Oracle® Advanced Services Gateway Security Guide

Part No: E40643-66
January 2026

ORACLE

Oracle Advanced Services Gateway Security Guide

Part No: E40643-66

Référence: E40643-66

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info ou le site http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs si vous êtes malentendant.

Contents

Oracle Advanced Services Gateway Security Guide 13
About the Gateway 13
General Requirements 13
Changes to the Security Guide Since the Last Release 14
Firewall Port Requirements 16
Downloading the Firewall Rules Document from My Oracle Support 17
External Connection 18
TLS VPN and the Gateway 18
Alternative External Connection Option 19
Controlling Remote Access 20
Customer Access to the Gateway 20
Internal Connection 20
Firewall Rules: Ports and Protocols 20
Firewall Rules for External Traffic 21
Firewall Rules for External Traffic Through the Encrypted VPN Tunnel 21
Firewall Rules for Internal Traffic 21
Firewall Rules Between the Gateway and the Customer Network 22
Firewall Rules for Gateway Hardware Self-Monitoring 22
Firewall Rules Between the Gateway and Exadata 23
Firewall Rules Between the Gateway and ZDLRA 23
Firewall Rules Between the Gateway and ZFS 23
Firewall Rules Between the Gateway and SuperCluster 24
Firewall Rules Between the Gateway and Exalytics 24
Firewall Rules Between the Gateway and Oracle Database Appliance 25
Firewall Rules Between the Gateway and Oracle Big Data Appliance 25
Firewall Rules Between the Gateway and Oracle Private Cloud Appliance 25
Firewall Rules Between the Gateway and Oracle Standalone Hosts 26
Firewall Rules Between the Gateway and Oracle Third-Party Hosts 26

Implementation Changes to a Customer System 26
The Monitoring Matrix 27
Implementation Impact on the Environment 28
All Systems With An Agent Deployed 29
Engineered Systems Storage Cells 31
Engineered System Cisco Switches 31
Engineered System InfiniBand Switches 31
Engineered System PDU's 32
Engineered Systems Compute Nodes (Physical Implementation) and Virtual Machines 32
OVS Compute Nodes 32
KVM Compute Nodes 33
ZFS Storage Array Storage Heads 35
Utilization Impact Risk of OEM Cloud Control Agent on Monitored Systems 35
Backout Plan 36
Server Prerequisites for Monitoring Deployment 37
Server Prerequisites for Monitoring Deployment 37
Monitoring Access: an Overview 37
User Privileges 38
Solaris 11 Initial Setup User RBAC Profile 40
Solaris 10 Initial Setup User RBAC Profile 42
Solaris sudo Profile 43
Linux sudo Profile 44
ILOM User Privileges 45
Storage Prerequisites for Monitoring Deployment 45
Monitoring Deployment: an Overview 46
Oracle ZFS Storage Appliances 46
Using the Gateway User Interface 47
Logging on to the Gateway User Interface in Interactive Mode 48
Using Remote Access Control in Interactive Mode 49
Using syslog Forwarding in Interactive Mode 50
Using System Proxy in Interactive Mode 51
Using the Gateway User Interface in Non-Interactive Mode 52
Using Remote Access in Non-Interactive Mode 52
Using System Proxy in Non-Interactive Mode 53
Using syslog Forwarding in Non-Interactive Mode 54
Audit Logging 56
Sample Logging Messages 57
Managing ASR Audit Logs 59
About ASR Audit Logs 59

Viewing ASR Audit Logs....59
Downloading ASR Audit Logs....60
Installing the Gateway....60
Gateway Infrastructure Maintenance and Change Management Process....61
Understanding Responsibilities....61
Customer Responsibilities....61
Oracle Responsibilities....62
Generating a Change Management Request....62
Understanding the Change Management Workflow....63
Understanding Maintenance Activities....63

Oracle Advanced Services Gateway Security Guide

This document outlines the requirements for deploying Oracle Advanced Services Gateway (hereafter referred to as "the Gateway") into the customer environment to support the delivery of certain Oracle remote services (hereafter referred to as Oracle Services.) The Gateway is an important part of the Oracle delivery architecture for Oracle Services and its placement must be carefully considered in order for Oracle to deliver Oracle Services. This document outlines network configuration options when integrating the Gateway device within the customer environment. To help explain these options, this document assumes a "simple" customer-side network topology. However, these options can extend to more complex network topologies.

About the Gateway

The Gateway is a multi-purpose platform designed to facilitate a number of Oracle Services including Oracle Platinum Services, Advanced Monitoring and Resolution, LifeCycle services, and Business Critical Service for Systems. The Gateway enables the simplification of network requirements and a single point of access for the provision and delivery of these services.

The Gateway platform is based on the Oracle Linux operating system and hosts a full set of Oracle software stacks, including Automated Service Request (ASR), Oracle Enterprise Manager 13*c*, patch management (such as YUM services), and a suite of Java applications. Together, these applications aggregate and route telemetry messages from the customer environment to the Oracle Support Services infrastructure. The Gateway provides remote access for Oracle engineers to access the customer network (with customer permission) and to carry out approved actions on customers' monitored systems.

General Requirements

There are a number of general requirements that are necessary for Oracle to deliver Oracle Services:

- A Gateway must be provisioned into the customer's environment.
- All monitored systems must be network accessible from the Gateway.
- The monitored systems must be dedicated to the customer. Oracle will not be able to deliver services for monitored systems which are not exclusively owned and controlled by the customer. Oracle recommends a dedicated, physical server. If you do not wish to purchase

the certified server from Oracle, you can use a server or Virtual Machine (VM) that meets your particular requirements. See "Installing the Gateway" on page 60.

- Oracle must have access to certain ports and protocols (described below) in order to implement and deliver Oracle Services.
- The Gateway must be continuously accessible from the Oracle Support Platform using the secure protocols described below. However, the Gateway must not be directly exposed to the Internet.
- To access the Gateway, your Web browser must be able to log in to http://www.oracle.com to enable access to the Gateway user interface using your Oracle Single Sign-on (SSO) authentication.
- Customers must not attempt to gain access to the Gateway using SSH. Customer access to the Gateway is restricted only to the approved web interface.
- Customers must not attempt to install other, third party, software onto the Gateway unless the software has been explicitly approved by Oracle. The Gateway should be viewed as an appliance that is installed into the customer network.
- Customers must not put a Transport Layer Security (TLS) break between the Gateway and the Internet.

In order to expedite the implementation process, the customer will be required to provide high level network topology which should include:

- IP numbering scheme
- Routing policy
- Locations of firewalls
- Locations of monitored systems
- Proposed location of Gateway

Having this information enables Oracle to provide a recommendation regarding the Gateway placement.

Changes to the Security Guide Since the Last Release

This section outlines the principal changes made to *Oracle Advanced Services Gateway Security Guide* (this document) since the last release (E40643-65; December 2025).

- The following was added under Linux sudo Profile section:

  /sbin/service init.tfa start, \

Firewall Port Requirements

The specifics of the Oracle Services network requirement depends on the customer network topology relative to the Oracle Services Support centers, the Gateway, and the monitored systems. The customer networks must be configured to permit traffic flow as shown in the diagram below.

The firewall rules must be set up to allow traffic flow in two situations:

- Between the Gateway and Oracle Services Support centers. This is referred to as the *external connection.*

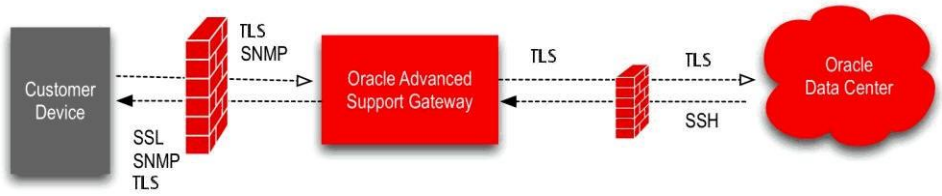
Note - A web proxy can be used to proxy the HTTPS traffic across the external connection. However, the Gateway does not support NTLM or Kerberos proxy authentication. Transport Layer Security (TLS) VPN traffic can be routed through an unauthenticated proxy server.

Caution - To defend against security attacks, you should never connect the Gateway interfaces or the Oracle ILOM Service Processor to a public network, such as the Internet. The Gateway should never be exposed directly to the Internet without the protection of a customer firewall or Access Control List (ACL.) You should keep the Oracle ILOM Service Processor management traffic on a separate management network and grant access only to system administrators. For further information, see the section on Securing the Physical Management Connection in the Oracle ILOM Security Guide.

- Between the Gateway and the customer's monitored devices, through a customer-controlled firewall or other security devices. This is referred to as the *internal connection*.

The diagram below depicts an example traffic flow between monitored systems and Oracle. (Detailed firewall rules and templates are provided to the customer during the implementation process.)

FIGURE 1 High Level Traffic Flow and Firewall Requirement



Downloading the Firewall Rules Document from My Oracle Support

Information about firewall rules is no longer published in *Oracle Advanced Services Gateway Security Guide* (this document). This information is now available in the form of a knowledge document on My Oracle Support (MOS) instead. To download this document, users are required to log on to MOS using their Oracle Account.

The firewall rules document from MOS provides essential information for customers on:

- All standard firewall port configurations necessary for the delivery of Oracle Services;
- All internal firewall rules for the customer network, Gateway hardware self-monitoring, Oracle Engineered Systems such as Exadata Database Machine (Exadata), SuperCluster, Exalytics In-Memory Machine (Exalytics) and so on, as well as standalone hosts (both Oracle and third-party).

All Gateways must implement:

- Firewall rules between the Gateway and the customer network. See "Firewall Rules Between the Gateway and the Customer Network" on page 22.
- Firewall rules for Gateway hardware self-monitoring. See "Firewall Rules for Gateway Hardware Self-Monitoring" on page 22.
- Firewall rules that apply for the systems to be monitored by the Gateway.

To download the document:

1. Click the following link: Firewall Rules for Oracle Advanced Support Gateway
2. Enter your Oracle Account details.
3. Download and save the PDF.

   Use the firewall rules information to configure traffic flow as outlined in "Firewall Port Requirements" on page 14.

External Connection

Oracle utilizes a combination of a VPN solution and to secure communications between the Gateway, located within the customer's environment, and the Oracle Services Support center locations. The VPN is primarily used for tasks such as facilitating patching requirements from Oracle Services Support center locations to the Gateway and TLS is used for transporting the monitoring telemetry from the Gateway to the Oracle Services Support center locations.

