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

ORACLE

Exadata Database Service on Cloud@Customer Security Controls

Features to help prevent, detect, and respond to unauthorized actions to support IT security policy requirements

November 11, 2024 | Version 2.29

PURPOSE STATEMENT

This document provides an overview of features and enhancements included in release 24.1.4.0.0.241007, 23.1.19.0.0.241015, and 22.1.27.0.0.240911.[1] It is intended solely to help you assess the business benefits of upgrading to 24.1.4.0.0.241007, 23.1.19.0.0.241015, and 22.1.27.0.0.240911 and to plan your I.T. projects.

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

- 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 authorized to access the ExaDB-C@C infrastructure will use Oracle provided software and hardware to gain access to the infrastructure
- Oracle staff will perform software and hardware maintenance operations on the infrastructure, including maintenance that must be executed as the superuser (root) account
- Oracle staff will access hardware and software components necessary to perform diagnosis and resolution of hardware and software issues related to the ExaDB-C@C deployment

Customers can use Oracle Operator Access Control[3] (OpCtl) and Delegate Access Control (DaCtl),[4] included Privileged Access Management (PAM) services, to control Oracle staff access to Oracle-managed infrastructure and customer VMs. OpCtl and DaCtl provide OCI interfaces to manage entitlements, Oracle Linux security software to enforce privileges, and Oracle Linux audit to provide command and keystroke logs. Access with these services is granted as follows:

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

Security staff chartered with evaluating ExaDB-C@C should also review the following related documentation that describes additional security controls available with ExaDB-C@C:

- Oracle Cloud Infrastructure Security Architecture[5]
- Oracle Cloud Infrastructure Security Guide[6]
- Security Features in Autonomous Database[7]
- Security and Authentication in Oracle Autonomous Database[8]
- Exadata Database Service on Cloud@Customer Security Guide[9]
- Oracle Operator Access Control Tech Brief[10]
- Oracle Cloud Infrastructure Security Testing Policies[11]
- Oracle Cloud Services Contracts[12]
- Oracle Data Processing Agreement[13]

[1] https://support.oracle.com/knowledge/Oracle%20Database%20Products/2333222_1.html

[2] https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/gen2-exacc-ds.pdf

[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

[5] https://www.oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf

[6] https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_guide.htm

[7] https://docs.oracle.com/en-us/iaas/autonomous-database/doc/security-features-adb-d.html

[8] https://docs.oracle.com/en/cloud/paas/autonomous-database/adbsa/gs-security-and-authentication-autonomous-database.html

[9] https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/exadata/doc/exacc-secguide.html

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

[11] https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm

[12] https://www.oracle.com/corporate/contracts/cloud-services/

[13] https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf

- Oracle Cloud Services Agreement[14]
- Oracle Corporate Security Practices[15]

DISCLAIMER

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

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.

[14] https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#online

[15] https://www.oracle.com/corporate/security-practices/

TABLE OF CONTENTS

LIST OF IMAGES

LIST OF TABLES

INTRODUCTION

Exadata Database Service on Cloud@Customer (ExaDB-C@C) provides Oracle's public Exadata Cloud Service at a customer's data center using Oracle-owned and managed infrastructure located at a customer's data center. The advantage of ExaDB-C@C is that the customer retains physical control of the ExaDB-C@C hardware by locating it in a data center of their choice while still receiving the efficiency and automation of the Oracle Cloud Infrastructure (OCI) control plane and ExaDB-C@C Cloud Ops staff support for infrastructure maintenance.

ExaDB-C@C is the right database service for use cases where customers seek to gain the operational and financial value of a cloud implementation while honoring policy, legal, and regulatory requirements dictated to mission critical applications and highly regulated industries. For example, ExaDB-C@C 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. Customers operating in these industries and interested in pursuing a cloud strategy must ensure that their chosen cloud provider has comprehensive support of these capabilities within their standardized service offering.

