zone from the drop-down menu.
6. In the **Member** section, click **Add**.

7. Choose the targets that will be part of your primary system, and click **Select**. Following are examples of targets that are usually added:
   - Oracle Fusion Middleware Farm which includes:
     - Administration Server
     - Managed Servers
     - System components (for example, Oracle HTTP Server)
   - If you are using Oracle RAC Database then you must associate it with a **Cluster Database** target. For a single database instance, you must associate it with a **Database Instance** target.

   > **Note:**
   >
   > Ensure that the following target types are *not* added to the generic system:
   >
   > - Database System
   > - Individual RAC Database instances

8. Click **Next**.

   The **Define Associations** page is displayed.

9. Click **Next**.

   The **Availability Criteria** page is displayed.

10. From **Availability Criteria**, select the **Any Of The Key Members** option, and double-click a target in the Members pane. The selected member is removed from the Members pane and added in the Key Members pane.

11. Click **Next**.

    The **Charts** page is displayed.

12. Click **Next**.

    The **Review** page is displayed.

13. Review your settings, and click **Finish**.

Creating a Generic System with Enterprise Manager Command-Line Interface

Create a generic site with Enterprise Manager Command-Line Interface (EMCLI) and use it as a primary or secondary site.

To create a generic system, run the following EMCLI command (located at *OMS_HOME*`/bin/emcli`):

> **Note:**
>
> For information about setting up a new EMCLI client, see the Enterprise Manager Command-Line Interface Download page within the Cloud Control console. To access the page, in **Cloud Control**, from the **Setup** menu, click **Command Line Interface**.

```
emcli create_system
      -name="name"
      -type=generic_system
      -add_members="name1:type1;name2:type2;..."]...
      -timezone_region="actual_timezone_region"
```

> **Note:**
>
> To get status and alert information for targets, you can run `emcli get_targets` command. For more information on Enterprise Manager command line, see Verb Reference in the *Oracle Enterprise Manager Command Line Interface Guide*.

Parameter	Description
`-name`	Enter a name for the system.
`-type`	Enter `generic_system` as the type.
`-add_members`	Add existing targets to the system. Each target is specified as a name-value pair `target_name:target_type`. You can specify this option more than once.
`-timezone_region`	Specify the time zone region. The time zone you specify here is used for scheduling operations such as jobs and blackouts, on the system.

See also create_system.

Creating Credentials

Credentials are required to access the targets (hosts, servers, and databases) associated with Oracle Site Guard.

You can create and delegate named credentials or preferred credentials for the following targets associated with Oracle Site Guard:

- Host (for normal or non-root user)
- Host (for user with root privileges)
- Oracle Node Manager (use Oracle Weblogic Domain as the Target Type and Node Manager as the Credential Type)
- Oracle Weblogic Server
- Oracle Database (SYSDBA)

This section contains the following topics:

> **Note:**
>
> You must associate the credentials that you create with the Oracle Site Guard configuration. Oracle Site Guard supports specifying the same credentials for all targets of the same target type. For example, all databases in a system can have the same `sysdba` credentials. Oracle Site Guard also allows the targets of same type to have different credentials.
>
> You need not create credentials for the targets running at the standby site if the credentials are the same across all targets on the primary and standby sites.

Creating Named Credentials

Learn how to create a named credential with with Enterprise Manager Cloud Control Console or EMCLI commands.

You can create named credentials using Enterprise Manager Cloud Control Console or EMCLI commands as explained in the following tasks.

To create named credentials with Enterprise Manager Cloud Control Console, perform the following steps:

1. Login to Enterprise Manager, preferably as an `EM_CLOUD_ADMINISTRATOR` user.
2. From the Setup menu, select **Security**, then select **Named Credentials**.

   The Named Credentials page is displayed.
3. Click **Create**.

   The Create Credential page is displayed.
4. In the General Properties section, specify the following:
   - **Credential name**: Enter a name for the credential.
   - **Credential description**: Enter the credential description.
   - **Authenticating Target Type/ Credential type/ Scope**: Enter the details as specified in the following table:

Element	Host	Host (`root`-User Privileges)	Oracle Node Manager	Oracle WebLogic Server	Database Instance
Authenticating Target Type	Host	Host	Oracle Weblogic Domain	Oracle WebLogic Server	Database Instance
Credential type	Host Credentials	Host Credentials	Node Manager Credentials	Oracle WebLogic Credentials	Database Credentials
Scope	Global	Global	Global	Global	Global

- If these credentials are valid for all targets of the selected **Authenticating Target Type**, then set **Scope** to **Global**.

  If these credentials are only valid for a specific target, then set **Scope** to **Target**, and set the **Target Type** and **Name** fields to match the specific target.

5. In the Credential Properties section, specify the following:
   - **UserName**: Enter the user name.
   - **Password**: Enter the password.
   - **Confirm Password**: Enter the password again.
   - **Run Privilege**: Enter the details as specified in the following table:

Element	Host	Host (Users with `root` privileges)	Oracle WebLogic Server	Database Instance
Run Privilege	None	Select **Sudo** and enter values in the **Run As** fields	Oracle WebLogic Server Administration user credentials	Oracle Database SYS user credential

> **Note:**
>
> When the credentials used by Oracle Site Guard are configured to use `sudo` privileges to run as `root`, the `sudo` privilege must be configured as PDP (Privilege Delegation Provider) on all the agents running on the respective hosts of the target.
>
> PDP (Privilege Delegation Provider) can be configured from Enterprise Manager Cloud Control console. To configure PDP, go to **Setup** -> **Security** -> **Privilege Delegation** in the Enterprise Manager Cloud Control console.

6. If you are creating this credential as a user other than the Oracle Site Guard Administrator, you must grant view credential access to the Oracle Site Guard Administrator who will use the credential. To provide access, use the procedure in Granting Credential Privileges to Oracle Site Guard Administrator Users.

   To provide access, complete the following steps in the Access Control section.

   a. Click **Add Grant**. The Add Grant pop-up window appears.

   b. Select the rows for all the Oracle Site Guard Administrator users you created while creating Oracle Site Guard Administrator users. See Creating Oracle Site Guard Administrator Users.

   c. Click **Select**.

   d. Verify that the users you selected appear in the list of Grantees in the Access Control table.

7. Click **Test and Save**. To test credentials, select the appropriate **Test Target Type** from the drop-down menu for which you want to test the credentials, and specify **Test Target Name**.

To create named credentials with EMCLI:

```
emcli create_named_credential
         -cred_name="cred_name"
         -auth_target_type="auth_target_type"
         -cred_type="cred_type"
         -attributes="p1:v1;p2:v2"
```

Parameter	Description
`cred_name`	Set the name for this credential set.
`auth_target_type`	Set the authenticating target type.
`cred_type`	Set the credential type for the target/credential set.
`attributes`	Enter the following credential column values: `colname:colvalue;colname:colvalue` To change the value of the separator, use `-separator=attributes=newvalue`. To change the value of the sub-separator, use `-subseparator=attributes=newvalue`.

Creating Preferred Credentials

Learn how to create preferred credentials using Enterprise Manager Cloud Control Console or EMCLI commands.

You can create preferred credentials using Enterprise Manager Cloud Control Console and set them as target of a preferred credential with EMCLI Commands, as explained in the following tasks.

To create preferred credentials with the Enterprise Manager Cloud Control Console:

1. Login to Enterprise Manager as a super user or `EM_CLOUD_ADMINISTRATOR`.
2. From the Setup menu, select **Security**, then select **Preferred Credentials**.

   The Preferred Credentials page is displayed.
3. Select a target type, and click **Manage Preferred Credentials**. The target specific Preferred Credentials page is displayed.
4. Select the credential type from the Default Preferred Credentials table, and click **Set**. The Select Named Credential pop-up window is displayed.
5. Select an existing named credential to be the Preferred Credential and click **Save**.
   a. Select **New** to create a new named credential to be set as Preferred Credential.
   b. Enter a user name and password for the credential.
   c. Enter a credential name, and select **Save As**. The credential will be saved with the name that you have provided.
   d. Click **Test and Save**.

To set a named credential as a target preferred credential with EMCLI, use the `set_preferred_credential` command.

> **Note:**
>
> Oracle recommends that you to create preferred credentials with the `emcli` commands.

```
emcli set_preferred_credential
        -set_name="set_name"
        -target_name="target_name"
        -target_type="type"
        -credential_name="name"
        [-credential_owner ="owner"]
```

> **Note:**
>
> [ ] indicates that the parameter is optional.

Parameter	Description
`set_name`	Set the preferred credential for this credential set.
`target_name`	Set the path for the software library location.
`target_type`	Target type for the target/credential set.
`credential_name`	Name of the credential.
`credential_owner`	Owner of the credential. This defaults to the currently logged-in user.

Example:

```
emcli set_preferred_credential
        -set_name="HostCredsNormal"
        -target_name="test.example.com"
        -target_type="host"
        -credential_name="MyHostCredentials"
        -credential_owner="Admin"
```

Granting Credential Privileges to Oracle Site Guard Administrator Users

Named credentials are used to grant Oracle Site Guard administrators privileges to access and manage targets in disaster recovery operations.

The named credentials you created and configured as described in Creating Named Credentials, are used to grant access and manage targets during disaster recovery operations. The Oracle Site Guard administrators you created as described in Creating Oracle Site Guard Administrator Users, must be assigned privileges using those named credentials.

To grant privileges to Oracle Site Guard administrators, see Granting Credential Privileges with Enterprise Manager Cloud Control Console.

Granting Credential Privileges with Enterprise Manager Cloud Control Console

Learn how to grant privileges with Enterprise Manager Cloud Control Console.

To grant credential privileges with Enterprise Manager Cloud Control Console:

1. Login to Enterprise Manager as a super user or `EM_CLOUD_ADMINISTRATOR`.
2. From the Setup menu, select **Security**, then select **Named Credentials**.

   The Named Credentials page is displayed.
3. Select the named credential to be granted, and click **Manage Access**. The Manage Access page for that credential is displayed.
4. Click **Add Grant**.
5. In the pop-up window, select the Oracle Site Guard administrator whom to grant privileges. Then click **Select.**
6. Click **Save** to save the privilege granted to the selected administrator.

Configuring Software Library Storage Location

The Oracle Enterprise Manager Software Library (Software Library) is a repository that stores scripts and artifacts used by Oracle Enterprise Manager and its plug-ins.

This repository includes the scripts required to execute Site Guard operation plans. The storage location for the Software Library needs to be configured only once when you initially install and set up Oracle Enterprise Manager.

For information about the Software Library and how to determine whether a storage location for the Software Library is already configured, see section Configuring a Software Library.

To configure the Software Library storage location, use one of the following methods:

Configuring Software Library Storage Location with Enterprise Manager Cloud Control Console

Learn how to configure the Software Library storage location with Enterprise Manager Cloud Control Console.

To configure the storage location for the Oracle Software Library with Enterprise Manager Cloud Control Console:

> **Note:**
>
> Configuring Oracle Software Library is a one-time process. Enterprise Manager requires you to configure Oracle Software Library before proceeding with any deployment-procedure related tasks. Perform the steps listed in this section after confirming that Oracle Software Library is not already configured.

1. Login to Enterprise Manager as an `EM_CLOUD_ADMINISTRATOR` user.

2. From the Setup menu, select **Provisioning and Patching**, then select **Software Library**.

   The Software Library: Administration page is displayed.

3. Select **OMS Shared File System** from the Storage Type drop-down box.
4. Click **Add**.
5. Specify a name and location that is accessible to all OMS users, and click **OK**.

> **Note:**
>
> As the storage location for the Software Library must be accessible to all OMS as local directories, in a multi-OMS scenario, you must set up a clustered file system using OCFS2 or NFS. For single OMS systems, any local directory is sufficient.

Oracle Enterprise Manager begins execution of a new job to upload Software Library content to the specified location.

> **Note:**
>
> For more information about Software Library, see Configuring Software Library.

Configuring Software Library Storage Location with Enterprise Manager Command-Line Interface

Learn how to configure the Software Library storage location with Enterprise Manager Command-Line Interface (EMCLI).

To configure storage location in the software library for the Oracle Software Library with EMCLI:

```
emcli add_swlib_storage_location
       -name="name_of_software_library"
       -path="path_to_the_software_library_location"
```

Parameter	Description
`name`	The name for the software library.
`path`	The path to the software library location.

For example:

```
emcli add_swlib_storage_location
       -name="Softlib"
       -path="/u01/em/swlib"
```

Verifying Database and Data Guard Configurations

Oracle Site Guard uses Oracle Data Guard to perform database switchover and failover operations. Ensure that Oracle Site Guard can perform database operations during a disaster recovery operation.

To ensure that Oracle Site Guard can perform database operations during a disaster recovery operation:

1. Ensure that Flashback Recovery is configured and enabled on both, the primary and the standby databases. If Flashback is not correctly configured, the standby database will have to be recreated after a failover operation. Whereas if Flashback is correctly configured the standby database can be easily reinstated after a failover operation with Data Guard Broker. Flashback need to be enabled only for failover operations and it is not required for switchovers.
2. Verify the status and its configuration by ensuring that Oracle Data Guard is functional on the primary and standby databases (either single-instance or RAC).
3. Ensure that you can perform Oracle Data Guard switchover and failover operations outside Site Guard (for example, with the `DGMGRL` utility).

4
Configuring Oracle Site Guard

Configure Oracle Site Guard and create your own configuration scripts, auxiliary hosts, and database lag checks.

This chapter includes the following sections:

- Overview
- Configuring Sites
- Updating Site Configuration
- Creating Credential Associations
- Configuring Scripts
- Configuring Auxiliary Hosts
- Configuring Database Lag Checks with EMCLI Commands

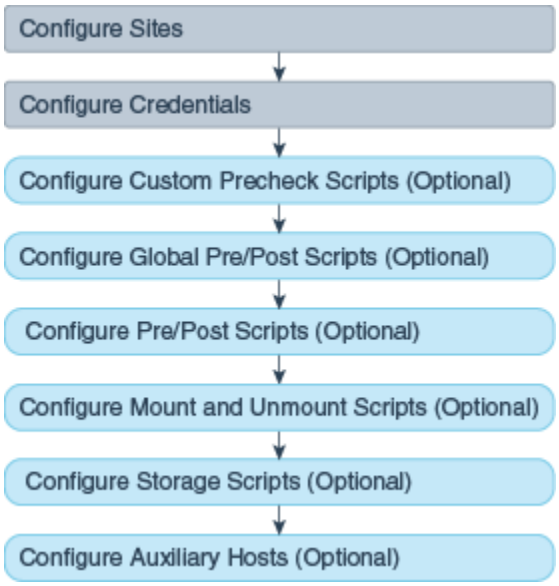
Overview

Configure Oracle Site Guard before creating disaster recovery operation plans.

Before you create an operation plan for disaster recovery, you must configure Oracle Site Guard. All operation plans that you create use this configuration.

Figure 4-1 shows the roadmap for configuring Oracle Site Guard. Steps marked *optional* are required if the site topology and operation plans require a specific type of configuration. However, since most enterprise deployments are large and complex, they typically require all the configuration steps listed in the figure.

Figure 4-1 Workflow of Oracle Site Guard Configuration



> **Note:**
>
> - Before you configure Oracle Site Guard, ensure that you complete the tasks described in Preparing Oracle Site Guard for Operation.
> - You must login using the `EM_SG_ADMINISTRATOR` role privilege to perform configuration tasks. Ensure that you have created the required user credentials as described in Creating Credentials.

Configuring Sites

Configure sites and designate a site as a primary or secondary site.

As the first step towards setting up a disaster recovery operation, you must configure sites and assign roles to those sites. Then you designate a configured site as a primary (production) sites or a standby site.

To configure sites, use one of the following methods:

- Configuring Sites with Enterprise Manager Cloud Control Console
- Configuring Sites with EMCLI Commands
- Configuring Site Properties with EMCLI Commands

Configuring Sites with Enterprise Manager Cloud Control Console

Learn how to configure sites with Enterprise Manager Cloud Control Console.

To create an Oracle Site Guard configuration and to associate a standby system with a primary system with Enterprise Manager Cloud Control Console:

1. Login to Enterprise Manager as an `EM_SG_ADMINISTRATOR` user.
2. From the Targets menu, click **Systems**.

   The Systems page is displayed.
3. Click the name of the system (**Generic System**) for the primary site created as described in Creating Primary and Standby Sites.

   The Generic System page for the primary site is displayed.
4. On the system's home page, from the **Generic System** menu, select **Site Guard** > **Configure**.

   The Site Guard Configuration page is displayed.
5. On the General tab, in the **Standby System(s)** section, click **Add**.

   The Search and Select: Standby Systems page is displayed.
6. Choose the standby system, and click **Select**.
7. Click **Create**. Or, if an Oracle Site Guard configuration already exists, click **Save**.
8. Click **OK** to confirm the action.

   Site Guard saves the standby system configuration.

Configuring Sites with EMCLI Commands

Learn how to use EMCLI commands to configure primary and secondary sites.

To configure primary and standby sites:

> **Note:**
>
> For information about logging in to `emcli`, see EM CLI Overview and Concepts.

```
emcli create_siteguard_configuration
      -primary_system_name="system_name1"
      -standby_system_name="system_name2"
```

Parameter	Description
`-primary_system_name`	Enter the name of your system, which is associated with the primary site.
`-standby_system_name`	Enter the name of your system, which is associated with the standby site.

To display information about the association between configured primary and standby sites:

```
emcli get_siteguard_configuration
        [-primary_system_name="name_of_the_primary_system"]
        [-standby_system_name="name_of_the_standby_system"]
```

> **Note:**
>
> [ ] indicates that the parameter is optional.

Configuring Site Properties with EMCLI Commands

Site Properties allows user to associate user-defined properties to a site. Use Site Properties to group and search for sites that share common attributes. Each property consists of a name and value associated with a site. Site Properties is an EMCLI-only feature.

To configure a Site Property:

> **Note:**
>
> For information about logging in to `emcli`, see EM CLI Overview and Concepts.

```
emcli add_site_properties
      -system_name="Name of the system (site)"
      -properties="property name=value pairs separated by ;"
```

Parameter	Description
`-system_name`	Name of the generic system (site).
`-properties`	Semicolon (;) separated list of property name=value pairs to be added to the site.

To list Site Properties , or list sites that match the specified property names and values:

```
emcli get_site_properties
         -system_name="Name of the system (site)"
            -properties="property names list or name=value pairs separated by ;"
```

Parameter	Description
`-system_name`	Name of the generic system (site).
`-properties`	Semicolon (;) separated list of property names or name=value pairs to search for.

For more information on how to update or delete a Site Property, see Oracle Site Guard Command Line Interface .

Updating Site Configuration

Designate the role of a site as Primary, Standby, or Validate Standby site with EMCLI commands or Enterprise Manager Cloud Control Console.

You can update the role of a site after a site has been created and set it up as a primary or standby site. In this way, you designate a site's role as *Primary*, *Standby*, or *Validate Standby*. This is useful when you have performed actions outside Oracle Site Guard that modify or reverse the roles of sites in a Site Guard configuration and you want to update the Oracle Site Guard configuration to correctly reflect the site's new role.

You can update a site configuration using Enterprise Manager Cloud Control Console or EMCLI commands:

Updating Site Configuration with Enterprise Manager Cloud Control Console

Learn how to update the role of a site with Enterprise Manager Cloud Control Console.

To update a site's role with Enterprise Manager Cloud Control Console:

1. Login to Enterprise Manager as an `EM_SG_ADMINISTRATOR` user.
2. From the Targets menu, click **Systems.**

   The Systems page is displayed.
3. Click the name of the system (**Generic System**) for the standby site created as described in Creating Primary and Standby Sites.

The Generic System page for the standby site is displayed.

4. On the system's home page, from the **Generic System** menu, select **Site Guard** > **Configure**.

   The Site Guard Configuration page is displayed.

5. On the General tab, click the **Set as Primary** button on the upper right.

6. Click **Yes** to acknowledge the confirmation dialog.

   This designates the standby site as the new primary site and will automatically designate it's paired primary site as the new standby site. Effectively, the site roles are reversed.

> **Note:**
>
> Reversing site roles cancels all configured health checks for the sites involved in the role reversal.

Updating Site Configuration with EMCLI Commands

Learn how to update the role of a site with EMCLI commands.

> **Note:**
>
> For information about logging in to the Enterprise Manager Command-Line Interface, see *Oracle Enterprise Manager Command Line Interface Guide*.

To update a site's role, use the `update_siteguard_configuration` EMCLI command:

1. Login to `emcli`.

2. Run the `update_siteguard_configuration` command:

```
emcli update_siteguard_configuration
      -primary_system_name="system_name1"
      -standby_system_name="system_name2"
      -reverse_role="flag specifying whether system roles should be reversed"
      -role="new role of the standby system"
```

Parameter	Description
`-primary_system_name`	The name of your system associated with the primary site.
`-standby_system_name`	The name of your system associated with the standby site.
`-reverse_role`	Reverse roles between primary and standby systems. Optional. If this option is specified, only one standby system can be specified in the `-standby_system_name` parameter.

Parameter	Description
`-role`	The new role for the site. Optional. Specify one of the following: • *Primary* - the roles of the primary and standby are swapped. • *Standby* - the role of the standby site is changed from ValidateStandby to Standby. • *ValidateStandby* - the role of the standby site is changed from Standby to ValidateStandby.

Creating Credential Associations

Credentials are associated with targets and used by Oracle Site Guard operation plans when they are executing.

The credentials to associate are the ones that you created in Creating Credentials.

> **Note:**
>
> - If you are using Named Credentials or Preferred Credentials, ensure that you have created all the necessary credentials for managing targets as described in Creating Credentials.
> - Ensure that you have created a user with `EM_SG_ADMINISTRATOR` privileges, as described in Creating Oracle Site Guard Administrator Users, and granted credential privileges to that user as described in Granting Credential Privileges to Oracle Site Guard Administrator Users.

You must set up named or preferred credential associations for the following targets:

- Each host, where Oracle Fusion Middleware and Oracle Database are installed and configured (for normal user and users with root privileges)
- Oracle WebLogic Administration Server
- Oracle Database
- Oracle WebLogic Node Manager

To associate credentials to targets, use any of the following tasks:

Creating Named or Preferred Credential Associations

Credentials must be created and associated with targets, such as Oracle WebLogic Servers, hosts where Oracle Fusion Middleware is installed, Oracle Databases, and Oracle WebLogic Node Manager.

To create named or preferred credential and to associate it with a target, use one of the following methods:

- Creating Named or Preferred Credential Associations with Enterprise Manager Cloud Control Console

- Creating Named or Preferred Credential Associations with EMCLI Commands

Creating Named or Preferred Credential Associations with Enterprise Manager Cloud Control Console

Learn how to create a named or preferred credential association with Enterprise Manager Cloud Control Console.

To create and associate credentials with Enterprise Manager Cloud Control Console:

1. Login to Enterprise Manager as an `EM_SG_ADMINISTRATOR` user.
2. From the Targets menu, click **Systems**.
3. On the Systems page, click the name of the system for which you want to configure credential associations.
4. On the system's home page, from the Generic System menu, select **Site Guard** > **Configure**.
5. Click the **Credentials** tab.

   Associate the different types of credentials as described:

   Associate Normal Host Credentials

   Associate normal host credentials to run specific commands or scripts on the target host.

   To associate normal host credentials, follow these steps:

   a. In the Credential tab, in the **Normal Host Credentials** section, click **Add**.

      The Add Normal Host Credentials dialog appears.

   b. Select the target for which you want to associate normal host credentials. Select **All** to select all the systems in the list.

      You can select the credentials set, by default, by selecting the **Preferred** option on the page. On selecting **Preferred**, the Named Credentials section is disabled. To select named credentials, deselect Preferred.

   c. Click **Save**.

   Associate Privileged Host Credentials

   Associate privileged host credentials to mount or unmount storage on the target host.

   To associate privileged host credentials, follow these steps:

   a. In the Credential tab, in the **Privileged Host Credentials** section, click **Add**.

      The Add Privileged Host Credentials dialog appears.

   b. Select the target for which you want to associate privileged host credentials. Select **All** to select all the targets in the list.

      You can select the credentials set, by default, by selecting the **Preferred** option on the page. On selecting **Preferred**, the Named Credentials section is disabled. To select named credentials, deselect **Preferred**.

   c. Click **Save**.

   Associate Oracle Node Manager Credentials

Associate Oracle Node Manager credentials to connect node manager targets. You must associate Oracle Node Manager credentials for each site that has a Oracle Weblogic Server target.

To associate Oracle Node Manager credentials, follow these steps:

a. In the Credential tab, in the **Oracle Node Manager Credentials** section, click **Add**.

   The Add Oracle Node Manager Credentials dialog appears.

b. Select the target host for which you want to associate Oracle Node Manager credentials. Select **All** to select all the target hosts in the list.

   You can select the credentials set, by default, by selecting the **Preferred** option on the page. On selecting **Preferred**, the Named Credentials section is disabled. To select named credentials, deselect **Preferred**.

c. Click **Save**.

Associate Oracle WebLogic Administration Credentials

Associate Oracle WebLogic Administration credentials to connect to the administration server, or to start or stop managed servers.

To associate Oracle WebLogic administration credentials, follow these steps:

a. In the Credential tab, in the **Oracle WebLogic Administration Credentials** section, click **Add**.

   The Add Oracle WebLogic Administration Credentials dialog appears.

b. Select the target for which you want to associate Oracle WebLogic administration credentials. Select **All** to select all the targets in the list.

   You can select the credentials set, by default, by selecting the **Preferred** option on the page. On selecting **Preferred**, the Named Credentials section is disabled. To select named credentials, deselect **Preferred**.

c. Click **Save**.

Associate SYSDBA Database Credentials

Associate SYSDBA database credentials to perform switchover or failover operations through Data Guard Broker.

To associate database credentials, follow these steps:

a. In the Credential tab, in the **SYSDBA Database Credentials** section, click **Add**.

   The Add Database Credentials dialog appears.

b. Select the target for which you want to associate SYSDBA Database credentials. Select **All** to select all the targets in the list.

   You can select the credentials set, by default, by selecting the **Preferred** option on the page. On selecting **Preferred**, the Named Credentials section is disabled. To select named credentials, deselect **Preferred**.

c. Click **Save**.

Creating Named or Preferred Credential Associations with EMCLI Commands

Learn how to create named or preferred credential associations with EMCLI commands.

> **Note:**
>
> For information about logging in to the Enterprise Manager Command-Line Interface, see *Oracle Enterprise Manager Command Line Interface Guide*.

To create named or preferred credential associations for targets, use the `create_siteguard_credential_association` EMCLI command:

```
emcli create_siteguard_credential_association
         -system_name="name_of_the_system"
         [-target_name="name_of_the_target"]
         -credential_type="type_of_credential"
         [-credential_name="name"]
         [–use_preferred_credential="true_or_false"]
         -credential_owner="owner"
```

> **Note:**
>
> [ ] indicates that the parameter is optional.

Parameter	Description
`-system_name`	The name of the system.
`-target_name`	The name of the target. This parameter is optional and required to associate the credential with a specific target only.
`-credential_type`	The type of the credential. Example: `HostNormal`, `HostPrivileged`, `NodeManager`, `WLSAdmin`, or `DatabaseSysdba`.
`-credential_name`	The name of the credential. If the value for `credential_name` is not specified, then `use_preferred_credential` has to be set to `true`.
`-credential_owner`	The owner of the credential.
`–use_preferred_credential`	If you are using Preferred Credentials, then specify `true`. The default value is `false`. If you do not specify the use of preferred credentials, then to use named credentials you must specify the `credential_name` parameter.

Configuring Scripts

Oracle Site Guard provides a mechanism for you to configure scripts for managing disaster recovery operations.

Depending on their function, these scripts either come bundled with Oracle Site Guard, or you can be provided them. You must configure these scripts while configuring Oracle Site Guard. Note that you must add these scripts to the Enterprise Manager software library so that they can be automatically staged (deployed) on the hosts

where they need to run. Scripts that are not part of the software library are manually staged (deployed) on each host where they are defined to run.

You can configure the following scripts with Oracle Site Guard:

- Custom Precheck Scripts

  Custom Precheck scripts are used to extend the Precheck and Health Check functionality that Oracle Site Guard provides. For information about Precheck and Health Check functionality of Oracle Site Guard, see Extensibility.

- Pre Scripts, Post Scripts, Global Pre Scripts, and Global Post Scripts

  Pre scripts, Post Scripts, Global pre scripts, and Global Post Scripts are used for extending the functionality of Oracle Site Guard when executing operation plans. For more information on various scripts, see Extensibility.

- Mount and Unmount scripts

  Mount and Unmount scripts as described in Storage Integration, are needed for Filesystem mount and unmount operations that are performed during operations. You can use the `mount_unmount.sh` script or provide your own scripts.

