Oracle Gen 2 Exadata Database Service on Cloud@Customer Security Controls

ORACLE

Exadata Database Service on Cloud@Customer Security Controls

A Technical Summary for Security Approvers and Developers

December 8, 2025 | Version 2.35

PURPOSE STATEMENT

This document provides an overview of features and enhancements included in releases 25.1.7.0.0.250711 and 24.1.14.0.0.250706[1] It is intended solely to help you assess the business benefits of upgrading to 25.1.7.0.0.250711 and 24.1.14.0.0.250706 and to plan your I.T. projects.

This document summarizes the security features the Oracle Exadata Database Service on Cloud@Customer[2] (ExaDB-C@C) delivered through the Gen 2 Oracle Cloud Infrastructure (OCI) control plane. It is intended for security staff chartered at evaluating adoption of ExaDB-C@C, which requires the following service delivery mechanics:

- Oracle chooses the staff that are authorized to connect to the ExaDB-C@C infrastructure
- Oracle is the identity provider for the staff accessing the ExaDB-C@C infrastructure
- Oracle staff use Oracle provided software and hardware to access to the infrastructure
- Oracle staff perform infrastructure maintenance, including periodic superuser (root) access
- Oracle staff access components necessary to perform diagnosis and resolution of service issues

You can use Oracle Operator Access Control[3] and Delegate Access Control[4] to control Oracle staff access to your Oracle-managed infrastructure and your VMs. These privileged access management services provide OCI interfaces for entitlement management, Oracle Linux security software for privilege enforcement, and Oracle Linux audit for command and keystroke logs. These services provide access

- Only when asked for by Oracle and approved by you
- Only for the duration necessary to perform the work
- Using temporary, minimum privileged credentials
- Using temporary networks, ssh tunnels, and bastion servers

DISCLAIMER

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. 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.

Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

[1] https://support.oracle.com/knowledge/Oracle%20Database%20Products/2333222_1.html
[2] https://www.oracle.com/engineered-systems/exadata/cloud-at-customer/
[3] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-7CF13993-DB16-485A-A9FA-399E0049740B
[4] https://docs.oracle.com/en-us/iaas/delegate-access-control/doc/overview-of-delac.html

TABLE OF CONTENTS

LIST OF IMAGES

LIST OF TABLES

INTRODUCTION

Exadata Database Service on Cloud@Customer (ExaDB-C@C) provides Exadata as a managed cloud service in your data center. You get all Exadata features, OCI orchestration, and Oracle support. This paper describes the security controls built into the service. These controls follow industry best practices and Oracle corporate security standards to protect user data and mission-critical workloads. If your current security standards differ, this paper suggests alternative controls so you can update or adjust your policies and grant exceptions when necessary.

ROLES AND RESPONSIBILITIES

ExaDB-C@C follows a shared responsibility model where you and Oracle each manage specific aspects of the system. Responsibilities are separated as follows:

Your services:

- Virtual machines (VM)
- Databases running within them

Oracle managed infrastructure:

- Physical servers (Exadata Database and Storage Servers)
- Storage networking switches
- Out of band (OOB) management switches

- Power Distribution Units (PDUs)

Oracle managed cloud control plane:

- Web UI and API interfaces
- Public OCI endpoints (e.g., service APIs)
- Private endpoints (e.g., OCI Fast Connect)
- OCI cloud automation for service lifecycle management

You are responsible for securing, monitoring, and managing access to your VMs and databases. You manage authentication to you VMs and Oracle Databases using standard operating system and database tools.[5] Oracle controls and monitors access to Oracle-managed infrastructure components. Oracle staff are not authorized to access your VMs and databases, save certain support exceptions detailed in Exception Workflows - Oracle Access to Customer VM. Detailed breakdowns of roles and responsibilities are provided in Table 1, ExaDB-C@C Service Description,[6] and ExaDB-C@C Explanation of Services.[7]

Table 1: Roles and Responsibilities

WORK FUNCTION	ORACLE MANAGED INFRASTRUCTURE		YOUR MANAGED SERVICES	
	Oracle Cloud Ops	Your Staff	Oracle Cloud Ops	Your Staff
Monitoring	Infrastructure, Control Plane, Hardware Faults, Availability, Capacity	Provide network access to support Oracle infrastructure log collection and monitoring	Infrastructure availability to support your monitoring of your services	Monitoring of your OS, Databases, Apps
Incident Management & Resolution	Incident Management and Remediation Spare Parts and Field Dispatch	Onsite Diagnostic Assistance (e.g., network troubleshooting)	Support for any incidents related to the underlying platform	Incident Management and resolution for Customer's Apps
Patch Management	Proactive patching of Hardware, IaaS/PaaS control stack	Provide network access to support patch delivery	Staging of available patches (e.g., Oracle DB patch set)	Patching of tenant instances Testing
Backup & Restoration	Infrastructure and Control Plane backup and recovery, recreate your VMs	Provide network access to support cloud automation delivery	Provide running and customer accessible VM	Snapshots / Backup & Recovery of customer's IaaS and PaaS data using Oracle native or 3rd party capability
Cloud Support	Response & Resolution of SR' related to infrastructure or subscription issues	Submit SRs via MOS	Response & Resolution of SR	Submit SRs via Support Portal

[5] https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/exaconnectingDB.htm
[6] https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/exadata/doc/ecc-system-config-options.html
[7] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2707015.1

EXADB-C@C SERVICE ARCHITECTURE

Figure 1 shows the ExaDB-C@C architecture block diagram. The service is deployed in an Exadata rack in your data center. The rack contains all the components of a standard Exadata Database Machine, plus 2 Control Plane Servers (CPS) in a highly available (HA) configuration. The CPS connect the Exadata rack to the OCI Control plane so that you and Oracle can manage the service.[8]

The service helps to secure your data in the ExaDB-C@C rack on your premises. Access to your databases is made using network connections you control. You control the credentials that can authenticate your VMs and databases. You have root-level and SYS-level access to your virtual machines and databases. You can set security policies, install agents, forward logs, and manage identities to help you comply with regulations.

An OCI region you choose delivers ExaDB-C@C lifecycle management functionality, including cloud automation for operating system and database management, and infrastructure maintenance and support. You control cloud automation functionality with OCI Identity and Access Management (IAM). OCI Audit provides you with a record of all your management actions invoked via the OCI Console or OCI REST endpoints, such as creating and deleting databases, and scaling OCPUs. You control network access from the Control Plane Server to the required OCI management endpoints. Preparing for Exadata Database Service on Cloud@Customer[9] describes network requirements for the service. You can allow Oracle to control Oracle staff access to the infrastructure, or you can control Oracle staff with Operator Access Control.

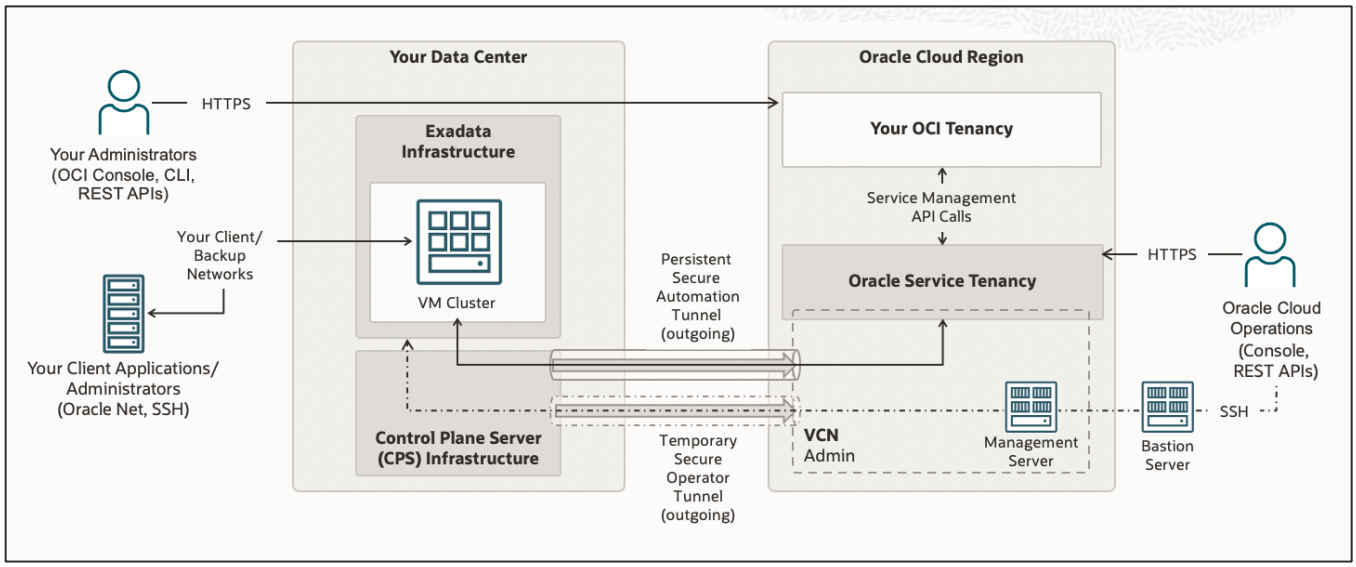

Figure 1: Architecture Block Diagram for Oracle ExaDB-C@C

Network Architecture

Figure 2 shows the physical network implementation.[10] The components you control are shown in blue. The components that Oracle controls are shown in red. An isolated layer 2 management network interconnects the infrastructure components (red). There is no direct network access from the management or storage networks to your client and backup networks. Nominally, the Exadata Database Server does not have an IP address configured (plumbed) on your client or backup networks. The ExaDB-C@C control plane software temporally configures IP addresses on the Exadata Database Server to perform network validation checks on the Client and Backup networks when you create a VM Cluster Network resource.[11]

---

[8] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/eccid/exacc_overview.html

[9] https://docs.oracle.com/en-us/iaas/exadata/doc/eccpreparing.html#GUID-A29A2B1C-708F-4AF2-BE6E-0B4916F6CB25

[10] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/eccid/exacc_netinterfaces.html

[11] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-setting-up-the-network.html#GUID-C1F49BDB-1249-4AE7-9ECB-7AEC406F05ED

You connect the Exadata Database Server client and backup network ports to your layer 2 switch using 10Gb or 25Gb Ethernet. You control the VLAN tags for these networks. The Exadata Database Server host operating system implements highly available network connections for the VM with an active/standby configuration. You can optionally implement LACP.

Your VM accesses Exadata Storage through a private, non-routed interconnect network with SR-IOV mapped interfaces (yellow). Each physical Exadata Database Server and Storage Server has an HA (active/standby) connection to redundant storage networking switches. The default storage network configuration is 100.107.0.0/24. You can override this CIDR block with an arbitrary IP address range if required.

ADB-D services may be run on the ExaDB-C@C service. When ADB-D services are deployed, the following updates are applied to the ExaDB-C@C service:

- The Customer VM becomes the ADB-D VM, and Oracle retains control to log into the ADB-D VM (token-based `ssh` as a named user) to support the ADB-D service; you may not access the ADB-D VM per the ADB-D service definition; you can use Operator Access Control to control Oracle access to the ADB-D VM
- ADB-D configures a second persistent Secure Outgoing Tunnel Service to ADB-D-specific management endpoints
- ADB-D configures a separate temporary Secure Operator Tunnel Service to ADB-D-specific endpoint for remote `ssh` access to the ADB-D VM

Oracle enforces separation of duties between ExaDB-C@C infrastructure operations and ADB-D operations.

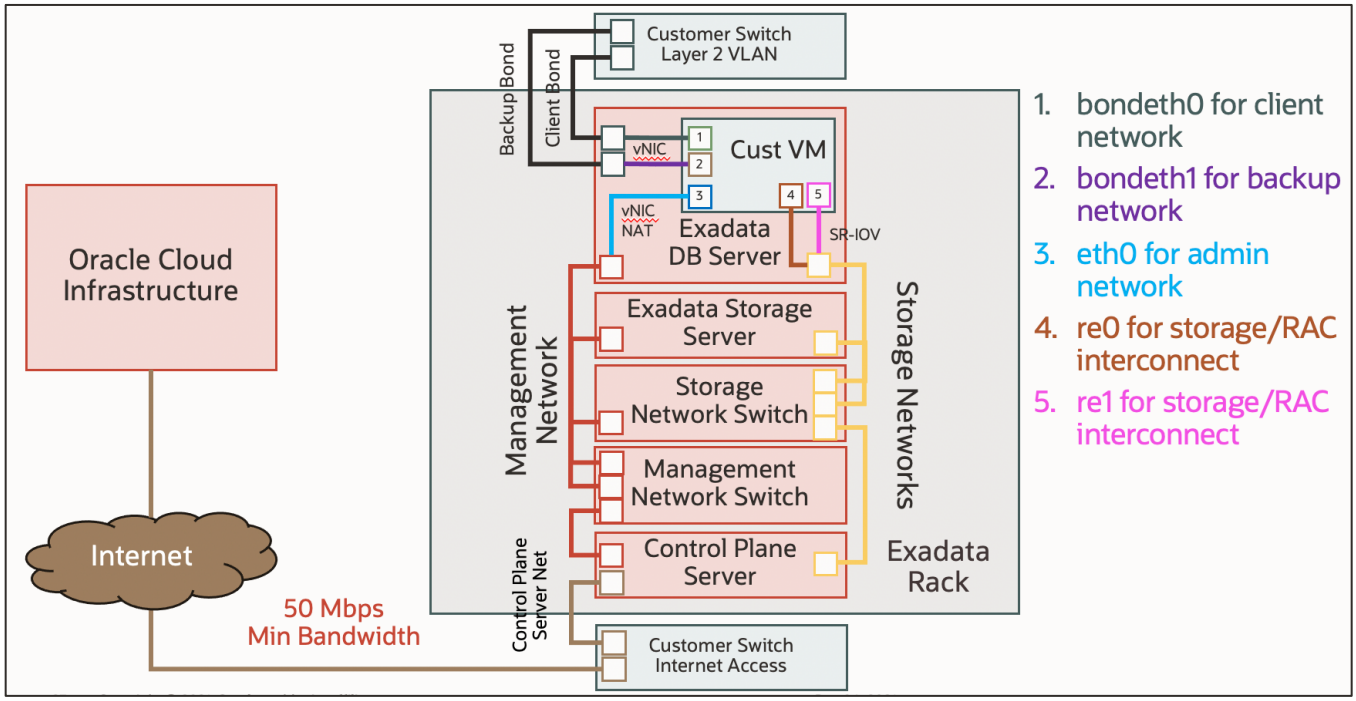

Figure 2: ExaDB-C@C physical network implementation

Figure 3 shows the CPS networking architecture. The CPS reaches the Internet via a layer 2 Ethernet connection through your switches, routers, and proxy servers.[12] Table 2 and Network Requirements for Exadata Cloud@Customer[13] show the URLs required for service delivery. Access to URLs is outbound on port 443 only. The table indicates TLS protocol version and certificate authority for each URL. You can impose network access rules to deny inbound access to the CPS and to only permit outbound access to required Oracle endpoints. The service supports `http` proxy (e.g., corporate proxy, passive proxy) to manage connections from the CPS to OCI endpoints. ExaDB-C@C does not support challenge proxies or SSL decryption (traffic inspection). You may need to update your permitted URLs when Oracle adds new features to the service. If you use IP address filtering you must allow traffic to all the relevant IP CIDR ranges associated with your OCI region.[14] Figure 5 shows examples of how infrastructure software processes access OCI endpoints.

[12] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/eccid/exacc_network.html
[13] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-network-requirements.html#GUID-F06BD75B-E971-48ED-8699-E1004D4B4AC1
[14] https://docs.oracle.com/en-us/iaas/tools/public_ip_ranges.json.

