Oracle® Advanced Support Gateway for Cloud at Customer Security Guide

Part No: E91624-10
August 2020

Oracle Advanced Support Gateway for Cloud at Customer Security Guide

Part No: E91624-10

License Restrictions Warranty/Consequential Damages Disclaimer

Warranty Disclaimer

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

Restricted Rights Notice

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

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

Hazardous Applications Notice

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

Trademark Notice

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

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

Third-Party Content, Products, and Services Disclaimer

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

Pre-General Availability Draft Label and Publication Date

Pre-General Availability: 2020-01-15

Pre-General Availability Draft Documentation Notice

If this document is in public or private pre-General Availability status:

This documentation is in pre-General Availability status and is intended for demonstration and preliminary use only. It may not be specific to the hardware on which you are using the software. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to this documentation and will not be responsible for any loss, costs, or damages incurred due to the use of this documentation.

Oracle Confidential Label

ORACLE CONFIDENTIAL. For authorized use only. Do not distribute to third parties.

Revenue Recognition Notice

If this document is in private pre-General Availability status:

The information contained in this document is for informational sharing purposes only and should be considered in your capacity as a customer advisory board member or pursuant to your pre-General Availability trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle Master Agreement, Oracle License and Services Agreement, Oracle PartnerNetwork Agreement, Oracle distribution agreement, or other license agreement which has been executed by you and Oracle and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

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: E91624-10

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 for Cloud at Customer Security Guide

Part No: E91624-10

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: E91624-10

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.

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 :

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 ce 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.

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.

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 for Cloud at Customer Security Guide

This document outlines the requirements for deploying Oracle Advanced Support Gateway for Cloud at Customer infrastructure within the customer environment to support the delivery of certain Oracle cloud services (hereafter referred to as Oracle cloud services.) The Oracle Advanced Support Gateway is an important part of the Oracle delivery platform for Oracle cloud services and its placement has been carefully considered in order for Oracle to deliver Oracle cloud services. This document outlines Oracle recommendations when integrating the Oracle Advanced Support 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 Oracle Advanced Support Gateway

Oracle Advanced Support Gateway is a multi-purpose platform designed to facilitate Oracle Cloud at Customer. The Oracle Advanced Support Gateway enables the simplification of network requirements and a single point of access for the provision and delivery of these services.

The Oracle Advanced Support 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, and a suite of Java applications. Together, these applications aggregate and route telemetry messages from the Cloud at Customer infrastructure to the Oracle Support Services infrastructure. The Oracle Advanced Support 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 cloud services:

- An Oracle Advanced Support Gateway must be hosted within the customer environment along with Cloud at Customer Infrastructure.
- Oracle Advanced Support Gateway will be directly connected to the Cloud at Customer infrastructure via the management network.
- Oracle must have access to certain ports and protocols (described below) in order to implement and deliver Oracle cloud services.
- Oracle Advanced Support Gateway must be continuously accessible from the Oracle Support Platform using the secure protocols described below. However, Oracle Advanced Support Gateway must not be directly exposed to 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 Cloud at Customer Infrastructure.
- Proposed location of Oracle Advanced Support Gateway

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

Changes to the Security Guide Since the Last Release

This section outlines the principal changes made to *Oracle Advanced Support Gateway for Cloud at Customer Security Guide* (this document) since the last release (E91624-09; July 2020.)

- A firewall rule has been added to provide support for Oracle centralized authentication for Oracle Enterprise Manager. See “Firewall Rules for External Traffic” on page 16.

  The MOS authentication process is used for the implementation of new services and adding additional assets for monitoring. Failure to allow firewall access to the new IP address will cause delays executing these activities.

Firewall Port Requirements

The specifics of the Oracle cloud services network requirement depend on the customer network topology relative to the Oracle Services Support centers, Oracle Advanced Support

Gateway, and the monitored systems. The customer networks must be configured to permit traffic flow between Oracle Advanced Support Gateway and Oracle Services Support centers. This is referred to as the *external connection*.

