Oracle® Advanced Support Gateway Security Guide

Part No: E40643-49
September 2023

ORACLE

Oracle Advanced Support Gateway Security Guide

Part No: E40643-49

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.

Référence: E40643-49

Restrictions de licence/Avis d'exclusion de responsabilité en cas de dommage indirect et/ou consécutif

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf stipulation expresse de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, accorder de licence, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Exonération de garantie

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Avis sur la limitation des droits

Si ce logiciel, ou la documentation qui l'accompagne, est livré sous licence au Gouvernement des Etats-Unis, ou à quiconque qui aurait souscrit la licence de ce logiciel pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

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

Avis sur les applications dangereuses

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer un risque de dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour des applications dangereuses.

Marques

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Inside sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Epyc, et le logo AMD sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée de The Open Group.

Avis d'exclusion de responsabilité concernant les services, produits et contenu tiers

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers, sauf mention contraire stipulée dans un contrat entre vous et Oracle. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation, sauf mention contraire stipulée dans un contrat entre vous et Oracle.

Date de publication et mention de la version préliminaire de Disponibilité Générale ("Pre-GA")

Version préliminaire de Disponibilité Générale ("Pre-GA") : 15.01.2020

Avis sur la version préliminaire de Disponibilité Générale ("Pre-GA") de la documentation

Si ce document est fourni dans la Version préliminaire de Disponibilité Générale ("Pre-GA") à caractère public ou privé :

Cette documentation est fournie dans la Version préliminaire de Disponibilité Générale ("Pre-GA") et uniquement à des fins de démonstration et d'usage à titre préliminaire de la version finale. Celle-ci n'est pas toujours spécifique du matériel informatique sur lequel vous utilisez ce logiciel. Oracle Corporation et ses affiliés déclinent expressément toute responsabilité ou garantie expresse quant au contenu de cette documentation. Oracle Corporation et ses affiliés ne sauraient en aucun cas être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'utilisation de cette documentation.

Mention sur les informations confidentielles Oracle

INFORMATIONS CONFIDENTIELLES ORACLE. Destinées uniquement à un usage autorisé. Ne pas distribuer à des tiers.

Avis sur la reconnaissance du revenu

Si ce document est fourni dans la Version préliminaire de Disponibilité Générale ("Pre-GA") à caractère privé :

Les informations contenues dans ce document sont fournies à titre informatif uniquement et doivent être prises en compte en votre qualité de membre du customer advisory board ou conformément à votre contrat d'essai de Version préliminaire de Disponibilité Générale ("Pre-GA") uniquement. Ce document ne constitue en aucun cas un engagement à fournir des composants, du code ou des fonctionnalités et ne doit pas être retenu comme base d'une quelconque décision d'achat. Le développement, la commercialisation et la mise à disposition des fonctions ou fonctionnalités décrites restent à la seule discrétion d'Oracle.

Accessibilité de la documentation

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité de la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse : http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

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.

Oracle Advanced Support Gateway Security Guide

Part No: E40643-49

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.

Référence: E40643-49

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 Support Gateway Security Guide

This document outlines the requirements for deploying Oracle Advanced Support 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 69.
- 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 Support Gateway Security Guide* (this document) since the last release (E40643-48; July 2023).

- We have removed one of the firewall rules for external traffic between the Gateway and the Oracle Services Support Center. This rule - for which the destination was ccr.oracle.com - was used to upload diagnostic data to a Service Request (SR) from the database monitoring.

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*.

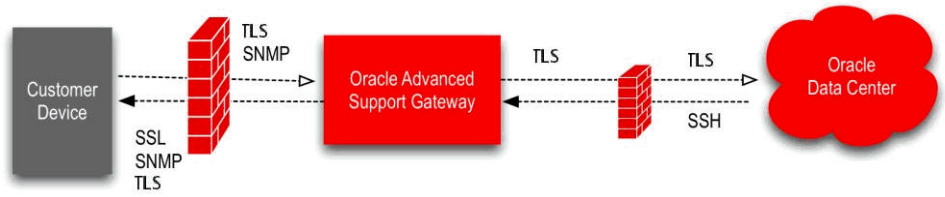
Note - A web proxy can be used to proxy the HTTPS traffic across the external connection. However, the Gateway does not support NTLM or Kerberos proxy authentication. Transport Layer Security (TLS) VPN traffic can be routed through an unauthenticated proxy server.

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



External Connection

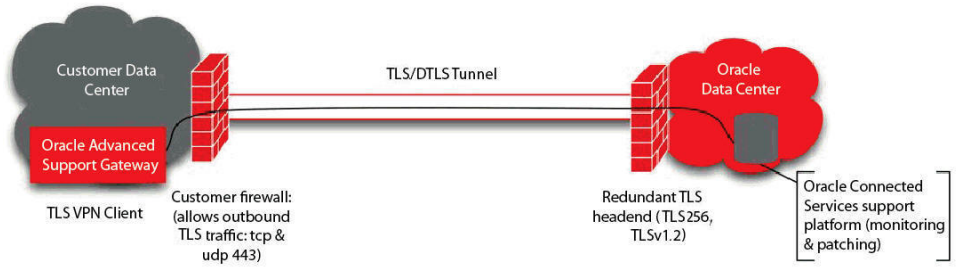
Oracle utilizes a combination of a VPN solution and to secure communications between the Gateway, located within the customer's environment, and the Oracle Services Support center locations. The VPN is primarily used for tasks such as facilitating patching requirements from Oracle Services Support center 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 in this guide (see "Firewall Rules Between the Gateway and Oracle Standalone Hosts" on page 43) 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 VPN 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 remote access to enable and disable VPN connectivity with Oracle. 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 a VPN session, toggle the icon to turn the remote access session on or off, or view a history of remote access control sessions.

Note - Remote VPN Access functionality is not available for all Oracle Connected Services. Please refer to your Oracle representative for further details.

The Remote VPN Access feature is described in *Oracle Advanced Support Gateway User's Guide*. See the Advanced Support Gateway Documentation Library.

Customer Access to the Gateway

Customer access to the Lights Out Management (LOM) section of the server is permitted for emergency power operations. To obtain this access, a customer must submit a service request to obtain the 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 provides information about the standard firewall port configurations necessary for the delivery of Oracle Services.

Note - The final port and firewall requirements depend on the specific Engineered System being monitored by Oracle Services, the connectivity method chosen, and the actual customer network design.

The following table outlines firewall port configurations and tables that provide information on monitoring requirements. Each table is associated with the services and systems which apply to it, for example, *All Services* means all remotely delivered services: Oracle Platinum Services and Oracle Advanced Monitoring and Resolution.