TLS VPN and the Gateway

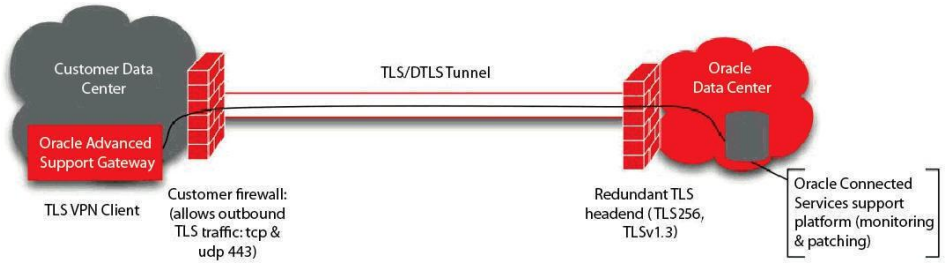
The Gateway is configured with a software TLS-based VPN client. When the Gateway boots up, it opens an outbound connection to one of three Oracle Services Support centers, establishing a TLS VPN tunnel. At that point, this connection is used for inbound connectivity between the Oracle Services Support center and the Gateway. No inbound firewall port openings are required, as the initial connection is outbound. The Gateway is assigned a unique ID and password and connects to one of three Oracle VPN concentrators. The TLS-based VPN has the following features:

- Connection based on TLS, AES256 symmetric encryption to ensure traffic integrity and confidentiality
- Continuous VPN connection availability through the use of active/passive VPN cluster

servers at the Oracle Services Support centers. Any hardware or software issues on the active VPN server failover all connections to the backup VPN.

- Disaster recovery processes that use multiple clusters around the world. Any connection issue with one of the Oracle Services Support centers failover client connections to the other Oracle Services Support centers.

FIGURE 2 A TLS-Based VPN Client Connection from the Gateway to Oracle



Note - The TLS VPN is the standard method for establishing the connection with Oracle. Alternative connection methods are available on an exception, customer-by-customer basis that is summarized in "Alternative External Connection Option" on page 17. If you wish to explore these options further, please contact your Oracle Implementation Manager.

Alternative External Connection Option

Oracle offers an alternate method for establishing a connection using IPSec. The connection is terminated on the customer's existing VPN hardware. This option generally requires an extended implementation cycle and is approved on an exception basis. If the customer chooses to use their existing VPN device (for example, firewall or VPN concentrator) as a termination point, the VPN overall requirements described above remain the same. The encryption domain requirements for this connection will create a more complex configuration.

The requirements include, but are not limited to:

- A public IP per Gateway connection supplied by the customer for use inside the VPN encryption domain;
- Access to one /26 subnet and multiple /32 addresses inside the encryption domain;
- Allowing the ports and protocols listed in the table specifying firewall rules between the Gateway and Oracle standalone hosts (see "Downloading the Firewall Rules Document from My Oracle Support" on page 15) to communicate across the VPN;
- Network Address Translation (NAT) can be used for the source address of the Gateway outbound to the Internet for external communication back to Oracle. For the Oracle Service endpoints to which the Gateway needs to communicate, NAT is not supported. These Oracle Service endpoints must reside on their public IP addresses.

Controlling Remote Access

Oracle security policies require a VPN between Oracle and the customer so that Oracle can access the customer systems. The Gateway enables the customer to control the firewall settings to determine whether Oracle can log on to the Gateway. The Remote Access icon (a green button) is displayed in the utility menu on the top-right of the Gateway user interface. You can set the duration of allowing remote access to a maximum of 200 minutes, toggle the icon to turn the remote access session on or off, or view a history of remote access control sessions. The default is to allow the connection indefinitely. Remote Access Control functionality is not available for all Oracle Connected Services. Please refer to your Oracle representative for further details.

The Remote Access feature is described in this document.

Customer Access to the Gateway

If Oracle Hardware is used to host the Advanced Services Gateway (Gateway), Oracle will retain and maintain root access for the out of band management processor on the Gateway. Customer access to the Lights Out Management (LOM) section of the server is only permitted for emergency power operations. To obtain this access, a customer must submit a service request (SR) to obtain the required credentials for a specific period of time.

Internal Connection

Placing the Gateway in a customer's DMZ that is not directly exposed to the Internet is the recommended internal connection option. By placing the Gateway in a DMZ behind an Internet firewall, the customer has control of traffic traversing their internal networks and also of inbound connections from the Internet.

Firewall Rules: Ports and Protocols

This section no longer provides information about the standard firewall port configurations necessary for the delivery of Oracle Services. Information about firewall rules is no longer published in *Oracle Advanced Services Gateway Security Guide* (this document).

This page is maintained only to redirect customer users to the new location of the information.

This information is now available in the form of a knowledge document on My Oracle Support (MOS) instead.

To download this document, please refer to "Downloading the Firewall Rules Document from My Oracle Support" 15.

Firewall Rules for External Traffic

This section no longer provides information about firewall rules for external traffic. Information about firewall rules is no longer published in *Oracle Advanced Services Gateway Security Guide* (this document).

This page is maintained only to redirect customer users to the new location of the information.

This information is now available in the form of a knowledge document on My Oracle Support (MOS) instead.

To download this document, please refer to "Downloading the Firewall Rules Document from My Oracle Support" on page 15.

Firewall Rules for External Traffic Through the Encrypted VPN Tunnel

This section no longer provides information about firewall rules for external traffic through the encrypted VPN tunnel. Information about firewall rules is no longer published in *Oracle Advanced Services Gateway Security Guide* (this document).

This page is maintained only to redirect customer users to the new location of the information.

This information is now available in the form of a knowledge document on My Oracle Support (MOS) instead.

To download this document, please refer to "Downloading the Firewall Rules Document from My Oracle Support" on page 15.

Firewall Rules for Internal Traffic

This section no longer provides information about firewall rules for internal traffic. Information about firewall rules is no longer published in *Oracle Advanced Services Gateway Security Guide* (this document).

This page is maintained only to redirect customer users to the new location of the information.

This information is now available in the form of a knowledge document on My Oracle Support (MOS) instead.

To download this document, please refer to "Downloading the Firewall Rules Document from My Oracle Support" on page 15.

Firewall Rules Between the Gateway and the Customer Network

This section no longer provides information about firewall rules between the Gateway and the customer network. Information about firewall rules is no longer published in *Oracle Advanced Services Gateway Security Guide* (this document).

This page is maintained only to redirect customer users to the new location of the information.

This information is now available in the form of a knowledge document on My Oracle Support (MOS) instead.

To download this document, please refer to "Downloading the Firewall Rules Document from My Oracle Support" on page 15.

Firewall Rules for Gateway Hardware Self-Monitoring

This section no longer provides information about firewall rules for Gateway hardware self-monitoring. Information about firewall rules is no longer published in *Oracle Advanced Services Gateway Security Guide* (this document).

This page is maintained only to redirect customer users to the new location of the information.

This information is now available in the form of a knowledge document on My Oracle Support (MOS) instead.

To download this document, please refer to "Downloading the Firewall Rules Document from My Oracle Support" on page 15.

Firewall Rules Between the Gateway and Exadata

This section no longer provides information about firewall rules. Information about firewall rules is no longer published in *Oracle Advanced Services Gateway Security Guide* (this document).

This page is maintained only to redirect customer users to the new location of the information.

This information is now available in the form of a knowledge document on My Oracle Support (MOS) instead.

To download this document, please refer to "Downloading the Firewall Rules Document from My Oracle Support" on page 15.

Firewall Rules Between the Gateway and ZDLRA

This section no longer provides information about firewall rules. Information about firewall rules is no longer published in *Oracle Advanced Services Gateway Security Guide* (this document).

This page is maintained only to redirect customer users to the new location of the information.

This information is now available in the form of a knowledge document on My Oracle Support (MOS) instead.

To download this document, please refer to "Downloading the Firewall Rules Document from My Oracle Support" on page 15.

Firewall Rules Between the Gateway and ZFS

This section no longer provides information about firewall rules. Information about firewall rules is no longer published in *Oracle Advanced Services Gateway Security Guide* (this document).

This page is maintained only to redirect customer users to the new location of the information.

This information is now available in the form of a knowledge document on My Oracle Support (MOS) instead.

To download this document, please refer to "Downloading the Firewall Rules Document from My Oracle Support" on page 15.

Firewall Rules Between the Gateway and SuperCluster

This section no longer provides information about firewall rules. Information about firewall rules is no longer published in *Oracle Advanced Services Gateway Security Guide* (this document).

This page is maintained only to redirect customer users to the new location of the information.

This information is now available in the form of a knowledge document on My Oracle Support (MOS) instead.

To download this document, please refer to "Downloading the Firewall Rules Document from My Oracle Support" on page 15.

Firewall Rules Between the Gateway and Exalytics

This section no longer provides information about firewall rules. Information about firewall rules is no longer published in *Oracle Advanced Services Gateway Security Guide* (this document).

This page is maintained only to redirect customer users to the new location of the information.

This information is now available in the form of a knowledge document on My Oracle Support (MOS) instead.

To download this document, please refer to "Downloading the Firewall Rules Document from My Oracle Support" on page 15.

Firewall Rules Between the Gateway and Oracle Database Appliance

This section no longer provides information about firewall rules. Information about firewall rules is no longer published in *Oracle Advanced Services Gateway Security Guide* (this document).

This page is maintained only to redirect customer users to the new location of the information.

This information is now available in the form of a knowledge document on My Oracle Support (MOS) instead.

To download this document, please refer to "Downloading the Firewall Rules Document from My Oracle Support" 15.

Firewall Rules Between the Gateway and Oracle Big Data Appliance

This section no longer provides information about firewall rules. Information about firewall rules is no longer published in *Oracle Advanced Services Gateway Security Guide* (this document).

This page is maintained only to redirect customer users to the new location of the information.

This information is now available in the form of a knowledge document on My Oracle Support (MOS) instead.

To download this document, please refer to "Downloading the Firewall Rules Document from My Oracle Support" on page 15.

Firewall Rules Between the Gateway and Oracle Private Cloud Appliance

This section no longer provides information about firewall rules. Information about firewall rules is no longer published in *Oracle Advanced Services Gateway Security Guide* (this document).

This page is maintained only to redirect customer users to the new location of the information.

This information is now available in the form of a knowledge document on My Oracle Support (MOS) instead.

