

# **Oracle® Site Guard**

Administrator's Guide

Release 12.1.0.7

**E52894-04**

February 2015

Oracle Site Guard Administrator's Guide, Release 12.1.0.7

E52894-04

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

Primary Author: Rekha M. Kamath

Contributor: Praveen Sampath, Shekhar Borde, Shane Vermette, Leo Cloutier, Mahesh Desai, Rama Vijapurapu, Satheesh Amilineni, Allwarappan Sundarraj, Puligundla Sasidhar, Srinagesh Battula

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

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

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

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

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

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

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

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

---

# Contents

<b>Preface</b> .....	ix
Audience .....	ix
Documentation Accessibility .....	ix
Related Documents .....	ix
Conventions .....	x
 <b>1 Introduction to Oracle Site Guard</b>	
1.1 What is Oracle Site Guard .....	1-1
1.2 Benefits of Oracle Site Guard .....	1-1
1.3 What is New in This Release .....	1-2
 <b>2 Understanding Oracle Site Guard Concepts</b>	
2.1 Oracle Site Guard Terminology .....	2-1
2.2 Representation of a Site in Enterprise Manager Cloud Control Console .....	2-3
2.3 Oracle Site Guard Features .....	2-4
2.3.1 Extensibility .....	2-4
2.3.1.1 Types of Scripts for Extensibility .....	2-5
2.3.1.2 Sequence of Script Execution .....	2-7
2.3.1.3 Configuring Script Path .....	2-9
2.3.2 Prechecks and Health Checks .....	2-10
2.3.2.1 Prechecks .....	2-10
2.3.2.2 Health Checks .....	2-11
2.3.2.3 Customizing Prechecks and Health Checks .....	2-12
2.3.2.4 Lag Checks .....	2-12
2.3.3 Storage Integration .....	2-12
2.3.3.1 Oracle Sun ZFS .....	2-13
2.3.3.2 Integrating Other Storage Types .....	2-13
2.3.3.3 Mount and Unmount Scripts .....	2-13
2.3.4 Monitoring Executions and Managing Errors .....	2-13
2.3.4.1 Customizing Operations .....	2-13
2.3.4.2 Monitoring Executions .....	2-14
2.3.4.3 Operation Error Modes .....	2-14
2.3.4.4 Retrying Failed Operations .....	2-14
2.3.4.5 Suspending and Resuming Operations .....	2-14
2.3.5 Credential Management .....	2-15

2.3.5.1	Enterprise Manager Credential Framework.....	2-15
2.3.5.2	Oracle Site Guard Credential Configuration.....	2-15
2.3.6	Role-Based Access Control .....	2-15
2.3.7	.....Software Library Integration	2-15
2.3.8	.....Custom Credentials for Script Execution	2-16
2.3.9	.....Passing Credentials as Script Parameters	2-16
2.4	Oracle Site Guard Workflows .....	2-16
2.4.1	Switchover Workflow .....	2-17
2.4.2	Failover Workflow .....	2-18
2.4.3	Start Workflow .....	2-19
2.4.4	Stop Workflow .....	2-20

### 3 Installing Oracle Site Guard

3.1	Installing Oracle Site Guard .....	3-1
3.2	Prerequisites for Using Oracle Site Guard .....	3-1
3.2.1	Discovering Targets on the Primary Site and the Standby Site .....	3-2
3.2.2	Creating Oracle Site Guard Administrator Users.....	3-2
3.2.2.1	Creating a Oracle Site Guard Administrator User Using Enterprise Manager Cloud Control Console	3-3
3.2.2.2	Creating a Oracle Site Guard Administrator User Using Enterprise Manager Command-Line Interface	3-4
3.2.3	Creating Primary and Standby Sites.....	3-4
3.2.3.1	Creating a Generic System Using Enterprise Manager Cloud Control Console.	3-4
3.2.3.2	Creating a Generic System Using EMCLI Commands .....	3-5
3.2.4	Creating Credentials.....	3-6
3.2.4.1	Creating Named Credentials .....	3-6
3.2.4.2	Creating Preferred Credential .....	3-9
3.2.5	Granting Credential Privileges to Oracle Site Guard Administrator Users.....	3-10
3.2.5.1	Granting Credential Privileges Using Enterprise Manager Cloud Control Console .	3-10
3.2.6	Configuring Software Library Storage Location.....	3-11
3.2.6.1	Configuring Software Library Storage Location Using Enterprise Manager Cloud Control Console	3-11
3.2.6.2	Configuring Software Library Storage Location Using Enterprise Manager Command-Line Interface	3-12
3.2.7	Verifying Database and Data Guard Configurations.....	3-12

### 4 Configuring Oracle Site Guard

4.1	Overview .....	4-1
4.2	Configuring Sites.....	4-2
4.2.1	Configuring Sites Using Enterprise Manager Cloud Control Console.....	4-2
4.2.2	Configuring Sites Using EMCLI Commands .....	4-3
4.3	Creating Credential Associations .....	4-3
4.3.1	Creating Named or Preferred Credential Associations .....	4-4
4.3.1.1	Creating Named or Preferred Credential Associations Using Enterprise Manager Cloud Control Console	4-4
4.3.1.2	Creating Named or Preferred Credential Associations Using EMCLI Commands ..	4-6

4.4	Configuring Scripts.....	4-7
4.4.1	Configuring Custom Precheck Scripts, Pre Scripts, Post Scripts, Global Pre Scripts, and Global Post Scripts	4-8
4.4.1.1	Configuring Custom Precheck Scripts, Pre Scripts, Post Scripts, Global Pre Scripts, and Global Post Scripts Using Enterprise Manager Cloud Control Console	4-9
4.4.1.2	Configuring Custom Precheck Scripts, Pre Scripts, Post Scripts, Global Pre Scripts, and Global Post Scripts Using EMCLI Commands	4-10
4.4.2	Configuring Mount and Unmount Scripts.....	4-12
4.4.2.1	mount_umount.sh .....	4-13
4.4.2.1.1	Configuring Mount or Unmount Scripts Using Enterprise Manager Cloud Control Console	4-13
4.4.2.1.2	Configuring Mount or Unmount Scripts Using EMCLI Commands .....	4-15
4.4.3	Configuring Storage Scripts .....	4-17
4.4.3.1	zfs_storage_role_reversal.sh .....	4-17
4.4.3.2	Configuring Storage Scripts Using Enterprise Manager Cloud Control Console .....	4-19
4.4.3.3	Configuring Storage Scripts Using Enterprise Manager Command-Line Interface...	4-21
4.4.4	Configuring Credentials as Parameters for Scripts .....	4-23
4.4.4.1	Adding Credential Parameters to a Script.....	4-23
4.4.4.2	Deleting Credential Parameters from a Script .....	4-23
4.4.4.3	Getting Credential Parameters for a Script.....	4-24
4.4.5	Cloning a Script Using Existing Scripts.....	4-24
4.5	Configuring Auxiliary Hosts.....	4-25
4.5.1	Adding an Auxiliary Host Using EMCLI Commands.....	4-25
4.5.2	Deleting an Auxiliary Host Using EMCLI Commands.....	4-25
4.5.3	Listing Auxiliary Targets Using EMCLI Commands .....	4-25
4.6	Configuring Database Lag Checks .....	4-26
4.6.1	Configuring Database Lag Checks Using EMCLI Commands .....	4-26
4.6.2	Updating Threshold Value for Database Lag Using EMCLI Commands.....	4-26
4.6.3	Deleting Threshold Value for Database Lag Using EMCLI Commands.....	4-27
4.6.4	Listing Database Lag Thresholds Using EMCLI Commands .....	4-27

## 5 Troubleshooting Oracle Site Guard

5.1	Operation Plan Failure .....	5-1
5.1.1	Targets Not Discovered in Operation Plan Workflow .....	5-2
5.1.2	Oracle WebLogic Server Managed-Server Target Not Identified .....	5-2
5.1.3	Manual Intervention Needed for Hung Operation Step.....	5-2
5.1.4	OPMN Managed System Components Not Discovered In Operation-Plan Workflow....	5-2
5.1.5	Oracle RAC Database Not Discovered in Operation-Plan Workflow .....	5-3
5.1.6	Failure of Operation Step When Accessed with Sudo Privileges.....	5-3
5.1.7	.....Error While Creating Operation Plan Indicating Credential Association Not Configured	5-3
5.1.8	Inability to Associate Credentials for Targets Added to a Site .....	5-4
5.1.9	Error While Deleting Or Updating Operation Plans .....	5-4
5.1.10	Error Indicating Inability to Create Scalar Value While Creating Operation Plan ....	5-4

5.1.11	Error While Creating Operation Plan Indicating Missing Node Manager Credentials....	5-5
5.2	Switchover or Failover Operations Failure .....	5-5
5.2.1	WebLogic Administration Server Does Not Start After Performing Switchover or Failover Operation	5-5
5.2.2	WebLogic Administration Server Fails to Restart After Performing Switchover or Failover Operations	5-6
5.2.3	Host Not Available During Switchover or Failover Operations .....	5-6
5.2.4	Switchover or Failover Operations Fail When Oracle RAC Database Instances Are Not Available	5-6
5.3	Precheck Failure .....	5-6
5.3.1	Failure of Prechecks.....	5-7
5.3.2	Prechecks Hang When Oracle Management Agent Is Not Available.....	5-7
5.4	Oracle WebLogic Server Failure .....	5-7
5.4.1	Node Manager Fails to Restart .....	5-7
5.4.2	Managed Server Fails to Start .....	5-8
5.4.3	Oracle Site Guard Does Not Include Oracle WebLogic Server Instances That Are Migrated to a Different Host	5-8
5.4.4	Error Displayed While Creating Operation Plan .....	5-8
5.4.5	.....WebLogic Administration Server Able to Communicate With Node Manager When Site Guard Cannot	5-9
5.4.6	Unable to Associate More Than One Node Manager Per Host .....	5-9
5.5	Database Failure.....	5-9
5.5.1	Prechecks for Database Switchover and Database Failover Operations Fail.....	5-10
5.5.2	Databases Protected by Data Guard Included in the Incorrect Operation-Plan Category	5-10
5.6	Storage Failures .....	5-10
5.6.1	Attempt to Log In to ZFS Storage Appliance Might Fail During Execution of Operation Plan	5-11
5.6.2	Storage Role Reversal Operation Might Fail During Execution of Operation Plan While Deleting Empty Project on Target Appliance	5-11
5.6.3	Storage Role Reversal Operation Might Fail During Execution of Operation Plan While Executing 'confirm reverse'	5-11

## 6 Performing Oracle Site Guard Operations

6.1	Overview .....	6-1
6.2	Managing Operation Plans .....	6-2
6.2.1	Creating Operation Plans .....	6-3
6.2.1.1	Creating an Operation Plan Using Enterprise Manager Cloud Control Console.....	6-3
6.2.1.2	Creating an Operation Plan Using EMCLI Commands.....	6-4
6.2.2	Creating New Operation Plans Using Existing Plans .....	6-4
6.2.3	Editing and Updating Operation Plans.....	6-5
6.2.3.1	Editing and Updating Operation Plans Using Enterprise Manager Cloud Control Console	6-5
6.2.3.2	Editing and Updating Operation Plans Using EMCLI Command .....	6-6
6.2.4	Deleting an Operation Plan .....	6-7
6.2.4.1	Deleting an Operation Plan Using Enterprise Manager Cloud Control Console .....	6-7

6.2.4.2	Deleting an Operation Plan Using Command-Line Interface.....	6-8
6.3	Running Prechecks .....	6-8
6.3.1	Running Precheck Utility Using Enterprise Manager Cloud Control Console .....	6-8
6.3.2	Running Precheck Utility Using Command-Line Interface .....	6-9
6.4	Scheduling Health Checks.....	6-9
6.4.1	Scheduling a Health Check Using Enterprise Manager Cloud Control Console.....	6-9
6.4.2	Scheduling a Health Check Using EMCLI.....	6-10
6.5	Executing Oracle Site Guard Operation Plans.....	6-11
6.5.1	Executing Oracle Site Guard Operation Plan Using Enterprise Manager Cloud Control Console 6-12	
6.5.2	Executing Oracle Site Guard Operation Plan Using EMCLI Command .....	6-12
6.6	Monitoring Oracle Site Guard Operations .....	6-13
6.6.1	Monitoring an Operation Plan Using Enterprise Manager Cloud Control Console .....	6-13
6.6.1.1	Viewing an Operation Activity .....	6-13
6.6.1.2	Suspending, Resuming, or Stopping an Operation .....	6-14
6.6.2	Monitoring an Operation Plan Using EMCLI .....	6-14
6.7	Managing Execution Errors.....	6-15
6.8	Manually Reversing Site Roles.....	6-16
6.8.1	Manually Reversing Site Roles Using Enterprise Manager Cloud Control Console.....	6-17
6.8.2	Manually Reversing Site Roles Using EMCLI .....	6-17

## 7 Oracle Site Guard Command-Line Interface

7.1	add_siteguard_aux_hosts .....	7-2
7.2	add_siteguard_script_credential_params .....	7-3
7.3	add_siteguard_script_hosts.....	7-3
7.4	configure_siteguard_lag .....	7-4
7.5	create_operation_plan .....	7-5
7.6	create_siteguard_configuration .....	7-6
7.7	create_siteguard_credential_association .....	7-6
7.8	create_siteguard_script .....	7-8
7.9	delete_operation_plan.....	7-10
7.10	delete_siteguard_aux_host .....	7-11
7.11	delete_siteguard_configuration .....	7-11
7.12	delete_siteguard_credential_association .....	7-12
7.13	delete_siteguard_lag.....	7-13
7.14	delete_siteguard_script .....	7-13
7.15	delete_siteguard_script_credential_params .....	7-14
7.16	delete_siteguard_script_hosts .....	7-15
7.17	get_operation_plan_details .....	7-15
7.18	get_operation_plans .....	7-16
7.19	get_siteguard_aux_hosts.....	7-17
7.20	get_siteguard_configuration .....	7-17
7.21	get_siteguard_credential_association .....	7-18
7.22	get_siteguard_health_checks.....	7-19
7.23	get_siteguard_lag.....	7-19

7.24	get_siteguard_script_credential_params.....	7-20
7.25	get_siteguard_script_hosts .....	7-21
7.26	get_siteguard_scripts.....	7-21
7.27	get_siteguard_supported_targets.....	7-22
7.28	run_prechecks.....	7-23
7.29	schedule_siteguard_health_checks .....	7-23
7.30	stop_siteguard_health_checks .....	7-25
7.31	submit_operation_plan .....	7-26
7.32	update_operation_plan .....	7-26
7.33	update_siteguard_configuration .....	7-27
7.34	update_siteguard_credential_association .....	7-28
7.35	update_siteguard_lag.....	7-29
7.36	update_siteguard_script .....	7-30

## 8 Upgrading or Downgrading Oracle Site Guard

8.1	Upgrading Oracle Site Guard .....	8-1
8.2	Downgrading Oracle Site Guard .....	8-2

## A Extracting Credentials Passed as Parameters (Examples)

extract_credentials_sample_script.sh.....	A-2
extract_credentials_sample_script.py .....	A-4
extract_credentials_sample_script.pl .....	A-6



---

# 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 solution. As an administrator, you can be either 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 in the Oracle Other Product One Release 7.0 documentation set or in the Oracle Other Product Two Release 6.1 documentation set:

- *Oracle Fusion Middleware Disaster Recovery Guide*
- *Oracle Fusion Middleware High Availability Guide*
- *Oracle Data Guard Broker*
- *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*

## Conventions

The following text conventions are used in this document:

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

---

# Introduction to Oracle Site Guard

This chapter provides a brief introduction to Oracle Site Guard. It also describes the benefits of using Oracle Site Guard as a disaster-recovery solution.

It contains the following topics:

- [Section 1.1, "What is Oracle Site Guard"](#)
- [Section 1.2, "Benefits of Oracle Site Guard"](#)
- [Section 1.3, "What is New in This Release"](#)

## 1.1 What is Oracle Site Guard

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

## 1.2 Benefits of 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.

## **1.3 What is New in This Release**

The following new features are available in this release:

### **Customize Prechecks**

Enhance the Prechecks and Health Checks performed by Oracle Site Guard by adding your own Custom Precheck scripts. Use this feature to customize and improve the Prechecks and Health Checks that precede any operation plan.

### **Add User Scripts to Oracle Enterprise Manager's Software Library**

Add your own scripts to Oracle Enterprise Manager's software library and use them in Oracle Site Guard work flows. This leverages the ability of Oracle Site Guard to automatically deploy the scripts at runtime, thereby eliminating the need to manually pre-deploy your scripts on the hosts where they need to run.

### **Configure Custom Credentials for Script Execution**

Configure an alternate set of credentials for executing any configured script. This allows you to execute scripts using credentials that are different than the credentials configured for the script host.

### **Provide Credentials as Parameters to Scripts**

Provide one or more credentials as parameters for configured scripts. This allows you to securely pass credentials to any configured script when the script needs to perform additional authentication functions.

### **Stop the Primary Site during a Failover Operation**

Configure Oracle Site Guard to optionally stop the primary site during a failover operation. Oracle Site Guard attempts to stop the primary site components on best effort basis before failing over to the standby site.

### **Clone Operation Plans**

Using the **Create Like** feature, create a new operation plan by cloning existing plans. This saves time during configuration, especially when the new operation plan is very similar to an existing plan or script.

### **Clone Configured Scripts**

Using the **Create Like** feature, configure a new script by cloning an existing script configuration. This saves time during configuration, especially when the new script configuration is very similar to an existing script configuration.

**Support for Oracle Fusion Middleware 12c**

Protect your Oracle Fusion Middleware 12c deployment using Oracle Site Guard.

**Support for Oracle Database 12c**

Protect your Oracle Database 12c deployment using Oracle Site Guard.



---

## Understanding Oracle Site Guard Concepts

This chapter describes Oracle Site Guard terminology and the architecture of a site in an Enterprise Manager Cloud Control Console. It also provides an overview of the workflow of different operations that Oracle Site Guard performs.