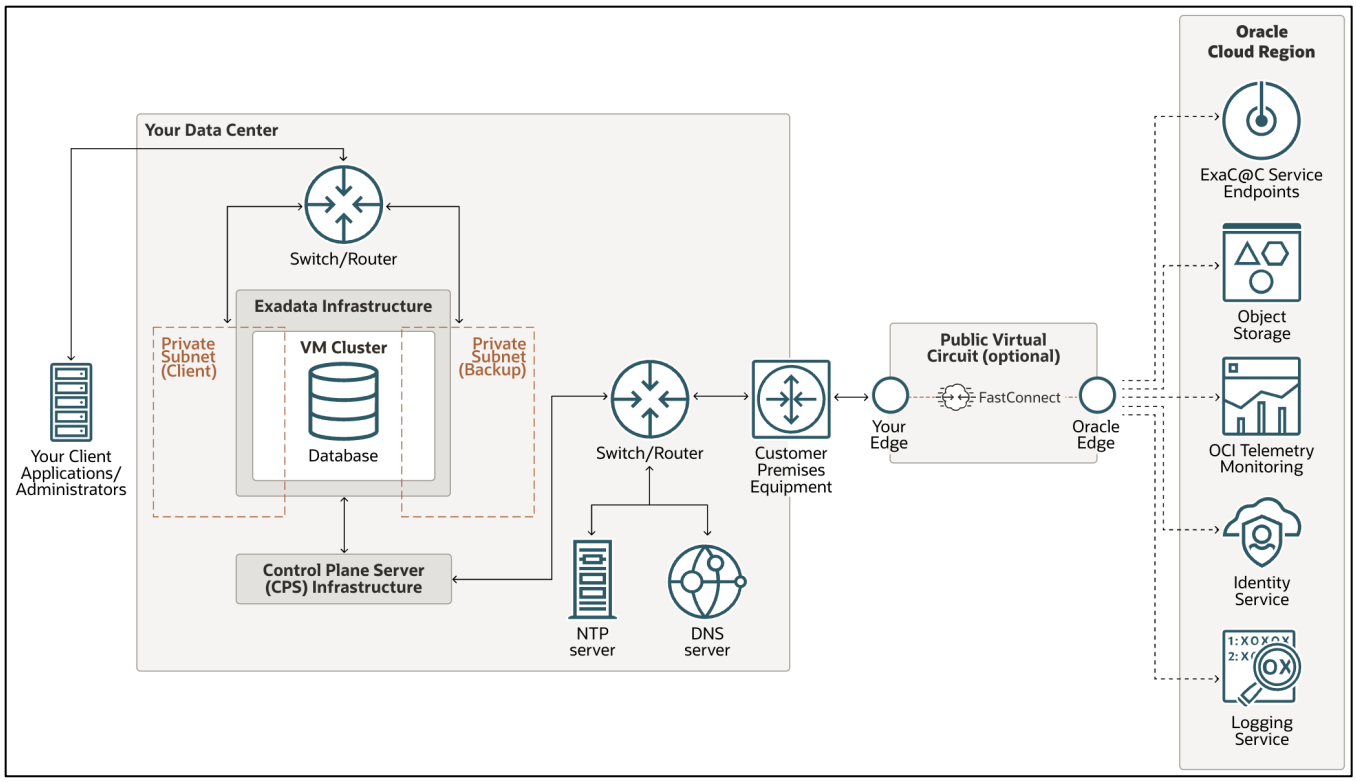

Figure 3: Control Plane Server networking

Table 2: Required URLs for service delivery- all access is outbound on port 443

DESCRIPTION/PURPOSE	TLS VERSION	CERTIFICATE AUTHORITY	LOCATION REPLACE *OCI_REGION* WITH YOUR REGION[15]
Persistent Outgoing Tunnel Service for cloud automation Delivery	1.3	DigiCert	https://wss.exacc.*oci_region*.oci.oraclecloud.com
Persistent Outgoing Tunnel Service for Autonomous Database Dedicated (ADB-D) cloud automation Delivery; TLS 1.3 protocol	1.3	DigiCert	https://wsshe.adbd-exacc.*oci_region*.oci.oraclecloud.com
Temporary Secure Tunnel Service for remote Oracle operator access supporting ExaDB-C@C Infrastructure; TLS 1.2 protocol	1.2	DigiCert	https://mgmthe1.exacc.*oci_region*.oci.oraclecloud.com https://mgmthe2.exacc.*oci_region*.oci.oraclecloud.com
Temporary Secure Tunnel Service for remote Oracle operator access for ADB-D resources; TLS 1.3 protocol	1.3	DigiCert	https://mgmthe.adbd-exacc.*oci_region*.oci.oraclecloud.com
Object Storage Service to retrieve system updates; TLS 1.2 protocol	1.2	DigiCert	https://objectstorage.*oci_region*.oraclecloud.com https://swiftobjectstorage.*oci_region*.oraclecloud.com https://*.objectstorage.oci_region.oci.customer-oci.com

[15] https://docs.oracle.com/en-us/iaas/Content/General/Concepts/regions.htm

Monitoring Service to record and process Infrastructure Monitoring Metrics (IMM)	1.2	DigiCert	https://telemetry-ingestion.*oci_region*.oraclecloud.com
Identity Service for name resolution of Oracle operators	1.2	DigiCert	https://identity.*oci_region*.oraclecloud.com https://auth.*oci_region*.oraclecloud.com
Logging Service for application and security logs	1.2	Oracle PKISVC CrossRegion Intermediate r2[16]	https://frontend.logging.ad1.oci_region.oracleiaas.com https://frontend.logging.ad2.oci_region.oracleiaas.com https://frontend.logging.ad3.oci_region.oracleiaas.com https://controlplane.logging.ad1.*oci_region*.oracleiaas.com https://controlplane.logging.ad2.*oci_region*.oracleiaas.com https://controlplane.logging.ad3.*oci_region*.oracleiaas.com
Resource Principal based authentication and Autonomous Database service delivery	1.2	DigiCert	https://database.*oci_region*.oraclecloud.com
VM Console	1.2	DigiCert	https://console1.exacc.*oci_region*.oci.oraclecloud.com https://console2.exacc.*oci_region*.oci.oraclecloud.com
Monitoring Service to record and process Infrastructure Monitoring Metrics (IMM) resources	1.2	DigiCert	https://ingestion.logging.region.oci.oraclecloud.com
Metering and Monitoring	1.2	DigiCert	https://*.functions.oci_region.oci.oraclecloud.com

You can use other OCI services with your ExaDB-C@C service, including:

- FastConnect17 or site-to-site VPN18,19 to connect your ExaDB-C@C infrastructure to OCI.
- Transit Routing20 and Network Security Lists21 to help control ExaDB-C@C infrastructure access to OCI services.
- VCN Flow Logs22 to monitor traffic volume to network endpoints
- Network Firewall23 in your Transit VCN to implement allow lists for the URLs and IP addresses required to support the ExaDB-C@C service.

Figure 4 shows the Transit Routing VCN implementation.

[16] PKISVC CrossRegion Intermediate r2 is an Oracle Cloud Infrastructure Certificate Authority (CA) managed by Oracle for Oracle cloud control plane services, such as internal logging systems used by ExaDB-C@C
[17] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/fastconnect.htm
[18] https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/overviewIPsec.htm
[19] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-network-requirements.html#GUID-E53A5DCF-CCCD-4493-B1D2-4EA6FA30B8A1
[20] https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/transitroutingoracleservices.htm
[21] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/securitylists.htm
[22] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/vcn_flow_logs.htm
[23] https://docs.oracle.com/en-us/iaas/Content/network-firewall/overview.htm

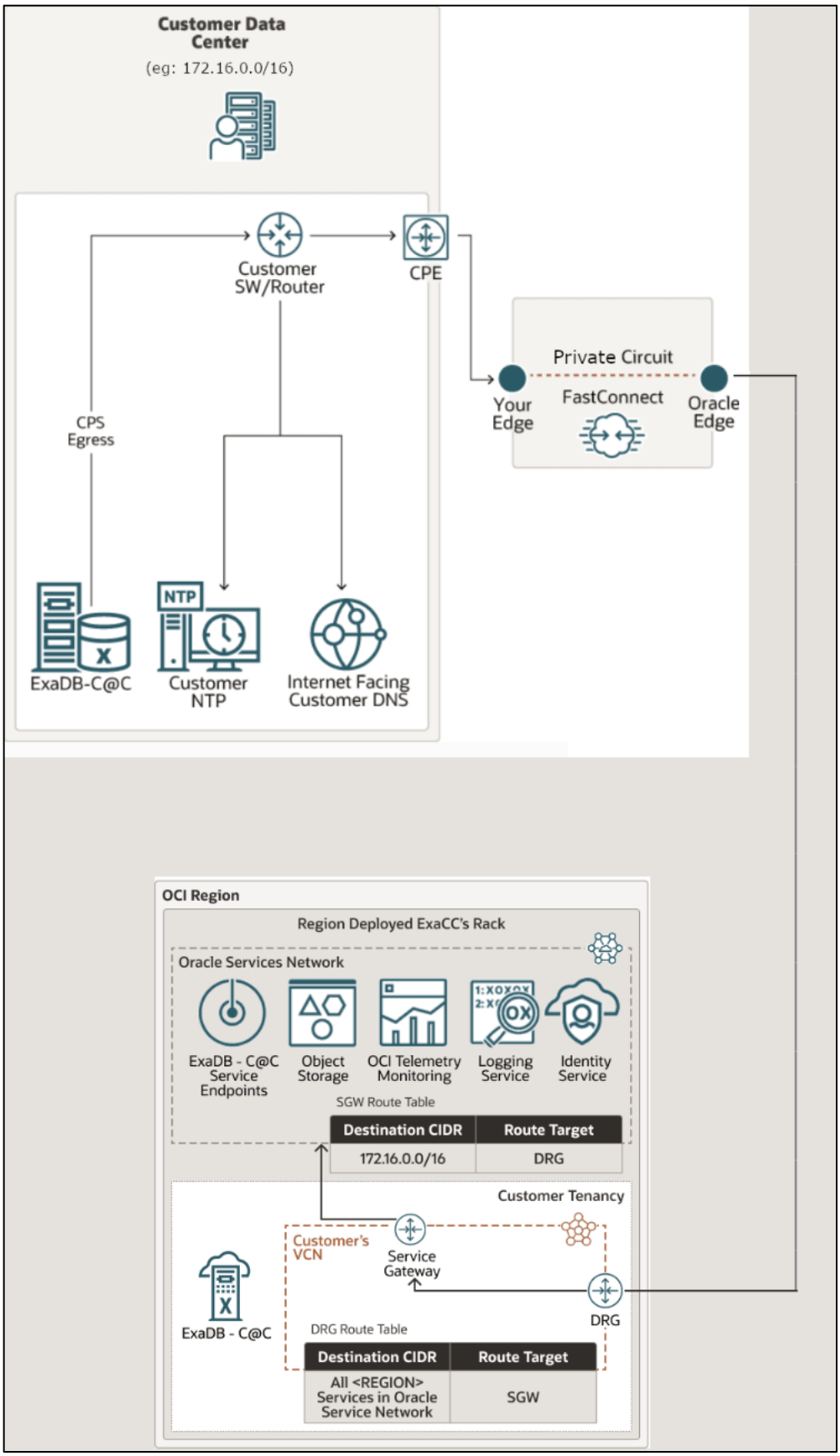

Figure 4: Control Plane Server networking with Transit VCN

Figure 5 shows examples of how software processes manage communication between OCI and the on-premises rack. The Persistent Secure Tunnel Service for Automation Delivery transmits cloud automation commands (REST API calls) and returns minimal diagnostics to assess service availability. The Secure Tunnel Service for Remote Operator Access provides temporary Oracle operator access (ssh) to Oracle Managed Infrastructure and ADB-D resources when applicable. These services are limited to ExaDB-C@C and not part of OCI's public services. Connections to OCI services are temporary and configured just-in-time when they are required for service functionality, such as downloading software updates from object storage, authenticating resource and service principals, and transmitting monitoring and logging records.

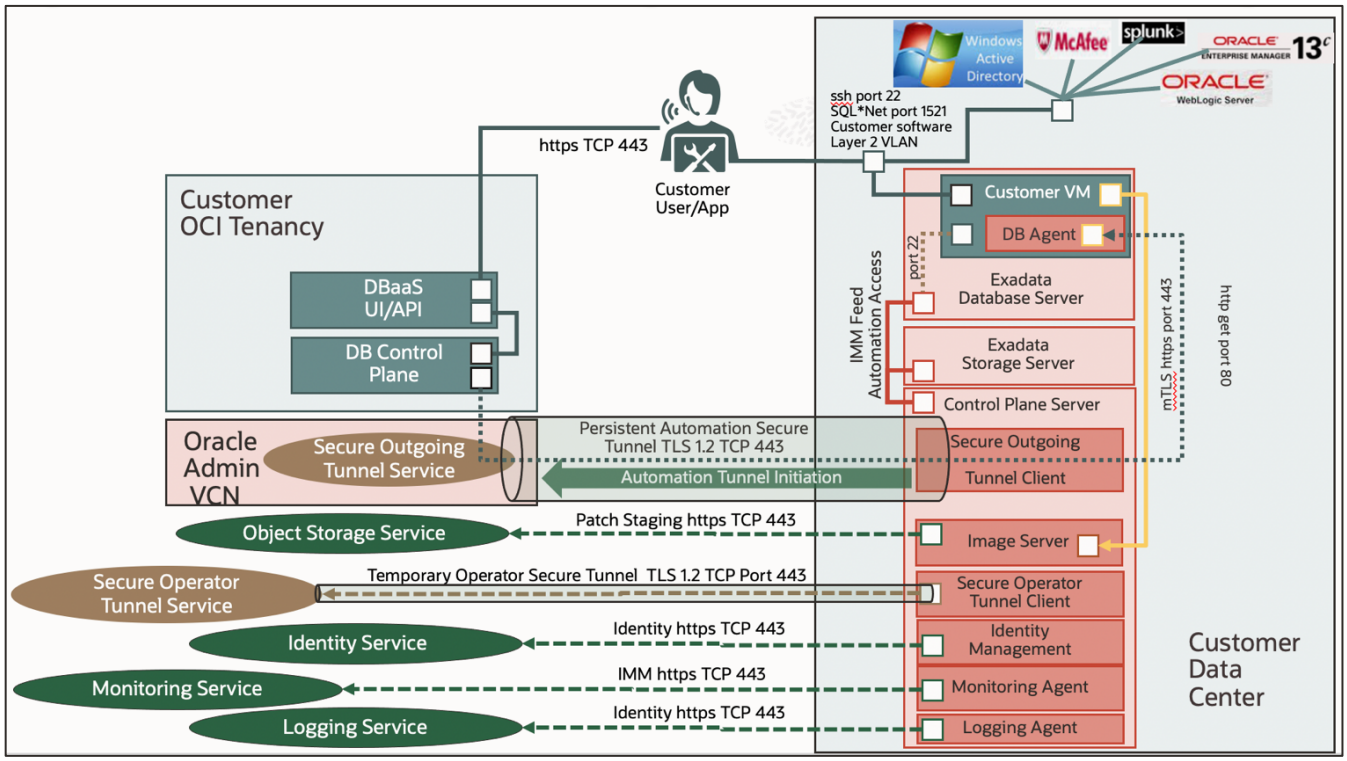

Figure 5: Infrastructure access to OCI services

Oracle manages TLS and mTLS certificates for the connectivity from infrastructure to OCI exclusively. Oracle rotates client certificates for the Persistent Secure Tunnel Service on 6-month schedule. Oracle rotates client certificates for the Secure Tunnel Service for Remote Operator Access on a 15-day schedule. Client certificates are unique to each ExaDB-C@C infrastructure. The subject alternate name (SAN) of the certificates includes the ExaDB-C@C infrastructure Oracle Cloud Identity (OCID).

VM Network and CPU Isolation

Figure 6 shows the network isolation between different Virtual Machine Clusters (VM Clusters) deployed on the same Exadata Database Server (DB Server).[24] VMs share physical links for their client (network 1) and backup (network 2) networks. You can specify different VLAN tags for different networks on different VM clusters to isolate network access. Software automatically configures VLANs to isolate the storage networks of each VM Cluster (networks 4 and 5). The /30 vNIC admin network (network 3) isolates admin networks of different VMs on the same Exadata DB Server. The Exadata Database Server does not route between different admin networks. CPU cores are pinned to specific VMs to help prevent in-VM methods from accessing CPU-cached data from other VMs. You can reference Oracle Database Machine and Compliance with PCI DSS V3.2[25] to see an example of VM cluster network isolation and how it can help you to operate in compliance with PCI DSS.