The ExaDB-C@C service delivery model is a standardized offering based on industry best practices for protecting customer data and mission critical workloads. To facilitate customer adoption of the ExaDB-C@C service delivery model, ExaDB-C@C includes the security controls described in this paper as compensating measures for edge cases where customer approved security standards may differ from the ExaDB-C@C model. The intent of this paper is to describe the controls such that they may be used by customer security teams to validate the security posture of the ExaDB-C@C meets applicable requirements, to grant exceptions to historical standards, and to create future standards based on these controls.

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 the following standards:

- 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)

Customers may request compliance documents from an Oracle sales representative, and customers may access them directly from their OCI Cloud Console.[16]

To help customers meet European Union General Data Protection Regulation (GDPR) requirements with OCI services, Oracle publishes the Oracle Cloud Infrastructure and GDPR[17] paper.

ORACLE CONTRACTS

The Oracle Data Processing Agreement[18] describes how Oracle controls, protects, and processes data related to Oracle services, including ExaDB-C@C, such as

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

The Oracle Cloud Services Agreement[19] provides information about customer 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

The Oracle Trust Center[20] provides an index to Oracle's security, compliance, privacy, and commercial contracts.

ORACLE COPORATE SECURITY PRACTICES

Oracle Corporate Security Practices[21] cover the management of security for both Oracle's internal operations and cloud services, Oracle provides to its customers, 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. Oracle's published Corporate Security Practices[22] including the following information:

- Objective[23] – help protect the confidentiality, integrity, and availability of both Oracle and customer data
- Human Resources Security[24]
- Access Control[25]
- Network Communications Security[26]

[16] https://docs.oracle.com/en-us/iaas/Content/ComplianceDocuments/Concepts/compliancedocsoverview.htm
[17] https://docs.oracle.com/en-us/iaas/Content/Resources/Assets/whitepapers/oci-gdpr.pdf
[18] https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf
[19] https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#online
[20] https://www.oracle.com/trust/
[21] https://www.oracle.com/corporate/security-practices/ and https://www.oracle.com/assets/corporate-security-practices-4490843.pdf
[22] https://www.oracle.com/corporate/security-practices/corporate/
[23] https://www.oracle.com/corporate/security-practices/corporate/objectives.html
[24] https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
[25] https://www.oracle.com/corporate/security-practices/corporate/access-control.html
[26] https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html

- Data Security[27]
- Laptop and Mobile Device Security[28]
- Physical and Environmental Security[29]
- Supply Chain Security and Assurance[30]

When Oracle is working on customer site or systems at customer direction, Oracle consultants and support staff will observe customer practices as agreed to between Oracle and the customer.

Oracle Vulnerability Disclosure Policies

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 or Security Alert notification, the pre-installation notes, the readme files, and FAQs[31] Oracle provides all customers with the same information in order to protect all customers equally. Oracle will not provide advance notification or "insider information" on Critical Patch Update or Security Alerts to individual customers. Finally, Oracle does not develop or distribute active exploit code (or "proof of concept code") for vulnerabilities in our products.

The Oracle Critical Updates, Security Alerts, and Bulletins[32] 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.

ROLES AND RESPONSIBILITIES

ExaDB-C@C is jointly managed by the customer and Oracle, as described by the ExaDB-C@C Service Description[33] and detailed on My Oracle Support (MOS) in the ExaDB-C@C Explanation of Services[34] document. The ExaDB-C@C deployment is divided into 2 areas of responsibility:

- Customer managed services - components that the customer can access as part of their subscription to ExaDB-C@C
  - Customer accessible virtual machines (VM)
  - Customer accessible database services
- Oracle managed infrastructure - hardware that is owned and operated by Oracle to run customer accessible services
  - Power Distribution Units (PDUs)
  - Out of band (OOB) management switches
  - Storage networking switches
  - Exadata Storage Servers
  - Physical Exadata Database Servers

Customers control and monitor access to customer services, including network access to their VMs (via layer 2 VLANs and firewalls implemented in the customer VM), authentication to access the VM, and authentication to access databases running in the VMs. Oracle controls and monitors access to Oracle Managed Infrastructure components. Oracle staff are not authorized to access customer services, including customer VMs and databases. Table 1 summarizes the division of roles and responsibilities for Oracle and the customer.