It contains the following topics:

- [Section 2.1, "Oracle Site Guard Terminology"](#)
- [Section 2.2, "Representation of a Site in Enterprise Manager Cloud Control Console"](#)
- [Section 2.3, "Oracle Site Guard Features"](#)
- [Section 2.4, "Oracle Site Guard Workflows"](#)

### 2.1 Oracle Site Guard Terminology

The following terms are used in 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*.

- **Operation Plan**

An operation plan contains the flow of execution for a particular Oracle Site Guard operation. It defines the order in which the steps of an 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.

#### ■ Super Administrator

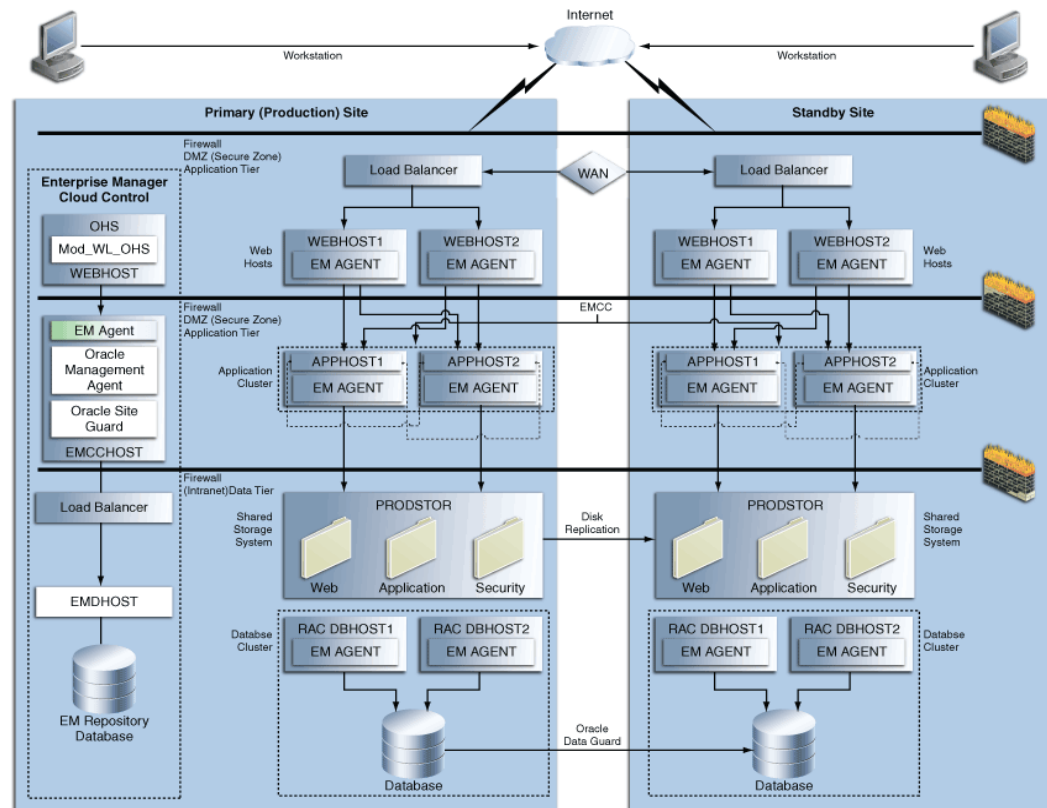
A super administrator is a privileged user who has access to all Enterprise Manager targets, and to all Oracle Site Guard configurations, operations, and activities.

## 2.2 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. For example, a site could consist 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.

Figure 2-1 shows an overview 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**



Following are the key aspects of the Oracle Fusion Middleware Disaster Recovery topology:

- A single Enterprise Manager Cloud Control instance 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.

## 2.3 Oracle Site Guard Features

This section describes the features of Oracle Site Guard.

It contains the following topics:

- [Extensibility](#)
- [Prechecks and Health Checks](#)
- [Storage Integration](#)
- [Monitoring Executions and Managing Errors](#)
- [Credential Management](#)
- [Role-Based Access Control](#)
- [Software Library Integration](#)
- [Custom Credentials for Script Execution](#)
- [Passing Credentials as Script Parameters](#)

### 2.3.1 Extensibility

Oracle Site Guard provides the ability to extend the built-in disaster-recovery functionality by allowing you to insert custom scripts at specific points in the operation workflow. This provides a mechanism for performing customized, site-specific, or 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](#)
- [Sequence of Script Execution](#)
- [Configuring Script Path](#)

### 2.3.1.1 Types of Scripts for Extensibility

For customizing and extending Oracle Site Guard functionality, the following types of scripts are available:

- [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 come bundled with Oracle Site Guard and users can also define their 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 come bundled with Oracle Site Guard. Users can also define their own storage scripts. These scripts 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.

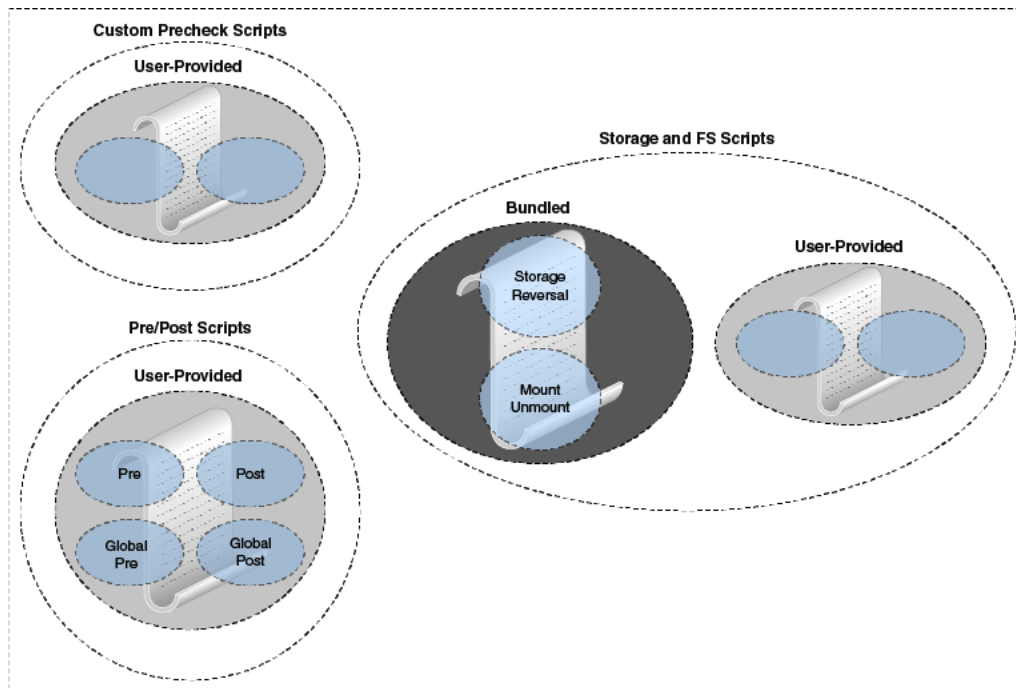
Table 2–1 provides an overview of the various types of scripts that are used while using Oracle Site Guard to set up sites.

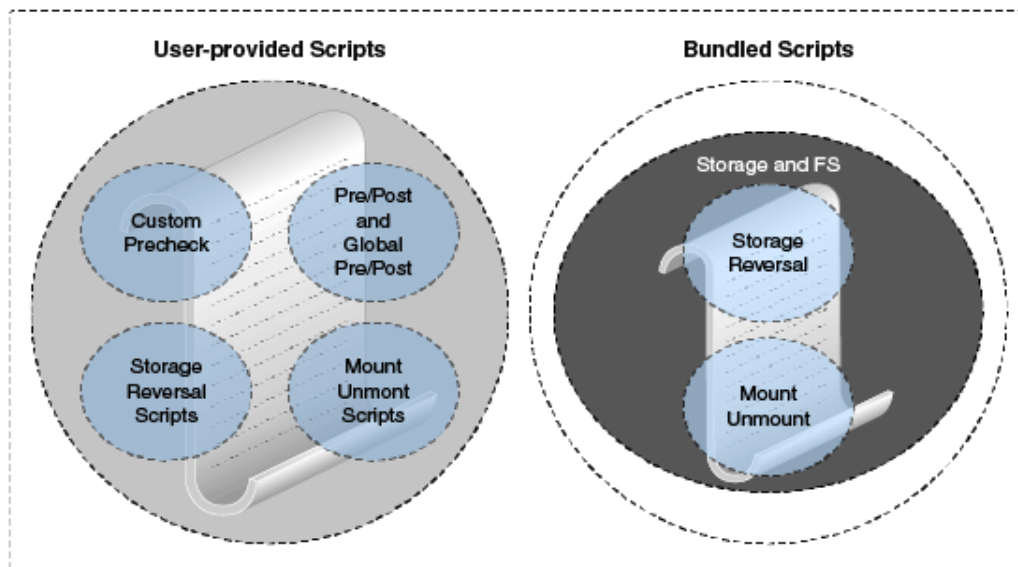
Figure 2–2 and Figure 2–3 provide a visual representation of the source of the scripts and their functions.

**Table 2–1 Types of Scripts Used by Oracle Site Guard**

Types of Script	Provided by the User? (Custom Scripts)	Provided by 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. To be configured by user.)

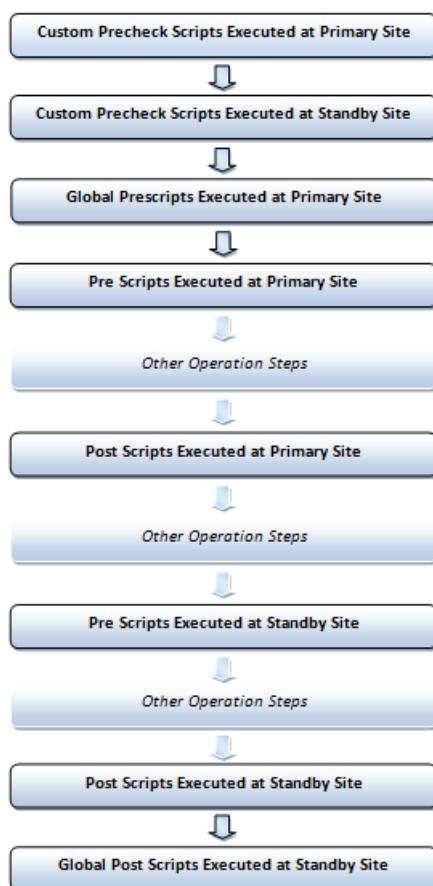
**Figure 2–2 Oracle Site Guard Scripts: What They Do**

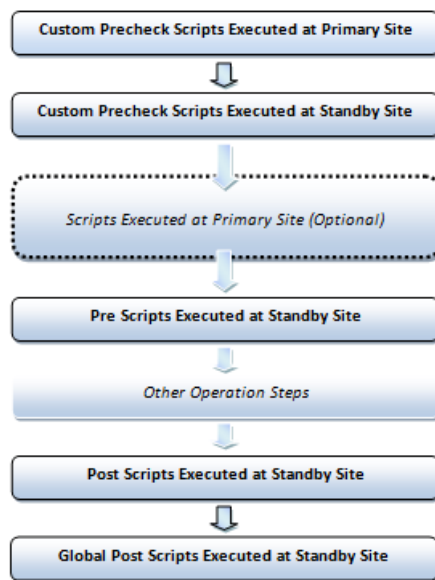


**Figure 2–3 Oracle Site Guard Scripts: Who Provides Them**

### 2.3.1.2 Sequence of Script Execution

Figure 2–4, Figure 2–5, and Figure 2–6 show the sequence in which Oracle Site Guard executes various types of user-defined scripts for different 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.

---

### 2.3.1.3 Configuring Script Path

Depending on the type of script and the desired runtime behavior, you must configure the path of the script using the appropriate format. Oracle Site Guard determines the location (path) of the script using the configuration path and type of script provided by the user. Table 2–2 shows examples of how to configure the 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. Script path formats, other than those listed in Table 2–2, are not supported.

**Table 2–2 Example: Configuring Script Path**

Script Location	Script Type	User Configured Path	Script Path Extracted by Oracle Site Guard
Enterprise Manager Software Library	Shell script	sh swlib_script.sh	swlib_script.sh
		sh ./swlib_script.sh	
		sh ./swlib_script.sh -	
		sh ./swlib_script.sh	
		-option1 -option2	
		/home/bash swlib_script.sh	
	Perl script	/home/bash swlib_script.sh	swlib_script.pl
		-a param1 -b param2	
		perl swlib_script.pl	
		perl swlib_script.pl -a	
		param1 -b param2	
		/home/perl swlib_script.pl	
	Python script	/home/perl swlib_script.pl	swlib_script.py
		-a param1 -b param2	
		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	

**Table 2–2 (Cont.) Example: Configuring Script Path**

Script Location	Script Type	User Configured Path	Script Path Extracted by Oracle Site Guard
User defined (Custom)	Shell script	sh /home/oracle/custom_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
		/home/oracle/custom_script.sh -a param1 -b param2	
	Perl script	/home/bash	
		/home/oracle/custom_script	
		/home/oracle/custom_script	
		perl /home/oracle/custom_script.pl	/home/oracle/custom_script.pl
		/home/perl	
		/home/oracle/custom_script.pl -a param1 -b param2	
	Python script	param2	
		/home/python	/home/oracle/custom_script.py
		/home/oracle/custom_script.py	
		/home/python	
		/home/oracle/custom_script.py -a param1 -b param2	
		param2	

## 2.3.2 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. It is also very important to ensure that the standby site is ready to perform the production role, before initiating any disaster recovery operation.

Oracle Site Guard provides a solution to this problem with the Precheck and Health Check features.

### 2.3.2.1 Prechecks

A Precheck provides a convenient and fully automated mechanism for assessing disaster-recovery readiness on demand. 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.



### 2.3.2.2 Health Checks

Health Checks are a special category of Prechecks. They are Prechecks that can be scheduled to run periodically. Thus, health checks provide a mechanism to perform 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 every operation plan.

---

### 2.3.2.3 Customizing Prechecks and Health Checks

The Precheck process can be customized by adding custom (user-defined) scripts that will execute as part of the Precheck, and also as part of any Health Checks that are then scheduled. This allows users to enhance the Precheck and Health Check capabilities of Oracle Site Guard by adding Prechecks for third-party components that need to be included in the disaster recovery workflow. Custom Precheck scripts function in the same way that built-in Prechecks function. If a user-defined Precheck script detects an anomaly and returns an error to Site Guard, that Precheck step is regarded as failed, and depending on how the Precheck 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.

### 2.3.2.4 Lag Checks

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.

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

This parameter specifies the permissible lag for application-tier storage replication which is managed by ZFS.

## 2.3.3 Storage Integration

Storage-management operations are an essential part of disaster-recovery operations. During disaster recovery, storage replication must be reversed and storage appliances must be reconfigured before applications can be migrated to a standby site. Oracle Site Guard offers storage integration options for various storage technologies.

The following topics describe the storage integration options that Oracle Site Guard provides:

- [Oracle Sun ZFS](#)
- [Integrating Other Storage Types](#)
- [Mount and Unmount Scripts](#)

### 2.3.3.1 Oracle Sun ZFS

Oracle Site Guard provides built-in integration capabilities for Oracle Sun ZFS storage. If you are deploying Oracle Sun ZFS storage appliances, you can use the bundled storage management scripts (`zfs_storage_role_reversal.sh`) provided by Oracle Site Guard to orchestrate Sun ZFS storage role reversal as part of Oracle Site Guard disaster-recovery operations.

### 2.3.3.2 Integrating Other Storage Types

Oracle Site Guard offers integration capabilities for other storage technologies by providing a script integration framework that allows 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.

### 2.3.3.3 Mount and Unmount Scripts

In addition to the capability for integrating storage management scripts, Oracle Site Guard also offers the capability for integrating user scripts for mounting and unmounting 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 a bundled script for file system mount and unmount operations called `mount_umount.sh`. Alternately, you can define your own custom scripts that will be invoked at appropriate points in the operation plan.

## 2.3.4 Monitoring Executions and Managing Errors

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](#)
- [Monitoring Executions](#)
- [Operation Error Modes](#)
- [Retrying Failed Operations](#)


### 2.3.4.1 Customizing Operations

Oracle Site Guard operation plans can be customized according to the topology and environment. Each step in an operation plan can be customized by using the following parameters:

- 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 a step need to be handled (that is, stopping or continuing the execution of an operation if an error is encountered)

- Specifying whether the steps of a given group need to be executed serially or in parallel (for example, attempting to start up all the managed servers at the same time (in parallel), in a given domain group)

#### 2.3.4.2 Monitoring Executions

Oracle Site Guard disaster-recovery operations are executed as Oracle Enterprise Manager procedures, and the results of each operation can be monitored on the Procedure Activity page in Oracle Enterprise Manager Cloud Control Console. The procedure activity screen for a 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 green check mark is displayed if the step succeeds, or a red 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 progress of the operation plan.

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.

#### 2.3.4.3 Operation Error Modes

Each step in a Oracle Site Guard operation plan has an error mode an associated error mode that is configurable. 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.

#### 2.3.4.4 Retrying Failed Operations

If Oracle Site Guard encounters an error during an operation and stops the operation, you can resolve the issue that caused the failure, and then retry the failed 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.

#### 2.3.4.5 Suspending and Resuming Operations

You can suspend the operation at any point in time, when an Oracle Site Guard operation is in progress. You can then resume the suspended operation and 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.

---

## 2.3.5 Credential Management

The following sections describe the comprehensive credential management framework that Oracle Site Guard offers:

- [Enterprise Manager Credential Framework](#)
- [Oracle Site Guard Credential Configuration](#)

### 2.3.5.1 Enterprise Manager Credential Framework

Oracle Enterprise Manager provides a comprehensive Credential Management framework to manage identities and ensure that access to 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" in *Enterprise Manager Lifecycle Management Administrator's Guide*.

### 2.3.5.2 Oracle Site Guard Credential Configuration

After the required target credentials have been configured in Enterprise Manager's Credential Management framework, you can utilize these credentials during Oracle Site Guard's credential configuration process. Oracle Site Guard credential configuration requires that 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 and associating credentials, see [Section 4.3, "Creating Credential Associations"](#).