To download this document, please refer to "Downloading the Firewall Rules Document from My Oracle Support" on page 15.

Firewall Rules Between the Gateway and Oracle Standalone Hosts

This section no longer provides information about firewall rules. Information about firewall rules is no longer published in *Oracle Advanced Services Gateway Security Guide* (this document).

This page is maintained only to redirect customer users to the new location of the information.

This information is now available in the form of a knowledge document on My Oracle Support (MOS) instead.

To download this document, please refer to "Downloading the Firewall Rules Document from My Oracle Support" on page 15.

Firewall Rules Between the Gateway and Oracle Third-Party Hosts

This section no longer provides information about firewall rules. Information about firewall rules is no longer published in *Oracle Advanced Services Gateway Security Guide* (this document).

This page is maintained only to redirect customer users to the new location of the information.

This information is now available in the form of a knowledge document on My Oracle Support (MOS) instead.

To download this document, please refer to "Downloading the Firewall Rules Document from My Oracle Support" on page 15.

Implementation Changes to a Customer System

This section outlines the changes made to a customer's system during the implementation of Oracle Gateway Enabled services, including Platinum Services, Business Critical Service for Systems, Lifecycle Support Services, and Advanced Monitoring and Resolution. The Gateway runs Oracle Enterprise Manager Cloud Control to perform its monitoring. Oracle Enterprise

Manager Cloud Control requires agents to be installed on hosts, and then uses various plug-ins to monitor those devices that cannot be monitored directly. This section describes the monitoring method for a device and the configuration to be performed.

Refer to the following sections:

- "The Monitoring Matrix" on page 27
- "Implementation Impact on the Environment" on page 28
- "Utilization Impact Risk of OEM Cloud Control Agent on Monitored Systems" on page 35

The Monitoring Matrix

This section provides a table of devices and shows how each device is monitored.

TABLE 1 Devices and their Associated Monitoring Methods

Device		Monitor			
	Component	**Cloud Control Agent**	**Plug-in Target Type**	**SNMP Trap**	**ASR**
Engineered System	Exadata Storage Cell	No	Oracle Exadata Storage Server	Yes	Yes
Engineered System	Cisco Switch	No	Systems Infrastructure Network Switch	Yes	Yes
Engineered System	InfiniBand Switch	No	Systems Infrastructure Network Switch	Yes	Yes
Engineered System	PDU	No	Systems Infrastructure PDU	Yes	No
Engineered System	OVS Compute Node	No	Systems Infrastructure Server Oracle Virtual Platform Oracle Server	Yes	Yes
Engineered System	ZFS Array Storage Heads	No	Oracle ZFS Appliance	No	Yes (configured by the customer)
Exadata	Database Node	Yes	Systems Infrastructure Server Host	Yes	Yes

Device		Monitor			
	Component	**Cloud Control Agent**	**Plug-in Target Type**	**SNMP Trap**	**ASR**
			Host		
SuperCluster	Control Domains	Yes	Systems Infrastructure Server Host	Yes	Yes
SuperCluster	Logical Domains	Yes		Yes	No (covered by Control Domain)
Standalone Server (including other Engineered System nodes and VMs, for example: ODA, BDA, Exalytics)		Yes	Oracle Engineered System ILOM Server (if Oracle hardware) Systems Infrastructure Server Host	Yes	Yes
Standalone ZFS Array Storage Heads		No	Oracle ZFS Storage Appliance	No	Yes (configured by the customer)

Implementation Impact on the Environment

The following sections describe the changes that are made to various types of system during the implementation process:

- Systems with an agent deployed. See “All Systems With An Agent Deployed” on page 29.
- Engineered System Storage Cells. See “Engineered Systems Storage Cells” on page 31.
- Engineered System Cisco Switch. See “Engineered System Cisco Switches” on page 31.
- Engineered System InfiniBand Switches. See “Engineered System InfiniBand Switches” on page 31.
- Engineered System PDU's. See “Engineered System PDU's” on page 32.
- Engineered Systems Compute Nodes (Physical Implementation) and Virtual Machines. “Engineered Systems Compute Nodes (Physical Implementation) and Virtual Machines” on page 32.
- OVS Compute Nodes. See “OVS Compute Nodes” on page 32.
- KVM Compute Nodes. See “KVM Compute Nodes” on page 33.

- Exalogic Compute Nodes (Physical Implementation) and Exalogic Virtual Machines / Control Virtual Machines. See "Exalogic Compute Nodes (Physical Implementation) and Exalogic Virtual Machines / Control Virtual Machines" on page 34.
- ZFS Storage Array Storage Heads. See "ZFS Storage Array Storage Heads" on page 35.

All Systems With An Agent Deployed

The following changes are made to every system on which an agent is deployed:

- An entry is added to the `/etc/hosts` file for the Gateway.
- A new group is created on the operating system (OS) of the monitored server. The default group name is *orarom*.
- A new user is created on the ILOM of the monitored server (if applicable). The default username is *orarom*.
- A new user is added on the operating system (OS) (*orarom*) of the monitored server.

Note - The password for the *orarom* account is typically set to expire after 90 days. You can manage the password on the Gateway. If access is needed for troubleshooting and the account is expired, Oracle will reset the *orarom* password. For further information about password management, see this MOS knowledge article.

- The new OS user is added to the group that owns the Oracle Inventory.
- A new user is added into the group that owns the database diag directories that are listed in the `oratab` file (required for monitoring databases and generating ADR packages).
- The Oracle Inventory directory is updated for group read/write permissions.
- The Database diag directories are updated for group read/write permissions.
- A directory (`/opt/OracleHomes`) is created for the agent information based on the information provided in the System Install flow or discussion with your implementation engineer.
- If permission to retain root privileges is given in the configuration worksheet, the sudoers or RBAC files are updated to allow the new OS user to execute commands as root.
- For Linux systems, the group of the `/var/log/messages` file is changed to the new group (*orarom*) if the group owner is root.

  This allows the agent user to be part of a group that can read the file and the group read permission is granted. The agent user can then monitor the messages file. If the messages file is already owned by a different group, the new user is added to that group instead.
- For Linux systems, the `/etc/security/limits.conf` file is updated to add the required settings for the new user (*orarom*) to meet the agent requirements.

- Agents are pushed from the Gateway to the server using the new user. The storage requirement for the agent is initially around 5GB.
- Once the agents have been installed, the root.sh script for the agent is executed.

  Root.sh creates or updates /etc/oragchomelist, creates /etc/init.d/gcstartup, creates /etc/init.d/lockgcstartup, and creates /etc/init.d/lockgcstartup.
- For Solaris systems, the explorer tool may be scheduled to execute once per week at 11 PM on Sunday in root's crontab.
- For some Solaris systems, host-based fault telemetry is configured for ASR, either updating snmpd.conf or using *asradm*, and starting the required services.
- ILOMs are configured to send SNMP traps to the Gateway for all ILOM detected faults of level minor or above for ASR.

Note - For Exadata Nodes, the ILOM rules are configured on the operating system of the node using the Exadata CLIs (cellcli and dbmcli) rather than directly on the ILOM.

- Install or upgrade the Oracle Autonomous Health Framework (AHF) to a minimum version of 22.3.1.

  The storage requirement for AHF is 2GB of space in /opt and a minimum of 6GB (with a recommendation of 10GB) on /u01.
- Configure Oracle Autonomous Health Framework (AHF) to auto-update from the Gateway when a new version is available.
- A monitoring sudoers profile is added to allow the monitoring of the system and a restart of the agents by the monitoring user:

  /usr/sbin/dmidecode, /sbin/ethtool, /usr/bin/ipmitool, /usr/sbin/imageinfo, /usr/local/bin/imageinfo, /opt/oracle/bda/bin/imageinfo, /usr/bin/systemctl stop oracle-oasgagent.service, /usr/bin/systemctl start oracle-oasgagent.service, /usr/bin/systemctl restart oracle-oasgagent.service, /usr/bin/systemctl status oracle-oasgagent.service, /sbin/service oasgagent start, /sbin/service oasgagent stop, /sbin/service oasgagent restart, /sbin/service oasgagent status

Engineered Systems Storage Cells

An Engineered System storage cell has strict policies not to allow the creation of new users or the deployment of agents on the OS.

The changes that are made to these systems are performed in three stages:

- Create a user on the ILOM of the system to allow Oracle to access the ILOM and the console of the system during troubleshooting. The default username is *orarom*.
- When the system is discovered by Oracle Enterprise Manager Cloud Control, it creates SSH/SCP keys from the monitoring user on the database node(s) to the cellmonitor user within the storage cell.
- Update the snmpsubscribers in the cell software to send the traps to the Gateway for ASR and the Enterprise Manager Agents. This removes any current subscribers that have a type of *ASR*.
- Update the notificationpolicy in the cell software to include "critical,warning,clear".
- Update the notificationmethod in the cell software to include snmp.

Engineered System Cisco Switches

The Cisco switch that is installed in the racks of an Engineered System is updated to send traps to the Gateway, and the SNMP server is enabled to send traps. The community string is entered if not already set with an access list. For the Cisco switches that support the Oracle ASR functionality, this is configured to send alerts to the Gateway.

Engineered System InfiniBand Switches

The InfiniBand switches that are installed in the racks of an Engineered System are updated to send traps to the Gateway and a set of SSH/SCP keys is created to allow password-less login from the monitoring agent to the ilom-operator on the switch.

The SSH/SCP keys for Exadata and SuperCluster systems are configured at discovery time. For the other systems, these are created manually by the installation engineer during the implementation prior to the target discoveries.

Engineered System PDU's

The PDU modules within the racks of an Engineered System are updated to send traps to the Gateway, and the PDU thresholds are set to generate alerts based on the values from Oracle Engineering teams.

Engineered Systems Compute Nodes (Physical Implementation) and Virtual Machines

A user (orarom) will be granted the following privileges in the sudoers file:

<**user**> <user> <user> ALL= NOPASSWD: /usr/sbin/dmidecode, /sbin/ethtool, /usr/bin/ipmitool, /usr/sbin/imageinfo, /usr/local/bin/imageinfo, /opt/oracle/bda/bin/imageinfo, /usr/bin/systemctl stop oracle-oasgagent.service, /usr/bin/systemctl start oracle-oasgagent.service, /usr/bin/systemctl restart oracle-oasgagent.service, /usr/bin/systemctl status oracle-oasgagent.service, /sbin/service oasgagent start, /sbin/service oasgagent stop, /sbin/service oasgagent restart, /sbin/service oasgagent status, /usr/bin/systemctl stop oracle-oasgagent.service, /usr/bin/systemctl start oracle-oasgagent.service, /usr/bin/systemctl restart oracle-oasgagent.service, /usr/bin/systemctl status oracle-oasgagent.service, /sbin/service oasgagent start, /sbin/service oasgagent stop, /sbin/service oasgagent restart, /sbin/service oasgagent status

Note - The profile may be updated if the option for Oracle to retain sudo privilege is granted.