[24] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/eccid/exacc_vmdb.html

[25] https://www.oracle.com/assets/exadata-pci-dss-compliance-wp-3157442.pdf

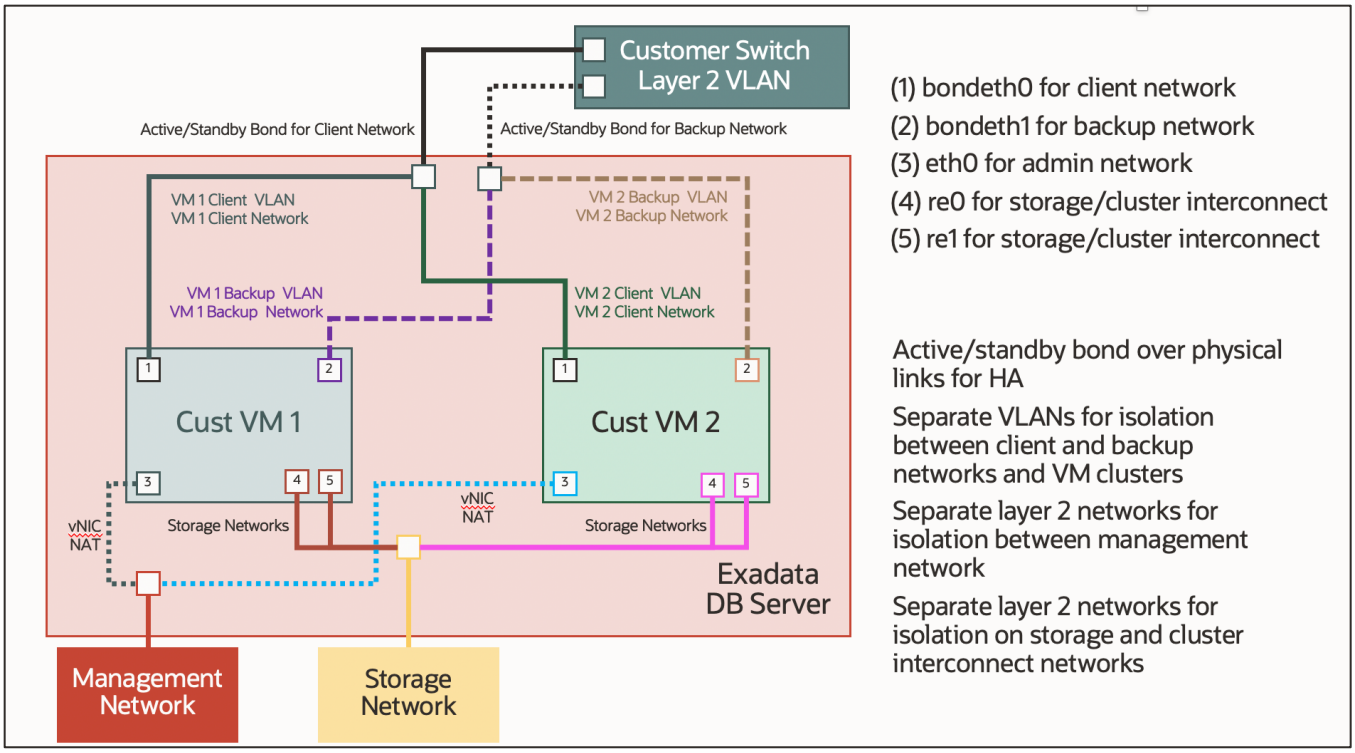

Figure 6: VM Cluster network isolation

CUSTOMIZATION AND THIRD-PARTY SOFTWARE

ExaDB-C@C provides you with privileged access to your environments, including `root` access to guest operating systems and `SYSDBA` access to Oracle Databases. This level of control allows you to make configuration changes and install third-party software. Such changes and additions may lead to exceptions or issues elsewhere in the stack over time.

Oracle will not provide technical support for non-Oracle software. This includes installation, testing, certification, and error resolution. The supplier of the custom/third party software is responsible for any technical support for it. Oracle recommends that all non-Oracle software be certified by the vendor for use in an Oracle Linux and/or Exadata environment and thorough testing is performed in the target environment by you. Details for third party software support on Exadata Database Service are published on My Oracle Support document, Installing Third Party Software on Exadata Components (Doc ID 1593827.1).[26]

If a problem arises, Oracle Support will help diagnose it through the Oracle Service Request (SR) process. Depending on the issue, Oracle may recommend reverting the change. In some cases, particularly those involving third-party software, Oracle may request that the issue be reproduced without the third-party components, following its standard support policies.[27] Oracle support is included with your database service subscription at no additional charge.

Oracle recommends using the service as delivered. The design of Exadata Database Service incorporates oversight from Oracle Corporate Security Architecture[28] and Oracle Software Security Assurance.[29] Following the prescribed service design helps reduce the need for extensive testing, validation, and troubleshooting of changes.

SERVICE LIFECYCLE MANAGEMENT

You use `https` connections to OCI interfaces to manage the service, including:

- Web User Interface (web UI): for ad hoc actions via OCI Console
- Oracle Cloud Shell: a browser-based Linux shell within the OCI Console

[26] https://support.oracle.com/knowledge/Oracle%20Cloud/1593827_1.html
[27] https://support.oracle.com/knowledge/Oracle%20Cloud/1593827_1.html
[28] https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html
[29] https://www.oracle.com/corporate/security-practices/assurance/

- OCI Command Line Interface (OCI CLI): command line interface for scripting and automation
- OCI SDK/RESTAPI: for application integration
- OCI Terraform Provider[30] with documentation provided by Hashicorp[31]

If an OCI identity is authorized to perform a requested action, then the control plane sends the commands to the necessary components through the Secure Automation Tunnel, as follows:

Database operations:
- REST API access to agent software in the VM
- Secured by mTLS
- Transported over the storage network

VM operations:
- Token-based ssh from Control Plane Server processes to service accounts
- Secured by temporary keys managed by the control plane and delivered via agent software in the VM
- Transported over the management network

Infrastructure operations:
- REST API access to agent software in the infrastructure and token-based ssh from the control plane to infrastructure service accounts
- Secured via mTLS and keys managed by the control plane
- Transported over control plane management network

You can also perform some management functionality by accessing the VMs and databases directly. Oracle recommends using OCI interfaces when available to reduce complexity and operational burden, and to improve audit.

Quarterly Software Updates

Oracle Software Security Assurance Practices[32] and Oracle Software Security Assurance[33] standards control Oracle software development. Oracle implements segregation of duties[34] for development, test, quality assurance, and deployment of software. Reference the following documentation for details:

- Oracle Critical Patch Updates for Security Alerts and Bulletins[35]
- My Oracle Support Document 2333222.1 for Exadata Cloud Software Versions[36]
- Oracle Cloud Infrastructure Maintenance documentation[37] for infrastructure updates
- Exadata Cloud@Customer documentation for VM, Grid Infrastructure, and Oracle Database software updates[38]

Oracle stages quarterly software updates for the Oracle Database, Grid Infrastructure, and Linux operating system in OCI Object Storage. These updates are listed in OCI interfaces when they are available. You can schedule maintenance during a period that will have the least impact on your users. OCI interfaces provide full control and visibility over when quarterly maintenance will be applied and functionality to reschedule maintenance when required.[39]

Oracle minimizes the impact of quarterly maintenance on your applications with rolling maintenance operations. This preserves database availability throughout the update process. Rolling maintenance reboots each Database Server, one at a time, with at most one server offline at any time. Applications designed for high availability automatically and transparently migrate their database connections between available database instances without disruption, eliminating the need for scheduling downtime. Storage server updates are also applied in a rolling manner. You can perform offline maintenance, which updates components in parallel to shorten the maintenance window. Databases will not be available during offline maintenance.

---

[30] https://docs.oracle.com/en-us/iaas/Content/API/SDKDocs/terraform.htm
[31] https://registry.terraform.io/providers/hashicorp/oci/latest/docs
[32] https://www.oracle.com/corporate/security-practices/assurance/
[33] https://www.oracle.com/corporate/security-practices/assurance/
[34] https://www.oracle.com/corporate/security-practices/corporate/access-control.html
[35] https://www.oracle.com/security-alerts/
[36] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2333222.1
[37] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-system-config-options.html
[38] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-update-exacc-system.html
[39] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-vw-maint-hist.html

Monthly Infrastructure Security Scanning and Updates

Oracle performs monthly infrastructure security scans and updates[40] to ExaDB-C@C infrastructure to remain in compliance with Oracle corporate security standards. These standards align with and support various industry standards, including PCI-DSS, and government security standards, including FedRAMP High and ISO/IEC 27001. Oracle performs updates to infrastructure online, with no reboot, and designed to have no impact to compatible applications.[41] Oracle applies monthly security updates to Storage Servers in a rolling manner, also designed to have no impact to applications. You may schedule monthly security maintenance at a specific time during the month, albeit in a single maintenance window. Oracle will publish a schedule for monthly maintenance at least one week prior to start of the maintenance period. You may reschedule if required. You are not permitted to access infrastructure components directly, nor can you install monitoring agents or transfer files to Oracle-managed infrastructure.

Oracle Infrastructure Monitoring

Oracle detects and responds to issues that fall within Oracle's operational responsibility,[42] such as:

- Infrastructure security and access control
- Exadata Compute, Storage, and Network infrastructure hardware and software[43] monitoring and maintenance
- Auto Service Request Qualified Engineered Systems Products[44] event monitoring and maintenance

Your ExaDB-C@C automatically sends Infrastructure Monitoring Metrics (IMM) to monitoring systems in the OCI control plane. Oracle support triages this data and assigns tickets to support staff for resolution when required.

Oracle does not monitor components which are not actionable by Oracle, such as:

- Flash Cache usage
- Guest VM security and access logs
- Oracle CRS, ASM, and Database
- Customer software running in the Guest OS

Security Testing and Scanning of Your VM

You may test the security of ExaDB-C@C in accordance with Oracle Cloud Testing Policies.[45] You can use OpenSCAP[46] to scan the VM for compliance. You can use third-party scanning tools to scan your VMs. Your third-party scanning tools and benchmarks should be compatible with the Exadata Database Service software distribution and configuration. In some cases, arbitrary benchmarks flag security issues on the Exadata Database Service VM that are not a material. Reference My Oracle Support Note, "Responses to common Exadata security scan findings (Doc ID 1405320.1)"[47] to learn more about how common benchmarks may be adjusted to work with Exadata. If the Exadata Database Service VM is modified to comply with a benchmark, you should test these modifications to validate that they do not compromise service functionality. Automated software updates, including operating system, Oracle Database, and Grid Infrastructure updates can revert your changes and should be tested prior to production deployment.

PREVENTIVE CONTROLS

Oracle designed ExaDB-C@C to help protect your database data from unauthorized access. The service separates access control duties between you and Oracle, as follows:

- You control access to the physical equipment
- You control access to your OCI tenancy, VMs, databases, and data

---

[40] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-vw-maint-hist.html
[41] https://docs.oracle.com/en/database/oracle/oracle-database/19/racad/ensuring-application-continuity.html#GUID-C1EF6BDA-5F90-448F-A1E2-DC15AD5CFE75
[42] https://support.oracle.com/knowledge/Oracle%20Cloud/2707015_1.html
[43] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2875973.1
[44] https://docs.oracle.com/cd/E37710_01/doc.41/e37287/toc.htm
[45] https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm
[46] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-scap-sec.html.
[47] https://support.oracle.com/knowledge/Oracle%20Database%20Products/1405320_1.html

- Oracle controls logical access to Oracle-managed infrastructure components or you can use Operator Access Control to control to control Oracle's logical access to Oracle-managed infrastructure

You control access to your OCI tenancy, VMs, databases, and data with 3 types of controls:

Authentication and authorization controls

- Credentials to access OCI Console, APIs, and services
- Credentials to VM operating systems and database administration accounts
- Credentials for database users to access databases and database data

Data encryption controls

- Oracle Native Network Encryption or TLS/SSL for application to database network encryption[48]
- Transparent Database Encryption (TDE) for user tablespace[49] data encryption at rest

Network controls

- Your switch and firewall network security controls for layers 2 and 3 access to VMs
- Network access rules implemented in the VM operating system[50] and Oracle Database[51]
- Temporary Delegate Access Control networks and bastion servers to allow Delegate Access Control credentials to authenticate to the VM
- Temporary Operator Access Control networks and bastion servers to allow Operator Access Control credentials to authenticate to the infrastructure.

The ExaDB-C@C software automation does not provide interfaces to configure firewalls, disable network interfaces, or disable cloud automation software agents running in the VM. If you have exceptional security requirements, you can implement such controls using operating system tools; however, you should take care to allow cloud automation functionality that accesses the VM.

Database Security Controls

You can use Oracle Database security controls included in the Oracle Database software, compatible OCI services, and compatible key management systems with ExaDB-C@C, such as:

- Oracle Database authentication
- Oracle Database network encryption
- Oracle Transparent Data Encryption
- Oracle Database Vault
- Database backup encryption
- Data Safe
- Database Security Assessment tool

Database Authentication

You can configure Oracle Database authentication with Centrally Managed Users,[52] including password authentication, Kerberos authentication,[53] or public key infrastructure (PKI) authentication. With centrally managed users, you can manage the authorization for Active Directory users to access Oracle Databases. Oracle Database allows multifactor authentication

---

[48] Exadata Database Service automation configures Oracle Native Network Encryption; Oracle strongly recommends that customers preserve this control

[49] Exadata Database Service automation configured Oracle Transparent Data Encryption (TDE); Oracle strongly recommends that customers preserve this control

[50] https://docs.oracle.com/en/operating-systems/oracle-linux/8/firewall/firewall-AboutPacketFilteringFirewalls.html

[51] https://docs.oracle.com/en/database/oracle/oracle-database/19/netag/configuring-oracle-connection-manager.html#GUID-AF8A511E-9AE6-4F4D-8E58-F28BC53F64E4

[52] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/integrating_mads_with_oracle_database.html#GUID-9739D541-FA9D-422A-95CA-799A4C6F488D

[53] https://support.oracle.com/knowledge/Oracle%20Cloud/2621025_1.html

(MFA) configuration for native users in the form of either push notifications through Oracle Mobile Authenticator (OMA) or Cisco Duo, or certificate-based authentication.[54] You can implement MFA by existing external authentication methods for human users with OCI IAM, MS-EI, and RADIUS.

Network Encryption

ExaDB-C@C encrypts data in flight from the client to the Oracle Database instance with Oracle Native Network Encryption (NNE). NNE is automatically configured for databases created by the service automation. The Oracle Database instance requests encrypted connections from applications[55] and implement an encrypted connection for capable applications. If an application cannot support an encrypted connection, the Oracle Database instance will permit the application to connect without encryption. The service automation does not provide interfaces to configure TLS/SSL for Oracle Database connections. You can configure TLS/SSL and mTLS using operating system tools deployed in the VM.[56] Documentation for Oracle Native Network Encryption and TLS/SSL is published in the Security Guide for each Oracle Database version.[57]

Data at Rest Encryption

ExaDB-C@C encrypts user tablespace data at rest with Oracle Transparent Data Encryption (TDE). TDE is a two-tier key architecture comprising of a data encryption key (DEK) and master encryption key (MEK). The DEK that encrypts table and tablespace data is wrapped by the MEK. The MEK is separated from encrypted data and are stored outside of the database. You can store the TDE MEK in the following:

- PKCS#12 wallet
- Oracle Key Vault
- Compatible third-party HSM

Oracle TDE is engineered to be highly performant. It automatically leverages special instructions in Intel CPUs (AES-NI) to accelerate cryptographic operations. In addition, TDE tablespace encryption works seamlessly with Exadata Hybrid Columnar Compression (EHCC) and Smart Scan technology. With TDE, sensitive user data remains encrypted throughout the database, whether it is in tablespace storage files, temporary or undo tablespaces, or other files such as redo logs. In addition, TDE can encrypt entire database backups. Data Pump and Oracle Recovery Manager (RMAN) both integrate with TDE encrypted data. Details for the TDE implementation on Exadata Database Service are shown in the Exadata Database Machine Cryptographic Services[58] documentation. For further information on Oracle TDE, consult the Advanced Security Guide for the Oracle Database version you are running. The Oracle TDE FAQ[59] provides answers to common Oracle TDE architecture and implementation questions.

Encryption Key Management with PKCS#12 Wallet

The TDE MEK is stored outside of the database, by default in a PKCS#12 compliant container called a 'wallet'. The wallet is stored in file systems accessible by the ExaDB-C@C VMs. Oracle Databases 18c and later allow customers to upload their own, externally generated encryption keys (called Bring-Your-Own-Key, BYOK) into the shared wallet, maintaining separation of duties between the database administrators and key custodians.