[27] https://www.oracle.com/corporate/security-practices/corporate/data-protection/

[28] https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html

[29] https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html

[30] https://www.oracle.com/corporate/security-practices/corporate/supply-chain/

[31] https://www.oracle.com/corporate/security-practices/assurance/vulnerability/disclosure.html

[32] https://www.oracle.com/security-alerts/#CVEOtherDocs

[33] https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/exadata/doc/ecc-system-config-options.html

[34] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2707015.1

Table 1: Roles and Responsibilities

WORK FUNCTION	ORACLE MANAGED INFRASTRUCTURE		CUSTOMER MANAGED SERVICES	
	Oracle Cloud Ops	Customer	Oracle Cloud Ops	Customer
Monitoring	Infrastructure, Control Plane, Hardware Faults, Availability, Capacity	Provide network access to support Oracle infrastructure log collection and monitoring	Infrastructure availability to support customer monitoring of customer services	Monitoring of Customer 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 customer 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

CONSIDERATIONS WHEN MAKING CHANGES TO THE SERVICE SOFTWARE

ExaDB-C@C provides customers with interfaces to access operating systems and databases that they subscribe to. This access includes root access to guest operating systems and SYSDBA access to Oracle databases. This access permits customers to make changes to the service; however, with any changes there is a risk of that change triggering an exception somewhere in the stack at a later time. If you encounter an exception, then the Oracle service request (SR) process will identify best way to resolve the exception. A possible resolution recommended by Oracle support may be to revert the configuration change, and there are cases related to 3rd party products where Oracle may ask to reproduce the problem without the 3rd party products, per Oracle 3rd party software support policies.[35] Oracle support is included in your subscription, so there is no additional fee to you when you open up an Oracle service request.

Oracle's recommendation for the service is to use the service as Oracle ships it. The service design process that includes Oracle Corporate Security Architecture Oversight,[36] Oracle Software Security Assurance,[37] and the Exadata Cloud@Customer Security Features.[38] The intent of the controls described in this paper is to help you to use the service as Oracle ships it so that you may reduce your operational expenses related to testing, validating, and maintaining changes to the service.

EXADB-C@C SERVICE ARCHITECTURE

[35] https://support.oracle.com/knowledge/Oracle%20Cloud/1593827_1.html

[36] https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html

[37] https://www.oracle.com/corporate/security-practices/assurance/

[38] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html

Figure 1 shows the architecture block diagram the Gen 2 ExaDB-C@C service.