OVS Compute Nodes

- Install or upgrade the Oracle Autonomous Health Framework (AHF) to a minimum version of 23.10.

  The storage requirement for AHF is 2GB of space in /opt and a minimum of 6GB (with a recommendation of 10GB) on /EXAVMIMAGES.
- Install *oasg-agent* software.
- Configure Oracle Autonomous Health Framework (AHF) to auto-update from the Gateway when a new version is available.
- Configure Oracle Autonomous Health Framework (AHF) to communicate to all KVM Nodes via socket for data collection.

The Oracle Virtual Server operating system that is used within an Engineered System that is running the virtualized stack has strict policies that do not allow the installation of Oracle Enterprise Manager (EM) agents on to the systems. These nodes will have the ILOMs configured to send traps to the Gateway for ASR. A user (*orarom*) will be created on the OVS Server and granted the following privileges in the sudoers file:

<**user**> ALL= NOPASSWD: /usr/sbin/xentop, /usr/sbin/dmidecode, /sbin/ethtool, /usr/bin/xenstore-ls, /usr/bin/xenstore-read, /usr/bin/xenstore-list, /usr/sbin/xl, /usr/bin/ipmitool, /usr/sbin/xm, /usr/sbin/imageinfo, /usr/local/bin/imageinfo, /opt/oracle/bda/bin/imageinfo, /usr/bin/systemctl stop oracle-oasgagent.service, /usr/bin/systemctl start oracle-oasgagent.service, /usr/bin/systemctl restart oracle-oasgagent.service, /usr/bin/systemctl status oracle-oasgagent.service, /sbin/service oasgagent start, /sbin/service oasgagent stop, /sbin/service oasgagent restart, /sbin/service oasgagent status

This list of commands is used by the Oracle Virtual Platform and Oracle Server target types to read information about the system, relay the information to OEM, and manage the *oasg_agent*.

Note - The profile may be updated if the option for Oracle to retain sudo privilege is granted.

KVM Compute Nodes

- Install or upgrade the Oracle Autonomous Health Framework (AHF) to a minimum version of 23.10.

  The storage requirement for AHF is 2GB of space in /opt and a minimum of 6GB (with a recommendation of 10GB) on /EXAVMIMAGES.
- Install *oasg-agent* software.
- Configure Oracle Autonomous Health Framework (AHF) to auto-update from the Gateway when a new version is available.
- Configure Oracle Autonomous Health Framework (AHF) to communicate to all KVM Nodes via socket for data collection.

The Oracle Linux 7 Server used within an Engineered System that is running the virtualized stack has strict policies that do not allow the installation of Oracle Enterprise Manager (EM) agents on to the systems. These nodes will have the ILOMs configured to send traps to the Gateway for ASR. A user (*orarom*) will be created on the KVM Server and granted the following privileges in the sudoers file:

<user> ALL= NOPASSWD: /usr/bin/virsh list*, /usr/bin/virsh dominfo*, /usr/bin/virsh nodememstats*, /usr/bin/virsh domstats*, /usr/bin/virsh

capabilities, /usr/bin/virsh domblklist*, /usr/bin/virsh domiflist*, /usr/bin/virsh domifstat*, /usr/bin/virsh vcpupin*, /bin/virsh cpu-stats*, /bin/virsh domblkstat*, /bin/virsh dommemstat*, /bin/virsh nodeinfo, /sbin/dmsetup info, /sbin/service --status-all, /usr/sbin/dmidecode, /sbin/ethtool, /usr/bin/ipmitool, /usr/sbin/imageinfo, /usr/local/bin/imageinfo, /opt/oracle/bda/bin/imageinfo, /opt/exadata_ovm/vm_maker, /usr/sbin/brctl, /sbin/fdisk -l*, /bin/virsh domblkinfo*, /usr/bin/lvs*, /usr/bin/smartctl*, /usr/sbin/ibnetdiscover, /usr/sbin/sminfo, /sbin/dmsetup info*, /bin/cat /etc/iscsi/iscsid.conf, /usr/bin/systemctl stop oracle-oasgagent.service, /usr/bin/systemctl start oracle-oasgagent.service, /usr/bin/systemctl restart oracle-oasgagent.service, /usr/bin/systemctl status oracle-oasgagent.service, /sbin/service oasgagent start, /sbin/service oasgagent stop, /sbin/service oasgagent restart, /sbin/service oasgagent status

This list of commands is used by the Oracle Enterprise Manager (OEM) targets to read information about the system, relay the information to OEM, and manage the *oasg_agent*.

Note - The profile may be updated if the option for Oracle to retain sudo privilege is granted.

ZFS Storage Array Storage Heads

The ZFS arrays are appliances that cannot have agents installed on them. Consequently, they are monitored from another agent using a specific monitoring user. The changes that are carried out on both of the storage heads in a cluster are as follows:

- Execute the workflow “Configure for Oracle Enterprise Manager”. This always has the *recreateWorksheet* setting enabled. If the *oracle_agent* user and role are already created, then the *recreateUser* setting is not enabled. Otherwise it is enabled. If the user is set to be recreated, the password used is a strong, randomly generated, 16-character password.

  Note - The customer can change the password on the *oracle_agent* user without affecting the Oracle monitoring solution.

- Create a new user for the Oracle monitoring solution using the role *oracle_agent* created by the above workflow. The default username is *orarom*, but the name is customizable from the Service Implementation Worksheet (SIW).
- Enable *advanced_analytics* for the new user created above.

Utilization Impact Risk of OEM Cloud Control Agent on Monitored Systems

Oracle's implementation is designed to be a low risk deployment using scripts to ensure consistent deployments across all customer implementations. Furthermore, the implementation is validated for monitoring within Oracle test systems. Oracle makes no changes to customer applications or files outside of the steps described in the relevant sections on impacts on the environment above.

The table below outlines the utilization impact that OEM has on the monitored systems.

TABLE 2 Utilization Impact of Oracle Enterprise Manager Cloud Control Agent on Monitored Systems

Overhead Impact of the Oracle Tools in the Environment	
Metric	**OEM**
CPU Utilization	The OEM Agent uses from 0.02% to 1% of CPU utilization. The agent may utilize more CPU cycles, depending on the number of processes or applications monitored.
Memory Utilization	The OEM Agent needs from 1GB to 2GB RAM to operate correctly. The actual memory utilization of the agent varies depending on the number of processes or applications monitored.
Disk Space Utilization	The OEM agent requires at least 2GB of free disk space for the installation files. After installation is complete, the installation files are removed. The installed OEM agent requires about 1GB of space initially. As the agent operates, disk space gradually increases up to 5GB. To apply patches to the agent, 5GB of space is required in `/tmp` to download and extract the installer before updating the agent binaries. Oracle Autonomous Health Framework (AHF) software requires 2GB of space in `/opt` and a minimum of 6GB (with a recommendation of 10GB) on `/u01` to store the diagnostic bundles created by the software for configuration review and troubleshooting.

Backout Plan

If it is necessary for the installation to be rolled back, Oracle will:

- Shut down the agents that have been configured;
- Work with the customer to schedule a maintenance window to remove the agents and trap destinations for all the devices configured for monitoring.

Server Prerequisites for Monitoring Deployment

This section outlines the methods used to provide Oracle with the necessary server access for implementing monitoring on the Gateway. Refer to the following:

- "Server Prerequisites for Monitoring Deployment" on page 37
- "Monitoring Access: an Overview" on page 37.
- "User Privileges" on page 38
- "Solaris 11 Initial Setup User RBAC Profile" on page 40
- "Solaris 10 Initial Setup User RBAC Profile" on page 42
- "Solaris sudo Profile" on page 43
- "Linux sudo Profile" on page 44
- "ILOM User Privileges" on page 45

Server Prerequisites for Monitoring Deployment

For services that are performed using Oracle Enterprise Manager (OEM), agents must be deployed to the systems. These systems must meet the prerequisites for an EM agent as described in the Package Requirements for Oracle Management Agent section of *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

Monitoring Access: an Overview

In general, there are three methods for providing Oracle with the necessary access for implementing monitoring:

- Provide root access to all systems.
- Enable access using Role-based Access Control (RBAC.) RBAC is a security feature for controlling user access to tasks that would normally be restricted to the root role. By applying security attributes to processes and to users, RBAC can divide superuser capabilities among several administrators. This option is applicable only to systems running the Solaris operating system.
- Provide access via *sudo* (*superuser do*.) sudo is a program for operating systems such as Linux and Solaris that allows users to run programs as another user - normally as the system's superuser (root) - as specified in the `/etc/sudoers` file. This section outlines the methods used to provide Oracle with the necessary access for implementing monitoring on the Gateway.

During activation of database services, the following users and accounts are used to monitor the database:

- For storage/cluster monitoring, the user *asmsnmp* is used;
- For database monitoring, the user *dbsnmp* is used;
- For standby database monitoring, the user *sys* is used.

Note - Passwords for all of the above users must be available during installation. They can be entered by the customer into the Gateway user interface when needed.