TABLE 1 Firewall Rules Tables, Other Monitoring Tables and Applicable Oracle Services and Systems

Table Description	Applicable Oracle Services/Systems
"Firewall Rules for External Traffic" on page 20	All Oracle Services
"Firewall Rules Between the Gateway and the Customer Network" on page 23	■ Oracle Platinum Services ■ Oracle Advanced Monitoring and Resolution
"Firewall Rules for Gateway Hardware Self-Monitoring" on page 24	■ Oracle Platinum Services ■ Oracle Advanced Monitoring and Resolution
"Firewall Rules Between the Gateway and Exadata" on page 25	■ Oracle Platinum Services ■ Oracle Advanced Monitoring and Resolution
"Firewall Rules Between the Gateway and ZDLRA" on page 28	■ Oracle Platinum Services ■ Oracle Advanced Monitoring and Resolution
"Firewall Rules Between the Gateway and ZFS" on page 30	■ Oracle Platinum Services ■ Oracle Advanced Monitoring and Resolution
"Firewall Rules Between the Gateway and Exalogic" on page 31	■ Oracle Platinum Services ■ Oracle Advanced Monitoring and Resolution
"Firewall Rules Between the Gateway and SuperCluster" on page 34	■ Oracle Platinum Services ■ Oracle Advanced Monitoring and Resolution
"Firewall Rules Between the Gateway and Exalytics" on page 37	Oracle Advanced Monitoring and Resolution
"Firewall Rules Between the Gateway and Oracle Database Appliance" on page 38	Oracle Advanced Monitoring and Resolution
"Firewall Rules Between the Gateway and Oracle Big Data Appliance" on page 40	Oracle Advanced Monitoring and Resolution
"Firewall Rules Between the Gateway and Oracle Private Cloud Appliance" on page 41	■ Oracle Platinum Services ■ Oracle Advanced Monitoring and Resolution
"Firewall Rules Between the Gateway and Oracle Standalone Hosts" on page 43	Oracle Advanced Monitoring and Resolution
"Firewall Rules Between the Gateway and Oracle Third-Party Hosts" on page 45	Oracle Advanced Monitoring and Resolution
"Firewall Rules for External Traffic Through the Encrypted VPN Tunnel" on page 21	■ Oracle Platinum Services ■ Oracle Advanced Monitoring and Resolution
"The Monitoring Matrix" on page 46	■ Oracle Platinum Services ■ Oracle Advanced Monitoring and Resolution

Table Description	Applicable Oracle Services/Systems
"Utilization Impact Risk of OEM Cloud Control Agent on Monitored Systems" on page 53	All Oracle Services
"Restricted User for Monitoring Deployment (AKSH Shell)" on page 64	■ Oracle Platinum Services ■ Oracle Advanced Monitoring and Resolution

The section on firewall port configuration is divided as follows:

- "Firewall Rules for External Traffic" on page 20
- "Firewall Rules for External Traffic Through the Encrypted VPN Tunnel" on page 21
- "Firewall Rules for Internal Traffic" on page 22

Firewall Rules for External Traffic

Note - The source for all these entries is the Gateway. The rules in Table 2, "Firewall Rules Between the Gateway and the Oracle Services Support Center," on page 20 apply to all of Oracle's Connected Services. In order to log in to the Gateway portal, your local browser is redirected to https://amr.oracle.com and https://login-ext.identity.oraclecloud.com for the authentication and authorization required.

TABLE 2 Firewall Rules Between the Gateway and the Oracle Services Support Center

Destination	Destination IP Address(es)	Application Protocol	Network Protocol/ Port	Purpose
adc-ps-ssl-vpn.oracle-occn.com llg-ps-ssl-vpn.oracle-occn.com tokyo-ps-ssl-vpn.oracle-occn.com	198.17.210.28 141.143.215.68 140.83.95.28	TLS VPN	TCP/443 - TLS UDP/443 - DTLS (Datagram TLS)	To establish a TLS VPN connection between Oracle and the Gateway. VPN communication over a proxy is supported if the provided proxy does not require authentication.
dts.oracle.com	192.206.43.1	HTTPS	TCP/443	To securely transport monitoring data to Oracle.
transport-adc.oracle.com	141.146.156.41	HTTPS	TCP/443	To securely transport monitoring and other data to Oracle.
support.oracle.com	141.146.54.16	HTTPS	TCP/443	To download patches onto the Gateway from My Oracle Support (MOS) via the Oracle Enterprise Manager (OEM) Cloud Control UI.
linux-update.oracle.com linux-update-adc.oracle.com	138.1.51.46 137.254.56.42	HTTPS	TCP/443	To patch the Gateway and to download patches (from Unbreakable Linux Network servers) for customers who have patching services.

Destination	Destination IP Address(es)	Application Protocol	Network Protocol/ Port	Purpose
linux-update-ucf.oracle.com	156.151.58.24			
updates.oracle.com	141.146.44.51	HTTPS	TCP/443	To provide patch downloads via Oracle Enterprise Manager (OEM).
epoah.oracle.com	138.1.50.56	HTTPS	TCP/443	To download updated virus definitions used by security tooling for scans and to upload scans back to Oracle.
acs-rac.oracle.com	129.157.65.44	HTTPS	TCP/2056	When the Remote Access Control feature is active on the Gateway (that is, the "Green Button" is on), rsyslog is used to send audit logs to Oracle via a secured channel.
acs-rac.oracle.com	129.157.65.44	HTTPS	TCP/443	Gateway file integrity monitoring using a secured channel.
oauth-e.oracle.com	■ 141.146.8.119 ■ 209.17.4.26 **Note -** 141.146.8.119 and 209.17.4.26 are multiple IP addresses used to service oauth-e.oracle.com. DNS resolution may return a different IP address. Ensure access is granted for each IP directly.	HTTPS	TCP/443	To provide support for Oracle centralized authentication for Oracle Enterprise Manager.

Firewall Rules for External Traffic Through the Encrypted VPN Tunnel

If you use the Oracle-provided TLS VPN solution, the following table is informational only, illustrating the traffic transmitted over the VPN in support of the Gateway. If the alternative VPN solution is used, the following traffic must be allowed to communicate over the VPN.

TABLE 3 Firewall Rules between the Gateway and the Oracle Data Center Using VPN Tunnel

Source	Destination	Network Protocol/Port	Purpose
Gateway	■ 192.206.43.197/32 ■ 198.51.38.199/32 ■ 137.254.105.5	NTP (UDP/123)	Network Time Protocol (NTP)
Gateway	192.206.43.194/32	Syslog (TCP/514)	Gateway Syslog
Gateway	198.51.38.194/32	HTTPS (TCP/8080,9898)	Gateway file integrity monitoring

Source	Destination	Network Protocol/Port	Purpose
198.51.38.193/32	Gateway	HTTPS (TCP/8080,9898)	Gateway file integrity monitoring
■ 192.206.43.209/32 ■ 198.51.38.209/32 ■ 140.85.164.34/32	Gateway	Security Scanner ■ TCP/UDP/1-65535 ■ ICMP (Types 8 & 0)	Gateway availability and security scanning
■ 198.51.37.1/32 ■ 193.188.5.1/32 ■ 140.83.88.1/32 ■ 140.83.88.129/32 ■ 140.83.89.1/32 ■ 141.146.155.40/32 ■ 141.146.155.41/32 ■ 192.206.43.208/32 ■ 198.51.38.208/32	Gateway	■ ICMP (Types 8 & 0) ■ SSH/SCP (TCP/22) ■ HTTPS (TCP/443, 7799, 9702) ■ SGD (TCP/5307)	Management traffic to remotely manage the Gateway and also facilitate remote access
Gateway	192.206.43.196/32	HTTPS (TCP/443)	REST services for the Gateway
Gateway	■ 192.206.43.193/32 ■ 198.51.38.196/32	LDAP (TCP/636)	Gateway authentication (LDAP)

Firewall Rules for Internal Traffic

This section provides internal firewall rules tables for the customer network, the Gateway hardware self-monitoring, Exadata Database Machine (Exadata), Zero Data Loss Recovery Appliance, ZFS Storage Appliance Racked System, Exalogic Elastic Cloud (Exalogic), SuperCluster, Exalytics In-Memory Machine (Exalytics), Oracle Database Appliance, Oracle Big Data Appliance, and standalone hosts (both Oracle and third-party.)