- Storage scripts

  Storage scripts as described in Storage Integration, are needed for storage management that must be performed during operations. You can use the scripts bundled with Oracle Site Guard or provide your own scripts.

> **Note:**
>
> - A user-defined script must be an executable script, and must have clearly defined return codes. The script must return `0` on success, and non-zero values on failure.
> - Ensure that you configure the required privileges to run all user-defined scripts.

The following topics explain how to configure different kinds scripts:

Configuring Custom Precheck Scripts, Pre Scripts, Post Scripts, Global Pre Scripts, and Global Post Scripts

Learn how to customize pre and post checks.

The following attributes are available for customizing a Pre Script, Post Script, Global Pre Script, and Global Post Script:

Parameter	Description
script path	The location where the script resides. Note that the script must reside at the same path location on each host specified in the `target hosts` parameter.
software library path (component)	Path to the entity in software library. If component is specified, path should contain only the file name and its parameters. This parameter is optional.

Parameter	Description
target hosts	The list of hosts where the script will run.
run on	Whether the script should run on `Any` or `All` of the hosts specified in the `target hosts` parameter. The first available host in the `target_hosts` list is chosen. `Any` executes the script on any one of the available hosts specified in the `target_hosts` parameter. `All` executes the script on each and every host specified in the `target_hosts` parameter.
operation type	The operation type that the script is configured for (switchover, failover, start, or stop).
role	The role of the site during which the script will run (primary or standby). For example, a script configured for a `primary` role will only run when the site has a primary role.
runtime	Whether the script is a runtime script. Runtime scripts are not expected to be available before operation execution begins. Using this flag tells Site Guard not to check for the script existence during the Precheck phase.
credential type	The type of credential to use to execute the script on the specified hosts (Normal Host Credentials or Privileged Host Credentials). For information about various types of credentials, see Creating Credential Associations.
credential parameters	One or more sets of credentials to pass to the script. This option is only available in the Cloud Control Console. To configure credential parameters with EMCLI, use the command `add_siteguard_script_credential_params`.

To configure Custom Precheck Scripts, Pre Scripts, Post Scripts, Global Pre Scripts, and Global Post Scripts use any of the following tasks:

- Configuring Custom Precheck Scripts, Pre Scripts, Post Scripts, Global Pre Scripts, and Global Post Scripts with Enterprise Manager Cloud Control Console
- Configuring Custom Precheck Scripts, Pre Scripts, Post Scripts, Global Pre Scripts, and Global Post Scripts with EMCLI Commands

Configuring Custom Precheck Scripts, Pre Scripts, Post Scripts, Global Pre Scripts, and Global Post Scripts with Enterprise Manager Cloud Control Console

Learn how to configure pre and post scripts for the primary site.

To configure Pre Scripts, Post Scripts, Global Pre Scripts, and Global Post Scripts for the primary site:

1. Login to Enterprise Manager as an `EM_SG_ADMINISTRATOR` user.
2. From the **Targets** menu, click **Systems**.

The Systems page is displayed.

3. Select the system name (**Generic System**) for which the script must be configured.

   The Generic System page for that site is displayed.

4. Click **Generic System** > **Site Guard** > **Configure**.

   The Site Guard Configuration page is displayed.

5. Click the **Pre/Post Scripts** tab.

6. Click **Add**.

   The **Add Pre/Post Scripts** page is displayed.

7. Enter the following details:

   - **Software Library Path**: Enter the path to the software library entity that contains the script. Alternately, browse for the entity in the software library by clicking on the icon. This only applies if the script has already been added to the Enterprise Manager software library.

     The entity in the Software Library must be present in a folder which is not locked. The symbol, indicates that the folder is locked.

   - **Script Path**: Enter the path to the script, or click the search icon and browse the Filesystem for the script. You can also browse Filesystems on the remote host after specifying the login credentials.

   - **Target Host**s: Select one or more target hosts, or select **All** to configure the script to run on all hosts.

   - **Script Type**: Select one of the following options depending on the type of script being configured:

     – **Custom Precheck Script**

     – **Pre Script**

     – **Post Script**

     – **Global Pre Script**

     – **Global Post Script**

   - **Operation Type**: The operation during which this script will run. Choose from the options - **Switchover**, **Failover**, **Start**, **Stop, Open for Validation**, or **Revert to Standby**.

   - **Role**: Select **Primary**, **Standby**, or **Stanby (Open for Validation)** based on the system role. The script only runs when the system has the specified role.

> **Note:**
>
> For **Global Pre-Script** and **Global Post-Script** script types, the site **Role** cannot be changed.
>
> For **Pre-Script**, **Post-Script** and **Custom Precheck Script** the **Role** cannot be changed when the operation type is **Start** or **Stop**.

- To configure additional options, click the arrow next to **Advanced Options** region. The following advanced options are available:
  - **Runtime Script**: Select if this is a Runtime script that will only be available during operation execution. Normally, scripts that are part of the Software Library should be designated as Runtime scripts, however any user script may be designated a Runtime script.

    Note that during a Precheck or Health Check, Oracle Site Guard checks the existence of runtime scripts that have been added to the Software Library. However, if the scripts are not part of the Software Library, Oracle Site Guard does not check for their existence before an operation plan is executed
  - **Run On**: Select **All Hosts** to run the script on all selected hosts, or to run the script on any one of the selected target hosts, select **Any Host**.
- **Credential Type**: Select one of the following credential types for executing the script:
  - **Normal Host Credentials**

    Select the Normal (non-root) privileges configured for the script host
  - **Privileged Host Credentials**

    Select the Privileged (root) privileges configured for the script host
  - **Custom Host Credentials**

    Select an alternate set of named credentials. If this option is chosen, select the named credential from the Named Credential drop-down menu.
- **Named Credential**: Select the named credential to use when executing the script. This selection is only applicable if **Credential Type** is set to **Custom Host Credentials**.
- **Credential Parameters**: Select one or more configured credentials to pass as parameters to this script. To select the credentials to pass to the script, move those credentials from the **Available Values** column to the **Selected Values** column. The selected credential parameters will be passed to this script in the order selected. This credential order is important for scripts that expect a list of credentials in a specified order.

8. Click **Save**.

Configuring Custom Precheck Scripts, Pre Scripts, Post Scripts, Global Pre Scripts, and Global Post Scripts with EMCLI Commands

Learn how to configure pre and post scripts with EMCLI commands.

To configure Pre Scripts, Post Scripts, Global Pre Scripts, and Global Post Scripts with EMCLI commands:

```
emcli create_siteguard_script
         -system_name=name_of_the_system
         -operation=name_of_the_operation
         -script_type=type_of_the_script
         [-host_name=name_of_the_host_where_the_scripts_are_run]
         -path=path_of_the_script
         [-component="path_of_the_entity_in_software_library"]
         [-
```

```
runtime_script="flag_to_specify_if_prechecks_to_check_availability_of_this_script
"]
        [-run_on=flag_specifying_the_host]
        [-all_hosts=flag_to_run_script_on_all_the_hosts_in_the_system]
        [-role=role_associated_with_the_system]
        [-credential_type=type_of_the_credential]
        [-credential_name="name_of_the_credential"]
        [-credential_owner=credential_owner]
```

Note:

- A parameter enclosed in [ ] indicates that the parameter is optional.
- You can specify the `-host_name` parameter more than once.
- Specifying the value `true` for the parameter `-all_hosts=true` overrides any host selected using the `-host_name` option.

Parameter	Description
`-system_name`	The name of the system.
`-operation`	The name of the operation: `Switchover`, `Failover`, `Start`, `Stop`, `Open for Validation`, or `Revert to Standby`.
`-script_type`	The type of the script. It can be `Custom Precheck Script`, `Global-Pre-Script, Global-Post-Script, Pre-Script`, or `Post-Script`.
`-host_name`	The name of the host where this script will be executed. This parameter is optional and can be specified more than once.
`-path`	The path to the script.
`-component`	The path to the entity in the software library. If component is specified, path should contain only the file name and its parameters. This parameter is optional.
`-runtime_script`	The value as `true` or `false`. If the script is designated as a runtime script, Precheck will not verify the existence of script. This parameter is used when the script is dynamically mounted or generated as part of execution of operation plan. By default, all scripts staged from the software library are designated as runtime scripts. The default value for scripts that are not staged from software library is `false`. This parameter is optional.
`-run_on`	Whether the script needs to be executed on only one of the available hosts (enter `any`) or on all hosts (enter `all`). This parameter is optional and default value is all.
`-all_hosts`	Optional flag to allow the script to run on all the hosts in the system. This parameter overrides the `host_name`. Enter `true` or `false`.

Parameter	Description
`-role`	Optional flag to configure script based on the system role. By default, the script is configured for both primary and standby roles for a given system. For example: `Primary` or `Standby`.
`–credential_type`	`HostNormal` or `HostPrivileged` if you have `root` privileges.
`-credential_name`	The name of the credential that is used to execute this script. If the value for the parameter `credential_name` is not specified, then the value for the parameter `credential_type` needs to be specified.
`-credential_owner`	The owner of the credential. If `target_storage_credential_name` and `source_storage_credential_name` are specified then the attribute `credential_owner` must be specified. This argument need not be specified if the owner of the credential is same as logged in user.

Note:

- `[ ]` indicates that the parameter is optional.
- You may specify the option `host_name` more than once.
- `-all_hosts=true` overrides any hosts specified with the `-host_name` option.
- The `-role` option is only applicable for Pre-Script or Post-Script.

To pass credentials to a script, first configure the script and then configure the credentials to pass as parameters, as described in Configuring Credentials as Parameters for Scripts.

Configuring Mount and Unmount Scripts

The mount and unmount scripts are scripts used in storage operations to mount and unmount file systems.

These scripts are storage scripts that come in two flavors:

- **Bundled**

  Oracle Site Guard provides a bundled script for handling file system mount and unmount operations. The `mount_umount.sh` script is part of the Enterprise Manager Software Library. Oracle Site Guard automatically deploys bundled scripts on all hosts on which the scripts are defined to run.

- **User-defined**

  You can define your own custom script for the Filesystem mount and unmount operations.

You can add your own scripts to the Enterprise Manager software library. If you do this, Oracle Site Guard will deploy your scripts to all configured hosts at runtime. This is similar to how Oracle Site Guard automatically deploys bundled scripts such as `mount_umount.sh`. However, if your scripts are not part of the software library, then you must deploy them on all hosts where they need to run.

To mount and unmount file systems, you can use the following bundled script:

mount_umount.sh

Learn how to use the `mount_umount.sh` script to mount or unmount file systems and directories.

The script has the following syntax:

```
sh mount_umount.sh [-o operation_type ][-f directories_to_mount_or_unmount]
```

> **Note:**
>
> - If there are multiple directories to be mounted or unmounted, use commas to separate the directories. Ensure that there are no spaces between the directory names.
> - Ensure that the `/etc/fstab` file is updated with the entries that you want to mount or unmount.
> - Ensure that you have the privileges to mount or unmount Filesystems.

To mount multiple directories:

```
sh mount_umount.sh -o mount -f '/u02/oracle/config,/u02/oracle/product,/u02/
oracle/stage'
```

To mount a single directory:

```
sh mount_umount.sh -o mount -f /u01/app/oracle/product/test
```

To unmount multiple directories:

```
sh mount_umount.sh -o umount -f '/u02/oracle/config,/u02/oracle/product,/u02/
oracle/stage'
```

To unmount a single directory:

```
sh mount_umount.sh -o umount -f /u01/app/oracle/product/test
```

To configure mount or unmount scripts, use one of the following options:

- Configuring Mount or Unmount Scripts with Enterprise Manager Cloud Control Console
- Configuring Mount or Unmount Scripts with EMCLI Commands

Configuring Mount or Unmount Scripts with Enterprise Manager Cloud Control Console

Learn how to configure mount and unmount scripts with Enterprise Manager Cloud Control Console.

> **Note:**
>
> For information about logging in to the Enterprise Manager Command-Line Interface, see *Oracle Enterprise Manager Command Line Interface Guide*.

To configure a mount or unmount script with Enterprise Manager Cloud Control Console:

1. Login to Enterprise Manager as an `EM_SG_ADMINISTRATOR` user.
2. From the **Targets** menu, click **Systems**.

   The Systems page is displayed.
3. Select the system name (**Generic System**) on which the script must be configured.

   The Generic System page for that site is displayed.
4. Click **Generic System** > **Site Guard** > **Configure**.

   The Site Guard Configuration page is displayed.
5. Click the **Storage Scripts** tab.
6. Click **Add**.

   The **Add Storage Scripts** page is displayed.
7. Enter the following details:
   - **Software Library Path**: Enter the path to the software library entity that contains the script. Alternately, browse for the entity in the software library by clicking the search icon. This only applies if the script has already been added to the Enterprise Manager software library.
   - **Script Path**: the bundled `mount_umount.sh` script with the appropriate options (see mount_umount.sh), or provide a path to your own user-defined script.

     To enter a user-defined script you can click the search icon, and browse the Filesystem. You can also browse Filesystems on the remote host after specifying login credentials.
   - **Target Hosts**: Select one or more target hosts, or select **All** to configure the script to run on all hosts.
   - **Script Type**: Select one of the following options:
     - **Mount**
     - **UnMount**
   - **Run On**: This option is disabled. The value is set to **All Hosts**.
   - **Operation Type**: The operation during which this script will run. Choose from the options - **Switchover**, **Failover**, **Open for Validation**, or **Revert to Standby**.
   - To configure additional options, click the arrow next to **Advanced Options** region. The following advanced options are available:
     - **Runtime Script**: Select whether this is a Runtime script that will only be available during operation execution. Normally, scripts that are part of the

Software Library should be designated as Runtime scripts, however any user script may be designated a Runtime script.

> **Note:**
>
> During a Precheck or Health Check, Oracle Site Guard checks the existence of runtime scripts that have been added to the Software Library. However, if the scripts are not part of the Software Library, Oracle Site Guard does not check for their existence before an operation plan is executed.

- **Credential Type**: Select one of the following credential types while executing the script:
  - **Normal Host Credentials**: Select these credentials to use the Normal (non-root) privileges configured for that script host.
  - **Privileged Host Credentials**: Select these credentials to use the Privileged (`root`) privileges configured for that script host.
  - **Custom Host Credentials**: Select these credentials to use an alternate set of named credentials. If this option is chosen, select the named credential from the Named Credential drop-down menu.
- **Named Credential**: the named credential to be used when executing the script. This selection is only applicable if **Credential Type** is set to **Custom Host Credentials**.
- **Credential Parameters**: Select one or more configured credentials to be passes as parameters for this script. To select the credentials to be passed to the script, move those credentials from the Available Values column to the Selected Values column.

8. Click **Save**.

Configuring Mount or Unmount Scripts with EMCLI Commands

Learn how to configure mount and unmount scripts with EMCLI commands.

> **Note:**
>
> For information about logging in to the Enterprise Manager Command-Line Interface, see *Oracle Enterprise Manager Command Line Interface Guide*.

To configure a mount or unmount script use, the `create_siteguard_script` EMCLI command:

```
emcli create_siteguard_script
        -system_name="system_name"
        -operation="operation_name"
        -script_type="type_of_script"
        [-host_name="name_of_the_host"]
        -path="path_of_the_script"
        [-component="path_of_the_entity_in_software_library"]
        [-
```

```
runtime_script="flag_to_specify_if_prechecks_should_check_availability_of_this_sc
ript"]
        [-run_on="flag_specifying_hosts_that_will_run_the_script"]
        [-all_hosts="flag_to_run_the_script_on_all_the_hosts_on_the_system"]
        [-role="role_associated_with_the_system"]
        [-credential_type="type_of_credential"]
        [-credential_name="name_of_the_credential"]
        [-target_storage_credential_name="target_storage_credential"]
        [-source_storage_credential_name="source_storage_credential"]
        [-credential_owner="credential_owner"]
```

Note:

[ ] indicates that the parameter is optional.

Parameter	Description
`-system_name`	The system for which the script is being configured.
`-operation`	The function of the operation. Example: `Switchover`, `Failover`, `Open for Validation`, or `Revert to Standby`.
`-script_type`	The type of script. Depending on the function you want to perform, enter one of the following options: • Mount • UnMount
`-host_name`	The name of the host where the script will be run. To specify a list of hosts, separate host names with semi-colons, or provide the `-host_name` option multiple times. **Note**: Ensure that all hosts are part of the system specified in `system_name`.

Parameter	Description

`-path`	Enter the path to the script.
	If you are configuring the bundled `mount_umount.sh` script specify the path as described in `mount_umount.sh`.
	For example:
	`sh mount_umount.sh -o mount -f /u02/oracle/config,/u02/oracle/product,/u02/oracle/stage`
	If you are configuring a user-defined script that you have added to the Enterprise Manager software library, provide only the name of the script and any additional arguments that the script requires.
	For example:
	`sh example_script.sh -a value1 -b value2 -c value3`
	If you are configuring a user-defined script that you will deploy on all the configured hosts, provide the full path to the script location and any additional arguments that the script requires.
	Note: The script must reside at the same path location on each host.
	For example:
	`/path_to_the_script/example_script.sh -a value1 -b value2 -c value3`

`-component`	The path to the entity in the software library. If the component is specified, the `-path` option should contain only the script name and its parameters.
`-runtime`	Whether the script is a runtime script. If the script is a runtime script, Prechecks will not verify the existence of script. This option can be used when the script is dynamically mounted or generated as part of execution of operation plan. By default, all scripts staged from the software library are designated as runtime scripts. For scripts that are not staged from the software library, the default value is `false`.
`-run-on`	Whether the script needs to be executed on only one of the available hosts (enter `any`) or on all hosts (enter `all`).
`-all_hosts`	Optional flag to enable the script to run on all the hosts in the system. This parameter overrides the `-host_name` parameter.
`-role`	This option is not applicable for scripts of type `Mount` and `UnMount`.
`-credential_type`	`HostNormal` credentials or `HostPrivileged` credentials for users with `root` privileges. If values for `credential_type` are not specified, then the values for `credential_name` must be specified.

Parameter	Description
`-credential_name`	An alternate named credential to use when executing this script. If the values for `credential_name` are not specified, then the values for `credential_type` must be specified.
`-credential_owner`	The owner of the credential. This argument need not be specified if the owner of the credential is same as logged in user.

To pass credentials to a script, first configure the script and then configure the credentials you want to pass as parameters as described in Configuring Credentials as Parameters for Scripts .

Configuring Storage Scripts

Storage scripts are used in Storage Switchover and Storage Failover operations.

There are two types of storage scripts:

- **Bundled**

  Oracle Site Guard provides a bundled script for handling Filesystem mount and unmount operations. The script, `zfs_storage_role_reversal.sh`, is part of the Enterprise Manager Software Library. Oracle Site Guard automatically deploys bundled scripts on all hosts on which the scripts are defined to run.

- **User-defined**

  You can define your own custom script for the Filesystem mount and unmount operations.

  You can add your own scripts to the Enterprise Manager software library. If you do this, Oracle Site Guard will deploy your scripts to all configured hosts at runtime. This is similar to how Oracle Site Guard automatically deploys bundled scripts like `zfs_storage_role_reversal.sh`. However, if your scripts are not part of the software library, you must deploy them on all hosts where they need to run.

  When configuring replication between ZFS storage appliances for a Site Guard disaster recovery configuration, follow these guidelines:

  – Ensure that you do not use private interface names as source and target appliance parameters when configuring the Site Guard ZFS storage role reversal script.

  – When replicating to a target appliance from a clustered source appliance, configure replication on each head of the source appliance head using different replication targets.

  – During replication configuration both source cluster heads should be in a `CLUSTERED` state (not `STRIPPED` for example).

  – Do not use private interfaces for replication configuration. Creating static routes and verifying them on the source and target before setting up replication configuration will ensure that you use public interfaces, not private interfaces.

  – Ensure that storage pools and IP addresses maintain their cluster node assignment.

You can configure storage scripts by performing one of the following tasks:

- zfs_storage_role_reversal.sh
- Configuring Storage Scripts with Enterprise Manager Cloud Control Console
- Configuring Storage Scripts with EMCLI Commands

zfs_storage_role_reversal.sh

The `zfs_storage_role_reversal.sh` script is a script used to perform role-reversal operations.

This script comes bundled with Oracle Site Guard and can be used to perform storage role-reversal operations as part of a switchover or failover operation plan.

> **Note:**
>
> The ZFS administrator account used for performing storage operations must have the following roles granted for the ZFS pool or project that is part of the Site Guard disaster recovery operation:
>
> - `rrsource`— a role that allows administrators to create, edit, and destroy replication targets and actions, and send and cancel updates for replication actions.
> - `rrtarget`— a role that allows administrators to manage replicated packages, including disabling replication at the package level, cloning a package or its members, modifying properties of received datasets, and severing or reversing replication. Other authorizations may be required for some of these operations, such as setting properties or cloning individual shares. See the available authorizations in the Projects and Shares scope for details.
> - `destroy`— a role that you can configure at the project or pool level. Either level will work provided you assign it the pool or project being reversed. This role allows deleting an empty project right before attempting 'confirm reverse' on a package on the target appliance.
> - `rename`— a role you can configure at the project or pool level. Either level will work provided you assign it to the pool or project being reversed. This role allows renaming non-empty project right before attempting 'confirm reverse' on a package on the target appliance.
> - `changeProtocolProps`— this role is optional. If assigned, the scope must be `sas` and there must not be any further filters.
>
> Configure these roles with the ZFS appliance BUI or with EMCLI commands.

Run the bundled `zfs_storage_role_reversal.sh` script:

```
zfs_storage_role_reversal.sh  [options]
```

The operation types available are:

- `switchover`
- `switchover_prechecks`

- failover
- failover_prechecks
- create_clone
- create_clone_prechecks
- delete_clone
- delete_clone_prechecks

Option	Description	Mandatory?
--use_default_zfs_lag or -i	Maximum ZFS Lag will be calculated based on replication schedule.	No
--target_appliance or -t	The host name of the target ZFS appliance. For example: zfssite1.example.com	Yes
--target_user or -w	The username on the target ZFS appliance with privileges to execute the script. If not specified, the username of the user executing the script will be used. For example: root	No
--source_appliance or -h	The host name of the source ZFS appliance. For example: zfsite2.example.com	Yes
--source_user or -u	The user name on the source ZFS appliance with privileges to execute the script. If not specified, the user name of the user executing the script will be used. For example: root.	No
--project_name or -j	The name of the replicated ZFS project. For example: ZFS-DR-Project.	Yes
--target_pool_name or -p	The name of the storage pool on the target ZFS appliance. For example: zfssite1-pool-0	Yes
--source_pool_name or -q	The name of the storage pool on the source ZFS appliance. For example: zfssite2-pool-0	Yes
--operation_type or -o	The operation for which this script is being configured. For example: switchover, switchover_prechecks, failover, failover_prechecks, create_clone, create_clone_prechecks, delete_clone, or delete_clone_prechecks.	Yes

Option	Description	Mandatory?
`--is_sync_needed or -c`	Whether the replication package should be updated or synchronized before starting the role reversal. Applicable values are `Y` or `N`. If not provided, the default value is `Y` for switchover and `N` for failover operations.	No
`--continue_on_sync_failure or -f`	Whether the role reversal should continue if the update or synchronization fails. Applicable values are `Y` or `N`. This option only applies if the parameter `-is_sync_needed` is enabled.The default value is `N`.	No
`--sync_timeout or -e`	The timeout value (in seconds) before declaring that the update or synchronization has failed. This option only applies if `-is_sync_needed` is enabled. For example: `600` (equivalent to ten minutes)	No
`--keep_log_file` or `-l`	Whether the script should send output to a log file. Applicable values are `Y` or `N`. If not specified, the default is `N` (no log output will be sent to log file).	No
`--zfs_lag_in_seconds` or `-z`	The ZFS replication lag threshold value (in seconds). If the replication lag exceeds this value, do not reverse storage roles.Example: `300` (equivalent to five minutes). If --is_sync_needed is enabled, zfs lag will still be calculated but will not be enforced.	No
`--is_source_reachable` or `-x`	Whether Site Guard should check whether the source appliance is reachable. This option only applies to the failover case and should be used to prevent the script from trying to check source appliance reachability. Applicable values are `Y` or `N`. If not specified, the default value is `Y`.	No
`--source_user_equivalence` or `-m`	The SSH user name to use when establishing an SSH connection to the source appliance. If this is not specified, the script attempts an SSH connection without specifying an alternate user name. For example: `--source_user_equivalence user1`	No

Option	Description	Mandatory?
`--target_user_equivalence` or `-n`	The SSH username to use when establishing an SSH connection to the target appliance. If this is not specified, the script attempts an SSH connection without specifying an alternate username. For example: `--target_user_equivalence user2`	No

To configure storage scripts, use one of the following options:

- Configuring Storage Scripts with Enterprise Manager Cloud Control Console
- Configuring Storage Scripts with EMCLI Commands

Configuring Storage Scripts with Enterprise Manager Cloud Control Console

Learn how to configure storage scripts with Enterprise Manager Cloud Control Console.

To configure storage scripts with Enterprise Manager Cloud Control Console:

1. Login to Enterprise Manager as an `EM_SG_ADMINISTRATOR` user.
2. From the **Targets** menu, click **Systems**.

   The Systems page is displayed.
3. Select the system name (**Generic System**) on which the script must be configured.

   The Generic System page for that site is displayed.
4. Click **Generic System** > **Site Guard** > **Configure**.

   The Site Guard Configuration page is displayed.
5. Click the **Storage Scripts** tab.
6. Click **Add**.

   The **Add Storage Scripts** page is displayed.
7. Enter the following details:
   - **Software Library Path**: The path to the software library entity that contains the script. Alternately, browse for the entity in the software library by clicking the search icon. This only applies if the script has already been added to the Enterprise Manager software library.
   - **Script Path**: The bundled `zfs_storage_role_reversal.sh` script with the appropriate options (see zfs_storage_role_reversal.sh), or provide a path to your own user-defined script. To browse for a user-defined script you can click the search icon and browse the Filesystem. You can also browse Filesystems on the remote host after specifying login credentials.

     For example:

```
sh zfs_storage_role_reversal.sh -t zfssite1.mycompany.com -h
zfssite2.mycompany.com -j ZFS-DR-Project -p zfssite1-pool-0 -q zfssite2-
pool-0 -c N -f Y -z 300 -l Y -o switchover
```

- **Target Hosts**: Select one or more target hosts, or select **All** to configure the script to run on all hosts.
- **Script Type**: Select one of the following options depending on the function that Oracle Site Guard needs to perform:
  - **Storage Switchover**
  - **Storage Failover**
  - **Storage CreateClone**
  - **Storage DeleteClone**
- **Operation Type**: The operation during which this script will run. Selecting the **Script Type** automatically sets the **Operation Type**. This field cannot be modified.
- **Run On**: For mount or unmount operations this field is automatically set to **All Hosts**. For storage scripts, this field is automatically set to **Any Host**. This field cannot be modified.

8. Click the arrow next to the **Advanced Options** region to configure additional options if required. The following advanced options are available:
   - **Runtime Script**: Select to specify that this is a Runtime script that will only be available during operation execution. Normally, scripts that are part of the Software Library should be designated as Runtime scripts, however any user script may be designated a Runtime script.

     > **Note:**
     >
     > During a Precheck or Health Check, Oracle Site Guard checks the existence of runtime scripts that have been added to the Software Library. However, if the scripts are not part of the Software Library, Oracle Site Guard does not check for their existence before an operation plan is executed.

   - **Credential Type**: Select one of the following credential types while executing the script:
     - **Normal Host Credentials**: Select to use the Normal (non-root) privileges configured for that script host.
     - **Privileged Host Credentials**: Select these credentials to use the Privileged (`root`) privileges configured for that script host.
     - **Custom Host Credentials**: Select to use an alternate set of named credentials. If you select this option, also select the named credential from the Named Credential drop-down menu.
   - **Named Credential**: The named credential to use when executing the script. This selection is only applicable if **Credential Type** is set to **Custom Host Credentials**.

- **Credential Parameters**: Select one or more configured credentials to pass as parameters for this script, by moving credentials from the Available Values column to the Selected Values column.

> **Note:**
>
> For ZFS storage scripts, you must pass the source and target appliance credentials as credential parameters to the configured script.
>
> The order of credentials passed to the script is important. You must pass the source credential first, followed by that target credential.

9. Click **Save**.

Configuring Storage Scripts with EMCLI Commands

Learn how to create and configure a storage script with EMCLI commands.