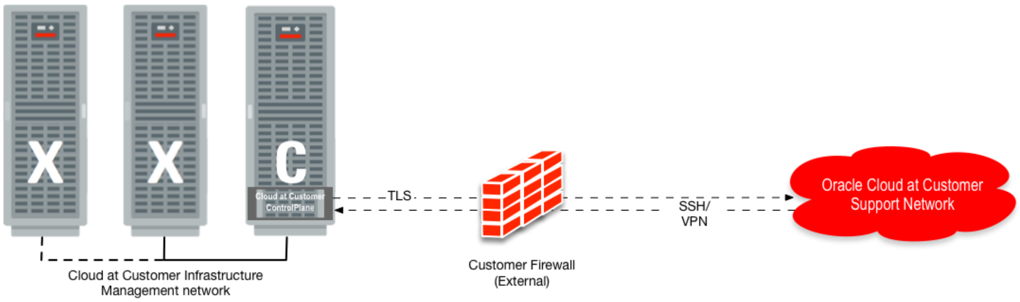
Note - A web proxy can be used to proxy the HTTPS traffic across the external connection. However, Oracle Advanced Support Gateway does not support NTLM or Kerberos proxy authentication. The Transport Layer Security (TLS) VPN traffic cannot be routed through a proxy server.

Caution - To defend against security attacks, you should never connect Oracle Advanced Support 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.)

Oracle Advanced Support Gateway comes with multiple network interfaces. Of these interfaces, two are utilized to support connectivity requirements. The first interface is used primarily for external connectivity while the second interface is connected directly to the Cloud at Customer Infrastructure management network. This provides, in effect, the required isolation between the Cloud at Customer infrastructure and the customer internal network.

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


X
X
C
Cloud at Customer ControlPlane
TLS
SSH/ VPN
Oracle Cloud at Customer Support Network
Cloud at Customer Infrastructure Management network
Customer Firewall (External)

External Connection

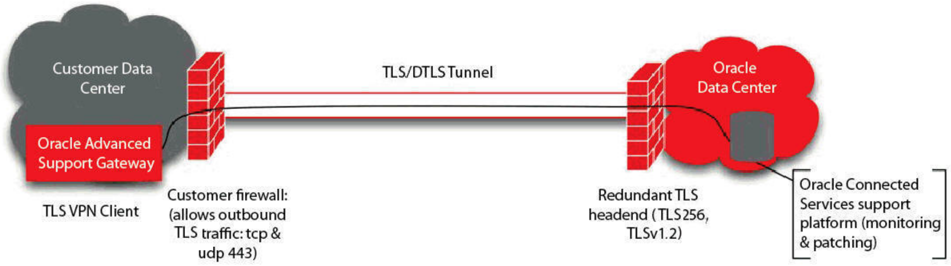
Oracle utilizes a combination of a VPN solution and TLS to secure communications between Oracle Advanced Support Gateway, located within the customer's environment, and the Oracle Services Support center locations. The VPN is primarily used for tasks such as facilitating patching requirements from Oracle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

TLS VPN and Oracle Advanced Support Gateway

The Oracle Advanced Support 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 1.2, 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 Oracle Advanced Support Gateway to Oracle


Customer Data Center
Oracle Advanced Support Gateway
TLS VPN Client
Customer firewall: (allows outbound TLS traffic: tcp & udp 443)
TLS/DTLS Tunnel
Oracle Data Center
Redundant TLS headend (TLS256, TLSv1.2)
Oracle Connected Services support platform (monitoring & patching)

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 15. 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 three /26 subnets and multiple /32 addresses inside the encryption domain;
- Network Address Translation (NAT) between the host and the Oracle resources over the tunnel is not supported (the Gateway must communicate directly to the public IP addresses inside the Oracle VPN.)

Firewall Rules: Ports and Protocols

This section provides information about the standard firewall port configurations necessary for the delivery of Oracle cloud services.