---

[54] https://docs.oracle.com/en/database/oracle/oracle-database/23/dbseg/configuring-authentication.html#GUID-10E4F568-0FA3-4F82-99AA-14FB2947469C

[55] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-network-data-encryption-and-integrity.html#GUID-42863092-227B-437C-AFFA-623BE6AEA0EA

[56] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-using-dbaascli.html#GUID-4021F2D5-E822-470D-8570-A28EC650D905

[57] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-network-data-encryption-and-integrity.html#GUID-7F12066A-2BA1-476C-809B-BB95A3F727CF

[58] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/exadata-security-features.html#GUID-FA8A2A69-AEFC-4FE3-959A-A6E584BD1F4F

[59] https://www.oracle.com/database/technologies/faq-tde.html

Encryption Key Management with Oracle Key Vault

You can migrate ExaDB-C@C databases to Oracle Key Vault (OKV).[60] OKV provides continuous online key management to all TDE-enabled databases and encrypted GoldenGate trail files. It also provides the capability to ingest externally generated keys (BYOK). Instructions for using operating system methods to migrate TDE Master Keys to OKV are published in Managing Encryption Keys on External Devices product documentation[61] and Migration of File based TDE to OKV for Exadata Database Service Using Automation via REST (Doc ID 2924192.1).[62] You can use the OKV Persistent Master Encryption Key Cache[63] to enable databases to be operational if the OKV server is unavailable.

Encryption Key Management and Third-Party Hardware Security Modules (HSM)

Oracle Database is compatible with PKCS#11 compatible key management devices.[64] Third-party key management and HSM vendors have used this interface to implement TDE key management for Oracle Databases. Reference My Oracle Support (MOS) note Oracle TDE Support With 3rd Party HSM Vendors (Doc ID 2310066.1)[65] for implementation and support details. ExaDB-C@C automation provides interfaces to configure external key managers.[66]

Integrating an external key manager requires you to install PKCS#11 libraries on your Exadata Database Service VM. Vendors or implementors of the third-party key managers and HSMs build, test, document, and support these integrations. Oracle does not maintain a program for certifying third-party key managers and HSMs with Oracle Databases, and Oracle corporation does not support third-party hardware security modules to provide key management for Transparent Data Encryption-enabled databases.

HSM vendors can self-certify their devices to provide root of trust to Oracle Key Vault. They should refer to "Vendor Instructions for Integrating an HSM as the Root of Trust for Oracle Key Vault" in the Oracle Key Vault Root of Trust HSM Configuration Guide.[67]

Preventing Database Administrators from Accessing User Data with SQL

Oracle Database Vault helps to both protect application data from database administrator access and address privacy and regulatory requirements. You can deploy controls to block database administrator access to application data and control sensitive operations inside the database using trusted path authorization. Oracle Database Vault helps to secure existing database environments transparently, eliminating costly and time-consuming application changes. Documentation for Oracle Database Vault is published in the Oracle Database Vault Administrator's Guide[68] for each database version.

Database Backup Encryption

All backups are encrypted with the same master key used for the Transparent Data Encryption wallet encryption.[69] The encryption key is not stored with the backup. When you use the Autonomous Recovery Service,[70] backups of encrypted

---

[60] https://docs.oracle.com/en/database/oracle/key-vault/21.2/okvag/okv_intro.html#GUID-0D169EB8-C355-459A-9ABD-325CA5B46DD0
[61] https://docs.oracle.com/en-us/iaas/exadatacloud/doc/managing-encryption-keys-on-external-devices.html#GUID-627C83FC-D8A3-4BF2-80F6-70B11DED0C43
[62] https://support.oracle.com/knowledge/Oracle%20Cloud/2924192_1.html
[63] https://docs.oracle.com/en/database/oracle/key-vault/21.7/okvag/security_objects.html#GUID-27DA6A5A-E405-4394-BD0D-C2B213391426
[64] https://docs.oracle.com/en/database/oracle/oracle-database/19/asoag/introduction-to-transparent-data-encryption.html#GUID-2D6C5B27-8E6A-4EF7-AABF-B0FB031C8374
[65] https://support.oracle.com/knowledge/Oracle%20Database%20Products/2310066_1.html
[66] https://docs.oracle.com/en-us/iaas/exadata/doc/manage-and-store-master-encryption-keys-on-an-external-hsm.html#GUID-C40542DB-A167-4503-B0DF-CC1C6DB04882
[67] https://docs.oracle.com/en/database/oracle/key-vault/21.3/okvhm/index.html#Oracle%C2%AE-Key-Vault
[68] For Oracle Database 19c, see https://docs.oracle.com/en/database/oracle/oracle-database/19/dvadm/introduction-to-oracle-database-vault.html#GUID-0C8AF1B2-6CE9-4408-BFB3-7B2C7F9E7284
[69] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html
[70] https://docs.oracle.com/en-us/iaas/recovery-service/index.html

tablespaces, and redo describing changes to these tablespaces, are encrypted.[71] The TDE-encrypted data blocks are encrypted on the database, Recovery Appliance storage, tape devices, and replicated appliances, and when transferred through any network connections.

Automated Database Security Monitoring and Management

You can use software and services compatible with the Oracle database and ExaDB-C@C to monitor and manage your database security posture. Oracle Data Safe is a cloud service you can integrate into your ExaDB-C@C databases. Oracle Database Security Assessment Tool (DBSAT) is standalone software you can download from Oracle and use with your ExaDB-C@C databases.

Oracle Data Safe

You can use Oracle Data Safe[72] to monitor and manage security for your databases. Data Safe and helps you to:

- Assess your database's security configuration
- Detect configuration drift
- Identify high-risk database accounts and view their activity
- Provision audit policies
- Analyze audit data, including generating reports and producing alerts
- Discover sensitive data, including what type of data, how much of it there is, and where the data is located
- Mask sensitive data to remove security risk from non-production databases copies

Oracle Data Safe Technical Architecture[73] shows functionality that supports an on-premises connector deployed on your servers to facilitate connecting databases running on ExaDB-C@C to the OCI Data Safe service. The Data Safe FAQ[74] provides answers to commonly asked questions about Data Safe. There is no additional cost to use Data Safe so long as you do not exceed one million audit records per database in a month.

Oracle Database Security Assessment Tool

The Oracle Database Security Assessment Tool (DBSAT)[75] is a stand-alone command line tool that accelerates the assessment and regulatory compliance process that you can download from Oracle. DBSAT collects relevant configuration information from the database, evaluates the security state, and provides recommendations on how to mitigate identified risks, such as:

- Security configuration issues, and how to remediate them
- Users and their entitlements
- Location, type, and quantity of sensitive data

DBSAT goes beyond simple configuration checking, examining user accounts, privilege and role grants, authorization control, separation of duties, fine-grained access control, data encryption and key management, auditing policies, and OS file permissions. DBSAT applies rules to quickly assess the current security status of a database and produce findings in all the areas above. For each finding, DBSAT recommends remediation activities that follow best practices to reduce or mitigate risk. By applying the comprehensive measurements and compensating controls described by DBSAT, you can help reduce data exposure risk throughout their enterprise.

VM Security Controls

The ExaDB-C@C VM deployment includes a security-hardened operating system based on industry best practices and Oracle security oversight. Security configuration features include:[76]

---

[71] https://docs.oracle.com/en/engineered-systems/zero-data-loss-recovery-appliance/23.1/amagd/data-encryption-techniques.html#GUID-3E1A521B-3B51-4D1F-BF88-27BBE41A4B03
[72] https://docs.oracle.com/en-us/iaas/data-safe/index.html
[73] https://docs.oracle.com/en/solutions/oracle-data-safe-for-on-prem-database/index.html#GUID-07534FC6-3B10-48E5-BD49-C011D55D1070
[74] https://www.oracle.com/security/database-security/data-safe/faq/
[75] https://www.oracle.com/security/database-security/assessment-tool/
[76] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html

Minimal package installation and enabled services:

- Only the necessary packages required to run an efficient system are installed
- Any services that may be installed on the system, but not required for normal operation, are disabled by default
- You may choose to optionally configure services per your requirements

Secure configuration:

- Configuration parameters are set during installation to enhance the security posture of the system
- `ssh` is configured to only listen on certain network interfaces
- `sendmail` is configured to only accept localhost connections
- grub passwords

Secure access methods:

- Accessing Database Servers via `ssh` using strong cryptographic ciphers
- Weak ciphers are disabled by default
- Accessing databases via encrypted Oracle Net connections
- By default, services are available using encrypted channels and a default configured Oracle Net client will use encrypted sessions
- Accessing diagnostics via Exadata MS web interface (https)

Auditing and logging:

- Auditing is enabled for administrative operations
- Audit records may be communicated to external systems for automated review and alerting

Access to the VM is implemented via token-based `ssh`.[77] You use your OCI credentials to add your specified public keys to the `/home/opc/.ssh/authorized_keys` file. Your staff with access to the private key associated with the installed public keys can access the VM as the `opc` user. Oracle cloud automation does not integrate with external key management systems; however, you can manage `ssh` keys using technology compatible with Oracle Linux. Consult with applicable PAM providers for details. You can control add `ssh` key functionality with API Access Control[78] so that an OCI identity seeking to add an `ssh` key must get approval from a different OCI identity.

As of Exadata software version 22.1.4.0.0.221020, you can implement Microsoft Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) for authentication to your VMs. You can configure AD and LDAP using standard operating system tools. You can configure the Linux System Security Services Daemon (SSSD) to facilitate access to your VM using LDAP to provide identity services. Oracle Exadata System Software contains the Linux packages to support SSSD, which you may configure according to your specific requirements. The SSSD support is enabled in conjunction with an Exadata-specific security profile using the Linux `authselect` utility on Oracle Linux 8. Oracle Exadata System Software maintains the existing SSSD configuration details during system updates.[79]

Oracle cloud automation secure login via token-based `ssh` is not compatible with Kerberos authentication.[80] Parts of the Oracle cloud automation functionality will fail if you implement Kerberos authentication in the VM.

VM Default Users

Each ExaDB-C@C VM includes standard privileged service accounts used by Oracle to deliver and maintain the service. Token-based `ssh` login is required. Password-based `ssh` login is disabled.[81] Service accounts include:

- `root:` required by Linux; used for privilege used for software updates and some background processes (e.g., Oracle Trace File Analyzer Agent and ExaWatcher)
- `grid`: owns, runs, and maintains the Oracle Grid Infrastructure software and processes

---

[77] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-connecting-to-exacc-system.html#GUID-C7C5C13C-B518-4FFC-B050-055E5C35EFA0

[78] https://docs.oracle.com/en-us/iaas/oracle-api-access-control/index.html

[79] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmso/linux-sssd-support.html

[80] https://support.oracle.com/knowledge/Oracle%20Cloud/2621025_1.html

[81] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html#GUID-ACA1086F-E46D-4AFA-97B0-EFA0C280784B

- `oracle`: owns, runs, and maintains the Oracle Database software and processes
- `opc`: used by Oracle cloud automation
  - Performs automation tasks
  - Can run certain privileged commands
  - Runs control plane agent software (DBCS Agent and DBCS Admin) for service lifecycle operations
- `dbmadmin`: used with the DBMCLI[82] tool to manage core Exadata features.

Security scanning tools should classify these accounts as service accounts. You can use the `opc` account for administrative purposes, including configuring LDAP or PAM software compatible with the Exadata Database Service software.

Oracle recommends retaining the deployed usernames, userids, group names, and group ids. Changing the Oracle Home user (`oracle`) or Grid Infrastructure user (`grid`) after install is not supported and will cause service exceptions.[83]

VM Default Security Settings

Software deploys the ExaDB-C@C VM with security settings aligned to industry standards and Oracle best practices.[84,85] These configurations help to enforce access control, reduce operational risks, and support automated lifecycle management. Key settings include:

- Password aging and complexity
- Account lockout and session timeout policies
- Deny direct root login via ssh

Technical configurations include:

- `PermitRootLogin` value in `/etc/ssh/sshd_config`, which permits or denies the root user to login through SSH.
  - Default: PermitRootLogin is set to without-password.
  - Recommendation: keep default to permit cloud automation capabilities like OS patching
- `session-limit`: Sets the hard `maxlogins` parameter in `/etc/security/limits.conf`, which is the maximum number of logins for all users. This limit does not apply to a user with `uid=0`.
  - Default: `hard maxlogins 10`
  - Recommendation: keep default
- `ssh-macs`: Specifies the available Message Authentication Code (MAC) algorithms.
- The MAC algorithm is used in protocol version 2 for data integrity protection.
  - Default: hmac-sha1, hmac-sha2-256, hmac-sha2-512 for both server and client
  - Recommendation: keep default
- `password-aging`: Sets or displays the current password aging for interactive user accounts.
  - `-M`: Maximum number of days a password may be used.
  - `-m`: Minimum number of days allowed between password changes.
  - `-W`: Number of days warning given before a password expires.
  - Default: `-M 99999`, `-m 0`, `-W 7`
  - Recommendation: for strict compliance `-M 60`, `-m 1`, `-W 7`

Shell timeouts are configured to allow long-running automation tasks (e.g., ASM rebalance). These values are part of the service configuration and should be allowed by security scanning tools. Oracle recommends customers to retain the deployed settings to reduce testing and maintenance effort, and to avoid service disruption risk caused by configuration changes.

---

[82] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmmn/using-dbmcli-utility1.html
[83] https://docs.oracle.com/en/database/oracle/oracle-database/19/cwwin/about-the-oracle-home-user-for-the-oracle-grid-infrastructure-installation.html
[84] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/security.html
[85] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html#GUID-4F68D138-3778-4AED-B501-3E1108831E9C

VM Default Processes and Certificates

ExaDB-C@C VMs run Oracle software processes that support database operations, including Oracle Database, Oracle Real Application Clusters (RAC), Oracle Trace File Analyzer (TAF), Exawatcher, and Exadata Management Server (MS).[86] Table 3 shows the services and ports. The table indicates the network interface, port number, process description, and certificate authority (CA) for each process. Oracle recommends that you configure security scanners to accept the Oracle CA and Oracle self-signed certificates for Oracle-managed services. These certificates and CAs are built into the service and managed by Oracle to secure the delivery of lifecycle management operations. Accepting them reduces the risk of certificate -related service issues and minimizes operational burden.

Table 3: Default Port Matrix for Guest VM Services

TYPE OF INTERFACE	NAME OF INTERFACE	PORT	PROCESS RUNNING	CERTIFICATE AUTHORITY
Bridge on client VLAN	bondeth0	22	sshd[87]	N/A
		1521 Optionally, customers can assign a SCAN listener port (TCP/IP) in the range between 1024 and 8999. Default is 1521. Note: TNS listener opens dynamic ports after initial contact to well-known ports (1521, 1525).	Oracle TNS listener[88] Receives incoming client connection requests and manages the traffic of these requests to the Database Server. Supports Oracle Native Network Encryption (NNE) and TLS/SSL as transport layer security authentication[89]	Oracle self-signed; customers may add customer-controlled certificates
		5000	Oracle Trace File Analyzer[90] Collector	Oracle self-signed
		7879	Jetty Management Server.[91] Application server engine that is used internally by Oracle Exadata System	Oracle self-signed

[86] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html#GUID-61DB809E-A676-4B11-BF45-35DB89FC87EC
[87] https://docs.oracle.com/en/operating-systems/oracle-linux/openssh/openssh-ConfiguringOpenSSHServer.html
[88] https://docs.oracle.com/en/database/oracle/oracle-database/19/netag/configuring-and-administering-oracle-net-listener.html
[89] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-secure-sockets-layer-authentication.html#GUID-6AD89576-526F-4D6B-A539-ADF4B840819F
[90] https://docs.oracle.com/en/database/oracle/oracle-database/19/atnms/managing-and-configuring-tfa.html
[91] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmso/application-server-update-management-server.html

			Software, in particular Management Server (MS).[92]	
	bondeth0:1	1521 Optionally, customers can assign a SCAN listener port (TCP/IP) in the range between 1024 and 8999. Default is 1521.	Oracle TNS Listener	Oracle self-signed; customers may add customer-controlled certificates
	bondeth0:2	1521 Optionally, customers can assign a SCAN listener port (TCP/IP) in the range between 1024 and 8999. Default is 1521.	Oracle TNS Listener	Oracle self-signed; customers may add customer-controlled certificates
Bridge on backup VLAN	bondeth1	7879	Jetty Management Server	Oracle self-signed
Oracle Clusterware[93,94] running on each cluster node communicates through these interfaces.	clib0/clre0	1525	Oracle TNS listener Oracle Clusterware running on each cluster node communicates through these interfaces.	N/A
		3260	Synology DSM iSCSI	N/A
		5054	Oracle Grid Interprocess Communication	N/A
		7879	Jetty Management Server	Oracle self-signed
		Dynamic Port: 9000-65500 Ports are controlled by the configured	System Monitor service (osysmond) Cluster Logger service (ologgerd)	Oracle self-signed