To configure a storage script, use with the `create_siteguard_script` EMCLI command:

```
emcli create_siteguard_script
        -system_name="name_of_the_system"
        -operation="name_of_the_operation"
        -script_type="type_of_the_script"
        -path="path_of_the_script"
        [-host_name="name_of_the_host_where_the_script_will_be_run"]
        [-component="path_of_the_entity_in_software_library"]
        [-
runtime_script="flag_to_specify_if_prechecks_should_check_availability_of_this_sc
ript"]
        [-run_on="flag_specifying_which_hosts_will_run_the_script"]
        [-all_hosts="flag_to_run_the_script_on_all_the_hosts_in_the_system"]
        [-role="role_associated_with_the_system"]
        [-credential_type="type_of_the_credential"]
        [-credential_name="name_of_the_credential"]
        [-target_storage_credential_name="target_storage_credential"]
        [-source_storage_credential_name="source_storage_credential"]
        [-credential_owner="credential_owner"]
```

> **Note:**
>
> [ ] indicates that the parameter is optional.

Parameter	Description.
`-system_name`	The system for which the script is being configured.
`-operation`	The function of the operation. Example: `Switchover`, `Failover`, `Start`, `Stop`, `Open for Validation`, or `Revert to Standby`.

Parameter	Description.
`-script_type`	The type of script depending on the operation you want to perform. For example: `Storage-Switchover`, `Storage-Failover`, `Storage-CreateClone`, or `Storage-DeleteClone`..
`-host_name`	The name of the host where the script will be run. This option can be specified more than once to configure multiple hosts. Ensure that each host is part of the system specified in the parameter `system_name`.

`-path`	Enter the path to the script.
	If you are configuring the bundled `zfs_storage_role.sh` script specify the path as described in "zfs_storage_role_reversal.sh".
	For example:
	`sh zfs_storage_role_reversal.sh -t zfssite1.mycompany.com -h zfssite2.mycompany.com -j ZFS-DR-Project -p zfssite1-pool-0 -q zfssite2-pool-0 -c N -f Y -z 300 -o switchover`
	If you are configuring a user-defined script that you have added to the Enterprise Manager software library, provide only the name of the script and any additional arguments that the script requires.
	For example:
	`sh example_script.sh -a value1 -b value2 -c value3`
	If you are configuring a user-defined script that you will deploy on all the configured hosts, provide the full path to the script location and any additional arguments that the script requires.
	Note: The script must reside at the same path location on each host.
	For example:
	`/path_to_the_script/example_script.sh -a value1 -b value2 -c value3`

`-component`	The path to the entity in software library. If component is specified, the `-path` option should contain only the script name and its parameters.
`-runtime_script`	Whether script is a runtime script. If the script is designated a runtime script, Prechecks will not verify the existence of script. This option can be used when the script is dynamically mounted or generated as part of execution of operation plan. By default, all scripts staged from software library are designated as runtime scripts. The default value is `false` for scripts that are not staged from software library.

Parameter	Description.
`-run_on`	Whether the script needs to be executed on only one of the available hosts (enter `any`) or on all hosts (enter `all`). This parameter is optional and default value is `all`.
`-all_hosts`	Optional flag to enable the script to run on all the hosts in the system. This parameter overrides the `host_name`.
`-role`	This option is not applicable for scripts of type **Storage Switchover** and **Storage Failover**.
`–credential_type`	The `HostNormal` credentials or `HostPrivileged` credentials for users with `root` privileges. If the values for the parameter `credential_type` are not specified, then the values for `credential_name` must be specified.
`-credential_name`	An alternate named credential to use when executing this script. If the values for the parameter `credential_name` are not specified, then the values for the parameter `credential_type` must be specified.
`-credential_owner`	The owner of the named credential for `target_storage_credential` and `source_storage_credential`.

To pass credentials to a script, first configure the script and then configure the credentials that you want to pass as parameters to the scrip, as explained in Configuring Credentials as Parameters for Scripts.

Configuring Credentials as Parameters for Scripts

Learn how to pass credentials to a script

When you configure Site Guard scripts with Enterprise Manager Cloud Control Console, you can configure the credentials to pass as a parameter to the script. However, if you configure scripts with the EMCLI commands, you must use separate additional EMCLI commands to add, delete or get credential parameters for scripts. Before you configure a script to receive credentials as parameters, ensure that you have created these credentials as described in Creating Credentials. Also, ensure that you have configured the script to which you want to pass credentials as described in Configuring Scripts.

To configure credentials as script parameters, perform any of the following tasks:

Adding Credential Parameters to a Script

Learn how to add credentials to a script with EMCLI commands.

To add credentials parameters to a configured script, run the EMCLI `add_siteguard_script_credential_params` command. You can either execute the command once for each set of credentials that need to be configured as parameters to a script, or provide all the credentials in one invocation in a comma-separated list:

```
emcli add_siteguard_script_credential_params
        -script_id="id_associated_with_the_script"
```

```
-credential_name="name_of_the_credential"
[-credential_owner="credential_owner"]
```

> **Note:**
>
> [ ] indicates that the parameter is optional.

Parameter	Description
-script_id	The script ID.
-credential_name	The name of the credential. Use a comma-separated list enclosed in double quotes to specify more than one credential.
-credential_owner	The credential owner details. You need not specify the values of this parameter if the owner of the credential is same as that of the logged-in user.

Deleting Credential Parameters with a Script

Learn how to delete configured credentials with EMCLI commands.

To delete one or more credentials parameters already configured for a script:

```
emcli delete_siteguard_script_credential_params
        -script_id="Id associated with the script"
        [-credential_name="name of the credential"]
        [-credential_owner="credential owner"]
```

> **Note:**
>
> [ ] indicates that the parameter is optional.

Parameter	Description
-script_id	The ID associated with the script.
-credential_name	The name of the credential. Use a comma-separated list enclosed in double-quotes to specify more than one credential. This parameter is optional. If unspecified, all credentials associated with the script are deleted.
-credential_owner	The owner of the credential. This parameter need not be specified if the owner of the credential is the same as the logged-in user.

Getting Credential Parameters for a Script

Learn how to obtain the list of credentials configured for a script with EMCLI commands.

To get a list of one or more credentials parameters configured for a script:

```
emcli get_siteguard_script_credential_params
        -script_id="Id_associated_with_the_script"
        [-credential_name="name_of_the_credential"]
        [-credential_owner="credential_owner"]
```

> **Note:**
>
> [ ] indicates that the parameter is optional.

Parameter	Description
`-script_id`	The ID associated with the script.
`-credential_name`	The name of the credential. If this argument is not specified, all credentials associated with the script will be deleted. This parameter is optional.
`-credential_owner`	The owner of the credential. This parameter need not be specified if the owner of the credential is the same as the logged-in user.

Cloning a Script with Existing Scripts

Learn how to clone (copy) a script of any kind with Enterprise Manager Cloud Control Console.

To clone a script with the Enterprise Manager Cloud Control Console:

1. Login to Enterprise Manager as an `EM_SG_ADMINISTRATOR` user.
2. From the Targets menu, click **Systems**.

   The Systems page is displayed.
3. Select the system name (**Generic System**) on which the script must be configured. The Generic System page for that site is displayed.
4. Click **Generic System** > **Site Guard** > **Configure**.

   The Site Guard Configuration page is displayed.
5. Click the **Pre/Post Scripts** tab or the **Storage Scripts** tab.

   The Pre/Post Scripts page or the Storage Scripts page is displayed.
6. Select a configured script from the Scripts table and click **Add Like**.
7. Modify any pre-configured values that you want to change.
8. Click **Save**.

Configuring Auxiliary Hosts

You can configure one or more hosts managed by Oracle Enterprise Manager as an auxiliary host to a site.

An auxiliary host to a site must be managed by Oracle Enterprise Manager. A host can be an auxiliary host for one or more sites. These hosts are used to run Pre Scripts, Post Scripts, or Storage Scripts on a site.

To manage auxiliary hosts, use the following tasks:

- Adding an Auxiliary Host with EMCLI Commands
- Deleting an Auxiliary Host with EMCLI Commands
- Listing Auxiliary Targets with EMCLI Commands

Adding an Auxiliary Host with EMCLI Commands

Learn how to add an auxiliary host to a site with EMCLI commands.

> **Note:**
>
> For information about logging in to the Enterprise Manager Command-Line Interface, see *Oracle Enterprise Manager Command Line Interface Guide*.

To add an auxiliary host on a site, run the following EMCLI command:

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

Parameter	Description
`-system_name`	The system on which you are performing the operation.
`-host_name`	The name of the host where the script will be executed. **Note**: Ensure that the hostname is part of the system specified in `system_name`.

Deleting an Auxiliary Host with EMCLI Commands

Learn how to delete an auxiliary host on a site with EMCLI commands.

> **Note:**
>
> For information about logging in to the Enterprise Manager Command Line Interface, see *Oracle Enterprise Manager Command Line Interface Guide*.

To delete a auxiliary host on a site, use the `delete_siteguard_aux_host` EMCLI command:

```
emcli delete_siteguard_aux_host
        -system_name="system_name"
        [-host_name="name_of_the_host"]
```

> **Note:**
>
> [ ] indicates that the parameter is optional.

Parameter	Description
`-system_name`	The system on which you are performing the operation.
`-host_name`	The name of the auxiliary host to delete. If unspecified, then all auxiliary hosts associated with the system are deleted. Optional. **Note**: Ensure that the host name is part of the system specified in `system_name`.

Listing Auxiliary Targets with EMCLI Commands

Learn how to view the list of auxiliary hosts for a system.

> **Note:**
>
> For information about logging in to the Enterprise Manager Command Line Interface, see *Oracle Enterprise Manager Command Line Interface Guide*.

To view a list of all auxiliary targets for a system, run the following EMCLI command:

```
emcli get_siteguard_aux_hosts
          -system_name="system_name"
```

Parameter	Description
`-system_name`	The name of the system for which you want the list of auxiliary hosts.

Configuring Database Lag Checks with EMCLI Commands

Learn how to configure database lags for databases in Oracle Site Guard operation plans.

> **Note:**
>
> For information about logging in to the Enterprise Manager Command Line Interface, see *Oracle Enterprise Manager Command Line Interface Guide*.

To manage values of the Apply Lag and the Transport Lag for one or more databases with EMCLI, use the following tasks:

- Configuring Database Lag Checks with EMCLI Commands

- Updating Threshold Value for Database Lag with EMCLI Commands
- Deleting Threshold Value for Database Lag with EMCLI Commands
- Listing Database Lag Thresholds with EMCLI Commands

Configuring Database Lag Checks with EMCLI Commands

Learn how to configure lags with EMCLI commands.

To configure values of Apply Lag and Transport Lag for databases, run the following EMCLI command:

```
emcli configure_siteguard_lag
        -system_name="system_name"
        -property_name="lag_type"
        -value="max_limit"
        [-target_name="database_target_name"]
```

> **Note:**
>
> [ ] indicates that the parameter is optional.

Parameter	Description
`-system_name`	The system on which you want to configure the threshold limit.
`-target_name`	The database target name for which the threshold limit is configured. If this parameter is not specified, then the threshold value is applied to all databases of the system.
`-property_name`	The property name. Valid values are `apply_lag` and `transport_lag`.
`-value`	The threshold value to be configured (in seconds).

Updating Threshold Value for Database Lag with EMCLI Commands

Learn how to update lag thresholds with EMCLI commands.

To update the values of Apply Lag and Transport Lag threshold for one or more Data Guard enabled database, run the following EMCLI command:

```
emcli update_siteguard_lag
        -system_name="system_name"
        [-target_name="database_target_name"]
        -property_name="lag_type"
        -value="max_limit"
```

> **Note:**
>
> [ ] indicates that the parameter is optional.

Parameter	Description
`-system_name`	The system for which you want to configure the threshold limit.
`-target_name`	The database target name for which the threshold limit is configured. If this parameter is not specified, then the threshold value is applied to all databases of the system.
`-property_name`	The property name. Valid values are `apply_lag` and `transport_lag`.
`-value`	The threshold value to be updated (in seconds).

Deleting Threshold Value for Database Lag with EMCLI Commands

Learn how to delete lag thresholds with EMCLI commands.

To delete the values of Apply Lag and Transport Lag threshold configured for one or more Data Guard enabled databases, run the following EMCLI command:

```
emcli delete_siteguard_lag
         -system_name="system_name"
         [-target_name="database_target_name"]
         -property_name="lag_type"
```

> **Note:**
>
> [ ] indicates that the parameter is optional.

Parameter	Description
`-system_name`	The system for which you want to configure the threshold limit.
`-target_name`	The database target name for which the threshold limit is configured. If the database name is not specified, the configured lag limit is deleted for all databases in the system.
`-property_name`	The property name. Valid values are `apply_lag` and `transport_lag`.

Listing Database Lag Thresholds with EMCLI Commands

Learn how to list lag thresholds with EMCLI commands.

To view values of the configured database Apply Lag and Transport Lag threshold limits of a system, run the following EMCLI command:

```
emcli get_siteguard_lag
        -system_name="system name"
        [-target_name="database_target_name"]
        -property_name="lag_type"
```

> **Note:**
>
> [ ] indicates that the parameter is optional.

Parameter	Description
`-system_name`	The system for which you want to retrieve the threshold limit.
`-target_name`	The database target name for which the threshold limit is to be retrieved. If the database name is not specified, the property is obtained for all databases in the system.
`-property_name`	The property name. Valid values are `apply_lag` and `transport_lag`.

5
Performing Oracle Site Guard Operations

An Oracle Site Guard operation plan specifies the action steps and their order of execution. Learn how to create, execute, and monitor Oracle Site Guard operation plans.

This chapter includes the following sections:

- Overview
- Managing Operation Plans
- Running Prechecks
- Scheduling and Stopping Health Checks
- Executing Oracle Site Guard Operation Plans
- Monitoring Oracle Site Guard Operations
- Managing Execution Errors
- Manually Reversing Site Roles

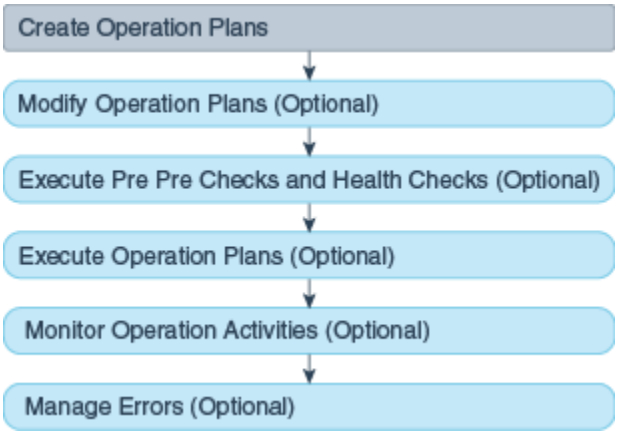
Overview

An Oracle Site Guard operation plans specifies the steps executed during a disaster recovery. This workflow allows step execution in series or in parallel.

An operation plan allows you to execute it on series or in parallel; in addition, you can set an operation to ignore or retry steps upon error.

Figure 5-1 shows the roadmap for Oracle Site Guard operations. Steps marked *optional* are required if the site topology and operation plans require the configuration. However, since most enterprise deployments are large, they typically require all the configuration steps in the workflow.

Figure 5-1 Workflow for Oracle Site Guard Operations



> **Note:**
>
> - Before you create operation plans, ensure that you complete the tasks listed in Configuring Oracle Site Guard .
> - You must login using the `EM_SG_ADMINISTRATOR` role privilege to perform configuration tasks. Ensure that you have created the required user credentials as described in Creating Oracle Site Guard Administrator Users.

Managing Operation Plans

An operation plan describes the flow of execution that Oracle Site Guard performs in a disaster recovery operation, and it consists of (ordered) actions that can be executed in series or in parallel.

Before you execute any Oracle Site Guard disaster recovery operation, you must create a plan for that operation.

An operation plan contains steps such as the following:

- Stopping Oracle HTTP Servers.
- Stopping the node managers, managed servers, and administration server in an Oracle WebLogic domain.
- Performing a database role reversal with Oracle Data Guard.
- Executing custom user scripts at certain points in the operation plan sequence.

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.

> **Note:**
>
> All existing Site Guard operation plans must be deleted and recreated after a major upgrade of the product.

This section contains the following topics:

- Creating Operation Plans
- Creating New Operation Plans with Existing Plans
- Editing and Updating Operation Plans
- Deleting an Operation Plan

Creating Operation Plans

You can create an operation plan with Enterprise Manager Cloud Control Console or with EMCLI commands.

To create an operation plan, use one of the following methods:

Creating an Operation Plan with Enterprise Manager Cloud Control Console

Learn how to create a new operation plan with Enterprise Manager Cloud Control Console.

To create an operation plan with the Enterprise Manager Cloud Control Console:

1. Login to Enterprise Manager as a user with `EM_SG_ADMINISTRATOR` role privileges.
2. From the Targets menu, click **Systems**.

   The Systems page is displayed.
3. On the Systems page, click the name of the system (**Generic System**) for which the plan is being created.

   The Generic System page for this site is displayed.
4. Click **Generic System** > **Site Guard** > **Operations**.

   The Site Guard Operations page is displayed.
5. Click **Create**.

   The **Create New Operation Plan** dialog is displayed.
6. Enter the following details:

   Plan Name: Enter a name for the plan.

   Operation Type: Select an operation type from the following options:

   - Switchover
   - Failover
   - Start
   - Stop
   - Open for Validation
   - Revert to Standby

   > **Note:**
   >
   > - For information about Oracle Site Guard operation types, see Oracle Site Guard Workflows.
   > - The options displayed in the dialog change depending on the operation type you select. For switchover and failover operation types, you must select the standby system for the plan. For start and stop operations, select the current role for the system.

   Primary System: This field displays the name of the system for which this plan is being created. You cannot change the values in this field.

   Standby System: Select a standby system from the list. Note that this option is enabled only when you select **Switchover** or **Failover** in the Operation Types field.

Current Role: Select either **Primary** or **Standby**. This is the role of the system that this plan applies to. The plan can only run when the system is assigned a role. Note that this option is enabled only when you select **Start** or **Stop** in the Operation Type field.

7. Depending on the Operation Type you select, configure the standby system accordingly.
8. Click **Save**.

Creating an Operation Plan with EMCLI Commands

Learn how to create an operation plan with EMCLI commands.

> **Note:**
>
> For information about logging in to the Enterprise Manager Command Line Interface, see *Oracle Enterprise Manager Command Line Interface Guide*.

To create a new operation plan, use the `create_operation_plan` EMCLI command:

```
emcli create_operation_plan
         [-primary_system_name="name_of_primary_system"]
         [-standby_system_name="name_of_standby_system"]
         [-system_name="name_of_the_system"]
         [-operation="name_of_the_operation"]
         [-name="name_of_the_operation_plan"]
         [-role="role_associated_with_the_system"]
         [-
like="name_of_the_operation_plan_from_which_the_steps_are_to_be_copied"
```

> **Note:**
>
> [ ] indicates that the parameter is optional.

Parameter	Description
`-primary_system_name`	The name of your system associated with the primary site. This option is used for switchover or failover operations.
`-standby_system_name`	The name of your system associated with the standby site. This option is used for switchover or failover operations.
`-system_name`	The name of the system. This option is used for start or stop operations.
`-operation`	The function of the operation. Example: `switchover`, `failover`, `start`, `stop`, `openforvalidation`, or `reverttostandby`.
`-name`	The name of the operation plan.

Parameter	Description
`-role`	The role associated with a system, when you run an operation (`start` or `stop`).
`-like`	Name of the operation plan from which the steps are to be copied. If this option is specified, system name, operation, and role are ignored.

Creating New Operation Plans with Existing Plans

Create and configure a new operation plan based on an existing operation plan with Enterprise Manager Cloud Control Console.

You can create and configure a new operation plan of any kind by cloning (copying) an existing plan.

To clone a plan with the Enterprise Manager Cloud Control Console:

1. Login to Enterprise Manager as an `EM_SG_ADMINISTRATOR` user.
2. From the **Targets** menu, click **Systems**.

   The Systems page is displayed.
3. Select the system name (**Generic System**) for which the operation plan is created. The Generic System page for that site is displayed.
4. Click **Generic System** > **Site Guard** > **Operations**.

   The Site Guard Operations page is displayed.
5. Select an existing operation plan from the table and click **Create Like**.
6. Enter a name for the new plan.
7. Click **Save**.

Editing and Updating Operation Plans

You can edit your operation plan to change the step execution order, to stop/continue step execution when it encounters an error, and to specify which steps are to run in series or parallel.

When editing an operation plan, you can:

- Change the order of the steps in an operation plan.
- Enable or disable individual steps in the operation plan.
- Choose to stop or continue a step in an operation plan if Oracle Site Guard encounters an error while running the operation plan.
- Customize each step to execute steps in a serial order or parallel on different hosts.
- Customize execution groups to sequence operation plan steps in a specific order.
- Change the timeout for an individual operation step.

You can save the updated operation plan at any point.

To edit or update an operation plan use one of the following methods:

- Editing and Updating Operation Plans with Enterprise Manager Cloud Control Console
- Editing and Updating Operation Plans with EMCLI Commands
- Adding and Deleting Operation Plan Tags with EMCLI Commands

Editing and Updating Operation Plans with Enterprise Manager Cloud Control Console

Learn how to edit an operation plan with Enterprise Manager Cloud Control Console.

To edit and update an operation plan with Enterprise Manager Cloud Control Console:

1. Login to Enterprise Manager with `EM_SG_ADMINISTRATOR` role privileges.
2. From the Targets menu, click **Systems**.

   The Systems page is displayed.
3. On the Systems page, click the name of the system (**Generic System**) for which this plan is being created.

   The Generic System page for that site is displayed.
4. On the system's home page, from the **Generic System** > **Site Guard** > **Operations**.

   The Site Guard Operations page is displayed.

   A list of configured operation plans is displayed in the Operation Plans tab.
5. Select an existing operation plan by clicking on the plan listed in the Plan Name column.

   The steps associated with the selected operation plan are listed in the Operation Details table located below the Operation Plan table. Each row in the table represents a step that is executed as part of the operation plan.
6. Select **View > Columns > Show All** to display all columns in the Operation Plan details table, including the additional columns for Script Id, Execution Group and Timeout (sec).
7. Click **Edit** to enable the options for updating and customizing the steps in the operation plan.
8. Select **Move Up** (green arrow), **Move Down** (red arrow), or **Delete Step** to sequence the steps in the operation plan.

   In addition, select the attribute from the **Error Mode**, **Execution Mode**, or **Run Mode** columns.

   An operation plan step cannot be moved out of the group it belongs to.
9. To use execution groups to sequence operation steps in a operation group:
   a. Set the **Execution Mode** for the operation group to **Parallel**.
   b. Select the **Execution Group** for each step in the operation group

   All the steps in an execution group are executed in parallel. All the steps that share an execution group will not begin execution until all the steps in the previous execution group have finished execution.

If the execution mode is Serial, execution groups do not apply. The steps are always executed sequentially in the order they are listed.

10. To change the timeout for a step in the plan, type in a new timeout value for that step.
11. Click **Save** to update the plan.

Editing and Updating Operation Plans with EMCLI Commands

Learn how to manage an operation plan with EMCLI commands.

> **Note:**
>
> For information about logging in to the Enterprise Manager Command Line Interface, see *Oracle Enterprise Manager Command Line Interface Guide*.

To edit or update an operation plan, use the `get_operation_plans`, `get_operation_plan_details`, and `update_operation_plan` EMCLI commands.

1. Get the list of operation plans:

```
emcli get_operation_plans
        [-name="name_of_the_operation_plan"]
        [-operation="type_of_operation"]
        [-system_name="name_of_the_system"]
        [-primary_system_name="name_of_the_primary_system"]
        [-standby_system_name="name_of_the_standby_system"]
```

> **Note:**
>
> [ ] indicates that the parameter is optional.

Parameter	Description
`-name`	The name of the operation plan.
`-operation`	The name of the operation. For example, `switchover`, `failover`, `start`, `stop`, `openforvalidation`, or `reverttostandby`. This is an optional parameter. If you do not specify this parameter, then all the operation plans will be listed.
`-system_name`	The name of system used in the operation plan. If you specify this value, then you do not need to specify values for `-primary_system_name` and `-standby_system_name`.
`-primary_system_name`	The name of primary system used in the operation plan. You can specify the values for this parameter instead of the value `-system_name`. You can also use the `-standby_system_name` parameter for better filtering.

Parameter	Description
`-standby_system_name`	The name of the standby system used in the operation plan. You can specify the value for this parameter instead of the value for `-system_name`. The `-primary_system_name` parameter can also be additionally used for better filtering.

2. Get the details of an operation plan that you want to update:

```
emcli get_operation_plan_details
      -name="name_of_the_operation_plan"
```

Parameter	Description
`-name`	The name of the operation plan.

3. Update the plan:

```
emcli update_operation_plan
        -plan_name="name of the plan"
        -step_number="plan step number to update"
        -target_host="name of the target host"
        -target_name="name of the target"
        [-error_mode="the error mode"]
        [-enabled="flag specifying whether the step should be enabled"]
        [-execution_mode="execution mode"]
        [-execution_group="when execution_mode is parallel, then targets
sharing the same execution group will execute in parallel"]
        [-timeout="timeout in seconds"]
        [-move="direction in which to move step"]
        [-delete "flag specifying whether step should be deleted"]
```

> **Note:**
>
> [ ] indicates that the parameter is optional.

Parameter	Description
`-plan_name`	The name of the operation plan.
`-step_number`	The number of the step that should be updated.
`-target_host`	The name of the system. Updates all the steps related to this target host.
`-target_name`	The database target name.
`-error_mode`	The function of the operation. For example:`stop` or `continue`.
`-enabled`	Enter `true` or `false`.
`-execution_mode`	The execution mode. For example: `Serial` or `Parallel` When set to `Parallel`, then targets sharing the same execution group execute in parallel.
`-execution_group`	The execution group (a value between 1 and n, where n is the number of targets in the bucket)

Parameter	Description
`-timeout`	The timeout in seconds for the execution of the step. Value must be between 1 and 86400 (24 hours).
`-move`	Change the order by specifying `Up` or `Down`.
`-delete`	Whether you want to delete steps. Enter `true` or `false`.

Adding and Deleting Operation Plan Tags with EMCLI Commands

Learn how to manage tags for an operation plan with EMCLI commands.

> **Note:**
>
> For information about logging in to the Enterprise Manager Command-Line Interface, see *Oracle Enterprise Manager Command Line Interface Guide*.

To manage tags (alphanumeric identifier strings) for an operation plan, use the `add_operation_plan_tags` and `delete_operation_plan_tags` EMCLI commands.

1. To assign tags to an operation plan:

```
emcli add_operation_plan_tags
        -name="name_of_the_operation_plan"
        -tags="names_of_tags separated by ;"
```

Parameter	Description
`-name`	The name of the operation plan.
`-tags`	A semicolon-separated list of tags to add to the operation plan. The comma (,) is an invalid character.

2. To delete tags assigned to an operation plan run:

```
emcli delete_operation_plan_tags
        -name="name_of_the_operation_plan"
        -tags="names_of_tags separated by ;"
        -all
```

Parameter	Description
`-name`	The name of the operation plan.
`-tags`	A semicolon-separated list of tags to add to the operation plan. The comma (,) is an invalid character.
`-all`	Delete all tags in the operation plan. Optional. This flag overrides all values passed to the `tags` argument.

Deleting an Operation Plan

Learn how to delete an operation plan with Enterprise Manager Cloud Control Console or EMCLI commands.

To delete an operation plan, use either of the following tasks:

> **Note:**
>
> All existing Site Guard operation plans must be deleted and recreated after a major upgrade of the product.

Deleting an Operation Plan with Enterprise Manager Cloud Control Console

Learn how to delete an operation plan with Enterprise Manager Cloud Control Console.

To delete an operation plan with Enterprise Manager Cloud Control Console:

1. Login to Enterprise Manager with `EM_SG_ADMINISTRATOR` role privileges.
2. From the Targets menu, click **Systems**.

   The Systems page is displayed.
3. On the Systems page, click the name of the system (**Generic System**) for which this plan is being created.

   The Generic System page for that site is displayed.
4. On the system's home page, from the **Generic System** > **Site Guard** > **Operations**.

   The Site Guard Operations page is displayed.

   A list of configured operation plans is displayed in the Operation Plans tab.
5. Select an existing operation plan by clicking on the plan listed in the Plan Name column.
6. Click **Delete** to delete the selected operation plan.

   A confirmation pop-up window appears. Click **Yes** to confirm the action.

Deleting an Operation Plan with EMCLI Commands

Learn how to delete an operation plan with EMCLI commands.

> **Note:**
>
> For information about logging in to the Enterprise Manager Command Line Interface, see *Oracle Enterprise Manager Command Line Interface Guide*.

To delete an operation plan, use the `delete_operation_plan` EMCLI command.

```
emcli delete_operation_plan
        –name="name_of_the_operation_plan"
```

Parameter	Description
`-name`	The name of the operation plan to delete.

Running Prechecks

Before executing an operation plan Oracle Site Guard runs checks, which you can also run separately to ensure that your operation plan is ready for execution.