User Privileges

Oracle requires that the user can execute the following commands using root privileges:

- <Service EM Base Directory>/agent_home/core/<*version*>/root.sh
- <Service EM Base Directory>/agent_home/agent_*/root.sh
- /opt/exalytics/asr/bda_mon_hw_asr.pl (*Exalytics only*)
- /opt/oracle/oak/bin/oakcli (*Oracle Database Appliance only*)
- /opt/oracle.cellos/compmon/exadata_mon_hw_asr.pl (*Exadata only)*
- /opt/oracle.cellos/imageinfo (*Exadata only*)
- /opt/oracle/dbserver/dbms/bin/dbmcli (*Exadata and ZDLRA only*)
- /opt/oracle/bda/bin/imageinfo (*Big Data only*)
- /opt/oracle/bda/bin/imageinfo (*Big Data only*)
- /opt/ipmitool/bin/ipmitool (*Solaris only*)
- /opt/ipmitool/sbin/ipmitool (*Solaris only*)
- /usr/bin/chmod
- /usr/bin/chown
- /usr/bin/chgrp
- /usr/bin/crontab (*Solaris only*)
- /usr/bin/cp
- /usr/bin/ex
- /usr/bin/ipmitool
- /usr/bin/grep
- /usr/bin/ls
- /usr/bin/mkdir
- /usr/bin/rmdir
- /usr/bin/passwd
- /usr/bin/profiles (*Solaris 11 only*)

- /usr/bin/systemctl
- /usr/bin/unzip
- /usr/bin/vim
- /usr/bin/virsh (Linux only)
- /usr/bin/xenstore-list
- /usr/lib/fm/notify/asr-notify (*Solaris 11 only*)
- /sbin/chkconfig
- /usr/sbin/dbmcli (*Exadata and ZDLRA only*)
- /usr/sbin/dmidecode (*Linux only*)
- /usr/sbin/groupadd
- /sbin/service
- /usr/sbin/svcadm (*Solaris only*)
- /usr/sbin/useradd
- /usr/sbin/usermod
- /usr/sbin/xm
- /usr/bin/tfactl
- /usr/bin/ahfctl
- <ServiceEMBase>/install_ahf_no_cfg.sh
- /usr/bin/systemctl start oracle-oasgagent.service
- /usr/bin/systemctl stop oracle-oasgagent.service
- /usr/bin/systemctl restart oracle-oasgagent.service
- /usr/bin/systemctl status oracle-oasgagent.service
- /sbin/service oasgagent start
- /sbin/service oasgagent stop
- /sbin/service oasgagent restart
- /sbin/service oasgagent status

The user provided for the initial setup can be removed once the monitoring has been deployed and the agent user has been created. The agent user can be a user defined within a naming service and a home directory mounted from an NFS server. However, the agent installation directory must be unique to each server to be monitored. If the agent user is configured as part of a naming service, then the user must belong to the group that owns the Oracle inventory on all of the servers. The deployment scripts will verify and enforce group write permissions on any Oracle inventory directory that is discovered by using the /etc/oraInst.loc or the /var/opt/oracle/oraInst.loc files.

Note - The command paths are related to Solaris. For the Linux paths, please refer to the sudo settings for Linux.

Solaris 11 Initial Setup User RBAC Profile

The user for the initial setup requires a profile built from the following configuration file:

```
set desc="ACS Service Profile"
add cmd=<ServiceEMBase>/agent_home/core/<version>/root.sh set
uid=0
end
add cmd=/opt/oracle.cellos/imageinfo
set uid=0
end
add cmd=/opt/oracle.cellos/compmon/exadata_mon_hw_asr.pl
set uid=0
end
add cmd=/opt/ipmitool/bin/ipmitool
set uid=0
end
add cmd=/opt/ipmitool/sbin/ipmitool
set uid=0
end
add cmd=/usr/bin/chmod
set uid=0
end
add cmd=/usr/bin/chown
set uid=0
end
add cmd=/usr/bin/chgrp
set uid=0
end
add cmd=/usr/bin/crontab
set uid=0
end
add cmd=/usr/bin/cp
```

```
set uid=0
end
add cmd=/usr/bin/ex
set  uid=0
end
add  cmd=/usr/bin/vim
set  uid=0
end
add cmd=/usr/bin/grep
set  uid=0
end
add cmd=/usr/bin/ls
set  uid=0
end
add cmd=/usr/sbin/groupadd
set  uid=0
end
add cmd=/usr/bin/mkdir
set  uid=0
end
add cmd=/usr/bin/rmdir
set  uid=0
end
add  cmd=/usr/bin/passwd
set  uid=0
end
add cmd=/usr/bin/profiles
set  uid=0
end
add cmd=/usr/lib/fm/notify/asr-notify
set  uid=0
end
add  cmd=/usr/sbin/svcadm
set  uid=0
end
add cmd=/usr/sbin/useradd
set  uid=0
end
add  cmd=/usr/sbin/usermod
set  uid=0
end
add cmd=/usr/bin/tfactl
set  uid=0
end
add cmd=/usr/bin/ahfctl
```

```
set uid=0
end
add cmd=<ServiceEMBase>/agent_home/agent_<version>/root.sh
set  uid=0
end
add
cmd=<ServiceEMBase>/install_ahf_no_cfg.sh
set  uid=0
end
```

To create the profile from the configuration file above, perform the following as root or as a user with permission to create new profiles:

```
profiles -p <Profile name> -f <configuration file>
usermod -P +<Profile name> <user>
```

This provides the required level of access to perform the creation of the user and group directories, as well as setting the permissions on the Oracle inventory.

Solaris 10 Initial Setup User RBAC Profile

Solaris 10 RBAC configuration is controlled through files located in the /etc/security directory. Append the following lines to the exec_attr file:

```
ACSSINITIAL:solaris:cmd:::<ServiceEMBase>/agent_home/core/<version>/root.sh:ui
d=0
ACSSINITIAL:solaris:cmd:::<ServiceEMBase>/agent_home/agent_<version>/<version
>/root.sh:uid=0 ACSSINITIAL:solaris:cmd:::/opt/ipmitool/bin/ipmitool:uid=0
ACSSINITIAL:solaris:cmd:::/opt/ipmitool/sbin/ipmitool:uid=0
ACSSINITIAL:solaris:cmd:::/usr/bin/chmod:uid=0
ACSSINITIAL:solaris:cmd:::/usr/bin/chown:uid=0
ACSSINITIAL:solaris:cmd:::/usr/bin/chgrp:uid=0
ACSSINITIAL:solaris:cmd:::/usr/bin/crontab:uid=0
ACSSINITIAL:solaris:cmd:::/usr/bin/cp:uid=0
ACSSINITIAL:solaris:cmd:::/usr/bin/ex:uid=0
ACSSINITIAL:solaris:cmd:::/usr/bin/vim:uid=0
```

```
ACSSINITIAL:solaris:cmd:::/usr/bin/grep:uid=0
ACSSINITIAL:solaris:cmd:::/usr/sbin/groupadd:uid=0
ACSSINITIAL:solaris:cmd:::/usr/bin/ls:uid=0
ACSSINITIAL:solaris:cmd:::/usr/bin/mkdir:uid=0
ACSSINITIAL:solaris:cmd:::/usr/bin/rmdir:uid=0
ACSSINITIAL:solaris:cmd:::/usr/bin/passwd:uid=0
ACSSINITIAL:solaris:cmd:::/usr/sbin/svcadm:uid=0
ACSSINITIAL:solaris:cmd:::/usr/sbin/useradd:uid=0
ACSSINITIAL:solaris:cmd:::/usr/sbin/usermod:uid=0
ACSSINITIAL:solaris:cmd:::/usr/bin/tfactl:uid=0
```

If Oracle Enterprise Manager (OEM) agents are installed on an Exalogic, an NFS mount is configured by Oracle, and the user must also have the following command added to the profile:

```
ACSSINITIAL:solaris:cmd:::/sbin/mount:uid=0
```

Append the following line to the prof_attr file:

```
ACSSINITIAL:::Oracle Install Profile:
```

Once these entries have been added, update the user that will be used for the initial installation to allow access to the profile:

```
usermod -P ACSSINITIAL <user>
```

Solaris sudo Profile

For Solaris users, add the following entries to the sudoers file:

```
Cmnd_Alias      ACSSINSTALL = /usr/bin/chmod, /usr/bin/chown, \
                  /usr/bin/chgrp, /usr/bin/crontab, /usr/bin/cp, \
                  /usr/bin/ex, /usr/bin/grep, /usr/sbin/groupadd, \
                  /usr/bin/ls, /usr/bin/mkdir, /usr/bin/passwd, \
                  /usr/bin/profiles,  /usr/lib/fm/notify/asr-notify,  \
                  /usr/bin/rmdir, /usr/sbin/svcadm,/usr/sbin/asradm, \
                  /usr/sbin/useradd, /usr/sbin/usermod, \
                  <ServiceEMBase>/agent_home/core/<version>/root.sh,\
                  /opt/ipmitool/bin/ipmitool, /opt/ipmitool/sbin/ipmitool, \
                  /opt/oracle.cellos/compmon/exadata_mon_hw_asr.pl,  \
                  /opt/oracle.cellos/imageinfo, \
                  /usr/bin/tfactl, \
                  /usr/bin/ahfctl, \
                  <ServiceEMBase>/agent_home/agent_<version>/root.sh,\
                  <ServiceEMBase>/install_ahf_no_cfg.sh, \
                  /usr/bin/exachk, \
                  /opt/oracle.ahf/exachk/exachk

  <user> ALL=(ALL) ACSSINSTALL
```

The user must also have the sudo binary in their path to allow it to execute without a full path.

If the OEM agents are installed using an NFS mount that is to be configured by Oracle, then the

user must also have the following command alias created as assigned to the user:

```
Cmnd_Alias      ACSSH/SCPAREDINSTALL = /sbin/mount
<user> ALL=(ALL) ACSSH/SCPAREDINSTALL
```

Linux sudo Profile

For Linux users, add the following entries to the sudoers file:

```
Cmnd_Alias      ACSSINSTALL = /bin/chmod, /bin/chown, \
                 /bin/chgrp, /bin/cp, /bin/ex, /usr/bin/unzip, \
                 /bin/grep, /bin/ls, /bin/mkdir, /bin/rmdir, \
                 /opt/exalytics/asr/bda_mon_hw_asr.pl, \
                 /usr/bin/passwd, /usr/sbin/groupadd, \
                 /usr/sbin/useradd, /usr/sbin/usermod, \
                 /usr/bin/ipmitool, /usr/bin/ipmitool, /usr/bin/xenstore-list, \
                 /opt/oracle/oak/oakcli, /usr/sbin/dmidecode, \
                 /opt/exalytics/asr/bda_mon_hw_asr.pl, \
                 <ServiceEMBase>/agent_home/core/<version>/root.sh,\
                 <ServiceEMBase>/agent_home/agent_<version>/root.sh,\
                 /opt/oracle.cellos/compmon/exadata_mon_hw_asr.pl, \
                 /opt/oracle.cellos/imageinfo, \
                 /opt/oracle/dbserver/dbms/bin/dbmcli, \
                 /usr/sbin/imageinfo, /usr/sbin/xm, \
                 /usr/bin/tfactl, /usr/bin/ahfctl, \
                 /opt/oracle/bda/bin/imageinfo, \
                 /usr/bin/exachk, \
                 /opt/oracle.ahf/exachk/exachk, \
                 /usr/local/bin/imageinfo, \
                 /opt/oracle/bda/bin/imageinfo, \
                 /usr/sbin/pca-admin, \
                 /usr/bin/virsh, \
                 /usr/bin/systemctl enable oracle-oasgagent.service, \
                 /usr/bin/systemctl start oracle-oasgagent.service, \
                 /usr/bin/systemctl stop oracle-oasgagent.service, \
                 /usr/bin/systemctl restart oracle-oasgagent.service, \
```

```
/usr/bin/systemctl status oracle-oasgagent.service, \
/sbin/chkconfig --add oasgagent, \
/sbin/chkconfig --on oasgagent, \
/sbin/chkconfig --off oasgagent, \
/sbin/service oasgagent start, \
/sbin/service oasgagent stop, \
/sbin/service oasgagent restart, \
/sbin/service oasgagent status, \
/sbin/service init.tfa start, \
/EXAVMIMAGES/install_ahf_no_cfg.sh, \
<ServiceEMBase>/install_ahf_no_cfg.sh, \
<ServiceEMBase>/agent_home/core/<version>/root.sh,\
 <ServiceEMBase>/agent_home/agent_<version>/root.sh,\
/usr/bin/python3 /tmp/db_compliance_check.py, \
/usr/bin/python2 /tmp/db_compliance_check.py
```

```
<user> ALL=(ALL) ACSSINSTALL
```

The user must also have the sudo binary in their path to allow it to execute without a full path.