[92] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmso/management-server-database-servers.html
[93] https://docs.oracle.com/en/database/oracle/oracle-database/19/cwadd/introduction-to-oracle-clusterware.html#GUID-7612C5C2-AC7C-4311-97B2-CF189268969A
[94] https://docs.oracle.com/en/database/oracle/oracle-database/19/rilin/port-numbers-and-protocols-of-oracle-components.html

		ephemeral range in the operating system and are dynamic.	Cluster Health Monitor[95] uses system monitor (osysmond) and cluster logger (ologgerd) services to collect diagnostic data.	
	clib1/clre1	5054	Oracle Grid Interprocess communication	N/A
		7879	Jetty Management Server	Oracle self-signed
Cluster nodes use these interfaces to access storage cells (ASM disks). However, the IP/ports 7060/7070 attached to the storage interfaces are used to access DBCS agent from the Control Plane server.	stib0/stre0	7060	dbcs-admin Cloud agent for handling database lifecycle operations[96]	Oracle self-signed
		7070	dbcs-agent Cloud agent for handling database lifecycle operations[97]	Oracle self-signed
	stib1/stre1	7060	dbcs-admin	Oracle self-signed
		7070	dbcs-agent	Oracle self-signed
Control Plane server to domU	eth0	22	sshd	N/A
Loopback	lo	22	sshd	N/A
		2016	Oracle Grid Infrastructure	N/A
		6100	Oracle Notification Service (ONS),[98] part of Oracle Grid Infrastructure	N/A

[95] https://docs.oracle.com/en/database/oracle/oracle-database/19/atnms/understanding-cluster-health-monitor-services.html
[96] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html#GUID-519A41E4-A97D-476E-B4BA-745C3486C779
[97] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html#GUID-519A41E4-A97D-476E-B4BA-745C3486C779
[98] https://docs.oracle.com/en/database/oracle/oracle-database/19/cwadd/introduction-to-oracle-clusterware.html

			The Cluster Synchronization Service (CSS), Event Management (EVM), and Oracle Notification Services (ONS) components communicate with other cluster component layers on other nodes in the same cluster database environment.	
		7879	Jetty Management Server	Oracle signed
		Dynamic Port 9000-65500	Oracle Trace File Analyzer collector	Oracle signed
Customer-controlled	Customer-controlled	customer-controlled	Optional Data Safe On-Premises Connector[99]	Customer-controlled or Oracle signed

VM Console Access

You can access your VM console through a token-based `ssh` tunnel.[100,101] The service controls the tunnel through the control plane to the hypervisor console of your VM in 3 steps:

1. Your OCI IAM credentials create a console connection, which includes deploying virtual machines and containers in the control plane to support an `ssh` proxy tunnel
2. Your `ssh` credentials create an `ssh` connection from your device on port 443 to an OCI endpoint, or from the OCI cloud shell, that provides access to the customer VM console through the OCI control plane
3. Login to your VM console using your username and password; typically, the `root` user

Software automatically terminates the cloud shell console connection after 24 hours. You must reauthenticate to OCI to reestablish the console connection. You may terminate the console connection at any time using the OCI console or API interfaces.

Figure 7 shows the steps to create the console connection for an `ssh` connection on port 443 to an OCI endpoint, as follows:

1. Your OCI IAM user connects to DBaaS control plane via OCI cloud console or API and requests to create a VM console connection; API payload includes an `ssh` public key used to establish an `ssh` session to the console endpoint
2. OCI IAM validates your OCI user is authorized by IAM Policy to create the VM console connection
3. Cloud automation software injects your public key to the target software that supports the connection to the VM console
4. ExaDB-C@C Control Plane Servers (CPS) create a temporary outbound connection from your data center to the OCI endpoint that supports the VM console ssh tunnel

[99] https://docs.oracle.com/en/cloud/paas/data-safe/admds/create-oracle-data-safe-onpremises-connector1.html
[100] https://docs.oracle.com/en-us/iaas/releasenotes/changes/9cee8331-1a56-494c-9bcc-f0dab3eea1b4/
[101] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-manage-vm-clusters.html#GUID-34F8308B-480A-4DAE-A158-2B4856E41A90

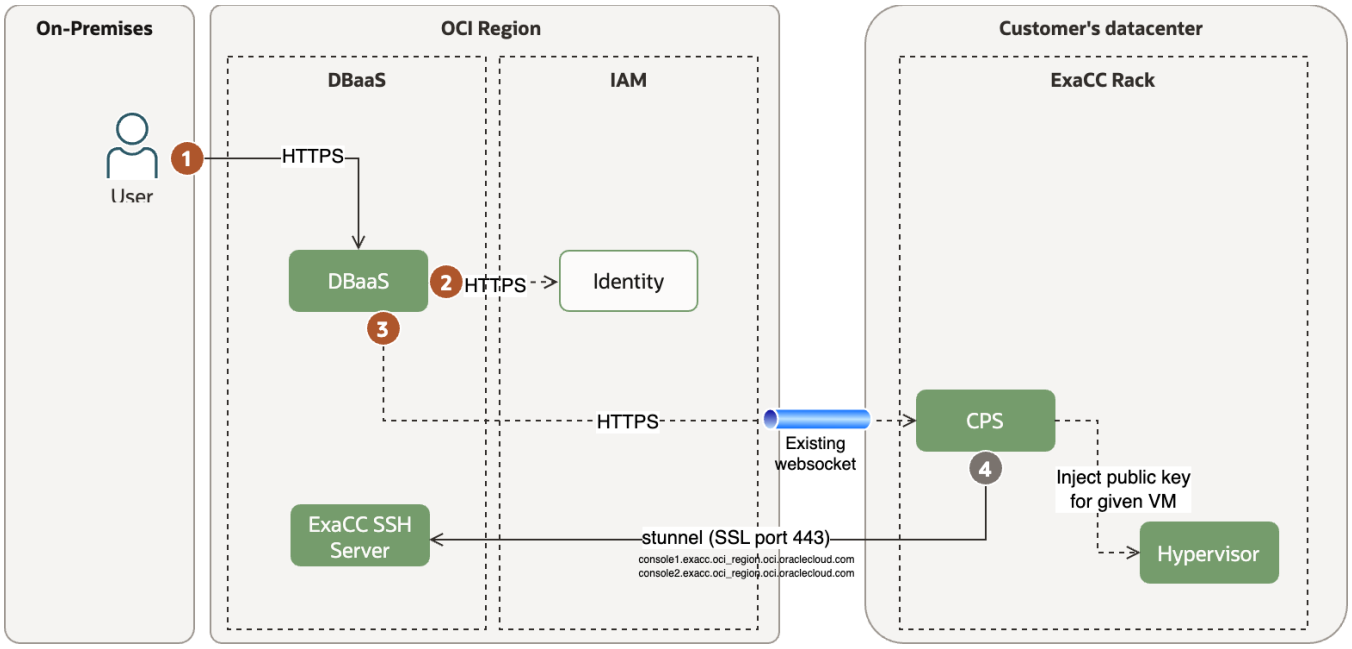

Figure 7: Workflow block diagram to create ssh tunnel to VM console

Figure 8 shows the steps to establish an ssh connection from a customer device to the VM console, as follows:

1. You initiate an ssh connection on port 443 to the necessary OCI endpoint using the ssh connection string provided by the OCI console API
2. The username for the connection is associated with the requesting user's IAM username
3. The ssh target in the connection is associated with the ExaDB-C@C virtual machine
4. OCI IAM validates that the username provided in the ssh connection is authorized by OCI Policy to connect to the target virtual machine
5. The ssh connection is forwarded on through the OCI control plane and the temporary ssh tunnel to the ExaDB-C@C CPS
6. The ssh connection is forwarded from the CPS to the virtual machine console running on the hypervisor

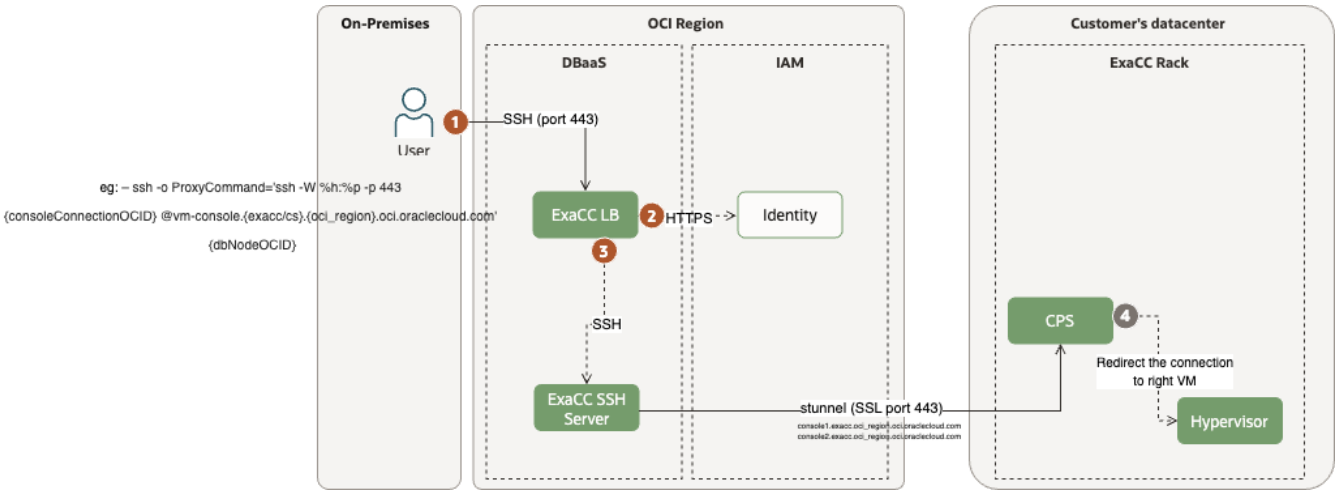

Figure 8: Workflow block diagram to establish an ssh connection via port 443 to an OCI endpoint

Figure 9 shows the steps to create a VM console connection and establish an ssh connection using the OCI Cloud Shell. This process uses system generated and protected temporary ssh keys to rather than user-supplied ssh keys, as follows:

1. Your OCI IAM user connects to DBaaS control plane via OCI cloud console or API and requests to create a VM console connection via OCI Cloud Shell
2. OCI IAM validates that the user is authorized by OCI IAM Policy to create the connection
3. Your OCI IAM user invokes Cloud Shell extension
4. OCI IAM validates your OCI user is authorized by OCI IAM Policy to use Cloud Shell via IAM

5. Cloud Shell creates a ssh key and invokes DBaaS public API and injects the public key to be used by connection
6. CPS injects the public key and creates the SSH connection tunnel
7. CPS creates ssh connection and Cloud Shell connects to the serial console

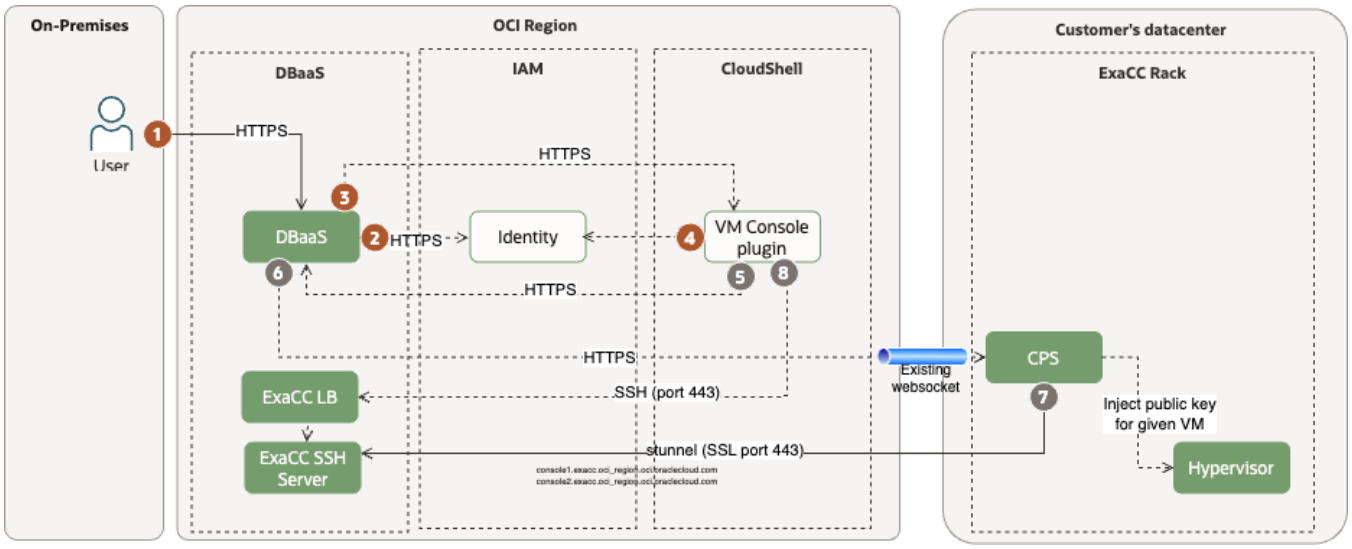

Figure 9: Workflow block diagram to establish an ssh connection to the VM console using the OCI Cloud Shell

Figure 10 shows the workflow to terminate a VM console connection

1. Your OCI IAM user connects to DBaaS control plane via OCI cloud console or API and requests to terminate the VM console connection
2. OCI IAM validates that the user is authorized by OCI IAM Policy to terminate the connection
3. The API to terminate the connection is sent to the CPS via the secure automation tunnel (websocket server)
4. The CPS terminates the secure tunnel that supports the ssh connection to the VM console

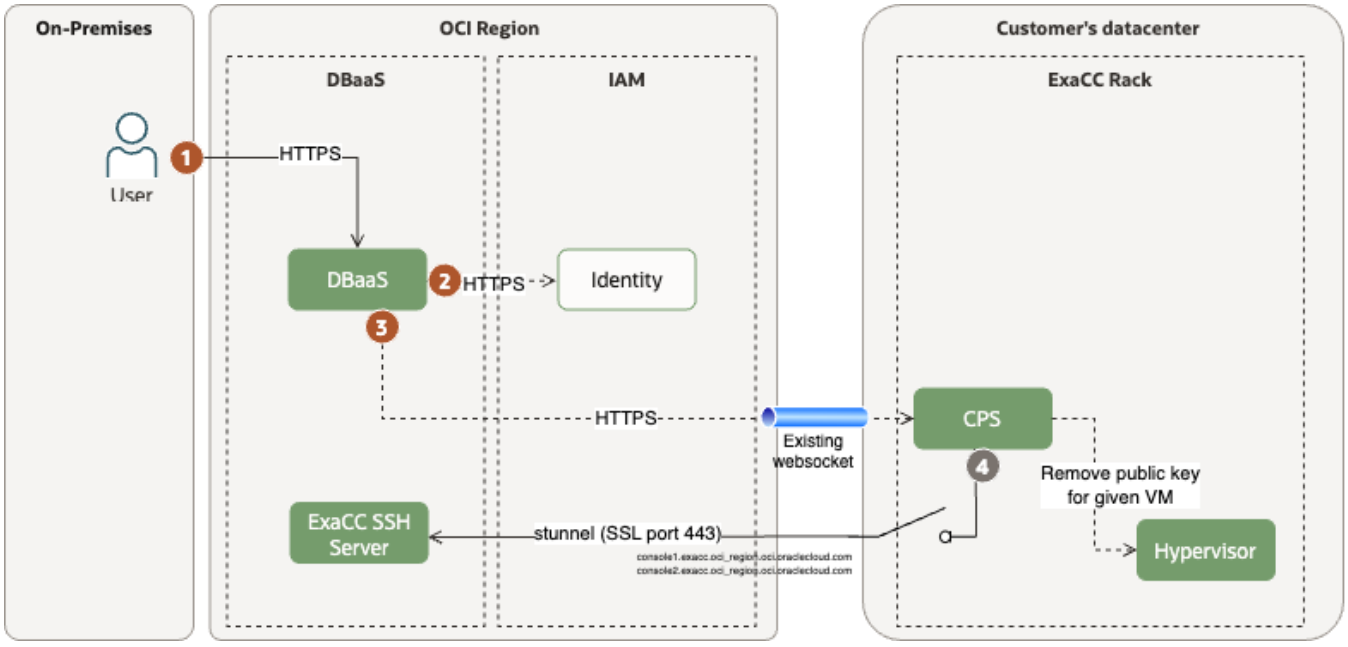

Figure 10: Workflow block diagram to terminate a VM console ssh connection

You can control the VM console connection with API Access Control[102] so that an OCI identity seeking to enable VM console access must get approval from a different OCI identity.