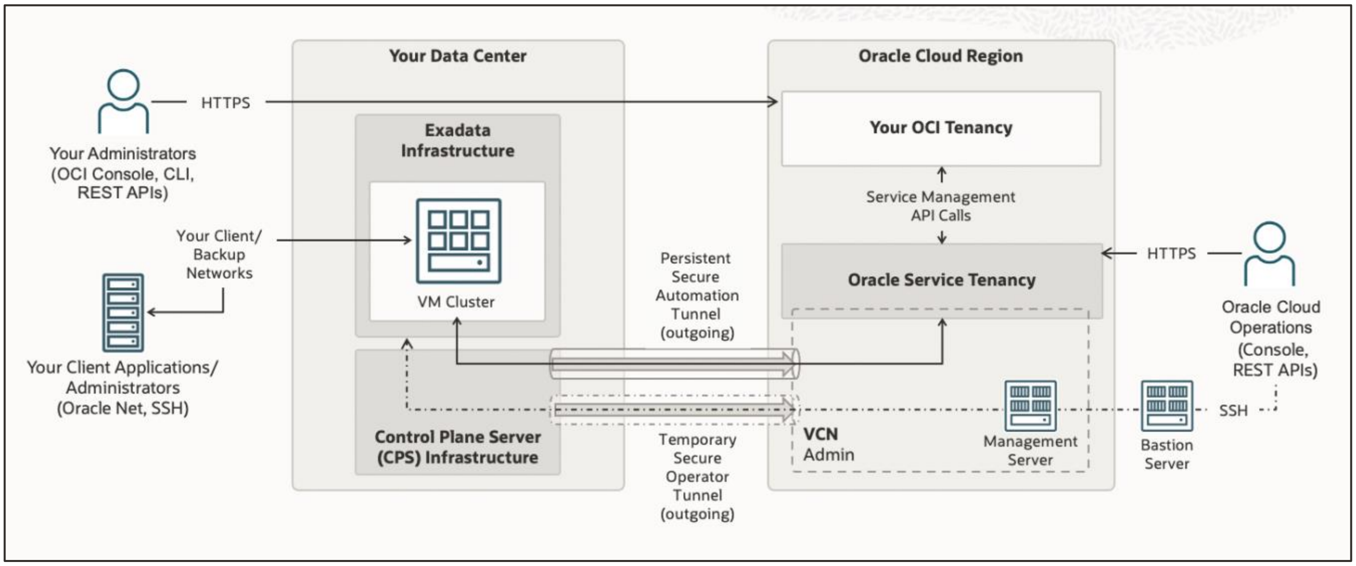
Your Data Center
Oracle Cloud Region
HTTPS
Your Administrators (OCI Console, CLI, REST APIs)
Exadata Infrastructure
Your OCI Tenancy
Service Management API Calls
Your Client/ Backup Networks
VM Cluster
Persistent Secure Automation Tunnel (outgoing)
Oracle Service Tenancy
HTTPS
Oracle Cloud Operations (Console, REST APIs)
Your Client Applications/ Administrators (Oracle Net, SSH)
Control Plane Server (CPS) Infrastructure
Temporary Secure Operator Tunnel (outgoing)
VCN Admin
Management Server
Bastion Server
SSH

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

The ExaDB-C@C service is deployed in an ExaDB-C@C rack in a data center of the customer's choice. The ExaDB-C@C rack contains all the components of a standard Exadata Database Machine, plus 2 Control Plane Servers (CPS) in a highly available (HA) configuration that connect to an OCI region.

The customer's database data is secured in the on-premises ExaDB-C@C rack, and all access to customer databases is made via network connections (intranet) the customer permits to access the VMs and databases in the ExaDB-C@C rack. Credentials to access the customer VMs and customer databases are retained and controlled by the customer. The customer has privileged access (e.g., root, SYS) to customer VMs and databases, and the customer can act with those credentials to secure the VM and database to help address local policy and regulatory requirements. This includes, and is not limited to, installing agents, forwarding operating system and database audit logs to customer security information event management (SIEM), and controlling access to and identity management for VMs and databases via tools that are compatible with the ExaDB-C@C Compute VM operating system and Oracle database.

The OCI region performs remote delivery of the ExaDB-C@C service, including customer-controlled cloud automation for database and system management and infrastructure maintenance and support. The customer controls access to the cloud automation's management functionality via the OCI Identity and Access Management (IAM) Service, and the OCI Audit Service provides the customer with a record of all customer-initiated management actions invoked via the OCI Console or OCI REST endpoints, such as creating or deleting databases. Oracle controls network access from the OCI region to the Control Plane Server, and operator access to perform infrastructure maintenance and support. Complete physical and logical networking deployment details are published in the Preparing for Exadata Database Service on Cloud@Customer[39] documentation. This documentation likewise includes power, space, cooling, and other customer data center requirements for service installation and operation.