ILOM User Privileges

Oracle requires that the implementation user has the following privileges on an ILOM:

- *Admin*: To update the alert rules to send traps to the Gateway.
- *User Management*: To create the monitoring user.
- *Read-Only*: To view other ILOM properties, for example: host name, IP address, serial number, and so on.

For example:

```
set /SP/users/oracledeployer role=auo
```

Storage Prerequisites for Monitoring Deployment

This section outlines storage requirements for the monitoring deployment. Refer to the following sections:

- "Monitoring Deployment: an Overview" on page 46
- "Oracle ZFS Storage Appliances" on page 46

Monitoring Deployment: an Overview

The storage systems do not have the same privilege promotion capabilities as the servers do; each storage system has a different method of granting access privileges. There are 3 options to provide Oracle with the necessary access for implementing monitoring:

- Provide administrator access to the system.
- For some systems, create a user with the necessary privileges for Oracle to configure a new user for monitoring.
- Create the monitoring user per the system requirements.

For information on which options are available for the various storage systems, refer to the following sections.

Oracle ZFS Storage Appliances

The information in the following sections defines the properties for the users used in the deployment of monitoring and the standard monitoring users. Further privileges are required for patching the systems during a patch cycle. Refer to the following sections:

- "Restricted User for Monitoring Deployment (AKSH Shell)" on page 46
- "Monitoring User Requirements" on page 47
- "Restricted User for Monitoring Deployment User (ILOM)" on page 47
- "Monitoring User Requirements (ILOM)" on page 47

Restricted User for Monitoring Deployment (AKSH Shell)

You can create a user with the following privileges to be used during the monitoring deployment:

TABLE 3 Privileges for a Restricted User for Monitoring Deployment

Object	Permissions
worksheet.*.*	modify
stat.*	■ read ■ create
user.*	■ changePassword ■ changePreferences ■ changeProperties

Object	Permissions
	■ changeRoles ■ create
workflow.*.*	read
role.*	■ changeAuths ■ changeDescription ■ create

Monitoring User Requirements

You can create the monitoring user using the following high level steps:

- Execute the workflow outlined in the section “Configure for Oracle Enterprise Manager Monitoring”, ensuring to select creation of the worksheet.
- Create a new user for monitoring.
- Assign the *oracle_agent* role to this user.
- Set the preferences for the user to enable Advanced Analytics.
- Add the *stat.** create authorization to the *oracle_agent* role.

Restricted User for Monitoring Deployment User (ILOM)

You can create a user with the role of *u* to allow Oracle to create a new user for use with the monitoring.

Monitoring User Requirements (ILOM)

In order to provide monitoring and diagnostic collection on the ZFS ILOM, including initiating an NMI to the host, the monitoring user requires the permissions *cro*.

Using the Gateway User Interface

In this release, we are distributing a new Gateway user interface that enables users to work on three main functional areas:

- Remote access control
- Syslog forwarding

- System proxy

Users can check the status of various system settings and make changes to these systems.

These Gateway features can be updated using the interface in two separate modes:

- Interactive, *or*
- Non-interactive

Logging on to the Gateway User Interface in Interactive Mode

This section outlines how to log on to the Gateway user interface in interactive mode. You log in as *custadmin* to access the user interface and use the menu to navigate through the available settings.

To access the user interface:

1. Log in as the *custadmin* user.

   The initial banner is displayed:

   ```
   #         Gateway User Interface              #
   #  This is a restricted interface that can be used  #
   # to view and update various settings on the Gateway   #
   # Press enter to start... #
   ```
2. Click **Enter**.

   The main menu is displayed:

   ```
   Main menu
   1) Remote access control
   2) Syslog forwarding
   3) System proxy
   Choose an option (q to quit):
   ```
3. Select one of the options offered. For example, click **1** to choose remote access control.

   The feature menu is displayed. Review the following sections to understand the interactive mode.

Choose the required feature outlined in the following sections:

- Remote access control.
- Syslog forwarding.

- System proxy.

Using Remote Access Control in Interactive Mode

After logging on to the Gateway user interface in interactive mode, you can access remote access control by selecting **1**.

To use remote access control:

1. From the main menu, click **1**.

   The remote access control menu is displayed:

   Remote access control menu

   Remote access is currently [disabled]

   No timer is currently set to disable remote access

   1) Toggle remote access status

   2) Enable remote access for a specific amount of time

   Choose an option (enter for main menu):

   This setting determines whether Oracle engineers have access to connect to the Gateway over its SSLVPN connection.

   The current remote access status is displayed (where *disabled* means that there is no inbound access over SSLVPN).

   You can set a timer to temporarily enable remote access for a set period of time. When the timer expires, access is disabled.

   You can cancel a set timer.
2. (Optional) Click **1** to toggle remote access status.

   This toggles the current status of remote access as *disabled* or *enabled*.

   The updated setting is displayed at the main menu.

   If remote access is disabled while a timer is set, the timer is removed and remote access is disabled.
3. (Optional) Click **2** to enable remote access for a specific time period.

   You are prompted to enter the length of time in minutes.
4. (Optional) When a timer is set, the main menu displays remote access status and the options change.

   The remote access control menu is displayed:

   Remote access control menu

   Remote access is currently [enabled]

A timer is set to disable remote access in [59] minutes

1) Toggle remote access status

2) Remove timer and disable remote access

Choose an option (enter for main menu):

5. (Optional) Click **2** to remove the timer and disable remote access.

   The timer is removed and remote access is immediately disabled.

Using syslog Forwarding in Interactive Mode

After logging on to the Gateway user interface in interactive mode, you can access syslog forwarding by selecting **2**.

To use syslog forwarding:

1. From the main menu, click **2**.

   The syslog forwarding menu is displayed:

   1) Message Forward Status [enabled]

   2) session Message Forward [disabled]

   3) Host Port Number [8080]

   4) OEM Audit Message Forward [enabled]

   5) firewall Message Forward [disabled]

   6) UID/GID Mapping [enabled]

   7) Host IP Address [1.2.3.4]

   8) ssh Message Forward [enabled]

   9) Protocol Used to Forward [UDP]

   Choose an option (enter for main menu):

   The Gateway can forward various information to a remote syslog server. You can use the menu to change all the related settings. The current status of each setting is displayed.
2. (Optional) Click **1** to completely enable/disable the syslog forwarding feature.
3. (Optional) Click **2** to toggle whether to forward session related information.
4. (Optional) Click **3** to set the port of the remote syslog server.
5. (Optional) Click **4** to toggle whether to forward OEM audit-related information.
6. (Optional) Click **5** to toggle whether to forward firewall-related information.
7. (Optional) Click **6** to toggle whether to map UID to GID in outgoing messages.
8. (Optional) Click **7** to set the IP address of the remote syslog server.
9. (Optional) Click **8** to toggle whether to forward SSH-related information.

10. (Optional) Click **9** to toggle the protocol used to forward syslogs between the UDP and TCP protocols.

Using System Proxy in Interactive Mode

After logging on to the Gateway user interface in interactive mode, you can access system proxy by selecting **3**.

To use system proxy forwarding:

1. From the main menu, click **3**.

   The system proxy menu is displayed:

   1) Host:Port Not set

   2) Credentials Not set

   [#] Edit an item

   [r] Remove proxy from system

   [s] Save proxy to system

   [q] Return without making changes

   Choose an option:

   You can configure the Gateway so all outbound traffic back to Oracle is sent through a proxy server. The current proxy settings are displayed in the menu.

   You can:

   - Set a proxy with just a host and port;
   - Set a username and password (you must provide both a username and password);
   - Update or remove all the proxy settings from the Gateway.
2. (Optional) Click **1** to enter a valid IP address and port for the proxy server. Host names are not accepted. The updated settings are reflected on the main menu but are not yet written to the system.
3. (Optional) Click **2** to enter a username and password to use for the proxy server. If no host and port have been set, you are prompted for those first. The updated settings are reflected on the main menu but are not yet written to the system.
4. (Optional) Click **r** to remove the proxy from the system.

   All proxy settings are immediately removed from the Gateway.
5. (Optional) Click **s** to save the proxy to the system.

   All current proxy settings are written to the system.
6. (Optional) Click **q** to return without making changes.

   You quit back to the main menu and discard any changes that may have been made.

Using the Gateway User Interface in Non-Interactive Mode

This section outlines how to use the Gateway user interface in non-interactive mode.

Standalone SSH commands are issued using LDAP credentials. Your level of access is determined by the authorization provided by LDAP. The SSH command contains a setting change or status request for the Gateway that is executed without having to interact with an actual interface.

The SSH commands used for the Gateway user interface in non-interactive mode consist of:

- A prefix, *and a combination of,*
- Options
- Settings

The available options and settings depend upon the feature being addressed. The exit code from the SSH command is *0* for success and *1* for failure.

Choose the required feature outlined in the following tables:

- Remote access control.
- Syslog forwarding.
- System proxy.

Using Remote Access in Non-Interactive Mode

This section outlines how to use remote access control in non-interactive mode.