[102] https://docs.oracle.com/en-us/iaas/oracle-api-access-control/index.html

Cloud Automation Access to VM

Oracle cloud automation software accesses your databases and VM via 2 access methods:

- REST API call to Oracle DBCS agent running in VM via mTLS authentication on port 443
- Secure login to VM as a privileged user (`root`, `opc`, `grid`, `oracle`) using token-based `ssh`

Oracle cloud automation accesses your VM via a NAT address on the Exadata Database Server management network. Software generates temporary and unique ssh key pairs for each management action. The public key is injected by the cloud automation through the DBCS agent into the `~/.ssh/authorized_keys` files of the necessary service account in the VM, such as `oracle`, `opc`, `grid`, or `root`. The private key is stored in an encrypted file on in the ExaDB-C@C hardware in your data center and discarded after the action is completed. The cloud automation software removes the temporary public key from the service account in the customer VM when the action is completed. The private keys are controlled such that the `root` account can access the keys.

The VM includes the Oracle Linux packet filtering software[103] as an additional data protection control to block network to the VM. Blocking `ssh` access from the control plane will break the following service functionality:

- Database software updates
- Grid Infrastructure software updates
- VM operating system software updates
- Oracle managed infrastructure quarterly software updates (used to validate CRS restarts in the VM)
- Add Database Server Infrastructure
- Add VM Cluster Node
- Delete VM Cluster Node
- Add Storage Server

OCPU scaling does not require `ssh` access to the VM and will continue to work even when cloud automation is blocked at the network layer.

Delegate Access Control

You can use Delegate Access Control[104] to subscribe your VMs to database maintenance and support services, and control and monitor access by service provider staff. You can subscribe to 4 types of Delegate Access Control services:

- Oracle Database Cloud Customer Support – Oracle customer support services for database and Oracle Linux technology that are included at no additional charge
- Oracle Database Cloud Operation – Oracle customer support services for cloud automation software deployed in the VM that are included at no additional charge
- Oracle Engineered Systems Deployment and Infrastructure Support – assisted patching and troubleshooting services that are negotiated separately from the Exadata Database Service subscription
- Strategic Customers Program for DB Cloud Platforms – custom support services that are negotiated separately from the Exadata Database Service subscription

Delegate Access Control preventive controls include:

- Oracle staff access only after your approval of a specific work request
- Access is limited to approved components related to the work request
- Access is temporary, just-in-time, and automatically revoked after a set time
- You control when Oracle staff can access your services
- Oracle Linux `chroot` jails[105] and other software enforce of privilege limits

Delegate Access Control detective controls include:

- Software notifies you when Oracle staff need to access the VM
- Command and keystroke logs traceable to an individual person

---

[103] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-implement-sec.html#ol7-firewall-sec

[104] https://docs.oracle.com/en-us/iaas/delegate-access-control/doc/overview-of-delac.html

[105] https://docs.oracle.com/en/operating-systems/oracle-linux/8/security/security-ProtectingtheRootDirectoryUsingchrootJails.html#ol-harden-implement

Delegate Access Control responsive controls include:

- Terminating ssh connections and Bastion servers
- Terminating Linux processes started by the ssh connection
- Removing temporary credentials

Figure 11 shows the Delegate Access Control approval and access workflow. The Delegate Access Control demonstration video[106] provides more detail. Delegate Access Control uses the same delivery mechanics as Operator Access Control[107] and is included in the scope of the Operator Access Control PCI-DSS attestation of compliance (AoC).

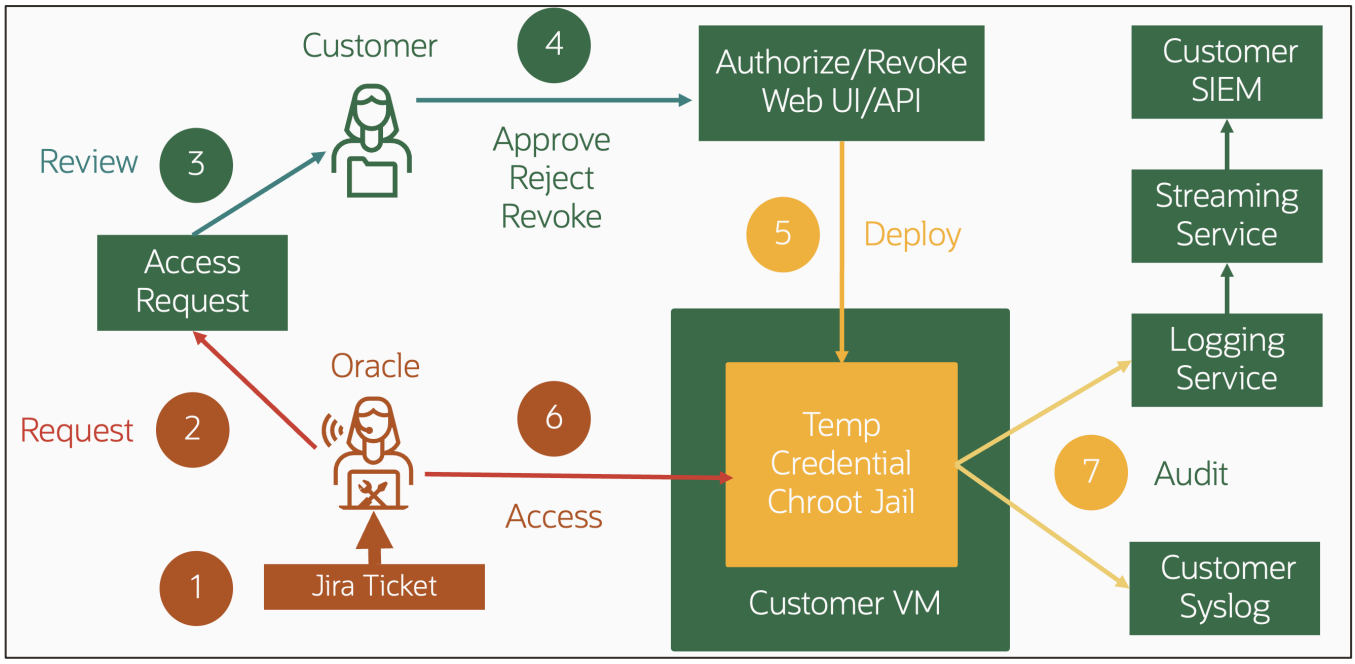

Figure 11: Delegate Access Control approval workflow

Network Security Controls

You can use your network security controls with the ExaDB-C@C client and backup networks. These controls must allow the ExaDB-C@C service to function, including:

- ICMP access between all VMs in a VM Cluster
- ssh between all VMs in a VM Cluster
- ssh inbound from your designated management sources
- SQLNet inbound from your clients to your databases
- Outbound DNS and NTP to your DNS and NTP servers

Additional OCI Security Services that Complement OCI IAM

OCI provides security services you can use with your ExaDB-C@C service. Network Sources and API Access Control help to complement OCI IAM by enforcing specific attributes beyond authentication and authorization. Network sources restrict authentication to your tenancy resource to connections initiating from IP addresses and VCNs that you specify. API Access Control intercepts privileged APIs and checks them against an approval workflow prior to sending the API to the target resource.

[106] https://www.youtube.com/watch?v=fwKtfp3aNuk

[107] https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/oracle-operator-access-control-tech-brief.pdf

Network Sources

OCI Network Sources[108] limits authentication to your tenancy resources to connections initiating from specific IP addresses, such as your proxy that allows egress from your corporate VPN. If you implement a site-to-site VPN or FastConnect from your data center to an OCI region, you can route OCI Console and API connections through an OCI Transit VCN.[109] This gives your on-premises network private access to Oracle services, so that your on-premises hosts can use their private IP addresses and the traffic does not go over the public internet. Network Sources is included with no additional charge.

API Access Control

API Access Control enforces a multi-identity approval workflow for privileged OCI Console and API functionality. Before a privileged API can be invoked, the user intending to invoke the API must raise an Access Request with their OCI identity, and a different OCI identity must approve the Access Request. Figure 12 shows the API Access Control approval workflow. Watch the API Access Control demonstration video[110] and see API Access Control at the Oracle Learning Center[111] for more details. AP Access Control is included with no additional charge.

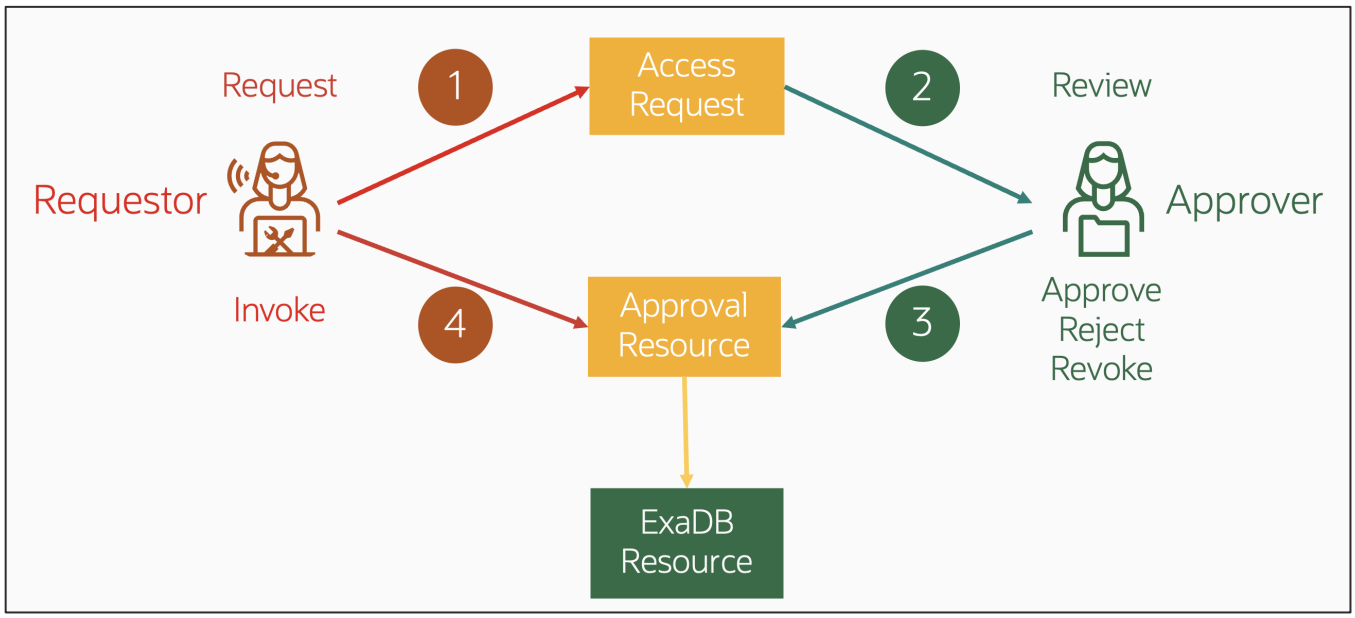

Figure 12: API Access Control approval workflow

Oracle Access Controls for Infrastructure Components

Oracle exclusively manages infrastructure security and availability as outlined in the Oracle PaaS and IaaS documentation.[112] Oracle Corporate Security Practices[113] cover the management of security for Oracle internal operations and cloud services. Oracle Global Trade Compliance[114] Prohibited End Users includes the countries and persons that are prohibited to access Oracle products and services. These apply to all Oracle personnel, such as employees and contractors. These policies are aligned with the ISO/IEC 27002:2022(formerly known as ISO/IEC 17799:2005) and ISO/IEC 27001:2022 standards and guide all areas of security within Oracle. Oracle implements an automated HR joiner/mover/leaver processes whereby authorization to access infrastructure is consistent with updates to employee job code, training records, and employment

[108] https://docs.oracle.com/en-us/iaas/Content/Identity/Tasks/managingnetworksources.htm
[109] https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/transitroutingoracleservices.htm
[110] https://www.youtube.com/watch?v=-kzyH4LzP3c&feature=youtu.be
[111] https://docs.oracle.com/en/learn/exadb-cc-api-access-control/
[112] https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf
[113] https://www.oracle.com/corporate/security-practices/corporate/
[114] https://www.oracle.com/corporate/security-practices/corporate/governance/global-trade-compliance/

status. Oracle further controls Oracle cloud operations access per Oracle Access Control Practices[115] with a least privilege, default deny approach where access is provided for:

- Those with a need-to-know
- The least privileges to do the work
- Separation of duties to help prevent conflicts of interest

Oracle ExaDB-C@C Cloud Operations staff are authorized to access and support Exadata Database Service infrastructure components, which include the following equipment:

- Power Distribution Units (PDUs)
- Out of band (OOB) management switches
- Storage Network switches
- Exadata Storage Servers
- Physical Exadata Database Servers

Oracle controls Oracle Cloud Ops staff access to ExaDB-C@C infrastructure, as follows:

OCNA access:

- Entitlement granted based on job-code
- Authenticated with FIPS 140-2 Level 3 hardware MFA
- User devices must pass security scans to connect to OCNA

Bastion server access:

- ssh access to Exadata Database Service infrastructure is through Bastion and management servers
- Access to management servers is tunneled through the Bastion server, which is isolated to privileged admin VCNs in the region hosting the service
- All Bastion connections are logged and monitored

Management server access:

- Staff log in as named users via ssh with FIPS 140-2 Level 3 hardware MFA
- Access is controlled to least privilege policies
- All management server access is logged and monitored

Exadata Database Service infrastructure access:

- Staff authenticate to service accounts using token-based ssh
- Command execution is auditable and traceable to named users
- All connections to infrastructure are logged and monitored

Figure 13 shows how Oracle Cloud Operations (Cloud Ops) staff access infrastructure components to manage the ExaDB-C@C. You can use Operator Access Control[116] to control Oracle when staff can gain shell access to ExaDB-C@C infrastructure and ADB-D VMs.

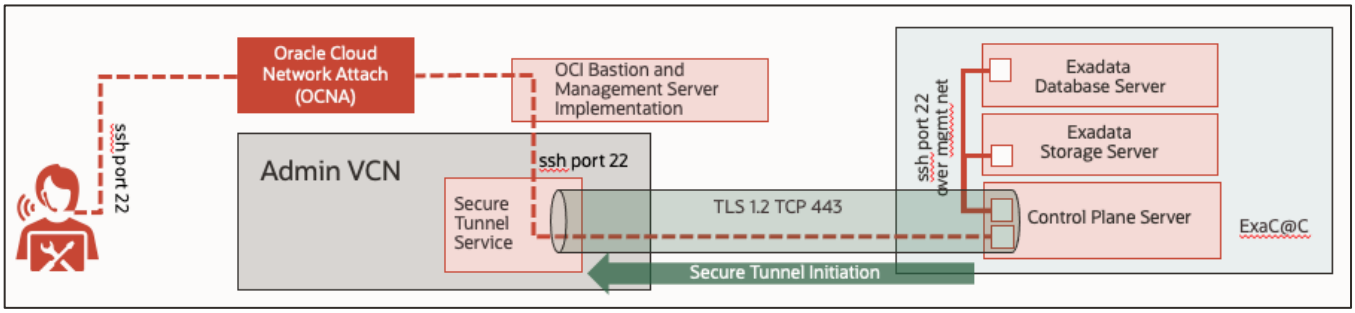

Figure 13: Cloud Operations Staff Access to ExaDB-C@C Infrastructure Components

[115] https://www.oracle.com/corporate/security-practices/corporate/access-control.html
[116] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html

Oracle Operator Access Control

An impediment to bringing a class of applications supporting mission critical and highly regulated workloads to a cloud platform is the shared responsibility model inherent to a cloud platform. In this model, the cloud service provider retains control to manage a subset of the system, such as the infrastructure (cloud provider tenancy), and the subscriber retains control to manage another part of the system, such as virtual machines, applications, and databases (customer tenancy). For mission critical and highly regulated workloads, the subscriber may have the responsibility to control the actions any person takes when accessing the any part of the system, including the actions by the cloud provider staff on cloud provider infrastructure. To meet these requirements, you can use Oracle Operator Access Control[117] with ExaDB-C@C and Autonomous Database Dedicated (ADB-D) on ExaDB-C@C. Operator Access Control is ideal for banking and financial services applications, energy utilities, and defense, and any other application where risk management is a key pillar of application success.