Before performing an operation plan Oracle Site Guard runs, by default, the Precheck utility. You can also run this utility separately at any time to ensure that your plan is ready for execution.

The Precheck utility performs the following checks:

- Checks the agent status on all hosts involved in the operation.
- Checks if any new targets are added to the generic system after the operation plan is created.
- Checks if all targets involved in the operation plan exist in the Enterprise Manager repository.
- Detects if any targets are moved out or deleted from the generic system after the operation plan is created.
- Performs Storage Role Reversal.
- Runs Oracle Data Guard Broker Prechecks to ascertain whether the Database is ready for role reversal (for switchover/failover operation).
- Performs Database Role Checks.
- Performs Database Lag (Apply and Transport) Checks.
- Runs checks on ZFS storage appliances to assert the role-change readiness.

To run the Precheck utility, use one of the following methods:

- Running Precheck Utility with Enterprise Manager Cloud Control Console
- Running Precheck Utility with EMCLI Commands

Running Precheck Utility with Enterprise Manager Cloud Control Console

Learn how to check an operation plan with Enterprise Manager Cloud Control Console.

To run the Precheck utility with Enterprise Manager Cloud Control:

1. Login to Enterprise Manager Cloud Console as a user with `EM_SG_ADMINISTRATOR` role privileges.
2. From the Targets menu, click **Systems**.

   The Systems page is displayed.
3. On the Systems page, click the name of the system (**Generic System**) for which the Prechecks are to be run.
4. Click **Generic System** > **Site Guard** > **Operations**. The **Site Guard Operations** page is displayed.
5. Select an operation plan from the list by clicking on the plan name from the list.

6. Click **Run Prechecks**.

   A dialog box is displayed. Click **Yes** to confirm the action.

To track the progress and results of the Precheck, click the **click here** link in the Confirmation pane at the top of the page, or navigate to **Enterprise** > **Provisioning and Patching** > **Procedure Activity**.

For details about monitoring a procedure activity, see Monitoring Oracle Site Guard Operations.

Running Precheck Utility with EMCLI Commands

Learn how to check an operation plan with EMCLI commands.

> **Note:**
>
> For information about logging in to the Enterprise Manager Command Line Interface, see *Oracle Enterprise Manager Command Line Interface Guide*.

To run the Precheck utility, use the `run_prechecks` EMCLI command.

```
emcli run_prechecks
       -operation_plan="operation_plan_name"
       [-database_lag_checks="true"|"false"]
```

> **Note:**
>
> `[ ]` indicates that the parameter is optional.

Parameter	Description
`-operation_plan`	Enter the name of your operation plan.
`-database_lag_checks`	Run database lag checks as part of Prechecks for all data guard configured databases. This parameter is optional. The default value is `true`.

Scheduling and Stopping Health Checks

Health checks are scheduled, periodic checks that can help you assess and monitor your disaster-recovery readiness on an ongoing basis.

To schedule or stop a health check for an operation plan, use either of the following methods:

- Scheduling a Health Check with Enterprise Manager Cloud Control Console
- Scheduling a Health Check with EMCLI Commands
- Stopping a Health Check with Enterprise Manager Cloud Control Console
- Stopping a Health Check with EMCLI Commands

Scheduling a Health Check with Enterprise Manager Cloud Control Console

Learn how to schedule a health check with Enterprise Manager Cloud Control Console.

To schedule Health Checks with Enterprise Manager Cloud Control Console:

1. Login to Enterprise Manager Cloud Console as a user with `EM_SG_ADMINISTRATOR` role privileges.
2. From the Targets menu, click **Systems**.

   The Systems page is displayed.
3. On the Systems page, click the name of the system (**Generic System**) for which the Prechecks are run.
4. Click **Generic System** > **Site Guard** > **Operations**.The **Site Guard Operations** page is displayed.
5. Select an operation plan from the list by clicking on the plan name from the list.
6. Click **Schedule Health Checks**.

   The Schedule Health Checks for operation plan dialog box is displayed.

   Configure the schedule for the health check.
7. From the drop-down menu next to **Send execution status email to**, select a user e-mail address to send notifications to.

   Note that this e-mail address must already be configured for the current user.
8. Check the **Notify on failed execution only**box if you wish to be notified only when a health check fails. Otherwise, you will receive notifications for all health check executions in this schedule.
9. Click **Save**.

To inspect the results for each Health Check, navigate to **Enterprise** > **Provisioning and Patching** > **Procedure Activity**.

For more information about monitoring procedure activity see Monitoring Oracle Site Guard Operations.

Scheduling a Health Check with EMCLI Commands

Learn how to schedule a health check with EMCLI commands.

> **Note:**
>
> For information about logging in to the Enterprise Manager Command Line Interface, see *Oracle Enterprise Manager Command Line Interface Guide*.

To schedule a Health Check, use the `schedule_siteguard_health_cheks` EMCLI command:

```
emcli schedule_siteguard_health_checks
        -operation_plan="name of the operation plan"
        -schedule=
           {
             start_time:yyyy/MM/dd HH:mm;
             [tz:{java timezone ID};]
             [frequency:interval/weekly/monthly/yearly;]
             [repeat:tx;]
                   [-email="email address to be notified]
                    [-notify_on_failure "flag specifying email notifications
will be sent on failed health check only"]
             [end_time:yyyy/MM/dd HH:mm;]
             [grace_period:xxx;]
           }
```

> **Note:**
>
> [ ] indicates that the parameter is optional.

Parameter	Description
-operation_plan	Enter the name of your operation plan.

Parameter	Description
-schedule	The schedule for the health check. Enter the values for the following parameters: - start_time: the time when health checks should begin. - tz: the time-zone ID. This parameter is optional. - frequency: the frequency of the health check (once/interval/weekly/monthly/yearly). This parameter is optional. If the frequency is set to interval, then you must specify the values for the parameter repeat. If the frequency is set to weekly or monthly, then you must specify the weekdays. If the frequency is set to yearly, both days and months must be specified. - repeat: the frequency with which health checks have to be repeated. These values are required only if the frequency is set to interval. - days: the list of days, separated by commas. These values are required only if the frequency is weekly, monthly, or yearly. If frequency is set to weekly, then the valid range is 1 to 7. If the frequency is set to monthly or yearly, then valid range is 1 to 30. - months: the list of months, separated by commas. These values are required only if the frequency is yearly (valid range 1 to 12). - end_time: the end time for execution of health checks. This parameter is optional. - grace_period: the grace period in minutes. This parameter is optional. For example: Examples: start_time:2014/06/10 15:45 start_time:2014/10/29 2:00;frequency:interval;repeat:1d start_time:2014/08/10 01:00;frequency:interval;repeat:1w start_time:2014/08/10 01:00;frequency:weekly;days:6,7;grace_period:60;tz:America/New_York
-email	The email address to use for notifications. This e-mail address must be a configured e-mail address for the current user. (Optional)
-notify_on_failure	If set, health check report will be e-mailed on failed execution only. (Optional)

> **Note:**
>
> When the Oracle Enterprise Manager job system cannot start the execution of a job within the scheduled time plus the grace period, it sets the job status to Skipped. By default, health check jobs are scheduled with unbound grace periods.

Stopping a Health Check with Enterprise Manager Cloud Control Console

Learn how to stop a health check with Enterprise Manager Cloud Control.

To stop a scheduled health check with the Enterprise Manager Cloud Control:

1. Login to Enterprise Manager Cloud Console as a user with `EM_SG_ADMINISTRATOR` role privileges.
2. From the Targets menu, click **Systems**.

   The Systems page is displayed.
3. On the Systems page, click the name of the system (Generic System) for which the Prechecks are run.
4. Click **Generic System** > **Site Guard** > **Operations**.The **Site Guard Operations** page is displayed.
5. Select an operation plan from the list by clicking on the plan name from the list. This operation plan must already have a health check scheduled.
6. Click the **Stop Health Checks** button.
7. Click **Yes** in the confirmation dialog.

Stopping a Health Check with EMCLI Commands

Learn how to stop a health check with EMCLI commands.

> **Note:**
>
> For information about logging in to the Enterprise Manager Command Line Interface, see *Oracle Enterprise Manager Command Line Interface Guide*.

To stop a scheduled health check, use the `stop_siteguard_health_checks` EMCLI command:

```
emcli stop_siteguard_health_checks
        -operation_plan="name of the operation plan"
```

Parameter	Description
`-operaton_plan`	The name of your operation plan.

Executing Oracle Site Guard Operation Plans

You can execute Oracle Site Guard operation plans with Enterprise Manager Cloud Control Console or with EMCLI commands.

To execute operation plan, use either of the following tasks:

Executing Oracle Site Guard Operation Plan with Enterprise Manager Cloud Control Console

Learn how to execute an operation plan with Enterprise Manager Cloud Control Console.

To execute an operation plan with Enterprise Manager Cloud Control Console:

1. Login to Enterprise Manager using the `EM_SG_ADMINISTRATOR` role privileges.
2. From the Targets menu, click **Systems**.

   The Systems page is displayed.
3. On the Systems page, click the name of the system (**Generic System**) for which the operation plan is being executed.
4. On the Generic System page, click **Generic System** > **Site Guard** > **Operations**.

   The Site Guard Operations page is displayed.
5. Select an operation plan from the list.
6. Click **Execute Operation**.

   A dialog box is displayed.

   a. Select **Run Prechecks** check box (selected by default) to run Prechecks before executing the operation plan.

   b. Select **Ignore Non-Fatal Warnings During Failover** to direct the operation plan to ignore non-fatal warnings during execution.
7. Click **Yes** to confirm the action.

To track the progress and results of the operation, click the **click here** link in the Confirmation pane at the top of the page, or navigate to **Enterprise** > **Provisioning and Patching** > **Procedure Activity**.

For more details about monitoring a procedure activity see Monitoring Oracle Site Guard Operations.

Executing Oracle Site Guard Operation Plan with EMCLI Command

Learn how to execute an operation plan with EMCLI commands.

> **Note:**
>
> For information about logging in to the Enterprise Manager Command Line Interface, see *Oracle Enterprise Manager Command Line Interface Guide*.

To execute an operation plan, use the `submit_operation_plan` `EMCLI` command:

```
emcli submit_operation_plan
         -name="name_of_operation_plan"
         [-run_prechecks="true | false"]
         [-
stop_primary="flag_specifying_whether_primary_site_to_be_stopped_during_failover"
]
         [-database_lag_checks="true"|"false"]
         [-ignore_warnings]
```

> **Note:**
>
> [ ] indicates that the parameter is optional.

Parameter	Description
`-name`	The name of the operation plan.
`-run_prechecks`	The `run_prechecks` value (`true` or `false`). By default, the value of this parameter is `true`. If you set the value to `false`, Prechecks will not be executed.
`-stop_primary`	Whether to stop targets on primary site during a Failover operation. Set value `true` or `false`.
`-database_lag_checks`	Run database lag checks as part of Prechecks for all Data Guard configured databases. This parameter is optional. The default value is `true`.
`-ignore_warnings`	When specified non-fatal warnings will be ignored during failovers.

Monitoring Oracle Site Guard Operations

You can monitor Oracle Site Guard operation plan executions with Enterprise Manager Cloud Control Console or with EMCLI commands.

To monitor an operation activity, use either of the following methods:

- Monitoring an Operation Plan with Enterprise Manager Cloud Control Console

- Monitoring an Operation Plan with EMCLI Commands

Monitoring an Operation Plan with Enterprise Manager Cloud Control Console

You can view, suspend, resume, or stop an operation activity with Enterprise Manager Cloud Control Console.

To monitor and manage operation activity, use the following tasks:

- Viewing an Operation Activity
- Suspending, Resuming, or Stopping an Operation

Viewing an Operation Activity

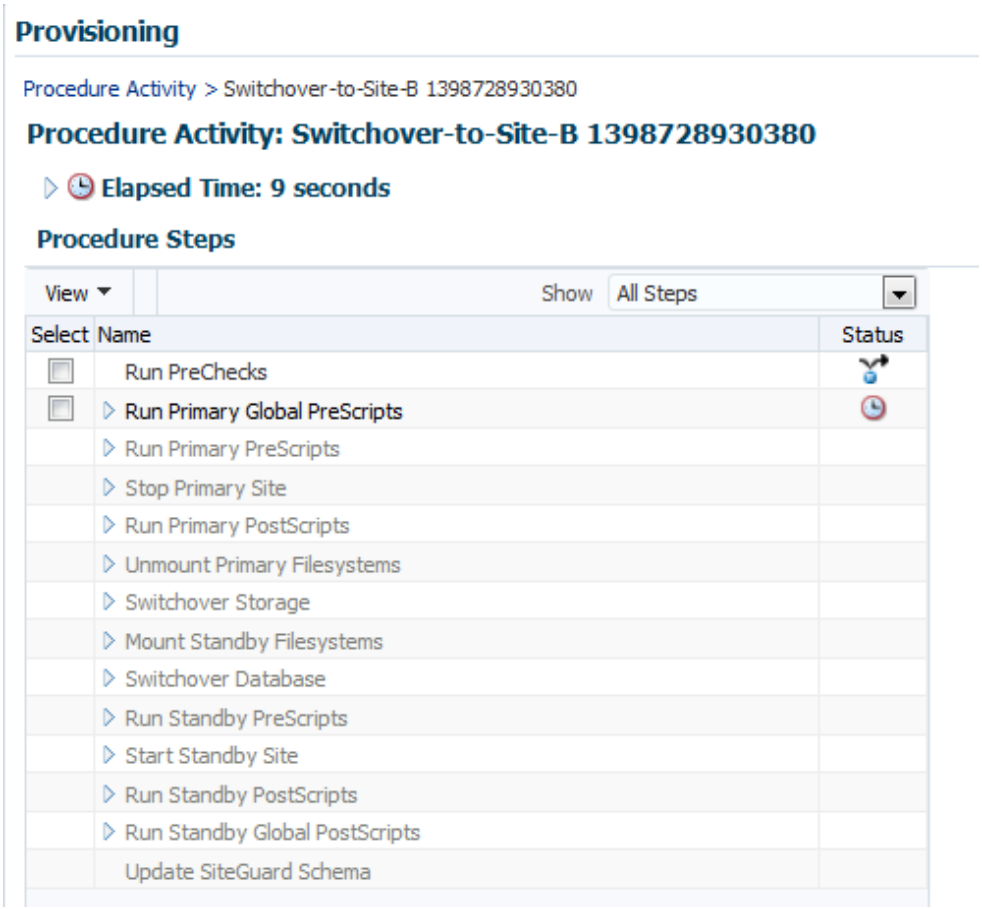
Learn how to view operation activity with Enterprise Manager Cloud Control Console.

To monitor an operation activity submitted for execution with Enterprise Manager Cloud Control Console:

1. Login to Enterprise Manager using the `EM_SG_ADMINISTRATOR` role privileges.
2. In the **Enterprise** menu, click **Provisioning and Patching** and then click **Procedure Activity**. The Provisioning page is displayed.
3. Alternately, navigate to a Site's operation activities page as follows:
   - On the Systems page, click the name of the system (Generic System) for which the operation plan was executed.
   - Click Generic System > Site Guard > Operations
   - Click the Operation Activities tab.
4. In the Procedure Activity table, click the name of the activity of operation you want to monitor.

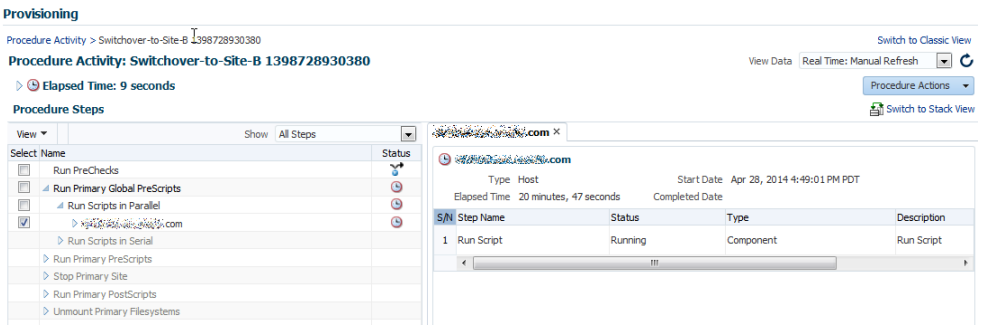
   The Procedure Activity page for that operation is displayed. See Figure 5-2.

Figure 5-2 Viewing an Operation Activity in the Enterprise Manager Cloud Control Console



5. Click the drop-down symbol next to the top-level step to view the sub-steps. The hierarchical steps of the activity are displayed. See Figure 5-3.

Figure 5-3 Viewing the Hierarchical Steps of an Operation Activity in the Enterprise Manager Cloud Control Console



Suspending, Resuming, or Stopping an Operation

Learn how to manage an operation execution with Enterprise Manager Cloud Control Console.

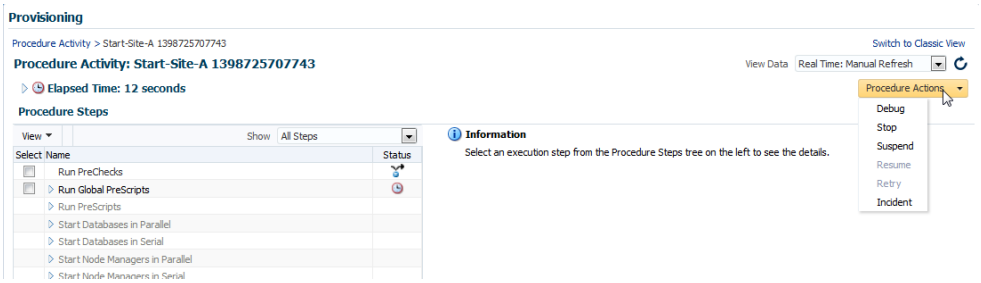
Operations in progress can be suspended and resumed later. You can also stop the operations that you do not want to resume.

To manage operation plans with Enterprise Manager Cloud Control Console:

1. Login to Enterprise Manager using the `EM_SG_ADMINISTRATOR` role privileges.
2. In the **Enterprise** menu, click **Provisioning and Patching** and then click **Procedure Activity**. The Provisioning page is displayed.
3. In the Procedure Activity table, click the name of the operation you want to monitor.

   The Procedure Activity page for that operation is displayed.
4. Click Procedure Actions located on the right-hand side of the page.
5. Click an action from the drop-down menu. See Figure 5-4.

Figure 5-4 Suspending, Resuming, or Stopping an Operation



Monitoring an Operation Plan with EMCLI Commands

Learn how to monitor operation plan executions with EMCLI commands.

> **Note:**
>
> For information about logging in to the Enterprise Manager Command Line Interface, see *Oracle Enterprise Manager Command Line Interface Guide*.

To monitor the status of an operation plan, use the `get_instances` and `get_instance_status`EMCLI commands.

1. Get a list of procedures by running the following command:

```
emcli get_instances
       [-type={procedure type}]
       [-format=name:]
       [-script]
       [-noheader]
```

> **Note:**
>
> [ ] indicates that the parameter is optional.

Parameter	Description
`-type`	The procedure type. This parameter is optional.
`-format`	The output format of the list of instances. Enter `pretty`, `script`, or `csv`. This parameter is optional and the default value is `pretty`.
`-script`	Whether the output format is script or not. This parameter is optional.
`-noheader`	Do not display column headers. This parameter is optional.

2. Note down the GUID for the operation in the list of operations displayed by the `get_instances` command.
3. Use that GUID with the `get_instance_status` EMCLI command:

```
emcli get_instance_status -instance="GUID"
```

Managing Execution Errors

Oracle Site Guard uses Enterprise Manager Cloud Control deployments to orchestrate disaster recovery operations on remote hosts. This framework provides error management support through execution error modes.

Errors encountered during an operation plan execution can be managed in multiple ways. Oracle Site Guard provides an option to define the error mode for individual steps, and also lets you enable or disable steps. For example, if an operation step has an associated error mode of 'Stop on Error', Oracle Site Guard stops the operation when it encounters and error while executing that step.

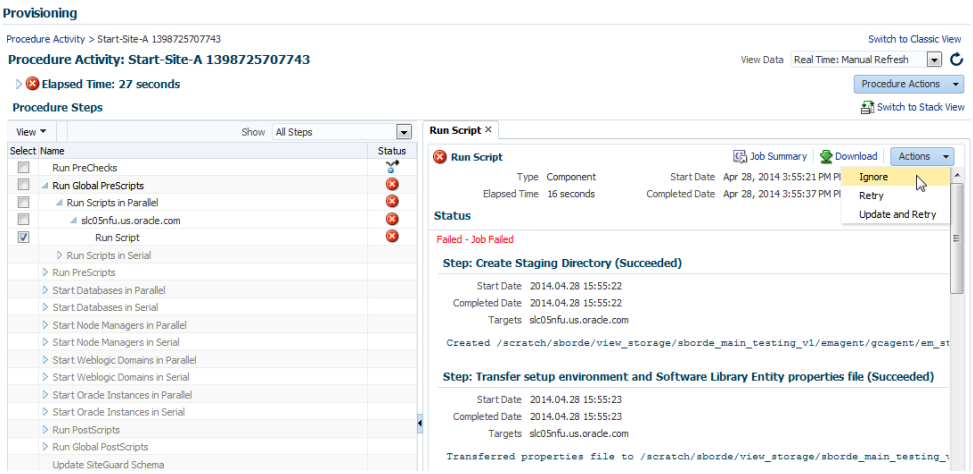
To retry the step that raised the error and to continue the operation:

1. Login to Enterprise Manager using the `EM_SG_ADMINISTRATOR` role privileges.
2. In the **Enterprise** menu, click **Provisioning and Patching** and then click **Procedure Activity**. The Provisioning page is displayed.
3. In the Procedure Activity table, click the name of the operation you want to change.

   The Procedure Activity page for that operation is displayed.
4. Click the drop-down symbol next to the top-level steps to view the sub-step. The hierarchical steps of the activity are displayed. Click the drop-down symbols at the hierarchical step until you reach the step that encountered the error.

   See Figure 5-5.

Figure 5-5 Status Details



5. Select the step, and click **Actions**. A drop-down menu is displayed.
6. From the drop-down menu, click the action that you want Oracle Site Guard to perform to manage this error.
   - Click **Ignore** to ignore the error, and continue with the other steps in the plan.
   - Click **Retry** to re-run the step.
   - Click **Update and Retry** to update the parameters for this step, and re-run the step.

> **Note:**
>
> - You cannot change the error mode of a step with the steps provided in this section. To change an error mode of a step, edit the operation as described in Editing and Updating Operation Plans.
> - For further information about how to diagnose execution errors, see Troubleshooting Oracle Site Guard.

Manually Reversing Site Roles

You can manually reconfigure site roles and explicitly designate a site as the primary site while testing disaster recovery work flows or in isolated parts of some work flows.

When you designate a site as a primary site, or manually reconfigure site roles, the other site is automatically designated as the Standby site.

To manually reconfigure site roles, use either of the following tasks:

- Manually Reversing Site Roles with Enterprise Manager Cloud Control Console
- Manually Reversing Site Roles with EMCLI Commands

Manually Reversing Site Roles with Enterprise Manager Cloud Control Console

Learn how to manually reconfigure site roles with Enterprise Manager Cloud Control Console.

To manually reconfigure site roles with Enterprise Manager Cloud Control Console:

1. Login to Enterprise Manager Cloud Console as a user with `EM_SG_ADMINISTRATOR` role privileges.
2. From the Targets menu, click **Systems**.

   The Systems page is displayed.
3. Click the name of the system (**Generic System**) that you want to designate as the primary site.

   The Generic System page for the site is displayed.
4. On the home page of the system, from the Generic System menu, click **Site Guard**, and then click **Configure**.

   The Site Guard Configuration page is displayed.
5. Click **Set as Primary**.

Manually Reversing Site Roles with EMCLI Commands

Learn how to manually reverse the roles of the primary and secondary sites.

> **Note:**
>
> For information about logging in to the Enterprise Manager Command Line Interface, see *Oracle Enterprise Manager Command Line Interface Guide*.

To manually reverse the roles of the primary and standby sites, run the `update_siteguard_configuration` EMCLI command.

```
emcli update_siteguard_configuration
         -primary_system_name="primary_system_name"
         -standby_system_name="standby_system_name"
         [-reverse_role="flag_specifying_whether_system_roles_to_be_reversed"]
         [-role="new role for the standby site"]
```

> **Note:**
>
> [ ] indicates that the parameter is optional.

Parameter	Description
`-primary_system_name`	The name of the system that is the current primary site and needs to be designated as the new standby site.
`-standby_system_name`	The name of the system that is the current standby site and needs to be designated as the new primary site.
`-reverse_role`	Reverse roles between primary and standby systems. Optional. If specified, only one standby system can be specified with the `-standby_system_name` parameter.
`-role`	The new role for the site. Optional. One of the following:Primary, Standby, or ValidateStandby. Optional flag. • *Primary* - the roles of the primary and standby are swapped. • *Standby* - the role of the standby site will be changed from ValidateStandby to Standby. • *ValidateStandby* - the role of the standby site will be changed from Standby to ValidateStandby.

6

Troubleshooting Oracle Site Guard

In this section, learn how to troubleshoot and workaround Oracle Site Guard deploying and managing issues in your disaster recovery topology.

The following topic describe how to troubleshoot Oracle Site Guard:

- Operation Plan Issues

Operation Plan Issues

Learn how to troubleshoot operation plan issues.

The following topics provide tips for troubleshooting operation plan issues:

- Targets Not Discovered in Operation Plan Workflow
- Oracle WebLogic Server Managed Server Target Not Identified
- Manual Intervention Needed for Hung Operation Step
- OPMN Managed System Components Not Discovered In Operation-Plan Workflow
- Oracle RAC Database Not Discovered in Operation Plan
- Operation Step Failure When Target is Accessed with Sudo Privileges
- Inability to Associate Credentials for Targets Added to a Site
- Error While Deleting Or Updating Operation Plans
- Error Indicating Inability to Create Scalar Value While Creating Operation Plan
- Error While Creating Operation Plan Indicating Missing Node Manager Credentials
- Error Indicating Inability to Stage SWLIB Artifacts Due To Insufficient Disk Space on Target Host
- Operation Plan Fails Because of Inability to Copy WLS Utility Script to Domain Directory

Targets Not Discovered in Operation Plan Workflow

Learn why targets might not be discovered in an operation plan.

Issue

Targets like Oracle Database or Oracle Fusion Middleware farm, which are part of the system, might not be discovered in the operation plan workflow.

Description and Solution

This problem may occur if you have added targets to the system after creating the operation plan. Oracle Site Guard only includes those targets that are part of the system during the creation of the operation plan. If you have added new targets, re-create the operation plan. If you have customized the plan, make note of those

customizations before you re-create the plan, and re-customize the new plan again after it is re-created.

Oracle WebLogic Server Managed Server Target Not Identified

Learn why an Oracle WebLogic Server Managed Server might not be identified in an operation plan.

Issue

The Oracle WebLogic Server managed-server target, which is part of the Oracle WebLogic Server domain, is not updated or identified by Oracle Site Guard when creating the operation plan workflow.

Description and Solution

Ensure that the managed servers are running, before performing an automatic discovery in Enterprise Manager Cloud Control. If the managed servers are already running but are not visible in Enterprise Manager, try refreshing the WebLogic Domain target to discover the managed servers.

Manual Intervention Needed for Hung Operation Step

Learn what to do when an operation plan hangs.

Issue

When an operation step (for example, database switchover or failover, custom scripts, and so on) hangs, manual intervention is needed.

Description and Solution

Suspend the operation from the Enterprise Manager Cloud Control console. Do not stop the operation.

Manually correct the condition that caused the operation plan to hang. After completing the manual procedures, resume the operation to complete the Oracle Site Guard operation. Do not re-submit the operation.

If Oracle Site Guard determines that the components are already in the desired state, it performs a 'no operation' for all the start or stop or database switchover operations. This appropriately ends the process, and updates the sites with the required roles. If an operation step fails, and if manual intervention is needed to resolve the issue, you can either retry the failed step or confirm the manual step, and proceed with the execution of the operation.

> **Note:**
>
> Restart or resume the operation after every manual intervention. Ensure that you complete the operations that you have started.

OPMN Managed System Components Not Discovered In Operation-Plan Workflow

Learn why system components might not be discovered in an operation plan.

Issue

OPMN Managed System Components, which are part of the system, might not be discovered in the operation-plan workflow.

Description and Solution

Oracle Site Guard discovers only those OPMN managed system components represented in Enterprise Manager Cloud Control. For example, OPMN Managed System Components like Oracle HTTP Server and Oracle Web Cache are represented in Enterprise Manager Cloud Control. These components are discovered as part of the Oracle Fusion Middleware farm.

Oracle RAC Database Not Discovered in Operation Plan

Learn why a RAC database might not be discovered in an operation plan.