## 2.3.6 Role-Based Access Control

Oracle Site Guard provides Role-Based Access Control (RBAC) using the User Accounts framework provided by Enterprise Manager. Enterprise Manager provides pre-configured 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 [Section 3.2.2, "Creating Oracle Site Guard Administrator Users"](#).

## 2.3.7 Software Library Integration

Oracle Site Guard includes built-in scripts (bundled scripts) for performing activities that are typically required while executing a disaster-recovery operation, such as,

switching over an Oracle Database, or starting or stopping an Oracle Weblogic Server. These built-in 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 built-in scripts, the user may require other custom scripts to be automatically deployed and executed as part of the operation. Oracle Site Guard provides a mechanism for users to upload their own custom scripts to the Enterprise Manager Software Library and add these scripts to the operation plan when the plan is created.

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 [Section 2.3.1, "Extensibility."](#)

### 2.3.8 Custom Credentials for Script Execution

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**. However, you can also add other sets of credentials to the credential repository and configure a script to execute with this alternate 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 using a specific user ID to shut down a server process on that host.

### 2.3.9 Passing Credentials as Script Parameters

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 [Appendix A, "Extracting Credentials Passed as Parameters \(Examples\)."](#)

## 2.4 Oracle Site Guard Workflows

Oracle Site Guard workflows, also referred to as operations, are modeled as Enterprise Manager deployment procedures.

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. Stops storage replication from the primary site to the standby site, and performs storage role reversal.
3. Performs a failover or switchover of the Oracle Databases using 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.

---

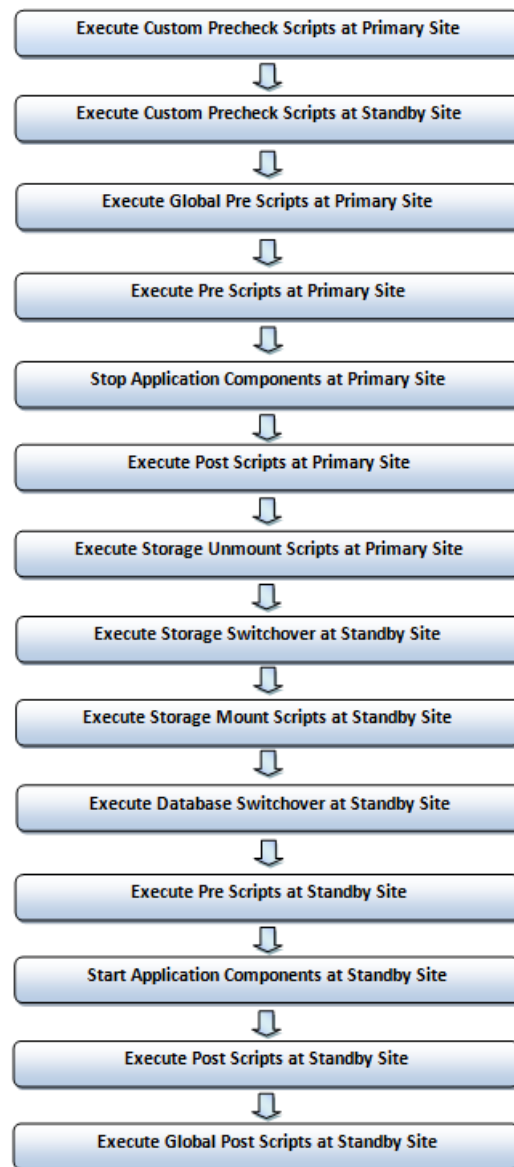
Oracle Site Guard workflow can be monitored, suspended, resumed, and stopped, using Enterprise Manager's Procedure Management framework.

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

- [Switchover Workflow](#)
- [Failover Workflow](#)
- [Start Workflow](#)
- [Stop Workflow](#)

### 2.4.1 Switchover Workflow

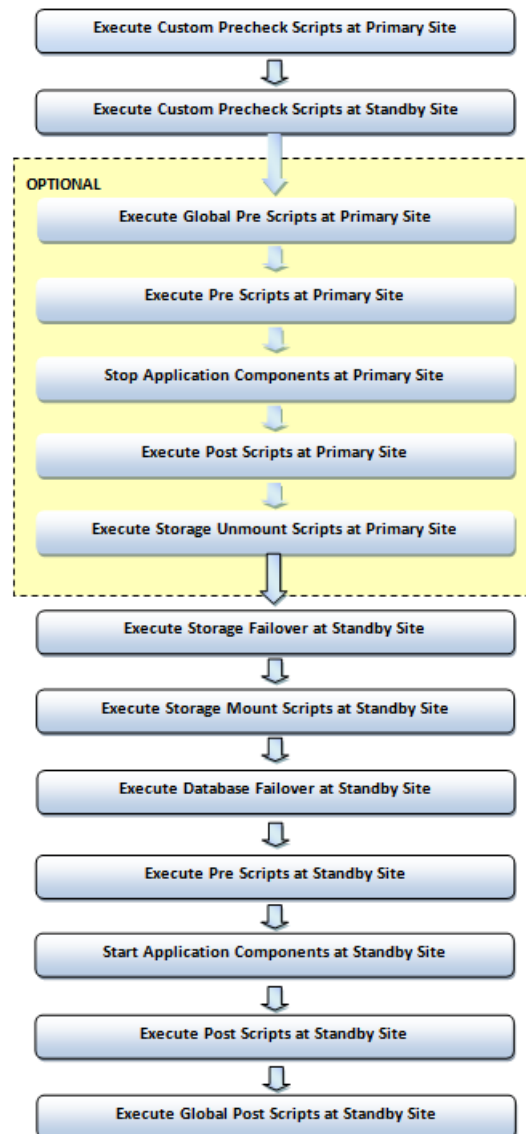
The switchover workflow provides the ability to perform a controlled transition of the production activity from the primary site to a standby site. [Figure 2-7](#) shows an example of the steps executed during a typical switchover operation.

**Figure 2–7 Switchover Workflow**

## 2.4.2 Failover Workflow

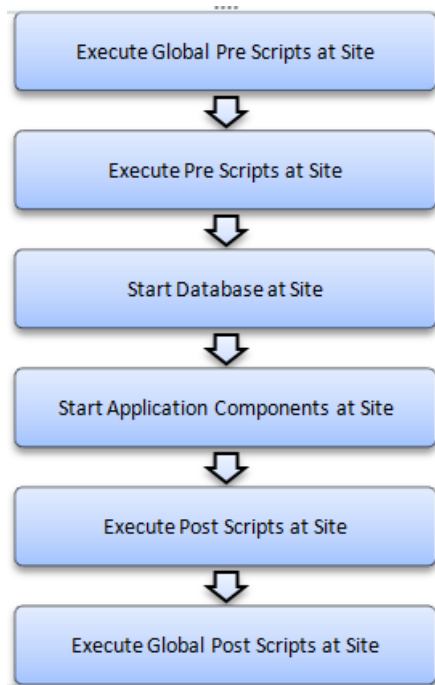
The failover workflow provides the ability to perform a forced transition of production activity to a standby site. When a failover operation is launched, Oracle Site Guard assumes that the primary site is unavailable, and starts all protected applications at the standby site. [Figure 2–8](#) shows an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



**Figure 2–8 Failover Workflow**

### 2.4.3 Start Workflow

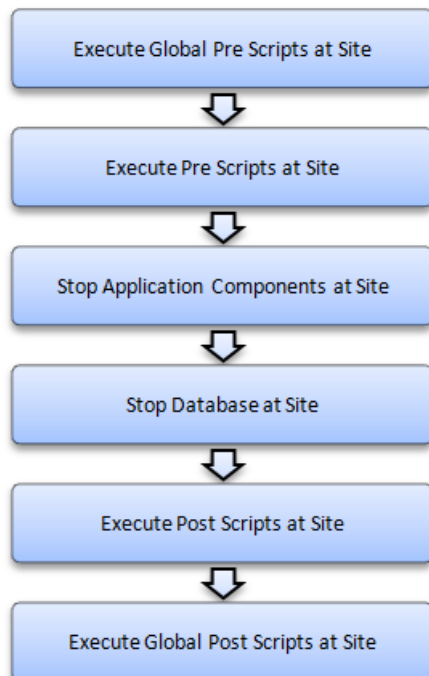
The start workflow provides the ability to start production activities at a site. This workflow is typically used to bring up a site after maintenance, or to test whether the site can be started as part of testing a larger workflow such as a switchover. [Figure 2–9](#) shows an example of the steps executed during a typical start operation.

**Figure 2–9 Start Workflow**

## 2.4.4 Stop Workflow

The stop workflow provides the ability to stop production activities at a 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 an example of the steps executed during a typical stop operation.

**Figure 2–10 Stop Workflow**

---

## Installing Oracle Site Guard

This chapter contains information about how to install Oracle Site Guard in an Enterprise Manager Cloud Control environment.

It contains the following sections:

- [Section 3.1, "Installing Oracle Site Guard"](#)
- [Section 3.2, "Prerequisites for Using Oracle Site Guard"](#)

### 3.1 Installing Oracle Site Guard

Oracle Site Guard is included with Enterprise Manager Cloud Control 12c Fusion Middleware Plugin 12.1.0.7.

You can manage an Oracle Site Guard configuration by using either Enterprise Manager Command-Line Interface (EMCLI), or a compatible version of Oracle Enterprise Manager Cloud Control (Cloud Control).

To install Oracle Site Guard, complete the following tasks:

- Install Enterprise Manager Cloud Control 12c Fusion Middleware Plugin 12.1.0.7 for your existing Oracle Fusion Middleware enterprise deployment. For information about installing Enterprise Manager Cloud Control 12c Fusion Middleware Plugin 12.1.0.7, 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 the Enterprise Manager Command-Line Interface (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`.

---

### 3.2 Prerequisites for Using Oracle Site Guard

After installing Oracle Site Guard, you must complete the following pre-requisites before beginning Oracle Site Guard Configuration.

- [Discovering Targets on the Primary Site and the Standby Site](#)
- [Creating Oracle Site Guard Administrator Users](#)
- [Creating Primary and Standby Sites](#)
- [Creating Credentials](#)
- [Granting Credential Privileges to Oracle Site Guard Administrator Users](#)
- [Configuring Software Library Storage Location](#)
- [Verifying Database and Data Guard Configurations](#)

### 3.2.1 Discovering Targets on the Primary Site and the Standby Site

As the first step towards getting started with Oracle Site Guard, you need to discover all the targets at the 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 "Performing a Switchover" 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 "Performing a Switchover" in *Oracle Fusion Middleware Disaster Recovery Guide*. You only need to switchover and switchback manually during the configuration process.

---

### 3.2.2 Creating Oracle Site Guard Administrator Users

It is recommended that you create Oracle Site Guard-focused users or administrators for managing 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.

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

- [Creating a Oracle Site Guard Administrator User Using Enterprise Manager Cloud Control Console](#)
- [Creating a Oracle Site Guard Administrator User Using Enterprise Manager Command-Line Interface](#)

### 3.2.2.1 Creating a Oracle Site Guard Administrator User Using Enterprise Manager Cloud Control Console

To create a Oracle Site Guard Administrator user using Enterprise Manager Cloud Control, complete the following steps:

1. Log in 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. Without making any changes to the other data fields, 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**.

### 3.2.2.2 Creating a Oracle Site Guard Administrator User Using Enterprise Manager Command-Line Interface

Create a Oracle Site Guard Administrator user by running the following EMCLI commands (located at OMS\_HOME/bin/emcli) in the command-line interface:

```
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_ADMINISTRATOR;EM_USER;PUBLIC.

For more information about using the `create_user` command, see "create\_user" in *Oracle Enterprise Manager Command Line Interface Guide*.

## 3.2.3 Creating Primary and Standby Sites

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

You can create a generic system using one of the following methods:

- [Creating a Generic System Using Enterprise Manager Cloud Control Console](#)
- [Creating a Generic System Using EMCLI Commands](#)

### 3.2.3.1 Creating a Generic System Using Enterprise Manager Cloud Control Console

To create a generic system for the primary site, using an Enterprise Manager Cloud Control console, complete the following steps:

1. Log in 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**.**

### 3.2.3.2 Creating a Generic System Using EMCLI Commands

Create a generic system by running the following `emcli` commands (located at `OMS_HOME/bin/emcli`) in the command-line interface:

---

**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, see the chapter "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 "create\_system" in the *Oracle Enterprise Manager Command Line Interface Guide*.

### 3.2.4 Creating Credentials

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 Host target credentials for Node Manager)
- Oracle Weblogic Server
- Oracle Database (SYSDBA)

This section contains the following topics:

- [Creating Named Credentials](#)
- [Creating Preferred Credential](#)

---

**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.

---

#### 3.2.4.1 Creating Named Credentials

You can create a named credential using one of the following methods:

- [Creating Named Credentials Using Enterprise Manager Cloud Control Console](#)
- [Creating Named Credentials Using EMCLI Commands](#)

##### **Creating Named Credentials Using Enterprise Manager Cloud Control Console**

To create a named credentials using Enterprise Manager Cloud Control Console, complete the following steps:

1. Log in 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 Details	Host (root-User Privileges) Details	Oracle Node Manager Details	Oracle WebLogic Server	Database Instance
Authenticating Target Type	Host	Host	Host	Oracle WebLogic Server	Database Instance
Credential type	Host Credentials	Host Credentials	Host 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 <b>Sudo</b> and enter values in the <b>Run As</b> 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 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. You can provide access using the procedure described 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**.

### Creating Named Credentials Using EMCLI Commands

You can create a named credential by running the following EMCLI commands in the command-line interface:

```
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	Sets 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.

Parameter	Description
attributes	<p>Enter the following credential column values:</p> <p>colname:colvalue;colname:colvalue</p> <p>You can change the value of the separator using <code>-separator=attributes=newvalue</code>. You can also change the value of the sub-separator using <code>-subseparator=attributes=newvalue</code>.</p> <p>Note: For more information about the values of this parameter, see <i>Oracle Enterprise Manager Command Line Interface Guide</i>.</p>

### 3.2.4.2 Creating Preferred Credential

You can create a preferred-credential association using one of the following methods:

- [Creating Preferred Credentials Using Enterprise Manager Cloud Control Console](#)
- [Creating Preferred Credentials Using EMCLI Commands](#)

#### Creating Preferred Credentials Using Enterprise Manager Cloud Control Console

To create preferred credentials using the Enterprise Manager Cloud Control Console, follow these steps:

1. Log in 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**.  
Select **New** to create a new named credential to be set as Preferred Credential.  
Enter a user name and password for the credential.  
Enter a credential name, and select **Save As**. The credential will be saved with the name that you have provided.  
Click **Test and Save**.

#### Creating Preferred Credentials Using EMCLI Commands

You can set a named credential as a target preferred credential by running the following `emcli` commands in the command-line interface:

---

**Note:** Oracle recommends that you to create preferred credentials using 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	Sets the preferred credential for this credential set.
target_name	Sets 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"
```

### 3.2.5 Granting Credential Privileges to Oracle Site Guard Administrator Users

The named credentials are configured as described in [Section 3.2.4.1, "Creating Named Credentials"](#), and are used to access and manage targets for disaster-recovery operations. If you have assigned Oracle Site Guard Administrator users as described in [Section 3.2.2, "Creating Oracle Site Guard Administrator Users"](#), you must also assign privileges to use these named credentials.

To grant credential privileges to Oracle Site Guard Administrators, use one of the following methods:

- [Granting Credential Privileges Using Enterprise Manager Cloud Control Console](#)

#### 3.2.5.1 Granting Credential Privileges Using Enterprise Manager Cloud Control Console

To grant credential privileges using the Enterprise Manager Cloud Control Console, follow these steps:

1. Log in 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 for which privilege is 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 user to whom the privilege is to be granted. Then click **Select**.
6. Click **Save** to save the privilege granted.

## 3.2.6 Configuring Software Library Storage Location

Oracle Software Library (Software Library) is a repository that stores scripts required to execute the operation plan.

For information about configuring a software library, see "Configuring a Software Library" in *Oracle Manager Cloud Control Administrator's Guide*.

To configure a storage location for the software library, use one of the following methods:

- [Configuring Software Library Storage Location Using Enterprise Manager Cloud Control Console](#)
- [Configuring Software Library Storage Location Using Enterprise Manager Command-Line Interface](#)

### 3.2.6.1 Configuring Software Library Storage Location Using Enterprise Manager Cloud Control Console

To configure the storage location for the Oracle Software Library, complete the following steps:

---

---

**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 configured.

---

---

1. Log in 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, see "Configuring Software Library" in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

---

---

### 3.2.6.2 Configuring Software Library Storage Location Using Enterprise Manager Command-Line Interface

You can configure storage location in the software library by running the following EMCLI command in the command-line interface:

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

Parameter	Description
name	Sets the name for the software library.
path	Sets the path to the software library location.

For example:

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

## 3.2.7 Verifying Database and Data Guard Configurations

Oracle Site Guard uses Oracle Data Guard to perform database switchovers and failovers. To ensure that Oracle Site Guard can correctly perform database operations as part of disaster recovery workflows, perform the following steps:

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 reinstated after a failover operation.
2. Ensure 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, using the DGMGRL utility).

---

---

**Note:** For more information about viewing the summary and status of the Data Guard Broker configuration, see "SHOW CONFIGURATION" in the *Oracle Data Guard Broker* guide.

---

---

---

# Configuring Oracle Site Guard

This chapter describes the tasks that you must follow to configure Oracle Site Guard.

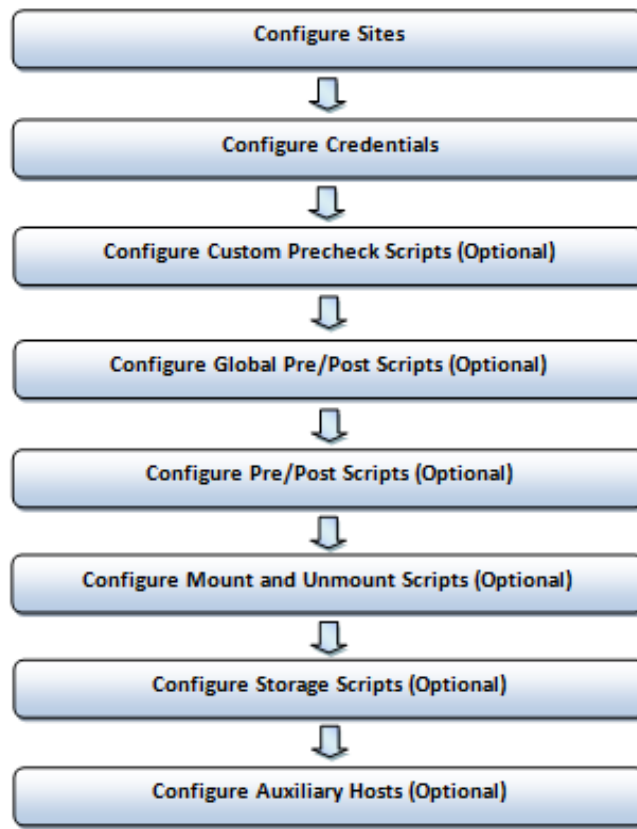
It contains the following topics:

- [Section 4.1, "Overview"](#)
- [Section 4.2, "Configuring Sites"](#)
- [Section 4.3, "Creating Credential Associations"](#)
- [Section 4.4, "Configuring Scripts"](#)
- [Section 4.5, "Configuring Auxiliary Hosts"](#)
- [Section 4.6, "Configuring Database Lag Checks"](#)

## 4.1 Overview

Before you create operation plans for disaster recovery, you must first configure Oracle Site Guard. After configuring Oracle Site Guard, you can create operation plans that use the configuration you have created.

[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 [Section 3.2, "Prerequisites for Using Oracle Site Guard"](#).
  - You must log in using the `EM_SG_ADMINISTRATOR` role privilege for performing the configuration tasks. Ensure that you have created the required user credentials as described in [Section 3.2.2, "Creating Oracle Site Guard Administrator Users"](#).
- 

## 4.2 Configuring Sites

As the first step towards setting up a disaster-recovery configuration, you must configure sites, and designate roles to the configured sites. The configured sites must be designated as the primary (production) sites and standby sites.

Configure sites using one of the following methods:

- [Configuring Sites Using Enterprise Manager Cloud Control Console](#)
- [Configuring Sites Using EMCLI Commands](#)

### 4.2.1 Configuring Sites Using Enterprise Manager Cloud Control Console

To create an Oracle Site Guard configuration and associate a standby system with the primary system, complete the following steps:



1. Log in 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 [Section 3.2.3, "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.

## 4.2.2 Configuring Sites Using EMCLI Commands

To add the configuration for the primary and standby sites, you must run the following `emcli` commands in the command-line interface:

---

**Note:** For information about logging in to `emcli`, see chapter "Command Line Interface Concepts and Installation" in the *Oracle Enterprise Manager Command Line Interface Guide*.

---

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

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

To display information about the association between existing primary and standby sites, run the following `emcli` commands in the command-line interface:

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

## 4.3 Creating Credential Associations

This section describes how to associate Site Guard managed targets and credentials that you created in [Section 3.2.4, "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 [Section 3.2.4, "Creating Credentials"](#).
  - Ensure that you have created a user with EM\_SG\_ADMINISTRATOR privileges, as described in [Section 3.2.2, "Creating Oracle Site Guard Administrator Users"](#), and granted credential privileges to that user as described in [Section 3.2.5, "Granting Credential Privileges to Oracle Site Guard Administrator Users"](#).
- 
- 

It is essential that you 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

### 4.3.1 Creating Named or Preferred Credential Associations

You can create Named or Preferred Credential associations using one of the following methods:

- [Creating Named or Preferred Credential Associations Using Enterprise Manager Cloud Control Console](#)
- [Creating Named or Preferred Credential Associations Using EMCLI Commands](#)

#### 4.3.1.1 Creating Named or Preferred Credential Associations Using Enterprise Manager Cloud Control Console

To create named credentials using Enterprise Manager Cloud Control Console, complete the following steps:

1. Log in 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 **Use Preferred Credentials** option on the page. On selecting **Use Preferred Credentials**, the Named Credentials section is disabled. To select named credentials, deselect **Use Preferred Credentials**.

- 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 **Use Preferred Credentials** option on the page. On selecting **Use Preferred Credentials**, the Named Credentials section is disabled. To select named credentials, deselect **Use Preferred Credentials**.

- c. Click **Save**.

### Associate Oracle Node Manager Credentials

Associate Oracle Node Manager credentials to connect to manage node manager targets. You must also associate Oracle Node Manager credentials each sites that have a Oracle Weblogic Server target, however when you configure Oracle Node Manager credentials, you must configure using credentials for the type `HostNormal` or `HostPrivileged`.

To associate Oracle Node Manager credentials, follow these steps:

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

The Add Oracle Node Manager Credentials dialog appears.

- 2. 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 **Use Preferred Credentials** option on the page. On selecting **Use Preferred Credentials**, the Named Credentials section is disabled. To select named credentials, deselect **Use Preferred Credentials**.

- 3. 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 **Use Preferred Credentials** option on the page. On selecting **Use Preferred Credentials**, the **Named Credentials** section is disabled. To select named credentials, deselect **Use Preferred Credentials**.

- 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 Oracle WebLogic Administration 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 **Use Preferred Credentials** option on the page. On selecting **Use Preferred Credentials**, the **Named Credentials** section is disabled. To select named credentials, deselect **Use Preferred Credentials**.

- c. Click **Save**.

#### 4.3.1.2 Creating Named or Preferred Credential Associations Using EMCLI Commands

You can create a named or preferred credential associations for targets by running the credential framework EMCLI commands in the command-line interface:

```
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"
```

Parameter	Description
-system_name	Specify the name of the system.
-target_name	Specify the name of the target. This parameter is optional.
-credential_type	Specify the type of the credential. Example: HostNormal, HostPrivileged, NodeManager, WLSAdmin, or DatabaseSysdba.  <b>Note:</b> For Node Manager credential, specify the NodeManager credential_type, and specify the values for target_name, but use HostNormal credential for credential_name.

Parameter	Description
<code>-credential_name</code>	Specify the name of the credential.  If the value for <code>credential_name</code> is not specified, then <code>use_preferred_credential</code> has to be set to <code>true</code> .
<code>-credential_owner</code>	Specify the owner of the credential.
<code>-use_preferred_credential</code>	If you are using Preferred Credentials, then specify <code>true</code> . The default value is <code>false</code> . If you use the default value, then you must specify the <code>-credential_name</code> parameter to use named credentials.

## 4.4 Configuring Scripts

Oracle Site Guard provides a mechanism for users to configure different types of scripts for managing disaster-recovery operations. Depending on their function, these scripts either come bundled with Oracle Site Guard, or they can be provided by the user. You must configure these scripts while configuring Oracle Site Guard. Note that these scripts must be added 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 must be manually staged (deployed) on each host where they are defined to run.

You can configure the following types of scripts using 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 [Section 2.3.1, "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, see [Section 2.3.1, "Extensibility."](#)

- Mount and Unmount scripts

Mount and Unmount scripts as described in [Section 2.3.3, "Storage Integration"](#), are needed for files system mount and unmount operations that are performed during operations. You can use the scripts that are bundled with Oracle Site Guard, or you can provide your own scripts.

- Storage scripts

Storage scripts as described in [Section 2.3.3, "Storage Integration"](#), are needed for storage management that must be performed during operations. You can use the scripts that are bundled with Oracle Site Guard, or you can 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.

This section contains the following topics:

- [Configuring Custom Precheck Scripts, Pre Scripts, Post Scripts, Global Pre Scripts, and Global Post Scripts](#)
- [Configuring Mount and Unmount Scripts](#)
- [Configuring Storage Scripts](#)
- [Configuring Credentials as Parameters for Scripts](#)
- [Cloning a Script Using Existing Scripts](#)

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

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

Parameter	Description
script path	The file system path where the script resides. Note that the script must reside at the same path location on each host specified in the <code>target hosts</code> parameter.
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.
target hosts	The list of hosts where the script will run.
run on	Specifies whether the script should run on Any or All of the hosts specified in the <code>target hosts</code> parameter.
operation type	The operation type that the script is configured for (switchover, failover, start, or stop).
role	Specifies 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.
credential type	Specifies the type of credential to be used for executing the script on the specified hosts (Normal Host Credentials or Privileged Host Credentials).  For information about various types of credentials, see <a href="#">Section 4.3, "Creating Credential Associations"</a>


To configure Custom Precheck Scripts, Pre Scripts, Post Scripts, Global Pre Scripts, and Global Post Scripts, follow one of these methods:

- [Configuring Custom Precheck Scripts, Pre Scripts, Post Scripts, Global Pre Scripts, and Global Post Scripts Using Enterprise Manager Cloud Control Console](#)

- [Configuring Custom Precheck Scripts, Pre Scripts, Post Scripts, Global Pre Scripts, and Global Post Scripts Using EMCLI Commands](#)

#### 4.4.1.1 Configuring Custom Precheck Scripts, Pre Scripts, Post Scripts, Global Pre Scripts, and Global Post Scripts Using Enterprise Manager Cloud Control Console

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

1. Log in 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 file system for the script. You can also browse file systems on the remote host after specifying the 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 depending on the type of script being configured:
    - **Custom Precheck Script**
    - **Pre Script**
    - **Post Script**
    - **Global Pre Script**
    - **Global Post Script**
  - **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**.
  - **Operation Type:** The operation during which this script will run. Choose from the options - **Switchover**, **Failover**, **Start**, or **Stop**.
  - **Role:** Select **Primary** or **Standby** 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** can only be selected when the operation type is **Start** or **Stop**. For **Switchover** and **Failover** operations, the **Role** parameter is selected by Oracle Site Guard and cannot be modified.

---

- **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**.
- **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 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.

8. Click **Save**.

#### 4.4.1.2 Configuring Custom Precheck Scripts, Pre Scripts, Post Scripts, Global Pre Scripts, and Global Post Scripts Using EMCLI Commands

To configure Pre Scripts, Post Scripts, Global Pre Scripts, and Global Post Scripts with Oracle Site Guard, run the following `emcli` commands in the command-line interface:

```
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"]
[-target_storage_credential_name=target_storage_credential]
[-source_storage_credential_name=source_storage_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	Specify the name of the system.
-operation	Specify the name of the operation. Name of the operation:  Switchover, Failover, Start, or Stop.
-script_type	Specify 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.
-host_name	Specify the name of the host where this script will be executed.  This parameter is optional and can be specified more than once.
-path	Specify the path to the script.
-component	Specify 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	Specify 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	Specify 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	Specify HostNormal or HostPrivileged if you have root privileges.
-credential_name	Specify 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.
-target_storage_credential_name	Specify the named credential for target storage. If target_storage_credential_name is specified then source_storage_credential_name and credential_owner must be specified.
-source_storage_credential_name	Specify the named credential for source storage. If source_storage_credential_name is specified then target_storage_credential_name and credential_owner must be specified.
-credential_owner	Specify 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.

**Note:**

- [ ] indicates that the parameter is optional.
- You may specify the option host\_name more than once.
- Specifying -all\_hosts=true overrides any hosts selected using the -host\_name option.
- The -role option is only applicable for Pre-Script or Post-Script.

## 4.4.2 Configuring Mount and Unmount Scripts

Mount and Unmount 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 script, mount\_umount.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 file system 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 mount\_umount.sh. However, if your scripts are not part of the software library, then you must deploy these scripts on all hosts where they need to run.

#### 4.4.2.1 mount\_umount.sh

This section provides the syntax and usage for the `mount_umount.sh` script.

For mounting and unmounting file systems, configure the bundled `mount_umount.sh` script as shown in [Example 4-1](#).

##### **Example 4-1 Usage of mount\_umount.sh Script**

```
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 file systems.
- 
- 

To mount multiple directories, run the following command:

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

To mount a single directory, run the following command:

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

To unmount multiple directories, run the following command:

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

To unmount a single directory, run the following command:

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

Configure mount or unmount scripts using one of the following options:

- [Configuring Mount or Unmount Scripts Using Enterprise Manager Cloud Control Console](#)
- [Configuring Mount or Unmount Scripts Using EMCLI Commands](#)

##### **4.4.2.1.1 Configuring Mount or Unmount Scripts Using Enterprise Manager Cloud Control**

**Console** To configure a mount or unmount script using Enterprise Manager Cloud Control Console, follow these steps:

1. Log in 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:** Specify the bundled `mount_umount.sh` script with the appropriate options (see [Section 4.4.2.1, "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 file system. You can also browse file systems 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** or **Failover**
- **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:** Specify 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**.

**4.4.2.1.2 Configuring Mount or Unmount Scripts Using EMCLI Commands** To configure a mount or unmount script, run the following `emcli` command using the command-line interface:

```
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_script"]
  [-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"]
```

Parameter	Description
-system_name	Specify the system for which the script is being configured.
-operation	Specify the function of the operation. Example: Switchover or Failover.
-script_type	The type of script. Depending on the function you want to perform, enter one of the following options: <ul style="list-style-type: none"> <li>■ Mount</li> <li>■ UnMount</li> </ul>
-host_name	Specify 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. <b>Note:</b> Ensure that all hosts are part of the system specified in system_name.

Parameter	Description
-path	<p>Enter the path to the script.</p> <p>If you are configuring the bundled <code>mount_umount.sh</code> script specify the path as described in <code>mount_umount.sh</code>.</p> <p>For example:</p> <pre>sh mount_umount.sh -o mount -f /u02/oracle/config,/u02/oracle/product,/u02/oracle/stage</pre> <p>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.</p> <p>For example:</p> <pre>sh example_script.sh -a value1 -b value2 -c value3</pre> <p>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.</p> <p><b>Note:</b> The script must reside at the same path location on each host.</p> <p>For example:</p> <pre>/path_to_the_script/example_script.sh -a value1 -b value2 -c value3</pre>
-component	Specify the path to the entity in the software library. If the component is specified, the <code>-path</code> option should contain only the script name and its parameters.
-runtime	Specify if 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 <code>false</code> .
-run-on	Specify whether the script needs to be executed on only one of the available hosts (enter <code>any</code> ) or on all hosts (enter <code>all</code> ).
-all_hosts	Specify this optional flag to enable the script to run on all the hosts in the system. This parameter overrides the <code>-host_name</code> parameter.
-role	This option is not applicable for scripts of type <code>Mount</code> and <code>UnMount</code> .
-credential_type	Specify <code>HostNormal</code> credentials or <code>HostPrivileged</code> credentials for users with <code>root</code> privileges. If values for <code>credential_type</code> are not specified, then the values for <code>credential_name</code> must be specified.
-credential_name	Specify an alternate named credential to use when executing this script. If the values for <code>credential_name</code> are not specified, then the values for <code>credential_type</code> must be specified.
-target_storage_credential_name	This option is not applicable for scripts of type <b>Mount</b> and <b>UnMount</b> .

Parameter	Description
<code>-source_storage_credential_name</code>	This option is not applicable for scripts of type <b>Mount</b> and <b>UnMount</b> .
<code>-credential_owner</code>	This option is not applicable for scripts of type <b>Mount</b> and <b>UnMount</b> .

### 4.4.3 Configuring Storage Scripts

Storage scripts are used for Storage Switchover and Storage Failover operations. There are two types of storage scripts:

- **Bundled**

Oracle Site Guard provides a bundled script for handling file-system 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 file system 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.

#### 4.4.3.1 `zfs_storage_role_reversal.sh`

This section provides the syntax and usage for the `zfs_storage_role_reversal.sh` script. 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.

For switchover and failover operations, configure the bundled `zfs_storage_role_reversal.sh` script as shown in [Example 4-2](#) and the following table.

**Example 4-2 Usage of `zfs_storage_role_reversal.sh` Script**

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

Option	Description	Mandatory?
<code>--target_appliance</code> or <code>-t</code>	Specify the host name of the target ZFS appliance. For example: <code>zfsite1.example.com</code>	Yes
<code>--target_user</code> or <code>-w</code>	Specify 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: <code>root</code>	No

Option	Description	Mandatory?
--source_appliance or -h	Specify the host name of the source ZFS appliance. For example: zfsite2.example.com	Yes
--source_user or -u	Specify 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	Specify the name of the replicated ZFS project. For example: ZFS-DR-Project.	Yes
--target_pool_name or -p	Specify the name of the storage pool on the target ZFS appliance. For example: zfssite1-pool-0	Yes
--source_pool_name or -q	Specify 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, failover, switchover_prechecks, or failover_prechecks.	Yes
--is_sync_needed or -c	Specify 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	Specify 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	Specify 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	Specify 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	Specify 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)	No



Option	Description	Mandatory?
<code>--is_source_reachable</code> or <code>-x</code>	Specify 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
<code>--source_user_equivalence</code> or <code>-m</code>	Specify 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: <code>--source_user_equivalence user1</code>	No
<code>--target_user_equivalence</code> or <code>-n</code>	Specify 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: <code>--target_user_equivalence user2</code>	No

Configure Storage scripts using one of the following options:

- [Configuring Storage Scripts Using Enterprise Manager Cloud Control Console](#)
- [Configuring Storage Scripts Using Enterprise Manager Command-Line Interface](#)

#### 4.4.3.2 Configuring Storage Scripts Using Enterprise Manager Cloud Control Console

1. Log in 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:** Specify the bundled `zfs_storage_role_reversal.sh` script with the appropriate options (see [Section 4.4.3.1](#), "`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 file system. You can also browse file systems 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 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**

Selecting **Storage Switchover** or **Storage Failover** for the **Script Type** changes the available options in the dialog. Two additional options called **Target Storage Credential** and **Source Storage Credential** appear.

- **Run On:** Select **All Hosts** to run the script on all selected hosts. To run the script on any one of the selected target hosts, select **Any Host**.
- **Operation Type:** The operation during which this script will run. Choose from the options - **Switchover** or **Failover**.
- **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 to use for executing the script.
  - **Normal Host Credentials** to use the Normal (non-root) privileges configured for that script host.
  - **Privileged Host Credentials** to use the Privileged (root) privileges configured for that script host.
  - **Custom Host Credentials** to use an alternate set of named credentials. If this option is chosen, select the named credential to use 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**.

- **Target Storage Credential:** Select the named credential to be used for accessing the target storage appliance.
- **Source Storage Credential:** Select the named credential to be used for accessing the source storage appliance.
- **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.

8. Click **Save**.

#### 4.4.3.3 Configuring Storage Scripts Using Enterprise Manager Command-Line Interface

To configure a storage script, run the following `emcli` command using the command-line interface:

```
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_script_will_be_run"]
    -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_script"]
    [-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"]
```

Parameter	Description
-system_name	Specify the system for which the script is being configured.
-operation	Specify the function of the operation. Example: Switchover, Failover, Start, or Stop.
-script_type	Specify the type of script depending on the operation you want to perform.  For example: Storage Switchover or Storage Failover.
-host_name	Specify 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 <code>system_name</code> .

Parameter	Description
-path	<p>Enter the path to the script.</p> <p>If you are configuring the bundled <code>zfs_storage_role.sh</code> script specify the path as described in "<a href="#">zfs_storage_role_reversal.sh</a>".</p> <p>For example:</p> <pre>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</pre> <p>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.</p> <p>For example:</p> <pre>sh example_script.sh -a value1 -b value2 -c value3</pre> <p>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.</p> <p><b>Note:</b> The script must reside at the same path location on each host.</p> <p>For example:</p> <pre>/path_to_the_script/example_script.sh -a value1 -b value2 -c value3</pre>
-component	Specify the path to the entity in software library. If component is specified, the <code>-path</code> option should contain only the script name and its parameters.
-runtime_script	Specify if 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 <code>false</code> for scripts that are not staged from software library.
-run_on	<p>Specify whether the script needs to be executed on only one of the available hosts (enter <code>any</code>) or on all hosts (enter <code>all</code>).</p> <p>This parameter is optional and default value is <code>all</code>.</p>
-all_hosts	Specify this optional flag to enable the script to run on all the hosts in the system. This parameter overrides the <code>host_name</code> .
-role	This option is not applicable for scripts of type <b>Storage Switchover</b> and <b>Storage Failover</b> .
-credential_type	Specify <code>HostNormal</code> credentials or <code>HostPrivileged</code> credentials for users with <code>root</code> privileges. If the values for the parameter <code>credential_type</code> are not specified, then the values for <code>credential_name</code> must be specified.
-credential_name	Specify an alternate named credential to use when executing this script. If the values for the parameter <code>credential_name</code> are not specified, then the values for the parameter <code>credential_type</code> must be specified.

Parameter	Description
-target_storage_credential_name	Specify the named credential to be used for accessing the target storage appliance. This option is only applicable for scripts of type <code>Storage Switchover</code> and <code>Storage Failover</code> . If the values for the parameter <code>target_storage_credential_name</code> are specified, then the values for <code>source_storage_credential_name</code> and <code>credential_owner</code> must be specified.
-source_storage_credential_name	Specify the named credential to be used for accessing the source storage appliance. This option is only applicable for scripts of type <code>Storage Switchover</code> and <code>Storage Failover</code> . If the values for the parameter <code>target_storage_credential_name</code> are specified, then <code>target_storage_credential_name</code> and <code>credential_owner</code> must be specified.
-credential_owner	Specify the owner of the named credential for <code>target_storage_credential</code> and <code>source_storage_credential</code> .

#### 4.4.4 Configuring Credentials as Parameters for Scripts

Oracle Site Guard provides EM CLI commands for adding, deleting, and getting credentials as parameters to scripts. Before you configure a script to receive credentials as parameters, ensure that you have created these credentials as described in [Section 3.2.4, "Creating Credentials."](#) Also, ensure that the script for which you will configure credential parameters for, is already configured as described [Section 4.4, "Configuring Scripts."](#)

The following actions can be performed for configuring credentials as script parameters:

- [Adding Credential Parameters to a Script](#)
- [Deleting Credential Parameters from a Script](#)
- [Getting Credential Parameters for a Script](#)

##### 4.4.4.1 Adding Credential Parameters to a Script

To add credentials parameters to a configured script, run the following EM CLI command using the command-line interface. You must execute this command once for each set of credentials that need to be configured as parameters to a script:

```
emcli add_siteguard_script_credential_params
    -script_id="id_associated_with_the_script"
    -credential_name="name_of_the_credential"
    [-credential_owner="credential_owner"]
```

Parameter	Description
-script_id	Specify the script ID.
-credential_name	Specify the name of the credential.
-credential_owner	Specify 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.

##### 4.4.4.2 Deleting Credential Parameters from a Script

To delete one or more credentials parameters that are already configured for a script, run the following EM CLI command using the command-line interface:

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

Parameter	Description
-script_id	Specify the ID associated with the script.
-credential_name	Specify 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	Specify 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.

#### 4.4.4.3 Getting Credential Parameters for a Script

To get a list of one or more credentials parameters configured for a script, run the following EM CLI command using the command-line interface:

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

Parameter	Description
-script_id	Specify the ID associated with the script.
-credential_name	Specify 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	Specify 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.

#### 4.4.5 Cloning a Script Using Existing Scripts

You can create and configure new scripts by cloning (copying) an existing script. This applies to all types of scripts.

To clone a script using the Enterprise Manager Cloud Control Console, follow these steps:

1. Log in 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**.

## 4.5 Configuring Auxiliary Hosts

You can configure one or more hosts managed by Enterprise Manager, as an auxiliary host to the site. An auxiliary host needs to be managed by Enterprise Manager. It can be part of one or more sites. These hosts can be used to run Pre Scripts, Post Scripts, or Storage Scripts on a site.

The following actions can be performed:

- [Adding an Auxiliary Host Using EMCLI Commands](#)
- [Deleting an Auxiliary Host Using EMCLI Commands](#)
- [Listing Auxiliary Targets Using EMCLI Commands](#)

### 4.5.1 Adding an Auxiliary Host Using EMCLI Commands

To add an auxiliary host on a site, run the following EMCLI command in the command-line interface:

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

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

### 4.5.2 Deleting an Auxiliary Host Using EMCLI Commands

To delete a auxiliary host on a site, run the following EMCLI command in the command-line interface:

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

Parameter	Description
-system_name	Specify the system on which you are performing the operation.
-host_name	The name of the host where the script will be run. <b>Note:</b> Ensure that the hostname is part of the system specified in system_name.

### 4.5.3 Listing Auxiliary Targets Using EMCLI Commands

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

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

Parameter	Description
-system_name	Specify the system on which you are performing the operation.

## 4.6 Configuring Database Lag Checks

This section describes how to configure values of Apply Lag and Transport Lag for one or more Data Guard enabled databases.

It contains the following topics:

- [Configuring Database Lag Checks Using EMCLI Commands](#)
- [Updating Threshold Value for Database Lag Using EMCLI Commands](#)
- [Deleting Threshold Value for Database Lag Using EMCLI Commands](#)
- [Listing Database Lag Thresholds Using EMCLI Commands](#)

### 4.6.1 Configuring Database Lag Checks Using EMCLI Commands

You can configure values of Apply Lag and Transport Lag for one or more Data Guard enabled databases by running the following commands:

```
emcli configure_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	Specify the system on which you want to configure the threshold limit.
-target_name	Specify 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	Specify the property name. Valid values are ApplyLag and TransportLag.
-value	Specify the threshold value to be configured (in seconds).

### 4.6.2 Updating Threshold Value for Database Lag Using EMCLI Commands

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

```
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	Specify the system for which you want to configure the threshold limit.
-target_name	Specify 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	Specify the property name. Valid values are ApplyLag and TransportLag.
-value	Specify the threshold value to be updated (in seconds).

### 4.6.3 Deleting Threshold Value for Database Lag Using 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 commands:

```
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	Specify the system for which you want to configure the threshold limit.
-target_name	Specify 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	Specify the property name. Valid values are ApplyLag and TransportLag.

### 4.6.4 Listing Database Lag Thresholds Using EMCLI Commands

To view values of the configured database Apply Lag and Transport Lag threshold limits of a system, run the following 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	Specify the system for which you want to retrieve the threshold limit.
-target_name	Specify the database target name for which the threshold limit is to be retrieved. If this parameter is not specified, then the threshold values of all databases of the system are listed.
-property_name	Specify the property name. Valid values are ApplyLag and TransportLag.

---

## Troubleshooting Oracle Site Guard

This chapter describes common situations that you might encounter when deploying and managing Oracle Site Guard in disaster-recovery topologies. It also includes the steps for addressing them.

This chapter contains the following sections:

- [Section 5.1, "Operation Plan Failure"](#)
- [Section 5.2, "Switchover or Failover Operations Failure"](#)
- [Section 5.3, "Precheck Failure"](#)
- [Section 5.4, "Oracle WebLogic Server Failure"](#)
- [Section 5.5, "Database Failure"](#)
- [Section 5.6, "Storage Failures"](#)

### 5.1 Operation Plan Failure

This section provides tips for troubleshooting the following operation-plan failure 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 Workflow](#)
- [Failure of Operation Step When Accessed with Sudo Privileges](#)
- [Error While Creating Operation Plan Indicating Credential Association Not Configured](#)
- [Inability to Associate Credentials for Targets Added to a Site](#)
- [Error Indicating Inability to Create Scalar Value While Creating Operation Plan](#)
- [Error While Deleting Or Updating Operation Plans](#)
- [Error While Creating Operation Plan Indicating Missing Node Manager Credentials](#)

### 5.1.1 Targets Not Discovered in Operation Plan Workflow

#### 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.

### 5.1.2 Oracle WebLogic Server Managed-Server Target Not Identified

#### 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.

### 5.1.3 Manual Intervention Needed for Hung Operation Step

#### 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.

---

---

### 5.1.4 OPMN Managed System Components Not Discovered In Operation-Plan Workflow

#### 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.

## 5.1.5 Oracle RAC Database Not Discovered in Operation-Plan Workflow

### Issue

Oracle RAC Database, which is part of the system, may not be 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.

## 5.1.6 Failure of Operation Step When Accessed with Sudo Privileges

### Issue

Site Guard operation step fails with the error `stageOmsFileEntry (Error)`, while 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.

## 5.1.7 Error While Creating Operation Plan Indicating Credential Association Not Configured

### 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 Manager, 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.

## 5.1.8 Inability to Associate Credentials for Targets Added to a Site

### 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 Manager, 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.

## 5.1.9 Error While Deleting Or Updating Operation Plans

### 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  
XXXXXXXXXXXXXXXXXXXX
```

### Description and Solution

This might occur when a user does not have the necessary privileges to delete or update the operation plan.

Log in using the credentials that were used while creating the operation plan, and then delete or update the plan.

## 5.1.10 Error Indicating Inability to Create Scalar Value While Creating 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 using `DGMGRL` or using Site Guard.)

To correct this issue, using Enterprise Manager Cloud Console, log in 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.

### 5.1.11 Error While Creating Operation Plan Indicating Missing Node Manager Credentials

#### 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.

## 5.2 Switchover or Failover Operations Failure

This section provides tips for troubleshooting the following issues that you may encounter during switchover or failover operations:

- [WebLogic Administration Server Does Not Start After Performing Switchover or Failover Operation](#)
- [WebLogic Administration Server Fails to Restart After Performing Switchover or Failover Operations](#)
- [Host Not Available During Switchover or Failover Operations](#)
- [Switchover or Failover Operations Fail When Oracle RAC Database Instances Are Not Available](#)

### 5.2.1 WebLogic Administration Server Does Not Start After Performing Switchover or Failover Operation

#### Issue

The WebLogic Administration Server might not start after performing 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/).

## 5.2.2 WebLogic Administration Server Fails to Restart After Performing Switchover or Failover Operations

### Issue

The WebLogic Administration Server might not start after performing 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 using 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.

## 5.2.3 Host Not Available During Switchover or Failover Operations

### 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.

## 5.2.4 Switchover or Failover Operations Fail When Oracle RAC Database Instances Are Not Available

### 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.

## 5.3 Precheck Failure

This section provides tips for troubleshooting the following Precheck failures:

- [Failure of Prechecks](#)
- [Prechecks Hang When Oracle Management Agent Is Not Available](#)



### 5.3.1 Failure of Prechecks

#### Issue

Prechecks fail, displaying 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, as described in the section "After You Install" in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

### 5.3.2 Prechecks Hang When Oracle Management Agent Is Not Available

#### 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.

## 5.4 Oracle WebLogic Server Failure

This section provides troubleshooting tips for the following Oracle WebLogic Server failure issues:

- [Node Manager Fails to Restart](#)
- [Managed Server Fails to Start](#)
- [Oracle Site Guard Does Not Include Oracle WebLogic Server Instances That Are Migrated to a Different Host](#)
- [Error Displayed While Creating Operation Plan](#)
- [WebLogic Administration Server Able to Communicate With Node Manager When Site Guard Cannot](#)

### 5.4.1 Node Manager Fails to Restart

#### 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 (using `wlst.sh`) 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.

---

---

## 5.4.2 Managed Server Fails 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.

## 5.4.3 Oracle Site Guard Does Not Include Oracle WebLogic Server Instances That Are Migrated to a Different Host

### 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.

## 5.4.4 Error Displayed While Creating Operation Plan

### Issue

While creating an operation plan, you might 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, using 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, refer to the *Oracle Fusion Middleware Disaster Recovery Guide*.

### 5.4.5 WebLogic Administration Server Able to Communicate With Node Manager When Site Guard Cannot

**Issue**

Oracle Site Guard is unable to access the Node Manager even though the Weblogic Administrator 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, complete 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.

### 5.4.6 Unable to Associate More Than One Node Manager Per Host

**Issue**

Oracle Site Guard is unable to associate credentials for more than one Node Manager 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.

## 5.5 Database Failure

This section provides tips for troubleshooting the following issues related to database operation failure:

- [Prechecks for Database Switchover and Database Failover Operations Fail](#)
- [Databases Protected by Data Guard Included in the Incorrect Operation-Plan Category](#)

## 5.5.1 Prechecks for Database Switchover and Database Failover Operations Fail

### Issue

The Prechecks for database switchover or database failover operations fail, and display 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. For more information, see "CommunicationTimeout" in *Oracle Data Guard Broker*.

## 5.5.2 Databases Protected by Data Guard Included in the Incorrect Operation-Plan Category

### 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 using `DGMGRL` or using Oracle 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.

## 5.6 Storage Failures

This section provides tips for troubleshooting the following issues related to storage and storage appliances:

- [Attempt to Log In to ZFS Storage Appliance Might Fail During Execution of Operation Plan](#)

- Storage Role Reversal Operation Might Fail During Execution of Operation Plan While Deleting Empty Project on Target Appliance
- Storage Role Reversal Operation Might Fail During Execution of Operation Plan While Executing 'confirm reverse'

### 5.6.1 Attempt to Log In to ZFS Storage Appliance Might Fail During Execution of Operation Plan

#### 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.

### 5.6.2 Storage Role Reversal Operation Might Fail During Execution of Operation Plan While Deleting Empty Project on 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 'nodelstroy' property set. Turn off the property for 'l\_test' and try again.

#### Description and Solution

This occurs if the project has the `nodelstroy` 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.

### 5.6.3 Storage Role Reversal Operation Might Fail During Execution of Operation Plan While Executing 'confirm reverse'

#### 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.

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.

---

# Performing Oracle Site Guard Operations

This chapter contains information about creating, executing and monitoring Oracle Site Guard operation plans.

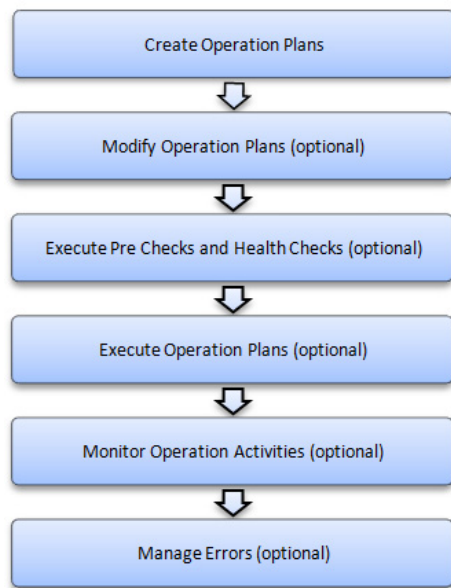
It contains the following topics:

- Section 6.1, "Overview"
- Section 6.2, "Managing Operation Plans"
- Section 6.3, "Running Prechecks"
- Section 6.4, "Scheduling Health Checks"
- Section 6.5, "Executing Oracle Site Guard Operation Plans"
- Section 6.6, "Monitoring Oracle Site Guard Operations"
- Section 6.7, "Managing Execution Errors"

## 6.1 Overview

Oracle Site Guard operation plans contain steps that must be executed during a disaster-recovery activity. In addition to the steps defined in an operation plan, the operation plan allows for such concepts as serial and parallel execution of steps, ignoring or retrying steps upon error, and so on.

Figure 6–1 shows the roadmap for managing 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 listed in the figure below.

**Figure 6–1 Workflow for Oracle Site Guard Operations**

---

**Note:**

- Before you create operation plans, ensure that you complete the tasks listed in [Chapter 4, "Configuring Oracle Site Guard"](#).
  - You must log in using the `EM_SG_ADMINISTRATOR` role privilege for performing the configuration tasks. Ensure that you have created the required user credentials as described in [Section 3.2.2, "Creating Oracle Site Guard Administrator Users"](#).
- 

## 6.2 Managing Operation Plans

An operation plan contains the execution flow for the Oracle Site Guard operation. It is a pre-configured workflow consisting of a set of ordered actions (steps).

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

Steps such as the following, can be included in an operation plan:

- Stopping Oracle HTTP Servers.
- Stopping the node managers, managed servers, and administration server in an Oracle WebLogic domain.
- Performing a database role reversal using 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.

This section contains the following topics:

- [Creating Operation Plans](#)
- [Creating New Operation Plans Using Existing Plans](#)



- [Editing and Updating Operation Plans](#)

## 6.2.1 Creating Operation Plans

You can create an operation plan using one of the following methods:

- [Creating an Operation Plan Using Enterprise Manager Cloud Control Console](#)
- [Creating an Operation Plan Using EMCLI Commands](#)

### 6.2.1.1 Creating an Operation Plan Using Enterprise Manager Cloud Control Console

To create an operation plan using the Enterprise Manager Cloud Control Console, follow these tasks:

1. Log in 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

---



---

#### Note:

- For information about Oracle Site Guard operation types, see [Section 2.4, "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. Click **Save**.

### 6.2.1.2 Creating an Operation Plan Using EMCLI Commands

Run the following `emcli` commands in the command-line interface to create a new operation plan:

```
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"]
```

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

## 6.2.2 Creating New Operation Plans Using Existing Plans

You can create and configure new operation plans by cloning (copying) an existing plan. This applies to all types of plans.

To clone a plan using the Enterprise Manager Cloud Control Console, follow these steps:

1. Log in 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**.

## 6.2.3 Editing and Updating Operation Plans

You can perform the following tasks to update or edit an operation plan:

- 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.

You can modify the steps in an operation plan, and save the updated operation plan at any point in time.

To edit and update operation plans use one of the following methods:

- [Editing and Updating Operation Plans Using Enterprise Manager Cloud Control Console](#)
- [Editing and Updating Operation Plans Using EMCLI Command](#)

### 6.2.3.1 Editing and Updating Operation Plans Using Enterprise Manager Cloud Control Console

To edit and update an operation plan using the Enterprise Manager Cloud Control Console, follow these steps:

1. Log in 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. Click **Edit** to enable the options for updating and customizing the steps in the operation plan.
7. 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.

8. Click **Save** to update the plan.

### 6.2.3.2 Editing and Updating Operation Plans Using EMCLI Command

To edit or update the operation plan, run the following emcli commands in the command-line interface:

1. Get the list of configured operation plans by running the following command:

```
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"]
```

Parameter	Description
-name	Specify the name of the operation plan.
-operation	Specify the name of the operation. For example, switchover, failover, start, or stop.  This is an optional parameter. If you do not specify this parameter, then all the operation plans will be listed.
-system_name	Specify the name of system used in the operation plan. If you specify these values, then the values for -primary_system_name and -standby_system_name need not be specified.
-primary_system_name	Specify the name of primary system used in the operation plan. You can specify 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	Specify the name of the standby system used in the operation plan. You can specify 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.

2. Get the details of an operation plan that you want to update by running the following command:

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

Parameter	Description
-name	Specify the name of the operation plan.

3. Update the plan by running the following command:

```
emcli update_operation_plan
    -name="operation_plan_name"
    -step_number="step_number"
    -target_host="host_name"
```

```

-target_name="target_name"
[error_mode="error_mode"]
[enabled="true" or "false"]
[-execution_mode="Serial" or "Parallel"]
[-move="up" or "down"]
[-delete="true" or "false"]

```

Parameter	Description
-name	Specify the name of the operation plan.
-step_number	Specify the number of the step that should be updated.
-target_host	Specify the name of the system. Specifying this will update all the steps related to this target host.
-target_name	Specify the database target name.
-error_mode	The function of the operation. For example: stop or continue.
-enabled	Enter true or false.
-execution_mode	Specify the execution mode. For example: Serial or Parallel
-move	Change the order by specifying Up or Down.
-delete	Specify whether you want to delete steps. Specify true or false.

## 6.2.4 Deleting an Operation Plan

You can delete an operation plan using one of the following methods:

- [Deleting an Operation Plan Using Enterprise Manager Cloud Control Console](#)
- [Deleting an Operation Plan Using Command-Line Interface](#)

### 6.2.4.1 Deleting an Operation Plan Using Enterprise Manager Cloud Control Console

To delete an operation plan using the Enterprise Manager Cloud Control Console, follow these steps:

1. Log in 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.
7. Click **Yes** to confirm the action.

### 6.2.4.2 Deleting an Operation Plan Using Command-Line Interface

To delete an operation plan, run the following `emcli` command in the command-line interface:

```
emcli delete_operation_plan
      -name="name_of_the_operation_plan"
```

Parameter	Description
-name	Specify the name of the operation plan.

## 6.3 Running Prechecks

Oracle Site Guard runs the Precheck utility before performing any operation, by default. You can also run the Precheck utility separately, before executing any Oracle Site Guard operations. The Precheck utility in Oracle Site Guard for Fusion Middleware plug-in release (12.1.0.7) is enhanced to include Prechecks for database lags and the replication health of the ZFS appliance.

Oracle Site Guard performs the following Prechecks:

- 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.
- Asserts the existence of non-runtime, configured scripts (Pre Scripts/Post Scripts/Mount Scripts/Unmount Scripts/storage role reversal) on their respective target hosts.
- 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.

You can run the Precheck utility using one of the following methods:

- [Running Precheck Utility Using Enterprise Manager Cloud Control Console](#)
- [Running Precheck Utility Using Command-Line Interface](#)

### 6.3.1 Running Precheck Utility Using Enterprise Manager Cloud Control Console

To run a Precheck utility using the Enterprise Manager Cloud Control follow these steps:

1. Log in 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.
7. 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 more details about monitoring a procedure activity see [Section 6.6, "Monitoring Oracle Site Guard Operations"](#).

### 6.3.2 Running Precheck Utility Using Command-Line Interface

To run the Oracle Site Guard Precheck utility using EMCLI, run the following command:

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

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.

---

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

---

## 6.4 Scheduling Health Checks

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

- [Scheduling a Health Check Using Enterprise Manager Cloud Control Console](#)
- [Scheduling a Health Check Using EMCLI](#)

### 6.4.1 Scheduling a Health Check Using Enterprise Manager Cloud Control Console

To schedule Health Checks using the Enterprise Manager Cloud Control follow these steps:

1. Log in to Enterprise Manager Cloud Control 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.
7. Configure the schedule for the health check.
8. 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 [Section 6.6, "Monitoring Oracle Site Guard Operations"](#).

## 6.4.2 Scheduling a Health Check Using EMCLI

To schedule a Health Check using EMCLI, run the following command in the command-line interface.

```
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;]
    [end_time:yyyy/MM/dd HH:mm;]
    [grace_period:xxx;]
  }
```

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



Parameter	Description
-schedule	<p>Specify the schedule for the health check. Enter the values for the following parameters:</p> <ul style="list-style-type: none"> <li>- start_time: Specify the time when health checks should begin.</li> <li>- tz: Specify the time-zone ID. This parameter is optional.</li> <li>- frequency: Specify the frequency of the health check (once/interval/weekly/monthly/yearly). This parameter is optional.</li> </ul> <p>If the frequency is set to interval, then you must specify the values for the parameter repeat.</p> <p>If the frequency is set to weekly or monthly, then you must specify the weekdays.</p> <p>If the frequency is set to yearly, both days and months must be specified.</p> <ul style="list-style-type: none"> <li>- repeat: Specify the frequency with which health checks have to be repeated. These values are required only if the frequency is set to interval.</li> <li>- days: Specify the list of days, separated by commas. These values are required only if the frequency is weekly, monthly, or yearly.</li> </ul> <p>If frequency is set to weekly, then the valid range is 1 to 7.</p> <p>If the frequency is set to monthly or yearly, then valid range is 1 to 30.</p> <ul style="list-style-type: none"> <li>- months: Specify the list of months, separated by commas. These values are required only if the frequency is yearly (valid range 1 to 12).</li> <li>- end_time: Specify the end time for execution of health checks. This parameter is optional.</li> <li>- grace_period: Specify the grace period in minutes. This parameter is optional.</li> </ul> <p>For example:</p> <p>Examples:</p> <pre> 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 </pre>

## 6.5 Executing Oracle Site Guard Operation Plans

Use one of the following methods to start a site:

- [Executing Oracle Site Guard Operation Plan Using Enterprise Manager Cloud Control Console](#)
- [Executing Oracle Site Guard Operation Plan Using EMCLI Command](#)

## 6.5.1 Executing Oracle Site Guard Operation Plan Using Enterprise Manager Cloud Control Console

To execute an operation plan using Enterprise Manager Cloud Control console, complete the following tasks:

1. Log in 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.
7. Select **Run Prechecks** check box to run Prechecks before executing the operation plan.
8. 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 [Section 6.6, "Monitoring Oracle Site Guard Operations"](#).

## 6.5.2 Executing Oracle Site Guard Operation Plan Using EMCLI Command

To execute an operation plan, run the following EMCLI command in the command-line interface:

```
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"]
```

Parameter	Description
-name	Specify the name of the operation plan.
-run_prechecks	Specify 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	Specify whether to stop targets on primary site during a Failover operation. Set value true or false.

Parameter	Description
-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.

## 6.6 Monitoring Oracle Site Guard Operations

You can monitor an operation activity using one of the following methods:

- [Monitoring an Operation Plan Using Enterprise Manager Cloud Control Console](#)
- [Monitoring an Operation Plan Using EMCLI](#)

### 6.6.1 Monitoring an Operation Plan Using Enterprise Manager Cloud Control Console

This section contains the following topics:

- [Viewing an Operation Activity](#)
- [Suspending, Resuming, or Stopping an Operation](#)

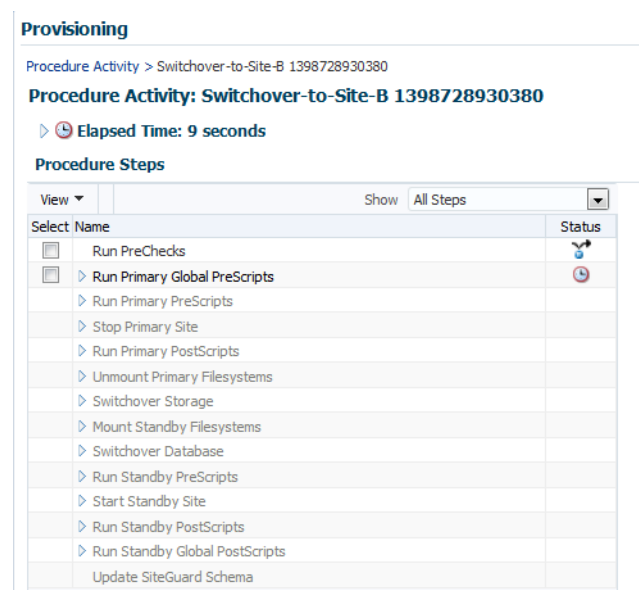
#### 6.6.1.1 Viewing an Operation Activity

To monitor an operation activity submitted for execution, complete the following steps:

1. Log in 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 activity of operation you want to monitor.

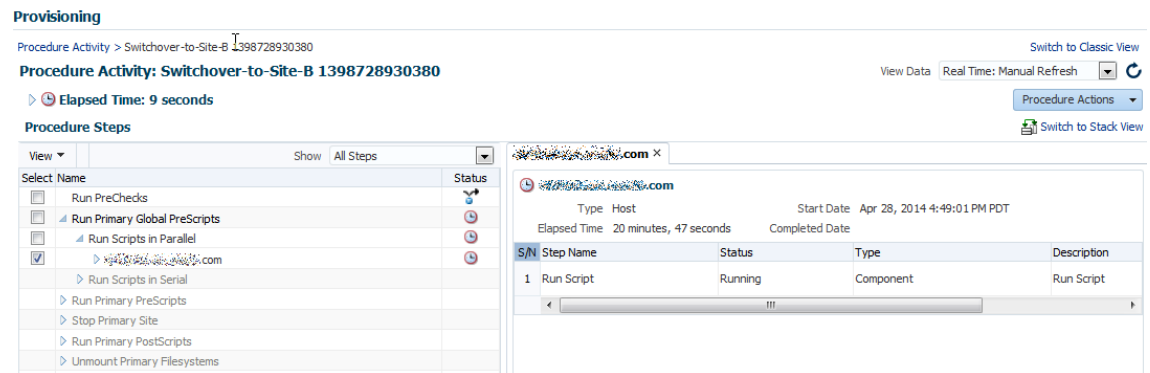
The Procedure Activity page for that operation is displayed. See [Figure 6–2](#).

**Figure 6–2 Viewing an Operation Activity in the Enterprise Manager Cloud Control Console**



- 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 6–3](#).

**Figure 6–3 Viewing the Hierarchical Steps of an Operation Activity in the Enterprise Manager Cloud Control Console**



### 6.6.1.2 Suspending, Resuming, or Stopping an Operation

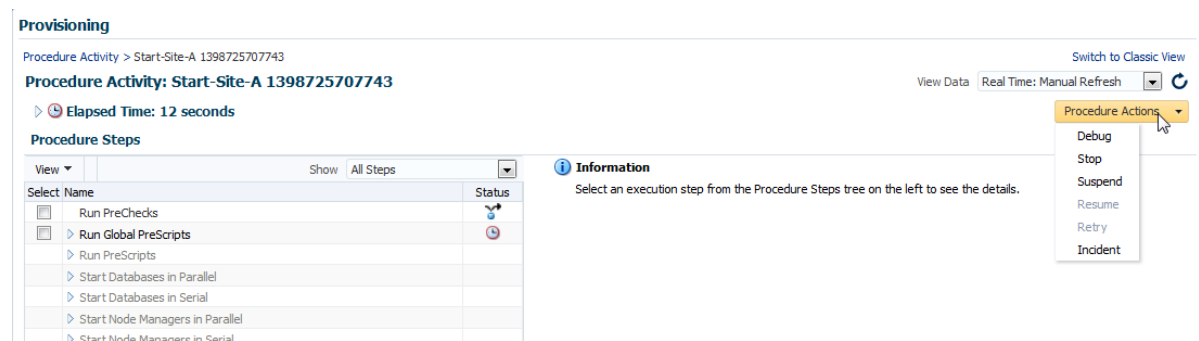
Operations in progress can be suspended and resumed later. You can also stop the operations that you do not want to resume. Follow these steps:

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

The Procedure Activity page for that operation is displayed.

- Click Procedure Actions located on the right-hand side of the page.
- Click an action from the drop-down menu. See [Figure 6–4](#).

**Figure 6–4 Suspending, Resuming, or Stopping an Operation**



## 6.6.2 Monitoring an Operation Plan Using EMCLI

To monitor the status of an operation plan using EMCLI, complete the following steps in the command-line interface:

- Get a list of procedures by running the following command:

```
emcli get_instances
```

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

Parameter	Description
-type	Specify the procedure type. This parameter is optional.
-format	Specify the output format of the list of instances. Enter <code>pretty</code> , <code>script</code> , or <code>csv</code> . This parameter is optional and the default value is <code>pretty</code> .
-script	Specify whether the output format is script or not. This parameter is optional.
-noheader	Do not display column headers. This parameter is optional.

- Note down the GUID for the operation in the list of operations displayed by the `emcli get_instances` command.
- Get the status of the operation using the following command:

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

## 6.7 Managing Execution Errors

Oracle Site Guard uses the Enterprise Manager Cloud Control deployment procedures framework to orchestrate disaster-recovery operations on remote hosts. The framework provides error management support through error modes.

Errors encountered during 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 while executing that step.

To retry that step and continue the operation, complete the following steps:

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

The Procedure Activity page for that operation is displayed.

- 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 6-5](#).

**Figure 6–5 Status Details**

The screenshot shows the 'Provisioning' section of the Oracle Site Guard Administrator's Guide. It displays a procedure activity for 'Start-Site-A 1398725707743'. The elapsed time is 27 seconds. The procedure steps are listed on the left, and the 'Run Script' step is selected. The detailed view of the 'Run Script' step shows its status as 'Failed - Job Failed'. The detailed view includes the step name, start and completed dates, targets, and a description of the step's purpose.

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 using the steps provided in this section. To change an error mode of a step, edit the operation as instructed in [Section 6.2.3, "Editing and Updating Operation Plans"](#).
- For more information about how to diagnose execution errors, see [Chapter 5, "Troubleshooting Oracle Site Guard."](#)

## 6.8 Manually Reversing Site Roles

While using Oracle Site Guard to test disaster recovery work flows or isolated parts of work flows, you might encounter a situation where you need to manually reconfigure site roles, and explicitly designate a site as the primary site. 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 one of the following methods:

- [Manually Reversing Site Roles Using Enterprise Manager Cloud Control Console](#)
- [Manually Reversing Site Roles Using EMCLI](#)

## 6.8.1 Manually Reversing Site Roles Using Enterprise Manager Cloud Control Console

To manually reconfigure site roles using Enterprise Manager Cloud Control Console, complete the following steps:

1. Log in 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**.

## 6.8.2 Manually Reversing Site Roles Using EMCLI

To manually reverse the roles of the primary and standby sites, run the following EMCLI commands in the command-line interface:

---

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

---

```
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"]
```

Parameter	Description
-primary_system_name	Enter the name of the system that is the current primary site and needs to be designated as the new standby site.
-standby_system_name	Enter the name of the system that is the current standby site and needs to be designated as the new primary site.
-reverse_role	Specify this option to reverse site roles.





---

## Oracle Site Guard Command-Line Interface

Oracle Site Guard uses the Enterprise Manager Command Line Interface (EMCLI) to manage Oracle Site Guard configuration directly from the command line, or from batch programs or scripts. This chapter lists all of the EM CLI verbs used for configuring Oracle Site Guard:

---

**Note:** EMCLI commands are case-sensitive. Ensure that you use the correct EMCLI verb, and enter the correct input.

---

- `add_siteguard_aux_hosts`
- `add_siteguard_script_credential_params`
- `add_siteguard_script_hosts`
- `configure_siteguard_lag`
- `create_operation_plan`
- `create_siteguard_configuration`
- `create_siteguard_credential_association`
- `create_siteguard_script`
- `delete_operation_plan`
- `delete_siteguard_aux_host`
- `delete_siteguard_configuration`
- `delete_siteguard_credential_association`
- `delete_siteguard_lag`
- `delete_siteguard_script`
- `delete_siteguard_script_credential_params`
- `delete_siteguard_script_hosts`
- `get_operation_plan_details`
- `get_operation_plans`
- `get_siteguard_aux_hosts`
- `get_siteguard_configuration`
- `get_siteguard_credential_association`
- `get_siteguard_health_checks`

- [get\\_siteguard\\_lag](#)
- [get\\_siteguard\\_script\\_credential\\_params](#)
- [get\\_siteguard\\_script\\_hosts](#)
- [get\\_siteguard\\_scripts](#)
- [get\\_siteguard\\_supported\\_targets](#)
- [run\\_prechecks](#)
- [schedule\\_siteguard\\_health\\_checks](#)
- [stop\\_siteguard\\_health\\_checks](#)
- [submit\\_operation\\_plan](#)
- [update\\_operation\\_plan](#)
- [update\\_siteguard\\_configuration](#)
- [update\\_siteguard\\_credential\\_association](#)
- [update\\_siteguard\\_lag](#)
- [update\\_siteguard\\_script](#)

**Note:**

- [] indicates that the parameter is optional.
- For more information about EMCLI, see *Oracle Enterprise Manager Command Line Interface*.

## 7.1 add\_siteguard\_aux\_hosts

Associates new auxiliary hosts with a Site Guard system.

An auxiliary host can be any host that is not part of the system but is managed by Enterprise Manager Cloud Control. These hosts can be used to execute any script. Any other targets running on this host will not be part of Site Guard operation plan(s).

**Format**

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

---

---

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

---

---

Parameter	Description
-system_name	Specify the system on which you are performing the operation.
-host_name	One or more names of the host. This host must be managed by Enterprise Manager Cloud Control.

**Example 7–1 Adding Auxiliary Hosts**

```
emcli add_siteguard_aux_hosts
    -system_name="austin-system"
```

```

-host_name="host1.domain.com"

emcli add_siteguard_aux_hosts
-system_name="austin-system"
-host_name="host2.domain.com"
-host_name="host3.domain.com"

```

**See:** ["delete\\_siteguard\\_aux\\_host"](#) and ["get\\_siteguard\\_aux\\_hosts"](#).

## 7.2 add\_siteguard\_script\_credential\_params

Adds a named credential as a parameter for an Oracle Site Guard script. Values of user name and password of this credential can be accessed within the script.

### Format

```

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 or conditionally optional.