Note - The final port and firewall requirements depend on the specific Cloud at Customer infrastructure being monitored by Oracle cloud services, the connectivity method chosen, and the actual customer network design.

The following sections outline firewall port configurations and provide information on monitoring requirements.

- "Firewall Rules for External Traffic" on page 16
- "Firewall Rules for External Traffic Through the Encrypted VPN Tunnel" on page 19
- "Firewall Rules for Oracle Exadata Cloud at Customer Machine to the Customer Network" on page 20
- "Firewall Rules for Oracle Exadata Cloud at Customer Machine to the Customer Network" on page 20
- "Firewall Rules Between the Gateway and Fusion Applications (SaaS at Customer)" on page 21

Firewall Rules for External Traffic

Note - The source for all these entries is Oracle Advanced Support Gateway. The rules in Table 1, "Firewall Rules Between Oracle Advanced Support Gateway and the Oracle Services Support Center," on page 16 apply to all of Oracle's Connected Services.

TABLE 1 Firewall Rules Between Oracle Advanced Support 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 Oracle Advanced Support Gateway. *Cannot support communication through an internet proxy.
telemetry-ingestion.us-phoenix-1.oraclecloud.com	129.146.13.236 129.146.14.243	HTTPS	TCP/443	To support telemetry for the Cloud at Customer Operations dashboard endpoint; Phoenix, USA.

Destination	Destination IP Address (es)	Application Protocol	Network Protocol/Port	Purpose
	129.146.12.201			
telemetry-ingestion.us-ashburn-1.oraclecloud.com	140.91.12.7 140.91.10.15 140.91.14.5	HTTPS	TCP/443	To support telemetry for the Cloud at Customer Operations dashboard endpoint; Ashburn, USA.
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.
ccr.oracle.com	141.146.54.49	HTTPS	TCP/443	To upload the customer's configuration data to Oracle's centralized configuration repository.
support.oracle.com	141.146.54.16	HTTPS	TCP/443	To download patches onto Oracle Advanced Support Gateway from My Oracle Support (MOS) via the Oracle Enterprise Manager (OEM) Cloud Control UI.
login.oracle.com **Note -** Each hostname currently resolves to multiple working IP addresses. Access to all addresses listed must be permitted as Oracle will switch from one to another in the near future.	209.17.4.8 156.151.58.18 141.146.8.119	HTTPS	TCP/443	To connect to Oracle's centralized authentication site.
updates.oracle.com	141.146.44.51	HTTPS	TCP/443	To provide patch downloads via Oracle Enterprise Manager (OEM).
acs-rac.oracle.com	129.157.65.44	HTTPS	TCP/2056	When the Remote Access Control feature is active on Oracle Advanced Support Gateway (that is, the "Green Button" is on), rsyslog is used to send audit logs to Oracle via a secured channel. **Note -** The RAC/Green Button feature is **not** supported on Oracle Advanced Support Gateway for Cloud at Customer.
ZFS Phone Home	129.157.65.13 129.157.65.14	ZFS Phone Home	TCP/443	ZFS fault monitoring is shipped direct to these Oracle systems. Used when Oracle Advanced Support Gateway hosts a proxy

Destination	Destination IP Address (es)	Application Protocol	Network Protocol/Port	Purpose
	141.146.1.169			server for the ZFS Storage Heads.
Oracle Public Cloud Object Store, that is, objectstorage.*. oraclecloud.com, where * is a location	Oracle recommends that customers open the firewall corresponding to the OCI site closest to the Gateway location. Select one of the following OCI sites: ■ ap-tokyo-1: ■ 134.70.80.0/22 ■ eu-frankfurt-1 ■ 134.70.40.0/21 ■ 134.70.48.0/22 ■ uk-london-1 ■ 134.70.56.0/21 ■ 134.70.64.0/22 ■ us-ashburn-1 ■ 134.70.24.0/21 ■ 134.70.32.0/22 ■ sa-saopaulo-1 ■ 134.70.84.0/22	HTTPS	TCP/443	Object Store content download to provide software and patches for the Oracle Advanced Support Gateway for Cloud at Customer system.
DNS servers for oraclecloud.com	■ 216.146.35.35 ■ 216.146.36.36	DNS	TCP/UDP 53	To resolve Oracle Object Store IP addresses hosted within Oracle Cloud Infrastructure (OCI).
oauth-e.oracle.com	■ 156.151.58.70 ■ 209.17.4.26 **Note -** 156.151.58.70 and 209.17.4.26 are multiple IP addresses used to service oauth-e.oracle.com. DNS resolution may return a different IP address.	HTTPS	TCP/443	To provide support for Oracle centralized authentication for Oracle Enterprise Manager.