To use remote access control, select the SSH commands from the following table:

TABLE 4 Remote Access Control SSH Commands

Prefix	Option	Setting	Description	Sample Usage	Sample Output
remoteaccess	*login*	*enabled/disabled*	Toggle the remote access.	`ssh -q user@gateway remoteaccess login=enabled`	YYYY-MM-DD HH:MM:SS [INFO] Successfully set remote access to [enabled]
	timer	Duration in minutes (see the sample usage)	Temporarily enable remote access for a set period of time.	`ssh -q user@gateway`	YYYY-MM-DD HH:MM:SS [INFO]

Prefix	Option	Setting	Description	Sample Usage	Sample Output
			When the timer expires, access is disabled.	remoteaccess timer=60	Successfully set remote access timer
		status	Check whether there is currently a timer set to control remote access.	ssh -q user@gateway remoteaccess timer=status	YYYY-MM-DD HH:MM:SS [INFO] There is no remote access timer currently set
		disabled	Immediately remove any remote access timer and disable remote access.	ssh -q user@gateway remoteaccess timer=disabled	YYYY-MM-DD HH:MM:SS [INFO] Successfully disabled remote access timer
	status		Check the current status of remote access.	ssh -q user@gateway remoteaccess status	YYYY-MM-DD HH:MM:SS [INFO] Remote access is currently [disabled]

Using System Proxy in Non-Interactive Mode

This section outlines how to use system proxy in non-interactive mode.

To use system proxy, select the SSH commands from the following table:

TABLE 5 System Proxy SSH Commands

Prefix	Option	Setting	Description	Sample Usage	Sample Output
proxy	*ip*	*proxy server ip address*	Valid IP address for the proxy server. You must always set the IP address and port together.	ssh -q user@gateway proxy ip=192.0.2.0 port=9001	YYYY-MM-DD HH:MM:SS [INFO] Successfully configured proxy
	port	*proxy server port*	Valid port number for the proxy server. You must always set the IP address and port number together.	ssh -q user@gateway proxy ip=192.0.2.0 port=9001	YYYY-MM-DD HH:MM:SS [INFO] Successfully configured proxy
	user	*proxy user*	User name for the proxy server. You must always set the user name and password together,	ssh -q user@gateway proxy ip=192.0.2.0 port=9001 user=MarkESmithBrix/	YYYY-MM-DD HH:MM:SS [INFO] Successfully configured proxy anchester

Prefix	Option	Setting	Description	Sample Usage	Sample Output
			with the IP address and port number.	pass=Fa!! GrannyB0ng0s	
	pass	*proxy password*	Password for the proxy server.	ssh -q user@gateway proxy ip=192. 0.2.0 port=9001 user=MarkESmithBrix pass=Fa!! GrannyB0ng0s	YYYY-MM-DD HH:MM:SS [INFO] Successfully configured proxy anchester
	disabled		Remove proxy settings from the Gateway.	ssh -q user@gateway proxy disabled	YYYY-MM-DD HH:MM:SS [INFO] Successfully removed proxy from system
	status		Return the current Gateway proxy settings.	ssh -q user@gateway proxy status	YYYY-MM-DD HH:MM:SS [INFO] Current proxy set to [192.0.2.0: 9001] [user = MarkESmithBrixManc hester]

Using syslog Forwarding in Non-Interactive Mode

This section outlines how to use syslog forwarding in non-interactive mode.

To use remote access control, select the SSH commands from the following table.

Note - You can send multiple option/setting pairs in the same SSH command: ssh -q user@gateway syslog ip=192.168.100.9 port=9001 protocol=tcp

TABLE 6 Syslog Forwarding SSH Commands

Prefix	Option	Setting	Description	Sample Usage	Sample Output
syslog	*ip*	*ip address*	Valid IP address for the remote syslog server	ssh -q user@gateway syslog ip==192. 0.2.0	YYYY-MM-DD HH:MM:SS [INFO] Successfully set [ip] to [192.0.2.0]
	port	*port*	Valid port number for the remote syslog server	ssh -q user@gateway syslog port=9001	YYYY-MM-DD HH:MM:SS [INFO] Successfully set [port] to [9001]
	protocol	*tcp/udp*	Protocol used to forward syslog data	ssh -q user@gateway	YYYY-MM-DD HH:MM:SS [INFO]

Prefix	Option	Setting	Description	Sample Usage	Sample Output
				syslog protocol=tcp	Successfully set [protocol] to [tcp]
	forward	*enabled/disabled*	Toggle remote syslog forwarding	ssh -q user@gateway syslog forward=disabled	YYYY-MM-DD HH:MM:SS [INFO] Successfully set [forward] to [disabled]
	mapping	*enabled/disabled*	Toggle whether to map UID to GID in outgoing messages	ssh -q user@gateway syslog mapping=disabled	YYYY-MM-DD HH:MM:SS [INFO] Successfully set [mapping] to [disabled]
	ssh	*enabled/disabled*	Toggle whether to forward SSH-related information	ssh -q user@gateway syslog ssh=disabled	YYYY-MM-DD HH:MM:SS [INFO] set [ssh] to [disabled]
	firewall	*enabled/disabled*	Toggle whether to forward firewall-related information	ssh -q user@gateway syslog firewall=disabled	YYYY-MM-DD HH:MM:SS [INFO] Successfully set [firewall] to [disabled]
	oem_audit	*enabled/disabled*	Toggle whether to forward OEM audit-related information	ssh -q user@gateway syslog oem_audit=disabled	YYYY-MM-DD HH:MM:SS [INFO] Successfully set [oem_audit] to [disabled]
	session	*enabled/disabled*	Toggle whether to forward session related information	ssh -q user@gateway syslog session=disabled	YYYY-MM-DD HH:MM:SS [INFO] Successfully set [session] to [disabled]
	status		Return the current syslog forwarding settings	ssh -q user@gateway syslog status	YYYY-MM-DD HH:MM:SS [INFO]---------- SyslogBroadcaster Configuration -------- Message Forward Status = disabled Host IP Address = 192.168.100.9 Host Port Number = 9001 Host Time Zone = GMT firewall Message Forward = disabled ssh Message Forward = disabled session Message Forward

Prefix	Option	Setting	Description	Sample Usage	Sample Output
					= disabled UID/ GID Mapping = disabled Protocol Used to Forward = TCP OEM Audit Message Forward = enable---------- ----------

Audit Logging

Note - Customers cannot themselves configure audit logging on Gateway 21.x. In order to set up audit logging, customers are asked to open an SR to enable Oracle personnel to perform the required configuration.

The audit logging feature of the Gateway provides audit information for four different categories of system events. The four categories are:

- Outbound network connections: The Linux firewall service (iptables) triggers notifications for all outbound network traffic with the exception of traffic to Oracle managed hosts used for monitoring and management (for example, Oracle VPN end points, dts.oracle.com, support.oracle.com).
- Outbound login activity: The Linux auditing service (auditd) triggers notifications for all outbound login attempts initiated from the Gateway. This is done by monitoring usage of the SSH/SCP system binaries. The Gateway sends a message that SSH/SCP has been used, by which user, and when. The destination is not provided. auditd logs contain that information. auditd logs are not directly accessible by the customer on the Gateway.
- Inbound Gateway user login activity: The Linux auditing service (auditd) triggers notifications each time any of the system logs used for tracking logins is updated. This includes failed logins and successful login attempts. It also triggers a notification each time a user logs in from a remote system. These activities are monitored using auditd and forwarded to the customer's central logging system.
- Enterprise Manager activity: The Enterprise Manager application logs any activity performed within the application to any of the targets or their credentials. The activity in Enterprise Manager is then forwarded to the customer's central logging system.

All audit notifications are delivered using standard syslog protocol. A central logging system must be provided to accept and process these messages. Syslog forwarding is described in this document.

The format of most of these messages is based on auditd. They can be managed using various auditd and related utilities.

Sample Logging Messages

In the examples below, user mapping is enabled: uid=#(*username*) and gid=#(*groupname*). In the event that user mapping is disabled, all instances of uid=# and gid=# are replaced with uid=0 and gid=0.

Outbound Network Connectivity.

These messages are generated by firewalld and represent all outbound network traffic with the exception of traffic to known addresses used for Oracle monitoring.

The following example shows messages as they are seen on the system that receives the forwarded syslog messages.

Result from an SSH/SCP command:

```
Start ssh
2022-12-09T11:41:55.587734-05:00 HS
gatewaynode.example.com HE [kern.info]
MS - 0:0:0:0:0:0:0:1 NA:
2022-12-09T17:20:26.946315+00:00 ct-
gateway-01 iptables: TCP_CONN_START
IN= OUT=enp1s0 SRC=gw.gw.gw.gw
DST=host.host.host.host LEN=60 TOS=
0x00 PREC=0x00 TTL=64 ID=55848 DF
PROTO=TCP SPT=16890 DPT=22
WINDOW=64240 RES=0x00 SYN URGP=0
UID=1000(jdoe) GID=1001(jdoe) MARK=
0x1

End of ssh
2022-12-09T11:41:55.587734-05:00 HS
gatewaynode.example.com HE [kern.info]
MS - 0:0:0:0:0:0:0:1 NA:
2022-12-09T17:20:36.450377+00:00 ct-
gateway-01 iptables: TCP_CONN_END IN=
OUT=enp1s0 SRC=gw.gw.gw.gw
DST=host.host.host.host LEN=40 TOS=
0x08 PREC=0x40 TTL=64 ID=55885 DF
PROTO=TCP SPT=16890 DPT=22
WINDOW=501 RES=0x00 ACK FIN URGP=0
UID=1000(setup) GID=1001(setup) MARK=
0x1
```

Outbound Login Activity.

The following example shows a message as it is seen on the system that receives the forwarded syslog messages.

Result from an SSH/SCP command:

```
2022-12-09T11:41:55.587734-05:00 HS
gatewaynode.example.com HE [kern.info]
MS - 0:0:0:0:0:0:0:1 NA:
2022-12-09T17:20:26.937571+00:00 ct-
gateway-01 gateway_audit: SYSCALL
arch=c000003e syscall=59 success=yes
exit=0 a0=55e05d4f03a0 a1=
55e05d4adfe0 a2=55e05d4c7cf0 a3=8
items=2 ppid=3957593 pid=3958481
auid=1000(jdoe) uid=1000(jdoe) gid=
1001(jdoe) euid=1000(jdoe) suid=
1000(jdoe) fsuid=1000(jdoe) egid=
1001(jdoe) sgid=1001(jdoe) fsgid=
1001(jdoe) tty=pts0 ses=63296
comm="ssh" exe="/usr/bin/ssh"
subj=unconfined_u:unconfined_r:unconfined
_t:s0-s0:c0.c1023 key="gateway_audit"
```

Gateway User Login Activity.