Operator Access Control is an OCI privileged access management (PAM) service. Operator Access Control provides interfaces to

- Control when and how much access Oracle staff have to ExaDB-C@C infrastructure and ADB-D VMs
- Observe and record Oracle operator commands and keystrokes Oracle staff execute on ExaDB-C@C infrastructure
- Terminate Oracle operator connections at the customer's discretion

These controls are a standard part of the ExaDB-C@C service and are available at no extra cost. Operator Access Control preventive controls include

- Oracle staff access only when authorized by you and only for a specific Oracle work request
- Oracle staff access is limited to explicitly approved components related to a stated and specific work request
- Oracle staff access is temporary, and is automatically revoked after the authorized task is completed or a timeout is reached
- You control when Oracle staff can access infrastructure
- Software enforcement of privilege levels

Operator Access Control detective controls include:

- Software notifies you when Oracle staff need to access infrastructure
- Command and keystroke logging for actions taken by Oracle staff
- Commands and keystrokes are traceable to an individual person
- You can monitor of all commands and keystrokes entered by Oracle staff
- Oracle-supplied record of the Oracle staff identity when required for any command executed

Operator Access Control responsive controls include:

- You can terminate Oracle staff access
- Software terminates processes started by Oracle staff
- Software removes remotely accessible accounts from ExaDB-C@C infrastructure and ADB-D VM

You must plan to ensure continuous monitoring (24x7x365) and response to Operator Access Control Access request events[118] for Oracle to support the ExaDB-C@C service. You can use the OCI Events[119] and Notifications[120] services to automate the process of notifying customer staff for the purposes of processing Operator Access Control Access Requests. See a Simple Guide to Managing OCI Alarms in ServiceNow[121] for an example of how to do this with ServiceNow. If you cannot ensure continuous monitoring, or your requirements can be met with software automatically approving access requests on your behalf, you can use Operator Access Control's preapproval feature.[122] With preapproval, you get all the benefit of temporary, just-in-time access and full command and keystroke audit logs without the need for your staff to

---

[117] https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/oracle-operator-access-control-tech-brief.pdf
[118] https://docs.oracle.com/en-us/iaas/operator-access-control/doc/auditing-operator-access-control-lifecycle-events.html#GUID-1C819283-0660-4828-8E11-09D897211436
[119] https://docs.oracle.com/en-us/iaas/Content/Events/Concepts/eventsoverview.htm
[120] https://docs.oracle.com/en-us/iaas/Content/Events/Concepts/eventsoverview.htm
[121] https://www.ateam-oracle.com/post/a-simple-guide-to-managing-oci-alarms-in-servicenow
[122] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-49AE3FAF-95E3-4D7D-B950-9FC52C4B5FA9

access OCI and approve access requests. This can ease operational burden and reduce the risk of delayed issue resolution leading to a more complex issue or service outage. You can configure preapproval for preconfigured maintenance windows to optimize software updates. You can selectively pre-approve lower access privileges and require explicit approval for higher access privileges.[123]

You can integrate Operator Access Control audit logs into compatible 3rd party software products. This includes sending audit logs to your syslog server[124] and integrating the OCI Logging service with Splunk.[125] See the Operator Access Control[126] product documentation, Operator Access Control Tech Brief,[127] and Operator Access Control Request and Audit Processing[128] video for more detail.

Software Development and Delivery Security Controls

ExaDB-C@C delivers the enterprise-class security features of Exadata Database Machine[129] as a cloud service. Software security for ExaDB-C@C includes:

- Software development performed under Oracle Software Security Assurance[130] practices
- Security architecture performed under Oracle Corporate Security Architecture[131] practices
- Development and debug tools to inspect customer data are not installed on ExaDB-C@C infrastructure

Software updates are signed and encrypted prior to transmission from OCI to ExaDB-C@C infrastructure to help prevent tampering.

DETECTIVE CONTROLS

ExaDB-C@C provides robust detective controls (auditing and logging) for your services and Oracle managed infrastructure. The service separates monitoring duties as follows:

- You control and monitor the logging configuration of your services
- Oracle controls and monitors the logging configuration of Oracle-managed infrastructure.

Oracle is not authorized to access your audit logs. You may request access to applicable Oracle infrastructure audit log information from Oracle via the Oracle service request (SR) process. Your audit rights are described in the Oracle Data Processing Agreement (DPA).[132]

Customer Service Audit Logging

ExaDB-C@C provides four capabilities for auditing and logging:

- OCI Audit: logs for control plane actions initiated by your OCI credential
- Oracle Database auditing: audit logs for database actions initiated by your Oracle Database credential
- VM operating system audit log: audit logs for actions initiated on a VM by your operating system credential
- Automated Intrusion Detection Environment (AIDE): for file integrity monitoring

---

[123] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-533A688A-FC75-43A8-B7DF-6481D781C872
[124] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-6526ADE1-C664-4600-A62B-5993EA25134E
[125] https://docs.oracle.com/en/solutions/logs-stream-splunk/index.html
[126] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-7CF13993-DB16-485A-A9FA-399E0049740B
[127] https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/oracle-operator-access-control-tech-brief.pdf
[128] https://www.youtube.com/watch?v=ZCLMs_kgSr4
[129] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/toc.htm
[130] https://www.oracle.com/corporate/security-practices/assurance/
[131] https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html
[132] https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf

You can send these audit logs to compatible technology. See Ingest Oracle Cloud Infrastructure Logs into Third-Party SIEM Platforms using Log Shippers[133] for implementation details.

OCI Audit Logging

OCI Audit[134] automatically records calls to all supported Oracle Cloud Infrastructure public application programming interface (API) endpoints as log events. All services support logging by Audit. Object Storage service supports logging for bucket-related events, but not for object-related events. Log events recorded by Audit include API calls made by the Oracle Cloud Infrastructure Console, Command Line Interface (CLI), Software Development Kits (SDK), your own custom clients, and other Oracle Cloud Infrastructure services. Information in the logs includes:

- Time the API activity occurred
- Source of the activity
- Target of the activity
- Type of action
- Type of response

Each log event includes a header ID, target resources, timestamp of the recorded event, request parameters, and response parameters. You can view events logged by the OCI Audit service by using the Console, API, or the SDK for Java. You can use data from events to perform diagnostics, track resource usage, monitor compliance, and collect security-related events. Audit logs are stored in the compartment of the target resource for the API.

Database Audit Logging

ExaDB-C@C provides comprehensive audit logging for the database with Oracle Database Unified Audit.[135] You can send these audit records to your syslog server[136] or compatible security information event management (SIEM) system. See the OCI solution playbook for streaming to SIEM[137] for an example. Oracle publishes documentation for configuring, managing, and monitoring of Oracle Database audit logs in the Oracle Database Security Guide[138] for each database version.

VM Audit Logging

The Oracle Linux audit log service (`auditd`)[139] records actions executed by operating system credentials. You can configure `auditd` per your standards, including sending the Oracle Linux audit log to a remote log server.[140] See the Oracle Linux Security Guide[141] for more detail. You can integrate the Oracle Linux audit logs into the OCI Log Analytics service.[142]

File Integrity Monitoring

Exadata Database Service includes the Oracle Linux Advanced Intrusion Detection Environment (AIDE)[143,144] to check file and directory integrity. AIDE is a small, yet powerful, intrusion detection tool automatically installed with the Linux Operating System, that uses predefined rules to check file and directory integrity. It is meant to protect the system internally, by providing a layer of protection against viruses, rootkits, malware, and detection of unauthorized activities. It is an independent static binary for simplified client/server monitoring configurations. AIDE runs on demand, and the time to report changes is dependent on the system checks (usually at least once a day). You can change the configuration in

---

[133] https://docs.oracle.com/en/learn/ocilogs-log-shipper/index.html#introduction
[134] https://docs.oracle.com/en-us/iaas/Content/Audit/Concepts/auditoverview.htm
[135] https://www.oracle.com/database/technologies/security/db-auditing.html
[136] https://support.oracle.com/knowledge/Oracle Cloud/2652319_1.html
[137] https://docs.oracle.com/en/solutions/oci-aggregate-logs-siem/#GUID-601E052A-8A8E-466B-A8A8-2BBBD3B80B6D
[138] Oracle Database 19c, see https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/introduction-to-auditing.html#GUID-94381464-53A3-421B-8F13-BD171C867405
[139] https://docs.oracle.com/en/learn/ol-auditd/
[140] https://support.oracle.com/knowledge/Oracle%20Cloud/2652319_1.html
[141] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-audit-sec.html
[142] https://blogs.oracle.com/ateam/post/harnessing-the-power-of-linux-logs-in-oci-logging-analytics-om
[143] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmso/aide.html
[144] https://support.oracle.com/knowledge/Oracle%20Linux%20and%20Virtualization/2616282_1.html

`/etc/aide.conf`. The configuration file is controls which files and directories are monitored by AIDE, and how logging and output are handled.

Oracle Infrastructure Audit Logging

Oracle is responsible for recording, analyzing, and responding to infrastructure audit logs. Infrastructure audit logs for Exadata Database Service X8 and earlier hardware include the following:

ILOM:

- syslog
- ILOM syslog redirected to the syslog of the physical infrastructure component

Physical Exadata Database Server:

- /var/log/messages
- /var/log/audit.log
- /var/log/secure
- /var/log/xen/xend.log

Exadata Storage Server:

- /var/log/messages
- /var/log/audit.log
- /var/log/secure

Storage Network Switch:

- `/var/log/messages`
- `/var/log/audit.log`
- `/var/log/secure`
- `/var/log/opensm.log`

Audit logs for Exadata Database Service X8M and later hardware include the following:

ILOM:

- syslog
- ILOM syslog redirected to the syslog of the physical infrastructure component

Physical Exadata Database Server:

- `/var/log/messages`
- `/var/log/secure`
- `/var/log/audit/audit.log`
- `/var/log/clamav/clamav.log`
- `/var/log/aide/aide.log`

Exadata Storage Server:

- /var/log/messages
- /var/log/secure
- /var/log/audit/audit.log

The retention period for Oracle infrastructure audit logs is at least 1 year.[145] Infrastructure audit logs are accessible by Oracle security staff.

RESPONSIVE CONTROLS

You and Oracle work together to secure and monitor access to ExaDB-C@C components. If either party detects an unauthorized action, that party can take responsive action immediately, prior to notifying the other party. If you detect an unauthorized action, you should notify Oracle of the action and response using the Oracle Service Request (SR) process.

You can take any responsive action on any services or equipment you control. This includes terminating Operator and Delegate Access Control Access Requests, network connections into your VM, and network connections between the CPS and OCI resources. Your databases should continue to function normally if you terminate connections between the CPS and OCI. Oracle's responsive controls include terminating connections at Bastion Servers in OCI, revoking access to Oracle-managed ExaDB-C@C infrastructure, and disconnecting ExaDB-C@C infrastructure from the OCI control plane.

---

[145] https://www.oracle.com/contracts/docs/ocloud_hosting_delivery_policies_3089853.pdf

Oracle Incident Response

Oracle Incident Response[146] describes how Oracle responds to security incidents, shown below.

"Learn about Oracle's robust program for responding to security events, some of which do represent incidents. A security incident is any accidental or intentional event that can impact the confidentiality, integrity, or availability of data hosted on Oracle corporate systems and in Oracle Cloud.

Global Information Security further defines roles and responsibilities for the incident response teams within the LoBs. All LoBs must comply with Global Information Security guidance for managing information security events and implementing timely corrective actions. LoB incident response programs must:

- *Investigate and validate that a security event has occurred*
- *Communicate with relevant parties and provide appropriate notifications*
- *Preserve evidence and forensic artifacts*
- *Document security event or incident and related response activities*
- *Contain security events or incidents*
- *Address the root cause of security events or incidents*
- *Escalate security events*

Upon discovery of a security event, Oracle incident response plans support rapid and effective event triage, including investigation, response, remediation, recovery, and post-incident analysis. LoB incident response teams, as required by the Security Incident Management Policy, conduct post-event analysis to identify opportunities for reasonable measures which improve security posture and defense in depth. Formal procedures and systems are utilized within the LoBs to collect information and maintain a chain of custody for evidence during event investigation. Oracle can support legally admissible forensic data collection when necessary."

15-Minute Service Response Time for Critical Issues

Oracle Cloud Hosting and Delivery Policies[147] describe Oracle's 15-minute service response time for critical issues, including security incidents, shown below:

"5.3.1 Severity 1 (Critical Outage)

Your production use of the Oracle Cloud Services is stopped or so severely impacted that You cannot reasonably continue work. You experience a complete loss of service. The impacted operation is mission critical to the business and the situation is an emergency. A Severity 1 service request has one or more of the following characteristics:

- *Data corrupted*
- *A critical documented function is not available*
- *Service hangs indefinitely, causing unacceptable or indefinite delays for resources or response*
- *Service crashes, and crashes repeatedly after restart attempts*
- *Security Incident with the potential to impact the confidentiality, integrity or availability of the service*

Oracle will use reasonable efforts to respond to Severity 1 service requests within fifteen (15) minutes. Throughout the period during which Oracle is working to address a Severity 1 service request, You agree to make available Your technical contact 24x7. Oracle will work 24x7 until the Severity 1 service request is resolved, a reasonable work-around is put in place, an approved action plan is in place or your 24x7 contact is no longer available. You must provide Oracle with a technical contact during this 24x7 period to assist with data gathering, testing, and applying fixes. You are required to propose this severity classification with great care, so that valid Severity 1 situations obtain the necessary resource allocation from Oracle."

COMMERCIAL REFERENCE INFORMATION

This section summarizes Oracle public commercial content related to common security questions for ExaDB-C@C. Visit the Oracle Trust Center[148] for an index to Oracle's security, compliance, privacy, and commercial contract documents.

---

[146] https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html

[147] https://www.oracle.com/contracts/docs/ocloud_hosting_delivery_policies_3089853.pdf

[148] https://www.oracle.com/trust/

Compliance

Oracle provides information about frameworks for which an Oracle line of business has achieved a third-party attestation or certification for one or more of its services in the form of "attestations." These attestations can assist in your compliance and reporting, providing independent assessment of the security, privacy and compliance controls of the applicable Oracle cloud services. In reviewing these third-party attestations, it is important that you consider they are generally specific to a certain cloud service and may also be specific to a certain data center or geographic region. You can access https://www.oracle.com/cloud/compliance/#attestations to access relevant detail about a specific standard. Please note that this information is subject to change and may be updated frequently, is provided "as-is" and without warranty and is not incorporated into contracts.

ExaDB-C@C is operated in compliance with common standards, including the following:

- ISO 27001
- System and Organization Controls 1 (SOC 1)
- System and Organization Controls 2 (SOC 2)
- System and Organization Controls 3 (SOC 3)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)

You can request compliance documents from an Oracle sales representative, and you can access them directly from their OCI Cloud Console.[149] Oracle publishes the Oracle Cloud Infrastructure and GDPR[150] paper to help you meet European Union General Data Protection Regulation (GDPR) requirements with OCI services.

Oracle Corporate Security Policies

Oracle Corporate Security Practices[151] help to protect the confidentiality, integrity, and availability of Oracle and customer data. These practices cover the management of security for Oracle's internal operations and cloud services, and apply to all Oracle personnel, such as employees and contractors. These policies are aligned with the ISO/IEC 27002:2022 (formerly known as ISO/IEC 17799:2005) and ISO/IEC 27001:2022 standards and guide all areas of security within Oracle. These practices include:

- Objectives[152]
- Human resources security[153]
- Access control[154]
- Network communications security[155]
- Data security[156]
- Laptop and mobile device security[157]
- Physical and environmental security[158]
- Supply Chain Security and Assurance[159]

[149] https://docs.oracle.com/en-us/iaas/Content/ComplianceDocuments/Concepts/compliancedocsoverview.htm
[150] https://docs.oracle.com/en-us/iaas/Content/Resources/Assets/whitepapers/oci-gdpr.pdf
[151] https://www.oracle.com/corporate/security-practices/corporate/
[152] https://www.oracle.com/corporate/security-practices/corporate/objectives.html
[153] https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
[154] https://www.oracle.com/corporate/security-practices/corporate/access-control.html
[155] https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html
[156] https://www.oracle.com/corporate/security-practices/corporate/data-protection/
[157] https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html
[158] https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
[159] https://www.oracle.com/corporate/security-practices/corporate/supply-chain/

Vulnerability Disclosure

As a matter of policy, Oracle will not provide additional information about the specifics of vulnerabilities beyond what is provided in the Critical Patch Update, Security Alert notification, pre-installation notes, readme files, and FAQs.[160] Oracle provides all customers with the same information to protect all customers equally. Oracle will not provide advance notification or "insider information" on Critical Patch Update or Security Alerts to individual customers. Oracle does not develop or distribute active exploit code (or "proof of concept code") for vulnerabilities in Oracle products.