Destination	Destination IP Address (es)	Application Protocol	Network Protocol/Port	Purpose
	Ensure access is granted for each IP directly.			

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 Oracle Advanced Support Gateway. If the alternative VPN solution is used, the following traffic must be allowed to communicate over the VPN.

TABLE 2 Firewall Rules between Oracle Advanced Support Gateway and the Oracle Data Center Using VPN Tunnel

Source	Destination	Network Protocol/Port	Purpose
Oracle Advanced Support Gateway	■ 192.206.43.197/32 ■ 198.51.38.199/32	NTP (UDP/123)	Network Time Protocol (NTP)
Oracle Advanced Support Gateway	■ 192.206.43.194/32 ■ 198.51.38.197/32	Syslog (TCP/514)	Oracle Advanced Support Gateway Syslog
Oracle Advanced Support Gateway	198.51.38.194/32	HTTPS (TCP/8080,9898)	Oracle Advanced Support Gateway file integrity monitoring
198.51.38.193/32	Oracle Advanced Support Gateway	HTTPS (TCP/8080,9898)	Oracle Advanced Support Gateway file integrity monitoring
■ 192.206.43.209/32 ■ 198.51.38.209/32 ■ 140.85.164.34/32	Oracle Advanced Support Gateway	Security Scanner ■ TCP/UDP/1-65535 ■ ICMP (Types 8 & 0)	Oracle Advanced Support 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	Oracle Advanced Support Gateway	■ ICMP (Types 8 & 0) ■ SSH (TCP/22) ■ HTTPS (TCP/443, 7799,9702) ■ SGD (TCP/5307)	Management traffic to remotely manage Oracle Advanced Support Gateway and also facilitate remote access
Oracle Advanced Support Gateway	■ 192.206.43.196/32 ■ 198.51.38.198/32	HTTPS (TCP/443)	REST services for Oracle Advanced Support Gateway

Source	Destination	Network Protocol/Port	Purpose
Oracle Advanced Support Gateway	■ 192.206.43.193/32 ■ 198.51.38.196/32	LDAP (TCP/636)	Oracle Advanced Support Gateway authentication (LDAP)

Firewall Rules for Oracle Cloud at Customer Machine to the Customer Network

The ports outlined in this table are required for accessing the Oracle Cloud at Customer system and for the system to access the services required.

TABLE 3 Firewall Rules between Oracle Cloud at Customer Machine and the Customer Network

Source	Destination	Network Protocol/Port	Purpose
Customer Shared IP Pool	Customer DNS	DNS Forwarding (UDP/53; TCP/53)	DNS forward is required to forward all lookups to non-oraclecloudatcustomer.com domains.
Customer DNS	Customer Shared IP Pool	DNS Forwarding (UDP/53; TCP/53)	DNS forward is required to forward all lookups to oraclecloudatcustomer.com domains that are Cloud Service endpoints on Oracle Cloud at Customer Machines.
Customer Shared IP Pool	Customer SMTP	SMTP (TCP/25 (or 587, 465, customer defined in PCMA, the Oracle Cloud at Customer configuration assistant))	Cloud notification and registration emails.
Customer Management Laptop	Customer Shared IP Pool	HTTPS (TCP/443)	Customer management of their Oracle Cloud at Customer Machine environment.