Control Plane Server Networking

The ExaDB-C@C service requires no inbound TCP connection for service delivery, support, or management purposes. The ExaDB-C@C service requires outbound TCP connections on port 443 to Oracle endpoints for the purposes of remote service delivery and management. Please note that after the TCP connection is established from the CPS to the OCI endpoint the TCP connection can permit payloads to be delivered from OCI into the ExaDB-C@C infrastructure. For example, the persistent secure automation tunnel is used to send REST API calls from OCI to the ExaDB-C@C infrastructure, and the temporary secure operator tunnel is used for Oracle Cloud Ops access ExaDB-C@C infrastructure via `ssh` protocol. These endpoints are shown in

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

Table 2: Required outbound URL access for ExaDB-C@C, and in the Network Requirements for Oracle Exadata Database Service on Cloud@Customer section[40] of the Exadata Database Service on Cloud@Customer product documentation.[41]

[40] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/eccad/eccpreparing.html#GUID-F06BD75B-E971-48ED-8699-E1004D4B4AC1

[41] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/eccad/index.html

Table 2: Required outbound URL access for ExaDB-C@C[42]

DESCRIPTION/PURPOSE	OPEN PORT	CERTIFICATE AUTHORITY	LOCATION REPLACE *OCI_REGION* WITH YOUR REGION[43]
Persistent Outgoing Tunnel Service for cloud automation Delivery	443 outbound	Oracle Self-Signed	https://wss.exacc.*oci_region*.oci.oraclecloud.com
Persistent Outgoing Tunnel Service for Autonomous Database Dedicated (ADB-D) cloud automation Delivery	443 outbound	Oracle Self-Signed	https://wsshe.adbd-exacc.*oci_region*.oci.oraclecloud.com
Temporary Secure Tunnel Service for remote Oracle operator access supporting ExaDB-C@C Infrastructure	443 outbound	Oracle Self-Signed	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	443 outbound	Oracle Self-Signed	https://mgmthe.adbd-exacc.*oci_region*.oci.oraclecloud.com
Object Storage Service to retrieve system updates	443 outbound	DigiCert	https://objectstorage.*oci_region*.oraclecloud.com https://swiftobjectstorage.*oci_region*.oraclecloud.com
Monitoring Service to record and process Infrastructure Monitoring Metrics (IMM)	443 outbound	DigiCert	https://telemetry-ingestion.*oci_region*.oraclecloud.com
Identity Service for name resolution of Oracle operators	443 outbound	DigiCert	https://identity.*oci_region*.oraclecloud.com https://auth.*oci_region*.oraclecloud.com
Logging Service for application and security logs	443 outbound	Oracle PKISVC CrossRegion Intermediate r2[44]	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	443 outbound	DigiCert	https://database.*oci_region*.oraclecloud.com
VM Console	443 outbound	DigiCert	https://console1.exacc.*oci_region*.oci.oraclecloud.com https://console2.exacc.*oci_region*.oci.oraclecloud.com

If you are using IP address filtering based firewall rules, due to the dynamic nature of cloud interfaces, you must allow traffic with all the relevant IP CIDR ranges associated with your OCI region as identified by https://docs.oracle.com/en-us/iaas/tools/public_ip_ranges.json.

ExaDB-C@C supports http proxy (e.g., corporate proxy, passive proxy) to manage connections from the CPS to OCI endpoints. An http proxy adds deployment complexity, and maintenance to support future ExaDB-C@C releases that may require access to additional OCI endpoints. Should you choose to selectively permit access to URLs for specific OCI services, you may need to update you permitted URLs when Oracle adds new features and services to ExaDB-C@C. Customer https, challenge proxy, and traffic inspection are not supported.

The ExaDB-C@C Persistent Secure Tunnel Service for Automation Delivery is used for remote delivery of cloud automation commands (REST API calls, exclusively). This service is limited to ExaDB-C@C and not part of OCI's public services. The URLs for this service are specific to the OCI region configured to manage the ExaDB-C@C infrastructure.

The ExaDB-C@C Secure Tunnel Service for Remote Operator Access is used exclusively for Oracle Operator Access (ssh) to Oracle Managed ExaDB-C@C Infrastructure and ADB-D resources when applicable. This service is limited to ExaDB-C@C, not part of OCI's public services. The URLs for this service are specific to the OCI region configured to permit Oracle Operator Access to the ExaDB-C@C infrastructure.