---

Parameter	Description
-script_id	Specify the script ID.
-credential_name	Specify the name of the credential.
-credential_owner	Specify 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.

### Example 7-2 Adding Site Guard Script Credential Parameters

```

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:** [delete\\_siteguard\\_script\\_credential\\_params](#) and [get\\_siteguard\\_script\\_credential\\_params](#).

## 7.3 add\_siteguard\_script\_hosts

Adds a host to the Oracle Site Guard configuration scripts. You can add more than one host.

### Format

```

emcli add_siteguard_script_hosts
-script_id="script_id"
-host_name="host_name"

```

---

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

---

Parameter	Description
-script_id	Specify the identification associated with the script.
-host_name	Specify the host that you want to associate with the script. You can specify more than one host name.

**Example 7–3 Adding Hosts**

```
emcli add_siteguard_script_hosts
    -script_id="10"
    -host_name ="host1.domain.com"
```

**See:** "create\_siteguard\_script" and "get\_siteguard\_script\_hosts".

## 7.4 configure\_siteguard\_lag

Configures limit for Apply Lag and Transport Lag for all or selected databases of the system.

**Format**

```
emcli configure_siteguard_lag
    -system_name="system_name"
    [-target_name="database_target_name"]
    -property_name="ApplyLag" or "TransportLag"
    -value="maximum_lag_limit_in_seconds"
```

---

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

---

Parameter	Description
-system_name	Specify the system on which you want to configure the threshold limit.
-target_name	Specify 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	Specify the property name. Valid values are ApplyLag and TransportLag.
-value	Specify the threshold value to be configured (in seconds).

**Example 7–4 Configuring Values of Apply Lag and Transport Lag**

```
emcli configure_siteguard_lag
    -system_name="example-system"
    -property_name="ApplyLag"
    -value="1000"

emcli configure_siteguard_lag
    -system_name="example-system"
```

```
-target_name="OID_db"
-property_name="TransportLag"
-value="2500"
```

**See:** "get\_siteguard\_lag", "update\_siteguard\_lag" and "delete\_siteguard\_lag".

## 7.5 create\_operation\_plan

Creates an operational plan for Oracle Site Guard operations.

### Format

```
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 or conditionally optional.

---

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

### Example 7-5 Creating Operation Plan

```
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:** ["get\\_operation\\_plans"](#) and ["submit\\_operation\\_plan"](#).

## 7.6 create\_siteguard\_configuration

Creates a site configuration for Oracle Site Guard.

### 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	Specify the name of the system that is associated with the primary site.
-standby_system_name	Specify the name of the system that is associated with the standby system. You can specify more than one option and one system name.

### Example 7–6 Creating Site Guard Configuration

```
emcli create_siteguard_configuration
  -primary_system_name="example1"

emcli create_siteguard_configuration
  -primary_system_name="example1"
  -standby_system_name="example2"
```

**See:** ["update\\_siteguard\\_configuration"](#) and ["delete\\_siteguard\\_configuration"](#).

## 7.7 create\_siteguard\_credential\_association

Associates the credentials with the targets in a site.

### Format

```
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 or conditionally optional.

---

Parameter	Description
-system_name	Specify the name of the system.
-target_name	Specify the name of the target. This parameter is optional.
-credential_type	Specify the type of the credential. Example: HostNormal, HostPrivileged, NodeManager, WLSAdmin, or DatabaseSysdba.  <b>Note:</b> For Node Manager credential, specify the NodeManager credential_type, and specify the values for target_name, but use HostNormal credential for credential_name.
-credential_name	Specify the name of the credential.  If credential_name is not specified, then use_preferred_credential has to be set to true.
-credential_owner	Specify the owner of the credential.
-use_preferred_credential	If you are using Preferred Credentials, then specify true. The default value is false. If you use the default value, then you must specify the -credential_name parameter to use named credentials.

#### **Example 7-7 Creating Site Guard Credential Association**

```
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="austin-system"
    -credential_type="HostPrivileged"
    -use_preferred_credential="true"
    -credential_owner="sysman"

emcli create_siteguard_credential_association
    -system_name="austin-system"
    -credential_type="HostNormal"
    -credential_owner="sysman"

emcli create_siteguard_credential_association
    -system_name="austin-system"
    -target_name="austin-database-instance"
    -credential_type="DatabaseSysdba"
    -credential_name="HOST-DBCRED"
    -credential_owner="sysman"
```

**See:** ["delete\\_siteguard\\_credential\\_association"](#) and ["update\\_siteguard\\_credential\\_association"](#).

## 7.8 create\_siteguard\_script

Create scripts (Pre Script, Post Script and storage script) for the Oracle Site Guard configuration.

### Format

```
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"]
    [-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 or conditionally optional.

---

Parameter	Description
-system_name	Specify the name of the system.
-operation	Specify the name of the operation. Name of the operation: Switchover, Failover, Start, or Stop.
-script_type	Specify 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.
-host_name	Specify the name of the host where this script will be executed.  This parameter is optional and can be specified more than once.
-path	Specify the path to the script.
-component	Specify 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.



Parameter	Description
-runtime_script	<p>Specify 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.</p> <p>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.</p> <p>This parameter is optional.</p>
-run_on	<p>Specify whether the script needs to be executed on only one of the available hosts (enter any) or on all hosts (enter all).</p> <p>This parameter is optional and default value is all.</p>
-all_hosts	<p>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.</p>
-role	<p>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.</p>
-credential_type	<p>Specify HostNormal or HostPrivileged if you have root privileges.</p>
-credential_name	<p>Specify the name of the credential that is used to execute this script.</p> <p>If the value for the parameter credential_name is not specified, then the value for the parameter credential_type needs to be specified.</p>
-target_storage_credential_name	<p>Specify the named credential for target storage. If target_storage_credential_name is specified then source_storage_credential_name and credential_owner must be specified.</p>
-source_storage_credential_name	<p>Specify the named credential for source storage. If source_storage_credential_name is specified then target_storage_credential_name and credential_owner must be specified.</p>
-credential_owner	<p>Specify 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.</p>

### Example 7-8 Creating Site Guard Script

```
emcli create_siteguard_script
    -system_name="austin-system"
    -operation="Switchover"
    -script_type="Precheck-Script"
    -role="Primary"
    -credential_type="HostNormal"
    -path="/tmp/precheckscript"
    -all_hosts="true"

emcli create_siteguard_script
    -system_name="austin-system"
    -operation="Failover"
```

```
-script_type="Post-Script"
-role="Standby"
-credential_name="MY_NAMED_HOST_CREDENTIAL"
-path="/tmp/postscript"
-host_name="host1.domain.com"
-host_name="host2.domain.com"
-run_on="any"
-runtime_script="true"
```

```
emcli create_siteguard_script
-system_name="austin-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="austin-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:** ["update\\_siteguard\\_script"](#), ["delete\\_siteguard\\_script"](#), and ["get\\_siteguard\\_scripts"](#).

## 7.9 delete\_operation\_plan

Deletes the specified operation plan from an Oracle Site Guard configuration.

### Format

```
emcli delete_operation_plan
-name="name_of_operation_plan"
```

---

---

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

---

---

Parameter	Description
-name	Specify the name of the operation plan you want to delete.

### Example 7–9 Deleting an Operation Plan

```
emcli delete_operation_plan
-name="austin-switchover"
```

**See:** ["create\\_operation\\_plan"](#) and ["get\\_operation\\_plans"](#).

## 7.10 delete\_siteguard\_aux\_host

Delete any auxiliary host associated with the system.

### Format

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

---

---

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

---

---

Parameter	Description
-system_name	Specify the system on which you are performing the operation.
-host_name	The name of the host where the script will be run. This is an optional parameter. If it is not specified, then all auxiliary hosts associated with the system will be deleted.  <b>Note:</b> Ensure that the host name is part of the system specified in system_name.

### Example 7-10 Deleting Auxiliary Hosts

```
emcli delete_siteguard_aux_host
      -system_name="austin-system"

emcli delete_siteguard_aux_host
      -system_name="austin-system"
      -host_name="example-host1.domain.com"

emcli delete_siteguard_aux_host
      -system_name="austin-system"
      -host_name="example-host2.domain.com"
```

**See:** ["add\\_siteguard\\_aux\\_hosts"](#) and ["get\\_siteguard\\_aux\\_hosts"](#).

## 7.11 delete\_siteguard\_configuration

Deletes the Oracle Site Guard configuration. The entire configuration (scripts, credential associations, site associations, operation plans) pertaining to the specified system and all of the associated standby systems are deleted.

### Format

```
emcli delete_siteguard_configuration
      -primary_system_name="name_of_the_primary_system"
      -standby_system_name="name_of_the_standby_system"
      [-force="flag_specifying_whether_old_configurations_to_be_deleted"]
```

---

---

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

---

---

Parameter	Description
-primary_system_name	Specify the name of the primary system.
-standby_system_name	Specify the name of the standby system. This parameter is optional. However, if you do not specify this parameter, the Oracle Site Guard configuration of the specified primary system and all its standby system are deleted.
-force	Specify whether old configuration(s) need to be deleted. Enter either true or false. This parameter is optional.

#### **Example 7–11 Deleting Site Guard Configuration**

```
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:** ["create\\_siteguard\\_configuration"](#) and ["get\\_siteguard\\_configuration"](#).

## 7.12 delete\_siteguard\_credential\_association

Deletes the credential association from the Oracle Site Guard configuration.

### **Format**

```
emcli delete_siteguard_credential_association
    -system_name="name"
    [-target_name=["name"]]
    -credential_type="type"
```

---

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

---

Parameter	Description
-system_name	Specify the system on which the service resides.
-credential_type	Specify the credential type. It can be HostNormal, HostPrivileged, NodeManager, WLSAdmin, or DatabaseSysdba.
-target_name	Specify the name of the target. This parameter is optional.

#### **Example 7–12 Deleting Site Guard Credential Association**

```
emcli delete_siteguard_credential_association
    -system_name="austin-system"
    -credential_type="HostNormal"

emcli delete_siteguard_credential_association
    -system_name="austin-system"
```

```
-target_name="austin-database-instance"
-credential_type="DatabaseSysdba"
```

**See:** "create\_siteguard\_credential\_association", "update\_siteguard\_credential\_association", and "get\_siteguard\_credential\_association".

## 7.13 delete\_siteguard\_lag

Deletes values of Apply Lag and Transport Lag threshold configured for one or more Data Guard enabled databases of the system.

### Format

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

---

---

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

---

---

Parameter	Description
-system_name	Specify the system for which you want to configure the threshold limit.
-target_name	Specify 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. This parameter is optional.
-property_name	Specify the property name. Valid values are ApplyLag and TransportLag.

### Example 7–13 Deleting Values of Apply Lag and Transport Lag

```
emcli delete_siteguard_lag
    -system_name="austin-system"
    -property_name="ApplyLag"

emcli delete_siteguard_lag
    -system_name="austin-system"
    -target_name="OID_db"
    -property_name="TransportLag"
```

**See:** "update\_siteguard\_lag", "configure\_siteguard\_lag", and "get\_siteguard\_lag".

## 7.14 delete\_siteguard\_script

Deletes the specified script from the Oracle Site Guard configuration.

### Format

```
emcli delete_siteguard_script
    -script_id="script id"
```

---

---

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

---

---

Parameter	Description
-script_id	Specify the ID associated with the script.

**Example 7-14 Deleting Site Guard Script**

```
emcli delete_siteguard_script
-script_id="10"
```

**See:** "create\_siteguard\_script", "get\_siteguard\_scripts", and "update\_siteguard\_script".

## 7.15 delete\_siteguard\_script\_credential\_params

Deletes a named credential that is a parameter to a Oracle Site Guard script. Values of the user name and password of this credential can be accessed within the 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	Specify the ID associated with the script.
-credential_name	Specify 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	Specify 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.

**Example 7-15 Deleting Site Guard Script Credential Parameters**

```
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:** ["add\\_siteguard\\_script\\_credential\\_params"](#) and ["get\\_siteguard\\_script\\_credential\\_params"](#).

## 7.16 delete\_siteguard\_script\_hosts

Deletes the host or hosts associated with a given script.

### Format

```
emcli delete_siteguard_script_hosts
    -script_id="script_id"
    -host_name="host_name"
```

---

---

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

---

---

Parameter	Description
-script_id	Specify the ID associated with the script.
-host_name	Specify the name of the host where this script will be executed.  This parameter can be specified more than once.

### Example 7–16 Deleting Site Guard Script Hosts

```
emcli delete_siteguard_script_hosts
    -script_id="10"
    -host_name="example-host.domain.com"
```

### Output Columns

Step Number, Operation name, Target Name, Target Host, Error Mode

**See:** ["create\\_siteguard\\_script"](#) and ["add\\_siteguard\\_script\\_hosts"](#).

## 7.17 get\_operation\_plan\_details

Provides the detailed step-by-step information about the specified operation plan.

### Format

```
emcli get_operation_plan_details
    -name="plan_name"
```

---

---

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

---

---

Parameter	Description
-name	Specify the name of the operation plan.

**Example 7–17 Obtaining Operation Plan Details**

```
emcli get_operation_plan_details
      -name="austin-switchover"
```

**See:** ["create\\_operation\\_plan"](#) and ["get\\_operation\\_plans"](#).

## 7.18 get\_operation\_plans

Lists all configured operation plans.

**Format**

```
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 or conditionally optional.

---

---

Parameter	Description
-name	Specify the name of the operation plan.
-operation	Specify the name of the operation. For example, switchover, failover, start, or stop.  This is an optional parameter. If you do not specify this parameter, then all the operation plans will be listed.
-system_name	Specify the name of system used in the operation plan. If you specify these values, then the values for -primary_system_name and -standby_system_name need not be specified.
-primary_system_name	Specify the name of primary system used in the operation plan. You can specify 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	Specify the name of the standby system used in the operation plan. You can specify 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.

**Example 7–18 Obtaining Operation Plans**

```
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"

```

### Output Columns

Plan name, Operation name, Primary System Name, Standby System Name, Created On

**See:** ["create\\_operation\\_plan"](#) and ["submit\\_operation\\_plan"](#).

## 7.19 get\_siteguard\_aux\_hosts

Get a list of all auxiliary hosts associated with the system.

### Format

```

emcli get_siteguard_aux_hosts
        -system_name="system_name"

```

---

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

---

Parameter	Description
-system_name	Specify the system on which you are performing the operation.

### Example 7–19 Listing Auxiliary Targets

```

emcli get_siteguard_supported_targets
        -system_name="example-system"

```

**See:** ["add\\_siteguard\\_aux\\_hosts"](#) and ["delete\\_siteguard\\_aux\\_host"](#).

## 7.20 get\_siteguard\_configuration

Provides the Oracle Site Guard configuration.

### Format

```

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 or conditionally optional.

---

Parameter	Description
-primary_system_name	Specify the name of the primary system.

Parameter	Description
-standby_system_name	Specify the name of the standby system.

### Output Columns

Primary System, Standby System(s)

#### **Example 7–20** Obtaining Site Guard Configuration

```
emcli get_siteguard_configuration
      -primary_system_name="austin-system"
      -standby_system_name="austin2-system"
```

**See:** ["create\\_siteguard\\_configuration"](#) and ["delete\\_siteguard\\_configuration"](#).

## 7.21 get\_siteguard\_credential\_association

Lists the credential associations configured for a system.

### 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	Specify the name of the system.
-target_name	Specify the name of the target. This parameter is optional.
-credential_type	Specify the type of the credential. It can be HostNormal, HostPrivileged, NodeManager, WLSAdmin, or DatabaseSysdba.  <b>Note:</b> For Node Manager credential type, specify the NodeManager as the credential_type, and specify the values of target_name, but use a HostNormal credential for the parameter credential_name.  This parameter is optional.

### Output Columns

Target Name, Credential Name, Credential Type

#### **Example 7–21** Obtaining Site Guard Credential Association

```
emcli get_siteguard_credential_association
      -system_name="austin-system"
      -credential_type="HostNormal"
```

```
emcli create_siteguard_credential_association
    -system_name="austin-system"
    -target_name="austin-database-instance"
    -credential_type="DatabaseSysdba"
```

**See:** ["create\\_siteguard\\_credential\\_association"](#) and ["update\\_siteguard\\_credential\\_association"](#).

## 7.22 get\_siteguard\_health\_checks

Displays schedule of health checks for an operation plan.