Issue

Oracle RAC Database, which is part of the system, is not discovered in the operation plan workflow.

Description and Solution

Oracle RAC Databases are grouped and represented under RAC Database target in the Enterprise Manager Cloud Control. When RAC database instances are discovered, the RAC database target is created, and all the database instances in the RAC deployment are grouped below the RAC database target. This issue may occur if individual RAC instance targets are added to the system, instead of the RAC database target. Oracle Site Guard cannot identify individual RAC instances.

Operation Step Failure When Target is Accessed with Sudo Privileges

Learn why a step might fail when using credentials with `sudo` privileges.

Issue

Site Guard operation step fails with the error `stageOmsFileEntry (Error)`, when using credentials with `sudo` privileges. You might encounter this issue during the Precheck operation as well.

Description and Solution

When the credentials used by Site Guard are configured to use `sudo` privileges to run as `root`, the `sudo` privilege must be configured as PDP (Privilege Delegation Provider) on all the agents running on the respective hosts of the target.

PDP can be configured from Enterprise Manager Cloud Control console. To configure PDP, go to **Setup** > **Security** > **Privilege Delegation** in the Enterprise Manager Cloud Control console.

Error While Creating Operation Plan Indicating Credential Association Not Configured

Learn why not configured credentials might cause an operation plan failure.

Issue

While creating an operation plan, you might encounter an error indicating that a target in the site does not have any credentials associated with it, despite having created and associated credentials for that target.

Description and Solution

This issue occurs when there are two targets with identical names in Enterprise Manger, and one of the targets is part of the site. For example, if a database instance target and a database system target are both named `db1`, and the database instance target is added to your site.

Delete the targets with identical names, and rediscover them. When you rediscover the targets ensure that each target name is unique across all of the Enterprise Manager targets.

Inability to Associate Credentials for Targets Added to a Site

Learn why credentials might not be associated for a target.

Issue

While configuring credentials for Oracle Site Guard, you might face issues when you attempt to associate credentials for a target. This occurs because the credential configuration for that target type is not enabled, or because the target does not show up in the list of targets for a specific target type. This error is seen despite adding the target to the site.

Description and Solution

This issue occurs when there are two targets with identical names in Enterprise Manger, and one of the targets is part of the site. For example, if a database instance target and a database system target are both named `db1`, and the database instance target is added to your site.

Delete the targets with identical names, and rediscover them. When you rediscover the targets ensure that each target name is unique across all of the Enterprise Manager targets.

Error While Deleting Or Updating Operation Plans

Learn why you might run into errors while updating or deleting an operation plan.

Issue

While deleting or updating an operation plan, you might encounter the following error:

```
Error:User does not have FULL_JOB privileges on execution with guid
XXXXXXXXXXXXXXXX
```

Description and Solution

This might occur when a user does not have the necessary privileges to delete or update the operation plan.

Login using the credentials that were used while creating the operation plan, and then delete or update the plan.

Error Indicating Inability to Create Scalar Value While Creating Operation Plan

Learn why you might not be able to create scalars in an operation plan.

Issue

While creating an operation plan, you might encounter an error such as the following:

```
oracle.sysman.ai.siteguard.model.exception.ConfigurationException: Cannot create
scalar value for name [PropertyType = DB_VERSION]. Value argument to the method
getScalarValue() is null
```

Description and Solution

Oracle Site Guard reads and uses the `DB_VERSION` property maintained by Enterprise Manager for database targets protected by Oracle Data Guard. The `DB_VERSION` property for the database can display as `NULL` in Enterprise Manager if a Data Guard switchover or failover occurred outside of Enterprise Manager (for example, if a Data Guard switchover was performed with `DGMGRL` or Site Guard.)

To correct this issue with Enterprise Manager Cloud Console, login to the Data Guard Administration page of the database target, and reset the `DataGuardStatus` property from `NULL` to `true`. On resetting the `DataGuardStatus` property, the other Data Guard related properties are automatically refreshed.

Error While Creating Operation Plan Indicating Missing Node Manager Credentials

Learn why credentials might be missing while creating an operation plan.

> **Note:**
>
> This issue and workaround are specific to Site Guard 12.1.0.7.

Issue

While creating an operation plan, you might encounter an error such as the following:

```
Credential association for credential type NODEMANAGER is missing for target
host_name belonging to system site_name.
```

Description and Solution

In Enterprise Manager, the Node Manager of a host is not a target type, and therefore, Enterprise Manager does not directly interact with it. Oracle Site Guard, on the other

hand, interacts with the Node Managers of hosts for managing disaster recovery operations of Oracle Fusion Middleware components. For this reason, Node Manager credentials must be configured and associated while configuring Oracle Site Guard. Since Enterprise Manager does not recognize Node Manager as a target type, you must create host credentials to be used with the node managers running on host targets, and associate these credentials with Oracle Site Guard using the Oracle Site Guard Credential Configuration page.

Error Indicating Inability to Stage SWLIB Artifacts Due To Insufficient Disk Space on Target Host

Learn why you might run into insufficient disk space on a host.

Issue

An operation plan may fail with an error similar to the following because of problems with disk space checks on a remote target host:

```
Value of property
oracle.sysman.core.swlib.disableFreeSpaceOnDestCheck:falseERROR [Wed Jun 03
07:29:31 PDT 2015]: Parameter validation failure. Reason: The space on the
destination host 'myhost.com' is not sufficient to stage the entity.
```

Description and Solution

The short-term solution to this issue is to ensure that the `/tmp` directory on the remote host has enough disk space available and then to disable the disk space check for Enterprise Manager jobs using `emcli`:

```
emctl set property -name oracle.sysman.core.swlib.disableFreeSpaceOnDestCheck -
value true
```

A more permanent solution to this issue is to inspect the Enterprise Manager logs (`emom.log` and `emoms.trc`) and determine the root cause for why this failure is occurring and fix that. The following example from the `emoms.trc` log file illustrates a disk space check failed on one particular VM host:

```
2015-06-03 10:53:16,628 [RJob Step 3818744] WARN swlib.storage logp.251 -
Unable to retrieve disk space details from agent myhost.com:/tmp/
JOB_17161DC66E0E5053BA46F40AE165',
output=[Error occurred during initialization of VM. Could not reserve enough
space for object heap
```

To determine the location of these log files, see section "Locating and Configuring Enterprise Manager Log Files" in the Enterprise Manager Cloud Control Administrator's Guide.

Operation Plan Fails Because of Inability to Copy WLS Utility Script to Domain Directory

Learn why copying might cause an operation plan failure.

Issue

An operation plan may fail because Site Guard fails to copy the WebLogic Server-related utility script (`siteguard_python_util.py`) to the WebLogic Server domain directory.

Description and Solution

This problem can occur if you use Privilege Delegation for the credential used to access the target host where the WebLogic Server resides. During WebLogic start/stop operations, Site Guard stages scripts to this host and then copies these scripts to the WebLogic Server domain directory. This copy process can fail if privilege delegation has not been set up correctly.

To avoid this issue, ensure that privileged credential delegation is correctly configured. For information about configuring privileged delegation for targets, see Oracle Enterprise Manager documentation. After this issue is corrected, you must delete the `siteguard_python_util.py` file from the WebLogic Server domain directory before you retry the failed operation.

Switchover and Failover Operation Issues

Learn how to troubleshoot switchover and failover operation issues.

The following topics provide tips for troubleshooting switchover and failover operation plan issues:

Oracle WebLogic Administration Server Not Starting After Switchover or Failover Operation

Learn why Oracle WebLogic Administration Server may not start after a switchover or failover operation.

Issue

The WebLogic Administration Server does not start after a switchover or failover operation. The output log file of the Administration Server reports an error, such as the following:

```
<Jan 19, 2012 3:43:05 AM PST> <Warning> <EmbeddedLDAP> <BEA-171520> <Could
not obtain an exclusive lock for directory: ORACLE_BASE/admin/soadomain/aserver/
soadomain/servers/AdminServer/data/ldap/ldapfiles. Waiting for 10 seconds and
then retrying in case existing WebLogic Server is still shutting down.>
```

Description and Solution

The error appears in the Administration Server log file due to unsuccessful lock cleanup. To fix this error, delete the `EmbeddedLDAP.lock` file (located at, `ORACLE_BASE/admin/`*`domain_name`*`/aserver/`*`domain_name`*`/servers/AdminServer/data/ldap/ldapfiles/`).

There may be multiple WebLogic Administration Server lock files that need be deleted. Repeat the process by attempting to start the WebLogic Administration Server and identifying each stale lock file that must be deleted.

Oracle WebLogic Administration Server not Restarting After Switchover or Failover Operation

Learn why Oracle WebLogic Administration Server may not restart after a switchover or failover operation.

Issue

The WebLogic Administration Server does not start after a switchover or failover operation. The Administration Server output log file reports the following error:

```
<Sep 16, 2011 2:04:06 PM PDT> <Error> <Store> <BEA-280061>
<The persistent store "_WLS_AdminServer" could not be deployed:
weblogic.store.PersistentStoreException:

[Store:280105]The persistent file store "_WLS_AdminServer" cannot open file
_WLS_ADMINSERVER000000.DAT.>
```

Description and Solution

This error might appear due to the locks from Network File System (NFS) storage. You must clear the NFS locks with the NFS utility of the storage vendor. You may also copy the `.DAT` file to a temporary location, and copy it back, to clear the locks.

Host Not Available During Switchover or Failover Operation

Learn why a host may not be available during a switchover or failover operation.

Issue

Some host on the new primary system might not be available, or might be down while performing switchover or failover operation. In such situations, Oracle Site Guard cannot perform any operation on these hosts.

Description and Solution

If the services running on these hosts are not mandatory, and the site can still be functional and active with the services running on the other nodes, the steps pertaining to the hosts, which are down, can be disabled by updating the operation plan. The Oracle Site Guard workflow skips all the disabled steps from the workflow.

Switchover or Failover Operation Fails When Oracle RAC Database Not Available

Learn why down Oracle RAC Databases may cause a switchover or failover operation to fail.

Issue

If all the Oracle RAC Database instances are down, the switchover or failover operation fails.

Description and Solution

While creating an operation plan, Oracle Site Guard determines the Oracle RAC Database instance on which the switchover or failover operation is performed. RAC

deployment can have multiple instances, and it is possible that some of the instances are down. Before running the switchover or failover operation, ensure that at least one instance is running. You can identify the name of the RAC instance, which is used by Oracle Site Guard to perform the role reversal operation, by running the `get_operation_plan_details` command.

Precheck and Healthcheck Issues

Learn how to troubleshoot Precheck and Healthcheck issues.

The following topics provide tips for troubleshooting Precheck and Healthcheck issues:

- Prechecks Failures
- Prechecks Hang When Oracle Management Agent Is Not Available
- Healthchecks Can Not Be Retried or Resumed

Prechecks Failures

Learn how to avoid Prechecks failures by running the `root.sh` script.

Issue

Prechecks fail and output the following error:

```
Nmo setuid status NMO not setuid-root (Unix-only)
```

Description and Solution

After installing the Oracle Management Agent, ensure that you run the `root.sh` script from the Enterprise Manager Cloud host and all hosts managed by Enterprise Manager. See Postinstallation Tasks in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

Prechecks Hang When Oracle Management Agent Is Not Available

Learn how not available Oracle Management Agents cause Prechecks to hang.

Issue

If the Oracle Management Agent is down, Prechecks hang while trying to run commands on the remote host.

Description and Solution

Ensure that all hosts involved in an operation are active, and all the configured scripts are available on remote hosts in the configured locations. If the Oracle Management Agent cannot be reached for some reason, then check the log files from the Enterprise Manager Cloud Control console. If you have identified the hosts that are down, skip the Precheck operation on those hosts.

Healthchecks Can Not Be Retried or Resumed

Learn why healthchecks can not be retried or resumed.

Issue

Healthchecks that fail cannot be retried or resumed.

Description and Solution

If a healthcheck fails, it cannot be retried or resumed. Either wait for the next healthcheck or execute a standalone precheck to verify a Site Guard operation plan's validity.

Oracle WebLogic Server Issues

Learn how to troubleshoot Oracle WebLogic Server issues.

The following topics provide tips for troubleshooting Oracle WebLogic Server issues:

- Node Manager Fails to Restart
- Node Manager Start/Stop Fails Due to Missing Properties File
- Oracle WebLogic Server Managed Server Fails to Start
- Oracle Site Guard Does Not Include Oracle WebLogic Server Instances That Are Migrated to a Different Host
- Error While Creating Operation Plan
- Oracle Site Guard Fails To Access Node Manager
- Unable to Associate Distinct Credentials for Node Manager
- Oracle WebLogic Server Password Updates and Site Guard Credentials
- Oracle Enterprise Manager Cannot Manage Domain Components

Node Manager Fails to Restart

Learn why Node Manager may fail to start.

Issue

Node Manager might fail to start due to an error, like the following:

```
<Sep 13, 2011 8:45:37 PM PDT> <Error> <NodeManager> <BEA-300033> <Could not
execute command "getVersion" on the node manager. Reason: "Access to domain
'base_domain' for user 'weblogic' denied".>
```

Description and Solution

This problem might occur if you have changed the Node Manager credentials and then have not run `nmEnroll` to ensure that the correct Node Manager username and password is supplied to each managed server.

To ensure that the correct Node Manager user name and password have been supplied, connect to WLST and execute the `nmEnroll` command using the following syntax:

```
nmEnroll(domain_directory, node_manager_home)
```

For example:

```
nmEnroll('C:/oracle/user_projects/domains/prod_domain',
'C:/oracle/wlserver_10.3/common/nodemanager')
```

> **Note:**
>
> Restart Node Manager for the changes to take effect.

Node Manager Start/Stop Fails Due to Missing Properties File

Learn why missing `nodemanager.properties` file causes Node Manager start/stop failures.

Issue

Node Manager Start or Stop operations may fail because of a missing `nodemanager.properties` file.

Description and Solution

Site Guard inspects the nodemanager.properties file to determine various properties of the Node Manager when starting or stopping the Node Managers during disaster recovery operations. If this file is missing, Node Manager start and stop operation steps will fail.

The `nodemanager.properties` file is created at a predetermined location the first time a Node Manager is started. Ensure that you have manually started all involved Node Managers at least once prior to executing any Site Guard operation plans that affect those Node Managers.

Oracle WebLogic Server Managed Server Fails to Start

Learn why an Oracle WebLogic Server Managed Server may fail to start.

Issue

The managed server does not start due to a connection failure of the WLS Administration Server in Enterprise Manager Cloud Control.

Description and Solution

To start the managed server, Oracle Site Guard requires the Administration Server and the Node Manager. To start and stop managed servers successfully, ensure that the Administration Server is running.

Oracle Site Guard Does Not Include Oracle WebLogic Server Instances That Are Migrated to a Different Host

Learn why Oracle WebLogic Server instances were not included in an operation plan.

Issue

Oracle Site Guard does not include the WebLogic Server instances that are migrated to a different host in the workflow.

Description and Solution

After you create the operation plan, Oracle Site Guard does not include the WebLogic Server instances involved in the operation plan that are migrated to different hosts, as a result of server migration.

After you complete the server migration, refresh the WebLogic Server farm target from the Enterprise Manager Cloud Control console to uptake the latest target changes in the farm. This step is mandatory for Enterprise Manager to resume its farm monitoring capabilities after any changes in the farm like server migration happens. After the farm target is refreshed, you need to recreate the Oracle Site Guard operation plans to include all of the farm targets in the Oracle Site Guard workflow. Any customizations made to operation plans must also be recreated.

Error While Creating Operation Plan

Invalid IP address causes operation plan creation failure.

Issue

While creating an operation plan, you see an error like the following:

```
oracle.sysman.ai.siteguard.model.common.exception.DAOException:
For hostName:
[2606:b400:800:89:214:4fff:fe46:2d52] credential of type HOSTNORMAL
does not exist for siteName: System1
```

Description and Solution
If you do not configure the listen address for the WebLogic Server instances running on the hosts where multiple IP addresses are configured, WebLogic Server randomly picks up an IP address, and reports that as the listen address. This IP address might not be a valid one, and it could be an issue when creating operation plans. To fix the issue with the Administration Console, configure WebLogic Server properly, with a resolvable listen address. After configuring Oracle WebLogic Server, restart the server, and re-discovered it again from the Enterprise Manager Cloud Control. For more information about listen address configuration, see: Recommendations for Oracle Fusion Middleware Components in *Oracle Fusion Middleware Disaster Recovery Guide*.

Oracle Site Guard Fails To Access Node Manager

Learn why Oracle Site Guard may fail to access Node Manager.

Issue

Oracle Site Guard is unable to access Node Manager even though the Oracle WebLogic Administrator Server is able to log in to the Node Manager.

Description and Solution

This issue occurs when the user name used to authenticate with Node Manager is randomly generate by the WebLogic Administration Server.

To correct this, perform the following steps:

1. Log in to the WebLogic Administration Server console.
2. Click **Domain** listed in the left-hand pane.

3. Click on the **Security** tab, and then click **Advanced link**.

   The Node Manager user name is displayed. The user name might appear to be a randomly generated string.

4. Update the Node Manager log-in credentials with the correct information.

Unable to Associate Distinct Credentials for Node Manager

Only one set of credentials is supported for all Node Manager instances running in the same host.

Issue

Oracle Site Guard is unable to associate different credentials for different Node Managers running on the same host.

Description

This is a limitation in the current version of Oracle Site Guard. The current version can only support one set of credentials for all the Node Managers running on a host. Ensure that all the Node Managers on a given host have been configured with an identical set of credentials.

Oracle WebLogic Server Password Updates and Site Guard Credentials

Learn why Oracle WebLogic Server start/stop operations may fail after updating the Oracle WebLogic Server Administrator password.

Issue

Oracle WebLogic Server start/stop operations in Site Guard operation plans may fail after you update the Oracle WebLogic Server Administrator password. This issue may occur even if Site Guard credential for the WebLogic Server target has been updated with the new password.

Description and Solution

In order for the updated Site Guard credentials to work with the updated WebLogic Server password, the WebLogic Administration Server must be restarted for the new password to be applicable for the administration functions that Site Guard performs. After each WebLogic Server password change, update the Site Guard credential and restart the WebLogic Administration Server.

Oracle Enterprise Manager Cannot Manage Domain Components

Learn how manage Oracle WebLogic domain components from Oracle Enterprise Manager after an Oracle Virtual Machine DR operation.

Issue

Management operations for WebLogic Server domain components may fail after WebLogic Server components running in Oracle Virtual Machine guests are relocated to a new site as part of a DR operation.

Description

To manage WebLogic Server domain components in an Oracle Virtual Machine guests after a Site Guard DR operation, perform an refresh on the WebLogic Server Domain target inside Enterprise Manager.

Database Issues

Learn how to troubleshoot database issues.

The following topics provide tips for troubleshooting database issues:

Prechecks for Database Switchover and Failover Operations Fail

Learn why Prechecks in a database switchover/failover operation may fail.

Issue

The Prechecks for database switchover or failover operations fail with the following error:

```
Database Status:
DGM-17016: failed to retrieve status for database "racs"
ORA-16713: the Data Guard broker command timed out
```

Description and Solution

This error might occur if the Data Guard Monitor process (DMON) in the target database instance is down.

> **Note:**
>
> The Data Guard Monitor process (DMON) is part of the Oracle Data Guard Broker.

If this error occurs, restart the database instance, and ensure that the DMON process is running. You can also see the database log file for DMON-process errors. Use the `CommunicationTimeout` parameter to select an appropriate time-out value for the environment.

Databases Protected by Data Guard Included in the Incorrect Operation Plan Category

Learn why a database may be included in the incorrect operation plan.

Issue

Oracle Site Guard adds the Oracle Data Guard protected database targets to the Start/Stop category instead of Switchover/Failover category of the operation plan.

Description and Solution

Oracle Site Guard uses the `DataGuardStatus` property maintained by Enterprise Manager for database targets to determine whether the database is protected by Data Guard. This determines which operation plan category the database is added to. If

the value of this property is `NULL` then Site Guard assumes that the database is not protected by Data Guard and adds the database target to the Start or Stop category of the operation plan, instead of the Switchover or Failover category.

The `DataGuardStatus` property for the database can display as `NULL` in Enterprise Manager if the Data Guard switchover or failover occurs outside of Enterprise Manager. For example, a Data Guard switchover is performed with `DGMGRL` or Site Guard.

Using the Enterprise Manager Cloud Console, log in to the Data Guard Administration page of the database target. Upon logging in, the Data Guard related properties are automatically refreshed.

Database Inaccessible When Opening a Site for Standby Validation

Learn why a database may be inaccessible when opening a site for Standby Validation.

Issue

After opening a Site Guard site in Standby Validation mode, one or more databases in the site are not accessible even though a database snapshot has been created.

Description and Solution

This can occur if the standby database does not have a snapshot service associated with the database. When configuring the standby site database, ensure that you have specifically created a separate snapshot service for the database so that the database snapshots can be accessed in Standby Validation mode. Refer to Oracle Database documentation for details on configuring services for databases.

Open For Validation plan operation fails with ORA-16692 error

Learn why open For Validation plan operation may fail.

Issue

The Open For Validation step of an Oracle Site Guard operation may fail with the following error:

```
ORA-16692: operation disallowed for a database or far sync instance that sends
redo data
```

Description and Solution

The Open For Validation plan operation converts a standby database to a snapshot standby. When the standby has a RedoRoutes property assigned to the primary database, it must be specified as (LOCAL : ...) in the rule. If not, Data Guard broker will not allow the conversion to a snapshot standby and the operation will fail with the ORA-16692 error. Refer to Oracle Database documentation for details on configuring RedoRoutes with the LOCAL primary database value.

Storage Issues

Learn how to troubleshoot storage issues.

The following topics provide tips for troubleshooting storage issues:

ZFS Storage Appliance Log in Failure

Learn why a logging in to a ZFS storage appliance may fail during an operation plan execution.

Issue

During a storage switchover or failover step of an Oracle Site Guard operation, logging into a ZFS appliance might fail, and you might see the following error in the log file generated by the `zfs_storage_role_reversal.sh` script:

```
Wrong credentials. Make sure that the given credentials are correct and
does not contain any special characters.
```

Description and Solution

This occurs if the password for the ZFS appliance credential contains special characters. Update the appliance password so that it does not contain special characters. Then, update the storage appliance credentials in the Enterprise Manager Credential Management Framework, and retry the operation step.

Storage Role Reversal Operation Failure

Learn why a storage role reversal may fail during an operation plan execution when deleting an empty project on the target appliance.

Issue

During a storage switchover or failover step of an Oracle Site Guard operation, storage role reversal operation might fail, and you might see the following error in the log file generated by the `zfs_storage_role_reversal.sh` script:

```
Error: The action could not be completed because the the target (or one of
its descendants) has the 'nodestroy' property set. Turn off the property for
'1_test' and try again.
```

Description and Solution

This occurs if the project has the `nodestroy` property set. This property is called as **Prevent destruction** in the Enterprise Manager Cloud Control interface.

Turn off this property and retry the operation step.

Storage Role Reversal Operation Failure

Learn why a storage role reversal operation may fail during an operation plan execution when executing the `confirm reverse` operation.

Issue

During a storage switchover or failover step of an Oracle Site Guard operation, storage role reversal operation might fail while executing `confirm reverse`, and you might see the following error in the log file generated by the `zfs_storage_role_reversal.sh` script:

```
Error: The action could not be completed because the mountpoint of
'<project_name>/<share_name>' would conflict with that of '<project_name>/
```

```
<share_name>' (/export/<project_name>/<share_name>). Change the mountpoint of
'<project_name>/<share_name>' and try again.
```

Description and Solution

This occurs if at least one of the shares inside all available packages for a given project, has exported as file system. Make sure that the `exported` property of all shares inside all packages for a given projects is turned off.

ZFS Storage Role Reversal Fails During Operation Plan Execution

Learn why a ZFS storage role reversal may fail during an operation plan execution because of insufficient privileges.

Issue

During a storage switchover or failover step of an Oracle Site Guard operation, ZFS storage role reversal operation might fail because the credentials used to perform ZFS operations do not have the necessary privileges to perform these ZFS operations.

Description and Solution

Ensure that the credentials used for ZFS operations are assigned the roles/privileges required for performing ZFS storage role reversal. Refer to the ZFS storage configuration section of this guide for additional details.

Remote Replication Targets List Multiple Appliances With The Same Name

Learn why remote replication targets on source ZFS Storage may list multiple target appliances with the same name during replication configuration..

Issue

When attempting to set up a replication action on source ZFS storage appliance, you may see multiple instances of the same replication target name in the drop-down list. This is a known ZFS issue.

Description and Solution

Only one of the instances of the target names seen in the drop-down list will actually work as a valid target. To determine which of these targets is a valid target, create a replication action using that target name/ and perform a replication sync. If the sync succeeds, then you have correctly found the replication target that works. However, if the replication sync fails, delete the replication action and create a new action using the next target name in the drop-down list. Keep repeating these steps until you have correctly found a target name with which replication succeeds.

ZFS Storage Role Reversal Failure

Learn why ZFS Storage role reversal may fail if storage scripts are configured to use physical addresses for clustered ZFS appliances.

Issue

ZFS storage role reversal scripts may fail with errors like “Replication action not found for given project on <source> appliance" if they are configured with source and target

appliance hostnames that are physical. This is especially true in the case of clustered (highly available) ZFS appliances.

Description and Solution

Physical hostnames or IP addresses are not relocated in a storage cluster when services failover from one storage head to another. If you use these physical addresses in your script configuration, and the storage appliance services relocate to a different head during an HA event, the storage script will be unable to find replication action id and its UUID.

Ensure that you use *management interfaces* (not physical interfaces) when configuring the source and target hostnames or IP addresses for Site Guard ZFS storage scripts.

7

Oracle Site Guard Command Line Interface

Manage Oracle Site Guard with Enterprise Manager Command Line Interface (EMCLI). EMCLI is a command line interface typically used in batch programs and scripts.

> **Note:**
>
> EMCLI commands are case-sensitive. For more information about EMCLI, see *Oracle Enterprise Manager Command Line Interface*.

This chapter includes the following EMCLI commands:

add_operation_plan_tags

A tag allows you to group and search operation plans across sites.

EMCLI command that adds tags to an operation plan.

Format

```
emcli add_operation_plan_tags
          -plan_name="Name of the operation plan"
          -tags="names of the tags separated by ;"
```

Parameter	Description
`-plan_name`	Name of the operation plan
`-tags`	Semicolon-separated list of tags to be added to the operation plan. The comma (,) is an invalid character.

```
emcli add_operation_plan_tags
   -plan_name="austin-switchover-plan"
   -tags="rack1_austin;created_by_john"

emcli add_operation_plan_tags
   -plan_name="austin-switchover-plan"
   -tags="created_by_john"
```

> **See Also:**
>
> The create_operation_plan and delete_operation_plan_tags commands.

add_site_properties

Adds user-defined properties to a site. Each property consists of a name and value associated with a site. Through **Site Properties** you can group and search for sites that share common attributes.

Format

```
emcli add_site_properties
          -system_name="Name of the system (site)"
          -properties="property name=value pairs separated by ;"
```

Parameter	Description
`-system_name`	Name of the generic system (site).
`-properties`	Semicolon (;) separated list of property name=value pairs to be added to the site.

Example

```
emcli add_site_properties -system_name="austin-system" -
properties="customer=acme corp; data center=austin dc"

emcli add_site_properties -system_name="utah-system" -properties="rack=08-57wvx"
```

> **Note:**
>
> Site Properties name/value pairs are not case-sensitive. Name and value are each restricted to 256 characters in length.

add_siteguard_aux_hosts

An auxiliary host is a host that is not part of the system but is managed by Oracle Enterprise Manager Cloud Control.

EMCLI command that adds an auxiliary host to an Oracle Site Guard system. Auxiliary hosts can execute any script. Other targets running on an auxiliary host are part of operation plans.

Format

```
add_siteguard_aux_hosts
-system_name="sytem name"
-host_name="host name"
```

Parameter	Description
`-system_name`	Name of the system.
`-host_name`	Name of the host.

```
emcli add_siteguard_aux_hosts
-system_name="sample-system"
```

```
-host_name="host1.example.com"

emcli add_siteguard_aux_hosts
-system_name="austin-system"
-host_name="host2.example.com"
-host_name="host3.example.com"
```

> **See Also:**
>
> The delete_siteguard_aux_host and get_siteguard_aux_hosts commands.

add_siteguard_script_credential_params

The user name and password in a credential passed to a script can be accessed within the script.

This EMCLI command adds a named credential parameter to an Oracle Site Guard script. See the following example:

```
emcli add_siteguard_script_credential_params
-script_id="id_associated_with_the_script"
-credential_name="name_of_the_credential"
-credential_owner="credential_owner"
```

> **Note:**
>
> The `-credential_owner` parameter is optional or conditionally optional.