The following examples show messages as they are seen on the system that receives the forwarded syslog messages.

Example of SSH/SCP being invoked to the Gateway:

```
2022-12-09T11:41:33.209326-05:00 HS
gatewaynode.example.com HE [auth.notice]
MS - 0:0:0:0:0:0:0:1 NA:
2022-12-09T17:20:04.735608+00:00 ct-
gateway-01 session: SYSCALL
arch=c000003e syscall=257 success=yes
exit=14 a0=ffffff9c a1=7fbb9f57f160 a2=
80002 a3=0 items=1 ppid=1245718() pid=
3957381(jdoe[priv]) auid=1000(jdoe) uid=
0(root) gid=0(root) euid=0(root) suid=0
(root) fsuid=0(root) egid=0(root) sgid=0
(root) fsgid=0(root) tty=(none) ses=63296
comm="sshd" exe="/usr/sbin/sshd"
subj=system_u:system_r:sshd_t:s0-
s0:c0.c1023 key="SESSION"
```

Result from an su command on the Gateway:

```
Aug 1 21:42:49 Aug-01 17: 42:49 GMT-04:00 0:0:0:0:0:0:0:1
NA: sample-host audispd: node=sample-host type=SYSCALL
msg=audit(1437567906.700:17840209): arch=c000003e syscall=2 success=yes
exit=3 a0=7f691418c518 a1=2 a2=7f691418c760 a3=fffffffffffffff0 items=1
```

```
ppid=22614 pid=25811 auid=54373 uid=54373 gid=501 euid=0 suid=0 fsuid=0
egid=501 sgid=501 fsgid=501 tty=pts4 ses=90594 comm="su" exe="/bin/su"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="SESSION"
```

Managing ASR Audit Logs

This section describes how to manage Oracle Auto Service Request (ASR) audit logs for the Gateway. It includes the following topics:

- "About ASR Audit Logs" on page 59
- "Viewing ASR Audit Logs" on page 59
- "Downloading ASR Audit Logs" on page 60

About ASR Audit Logs

Oracle Auto Service Request (ASR) allows customers to restore system availability if a hardware fault occurs. ASR is a secure, expedited diagnostic process with automatic service request generation, priority service request handling, and automatic parts dispatch. You can maintain an ASR audit log that enables you to view, download, and search for audits.

Viewing ASR Audit Logs

The ASR Audit Log page enables you to view and maintain all of your organization's Gateway ASR log entries, and to download cached log files.

To view ASR audit log entries:

1. Log in to the Gateway.

   The Gateway Home page appears.
2. From the **Gateway** menu, click **ASR Audit Log**.

   The ASR Audit Log page appears, displaying the following information for all entries in the ASR Log Entries table:

TABLE 7 Field Definitions in the ASR Log Entries Table

Property	Definition
#	The number of the ASR log entry.

Property	Definition
Time	The time at which the ASR log entry was made.
UUID	The UUID associated with the ASR log entry.
Site ID	The site ID at which the ASR log entry was made.
Host ID	The host ID at associated with the ASR log entry.
System ID	The system ID associated with the ASR log entry.
Asset ID	The asset ID associated with the ASR log entry.
Product Name	The product name associated with the ASR log entry.
Status	Indicates whether the ASR log entry status is: **Sent**: The ASR log entry has been delivered to Oracle ASR Infrastructure

Downloading ASR Audit Logs

The ASR Audit Log page enables you to download cached log files.

To download ASR log entries:

1. Log in to the Gateway.
   The Gateway Home page appears.
2. From the **Gateway** menu, click **ASR Audit Log**.
   The ASR Audit Log page appears.
3. Click **Download Log Files**.
   A list of timestamped ASR audit logs appears.
4. Click the required log to download it.
5. Save the log to the required location.

Installing the Gateway

The Gateway can be installed in **one of the following ways**:

- Directly onto any server hardware that is supported by Oracle Linux 8.*x* and Oracle Unbreakable Enterprise Kernel (UEK) 5.4 (or later), *or*
- On Oracle Cloud Infrastructure (OCI) via the custom image, *or*
- On Oracle VM, *or*
- On a VM that supports installation of Oracle Linux 8.*x* and Oracle Unbreakable Enterprise Kernel (UEK) 5.4 (or later) via an ISO.

To review the Oracle Support position for Oracle products running on virtualized environments, see MOS Note 249212.1.

For more information about installing the Gateway, see Oracle Advanced Services Gateway Installation Guide.

Gateway Infrastructure Maintenance and Change Management Process

This section describes the Gateway infrastructure maintenance and change management process for Oracle Platinum Services and other Oracle connected services such as Advanced Monitoring and Resolution, LifeCycle services, and Business Critical Service for Systems. Refer to the following sections:

- "Understanding Responsibilities" on page 61
- "Generating a Change Management Request" on page 62
- "Understanding the Change Management Workflow" on page 63
- "Understanding Maintenance Activities" on page 63

Understanding Responsibilities

This section lists the responsibilities of the Gateway customer and for Oracle. Refer to the following sections:

- "Customer Responsibilities" on page 61
- "Oracle Responsibilities" on page 62

Customer Responsibilities

The Customer is responsible for:

- Notifying Oracle of issues with, or changes to, any of their connected services.
- Providing advance notice and any required information to Oracle Support about any upcoming scheduled maintenance tasks by creating a Change Management (CM) request which is processed automatically.
- Informing Oracle Support when databases managed or maintained by the Gateway are added, moved, or deleted.

Tip - For Platinum customers who need to inform Oracle about upcoming changes to their Platinum certified configurations, please see the Oracle Knowledge Management article: How to Create Platinum Services Request [Video] (Doc ID 1958476.1).

- Providing access to their connected systems as needed for the effective delivery of their services.

Note - In certain limited cases, Oracle enables the customer to control remote access by providing the capability to enable and disable VPN connectivity with Oracle (this feature is sometimes referred to as "Green Button" functionality). Customers with remote VPN access or another form of restricted access must work with Oracle, when requested, to perform the required maintenance tasks on the Gateway.

- Maintaining the list of contacts in the Oracle Advanced Services Portal address book.
- Updating the passwords in the Gateway Password Management whenever passwords are changed on their systems.
- Monitoring emails and taking action as necessary.

Oracle Responsibilities

Oracle is responsible for:

- Maintaining the infrastructure used for supporting the various services delivered via the Gateway and related tools.
- Processing and performing tasks based on customer requests and updates.
- Identifying security risks promptly; developing and deploying a solution to address these risks.

Generating a Change Management Request

A Change Management (CM) request can be generated as follows:

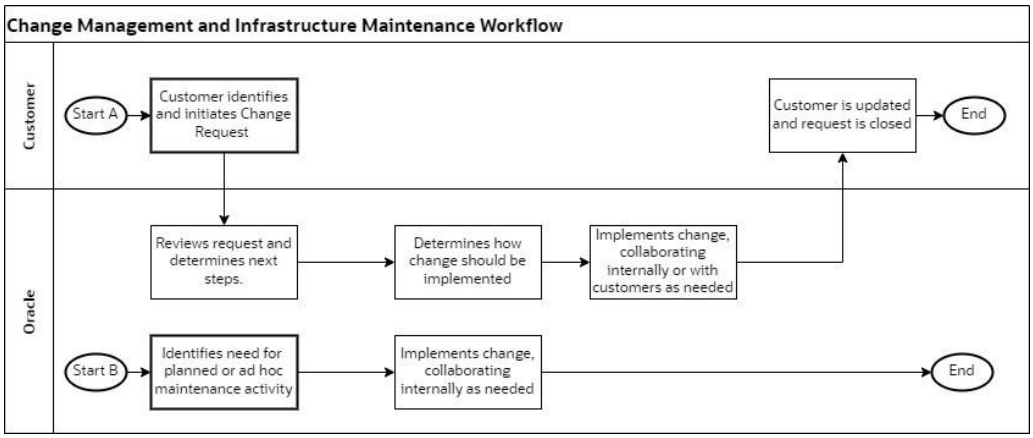
- *Customer*: Creates a Service Request (SR) in My Oracle Support. Based on the type of request, the SR is routed to the relevant Oracle team.
- *Oracle*: Identifies the need for regular maintenance on the Gateway or a request to address newly identified security risks.

Tip - For instructions on generating a CM request, please see the Oracle Knowledge Management article: How to Create a Change Management Ticket for Planned/Scheduled Outages on Oracle Advanced Support Platform (Doc ID 1663130.1).

Understanding the Change Management Workflow

This section illustrates the change management workflow. See Figure 3, "High Level Gateway Change Management and Infrastructure Maintenance Workflow," on page 63.

FIGURE 3 High Level Gateway Change Management and Infrastructure Maintenance Workflow



Understanding Maintenance Activities

This section describes the maintenance activity tasks performed by Oracle and the frequency with which each task is carried out.

TABLE 8 Maintenance Activities

Activity Type	Activity Name	Activity Description	Frequency
Upgrade	OEM upgrade	Upgrade performed on Oracle Enterprise Manager (OEM) on the Gateway.	Every 24 months

Activity Type	Activity Name	Activity Description	Frequency
Upgrade	Gateway application	Upgrade performed on the Gateway applications.	Every month
Upgrade	OS/kernel	Upgrade performed on the Gateway platform. Sometimes these are included in the Gateway application upgrade.	Every month
Upgrade	OEM agents	Upgrades performed on OEM agents installed on customer systems.	Every 3 months
Upgrade	Gateway agents (*oasg_agent*)	Upgrades performed on Gateway agents installed on customer systems.	Every month
Upgrade	Oracle Autonomous Health Framework (AHF) agent	Upgrades performed on AHF agents installed on customer systems.	Every month
Upgrade	Gateway ILOM	Upgrades performed on the ILOM version to the latest Oracle hardware version for the Gateway.	Every 6 months
Patching	Quarterly	Application of the latest quarterly patches.	Every 3 months
Patching	Security	Application of security patches at the express request of Oracle Global Information Security (GIS). This process may require 48 hours notice.	As required
Security	Password Change	Changes all Gateway passwords in accordance with Oracle security policies.	Every 90 days