To see which of the following tables apply for Oracle Platinum Services, please see the Oracle-certified Platinum Services configurations on the Oracle Support website.

Note - If communication between management interfaces (that are connected to the Cisco IP switch within the Engineered System) is separated by a firewall, Access Control List (ACL), or any form of network filtering, the firewall rules must allow communication between these interfaces.

- "Firewall Rules Between the Gateway and the Customer Network" on page 23
- "Firewall Rules for Gateway Hardware Self-Monitoring" on page 24
- "Firewall Rules Between the Gateway and Exadata" on page 25
- "Firewall Rules Between the Gateway and ZDLRA" on page 28

Firewall Rules Between the Gateway and the Customer Network

The ports outlined in this table are required for accessing the Gateway customer interfaces (command line and web interfaces) as well as ports required for integrating syslog and user management email notifications.

TABLE 4 Firewall Rules Between the Gateway and the Customer Network

Source	Destination	Network Protocol/Port	Purpose
Customer User Desktop/ Intranet	Gateway	ICMP Type 0 and 8	Optional: Used by customers to test connectivity to the Gateway from their internal networks.
Gateway	Customer default gateway on DMZ	ICMP Type 0 and 8	Ping between the Gateway and the default router is temporarily used during installation of the Gateway to confirm network connectivity.
Customer User Desktop/ Intranet	Gateway	TCP/22	Customer access to CLI for network and syslog configuration of the Gateway.
Customer User Desktop/ Intranet	Gateway	HTTPS (TCP/443)	Customer access to Portal interface for administration of the Gateway and access to services.
Customer User Desktop/ Intranet	amr.oracle.com **Note -** This IP address may resolve to multiple working IP addresses.	HTTPS (TCP/443)	Provides authorization for customer access to the Gateway portal.
Customer User Desktop/ Intranet	login-ext.identity.oraclecloud.com	HTTPS (TCP/443)	Provides authentication for customer access to the Gateway portal.

Source	Destination	Network Protocol/Port	Purpose
	Note - This IP address may fail over between Oracle data centers.		
Gateway	Customer syslog server	UDP/514	Rule required if the customer enables the Gateway Audit Logging feature.
Customer User Desktop/ Intranet	Gateway ILOM	TCP/22	Customer access from ILOM to assist in failure troubleshooting.
Customer User Desktop/ Intranet	Gateway ILOM	HTTPS (TCP/443)	Customer access from ILOM to assist in failure troubleshooting.
Customer User Desktop/ Intranet	Gateway	HTTPS (TCP/7799)	(Optional) Users of the Oracle Advanced Monitoring and Resolution service and the Oracle Lifecycle Support services can access a Reporting Dashboard on the Gateway.

Firewall Rules for Gateway Hardware Self-Monitoring

This section provides an internal firewall rules table for Gateway hardware self-monitoring.

Note - This functionality is required only if the Gateway ILOM has been configured on a different network than the Gateway Ethernet network interfaces.

TABLE 5 Firewall Rules for Gateway Hardware Self-Monitoring

Source	Destination	Network Protocol/Port	Purpose
Bidirectional (Gateway ILOM and Gateway)	Bidirectional (Gateway ILOM and Gateway)	ICMP Type 0 and 8	Used to test bidirectional network connectivity
Gateway ILOM	Gateway	SNMP (UDP/162)	SNMP traps for ASR telemetry (Gateway hardware self-monitoring)
Gateway ILOM	Gateway	SSH/SCP (TCP/22)	Allow secure transfer of the firmware image from the OS to ILOM
Gateway ILOM	Gateway	HTTP (TCP/8234)	ASR alerts from ILOM to the OS
Gateway	Gateway ILOM	RCMP+ (UDP/623; TCP/623)	Management and monitoring via ILOM interface (IPMI)
Gateway	Gateway ILOM	SNMP (UDP/161)	SNMP for ASR telemetry (Gateway hardware self-monitoring)
Gateway	Gateway ILOM	SSH/SCP (TCP/22)	Management and configuration of ILOM
Gateway	Gateway ILOM	ASR (TCP/6481)	ASR for discovery and monitoring by service tags

Source	Destination	Network Protocol/Port	Purpose
Gateway	Gateway ILOM	HTTPS (TCP/443)	Monitoring configuration and fault diagnostic collection

Firewall Rules Between the Gateway and Exadata

This section provides a table showing the internal firewall rules between the Gateway and Oracle Exadata Database Machine.

TABLE 6 Firewall Rules Between the Gateway and Exadata

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/Port	Purpose
ICMP	All monitored interfaces	Gateway	ICMP Type 0 and 8	Used to test network connectivity between customer systems and the Gateway
ICMP	Gateway	All monitored interfaces	ICMP Type 0 and 8	Used to test network connectivity between the Gateway and customer systems
ICMP	DB Node and DomU	Infiniband Cell Node Cell Node ILOM DB Node DB Node ILOM PDU Cisco Switch	ICMP Type 0 and 8	Monitoring of hardware components
OEM	Gateway	DB Node and DomU	TCP/1830-1839	OEM Agent communication; typically port 1830 is used for Oracle Services
SNMP	Gateway	Infiniband PDU Cisco Switch Cell Node ILOM Cell Node DB Node ILOM DB Node and DomU	UDP/161	SNMP for ASR telemetry

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/Port	Purpose
ASR	Gateway	Infiniband Cell Node Cell Node ILOM DB Node DB Node ILOM	TCP/6481	ASR for discovery and monitoring by service tags
HTTPS	Gateway	Cell Node ILOM DB Node ILOM Infiniband	TCP/443	Monitoring configuration and fault diagnostic collection
HTTPS	DB Node and DomU	Gateway	TCP/443	Patch Download Service for patching support.
HTTP/ HTTPS	Gateway	PDU **Note -** In late Exadata X4-2 and X5-2 or above, the PDU Web interface can only be accessed using HTTPS (not HTTP.)	TCP/80 (HTTP) Or TCP/443 (HTTPS)	PDU web interface for monitoring configuration and diagnostics
SSH/SCP	Gateway	Infiniband Cell Node Cell Node ILOM DB Node and DomU DB Node ILOM PDU	TCP/22	Monitoring configuration, fault diagnostics, and patching
SSH/SCP	DB Node and DomU	Infiniband Cell Node Cell Node ILOM DB Node DB Node ILOM PDU Cisco Switch	TCP/22	Monitoring of hardware components
SNMP	DB Node and DomU	PDU Cisco Switch	UDP/161	Monitoring of hardware components
SSH/SCP	Gateway	Cisco Switch	TCP/22 (SSH/ SCP)	Monitoring configuration, fault diagnostics, and patching

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/Port	Purpose
SQL	Gateway	DB listener IP (VIP) **Note -** If a database is only listening on a Client/VIP, then access to this interface must also be allowed.	DB listener port, default is TCP/1521	DB listener port for discovery and ongoing monitoring **Note -** This is not required for Platinum Services customers.
RCMP+	Gateway	Cell Node ILOM DB Node ILOM	UDP/623, TCP/623	Management and monitoring via ILOM interface (IPMI)
HTTPS (OEM Agent)	DB Node and DomU	Gateway	TCP/1159	OEM agent communication to the Gateway **Note -** For Exadata, customers must add static routes to force all traffic with the Gateway as its destination to use the Management Network as a primary interface for communication. The static route must be permanent because in the event of any restart of the nodes, the route will be deleted and communication between the agents and the Gateway will go down.
SNMP	Infiniband PDU Cisco Switch Cell Node ILOM Cell Node DB Node ILOM DB Node	Gateway	UDP/162	SNMP for monitoring events and/or network monitoring
HTTP	Cell Node ILOM Cell Node DB Node ILOM DB Node Cisco switch Infiniband	Gateway	TCP/8234	ASR assets to communicate with ASR manager

Firewall Rules Between the Gateway and ZDLRA

This section provides a table showing the internal firewall rules between the Gateway and Oracle Zero Data Loss Recovery Appliance (ZDLRA).