Parameter	Description
`-script_id`	The script ID.
`-credential_name`	The name of the credential.
`-credential_owner`	The credential owner details. You need not The values of this parameter if the owner of the credential is same as that of the logged in user.

```
emcli add_siteguard_script_credential_params
-script_id="1"
-credential_name="NAMED_CREDENTIAL_X"

emcli add_siteguard_script_credential_params
-script_id="2"
-credential_name="NAMED_CREDENTIAL_Y"
-credential_owner="SG_ADMIN"
```

> **See Also:**
>
> The delete_siteguard_script_credential_params and get_siteguard_script_credential_params commands.

add_siteguard_script_hosts

Add one or more hosts to an Oracle Site Guard configuration script..

EMCLI command that adds a host to a configuration script. More than one host can added to a script. See the following example:

```
emcli add_siteguard_script_hosts
-script_id="script_id"
-host_name="host_name"
```

Parameter	Description
-script_id	The identification associated with the script.
-host_name	The host that you want to associate with the script. You can specify more than one host name.

```
emcli add_siteguard_script_hosts
-script_id="10"
-host_name ="host1.example.com"
```

> **See Also:**
>
> The create_siteguard_script and get_siteguard_script_hosts commands.

configure_siteguard_lag

Configure lag limits for databases in an Oracle Site Guard system.

EMCLI command that configures Apply Lag and Transport Lag for one or all databases in system.

Format

```
emcli configure_siteguard_lag
        -system_name="system_name"
        -property_name="apply_lag or transport_lag"
        -value="maximum_lag_limit_in_seconds"
        [-target_name="database_target_name"]
```

> **Note:**
>
> [] indicates that the parameter is optional or conditionally optional.

Parameter	Description
-system_name	The system on which you want to configure the threshold limit.
-property_name	The property name. Valid values are apply_lag and transport_lag.
-value	The threshold value to be configured (in seconds).
-target_name	The database target name for which the threshold limit is configured. If this parameter is not specified, then the threshold value is applied to all databases of the system.

```
emcli configure_siteguard_lag
       -system_name="example-system"
       -property_name="apply_lag"
       -value="1000"

emcli configure_siteguard_lag
       -system_name="example-system"
       -target_name="OID_db"
       -property_name="transport_lag"
       -value="2500"
```

> **See Also:**
>
> The get_siteguard_lag, update_siteguard_lag and delete_siteguard_lag commands.

create_operation_plan

Create Oracle Site Guard operation plans.

EMCLI command that creates a new operation plan.

Format

```
emcli create_operation_plan
         -system_name="name_of_the_system"
         [-primary_system_name="name_of_primary_system"]
         [-standby_system_name="name_of_standby_system"]
         [-operation="name_of_the_operation"]
         [-plan_name="name_of_the_operation_plan"]
         [-
like="name_of_the_operation_plan_from_which_the_steps_are_to_be_copied"]
           [-tags=list of tags separated by ; ]
```

> **Note:**
>
> [] indicates that the parameter is optional or conditionally optional.

Parameter	Description
-system_name	The name of the system. This option is used for start or stop operations.
-primary_system_name	The name of your system associated with the primary site. This option is used for switchover or failover operations.
-standby_system_name	The name of your system associated with the standby site. This option is used for switchover or failover operations.
-operation	The function of the operation. Example: switchover, failover, start or stop.
-plan_name	The name of the operation plan.
-like	Name of the operation plan from which the steps are to be copied. If this option is specified, system name, operation, and role are ignored.
-tags	A semicolon-separated list of tags to delete from the operation plan. The comma (,) is an invalid character.

```
emcli create_operation_plan
         -primary_system_name="austin"
         -standby_system_name="austin2"
         -operation="switchover"
         -name="austin-switchover-plan"

emcli create_operation_plan
         -system_name="austin"
         -operation="start"
         -name="austin-start-plan"
         -role="Primary"

emcli create_operation_plan
         -like="austin-start-plan"
         -name="austin-start-plan-copy"
```

> **See Also:**
>
> The get_operation_plans and submit_operation_plan commands.

create_siteguard_configuration

Create Oracle Site Guard configurations.

EMCLI command that creates a new Site Guard configuration.

Format

```
emcli create_siteguard_configuration
         -primary_system_name="name_of_primary_system"
         [-standby_system_name="name_of_standby_system"]
```

> **Note:**
>
> [] indicates that the parameter is optional or conditionally optional.

Parameter	Description
-primary_system_name	The name of the primary site system.
-standby_system_name	The name of the standby system. May be specified more than once.

```
emcli create_siteguard_configuration
         -primary_system_name="example1"

emcli create_siteguard_configuration
         -primary_system_name="example1"
         -standby_system_name="example2"
```

> **See Also:**
>
> The update_siteguard_configuration and delete_siteguard_configuration commands.

create_siteguard_credential_association

Associate credentials with targets in a site.

EMCLI command that associates credentials with site targets.

Format

```
emcli create_siteguard_credential_association
         -system_name="name_of_the_system"
         -credential_type="type_of_credential"
         -credential_owner="credential_owner"
         [-target_name="name_of_the_target"]
         [-credential_name="name_of_the_credential"]
         [–use_preferred_credential="flag_to_use_preferred_credential"]
```

> **Note:**
>
> [] indicates that the parameter is optional or conditionally optional.

Parameter	Description
-system_name	The name of the system.

Parameter	Description
-credential_type	The type of the credential. It can be: HostNormal, HostPrivileged, NodeManager, WLSAdmin, or DatabaseSysdba.
-credential_owner	The owner of the credential. This argument need not be specified if the owner of the credential is the same as the logged in user (Optional).
-target_name	The name of the target (Optional).
-credential_name	The name of the credential (Optional). If credential_name is not specified, then use_preferred_credential must be set to true.
–use_preferred_credential	Flag to use a preferred credential instead of a named credential (Optional). If use_preferred_credential is not true, then credential_name has to be specified.

```
emcli create_siteguard_credential_association
         -system_name="austin-system"
         -credential_type="HostNormal"
         -credential_name="HOST-SGCRED"
         -credential_owner="sysman"

emcli create_siteguard_credential_association
         -system_name="utah-system"
         -credential_type="HostPrivileged"
         -use_preferred_credential
         -credential_owner="sysman"

emcli create_siteguard_credential_association
          -system_name="austin-system"
          -target_name="austin-database-instance1;austin-database-instance2"
          -credential_type="DatabaseSysdba"
          -credential_name="HOST-DBCRED"
          -credential_owner="sysman"
```

See Also:

The delete_siteguard_credential_association and update_siteguard_credential_association commands.

create_siteguard_script

Create pre, post, and storage scripts for an Oracle Site Guard configuration.

EMCLI command that creates a script for a configuration. See the following format guide:

```
emcli create_siteguard_script
         -system_name="name_of_the_system"
         -operation="name_of_the_operation"
         -script_type="type_of_the_script"
```

```
                -path="path_of_the_script"
                -role="role_associated_with_the_system"
                -host_name="name_of_the_host_where_the_scripts_are_run"
        <optional>
                -component="path_of_the_entity_in_software_library" <optional>
                -
        runtime_script="if_prechecks_to_check_availability_of_this_script"
        <optional>
                -run_on="flag_specifying_the_host" <optional>
                -all_hosts="flag_to_run_script_on_all_the_hosts_in_the_system"
        <optional>
                -credential_type="type_of_the_credential" <optional>
                -credential_name="name_of_the_credential" <optional>
                -credential_owner="credential_owner"
```

Parameter	Description
`-system_name`	The name of the system.
`-operation`	The name of the operation. Name of the operation: `Switchover`, `Failover`, `Start`, or `Stop`.
`-script_type`	The type of the script. It can be `Mount`, `UnMount`, `Global-Pre-Script, Global-Post-Script, Pre Script`, `Post-Script`, `Storage-Failover`, or `Storage-Switchover`.
`-path`	The path to the script.
`-role`	Flag to configure script based on the system role. By default, the script is configured for both primary and standby roles for a given system. For example: `Primary` or `Standby`.
`-host_name`	The name of the host where this script will be executed. Can be specified more than once.
`-component`	The path to the entity in the software library. If component is specified, path should contain only the file name and its parameters.
`-runtime_script`	The value is `true` or `false`. If the script is designated as a runtime script, Precheck will not verify the existence of script. This parameter is used when the script is dynamically mounted or generated as part of execution of operation plan. By default, all scripts staged from the software library are designated as runtime scripts. The default value for scripts that are not staged from software library is `false`.
`-run_on`	Whether the script needs to be executed on only one of the available hosts (enter `any`) or on all hosts (enter `all`). Default value is all.
`-all_hosts`	Flag to allow the script to run on all the hosts in the system. This parameter overrides the `host_name`. Enter `true` or `false`.
`–credential_type`	Specify `HostNormal` or `HostPrivileged` if you have `root` privileges.

Parameter	Description
-credential_name	The name of the credential that is used to execute this script. If the value for the parameter credential_name is not specified, then the value for the parameter credential_type needs to be specified.
-credential_owner	The owner of the credential. If target_storage_credential_name and source_storage_credential_name are specified then the attribute credential_owner must be specified.

```
emcli create_siteguard_script
-system_name="sample-system"
-operation="Switchover"
-script_type="Precheck-Script"
-role="Primary"
-credential_type="HostNormal"
-path="/tmp/precheckscript"
-all_hosts="true"

emcli create_siteguard_script
-system_name="sample-system"
-operation="Failover"
-script_type="Post-Script"
-role="Standby"
-credential_name="MY_NAMED_HOST_CREDENTIAL"
-path="/tmp/postscript"
-host_name="host1.example.com"
-host_name="host2.example.com"
-run_on="any"
-runtime_script="true"

emcli create_siteguard_script
-system_name="sample-system"
-operation="Switchover"
-script_type="Pre-Script"
-credential_type="HostNormal"
-path="stop_mycomponent.sh"
-component="/Components/MyScripts/LCM_Operations"
-all_hosts="true"
-role="Primary"

emcli create_siteguard_script
-system_name="sample-system"
-operation="Switchover"
-script_type="Global-Pre-Script"
-credential_type="HostNormal"
-path="/tmp/prescript"
-all_hosts="true"
-target_storage_credential_name="SGCRED-TARGET-STORAGE"
```

```
-source_storage_credential_name="SGCRED-SOURCE-STORAGE"
-credential_owner="sysman"
```

> **See Also:**
>
> The update_siteguard_script, delete_siteguard_script, and get_siteguard_scripts commands.

delete_operation_plan

Delete an Oracle Site Guard operation plan.

EMCLI command that deletes an operation plan.

Format

```
emcli delete_operation_plan
         -plan_name="name_of_operation_plan"
```

Parameter	Description
-plan_name	The operation plan to delete.

```
emcli delete_operation_plan
         -plan_name="austin-switchover"
```

> **See Also:**
>
> The create_operation_plan and get_operation_plans commands.

delete_operation_plan_tags

Delete tags in Oracle Site Guard operation plans.

EMCLI command that deletes tags in an operation plan.

Format

```
emcli delete_operation_plan_tags
    -plan_name="Name of the operation plan"
    [-tags="names of the tags separated by ;"]
    [-all="names of the tags separated by ;"]
```

Parameter	Description
-plan_name	The name of the operation plan.
-tags	A semicolon-separated list of tags to delete from the operation plan. The comma (,) is an invalid character.
-all	All tags of the operation plan are deleted. This value overrides any choices passed to the tags argument.

```
emcli delete_operation_plan_tags
    -plan_name="austin-switchover-plan"
    -tags="rack1_austin;created_by_john"

emcli delete_operation_plan_tags
    -plan_name="austin-switchover-plan"
    -all
```

> **See Also:**
>
> The add_operation_plan_tags, create_operation_plan, delete_operation_plan, get_operation_plans commands.

delete_site_properties

Deletes user-defined properties from a site. Specific properties being deleted must already be associated with a site.

Format

```
emcli delete_site_properties
         -system_name="Name of the system (site)"
         -properties="property names list separated by ;"
         -all
```

Parameter	Description
-system_name	Name of the generic system (site)
-properties	Semicolon (;) separated list of property names to delete from the site.
-all	If this option is specified, all properties assigned to the site are deleted. This option overrides any choices made using the "-properties" option.

Examples

```
emcli delete_site_properties -system_name="austin-system" -properties="customer;
data center"

emcli delete_site_properties -system_name="utah-system" -properties="rack"

emcli delete_site_properties -system_name="austin-system" -all
```

delete_siteguard_aux_host

Delete auxiliary hosts associated with an Oracle Site Guard system.

EMCLI command that deletes an auxiliary host associated with a system. See the follwing example:emcli

```
 delete_siteguard_aux_host
-system_name="system_name"
-host_name="name_of_the_host" <Optional>
```

Parameter	Description
-system_name	The system on which you are performing the operation.
-host_name	The name of the auxiliary host to delete. If it is not specified, then all auxiliary hosts associated with the system are deleted. Ensure that the host name is part of the system specified in system_name.

```
emcli delete_siteguard_aux_host
       -system_name="sample-system"

emcli delete_siteguard_aux_host
       -system_name="sample-system"
       -host_name="host1.example.com"

emcli delete_siteguard_aux_host
       -system_name="austin-system"
       -host_name="host2.example.com"
```

> **See Also:**
>
> The add_siteguard_aux_hosts and get_siteguard_aux_hosts commands.

delete_siteguard_configuration

Delete the entire configurations of a system and all associated standby systems..

EMCLI command that deletes an Oracle Site Guard configuration. This command deletes scripts, credential associations, site associations, and operation plans in a system and standby systems.

Format

```
emcli delete_siteguard_configuration
        [-primary_system_name="name_of_the_primary_system"]
        [-standby_system_name="name_of_the_standby_system"]
        [-force="delete all Site Guard stale configurations"]
```

> **Note:**
>
> [] indicates that the parameter is optional or conditionally optional.

Parameter	Description
-primary_system_name	The name of the primary system.
-standby_system_name	The name of the standby system. If you do not specify this parameter, the Site Guard configuration of the specified primary system and all its standby system are deleted.

Parameter	Description
-force	Whether stale configuration(s) need to be deleted. A configuration can become stale if one or more sites involved in the configuration have been altered or deleted. Enter either true or false.

```
emcli delete_siteguard_configuartion
         -primary_system_name="austin-system1"

emcli delete_siteguard_configuration
         -standby_system_name="austin2-system2"

 emcli delete_siteguard_configuration
         -force="true"
```

> **See Also:**
>
> The create_siteguard_configuration and get_siteguard_configuration commands.

delete_siteguard_credential_association

Delete credential associations from Oracle Site Guard configurations.

EMCLI command that deletes a credential association from a configuration.

Format

```
emcli delete_siteguard_credential_association
         -system_name="name"
         -credential_type="type"
         [-target_name="name"]
```

> **Note:**
>
> [] indicates that the parameter is optional or conditionally optional.

Parameter	Description
-system_name	The system on which the service resides.
-credential_type	The credential type. It can be HostNormal, HostPrivileged, NodeManager, WLSAdmin, or DatabaseSysdba.
-target_name	The name of the target.

```
emcli delete_siteguard_credential_association
         -system_name="austin-system"
         -credential_type="HostNormal"
```

```
emcli delete_siteguard_credential_association
         -system_name="austin-system"
         -credential_type="DatabaseSysdba"
         -target_name="austin-database-instance"
```

> **See Also:**
>
> The create_siteguard_credential_association, update_siteguard_credential_association, and get_siteguard_credential_association commands.

delete_siteguard_lag

Delete Apply Lag and Transport Lag thresholds for databases in your system.

EMCLI command that deletes Apply Lag and Transport Lag threshold configured values for one or more Oracle Data Guard enabled databases of a system.

Format

```
emcli delete_siteguard_lag
         -system_name="system name"
         -property_name="lag value"
         [-target_name="database target name"]
```

> **Note:**
>
> [] indicates that the parameter is optional or conditionally optional.

Parameter	Description
-system_name	The system for which you want to configure the threshold limit.
-property_name	The property name. Valid values are apply_lag and transport_lag.
-target_name	The name of the target database for which the threshold limit is configured. If this parameter is not specified, then the threshold value is applied to all databases of the system.

```
emcli delete_siteguard_lag
       -system_name="austin-system"
       -property_name="apply_lag"

emcli delete_siteguard_lag
       -system_name="austin-system"
       -target_name="OID_db"
       -property_name="transport_lag"
```

> **See Also:**
>
> The update_siteguard_lag, configure_siteguard_lag, and get_siteguard_lag commands.

delete_siteguard_script

Delete scripts from an Oracle Site Guard configuration.

EMCLI command that deletes a script from a site configuration.

Format

```
emcli delete_siteguard_script
         -script_id="script id"
```

Parameter	Description
-script_id	The ID associated with the script.

```
emcli delete_siteguard_script
         -script_id="10"
```

> **See Also:**
>
> The create_siteguard_script, get_siteguard_scripts, and update_siteguard_script commands.

delete_siteguard_script_credential_params

Delete a credential passed to an Oracle Site Guard script.

EMCLI command that deletes a named credential, which is passed as a parameter to a script.

Format

```
emcli delete_siteguard_script_credential_params
        -script_id="Id associated with the script"
        [-credential_name="name of the credential"]
        [-credential_owner="credential owner"]
```

> **Note:**
>
> [] indicates that the parameter is optional or conditionally optional.

Parameter	Description
-script_id	The ID associated with the script.
-credential_name	The name of the credential. If this argument is not specified, all credentials associated with the script will be deleted.
-credential_owner	The owner of the credential. This parameter need not be specified if the owner of the credential is the same as the logged-in user.

```
emcli delete_siteguard_script_credential_params
        -script_id="1"
        -credential_name="NAMED_CREDENTIAL_X"

emcli delete_siteguard_script_credential_params
        -script_id="2"
        -credential_name="NAMED_CREDENTIAL_Y"
        -credential_owner="SG_ADMIN"

emcli delete_siteguard_script_credential_params
        -script_id="3"
```

> **See Also:**
>
> The add_siteguard_script_credential_params and get_siteguard_script_credential_params commands.

delete_siteguard_script_hosts

Delete hosts associated with an Oracle Site Guard script.

EMCLI command that deletes hosts associated with a script. See the following example:

```
emcli delete_siteguard_script_hosts
-script_id="script id"
-host_name="host_name"
```

Parameter	Description
-script_id	The ID associated with the script.
-host_name	The name of the host where this script will be executed. This parameter can be specified more than once.

```
emcli delete_siteguard_script_hosts
         -script_id="10"
         -host_name="host.example.com"
```

> **See Also:**
>
> The create_siteguard_script and add_siteguard_script_hostscommands.

get_operation_plan_details

Get details for your Oracle Site Guard operation plan.

EMCLI command that outputs complete and detailed information about an operation plan set up. When used in script mode, this command outputs details in JSON format.

Format

```
emcli get_operation_plan_details
         -plan_name="plan_name"
```

Parameter	Description
`-plan_name`	The name of the operation plan.

```
emcli get_operation_plan_details
         -plan_name="austin-switchover"
```

> **See Also:**
>
> The create_operation_plan and get_operation_planscommands.

get_operation_plans

List all your configured Oracle Site Guard operation plans.

EMCLI command that lists all configured operation plans for a site. The output incudes information such as the plan name, the operation name, the primary site name, the standby site name, and tags.

Format

```
emcli get_operation_plans
        [-plan_name="name_of_the_operation_plan"]
        [-operation="type_of_operation"]
        [-system_name="name_of_the_system"]
        [-primary_system_name="name_of_the_primary_system"]
        [-standby_system_name="name_of_the_standby_system"]
        [-tags="tag names separated by ;" ]
```

> **Note:**
>
> [] indicates that the parameter is optional or conditionally optional.

Parameter	Description
-plan_name	The name of the operation plan.
-operation	The name of the operation. For example, switchover, failover, start, or stop. If you do not specify this parameter, then all the operation plans will be listed.
-system_name	The name of system used in the operation plan. If you These values, then the values for -primary_system_name and -standby_system_name need not be specified.
-primary_system_name	The name of primary system used in the operation plan. You can The values of this parameter instead of the values of -system_name. The -standby_system_name parameter can also be additionally used for better filtering.
-standby_system_name	The name of the standby system used in the operation plan. You can The values of this parameter instead of the values of -system_name. The -primary_system_name parameter can also be additionally used for better filtering.
-tags	Semicolon-separated list of tags to be added to the operation plan. The comma (,) is an invalid character.

```
emcli get_operation_plans
        -operation="switchover"
        -system_name="austin-system"

emcli get_operation_plans
        -operation="switchover"
        -primary_system_name="austin-system"

emcli get_operation_plans
        -operation="failover"
        -standby_system_name="austin2-system"

emcli get_operation_plans
        -name="austin-switchover-plan"
        -system_name="austin-system"

emcli get_operation_plans
        -tags="rack1_austin"
```

See Also:

The create_operation_plan and submit_operation_plancommands.

get_site_properties

A tag allows you to group and search operation plans across sites.

Lists user-defined properties assigned to a site, or lists sites that match the specified property names and values.

Format

```
emcli get_site_properties
          -system_name="Name of the system (site)"
          -properties="property names list or name=value pairs separated by ;"
```

Parameter	Description
-system_name	Name of the generic system (site).
-properties	Semicolon (;) separated list of property names or name=value pairs to search for.

Example 1

The following example gets the values of specified property names for the specified site:

```
emcli get_site_properties -system_name="austin-system" -properties="customer;
data center"
```

Example 2

The following example gets values of all properties for the specified site:

```
emcli get_site_properties -system_name="utah-system"
```

Example 3

The following example gets all sites matching to the specified properties:

```
emcli get_site_properties -properties="data center=austin dc; rack=11-935zxp"
```

get_siteguard_aux_hosts

List all auxiliary hosts for your Oracle Site Guard system.

EMCLI command that outputs the list of all auxiliary hosts associated with a system.

Format

```
emcli get_siteguard_aux_hosts
       -system_name="system_name"
```

Parameter	Description
-system_name	The system on which you are performing the operation.

```
emcli get_siteguard_supported_targets
       -system_name="example-system"
```

> **See Also:**
>
> The add_siteguard_aux_hosts and delete_siteguard_aux_hostcommands.

get_siteguard_configuration

List the details of your Oracle Site Guard configuration.

EMCLI command that outputs a configuration set up. The output includes the details of the configuration for the primary and standby sites.

Format

```
emcli get_siteguard_configuration
         [-system_name="name_of_the_system"]
         [-primary_system_name="name_of_the_primary_system"]
         [-standby_system_name="name_of_the_standby_system"]
```

> **Note:**
>
> [] indicates that the parameter is optional or conditionally optional.

Parameter	Description
-system_name	The name of the system used in the operation plan. If this is specified, then -primary_system_name and -standby_system_name should not be specified.
-primary_system_name	The name of the primary system.
-standby_system_name	The name of the standby system.

```
emcli get_siteguard_configuartion
         -primary_system_name="austin-system"
         -standby_system_name="austin2-system"

emcli get_siteguard_configuration
         -system_name="austin-system"
```

> **See Also:**
>
> The create_siteguard_configuration and delete_siteguard_configurationcommands.

get_siteguard_credential_association

List all credentials configured for your system.

EMCLI command that lists the credential associations configured for a system. The output includes target names, credential name, and credential types.

Format

```
emcli get_siteguard_credential_association
         -system_name="name_of_the_system"
```

```
[-target_name="name_of_the_target"]
[-credential_type="type_of_the_credential"]
```

> **Note:**
>
> [] indicates that the parameter is optional or conditionally optional.

Parameter	Description
-system_name	The name of the system.
-target_name	The name of the target.
-credential_type	The type of the credential. One of HostNormal, HostPrivileged, NodeManager, WLSAdmin, or DatabaseSysdba.

```
emcli get_siteguard_credential_association
         -system_name="austin-system"
         -credential_type="HostNormal"

emcli get_siteguard_credential_association
         -system_name="austin-system"
         -target_name="austin-database-instance"
         -credential_type="DatabaseSysdba"
```

> **See Also:**
>
> The create_siteguard_credential_association and update_siteguard_credential_associationcommands.

get_siteguard_health_checks

Get the schedule of health checks for your operation plan.

EMCLI command that displays the schedule of health checks for an operation plan.

Format

```
emcli get_siteguard_health_checks
         -plan_name="name_of_the_operation_plan"
```

Parameter	Description
-plan_name	The name of the operation plan for which schedule of health checks has to be displayed.

```
emcli get_siteguard_health_checks
         -plan_name="austin-switchover"
```

> **See Also:**
>
> The schedule_siteguard_health_checks, stop_siteguard_health_checks, and run_prechecksCommands.

get_siteguard_lag

Get the limits configured for lags in your database systems.

EMCLI command that retrieves configured limits for the `apply_lag` and `transport_lag` lags for one or all databases of a system.

Format

```
emcli get_siteguard_lag
         -system_name="name_of_the_system"
         -property_name="lag_type"
         [-target_name="database_target_name"]
```

> **Note:**
>
> `[]` indicates that the parameter is optional or conditionally optional.

Parameter	Description
`-system_name`	The name of the system.
`-property_name`	The name of the property. Valid values are `apply_lag` and `transport_lag`.
`-target_name`	The name of the database. If the database name is not specified, the property is obtained for all databases in the system.

```
emcli get_siteguard_lag
         -system_name="austin-system"
         -property_name="apply_lag"

emcli get_siteguard_lag
         -system_name="austin-system"
         -target_name="OID_db"
         -property_name="transport_lag"
```

> **See Also:**
>
> The update_siteguard_lag, configure_siteguard_lag, and delete_siteguard_lagCommands.

get_siteguard_script_credential_params

Get all credentials used as parameters for an Oracle Site Guard script.

EMCLI command that outputs all the credential parameters for a script.

Format

```
emcli get_siteguard_script_credential_params
    -script_id="Id_associated_with_the_script"
    [-credential_name="name_of_the_credential"]
    [-credential_owner="credential_owner"]
```

> **Note:**
>
> [] indicates that the parameter is optional or conditionally optional.

Parameter	Description
-script_id	The ID associated with the script.
-credential_name	The name of the credential. If this argument is not specified, all credentials associated with the script will be deleted.
-credential_owner	The owner of the credential. This parameter need not be specified if the owner of the credential is the same as the logged-in user.

```
emcli get_siteguard_script_credential_params
        -script_id="1"
        -credential_name="NAMED_CREDENTIAL_X"

emcli get_siteguard_script_credential_params
        -script_id="3"

emcli get_siteguard_script_credential_params
        -script_id="3"
        -credential_owner="SG_ADMIN"
```

> **See Also:**
>
> The add_siteguard_script_credential_params and delete_siteguard_script_credential_paramscommands.

get_siteguard_script_hosts

List all hosts associated with your Oracle Site Guard script.

EMCLI command that lists the hosts used in a script. The output includes host names.

Format

```
emcli get_siteguard_script_hosts
         -script_id="script_id"
```

Parameter	Description
-script_id	The ID associated with the script.

```
emcli get_siteguard_script_hosts
         -script_id="10"
```

> **See Also:**
>
> The create_siteguard_script and add_siteguard_script_hostscommands.

get_siteguard_scripts

List all Oracle Site Guard scripts in your system.

EMCLI command that outputs the scripts associated with a system. The output incudes the script ID, the type, the operation, paths, and roles.

Format

```
emcli get_siteguard_scripts
         -system_name="system_name"
         -operation="operation_name"
         -script_type="type_of_the_script"
         [-role="role_of_the_system"]
```

> **Note:**
>
> [] indicates that the parameter is optional or conditionally optional.

Parameter	Description
-system_name	The name of the system.
-operation	The name of the operation. One of switchover, failover, start, or stop.
-script_type	The type of the script. One of mount, unmount, pre-script, post-script, global pre-script, global post-script, storage-failover, or storage-switchover.
-role	Filters the scripts based on the role associated with the system. One of Primary or Standby.

```
emcli get_siteguard_scripts
         -system_name="austin-system"
         -operation="Switchover"
         -script_type="Pre-Script"

emcli get_siteguard_scripts
```

```
-system_name="austin-system"
-operation="Switchover"
-script_type="Pre-Script"
-role="Primary"
```

> **See Also:**
>
> The create_siteguard_script, delete_siteguard_script, and update_siteguard_scriptcommands.

get_siteguard_supported_targets

List all targets in your Oracle Site Guard system.

EMCLI command that outputs the list of all supported targets in a system.

Format

```
emcli get_siteguard_supported_targets
       -system_name="system name"
       [-target_type="target type"]
```

> **Note:**
>
> [] indicates that the parameter is optional or conditionally optional.

Parameter	Description
-system_name	The name of the system.
-target_type	The type of the target.

```
emcli get_siteguard_supported_targets
          -system_name="austin-system"

emcli get_siteguard_supported_targets
          -system_name="austin-system"
          -target_type="weblogic"

emcli get_siteguard_supported_targets
          -system_name="austin-system"
          -target_type="database"
```

run_prechecks

Run prechecks for your Oracle Site Guard operation plan.