The Oracle Critical Updates, Security Alerts, and Bulletins[161] page lists announcements of security fixes made in Critical Patch Update Advisories, Security Alerts and Bulletins, and it is updated when new Critical Patch Update Advisories, Security Alerts and Bulletins are released. Oracle will issue Security Alerts for vulnerability fixes deemed too critical to wait for distribution in the next Critical Patch Update, and a history of these alerts is maintained on the Critical Updates, Security Alerts, and Bulletins page.

Cloud customers, including ExaDB-C@C, requiring information that is not addressed in the Critical Patch Update Advisory may obtain information by submitting a My Oracle Support Service Request (SR) within their designated support system.

Oracle Data Processing Agreement

Oracle Data Processing Agreement for Oracle Services[162] describes how Oracle controls, protects, and processes data, such as:

- Cross Border Data Transfers
- Security and Confidentiality
- Audit Rights
- Incident Management and Breach Notification

As part of ExaDB-C@C, you may audit Oracle's compliance with its obligations under this Data Processing Agreement up to once per year. In addition, to the extent required by Applicable Data Protection Law, you or your Regulator may perform more frequent audits.

Oracle Cloud Services Agreement

Oracle Cloud Services Agreement[163] describes how your data is processed in Oracle Cloud Services, such as:

- Ownership Rights and Restrictions
- Nondisclosure
- Protection of Your Content
- Service Monitoring and Analysis
- Export
- Force Majeure
- Governing Law and Jurisdiction

Important Cloud Services Agreement information is shown below.

"5.1 In order to protect Your Content provided to Oracle as part of the provision of the Services, Oracle will comply with the applicable administrative, physical, technical and other safeguards, and other applicable aspects of system and content management, available at https://www.oracle.com/contracts/cloud-services.

11.1. We continuously monitor the Services to facilitate Oracle's operation of the Services; to help resolve Your service requests; to detect and address threats to the functionality, security, integrity, and availability of the Services as well as any content, data, or applications in the Services; and to detect and address illegal acts or violations of the Acceptable Use Policy. Oracle monitoring tools do not collect or store any of Your Content residing in the Services, except as needed for such purposes. Oracle does not monitor, and does not address issues with, non-Oracle software provided by You or any of Your Users that is stored in, or run on or through, the Services. Information collected by Oracle monitoring tools (excluding Your

[160] https://www.oracle.com/corporate/security-practices/assurance/vulnerability/disclosure.html
[161] https://www.oracle.com/security-alerts/#CVEOtherDocs
[162] https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf
[163] https://www.oracle.com/contracts/cloud-services/

Content) may also be used to assist in managing Oracle's product and service portfolio, to help Oracle address deficiencies in its product and service offerings, and for license management purposes.

11.2. We may (a) compile statistical and other information related to the performance, operation and use of the Services, and (b) use data from the Services in aggregated form for security and operations management, to create statistical analyses, and for research and development purposes (above clauses (a) and (b) are collectively referred to as "Service Analyses"). We retain all intellectual property rights in Service Analyses."

Oracle Management of Security Event Logs

Oracle Communications and Operations Management[164] describes how Oracle controls and manages security log information related to Oracle services, shown below:

"Oracle requires that system owners capture and retain logs for certain security-related activities on operating systems, applications, databases, and network devices. Systems are required to log access to Oracle systems and applications, as well as record system alerts, console messages, and system errors. Oracle implements controls designed to protect against operational problems, including log file media becoming exhausted, failing to record events, and/or logs being overwritten.

Oracle policy requires that Lines of Business monitor logs for security event investigation and forensic purposes. Identified anomalous activities must feed into the security event management processes for the Line of Business owning that system. Access to security logs is provided on the basis of need-to-know and least privilege. Where possible, log files are protected by strong cryptography in addition to other security controls, and access is monitored. Logs generated by internet-accessible systems are required to be relocated to systems that are not internet-accessible."

Oracle Consensus Assessment Initiative Questionnaire (CAIQ)[165] provides detail about how Oracle manages security logs, shown below:

"CCC-07.1 Are detection measures implemented with proactive notification if changes deviate from established baselines

The OCI Cloud Compliance Standard for Change Management outlines the procedures for Oracle personnel and programs that develop, administer, or support OCI, which includes unauthorized change prevention. OCI services monitor for unexpected and unauthorized changes and log deviations on the affected host, and alert the Detection and Response Team (DART) as necessary

DCS-02.2 Does a relocation or transfer request require written or cryptographically verifiable authorization?

OCI services log any changes to information assets and the location of an asset in the inventory register during asset acquisition, development, utilization, maintenance, and disposal.

LOG-01.1 Are logging and monitoring policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?

Logging and monitoring policies are established, documented, approved, communicated, applied, evaluated, and maintained by Oracle Corporate Security. Oracle logs certain security-related activities on operating systems, applications, databases, and network devices. Systems are configured to log access to Oracle programs, as well as system alerts, console messages, and system errors. Oracle implements controls designed to protect against operational problems, including log file media becoming exhausted or failing to record events, or logs being overwritten.

For more information, see oracle.com/corporate/security-practices/corporate/communications-operations-management.html.

The OCI Cloud Compliance Standard for Logging and Alerting specifies the requirements for the collection, maintenance, and review of audit logs.

LOG-09.1 Does the information system protect audit records from unauthorized access, modification, and deletion?

The OCI Cloud Compliance Standard for Logging and Alerting describes multiple layers of security to protect logs from unauthorized access, modification, or deletion, including the following measures:

- *Restricting access to log configuration capabilities to individuals with privileged access*

---

[164] https://www.oracle.com/corporate/security-practices/corporate/communications-operations-management.html

[165] https://www.oracle.com/a/ocom/docs/oci-corporate-caiq.pdf

- *Encrypting log data in transit*
- *Classifying log records in accordance with the Information Protection Policy*
- *Continuously monitoring log data with automated tools"*

One-Year Minimum Security Log Retention

Oracle Cloud Hosting and Delivery Policies[166] describes Oracle security log processing and retention, shown below:

"1.14 Security Logs

Oracle logs certain security-related activities on operating systems, applications, databases and network devices. Systems are configured to log default security activities, access to information or programs, system events such as alerts, console messages, and system errors. Oracle reviews logs for security event investigation and forensic purposes. Identified anomalous activities feed into the security event management process. Security logs are stored within the Security Information and Event Management system (or equivalent system) in a native, unaltered format and retained in accordance with Oracle's internal policies. Security logs are retained online for a minimum of 1 year. These logs are retained and used by Oracle for our internal security operations."

99.95% Monthly Uptime Service Level Agreement (SLA)

Oracle PaaS and IaaS Public Cloud Services Pillar Document[167] describes Oracle service credit remediation in cases where Oracle services are not delivered to 99.95% uptime, shown below:

"Availability Service Level Agreement With respect to a Cloud Service listed above for which the Availability Service Level Agreement under this subsection applies, Oracle will use commercially reasonable efforts to have each such Service available with a Monthly Uptime Percentage (as defined below) of at least 99.95% during any during any calendar month (the "Service Commitment"). In the event an applicable Cloud Service listed above does not meet its Service Commitment for the Availability Service Level Agreement under this subsection, You will be eligible to receive Service Credits for such Non-Compliant Service, with the Service Credit Percentage determined as follows:

Monthly Uptime Percentage: Service Credit Percentage

- *Less than 99.95% but equal to or greater than 99.0%: 10%*
- *Less than 99.0% but equal to or greater than 95.0%: 25%*
- *Less than 95.0%: 100%"*

60-Day Access Period After Service Termination

Oracle Cloud Hosting and Delivery Policies[168] describes the 60-day access period after service termination whereby you can retrieve your data from the service, shown below:

"6.1 Termination of Oracle Cloud Services

For a period of 60 days after the end of the Services Period for the Oracle Cloud Services or, if applicable, the 60 day period following Your termination of Cloud Services that You consume in a Pay as You Go model, following the end of their associated Services Period, Oracle will make available, via secure protocols and in a structured, machine-readable format, Your Content residing in the Oracle Cloud Services, or keep the service system accessible, for the purpose of data retrieval by You. At the end of the Services Period Your right to use such Services expires, except as otherwise permitted under the terms of the Oracle agreement, Your Order and the Service Specifications applicable to Your Oracle Cloud Services."

Exception Workflows - Oracle Access to Customer VM

ExaDB-C@C service support includes exception cases where a failure in your VM requires Oracle staff to access your VM to resolve the issue. The process and technical controls that govern how Oracle staff can access your VM depend on if you can or cannot access your VM. The following sections describe the processes and technology controls for these cases.

---

[166] https://www.oracle.com/contracts/docs/ocloud_hosting_delivery_policies_3089853.pdf
[167] https://www.oracle.com/contracts/docs/paas_iaas_pub_cld_srvs_pillar_4021422.pdf
[168] https://www.oracle.com/contracts/docs/ocloud_hosting_delivery_policies_3089853.pdf

VM is Controlled by Delegate Access Control

If you implement Delegate Access Control[169] and subscribe to Oracle Cloud Customer Support and Oracle Cloud Operation, then Oracle database cloud support or Oracle cloud operations support staff will issue a Delegate Access Control Access Request to you. After your approval, the Oracle support staff will access the VM with a unique, temporary, just-in-time credential deployed for least-privileged access that are implemented in a Linux chroot jail. The Oracle Linux audit service will provide command/keystroke logs to you through the OCI Logging service. You can optionally send the Oracle Linux audit logs to your syslog server.

VM is Accessible by You

If you can access your VM, then you can share your VM access with Oracle staff using remote collaboration technology (e.g., zoom, webex, skype, etc.). This access is controlled by the SR process as follows:

- You open a Service Request (SR) indicating the failure
- You or Oracle open a shared session and indicates session information in the SR
- You and Oracle access shared session information from the SR
- You access the VM using your credentials
- You either enter commands to resolve the issue as instructed by Oracle staff, or you permit the Oracle staff to control the keyboard entry for the VM session
- You update the SR with diagnostics information
- Oracle staff update the SR with resolution information

VM is not Accessible by You via Remote Login

If you cannot access your VM, or the VM is not accessible via remote login from infrastructure networks (e.g., VM is crashed), then specific process and technical controls can permit Oracle staff to access your VM from the infrastructure. This access is controlled by you and Oracle through the Oracle Service Request (SR) process, and the Operator Access Control (if implemented) as follows:

- If you are willing to permit Oracle Cloud Ops to access your VM without direct supervision, then you open a Service Request (SR) with the following language:
  - SR Title:
    - SR granting Oracle explicit permission to access a Guest VM of ExaCC with VM Name <insert VM Name as listed under the DB Server detail page→ Resources→ Virtual Machines>
  - SR Content:
    - We are opening this SR to grant explicit permission to Oracle to access our Guest VM in order for support to help resolve the issue described in SR# 1-xxxxxxxx. We acknowledge that by providing this permission, we understand that Oracle will have access to all files and memory that are part of the Guest VM. In addition, we also agree that the customer security team has authorized Oracle to have access to the customer Guest VM in order to resolve the issue described in the above SR.
    - DB Server OCID: <insert OCID of DB Server hosting the VM here>
    - VM Name: <insert VM Name as listed under the DB Server detail page→ Resources→ Virtual Machines>
- If you require Oracle to offer a shared screen to permit direct supervision of the Oracle cloud ops access, you open a Service Request (SR) with the following language
  - SR Title:
    - SR granting Oracle explicit permission to access a Guest VM of ExaCC with VM Name <insert VM Name as listed under the DB Server detail page→ Resources→ Virtual Machines>
  - SR Content:
    - We are opening this SR to grant explicit permission to Oracle to access our Guest VM in a shared screen session in order for support to help resolve the issue described in SR# 1-xxxxxxxx. We acknowledge that by providing this permission, we understand that Oracle will have access to all files and memory that are part of the Guest VM. This permission to access our VM is contingent on our representative being able to monitor in real-time via a screen-sharing session all activities performed by Oracle. In addition, we also agree that the customer security team has authorized

[169] https://docs.oracle.com/en-us/iaas/delegate-access-control/doc/overview-of-delac.html

Oracle to have access to the customer Guest VM via this shared screen session in order to resolve the issue described in the above SR.
    - DB Server OCID: <insert OCID of DB Server hosting the VM here>
    - VM Name: <insert VM Name as listed under the DB Server detail page→ Resources→ Virtual Machines>
- If you have implemented Operator Access Control, Oracle will open an Operator Access Control Access Request to resolve the issue; you must approve the Operator Access Control Access request to permit Oracle staff access to the appropriate system components
- Operator Access Control provides command and keystroke logging in near real time (<60 seconds) to your syslog server and/or the OCI Logging service in your tenancy

With you and Oracle both accessing the shared session, Oracle will work to resolve the issue. Appropriate technical processes will be determined on a case-by-case basis and specific to the failure mode indicated in the SR.

SERVICE TERMINATION AND DATA DESTRUCTION

You can terminate your ExaDB-C@C.[170] Oracle Exadata System Software includes the Secure Eraser utility,[171] which securely erases data on hard drives, flash devices, persistent memory, and internal USBs. It also resets ILOM to factory settings. Secure Eraser sanitizes all content, not only user data (Oracle Database data stored in the service), but also operating system, Oracle Exadata System Software, and user configurations. The Exadata Secure Eraser automatically detects the hardware capabilities of each storage device and selects the best erasure method supported. Cryptographic erasure is used whenever possible to provide better security and faster speed. The cryptographic erasure method used by Secure Eraser is designed to comply with the NIST SP-800-88r1 standard.[172] You can obtain secure erase certifications from Oracle by opening a My Oracle Support (MOS) Service Request (SR).

DEVICE AND DATA RETENTION

Oracle Customer Data and Device Retention for (DDR) Oracle Cloud at Customer[173] is an optional add-on service for ExaDB-C@C. Oracle DDR permits you to retain eligible hardware items that may contain sensitive, confidential, or classified customer data (Retained Hardware) that have been removed from the ExaDB-C@C. For purposes of DDR, Retained Hardware refers to the following components of Exadata database servers, storage servers, and control plane servers:

- Hard disk drives (HDD)
- Solid-state drives (SSD)
- Persistent memory (PMEM) components

[170] https://docs.public.content.oci.oraclecloud.com/en-us/iaas/exadata/doc/ecc-manage-databases.html#GUID-76C7A374-7E40-4E65-A6F1-AEE63D01CFE7

[171] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/exadata-secure-erase.html#GUID-6C9FD30C-FF88-4ABA-9249-93E183784B0D

[172] https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization

[173] https://www.oracle.com/assets/customer-data-device-retention-sd-4419287.pdf

SUMMARY

Security features throughout your VMs and databases are controlled by you. Oracle database encryption features encrypt data, you retain control of the encryption keys. Oracle database security features control authentication and access to data in the database, and you retain control of this authentication and access. Oracle Linux authentication features control access to your VMs, and you retain control of this authentication and access.

Security and auditing features throughout the Oracle-managed components of ExaDB-C@C help to prevent unauthorized actions on the infrastructure components of ExaDB-C@C. Security measures include multi-factor named user authentication and strong authentication with and FIPS 140-2 level 3 compliant token-based ssh access to Oracle-managed infrastructure components. Auditing and logging are implemented throughout the stack, and applicable audit logs are available to you through VM, Oracle Database, OCI services, and the Oracle Service Request (SR) process.

The combined security and auditing postures of customer-managed and Oracle-managed components separate duties and deliver the benefit of a high-security on-premises deployment with the ease-of-use and economics of the cloud. You and Oracle Cloud Operations work together to configure system security and help prevent unauthorized access to and theft of your data. Oracle Cloud Operations staff do not access your networks, services, or data to deliver the ExaDB-C@C service, and you do not access Oracle managed infrastructure to consume ExaDB-C@C Service. In the ExaDB-C@C deployment model, you gain the security of an on-premises deployment with the benefits of cloud economics, agility, and scale.

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

 blogs.oracle.com

 facebook.com/oracle

 twitter.com/oracle

Exadata Database Service on Cloud@Customer
Security Controls
December 2525