TABLE 7 Firewall Rules Between the Gateway and Zero Data Loss Recovery Appliance

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/Port	Purpose
ICMP	All monitored interfaces	Gateway	ICMP Type 0 and 8	Used to test network connectivity between customer systems and the Gateway
ICMP	Gateway	All monitored interfaces	ICMP Type 0 and 8	Used to test network connectivity between the Gateway and customer systems
OEM	Gateway	Compute Node	TCP/1830-1839	OEM Agent communication; typically port 1830 is used for Oracle Services
SNMP	Gateway	Infiniband PDU Cisco Switch Storage Node ILOM Storage Node Compute Node ILOM Compute Node	UDP/161	SNMP for ASR telemetry
SNMP	Compute Node and DomU	PDU Cisco Switch	UDP/161	Monitoring of hardware components
ASR	Gateway	Infiniband Storage Node Storage Node ILOM Compute Node Compute Node ILOM	TCP/6481	ASR for discovery and monitoring by service tags
HTTPS	Gateway	Storage Node ILOM Compute Node ILOM Infiniband	TCP/443	Monitoring configuration and fault diagnostic collection
HTTPS	Compute Node	Gateway	TCP/443	Patch Download Service for patching support.

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/Port	Purpose
HTTP/ HTTPS	Gateway	PDU **Note -** In late Exadata X4-2 and X5-2 or above, the PDU Web interface can only be accessed using HTTPS (not HTTP.)	TCP/80 (HTTP) Or TCP/443 (HTTPS)	PDU web interface for monitoring configuration and diagnostics
SSH/SCP	Gateway	Infiniband Storage Node Storage Node ILOM Compute Node Compute Node ILOM PDU	TCP/22	Monitoring configuration, fault diagnostics, and patching
SSH/SCP	Gateway	Cisco Switch	TCP/22 (SSH/ SCP)	Monitoring configuration, fault diagnostics, and patching
SQL	Gateway	DB listener IP (VIP) **Note -** If a database is only listening on a Client/VIP, then access to this interface must also be allowed)	DB listener port, default is TCP/1521	DB listener port for discovery and ongoing monitoring
RCMP+	Gateway	Storage Node ILOM Compute Node ILOM	UDP/623, TCP/623	Management and monitoring via ILOM interface (IPMI)
HTTPS (OEM Agent)	Compute Node	Gateway	TCP/1159	OEM agent communication to the Gateway **Note -** For Zero Data Loss Recovery Appliance, customers must add static routes to force all traffic with the Gateway as its destination to use the Management Network as a primary interface for communication. The static route must be permanent because in the event of any restart of the nodes, the route will be deleted and communication between the agents and the Gateway will go down.
SNMP	Infiniband PDU Cisco Switch Storage Node ILOM Storage Node	Gateway	UDP/162	SNMP for monitoring events and/or network monitoring

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/Port	Purpose
	Compute Node ILOM Compute Node			
HTTP	Storage Node ILOM Storage Node Compute Node ILOM Compute Node Cisco Switch Inifiniband	Gateway	TCP/8234	ASR assets to communicate with ASR manager

Firewall Rules Between the Gateway and ZFS

This section provides a table showing the internal firewall rules between the Gateway and Oracle ZFS Storage Appliance Racked System (ZFS).

TABLE 8 Firewall Rules Between the Gateway and ZFS Storage Appliance Racked System

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/Port	Purpose
ICMP	All monitored interfaces	Gateway	ICMP Type 0 and 8	Used to test network connectivity between customer systems and the Gateway
ICMP	Gateway	All monitored interfaces	ICMP Type 0 and 8	Used to test network connectivity between the Gateway and customer systems
SSH/SCP	Gateway	ZFS Controllers ZFS ILOM Cisco Switch	TCP/22	Monitoring configuration, fault diagnostics, and patching
SSH/SCP	Gateway	PDU	TCP/22	Monitoring configuration, fault diagnostics, and patching
HTTPS	Gateway	PDU	TCP/443 (HTTPS)	PDU web interface for monitoring configuration and diagnostics
HTTPS	Gateway	ZFS ILOM	TCP/443	Monitoring configuration and fault diagnostic collection
HTTPS	Gateway	ZFS Controllers	TCP/215	OEM plug-in communication to ZFS for monitoring
SNMP	Gateway	PDU ZFS ILOM	UDP/161	SNMP for ASR telemetry

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/Port	Purpose
		ZFS Controllers Cisco Switch		
SNMP	PDU Cisco Switch	Gateway	UDP/162	SNMP for Monitoring Events
RCMP+	Gateway	ZFS ILOM	UDP/623, TCP/623	Management and monitoring using the ILOM interface (IPMI)
ZFS Phone Home	ZFS Controllers	■ asr-services.oracle.com ■ inv-cs.oracle.com *Or*; Proxy IP	TCP/443 or proxy port	ZFS Phone Home can also support an internet proxy Direct access or proxy to: ■ 129.157.65.13 (asr-services.oracle.com) ■ 129.157.65.14 (inv-cs.oracle.com)
ZFS Phone Home	ZFS Controllers	Gateway	TCP/8000	Gateway hosting a proxy server
SSH/SCP	ZFS Controllers	Gateway	TCP/22	Used to copy patches from the gateway to the ZFS arrays as SCP is available only to pull from a remote system to the ZFS array.
HTTP	ZFS ILOM ZFS Controllers Cisco Switch	Gateway	TCP/8234	ASR assets to communicate with ASR manager

Note - ZFS reporting for ASR is an exception as error telemetry is reported directly to Oracle using port 443.

Firewall Rules Between the Gateway and Exalogic

This section provides a table showing the internal firewall rules between the Gateway and Oracle Exalogic Elastic Cloud.