EMCLI command that runs prechecks for an operation plan.

Format

```
emcli run_prechecks
        -plan_name="name_operation_plan"
        [-database_lag_checks="true or false"]
```

> **Note:**
>
> [] indicates that the parameter is optional or conditionally optional.

Parameter	Description
-plan_name	The name of the operation plan.
-database_lag_checks	Run database lag checks as part of Prechecks for all Data Guard configured databases. One of true or false.

```
emcli run_prechecks
         -plan_name="austin-switchover"

emcli run_prechecks
         -plan_name="austin-switchover"
         -database_lag_checks="true"
```

> **See Also:**
>
> The create_operation_plan, get_operation_plans, and submit_operation_plancommands.

schedule_siteguard_health_checks

Schedule health checks for your operation plans.

EMCLI command that schedules health checks for an operation plan. See the following example:

```
emcli schedule_siteguard_health_checks
-plan_name="name of the operation plan"
-schedule= "start_time:yyyy/MM/dd HH:mm;
tz:java timezone ID;
frequency:interval/weekly/monthly/yearly;
repeat:tx;
end_time:yyyy/MM/dd HH:mm;
grace_period:xxx;"
-email="email_address_to_be_notified" <Optional>
-notify_on_failure <Optional>
```

Parameter	Description
-plan_name	The name of the operation plan for which health checks have to be scheduled.

Parameter	Description
-schedule	The schedules at which health checks have to be scheduled. start_time - The time when health checks have to start executing. tz - The time-zone ID. frequency - Valid values are once/interval/weekly/monthly/yearly. If frequency is set to interval, then repeat has to be specified. If frequency is set to weekly or monthly, days has to specified. If frequency is set to yearly, both days and months have to specified. repeat - The frequency with which health checks have to be repeated. This is mandatory only if frequency is set to interval. days - The list of days separated by commas. This is required only if frequency is weekly, monthly, or yearly).If frequency is weekly, then valid range is 1 to 7. If frequency is monthly or yearly, then valid range is 1 to 30. months - The list of months separated by commas. This is required only if frequency is yearly. Valid range is 1 to 12. end_time - The end time for health check executions. If not specified, health checks will run indefinitely. grace_period - The grace period in minutes. If the value are set to false, Prechecks will not be executed.
-email	The email address that needs to be used for notification of health-check report. This email address must be a configured email address for the current user.
-notify_on_failure	If set, health check report will be e-mailed on failed execution only.

```
emcli schedule_siteguard_health_checks
-plan_name="sample-switchover"
-schedule="start_time:2014/06/10 15:45"

emcli schedule_siteguard_health_checks
-plan_name="sample-switchover"
-schedule="start_time:2014/10/29 2:00;frequency:interval;repeat:1d"
-email="admin@example.com"
-notify_on_failure

emcli schedule_siteguard_health_checks
-plan_name="sample-failover"
-schedule="start_time:2014/08/10 01:00;frequency:interval;repeat:1w"

emcli schedule_siteguard_health_checks
```

```
-plan_name="austin-failover"
-schedule="start_time:2014/08/10 1:00;frequency:weekly;days:6,7; grace
period:60;tz:America/New_York"
```

> **See Also:**
>
> The get_siteguard_health_checks, stop_siteguard_health_checks, and run_prechecks commands.

stop_siteguard_health_checks

Stop all heath check future executions in your Oracle Site Guard operation plan.

EMCLI command that stops health executions in an operation plan.

Format

```
emcli stop_siteguard_health_checks
        -plan_name="name_of_the_operation_plan"
```

Parameter	Description
-plan_name	The name of the operation plan for which health check executions has to be stopped.

```
emcli stop_siteguard_health_checks
         -plan_name="austin-switchover"
```

> **See Also:**
>
> The schedule_siteguard_health_checks, get_siteguard_health_checks, and run_prechecks commands.

submit_operation_plan

Submit an Oracle Site Guard operation plan for execution.

EMCLI command that submits an operation plan for execution.

Format

```
emcli submit_operation_plan
         -plan_name="name_of_operation_plan"
         [-disable_run_prechecks="whether_or_not_to_run_prechecks"]
         [-stop_primary="whether_to_stop_the_primary_site_during_failover"]
         [-database_lag_checks="whether to run database lag checks"]
         [-database_trace_enable="whether to enable database tracing"]
         [-database_immediate_failover="whether to fail over the database
immediately"]
         [-ignore_warnings]
```

> **Note:**
>
> [] indicates that the parameter is optional or conditionally optional.

Parameter	Description
-plan_name	The name of the operation plan.
-disable_run_prechecks	Not to run prechecks. One of true or false.
-stop_primary	Whether to stop targets on primary site during a Failover operation. One of true or false.
-database_lag_checks	Run database lag checks as part of Prechecks for all Data Guard configured databases. One of true or false.
-database_trace_enable	Send additional database trace messages to logs during Switchover or Failover operations. One of true or false.
-database_immediate_failover	Fail over the database immediately and do not apply redo logs. One of true or false.
-ignore_warnings	Ignore non-fatal warnings when performing failovers.

```
emcli submit_operation_plan
         -plan_name="example-switchover"

emcli submit_operation_plan
         -plan_name="example-switchover"
         -disable_run_prechecks

emcli submit_operation_plan
         -plan_name="austin-switchover"
         -disable_run_prechecks="true"
         -database_trace_enable="true"

emcli submit_operation_plan
         -plan_name="austin-switchover"
         -database_lag_checks="true"

emcli submit_operation_plan
         -plan_name="austin-failover"
         -stop_primary="true"
         -database_immediate_failover="true"

emcli submit_operation_plan
            -plan_name="austin-failover"
            -ignore_warnings

emcli submit_operation_plan
            -plan_name="austin-failover"
            -stop_primary -ignore_warnings
```

> **See Also:**
>
> The create_operation_planand get_operation_planscommands.

update_operation_plan

Update you Oracle Site Guard operation plan.

EMCLI command that updates an operation plan.

```
emcli update_operation_plan
-plan_name="name of the plan"
-step_number="plan step number to update"
-target_host="name of the target host"
-target_name="name of the target"
-error_mode="the error mode" <Optional>
-enabled="flag specifying whether the step should be enabled" <Optional>
-execution_mode="execution mode" <Optional>
-execution_group=when execution_mode is parallel, then targets sharing the same
execution group will execute in parallel <Optional>
-timeout="timeout in seconds" <Optional>
-move="direction in which to move step" <Optional>
-delete "whether step should be deleted" <Optional>
```

Parameter	Description
-plan_name	The name of the operation plan.
-step_number	The number of the step that should be updated.
-target_host	The name of the system. Specifying this will update all the steps related to this target host.
-error_mode	The function of the operation. One of stop or continue.
-enabled	One of true or false.
-execution_mode	The execution mode. One of Serial or Parallel.
-execution_group	The execution group of the target, all members of which to be executed in parallel, an integer between 1 and 10 with each group executed sequentially.
-timeout	Timeout in seconds for the execution of the step, between 1 second and 86400 seconds (24 hours).
-move	Change the order. One of Up or Down.
-delete	Whether you want to delete steps. One of true or false.

```
emcli update_operation_plan
-name="sample-switchover"
-step_number="1"
-error_mode="Continue"
-enabled="true"
-execution_mode="Serial"
-execution_group="2"
-timeout="10800"
```

```
emcli update_operation_plan
-name="sample-switchover"
-step_number="5"
-move="Up"

emcli update_operation_plan
-name="sample-switchover"
-target_host="myhost.example.com"
-error_mode="Continue"
-enabled="true"

emcli update_operation_plan
-name="example-switchover"
-target_name="/Farm1/MyDomain"
-delete="true"
```

> **See Also:**
>
> The create_operation_plan and get_operation_plan_detailscommands.

update_site_properties

Updates existing user-defined properties assigned to a site. Property names being updated must already be assigned to that site. To add new properties, use emcli add_site_properties command.

Format

```
emcli update_site_properties
          -system_name="Name of the system (site)"
          -properties="property name=value pairs separated by ;"
```

Parameter	Description
-system_name	Name of the generic system (site).
-properties	Semicolon (;) separated list of property name=value pairs to be updated for the site.

Example

```
emcli update_site_properties -system_name="austin-system" -
properties="customer=acme corp; data center=austin dc"

emcli update_site_properties -system_name="utah-system" -
properties="rack=08-57wvx"
```

update_siteguard_configuration

Add additional standby systems to your primary system.

EMCLI command that adds standby systems to an primary system. One primary system can be associated with one or more standby systems.

Format

```
emcli update_siteguard_configuration
         -primary_system_name="primary_system_name"]
         -standby_system_name="standby_system_name"]
         [-reverse_role="whether_to_reverse_system_roles"]
         [-role="new role of standby system"]
```

> **Note:**
>
> [] indicates that the parameter is optional or conditionally optional.

Parameter	Description
-primary_system_name	The name of the primary system.
-standby_system_name	The name of the standby system to add. This parameter can be specified more than once.
-reverse_role	Whether to reverse role of site from standby to primary. One of true or false. Default value is false. If this option is specified, only one standby system name can be submitted in the -standby_system_name parameter.
-role	The new role of the standby system. One of Primary, Standby, or ValidateStandby. If this option is specified, only one standby system name can be specified using -standby_system_name. If Primary is specified, roles of primary and standby systems will be swapped. If Standby is specified, role of standby system will be updated from Validate Standby to Standby. If Validate Standby is specified, role of standby system will be updated from Standby to Validate Standby.

```
emcli update_siteguard_configuartion
         -primary_system_name="austin-system"
         -standby_system_name="austin2-system"

emcli update_siteguard_configuration
         -primary_system_name="austin-system"
         -standby_system_name="austin2-system"
         -reverse_role

emcli update_siteguard_configuration
         -primary_system_name="austin-system"
         -standby_system_name="utah-system"
         -role="ValidateStandby"
```

> **See Also:**
>
> The create_siteguard_configuration and delete_siteguard_configurationcommands.

update_siteguard_credential_association

Update Oracle Site Guard credential associations.

EMCLI command that updates a credential association for a system.

Format

```
emcli update_siteguard_credential_association
         -system_name="name_of_the_system"
         -credential_type="type_of_the_credential"
         -credential_owner="credential_owner"
         [-target_name="name_of_the_target"]
         [-credential_name="name_of_the_credential"]
         [–use_preferred_credential="whether to use a preferred credential"]
```

> **Note:**
>
> [] indicates that the parameter is optional or conditionally optional.

Parameter	Description
-system_name	The name of the system.
-target_name	The name of the target.
-credential_type	The type of the credential. It can be HostNormal, HostPrivileged, WLSAdmin, or DatabaseSysdba.
-credential_name	The name of the credential.
–use_preferred_credential	If you are using Preferred Credentials, then specify true. If use_preferred_credential is false, then you must specify credential_name.
-credential_owner	The owner of the credential. You need not specify this argument if the owner of the credential is same as logged in user.

```
emcli update_siteguard_credential_association
         -target_name="austin-database-instance"
         -credential_type="DatabaseSysdba"
         -credential_name="HOST-DBCRED"
         -credential_owner="sysman"

emcli update_siteguard_credential_association
         -target_name="austin-database-instance"
         -credential_type="DatabaseSysdba"
         -credential_name="HOST-DBCRED"
         -credential_owner="sysman"
```

> **See Also:**
>
> The delete_siteguard_credential_association and create_siteguard_credential_associationcommands.

update_siteguard_lag

Update lag thresholds for databases in your system.

EMCLI command that updates the apply lag and transport lag threshold values for one or all databases in a system.

Format

```
emcli update_siteguard_lag
        -system_name="system_name"
        -property_name="lag_type"
        -value="max_limit"
        [-target_name="database_target_name"]
```

> **Note:**
>
> [] indicates that the parameter is optional or conditionally optional.

Parameter	Description
-system_name	The system for which you want to configure the threshold limit.
-target_name	The database target name for which the threshold limit is configured. If this parameter is not specified, then the threshold value is applied to all databases of the system.
-property_name	The property name. Valid values are apply_lag and transport_lag.
-value	The threshold value to be updated (in seconds).

```
emcli update_siteguard_lag
       -system_name="example-system"
       -property_name="apply_lag"
       -value="1000"

emcli update_siteguard_lag
       -system_name="example-system"
       -target_name="OID_db"
       -property_name="transport_lag"
       -value="2500"
```

> **See Also:**
>
> The get_siteguard_lag, configure_siteguard_lag, and delete_siteguard_lagcommands.

update_siteguard_script

Update the path and flag associated with an Oracle Site Guard script.

EMCLI command that updates the path and the `all_hosts` flag associated with a script.

```
emcli update_siteguard_script
-script_id="ID_associated_with_the_script"
-path="path_of_the_script" <Optional>
-component="path of the entity in Software library" <Optional>
-runtime_script="if_prechecks_to_check_availability_of_the_script"
<Optional>
–credential_type="type_of_credential" <Optional>
-credential_name="name of the credential" <Optional>
-host_name="name_of_the_host_where_this_script_will_run" <Optional>
-run_on="whether to run on ANY or ALL hosts" <Optional>
-all_hosts="whether to run the script on all the hosts in the system"
<Optional>
-credential_owner="credential_owner" <Optional>
```

Parameter	Description
`-script_id`	The script ID.
`-path`	The path to the script.
`-component`	The path to the entity in the software library. If the values for this parameter are specified, the path should contain only the file name and its parameters.
`-runtime_script`	Whether the script is a runtime script. If a script is designated as a runtime script, Precheck does not verify the script. This option can be used when the script is dynamically mounted or generated as part of execution of an operation plan. By default, all scripts staged from software library are designated as runtime scripts. Default value is false for scripts that are not staged from software library.
`–credential_type`	The type of the credential. One of `HostNormal` or `HostPrivileged`.
`-credential_name`	The name of the credential. If no value is specified, then the values for the parameter `credential_type` must be specified.
`-host_name`	Name of the host where this script will be run. Can be specified more than once.
`-run_on`	Whether the script needs to be executed on one of the available hosts (`any`) or on all hosts (`all`); default value is `all`.

Parameter	Description
-all_hosts	Optional flag to allow the script to run on all the hosts in the system. Specify true or false. Overrides all values entered in the host_name parameter.
-credential_owner	The owner of the credential. This argument need not be specified if the owner of the credential is same as logged in user.

Examples

```
emcli update_siteguard_script
-script_id="10"
-path="/tmp/script"
-all_hosts="true"

emcli update_siteguard_script
-script_id="10"
-path="stop_mycomponent.sh"
-component="/Components/MyScripts/LCM_Operations"
-all_hosts="true"

emcli update_siteguard_script
example.com-script_id="10"
example.com-host_name="host1.example.com"
example.com-host_name="host2.example.com"
example.com-run_on="any"

emcli update_siteguard_script
example.com-script_id="10"
example.com-all_hosts="false"
example.com-credential_name="MY_NAMED_HOST_CREDENTIAL"
example.com-host_name="host1.example.com"

emcli update_siteguard_script
example.com-script_id="16"
example.com-path="/tmp/script"
example.com-credential_type="HostPrivileged"
example.com-runtime_script="true"
```

See Also:

The create_siteguard_script, get_siteguard_scripts, and delete_siteguard_scriptcommands.

8

Upgrading or Downgrading Oracle Site Guard

Learn how to upgrade or downgrade Oracle Site Guard in your Enterprise Manager Cloud Control environment.

This chapter includes the following sections:

- Upgrading Oracle Site Guard
- Downgrading Oracle Site Guard

Upgrading Oracle Site Guard

Upgrade Oracle Site Guard from version 13.3.1.0.0

To upgrade from Oracle Site Guard (12.1.x, 13.1.x, 13.2.x) to Oracle Site Guard 13.3.1.0.0 operation plans must be recreated. Perform the following steps:

1. Delete all of the existing Oracle Site Guard operation plans by following the steps listed in Deleting an Operation Plan.

   > **Note:**
   >
   > Oracle recommends that you make a note of the details of the operation plans that you are deleting, as you will need to recreate these plans after the upgrade.

2. Delete all of the existing Oracle Site Guard configurations that you created using the instructions provided in Configuring Oracle Site Guard .

   Delete the configurations in the following order:

   a. Delete all configured Storage Scripts
   b. Delete all configured Pre Scripts and Post Scripts
   c. Delete all credential associations
   d. Delete all configured standby systems
   e. Delete the Oracle Site Guard configuration

   > **Note:**
   >
   > Oracle recommends that you make a note of the details of the configurations that you are deleting, as you will need to recreate these configurations after the upgrade.

3. Upgrade the Oracle Enterprise Manager Fusion Middleware plug-in (for example, from 12.1.0.7 to 13.3.1.0.0). For information about Oracle Enterprise Manager plug-ins, see Managing Plug-Ins.
4. Recreate the Oracle Site Guard configurations that you had deleted in step 2, using the configuration details that you noted down.

   Follow the procedure described in Configuring Oracle Site Guard .
5. Recreate the Oracle Site Guard operation plans that you had deleted in step 1, using the operation plan details that you noted down. Follow the instructions provided in Creating Operation Plans.

Downgrading Oracle Site Guard

Downgrade Oracle Site Guard from version 12.1.0.7 to version 12.1.0.6.

To downgrade from Oracle Site Guard (12.1.0.7) to Oracle Site Guard (12.1.0.6):

1. Delete all of the existing Oracle Site Guard operation plans by following the steps listed in Deleting an Operation Plan.

   > **Note:**
   >
   > Oracle recommends that you make a note of the details of the operation plans that you are deleting, as you will need to recreate these plans after the upgrade.

2. Delete all of the existing Oracle Site Guard configurations that you created using the instructions provided in Configuring Oracle Site Guard .

   Delete the configurations in the following order:

   a. Delete all configured Storage Scripts
   b. Delete all configured Pre Scripts and Post Scripts
   c. Delete all credential associations
   d. Delete all configured standby systems
   e. Delete the Oracle Site Guard configuration

   > **Note:**
   >
   > Oracle recommends that you make a note of the details of the configurations that you are deleting, as you will need to recreate these configurations after the upgrade.

3. Downgrade the Oracle Enterprise Manager Fusion Middleware plug-in (for example, from 12.1.0.7 to 12.1.0.6). For information about Oracle Enterprise Manager plug-ins, see Managing Plug-Ins.
4. Recreate the Oracle Site Guard configurations that you had deleted in step 2, using the configuration details that you noted down.

   Follow the procedure described in Configuring Oracle Site Guard .

5. Recreate the Oracle Site Guard operation plans that you had deleted in step 1, using the operation plan details that you noted down. Follow the instructions provided in Creating Operation Plans.

A

Passing Credentials as Parameters

Credentials passed as parameters to user-defined scripts are available as an input stream. Learn how to pass and extract credentials in your scripts.

This appendix includes the following sections:

Passing Credentials as Parameters

Pass credentials as parameter to your Oracle Site Guard scripts.

The following scripts illustrate how to pass credentials as parameters:

- extract_credentials_sample_script.sh
- extract_credentials_sample_script.py
- extract_credentials_sample_script.pl

> **Note:**
>
> The scripts in this appendix illustrate sample scripts only. Change and adapt them to suit your environment.

extract_credentials_sample_script.sh

Extract credentials from your Oracle Site Guard scripts.

```
#!/bin/bash

all_users=
all_passwords=
no_of_users=
no_of_passwords=

get_user_name() {
    local index=$(expr $1)

    if [ "$no_of_users" -lt $index ]; then
        echo ""
    else
        echo $(echo "$all_users" | awk -v userNameIndex="$index" -
F'<<SiteGuard_User>>' '{print $userNameIndex}')
    fi
}

get_password() {
    local index=$(expr $1)

    if [ "$no_of_passwords" -lt $index ]; then
```

```
        echo ""
    else
        echo $(echo "$all_passwords" | awk -v passwordIndex="$index" -
F'<<SiteGuard_Password>>' '{print $passwordIndex}')
    fi
}

load_credentials() {
    read -s all_credentials

    all_users=$(echo "${all_credentials}" | awk -F'<<SiteGuard_Credentials>>'
'{print $1}')
    all_passwords=$(echo "${all_credentials}" | awk -
F'<<SiteGuard_Credentials>>' '{print $2}')
    no_of_users=$(expr $(echo "$all_users" | awk -F'<<SiteGuard_User>>' '{print
NF}'))
    no_of_passwords=$(expr $(echo "$all_passwords" | awk -
F'<<SiteGuard_Password>>' '{print NF}'))

    if [ "$no_of_users" -ne "$no_of_passwords" ]; then
        echo "INFO: Total no. of users : '$no_of_users'"
        echo "INFO: Total no. of passwords : '$no_of_passwords'"
        echo "ERROR: Number of User Names and number of Passwords do not match"
        exit 1
    else
        echo "Total of '$no_of_users' credentials found"
    fi
}

load_credentials

userName=$(get_user_name '1')
password=$(get_password '1')

echo "[1] UserName : '$userName', Password : '$password'"

userName=$(get_user_name '2')
password=$(get_password '2')

echo "[2] UserName : '$userName', Password : '$password'"

userName=$(get_user_name '3')
password=$(get_password '3')

echo "[3] UserName : '$userName', Password : '$password'"

userName=$(get_user_name '4')
password=$(get_password '4')

echo "[4] UserName : '$userName', Password : '$password'"
```

extract_credentials_sample_script.py

Extract credentials from your Oracle Site Guard scripts.

```
#!/usr/bin/python

# -*- coding: utf-8 -*-

import sys
```

```
class SiteGuardCredentialUtil(object):
    userNames = passwords = ''
    noOfUsers = noOfPasswords = 0
    credentialNotSet = False

    def __init__(self):
        credentialsIO = sys.stdin.readlines()[0]

        if credentialsIO :
            credentials = credentialsIO.split('<<SiteGuard_Credentials>>')
            self.userNames = credentials[0].split('<<SiteGuard_User>>')
            self.passwords = credentials[1].split('<<SiteGuard_Password>>')
            self.noOfUsers = len(self.userNames)
            self.noOfPasswords = len(self.passwords)
            self.credentialNotSet = True

            if self.noOfUsers != self.noOfPasswords :
                print("INFO: Total no. of users : '%s'"%self.noOfUsers)
                print("INFO: Total no. of passwords : '%s'"%self.noOfPasswords)
                print('ERROR: Number of User Names and number of Passwords do
not match')
                sys.exit(1)
            else :
                print("INFO: Total of '%s' credentials found"%self.noOfUsers)

    def getCredential(self, credential):
        if self.credentialNotSet :
            if self.noOfUsers < int(credential) :
                print("ERROR: Credential not found at index '%s'"%credential)
                sys.exit(1)
            else :
                credentialIndex = credential - 1;
                return self.userNames[credentialIndex],
self.passwords[credentialIndex]
        else :
            print('WARNING: SiteGuard Credentials not set')

            return '', ''

def main():
    sgUtil = SiteGuardCredentialUtil()
    myUser, my_Password = sgUtil.getCredential(1)
    print("[1] UserName : '"+ myUser + "', Password : '" + my_Password + "'")

    myUser, my_Password = sgUtil.getCredential(2)
    print("[2] UserName : '"+ myUser + "', Password : '" + my_Password + "'")

    myUser, my_Password = sgUtil.getCredential(3)
    print("[3] UserName : '"+ myUser + "', Password : '" + my_Password + "'")

    myUser, my_Password = sgUtil.getCredential(4)
    print("[4] UserName : '"+ myUser + "', Password : '" + my_Password + "'")


"""
    Starting point...
"""
main()
```

extract_credentials_sample_script.pl

Extract credentials from your Oracle Site Guard scripts.

```
#!/usr/local/bin/perl

use strict;
use warnings;

our @ALL_USERS     = undef;
our @ALL_PASSWORDS = undef;

our $NO_OF_USERS     = 0;
our $NO_OF_PASSWORDS = 0;

my $CREDENTIALS = <STDIN>;

load_credentials($CREDENTIALS);

my $userId1   = get_user_name(1);
my $password1 = get_password(1);

print_msg("[1] UserName : '$userId1', Password : '$password1'");

my $userId2   = get_user_name(2);
my $password2 = get_password(2);

print_msg("[2] UserName : '$userId2', Password : '$password2'");

my $userId3   = get_user_name(3);
my $password3 = get_password(3);

print_msg("[3] UserName : '$userId3', Password : '$password3'");

my $userId4   = get_user_name(4);
my $password4 = get_password(4);

print_msg("[4] UserName : '$userId4', Password : '$password4'");

sub load_credentials {
    my ($credentials) = @_;
    chomp($credentials);
    if ( length($credentials) <= 0 ) {
        print_msg("WARNING: Credentials not found");
        return '';
    }
    else {
        my @userIds   = split( /<<SiteGuard_Credentials>>/, $credentials );
        my @passwords = split( /<<SiteGuard_Credentials>>/, $credentials );

        @ALL_USERS     = split( /<<SiteGuard_User>>/,     $userIds[0] );
        @ALL_PASSWORDS = split( /<<SiteGuard_Password>>/, $passwords[1] );

        $NO_OF_USERS     = $#ALL_PASSWORDS + 1;
        $NO_OF_PASSWORDS = $#ALL_PASSWORDS + 1;

        if ( "$NO_OF_USERS" != "$NO_OF_PASSWORDS" ) {
            print_msg("INFO: Total no. of users : '$NO_OF_USERS'");
            print_msg("INFO: Total no. of passwords : '$NO_OF_PASSWORDS'");
```

```
            print_msg("ERROR: Number of User Names and number of Passwords do
not match.");
            exit 1;
        }
        else {
            print_msg("Total of '$NO_OF_USERS' credentials found.");
        }
    }
}

sub get_user_name {
    my ($index) = @_;

    my $userName = "";

    if ( "$NO_OF_USERS" > $index - 1 ) {
        $userName = $ALL_USERS[ $index - 1 ];
    }
    else {
        print_msg("ERROR: Credential at index '$index' not found.");
        exit 1;
    }

    return $userName;
}

sub get_password {
    my ($index) = @_;

    my $password = "";

    if ( "$NO_OF_PASSWORDS" > $index - 1 ) {
        $password = $ALL_PASSWORDS[ $index - 1 ];
    }
    else {
        print_msg("ERROR: Credential at index '$index' not found.");
        exit 1;
    }
    return $password;
}

sub print_msg {
    my ($msg) = @_;
    print("$msg \n");
}
```

B
Bundled Scripts

Learn about scripts that illustrate database control, ZFS storage, and ZFS analysis.

This appendix includes the following sections:

Bundled Scripts

Scripts bundled with Oracle Site Guard.

The following scripts are bundled with Oracle Site Guard:

- Oracle Virtual Machine (OVM) DR Script — siteguard_ovm_control.py
- **WebLogic Server Control Script – wls_control_wrapper.pl**
- **Node Manager Control Script – nm_control_wrapper.pl**
- Database Control Script - db_control_wrapper.pl
- ZFS Storage Script - zfs_storage_role_reversal.sh
- ZFS Analysis Script - zfs_analysis.sh

Oracle Virtual Machine (OVM) DR Script — siteguard_ovm_control.py

A script to perform disaster recovery operations for OVM (Oracle Virtual Machine) deployments.

Site Guard provides the `siteguard_ovm_control.py` bundled script for performing disaster recovery operations for OVM deployments that use OVM version 3.3.x or 3.4.x. For deployments that have Oracle Fusion Middleware and Oracle Fusion Applications that are deployed inside OVM guests, Site Guard can facilitate the disaster recovery of the virtual machine guests in addition to the disaster recovery performed for middleware and applications. This means that the VM guests running middleware and applications are also relocated from the primary to the standby site.

> **Note:**
>
> Oracle strongly recommends against using OVM DR for Oracle Database disaster recovery. Oracle Database disaster recovery should use Active Data Guard for protecting databases.

Configuring siteguard_ovm_control.py

The `siteguard_ovm_control.py` script is a multipurpose script that is used during all stages of the disaster recovery operation for a Oracle Virtual Machine deployment.

The options and parameters provided to the script change depending on the specific stage of the DR operation.

Depending on the stage of the OVM DR operation, the `siteguard_ovm_control.py` script is configured either as Site Guard Custom Precheck Script, Pre Script, or a Post Script with the appropriate options as shows in the examples below in the Usage section.

Custom Precheck Script

When configured as a Custom Precheck Script with the *start_precheck* or *stop_precheck* options, the script performs Prechecks to ensure that OVM guests can be started or stopped as part of the DR operation.

Pre Script

When configured as a Pre Script with the *start_prepare* or *start* options, the script prepares OVM repositories and starts OVM guests at the standby site.

Post Script

When configured as a Post Script with the *stop* or stop_*cleanup options*, the script stops OVM guests and cleans up OVM repositories at the primary site.