### Format

```
emcli get_siteguard_health_checks
    -operation_plan="name_of_the_operation_plan"
```

---

---

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

---

---

Parameter	Description
-operation_plan	Specify the name of the operation plan for which schedule of health checks has to be displayed.

### Example 7-22 Obtaining Site Guard Health Checks

```
emcli get_siteguard_health_checks
    -operation_plan="austin-switchover"
```

**See:** ["schedule\\_siteguard\\_health\\_checks"](#), ["stop\\_siteguard\\_health\\_checks"](#), and ["run\\_prechecks"](#).

## 7.23 get\_siteguard\_lag

Retrieves and shows configured limit for ApplyLag and TransportLag for all or selected databases of the system.

### Format

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

---

---

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

---

---

Parameter	Description
-system_name	Specify the name of the system.
-target_name	Specify the name of the database.
-property_name	Specify the name of the property. Valid values are ApplyLag and TransportLag.

**Example 7–23   Obtaining Site Guard Lag**

```
emcli get_siteguard_lag
      [-system_name="austin-system"]
      [-property_name="ApplyLag"]

emcli get_siteguard_lag
      [-system_name="austin-system"]
      [-target_name="OID_db"]
      [-property_name="TransportLag"]
```

**See:** ["update\\_siteguard\\_lag"](#), ["configure\\_siteguard\\_lag"](#), and ["delete\\_siteguard\\_lag"](#).

**7.24 get\_siteguard\_script\_credential\_params**

Provides all the credential parameters for a Site Guard 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	Specify the ID associated with the script.
-credential_name	Specify 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	Specify 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.

**Example 7–24   Getting Oracle Site Guard Script Credential Parameters**

```
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:** [add\\_siteguard\\_script\\_credential\\_params](#) and [delete\\_siteguard\\_script\\_credential\\_params](#).

## 7.25 get\_siteguard\_script\_hosts

Lists the hosts associated with any script where the script is designated to run.

### Format

```
emcli get_siteguard_script_hosts
      -script_id="script_id"
```

---

---

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

---

---

Parameter	Description
-script_id	Specify the ID associated with the script.

### Output Columns

Host Name

### Example 7-25 Obtaining Site Guard Script Hosts

```
emcli get_siteguard_script_hosts
      -script_id="10"
```

**See:** "create\_siteguard\_script" and "add\_siteguard\_script\_hosts".

## 7.26 get\_siteguard\_scripts

Obtains the Oracle Site Guard scripts associated with the specified system.

### 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	Specify the name of the system.
-operation	Specify the name of the operation. For example, switchover, failover, start, or stop.
-script_type	Specify the type of the script. For example: mount, unmount, pre-script, post-script, global pre-script, global post-script, storage-failover, or storage-switchover.

Parameter	Description
-role	Optional parameter to filter the scripts based on the role associated with the system. For example: Primary or Standby.

### Output Columns

Script ID, Type, Operation, Path, Role

#### **Example 7–26** *Obtaining Site Guard Scripts*

```
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:** ["create\\_siteguard\\_script"](#), ["delete\\_siteguard\\_script"](#), and ["update\\_siteguard\\_script"](#).

## 7.27 get\_siteguard\_supported\_targets

Get the list of all Oracle Site Guard supported targets of the 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	Specify the name of the system.
-target_type	Specify the type of the target. This is an optional parameter.

#### **Example 7–27**

```
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"
```

**See:** ["create\\_siteguard\\_script"](#), ["delete\\_siteguard\\_script"](#), and ["update\\_siteguard\\_script"](#).

## 7.28 run\_prechecks

Run the Oracle Site Guard Prechecks for any given operation plan.

### Format

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

---

---

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

---

---

Parameter	Description
-operation_plan	Specify the name of the operation plan.
-database_lag_checks	Run database lag checks as part of Prechecks for all Data Guard configured databases. Enter value true or false.
	This parameter is optional.

### Example 7-28 Running Prechecks

```
emcli run_prechecks
      -operation_plan="austin-switchover"

emcli run_prechecks
      -operation_plan="austin-switchover"
      -database_lag_checks="false"
```

**See:** ["create\\_operation\\_plan"](#), ["get\\_operation\\_plans"](#), and ["submit\\_operation\\_plan"](#).

## 7.29 schedule\_siteguard\_health\_checks

Schedules health checks for an operation plan.

### Format

```
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;]
        [end_time:yyyy/MM/dd HH:mm;]
        [grace_period:xxx;]
      }
      [-notify="flag_specifying_whether_email_notifications_to_be_sent"]
      [-email="email_address_to_be_notified"]
```

---

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

---

Parameter	Description
-operation_plan	Specify the name of the operation plan for which health checks have to be scheduled.
-schedule	<p>Specify schedules at which health checks have to be scheduled.</p> <p>start_time - Specify the time when health checks have to start executing.</p> <p>tz - Specify the time-zone ID (optional).</p> <p>frequency - Valid values are once/interval/weekly/monthly/yearly (optional)</p> <p>If frequency is set to interval, then repeat has to be specified.</p> <p>If frequency is set to weekly or monthly, days has to be specified.</p> <p>If frequency is set to yearly, both days and months have to be specified.</p> <p>repeat - Specify the frequency with which health checks have to be repeated. This is mandatory only if frequency is set to interval.</p> <p>days - Specify the list of days separated by commas. This is required only if frequency is weekly, monthly, or yearly).</p> <p>If frequency is weekly, then valid range is 1 to 7.</p> <p>If frequency is monthly or yearly, then valid range is 1 to 30.</p> <p>months - Specify the list of months separated by commas. This is required only if frequency is yearly. Valid range is 1 to 12.</p> <p>end_time - Specify the end time for health check executions (optional).</p> <p>If not specified, health checks will run indefinitely.</p> <p>grace_period - Specify the grace period in minutes (optional).</p> <p>If the value are set to false, Prechecks will not be executed.</p>
-database_lag_checks	<p>Run database lag checks as part of Prechecks for all Data Guard configured databases. This parameter is optional.</p> <p>The default value is true.</p>
-notify	<p>Specify whether you want to be notified about the health-check report.</p> <p>If set to true, health check execution report are sent to the specified email address.</p> <p>This parameter is optional.</p>



Parameter	Description
-email	Specify 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.
	This parameter is optional.

#### Example 7–29 Scheduling Oracle Site Guard Health Checks

```
emcli schedule_siteguard_health_checks
    -operation_plan="austin-switchover"
    -schedule="start_time:2014/06/10 15:45"

emcli schedule_siteguard_health_checks
    -operation_plan="austin-switchover"
    -schedule="start_time:2014/10/29 2:00;frequency:interval;repeat:1d"

emcli schedule_siteguard_health_checks
    -operation_plan="austin-failover"
    -schedule="start_time:2014/08/10 01:00;frequency:interval;repeat:1w"

emcli schedule_siteguard_health_checks
    -operation_plan="austin-failover"
    -schedule="start_time:2014/08/10
                1:00;frequency:weekly;days:6,7;grace
period:60;tz:America/New_York"
```

**See:** ["get\\_siteguard\\_health\\_checks"](#), ["stop\\_siteguard\\_health\\_checks"](#), and ["run\\_prechecks"](#).

## 7.30 stop\_siteguard\_health\_checks

Stops all future health check executions of an operation plan.

### Format

```
emcli stop_siteguard_health_checks
    -operation_plan="name_of_the_operation_plan"
```

---

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

---

Parameter	Description
-operation_plan	Specify the name of the operation plan for which health check executions has to be stopped.

#### Example 7–30 Stopping Oracle Site Guard Health Checks

```
emcli stop_siteguard_health_checks
    -operation_plan="austin-switchover"
```

**See:** ["schedule\\_siteguard\\_health\\_checks"](#), ["get\\_siteguard\\_health\\_checks"](#), and ["run\\_prechecks"](#).

## 7.31 submit\_operation\_plan

Submits the specified operation plan for execution.

### Format

```
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"]
```

---

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

---

Parameter	Description
-name	Specify the name of the operation plan.
-run_prechecks	Specify 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	Specify 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.

### Example 7-31 Submitting Operation Plan

```
emcli submit_operation_plan
    -name="example-switchover"
    -database_lag_checks="false"

emcli submit_operation_plan
    -name="example-switchover"
    -run_prechecks="false"
```

**See:** ["create\\_operation\\_plan"](#) and ["get\\_operation\\_plans"](#).

## 7.32 update\_operation\_plan

Updates the Error Mode and Run Mode for any step in the given operation plan.

### Format

```
emcli update_operation_plan
    -name="operation_plan_name"
    -step_number="step_number"
    -target_host="host_name"
    -target_name="target_name"
    [error_mode="error_mode"]
    [enabled="true" or "false"]
```

```
[-execution_mode="Serial" or "Parallel"]
[-move="up"or"down"]
[-delete="true" or "false"]
```

---

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

---

Parameter	Description
-name	Specify the name of the operation plan.
-step_number	Specify the number of the step that should be updated.
-target_host	Specify the name of the system. Specifying this will update all the steps related to this target host.
-target_name	Specify the database target name.
-error_mode	The function of the operation. For example: stop or continue.
-enabled	Enter true or false.
-execution_mode	Specify the execution mode. For example: Serial or Parallel
-move	Change the order by specifying Up or Down.
-delete	Specify whether you want to delete steps. Specify true or false.

#### **Example 7–32 Updating an Operation Plan**

```
emcli update_operation_plan
  -name="austin-switchover"
  -step_number="1"
  -error_mode="Continue"
  -enabled="true"
  -execution_mode="Serial"

emcli update_operation_plan
  -name="austin-switchover"
  -step_number="5"
  -move="Up"

emcli update_operation_plan
  -name="austin-switchover"
  -target_host="myhost.domain.com"
  -error_mode="Continue"
  -enabled="true"

emcli update_operation_plan
  -name="example-switchover"
  -target_name="/Farm1/MyDomain"
  -delete="true"
```

**See:** ["create\\_operation\\_plan"](#) and ["get\\_operation\\_plan\\_details"](#).

## 7.33 update\_siteguard\_configuration

Updates the Oracle Site Guard configuration to add additional standby systems. 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="flag_specifying_whether_system_roles_to_be_reversed"]
```

---

---

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

---

---

Parameter	Description
-primary_system_name	Specify the name of the primary system.
-standby_system_name	Specify the name of the standby system. This parameter can be specified more than once.
-reverse_role	Specify whether to reverse role of site from standby to primary. Enter true or false.  If this option is specified, only one standby system name can be submitted using parameter -standby_system_name. The default value is false.

**Example 7-33 Updating Site Guard Configuration**

```
emcli update_siteguard_configuration
  -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
```

**See:** ["create\\_siteguard\\_configuration"](#) and ["delete\\_siteguard\\_configuration"](#).

## 7.34 update\_siteguard\_credential\_association

Updates the credential association.

**Format**

```
emcli update_siteguard_credential_association
  -system_name="name_of_the_system"
  [-target_name="name_of_the_target"]
  -credential_type="type_of_the_credential"
  [-credential_name="name_of_the_credential"]
  [-use_preferred_credential="true_or_false"]
  -credential_owner="credential_owner"
```

---

---

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

---

---

Parameter	Description
-system_name	Specify the name of the system.
-target_name	Specify the name of the target. This parameter is optional.
-credential_type	Specify the type of the credential. It can be HostNormal, HostPrivileged, WLSAdmin, or DatabaseSysdba.
-credential_name	Specify the name of the credential.
-use_preferred_credential	If you are using Preferred Credentials, then specify true. The default value is false. If you specify the default value, then you must specify the -credential_name parameter to use named credentials.
-credential_owner	Specify the owner of the credential.

#### **Example 7-34 Updating Site Guard Credential Association**

```
emcli update_siteguard_credential_association
    -credential_type="HostNormal"
    -credential_name="HOST-SGCRED"
    -credential_owner="sysman"

emcli update_siteguard_credential_association
    -credential_type="HostPrivileged"
    -use_preferred_credential="true"
    -credential_owner="sysman"

emcli update_siteguard_credential_association
    -target_name="austin-database-instance"
    -credential_type="DatabaseSysdba"
    -credential_name="HOST-DBCRED"
    -credential_owner="sysman"
```

**See:** ["delete\\_siteguard\\_credential\\_association"](#) and ["create\\_siteguard\\_credential\\_association"](#).

## 7.35 update\_siteguard\_lag

Updates the values of Apply Lag and Transport Lag threshold for one or more Data Guard enabled databases of the system.

### **Format**

```
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 or conditionally optional.

---

Parameter	Description
-system_name	Specify the system for which you want to configure the threshold limit.
-target_name	Specify 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	Specify the property name. Valid values are ApplyLag and TransportLag.
-value	Specify the threshold value to be updated (in seconds).

#### **Example 7–35 Updating Values of Apply Lag and Transport Lag**

```
emcli update_siteguard_lag
      -system_name="example-system"
      -property_name="ApplyLag"
      -value="1000"
```

```
emcli update_siteguard_lag
      -system_name="example-system"
      -target_name="OID_db"
      -property_name="TransportLag"
      -value="2500"
```

**See:** ["get\\_siteguard\\_lag"](#), ["configure\\_siteguard\\_lag"](#), and ["delete\\_siteguard\\_lag"](#).

## 7.36 update\_siteguard\_script

Updates the path and the all\_hosts flag associated with any script.

### **Format**

```
emcli update_siteguard_script
      -script_id="ID_associated_with_the_script"
      -path="path_of_the_script"
      [-component="path of the entity in Software library"]
      -runtime_script="flag_to_specify_if_prechecks_to_check_availability_of_
the_script"
      -credential_type="type_of_credential"
      [-host_name="name_of_the_host_where_this_script_will_run"]
      [-run_on="flag_specifying_the_host"]
      [-all_hosts="true" or "false"]
      [-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 or conditionally optional.

---

Parameter	Description
-script_id	Specify the script ID.
-path	Specify the path to the script.

Parameter	Description
-component	Specify 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	Specify 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 the software library are designated as runtime scripts.  The default value for scripts that are not staged from the software library, is false.
-credential_type	Specify HostNormal or HostPrivileged if you have root privileges.
-credential_name	Specify 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.  This parameter is optional and can be specified more than once.
-run_on	Specify whether the script needs to be executed on only one of the available hosts (any) or on all hosts (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. For example: true or false.
-target_storage_credential_name	Specify named credential for target storage.  If target_storage_credential_name is specified then source_storage_credential_name and credential_owner must be specified.
-source_storage_credential_name	Specify named credential for source storage.  If source_storage_credential_name is specified then target_storage_credential_name and credential_owner must be specified.
-credential_owner	Specify owner of the credential.  If target_storage_credential_name and source_storage_credential_name are specified, then credential_owner must be specified.

### **Example 7-36 Updating Site Guard Script**

```
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
    -script_id="10"
    -host_name="host1.domain.com"
    -host_name="host2.domain.com"
    -run_on="any"

emcli update_siteguard_script
    -script_id="10"
    -all_hosts="false"
    -credential_name="MY_NAMED_HOST_CREDENTIAL"
    -host_name="host1.domain.com"

emcli update_siteguard_script
    -script_id="16"
    -path="/tmp/script"
    -credential_type="HostPrivileged"
    -runtime_script="true"

emcli update_siteguard_script
    -script_id="20"
    -path="/tmp/script"
    -all_hosts="true"
    -target_storage_credential_name="SGCRED-TARGET-STORAGE"
    -source_storage_credential_name="SGCRED-SOURCE-STORAGE"
    -credential_owner="sysman"
```

**See:** ["create\\_siteguard\\_script"](#), ["get\\_siteguard\\_scripts"](#), and ["delete\\_siteguard\\_script"](#).



---

# Upgrading or Downgrading Oracle Site Guard

This chapter contains information about how to upgrade or downgrade to a different version of Oracle Site Guard in an Enterprise Manager Cloud Control environment.

It contains the following topics:

- [Section 8.1, "Upgrading Oracle Site Guard"](#)
- [Section 8.2, "Downgrading Oracle Site Guard"](#)

## 8.1 Upgrading Oracle Site Guard

To upgrade from Oracle Site Guard (12.1.0.6) to Oracle Site Guard (12.1.0.7), complete the following steps:

1. Delete all of the existing Oracle Site Guard operation plans by following the steps listed in [Section 6.2.4, "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 [Chapter 4, "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 12.1.0.6 to 12.1.0.7). For information about Oracle Enterprise Manager plug-ins, see "Managing Plug-Ins" in *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

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 [Chapter 4, "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 [Section 6.2.1, "Creating Operation Plans"](#).

## 8.2 Downgrading Oracle Site Guard

To downgrade from Oracle Site Guard (12.1.0.7) to Oracle Site Guard (12.1.0.6), complete the following steps:

1. Delete all of the existing Oracle Site Guard operation plans by following the steps listed in [Section 6.2.4, "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 [Chapter 4, "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" in *Oracle Enterprise Manager Cloud Control Administrator's Guide*.
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 [Chapter 4, "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 [Section 6.2.1, "Creating Operation Plans"](#).

---

## Extracting Credentials Passed as Parameters (Examples)

Credentials that are passed as parameters to user-defined scripts, are available as an input stream. This chapter contains code samples of scripts. The Bash shell script, Perl script, and the Python scripting language used in the sample codes demonstrate how credential parameters can be extracted.

---

**Note:** The scripts in this chapter are samples only. You should change and adapt them to suit your environment. For example, the number of credentials passed from Oracle Site Guard to the script must exactly match the requirements of the script.

---

## extract\_credentials\_sample\_script.sh

---

```
#!/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

```
#!/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, myPassword = sgUtil.getCredential(1)
        print("[1] UserName : '"+ myUser + "', Password : '" + myPassword + "'")

        myUser, myPassword = sgUtil.getCredential(2)
        print("[2] UserName : '"+ myUser + "', Password : '" + myPassword + "'")

        myUser, myPassword = sgUtil.getCredential(3)
        print("[3] UserName : '"+ myUser + "', Password : '" + myPassword + "'")
```

```
myUser, myPassword = sgUtil.getCredential(4)
print("[4] UserName : '" + myUser + "', Password : '" + myPassword + "'")

"""
    Starting point...
"""
main()
```

## extract\_credentials\_sample\_script.pl

```
#!/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");
}
```