TABLE 9 Firewall Rules Between the Gateway and Exalogic

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/Port	Purpose
ICMP	All monitored interfaces	Gateway	ICMP Type 0 and 8	Used to test network connectivity between customer systems and the Gateway

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/Port	Purpose
ICMP	Gateway	All monitored interfaces	ICMP Type 0 and 8	Used to test network connectivity between the Gateway and customer systems
OEM	Gateway	Compute Node Control VMs (virtual only)	TCP/1830-1839	OEM Agent communication, typically 1830 is used for Oracle Services
SNMP	Gateway	Infiniband PDU Cisco Switch Compute Node Compute Node ILOM Virtual Instances	UDP/161	SNMP for ASR telemetry
ASR	Gateway	Compute Node Compute Node ILOM Infiniband	TCP/6481	ASR for discovery and monitoring by service tags
HTTPS	Gateway	Compute Node ILOM Infiniband ZFS ILOM	TCP/443	Monitoring configuration and fault diagnostic collection
HTTPS	Compute Node OVS Compute Node Control VMs	Gateway	TCP/443	Patch Download Service for patching support.
SNMP	Gateway	ZFS ILOM ZFS Controllers	UDP/161	SNMP for ASR telemetry
HTTP/HTTPS	Gateway	PDU **Note -** In late Exalogic X4-2 and X5-2 or above, the PDU Web interface can only be accessed using HTTPS (not HTTP.)	TCP/80 (HTTP) Or TCP/443 (HTTPS)	PDU web interface for monitoring configuration and diagnostics
SSH/SCP	Gateway	PDU	TCP/22	Monitoring configuration, fault diagnostics, and patching
SSH/SCP	Gateway	Infiniband Control VMs (virtual only) ZFS Controllers Compute Node	TCP/22	Monitoring configuration, fault diagnostics, and patching

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/Port	Purpose
		ZFS ILOM Compute Node ILOM		
SSH/SCP	Gateway	Cisco Switch	TCP/22 (SSH/ SCP)	Monitoring configuration, fault diagnostics, and patching
SQL	Gateway	Control VMs (Virtual only) **Note -** If a database is only listening on a Client/VIP access to this interface must also be allowed.	DB listener port, default is TCP/1521	DB listener port for discovery and ongoing monitoring
RCMP+	Gateway	Compute Node ILOM ZFS ILOM	UDP/623, TCP/623	Management and monitoring using the ILOM interface (IPMI)
HTTPS	Gateway	Compute Node	TCP/7001-7002	Monitoring install and diagnostics collection
HTTPS - ZFS agent	Gateway	ZFS Controllers	TCP/215	OEM plug-in communication to ZFS for monitoring
HTTPS (OEM agent)	Compute Node Control VMs (virtual only)	Gateway	TCP/1159	OEM agent communication to the Gateway **Note -** For Exalogic, customers must add static routes to force all traffic with the Gateway as its destination to use the Management Network as a primary interface for communication. The static route must be permanent because in the event of any restart of the nodes, the route will be deleted and communication between the agents and the Gateway will go down.
SNMP	Infiniband PDU Cisco Switch Compute Node Compute Node ILOM	Gateway	UDP/162	SNMP for Monitoring Events
HTTP	Compute Node (Solaris) Zones	Gateway	TCP/5555	Solaris Explorer uploads for automatic uploads for events
ZFS Phone Home	ZFS Controllers	■ asr-services.oracle.com ■ inv-cs.oracle.com *Or*; Proxy IP	TCP/443 or proxy port	ZFS Phone Home can also support an internet proxy Direct access or proxy to: ■ 129.157.65.13 (asr-services. oracle.com)

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/Port	Purpose
				■ 129.157.65.14 (inv-cs.oracle.com)
ZFS Phone Home	ZFS Controllers	Gateway	TCP/8000	Gateway hosting a proxy server
HTTP	Compute Node Compute Node ILOM ZFS Controllers ZFS ILOM Infiniband	Gateway	TCP/8234	ASR Assets to communicate with ASR Manager

Firewall Rules Between the Gateway and SuperCluster

This section provides a table showing the internal firewall rules between the Gateway and Oracle SuperCluster.

TABLE 10 Firewall Rules Between the Gateway and SuperCluster

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/ Port	Purpose
ICMP	All monitored interfaces	Gateway	ICMP Type 0 and 8	Used to test network connectivity between customer systems and the Gateway
ICMP	Gateway	All monitored interfaces	ICMP Type 0 and 8	Used to test network connectivity between the Gateway and customer systems
OEM	Gateway	All Domains Zones based on monitoring service	TCP/1830-1839	OEM agent communication, typically 1830 is used for Oracle Services
SNMP	Gateway	Infiniband PDU Cisco Switch SPARC Server ILOMs (virtual/floating addresses as well as physical addresses) Primary Domains	UDP/161	SNMP for ASR telemetry

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/ Port	Purpose
		Cell Node Cell Node ILOM		
ASR	Gateway	Infiniband SPARC Server ILOMs (virtual/floating addresses as well as physical addresses) Primary Domains Cell Node Cell Node ILOM	TCP/6481	ASR for discovery and monitoring by service tags
HTTPS	Gateway	SPARC Server ILOMs (virtual/floating addresses as well as physical addresses) Infiniband ZFS ILOM Cell Node ILOM	TCP/443	Monitoring configuration and fault diagnostic collection
HTTPS	All Domains Zones based on monitoring service	Gateway	TCP/443	Patch Download Service for patching support.
HTTPS - ZFS agent	Gateway	ZFS Controllers	TCP/215	OEM plug-in communication to ZFS for monitoring
SSH/SCP	Gateway	Infiniband ZFS Controllers ZFS ILOM SPARC Server ILOMs (Virtual/Floating addresses as well as Physical addresses) Cell Node ILOM Cell Node PDU All Domains Zones based on monitoring service	TCP/22	Monitoring configuration, fault diagnostics, and patching
HTTP/HTTPS	Gateway	PDU	TCP/80 (HTTP) Or	PDU web interface for monitoring configuration and diagnostics

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/ Port	Purpose
			TCP/443 (HTTPS)	
SSH/SCP	Gateway	Cisco Switch	TCP/22 (SSH/SCP)	Monitoring configuration, fault diagnostics, and patching
SQL	Gateway	Database domains/zones Client/VIP **Note -** if a database is only listening on a Client/VIP, access to this interface must also be allowed.	DB listener port, default is TCP/1521	DB listener port for discovery and ongoing monitoring **Note -** This is not required for Platinum Services customers.
RCMP+	Gateway	SPARC Server ILOMs (virtual/floating addresses as well as physical addresses) Cell Node ILOM ZFS ILOM	UDP/623, TCP/623	Management and monitoring using ILOM interface (IPMI)
WebLogic	Gateway	WebLogic instances	TCP/7001-7002	Monitoring install and diagnostics collection
HTTPS (OEM Agent)	All Domains Zones based on monitoring service	Gateway	TCP/1159	OEM agent communication to the Gateway **Note -** For SuperCluster, customers must add static routes to force all traffic with the Gateway as its destination to use the Management Network as a primary interface for communication. The static route must be permanent because in the event of any restart of the nodes, the route will be deleted and communication between the agents and the Gateway will go down.
SNMP	Primary Domains Infiniband PDU Cisco Switch SPARC Server ILOMs (virtual/floating addresses as well as physical addresses) Cell Node Cell Node ILOM	Gateway	UDP/162	SNMP for monitoring events

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/ Port	Purpose
HTTP	Primary Domains	Gateway	TCP/5555	Solaris Explorer uploads for automatic uploads for events
HTTPS	Gateway	SuperCluster Control Domain	TCP/8000	Access to the IO Domain Creation Tool for monitoring and log file collection
ZFS Phone Home	ZFS Controllers	■ asr-services.oracle.com ■ inv-cs.oracle.com *Or*; Proxy IP	TCP/443 or proxy port	ZFS Phone Home can also support an internet proxy Direct access or proxy to: ■ 129.157.65.13 (asr-services.oracle.com) ■ 129.157.65.14 (inv-cs.oracle.com)
ZFS Phone Home	ZFS Controllers	Gateway	TCP/8000	Gateway hosting a proxy server
HTTP	Primary Domains SPARC Server ILOMs (virtual/floating addresses as well as physical addresses) Cell Node Cell Node ILOM ZFS ZFS ILOM Infiniband	Gateway	TCP/8234	ASR assets to communicate with ASR manager

Firewall Rules Between the Gateway and Exalytics

This section provides a table showing the internal firewall rules between the Gateway and Oracle Exalytics In-Memory Machine.