Firewall Rules for Oracle Exadata Cloud at Customer Machine to the Customer Network

The ports outlined in this table are required for accessing the Oracle Exadata Cloud at Customer system and for the system to access the services required.

TABLE 4 Firewall Rules between Oracle Exadata Cloud at Customer Machine and the Customer Network

Source	Destination	Network Protocol/Port	Purpose
Database client access network (as defined in PCMA, the Oracle Exadata Cloud at Customer Machine configuration assistant)	Customer NTP	NTP (UDP/123)	Oracle Exadata Cloud at Customer Machine DomU client network to the customer NTP server.

Firewall Rules Between the Gateway and Fusion Applications (SaaS at Customer)

This section provides a table showing the internal firewall rules between Oracle Advanced Support Gateway and Oracle Fusion Applications (SaaS at Customer.)

TABLE 5 Firewall Rules Between the Gateway and Fusion Applications (SaaS at Customer)

Application Protocol	Source Interface(s)	Destination Interface(s)	Network & Network Protocol/Port	Purpose
ICMP	Oracle Advance Support Gateway	Fusion Application DomU/ VMs	Tenant network ICMP/Echo, Reply	Used to test network connectivity between Oracle Cloud Machine systems and Oracle Advance Support Gateway
SSH	Oracle Advance Support Gateway	Fusion Application DomU/ VMs	Tenant network TCP/22	Supports user access to monitor configuration, review diagnostics (logs, thread dumps, JFR heap dump), operations/support and patching of Fusion Applications DomU's/VM's
HTTPS	Fusion Application DomU/ VMs	Oracle Advance Support Gateway	Tenant network TCP/1159	Agent communication, upload monitoring, lifecycle management (LCM), decoupled target discovery process
HTTPS	Oracle Advance Support Gateway	Fusion Application DomU/ VMs	Tenant network TCP/1830	OEM agent communication for Fusion Applications monitoring and support
HTTPS	Oracle Advance Support Gateway	Fusion Application DomU/ VMs	Tenant network TCP/ 7001, 7401, 7801, 8201, 8601, 9001, 9401, 9801, 10201, 11201, 17001, 10600-10625, 11401, 10663	Oracle WebLogic Server administration and operational support for Fusion Applications Connectivity is over HTTPS and exclusively connects to administration

Application Protocol	Source Interface(s)	Destination Interface(s)	Network & Network Protocol/Port	Purpose
				ports of Fusion Applications domains
SQLNet	Oracle Advance Support Gateway	Fusion Application DB hosts/Oracle Database Exadata Cloud at Customer (ExaCC)	Tenant network TCP/1521-1530	Target database discovery from Oracle Enterprise Manager for monitoring and ongoing support of the database

Audit Logging Feature

The Audit Logging Feature of Oracle Advanced Support Gateway provides audit information for three different categories of system events. The three 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 Oracle Advanced Support Gateway. This is done by monitoring usage of the `ssh` and `telnet` system binaries. Oracle Advanced Support Gateway sends a message that `ssh` or `telnet` 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 Oracle Advanced Support Gateway.
- Inbound Oracle Advanced Support 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.

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.

The audit logging feature is disabled by default, and must be explicitly enabled through the Oracle Advanced Support Gateway command line interface (CLI). The details of how to configure this feature are explained in the following section:

Initial Login.

1. Use `ssh` to connect to Oracle Advanced Support Gateway.

   Use the customer administrator account configured at installation time or any other user with the customer administrator role.
2. At the first (CLI or CLISH) prompt, enter the password.
3. At the next prompt enter **`configure terminal`**.
4. At the next prompt enter **`syslog`**.

   You are now in the syslog-specific section of the Oracle Advanced Support Gateway CLI where you can configure forwarding.

Available Commands.

Command	Description
`help`	To display a list of available commands.
`?`	To display a brief explanation of how to enter commands in the CLI.