Sequence of Operations

In a typical switchover operation, the following is the sequence of configured scripts that are executed as part of the operation.

1. Precheck Phase
   - Custom Precheck Primary Site (*stop_precheck* option)
   - Custom Precheck Standby Site (*start_precheck* option)
1. Post Script Phase at Primary Site
   - Post Script Primary Site (*stop* option
   - Post Script Primary Site (*start_cleanup* option)
1. Pre Script Phase at Standby Site
   - Pre Script Standby Site (*start_prepare* option)
   - Pre Script Standby Site (*start* option)

Usage

```
python siteguard_ovm_control.py
  --action <action>
  --uri <uri>
  --pool <pool_name>
  --vm <vm_list>
  --repo <repo_list>
  --cert <cert_path>
  --signed <signed_cert_path>
  [--force]
  [--nocert]
```

This is the top-level entry point for Site Guard OVM disaster recovery operations. This script can be invoked through a Site Guard operation plan, or can be run as a stand-alone mode script.

This script will perform the specified action on the specified list of VMs or repositories. For example:

- Specifying a "stop_precheck" action for a list of guest VMs will perform a Site Guard Precheck to ensure that all the specified guest VMs exist and can be stopped at the primary site.

  > **Note:**
  >
  > This will NOT actually stop the specified guest VMs.

- Specifying a "stop" action for a list of guest VMs will shut down all the guest VMs. You will typically do this to stop the guest VMs at the primary site as part of a Switchover to another site.
- Specifying a "start_precheck" action for list of guest VMs will perform a Site Guard Precheck to ensure that all the guest VMs can be started at the standby site.

  > **Note:**
  >
  > This will NOT actually start the guest VMs

- Specifying a "start_prepare" action for a list of repositories will prepare the guest VMs for a "start" operation. You will typically do this before you start the standby site during a Switchover or Failover operation.
- Specifying a "start" action for a list of guest VMs will assign all the guest VMs to the specified server pool and start the VMs. You will typically do this to after a "start_prepare" to start the guest VMs at the standby site during a Switchover or Failover operation.

> **Note:**
>
> Specifying the `--force` option with a "start_prepare" (or "start") action will forcibly acquire ownership of repositories (or start the specified guest VMs). You will typically do this during a Failover operation to forcibly start guest VMs at the standby site, without regard to what happened at the Primary site. This may be necessary because primary site may be unreachable and the guest VMs may not have been cleanly shut down at the primary site.

Options

- `-h, --help`

  Show the help message and exit.

- `-a ACTION, --action=ACTION`

  The disaster recovery action to perform <start | stop | start_prepare | stop_cleanup | start_precheck | start_prepare_precheck | stop_precheck | stop_cleanup_precheck>.

  MANDATORY argument. Default Value: <not applicable>.

Example: `--action start_precheck`.

- `-f, --force`

  Forcibly perform the specified action. Ignore any inconsistencies and forcibly perform the specified action. Can be used to forcibly start guest VMs in the specified repositories at the standby site in the event of a fail over. It may be necessary to do this in cases where the primary site is unreachable and a graceful shutdown of guest VMs is not possible. This flag only applies to the 'start' action. It is ignored for other actions.

  OPTIONAL argument. Default value: OFF (--force will not be used).

  Example: `--force`

- `-u URI, --uri=URI`

  The OVM Manager URI including the port number.

  MANDATORY argument. Default Value: <not applicable>.

  Example: `-uri https://ovmm.mycompany.com:7002`

- `-r "Repository Name(s)", --repo="Repository Name(s)"`

  A list of one or more repositories on which the action is to be performed.
  When specifying multiple repositories, separate repository names with commas. Repositories will be processed in the order specified.

  MANDATORY argument. Default Value: <not applicable>.

  Example: `--repo "SiteA Repo Prod CRM (NAS), SiteA Repo Prod ERP (SAN), SiteA Repo Prod IDM DB (NAS)"`

- `-v "Ordered list of VMs", --vm="Ordered list of VMs`

  An ordered list of VMs (and their containing repositories) on which the action must be performed. The pecified VMs will be processed in the order given. VMs and their repositories should be separated using the ":" character. When specifying multiple VM:repository pairs, separate the pairs with commas. To specify "All VMs in a repository", use the "*" character as a wild-card.

  MANDATORY argument. Default Value: <not applicable>.

  Example: `--vm "*:SiteA Repo Prod CRM DB (SAN), Mid-Tier VM1:SiteA Repo Prod CRM MT (NAS), Mid-Tier VM2:SiteA Repo Prod CRM MT (NAS), *:SiteA Repo Prod IDM DB (NAS)"`

- `-p "Pool Name", --pool="Pool Name`

  The server pool name on which the action is performed. This argument is mandatory when the 'start' action is specified. It is ignored otherwise.

  CONDITIONALLY MANDATORY argument. Default Value: <not applicable>.

  Example: `--pool "My Primary Pool"`

- `-c /path/to/unsigned_certificate, --cert=/path/to/unsigned_certificate`

  The path to your unsigned public SSL certificate (PEM).

  OPTIONAL argument. Default Value: <not applicable>

  Example: `--cert /opt/ovmdr/cert/my-unsigned-cert.pem`

- `-s /path/to/signed_certificate, --signed=/path/to/signed_certificate`

The path to store the signed OVM SSL certificate (PEM).

OPTIONAL argument. Default Value: <not applicable>

Example: `--signed /opt/ovmdr/cert/ovm-signed-cert.pem`

- `-n, --nocert`

  Do not user certificates. Suppress warnings.

  OPTIONAL argument Default value: OFF (`--nocert` will not be used).

  Example: `--signed /opt/ovmdr/cert/ovm-signed-cert.pem`

Usage Examples

Example 1

Perform a "stop_precheck" at the primary site to ensure that we can stop the guest VMs in the repositories "SiteA Repo Prod CRM (NAS)" and "SiteA Repo Prod ERP (SAN)". Use the unsigned certificate "/opt/ovmdr/cert/my-cert.pem" when communicating with the OVM server. Use the "/opt/ovmdr/cert/my-signed-cert.pe" file to save the signed certificate received from the OVM Manager.

```
siteguard_ovm_control.py
     --action stop_precheck
     --uri https://primovmm.mycompany.com:7002
     --vm "*:SiteA Repo Prod CRM (NAS), *:SiteA Repo Prod ERP (SAN)"
     --cert /opt/ovmdr/cert/my-cert.pem
     --signed /opt/ovmdr/cert/my-signed-cert.pem
```

Example 2

Perform a "start_prepare" at the standby site on the repositories "SiteA Repo Prod CRM (NAS)" and "SiteA Repo Prod ERP (SAN)". Assign all VMs to the server pool "Standby Server Pool Denver". Use the "--force" flag to indicate that this is part of a failover operation. Do not use signed or unsigned certificates and suppress any certificate-related warnings.

```
siteguard_ovm_control.py
     --action start_prepare --force
     --uri https://stbyovmm.mycompany.com:7002
     --repo "SiteA Repo Prod CRM (NAS), SiteA Repo Prod ERP (SAN)"
     --pool "Standby Server Pool Denver"
     --nocert
```

Example 3

Perform a sequenced (ordered) "start" at the standby site on the guest VMs "RAC DB VM1" and "RAC DB VM2" in the repository "SiteA Repo Prod CRM (NAS)" and all the guest VMs in the repository "SiteA Repo Prod ERP (SAN)". Use the "--force" flag to indicate that this is part of a failover operation. Do not use signed or unsigned certificates and suppress any certificate-related warnings.

```
siteguard_ovm_control.py
     --action start
     --force
     --uri https://stbyovmm.mycompany.com:7002
     --vm "RAC DB VM1:SiteA Repo Prod CRM (NAS), RAC DB VM2:SiteA Repo Prod CRM
(NAS), *:SiteA Repo Prod ERP (SAN)"
     --nocert
```

Example 4

Perform a sequenced (ordered) "stop" at the primary site on the guest VMs "Mid-Tier VM1" and "Mid-Tier VM2" in the repository "SiteA Repo Prod CRM (NAS)". Then, stop all remaining guest VMs in the repositories "SiteA Repo Prod CRM (NAS)" and "SiteA Repo Prod ERP (SAN)" (in any order). Do not use signed or unsigned certificates and suppress any certificate-related warnings.

```
siteguard_ovm_control.py
     --action stop
     --uri https://primovmm.mycompany.com:7002
     --vm "Mid-Tier VM1:SiteA Repo Prod CRM (NAS), Mid-Tier VM2:SiteA Repo Prod
CRM (NAS), *:SiteA Repo Prod CRM (NAS), *:SiteA Repo Prod ERP (SAN)"
     --nocert
```

Example 5

Perform a "stop_cleanup" at the primary site on the repositories "SiteA Repo Prod CRM (NAS)" and "SiteA Repo Prod ERP (SAN)". Do not use signed or unsigned certificates and suppress any certificate-related warnings.

```
siteguard_ovm_control.py
     --action stop_cleanup
     --uri https://primovmm.mycompany.com:7002
     --repo "SiteA Repo Prod CRM (NAS), SiteA Repo Prod ERP (SAN)"
     --nocert
```

Note:

The following installation pre-requsities must be satisfied before this script can execute on a host where it is configured to execute:

- You must install the python Requests module (version 2.5.1 or later). See http://docs.python-requests.org/en/master/.
- You must install Python 2.6.6 or later. Python 3 is not currently supported.

To ensure that you use the correct path to this python interpreter, specify the path to the correct python installation as part of the script configuration, such as:

```
/home/oracle/python2.6/bin/python siteguard_ovm_control.py
{options]
```

WebLogic Server Control Script – wls_control_wrapper.pl

A script that allows you to configure custom Oracle WebLogic Server operations in the Pre or Post stages of an operation plan.

In previous versions of Site Guard, Oracle WebLogic Server (WLS) operations were not directly available for configuration by users. WLS operations could not be be configured outside the operation plan bucket where WLS disaster recovery occurred. This WLS operation bucket was configured and pre-inserted by Site Guard at a fixed point in the operation plan.

The `wls_control_wrapper.pl` script solves this problem. The script is provided as a bundled (out-of-box) script and it gives you the ability to add and configure their own custom WLS operations anywhere in the Pre or Post stages of an operation plan.

Usage

```
perl wls_control_wrapper.pl
   --component '<component>'
   --usecase    '<usecase>'
   --wls_home '<wls_home>'
   --mw_home '<mw_home>'
   --oracle_home '<oracle_home>'
   --domain_name '<domain_name>'
   --domain_dir '<domain_directory>'
   --server_name '<server_name>'
   --server_type '<server_type>'
   --admin_host '<admin_host>'
   --admin_port '<admin_port>'
   --nm_host '<node_manager_host>'
   --timeout '<3600>'
```

Options

- `--component`

  The type of the component on which the operation needs to be executed. Supported components: ADMIN_SERVER, MANAGED_SERVER, and CAM_COMPONENT.

- `--usecase`

  The usecase to be executed. Supported usecases: ADMIN_SERVER_STATUS, ADMIN_SERVER_START, ADMIN_SERVER_STOP, MANAGED_SERVER_STATUS, MANAGED_SERVER_START, MANAGED_SERVER_STOP, CAM_COMPONENT_STATUS, CAM_COMPONENT_START, and CAM_COMPONENT_STOP

- `--wls_home`

  The WebLogic Server HOME directory.

- `--mw_home`

  The Oracle Fusion Middleware HOME directory.

- `--oracle_home`

  The WebLogic Server's ORACLE_HOME.

- `--domain_name`

  The domain name.

- `--domain_dir`

  The domain directory.

- `--server_name`

  The WebLogic Administration Server’s name.

- `--server_type`

  The type of the WebLogic Administration Server.

- `--admin_host`

The host of the WebLogic Administration Server.

- `--admin_port`

  The port of the WebLogic Administration Server.

- `--nm_host`

  The host of node manager.

- `--help`

  Print a brief help message and exits.

- `--usage`

  Prints the usage page and exits

- `--manual`

  Prints the manual page and exits.

> **Note:**
>
> When configuring this script as a Pre or Post script, the perl interpreter used to execute this script must be the perl binary that is bundled with the Oracle Enterprise Manager agent. To ensure that you use the correct path to this perl interpreter, use one of the following methods.
>
> - Use `$PERL_HOME/perl` as the path of the perl interpreter.
> - Locate the perl installed as part of the EM agent installation on the host where this script will execute, and specify the explicit path to the perl interpreter, such as `/home/oracle/emagent/ agent_13.2.0.0.0/ perl/bin/perl`.

Node Manager Control Script – nm_control_wrapper.pl

A script that allows you to configure custom Node Manager operations in the Pre or Post stages of an operation plan.

In previous versions of Site Guard, Node Manager (NM) operations were not directly available for configuration by users. NM operations could not be be configured outside the operation plan bucket where NM disaster recovery occurred. This NM operation bucket was configured and pre-inserted by Site Guard at a fixed point in the operation plan.

The `nm_control_wrapper.pl` script solves this problem. The script is provided as a bundled (out-of-box) script and it provides users with the ability to add and configure their own custom NM operation anywhere in the Pre or Post stages of an operation plan

Usage

```
perl nm_control_wrapper.pl
   --usecase '<usecase>'
   --wls_home '<wls_home>'
   --mw_home '<mw_home>'
   --oracle_home '<oracle_home>'
```

```
--domain_name '<domain_name>'
--domain_dir '<domain_directory>'
--nm_host '<node_manager_host>'
--timeout '<3600>'
```

Options

- `--usecase`

  The usecase to be executed. Supported usecases: NM_STATUS, NM_START, NM_STOP.

- `--wls_home`

  Weblogic server's HOME directory.

- `--mw_home`

  Middleware HOME directory

- `--oracle_home`

  Weblogic server's ORACLE_HOME.

- `--domain_name`

  Domain Name

- `--domain_dir`

  Domain directory

- `--nm_host`

  Host of node manager.

- `--help`

  Print a brief help message and exits

- `--usage`

  Prints the usage page and exits.

- `--manual`

  Prints the manual page and exits.

> **Note:**
>
> When configuring this script as a Pre or Post script, the perl interpreter used to execute this script must be the perl binary that is bundled with the Oracle Enterprise Manager agent. To ensure that you use the correct path to this perl interpreter, use one of the following methods.
>
> - Use `$PERL_HOME/perl` as the path of the perl interpreter.
> - Locate the perl installed as part of the EM agent installation on the host where this script will execute, and specify the explicit path to the perl interpreter, such as `/home/oracle/emagent/ agent_13.2.0.0.0/perl/bin/perl`.

Database Control Script - db_control_wrapper.pl

A ready-to-use script that allows you to add and configure custom database prechecks in the Pre or Post stages of an operation plan.

In previous versions of Site Guard, Oracle database operations were not directly available for configuration by users. You could not configure database operations outside the operation plan bucket where database disaster recovery occurred. This database operation bucket was configured and pre-inserted by Oracle Site Guard at a fixed point in the operation plan.

The `db_control_wrapper.pl` script solves this problem.

Description

Performs database start, stop, switchover, failover ,convert and revert operations, and additionally, it performs prechecks in these use cases.

Syntax

```
perl db_control_wrapper.pl
    --usecase <usecase>
    --oracle_home <oracle_home>
    --oracle_sid <oracle_sid>
    --is_rac_database  <true/false>
    --timeout <3600>
    --target_db <target_db>
    --target_optional_parameters <target_optional_parameters>
    --operation_optional_parameters <operation_optional_paramete
```

Parameter	Description
`--usecase`	One of the following: START, START_PRECHECK, STOP, STOP_PRECHECK, SWITCHOVER, SWITCHOVER_PRECHECK, FAILOVER, FAILOVER_PRECHECK, CONVERT_PHYSICAL_TO_SNAPSHOT_STANDBY, CONVERT_PHYSICAL_TO_SNAPSHOT_STANDBY_PRECHECK, REVERT_SNAPSHOT_TO_PHYSICAL_STANDBY, REVERT_SNAPSHOT_TO_PHYSICAL_STANDBY_PRECHECK
`--oracle_home`	The database `ORACLE_HOME`.
`--oracle_sid`	The database `ORACLE_SID`.
`--is_rac_database`	Set to `true` for RAC database; set to `false` for a non-RAC database.
`--timeout`	The time in seconds, for the database role reversal polling timeout.
`--target_db`	The target database name.
`--target_optional_parameters`	Target runtime optional parameters. Options: `apply_lag`, `transport_lag` Format: `'apply_lag=-1&transport_lag=-1'`

Parameter	Description

`--operation_optional_parameters`	Target operation optional parameters.
	Options:
	`force=<true/false>`
	`enable_trace=<true/false>`
	`immediate_failover=<true/false>`
	`lag_check=<true/false>`
	Format:
	`'force=false&lag_check=false&enable_trace=false'`

`--help`	Prints a brief help message.
`--usage`	Prints a brief usage message.
`--manual`	Prints the manual page.

> **Note:**
>
> When configuring this script as a Pre or Post script, the perl interpreter used to execute this script must be the perl binary that is bundled with the Enterprise Manager agent. To ensure that you use the correct path to this perl interpreter, do one of the following:
>
> - Use `$PERL_HOME/perl` as the path of the perl interpreter.
> - Locate the perl installed as part of the EM agent installation on the host where this script will execute, and specify the explicit path to the perl interpreter (e.g. `/home/oracle/emagent/ agent_13.2.0.0.0/perl/bin/perl`).

ZFS Storage Script - zfs_storage_role_reversal.sh

A ready-to-use script to perform ZFS storage-related prechecks in the Global Pre, Global Post, Pre, or Post stages of an operation plan.

In previous versions of Site Guard, ZFS storage role reversal operations were not directly available for configuration by users at any point in the operation plan. Although ZFS storage-related operations could be configured by users, you could not configure where these operations got inserted in the operation plan. This storage role reversal operation bucket was always pre-inserted by Site Guard at a fixed point in the operation plan.

The `zfs_storage_role_reversal.sh` script (previously available only as a storage script) solves this problem.

For more information about the use of this script, see zfs_storage_role_reversal.sh.

ZFS Analysis Script - zfs_analysis.sh

A ready-to-use script that analyzes and reports the lag in a ZFS replication configuration.

The script analyzes and prints all the occurrences when the replication lag exceeded the specified threshold (recovery point objective), and the amount of maximum lag during each of these occurrences. The script performs this analysis over the interval specified by the `start_time` and `end_time` parameters.

Oracle recommends that you use this script as a stand-alone tool for data collection and reporting in order to monitor the health of a ZFS replication configuration. You can also run this script as a Custom Precheck (and Health check) script in a traditional Site Guard operation plan, but you cannot depend on this script to trigger an operation plan failure, as you could with a traditional precheck script.

Script Usage

```
zfs_analysis.sh
  [--zfs_appliance <ZFS Appliance>]
  [--zfs_appliance_user <ZFS Appliance Username>]
  [--zfs_appliance_password <ZFS Appliance Password>]
  [--zfs_project_name <ZFS Project Name>]
  [--start_time <Start Time>]
  [--end_time <End Time>]
  [--objective <Replica Objective>]
  [--cluster_member_file <Cluster Member File>]
  [--objective_file <Objective File>]
  [--force <Force analytic start time>]

where,
  --zfs_appliance : [mandatory] ZFS zppliance host
  --zfs_appliance_user : [mandatory] ZFS zppliance username
  --zfs_appliance_password : [mandatory] ZFS zppliance password
  --zfs_project_name : [mandatory] Project name
  --start_time : [mandatory] Start date/time
  --end_time : [mandatory] End date/time
  --objective : [mandatory] Replica lag threshold
  --cluster_member_file : File that declares a common name to use for the two
nodes in each clustered storage appliance
  --objective_file : File that declares replica lag thresholds for specific
replication actions
  --force : Force the analysis interval to start at the specified date/time
```

To configure the script as an Oracle Site Guard Custom Precheck script:

1. Search for and select the entity "ZFS Lag Analysis Scripts" for the **Software Library Entity** field.
2. Set the **Script Path** as illustrated in the following example:

   ```
   sh zfs_analysis.sh
     --zfs_appliance zfsappl01.mycompany.com
     --zfs_project_name rproject01
     --end_time 2015-07-07
     --objective 30m
     --start_time 2015-07-08
   ```

3. Select the host(s) on which to run the script.

4. Under **Advanced Options**, select and configure the credential for the ZFS appliance to pass as a parameter to the script.

A sample script output follows:

```
Action: zfsappl01sn01&zfsappl02sn02:rproject01
Replication of rproject01 from zfsappl01sn01
to zfsappl02sn02(label=zfsappl02sn-fe)
during the 10172506 second analysis interval
beginning 2015-02-12 06:18:14 UTC and ending 2015-06-10 00:00:00 UTC.
Updates are manually initiated.
Recovery Point Objective is 1800 seconds (30 minutes).
Action UUID (unique identifier) = e1b57778-5e5a-4053-c96b-f5d6e15d3292
                                        |                            |  seconds
          replication update            | at completion, replica lag |   spent
_______________________________________|____________________________|   above
       started      |     completed     | had grown to | then became | objective
____________________|___________________|______________|_____________|___________
2015-02-12 06:18:14 2015-02-12 06:18:24          10             10            0
2015-02-12 06:50:21 2015-02-12 06:50:30        1936              9          136
2015-02-12 06:51:45 2015-02-12 06:51:53          92              8            0
2015-02-15 21:10:59 2015-02-15 21:11:19      310774             20       308974
2015-02-15 21:19:32 2015-02-15 21:19:52         533             20            0
2015-02-16 06:17:34 2015-02-16 06:17:43       32291              9        30491
2015-02-16 06:21:36 2015-02-16 06:21:44         250              8            0
2015-02-16 06:25:12 2015-02-16 06:25:23         227             11            0
2015-02-16 06:27:18 2015-02-16 06:27:30         138             12            0
2015-02-16 06:29:23 2015-02-16 06:29:35         137             12            0
2015-02-16 06:32:07 2015-02-16 06:32:19         176             12            0
2015-02-16 06:33:27 2015-02-16 06:33:39          92             12            0
2015-02-16 06:36:07 2015-02-16 06:36:22         175             15            0
2015-02-16 06:40:17 2015-02-16 06:40:35         268             18            0
2015-02-16 07:03:11 2015-02-16 07:03:33        1396             22            0
2015-02-16 07:26:19 2015-02-16 07:26:29        1398             10            0
2015-02-16 07:28:03 2015-02-16 07:28:15         116             12            0
2015-02-17 00:50:24 2015-02-17 00:50:36       62553             12        60753
2015-02-17 00:55:57 2015-02-17 00:56:09         345             12            0
2015-02-17 01:55:01 2015-02-17 01:55:13        3556             12         1756
2015-02-17 04:25:21 2015-02-17 04:25:32        9031             11         7231
2015-02-18 10:22:19 2015-02-18 10:22:31      107830             12       106030
2015-02-18 10:23:31 2015-02-18 10:23:43          84             12            0
2015-02-23 05:02:22 2015-02-23 05:02:34      412743             12       410943
2015-02-23 07:06:26 2015-02-23 07:06:38        7456             12         5656
at end of interval  2015-06-10 00:00:00     9219214                    9217414


Replication actions that did not satisfy their Recovery Point Objective
at some point during the 10172506 second analysis interval
beginning 2015-02-12 06:18:14 UTC and ending 2015-06-10 00:00:00 UTC.

 replication updates |   total   |     |     peak replica lag        |
_____________________|  seconds  |     |_____________________________|
       |    above    |   above   |     |          |                  |
 total |  objective  | objective | RPO | seconds |   date and time   |
source&target:project/share
______ |_____________|___________|_____|_________|___________________|
_____________________________
    59      48  81%   358352   4%  1800   340318  2015-06-08 17:47:55
zfsappl01sn01&zfsappl02sn02:1_WING
     3       2  67%  1493546  15%  1800   994866  2015-06-04 04:28:59
zfsappl01sn01&zfsappl02sn02:2_SG
     2       1  50%  1642394  16%  1800  1644194  2015-06-10 00:00:00
```

```
zfsappl01sn01&zfsappl02sn02:3_SG
     2       1  50%  1642180  16%  1800  1643980  2015-06-10 00:00:00
zfsappl01sn01&zfsappl02sn02:4_SG
     3       2  67%  1497621  15%  1800  1203470  2015-06-10 00:00:00
zfsappl01sn01&zfsappl02sn02:5_SG
     2       1  50%  6757712  66%  1800  6759512  2015-06-10 00:00:00
zfsappl01sn01&zfsappl02sn02:SiteGuard
    13       4  31%  9593787  94%  1800  9219201  2015-06-10 00:00:00
zfsappl01sn01&zfsappl02sn02:br_test
    26      10  38% 10149384 100%  1800  9219214  2015-06-10 00:00:00
zfsappl01sn01&zfsappl02sn02:rproject01
```

C

Oracle Site Guard Terminology

Learn Oracle Site Guard terminology.

The following terms are used throughout this document:

- **Target**

  Targets are core Enterprise Manager entities that represent the infrastructure and business components in an enterprise. These components need to be monitored and managed for efficient functioning of the business. An example of a target is an Oracle Fusion Middleware farm or an Oracle Database Instance. Oracle Site Guard disaster-recovery operations are designed to protect one or more targets at a site.

- **Site**

  A logical grouping of related entities in a data center. For example, software components in a Web tier, the Middleware tier, and Database tier, along with associated storage may all together comprise a Site. Oracle Site Guard performs disaster-recovery operations on a Site. A datacenter may have more than one Site defined by Oracle Site Guard and each of them can be managed independently for disaster-recovery operations.

- **Primary Site**

  The site currently hosting the active application (a set of targets) that Oracle Site Guard is configured to protect. The Primary Site is also referred to as the Production Site.

- **Standby Site**

  The site that is intended to host the protected application (a set of targets) in the event of a disaster-recovery operation.

- **Role**

  The current designation of a site. The role can be either Primary or Standby.

- **Switchover**

  The process of reversing the roles of the production site and standby site is termed as a *switchover*. Switchovers are planned operations done for periodic validation or to perform planned maintenance on the current production site. During a switchover, the current standby site becomes the new production site, and the current production site becomes the new standby site.

- **Failover**

  The process of making the current standby site the new production site after the production site becomes unexpectedly unavailable (for example, due to a disaster at the production site), is termed as a *failover*.

- **Open For Validation**

  The process of converting (opening) the current standby site into a fully functional site in order to test and validate operations at the standby site. When a site is opened for validation, it is not available as a standby site.

- **Revert to Standby**

  The process of reverting (closing) a site that has been opened for validation back to a standby site so that it is available as a standby site in disaster recovery operations.

- **Operation Plan**

  An operation plan contains the flow of execution for a particular Oracle Site Guard operation. It defines the order in which the steps of a disaster-recovery operation should be executed, in addition to other attributes, such as serial, parallel, and so on.

- **Prechecks**

  Prechecks are a pre-ordered set of checks that determine whether an operation plan is compliant with the environment it is supposed to protect. Prechecks are used to assess disaster-recovery readiness, and are performed on demand.

- **Health Checks**

  A pre-ordered set of checks, health checks can be programmed to run periodically based on a user-defined schedule. Health checks are used to maintain an ongoing assessment of disaster-recovery readiness.

- **Custom Precheck Scripts**

  Custom Precheck scripts are user-defined scripts that are executed as part of the Precheck procedure for an Oracle Site Guard operation plan. The number of Precheck Scripts and the sequence of their execution can be defined as part of an operation plan.

- **Pre Scripts**

  Pre scripts are site-specific, user-defined scripts that are executed at a site at the beginning of an Oracle Site Guard operation. The number of Pre Scripts and the sequence of their execution can be defined as part of an operation plan.

- **Post Scripts**

  Post scripts are site-specific, user-defined scripts that are executed at a site at the end of an Oracle Site Guard operation. The number of Post Scripts and the sequence of their execution can be defined as part of an operation plan.

- **Global Pre Scripts**

  Global Pre Scripts are operation-specific, user-defined scripts that are executed at the beginning of an Oracle Site Guard operation plan. The number of Global Pre Scripts and the sequence of their execution can be defined as part of an operation plan.

- **Global Post Scripts**

  Global Post Scripts are operation-specific, user-defined scripts that are executed at the end of an Oracle Site Guard operation plan. The number of Global Post Scripts and the sequence of their execution can be defined as part of an operation plan.

- **Execution Groups**

  Operation plan "Execution Groups" extend Site Guard's functionality for buckets (operation plan groups) whose Execution Mode setting is "parallel". Operation plan steps in the same execution group execute in parallel, but finish execution before any operation steps in a subsequently numbered execution group begin execution.

- **Tags**

  A tag is a user-defined alphanumeric string that can be associated with an operation plan. Tags can be used to search for operation plans that match one or more specified tags.

- **Super Administrator**

  A super administrator is a privileged user who has access to all Enterprise Manager targets, and to all Oracle Site Guard configurations, operations, and activities.