TABLE 11 Firewall Rules Between the Gateway and Exalytics

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/Port	Purpose
ICMP	All monitored interfaces	Gateway	ICMP Type 0 and 8	Used to test network connectivity between customer systems and the Gateway
ICMP	Gateway	All monitored interfaces	ICMP Type 0 and 8	Used to test network connectivity between the

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/Port	Purpose
				Gateway and customer systems
SNMP	Gateway	Exalytics Exalytics ILOM	UDP/161	SNMP for ASR telemetry
ASR	Gateway	Exalytics and Exalytics ILOM	TCP/6481	ASR for discovery and monitoring by service tags
OEM	Gateway	Exalytics Domains DomU	TCP/1830-1839	OEM Agent communication, typically 1830 is used for Oracle Services
SSH/SCP	Gateway	Exalytics Domains DomU Dom0 ILOM	TCP/22	Monitoring configuration, fault diagnostics, and patching
SNMP	Exalytics CDom and ILOM	Gateway	UDP/162	SNMP for monitoring events and/or network monitoring
HTTPS (OEM Agent)	Exalytics Domains and DomU	Gateway	TCP/1159	OEM agent communication to the Gateway
RCMP+	Gateway	Exalytics ILOM	UDP/623, TCP/623	Management and monitoring via ILOM interface (IPMI)
HTTPS	Gateway	Exalytics Exalytics ILOM	TCP/443	Monitoring configuration and fault diagnostic collection
HTTPS	Exalytics Domains, DomU, and Dom0	Gateway	TCP/443	Patch Download Service for patching support.
HTTP	Exalytics ILOM Exalytics Domains Exalytics CDom	Gateway	TCP/8234	ASR assets to communicate with ASR manager

Firewall Rules Between the Gateway and Oracle Database Appliance

This section provides a table showing the internal firewall rules between the Gateway and Oracle Database Appliance.

TABLE 12 Firewall Rules Between the Gateway and Oracle Database Appliance

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/Port	Purpose
ICMP	All monitored interfaces	Gateway	ICMP Type 0 and 8	Used to test network connectivity between customer systems and the Gateway
ICMP	Gateway	All monitored interfaces	ICMP Type 0 and 8	Used to test network connectivity between the Gateway and customer systems
SNMP	Gateway	DB, Compute Node, and Compute Node ILOM	UDP/161	SNMP for ASR telemetry
ASR	Gateway	DB, Compute Node, and Compute Node ILOM	TCP/6481	ASR for discovery and monitoring by service tags
OEM	Gateway	DB, DomU, or Compute Node	TCP/1830-1839	OEM Agent communication, typically 1830 is used for Oracle Services
SSH/SCP	Gateway	DB, DomU, Compute Node, and Compute Node ILOM	TCP/22	Monitoring configuration, fault diagnostics, and patching
SNMP	DB, Compute Node, and Compute Node ILOM	Gateway	UDP/162	SNMP for monitoring events and/or network monitoring
HTTPS (OEM Agent)	DB, DomU, and Compute Node	Gateway	TCP/1159	OEM agent communication to the Gateway
RCMP+ (IPMI)	Gateway	Compute Node ILOM	UDP/623, TCP/623	Management and monitoring via ILOM interface (IPMI)
HTTPS	Gateway	DB *or* Compute Node ILOM	TCP/443	Monitoring configuration and fault diagnostic collection
HTTPS	DB DomU Compute Node	Gateway	TCP/443	Patch Download Service for patching support.
HTTP	DB Compute Node Compute Node ILOM	Gateway	TCP/8234	ASR assets to communicate with ASR manager

Firewall Rules Between the Gateway and Oracle Big Data Appliance

This section provides a table showing the internal firewall rules between the Gateway and Oracle Big Data Appliance.

TABLE 13 Firewall Rules Between the Gateway and Oracle Big Data Appliance

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/Port	Purpose
ICMP	All monitored interfaces	Gateway	ICMP Type 0 and 8	Used to test network connectivity between customer systems and the Gateway
ICMP	Gateway	All monitored interfaces	ICMP Type 0 and 8	Used to test network connectivity between the Gateway and customer systems
SNMP	Gateway	Infiniband PDU Cisco Switch Compute Node ILOM DomU, or Compute Node	UDP/161	SNMP for ASR telemetry
ASR	Gateway	Infiniband Compute Node Compute Node ILOM	TCP/6481	ASR for discovery and monitoring by service tags
OEM	Gateway	DomU Or Compute Node	TCP/1830-1839	OEM Agent communication, typically 1830 is used for Oracle Services
SSH/SCP	Gateway	Infiniband DomU Compute Node ILOM PDU	TCP/22	Monitoring configuration, fault diagnostics, and patching
SNMP	Infiniband PDU Cisco Switch Compute Node ILOM	Gateway	UDP/162	SNMP for monitoring events and/or network monitoring

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/Port	Purpose
	Compute Node			
HTTPS (OEM Agent)	Compute Node DomU	Gateway	TCP/1159	OEM agent communication to the Gateway
RCMP+ (IPMI)	Gateway	Compute Node ILOM	UDP/623, TCP/623	Management and monitoring via ILOM interface (IPMI)
HTTPS	Gateway	Compute Node ILOM Infiniband	TCP/443	Monitoring configuration and fault diagnostic collection
HTTPS	Compute Node DomU	Gateway	TCP/443	Patch Download Service for patching support.
SSH/SCP	Gateway	Cisco Switch	TCP/22 (SSH/SCP)	Monitoring configuration, fault diagnostics, and patching
HTTP	Gateway	PDU	TCP/80 (HTTP) TCP/443 (HTTPS)	PDU web interface for monitoring configuration and diagnostics
HTTP/HTTPS	Gateway	Cloudera Manager	TCP/7180 (HTTP) Or TCP/7183 (HTTPS)	Cloudera Manager web interface for monitoring configuration and diagnostics. The Cloudera Manager must be HTTPS or HTTP. The customer may change the default ports.
HTTP	DB Compute Nodes Compute Node ILOM Infiniband	Gateway	TCP/8234	ASR assets to communicate with ASR manager

Firewall Rules Between the Gateway and Oracle Private Cloud Appliance

This section provides two separate tables showing the internal firewall rules between the Gateway and different versions of Oracle Private Cloud Appliance (PCA.)

PCA 3.*x* has been re-engineered and now has different access requirements. While PCA 2.4.*x* and earlier versions are still supported, and have the same access requirements as before, we have added updates to PCA 3.0.*x*.

Note - PCA 3.0.*x* is supported only on Gateway 21.6 and higher versions running Oracle Linux 8.*x*.

Refer to the following tables:

- Table 14, "Firewall Rules Between the Gateway and Oracle Private Cloud Appliance (PCA) 2.4.*x*," on page 42.
- Table 15, "Firewall Rules Between the Gateway and Oracle Private Cloud Appliance (PCA) 3.0.*x*," on page 43.