`stat`	To display the current configuration.
	This produces a display similar to the following:
	`------------ SyslogBroadcaster Configuration ------------`
	`Message Forward Status = enabled`
	`Host IP Address = 1.2.3.4`
	`Host Port Number = 514`
	`Host Time Zone = GMT`
	`firewall Message Forward = enabled`
	`ssh Message Forward = enabled`
	`session Message Forward = enabled`
	`UID/GUID MapICMP Type 0 and 8 = enabled`
	`-----------------------------------------------------------`

`forward enable`	To enable syslog forwarding.
`forward disable`	To disable syslog forwarding.
`ip` <*ip address*>	To enter the IP address of the remote syslog server (the one receiving the forwarded messages). You must enter a valid IP address, not a host name.
`port` <*port #*>	To change the port used for forwarding syslog messages.
`timezone` <*value*>	To set the time zone used in the forwarded syslog messages. Value must be -12 to +12 which is the offset from GMT.

`mapping enable`
`mapping disable`
	To convert the uid and guid contained in each message to the corresponding Unix user and group name.

Enabling and Disabling Logging Messages

The following paragraphs show the commands to enable and disable logging messages, and provide examples of the resulting 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.

Any combination of the following three categories can be enabled or disabled.

Outbound Network Connectivity.

- To enable or disable this type of message forwarding:

  ```
  firewall enable
  ```

  ```
  firewall disable
  ```

These messages are generated by iptables 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 `nslookup` command:

```
Jul 31 15:10:01 Jul-31 15: 10:01 GMT+00:00 0:0:0:0:0:0:0:1 NA:
sample-host kernel: iptables: IN= OUT=eth0 SRC=nn.nn.nn.nn
DST=nn.nn.nn.nn LEN=59 TOS=0x00 PREC=0x00 TTL=64 ID=33101 DF
PROTO=UDP SPT=30849 DPT=53 LEN=39 UID=jsmith GID=admin
```

Result from an `ssh` command:

```
Jul 31 15:13:22 Jul-31 15: 13:22 GMT+00:00 0:0:0:0:0:0:0:1 NA:
sample-host kernel: iptables: IN= OUT=eth0 SRC=nn.nn.nn.nn
DST=nn.nn.nn.nn LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=46937 DF
PROTO=TCP SPT=54842 DPT=22 WINDOW=14600 RES=0x00 SYN URGP=0 UID=jsmith GID=admin
```

Outbound Login Activity

- To enable or disable this type of message forwarding:

  ```
  ssh enable
  ```

  ```
  ssh disable
  ```

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

Result from an `ssh` command:

```
Jul 31 15:22:15 Jul-31 15: 22:14 GMT+00:00 0:0:0:0:0:0:0:1 NA:
sample-host audispd: node=sample-host type=SYSCALL
msg=audit(1437567767.027:17839321): arch=c000003e syscall=59
success=yes exit=0 a0=124e030 a1=123d7f0 a2=1246d90 a3=10
items=2 ppid=22614 pid=25252 auid=54373 uid=jsmith gid=admin euid=54373
suid=54373 fsuid=54373 egid=501 sgid=501 fsgid=501 tty=pts4 ses=90594
comm="ssh" exe="/usr/bin/ssh"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="gateway_audit"
```

Oracle Advanced Support Gateway User Login Activity.

- To enable or disable this type of message forwarding:

  `session enable`

  `session disable`

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

Example of `ssh` being invoked on Oracle Advanced Support Gateway:

```
Aug 1 21:37:02 Aug-01 17: 37:02 GMT-04:00 0:0:0:0:0:0:0:1
NA: sample-host audispd: node=sample-host type=SYSCALL
msg=audit(1375393022.626:187186): arch=c000003e syscall=59 success=yes
exit=0 a0=7fa860e69380 a1=7fa860e697e0 a2=7fa860e69ca0 a3=0 items=2
ppid=1428 pid=12967 auid=4294967295 uid=jsmith gid=admin euid=0 suid=0 fsuid=0
egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 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 Oracle Advanced Support 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"
```