The certificates for the mTLS connectivity from the ExaDB-C@C Infrastructure to OCI are managed by Oracle exclusively. Client certificates for the ExaDB-C@C infrastructure for the ExaDB-C@C Persistent Secure Tunnel Service are rotated by Oracle on a 6-month schedule. Client certificates for the ExaDB-C@C Secure Tunnel Service for Remote Operator Access are rotated on a 15-day schedule. ExaDB-C@C client certificates are unique to each ExaDB-C@C infrastructure. Customers are not permitted to manage these certificates or inspect the traffic contained in the secure tunnel connections.

The CPS requires a customer provided DNS for IP address resolution, NTP server for clock synchronization, and routing to OCI service URLs.

The minimum bandwidth requirements for the CPS Internet connection to OCI are 50/10 mbs download/upload.

ExaDB-C@C network connections back to OCI may be implemented via OCI FastConnect[45] or through an OCI site-to-site VPN.[46,47] OCI Transit Routing[48] and Network Security Lists[49] may be used to help control access by ExaDB-C@C infrastructure to OCI services, and OCI VCN Flow Logs[50] may be used to monitor traffic volume to network endpoints. The OCI Network Firewall[51] may be implemented in an OCI Transit VCN to implement an allow list for the URLs and OCI region IP addresses required to support the ExaDB-C@C service.

Customer Access to ExaDB-C@C Services

Customers access Oracle databases (DB) running on ExaDB-C@C via a layer 2 (tagged VLAN) connection from customer equipment to the databases running in the customer VM using standard Oracle database connection methods, such as Oracle Net on port 1521. Customer's access the customer VM running the Oracle databases via standard Oracle Linux methods, such as token based `ssh` on port 22.

Actions to manage infrastructure components, such as OCPU scaling and creating a Virtual Machine (VM) Cluster, are executed by the customer utilizing the cloud automation software in a tenancy designed with security in mind and hosted in the Oracle Cloud Infrastructure. Customers do not have to manage the infrastructure layer as Oracle maintains a 99.95% uptime service level objective (SLO). Customers are not authorized to directly access, load monitoring agents, or directly pull from or push files to the Oracle managed infrastructure in the ExaDB-C@C service.

[42] https://docs.oracle.com/en-us/iaas/exadata/doc/eccpreparing.html#GUID-D3C65CB4-965E-4670-B676-5EEA4C9282C9

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

[44] 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

[45] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/fastconnect.htm

[46] https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/overviewIPsec.htm

[47] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-network-requirements.html#GUID-E53A5DCF-CCCD-4493-B1D2-4EA6FA30B8A1

[48] https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/transitroutingoracleservices.htm

[49] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/securitylists.htm

[50] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/vcn_flow_logs.htm

[51] https://docs.oracle.com/en-us/iaas/Content/network-firewall/overview.htm

Network Architecture

Figure 2 describes the physical network implementation for ExaDB-C@C deployed in the Exadata rack, and the Exadata Database Service on Cloud@Customer Technical Architecture[52] details the architecture and implementation. The customer accessible and controlled components are shown in blue, and the Oracle managed components are shown in red. The ExaDB-C@C infrastructure components are interconnected via an isolated layer 2 management network, also shown in red. There is no direct network access from the management or storage networks to the customer client and backup networks, and the Exadata Database Server nominally does not have an IP address configured (plumbed) to access the client or backup networks. The ExaDB-C@C control plane software will temporally configure IP addresses on the Exadata Database Server to perform network validation checks on the Client and Backup networks when customers create a VM Cluster Network resource.[53]