TABLE 14 Firewall Rules Between the Gateway and Oracle Private Cloud Appliance (PCA) 2.4.*x*

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/Port	Purpose
ICMP	PCA Management Nodes Public addresses	Gateway	ICMP Type 0 and 8	Used to test network connectivity between customer systems and the Gateway
ICMP	Gateway	PCA management nodes public addresses	ICMP Type 0 and 8	Used to test network connectivity between the Gateway and customer systems
OEM	Gateway	PCA management nodes public addresses and virtual IP address	TCP/1830	OEM agent communication, typically 1830 is used for Oracle Services
SSH/SCP	Gateway	PCA management node public addresses and virtual IP address	TCP/22	Monitoring configuration, fault diagnostics, and patching
HTTP	PCA management nodes public addresses	Gateway	TCP/8234	PCA ASR Manager to communicate with the Gateway ASR Manager
HTTP	PCA management nodes public addresses	Gateway	TCP/8000	PCA ZFS Phone Home Proxy Service
HTTP	PCA management nodes public addresses	Gateway	TCP/5555	ASR Secure File Transport Service for upload of diagnostic packages
HTTPS	Gateway	PCA management node public addresses and virtual IP address	TCP/7002	Management Interface Access for troubleshooting
HTTPS	PCA management nodes public addresses	Gateway	TCP/443	Patch Download Service for patching support
HTTPS	Gateway	PCA management node public addresses and virtual IP address	TCP/8443	Management access to the Fabric Interconnect Switches
HTTPS (OEM Agent)	PCA management nodes public addresses	Gateway	TCP/1159	OEM agent communication to the Gateway

TABLE 15 Firewall Rules Between the Gateway and Oracle Private Cloud Appliance (PCA) 3.0.*x*

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/Port	Purpose
ICMP	PCA management nodes public addresses	Gateway	ICMP Type 0 and 8	Used to test network connectivity between customer systems and the Gateway
ICMP	Gateway	PCA management nodes public addresses	ICMP Type 0 and 8	Used to test network connectivity between the Gateway and customer systems
HTTPS	PCA management nodes public addresses	Gateway	TCP/443	PCA monitoring subsystem to communicate with the Gateway ASR Manager
HTTP	PCA management nodes public addresses	Gateway	TCP/8234	PCA ASR Manager to communicate with the Gateway ASR Manager
SSH/SCP	Gateway	PCA management node public addresses and virtual IP address	TCP/22	Monitoring configuration, fault diagnostics, and patching
HTTPS	Gateway	PCA management node public addresses and virtual IP address	TCP/443	Management Interface Access for monitoring configuration, fault diagnostics, and troubleshooting

Firewall Rules Between the Gateway and Oracle Standalone Hosts

This section provides a table showing the internal firewall rules between the Gateway and Oracle standalone hosts.

TABLE 16 Firewall Rules Between the Gateway and Oracle Standalone Hosts

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/Port	Purpose
ICMP	All monitored interfaces	Gateway	ICMP Type 0 and 8	Used to test network connectivity between customer systems and the Gateway
ICMP	Gateway	All monitored interfaces	ICMP Type 0 and 8	Used to test network connectivity between the Gateway and customer systems
SNMP	Gateway	Host Host ILOM (If Oracle hardware)	UDP/161	SNMP for ASR telemetry
OEM	Gateway	Host	TCP/1830-1839	OEM agent communication, typically 1830 is used for Oracle Services
ASR	Gateway	Host	TCP/6481	ASR for discovery and monitoring by service tags

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/Port	Purpose
		Host ILOM (If Oracle hardware)		
SSH/SCP	Gateway	Host Host ILOM (If Oracle hardware)	TCP/22	Monitoring configuration, fault diagnostics, and patching
SNMP	Host Host ILOM (If Oracle hardware)	Gateway	UDP/162	SNMP for monitoring events and/or network monitoring
HTTPS (OEM Agent)	Host	Gateway	TCP/1159	OEM agent communication to the Gateway
RCMP+	Gateway	Host Host ILOM (If Oracle hardware)	UDP/623, TCP/623	Management and monitoring using ILOM interface (IPMI)
HTTPS	Gateway	Host Host ILOM (If Oracle hardware)	TCP/443	Monitoring configuration and fault diagnostic collection
HTTPS	Host	Gateway	TCP/443	Patch Download Service for patching support.
HTTPS - ZFS agent	Gateway	ZFS Controllers	TCP/215	OEM plug-in communication to ZFS for monitoring
ZFS Phone Home	ZFS Controllers	■ asr-services.oracle.com ■ inv-cs.oracle.com *Or*; Proxy IP	TCP/443 or proxy port	ZFS Phone Home can also support an internet proxy Direct access or proxy to: ■ 129.157.65.13 (asr-services.oracle.com) ■ 129.157.65.14 (inv-cs.oracle.com)
ZFS Phone Home	ZFS Controllers	Gateway	TCP/8000	Gateway hosting a proxy server
HTTP	Primary Domain Host ZFS Controllers ZFS ILOM Host ILOM (If Oracle hardware)	Gateway	TCP/8234	ASR Manager to communicate with ASR assets

Firewall Rules Between the Gateway and Oracle Third-Party Hosts

This section provides a table showing the internal firewall rules between the Gateway and Oracle third-party hosts.

Note - ILOMs on non-Oracle hardware can be monitored by the Oracle Advanced Monitoring and Resolution service. ILOMs on non-Oracle hardware cannot be monitored by Oracle Platinum Services or Oracle Auto Service Request (ASR).

TABLE 17 Firewall Rules Between the Gateway and Third-Party Standalone Hosts

Application Protocol	Source Interface(s)	Destination Interface(s)	Network Protocol/Port	Purpose
ICMP	All monitored interfaces	Gateway	ICMP Type 0 and 8	Used to test network connectivity between customer systems and the Gateway
ICMP	Gateway	All monitored interfaces	ICMP Type 0 and 8	Used to test network connectivity between the Gateway and customer systems
SNMP	Gateway	Host Host ILOM (if Oracle hardware)	UDP/161	SNMP for ASR telemetry
OEM	Gateway	Host	TCP/1830-1839	OEM agent communication, typically 1830 is used for Oracle Services
SSH/SCP	Gateway	Host	TCP/22	SSH/SCP connection for implementation and ongoing support
SNMP	Host Host ILOM (if Oracle hardware)	Gateway	UDP/162	SNMP for monitoring events and/or network monitoring
HTTPS (OEM Agent)	Host	Gateway	TCP/1159	OEM agent communication to the Gateway
HTTPS	Host	Gateway	TCP/443	Patch Download Service for patching support.

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 46
- "Implementation Impact on the Environment" on page 47
- "Utilization Impact Risk of OEM Cloud Control Agent on Monitored Systems" on page 53

The Monitoring Matrix

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

TABLE 18 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	No
Engineered System	Infiniband Switch	No	Systems Infrastructure Network Switch	Yes	No
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**
Exalogic	Physical Compute Node	Yes	Oracle Engineered System ILOM Server Systems Infrastructure Server Host	Yes	Yes
Exalogic	Exalogic Control VM	Yes	Host	No	No
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 48.
- Engineered System Storage Cells. See “Engineered Systems Storage Cells” on page 49.
- Engineered System Cisco Switch. See “Engineered System Cisco Switches” on page 50.
- Engineered System Infiniband Switches. See “Engineered System Infiniband Switches” on page 50.
- Engineered System PDU's. See “Engineered System PDU's” on page 50.
- Engineered Systems Compute Nodes (Physical Implementation) and Virtual Machines. “Engineered Systems Compute Nodes (Physical Implementation) and Virtual Machines” on page 50.

- OVS Compute Nodes. See “OVS Compute Nodes” on page 51.
- KVM Compute Nodes. See “KVM Compute Nodes” on page 51.
- 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 52.
- ZFS Storage Array Storage Heads. See “ZFS Storage Array Storage Heads” on page 52.

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.
- 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.

Note - For Exalogic Virtual Machines, a further file is copied from the physical host to `/var/exalogic/info` to define it as part of an Exalogic.

- 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.

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 nm2user 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> ALL= NOPASSWD: /usr/sbin/dmidecode, /sbin/ethtool, /usr/bin/ipmitool, /usr/sbin/imageinfo, /usr/local/bin/imageinfo, /opt/oracle/bda/bin/imageinfo`.

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

OVS Compute Nodes

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 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`.

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

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

KVM Compute Nodes

The Oracle Linux 7 Server used within an Engineered System that is running the virtualized stack has strict policies that do not permit the installation of agents on 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
```

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

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

Exalogic Compute Nodes (Physical Implementation) and Exalogic Virtual Machines / Control Virtual Machines

These types of system have limited storage space on the root filesystem. Installing an agent on the root filesystem is deemed to put this limited space at risk. The implementation for these systems creates a project on the internal ZFS storage array in the rack and creates a filesystem for each node or VM that has an agent installed.

The installation on the node/VM will then perform the following:

- Update the (v)fstab to ensure the filesystem is mounted from the ZFS storage array at boot time.
- Mount the filesystem on the required directory.
- Install and configure the Exalogic Lifecycle Toolkit, release 14.2.

  Refer to the Exalogic Lifecycle Tools Note 1912063.1 on the My Oracle Support (MOS) website at: https://support.oracle.com/epmos/faces/DocumentDisplay?id=1912063.1.
- A user (orarom) will be granted the following privileges in the sudoers file:

  <user> `<user> ALL= NOPASSWD: /usr/sbin/dmidecode, /sbin/ethtool, /usr/bin/ipmitool, /usr/sbin/imageinfo, /usr/local/bin/imageinfo, /opt/oracle/bda/bin/imageinfo`

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 19 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.

Overhead Impact of the Oracle Tools in the Environment	
Metric	**OEM**
	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

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/exalogic/usr/sbin/imageinfo` (*Exalogic 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/vim`
- `/usr/bin/virsh` (Linux only)
- `/usr/bin/xenstore-list`
- `/usr/lib/fm/notify/asr-notify` (*Solaris 11 only*)
- `/usr/sbin/dbmcli` (*Exadata and ZDLRA only*)
- `/usr/sbin/dmidecode` (*Linux only*)
- `/usr/sbin/groupadd`
- `/usr/sbin/svcadm` (*Solaris only*)
- `/usr/sbin/useradd`
- `/usr/sbin/usermod`
- `/usr/sbin/xm`
- `/usr/bin/tfactl`
- `/usr/bin/ahfctl`
- `/tmp/install_ahf_no_cfg.sh`
- `/tmp/install_ahf.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.

User Privileges for Exalogic Systems.

If the user is part of a naming service and NFS mounts are to be defined (Exalogic systems require NFS mounts), use NFSv4 rather than NFSv3. The configuration of NFSv4 is outside the scope of this service, but the new mounts are defined with the NFSv4 options, and the following extra command must be added to the security profile, depending on OS:

- `/usr/sbin/mount` (*Linux*)
- `/sbin/mount` (*Solaris*)

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=<Service EM Base>/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=/opt/exalogic/usr/sbin/imageinfo
set uid=0
end
add cmd=/usr/bin/tfactl
set uid=0
end
add cmd=/usr/bin/ahfctl
set uid=0
end
add cmd=<Service EM Base>/agent_home/agent_<version>/root.sh
set uid=0
end
add cmd=/tmp/install_ahf_no_cfg.sh
set uid=0
end
add cmd=/tmp/install_ahf.sh
set uid=0
end
```

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:

```
add cmd=/sbin/mount
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:::<Service EM
Base>/agent_home/core/<version>/root.sh:uid=0
ACSSINITIAL:solaris:cmd:::<Service EM
Base>/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,\
                /tmp/install_ahf_no_cfg.sh, \
                /tmp/install_ahf.sh, \
                /opt/exalogic/usr/sbin/imageinfo
                /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, \
                /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/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, \
                /opt/exalogic/usr/sbin/imageinfo, \
                /usr/sbin/imageinfo, /usr/sbin/xm, \
                /usr/bin/tfactl, /usr/bin/ahfctl, \
                /tmp/install_ahf_no_cfg.sh, /tmp/install_ahf.sh, \
                /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

<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 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:

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

Note - The `systemctl` command applies only to Oracle Linux (OL) 7 and later versions. The `service` and `chkconfig` commands apply only to OL6 or earlier versions.

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 63
- "Oracle ZFS Storage Appliances" on page 63

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 64
- "Monitoring User Requirements" on page 64
- "Restricted User for Monitoring Deployment User (ILOM)" on page 64

- “Monitoring User Requirements (ILOM)” on page 65

Restricted User for Monitoring Deployment (AKSH Shell)

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

TABLE 20 Privileges for a Restricted User for Monitoring Deployment

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

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.

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

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 21 Field Definitions in the ASR Log Entries Table

Property	Definition
#	The number of the ASR log entry.
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 8.6 and Unbreakable Enterprise Kernel (UEK) 5.4 (or later), *or*
- On Oracle VM, *or*
- On a VM that supports installation of Oracle Linux 8.6 and Unbreakable Enterprise Kernel (UEK) 5.4 or later. For further information, see MOS Note 417770.1.

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 Support 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 70
- "Generating a Change Management Request" on page 71
- "Understanding the Change Management Workflow" on page 72
- "Understanding Maintenance Activities" on page 72

Understanding Responsibilities

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

- "Customer Responsibilities" on page 70
- "Oracle Responsibilities" on page 71

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 Support 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:

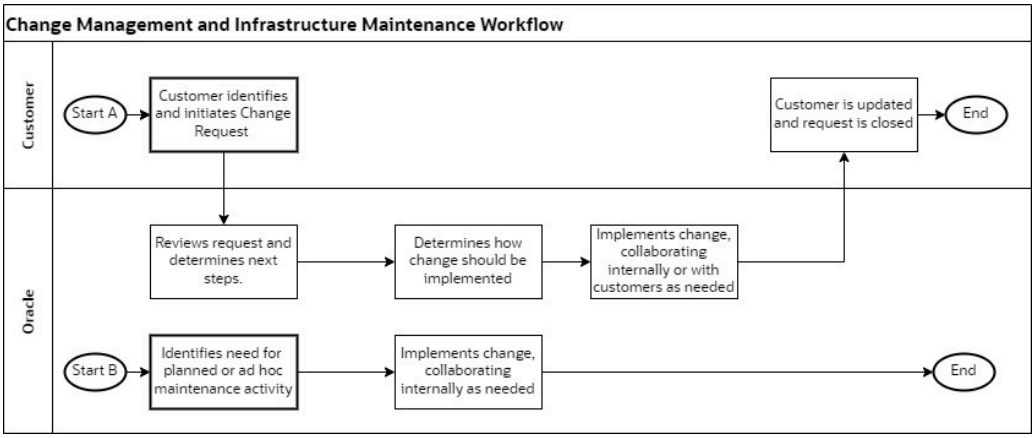
- *Customer*: Creates a Service Request (SR) in My Oracle Support. Based on the type of request, the SR is routed to the relevant Oracle team.
- *Oracle*: Identifies the need for regular maintenance on the Gateway or a request to address newly identified security risks.

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 72.

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 22 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 12 months
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