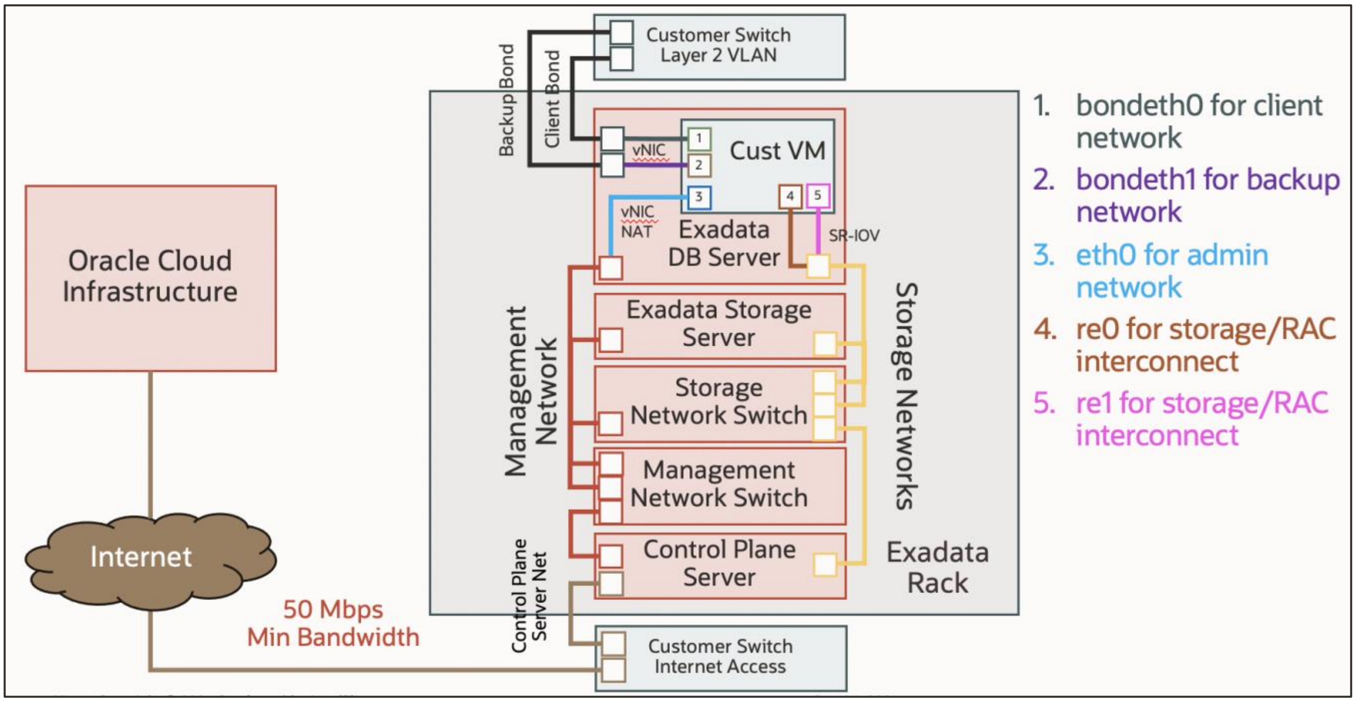

Figure 2: ExaDB-C@C Physical Network Implementation

Figure 3 details the network isolation between different Virtual Machine Clusters (VM Clusters) deployed on the same ExaDB-C@C Exadata Database Server (DB Server). When multiple VM clusters are configured, the customer controls the VLAN tags and IP networking configuration of each VM cluster, and the same physical links are shared for the client (indicated as network 1) and backup (indicated as network 1) networks for each VM on the same Exadata DB Server. Customers can specify different VLAN tags for different networks on different VM clusters to isolate network access into the VM cluster. The back-end storage networks of each VM cluster (networks 4 and 5) are isolated via layer 2 controls in the Converged Ethernet implementation that supports the back-end storage network, so there is no method for different VMs on the same Exadata Database Server to access each other via the back-end storage network. The vNIC/NAT admin network access (network 3) is implemented as an isolated /30 network so to prevent different VMs on the same Exadata DB Server from accessing one another on the admin network.

In addition to the network isolation, CPU cores are pinned to specific VMs on a given Exadata Database Server as a preventive control against in-VM executed methods to access cached data from other VMs.

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

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

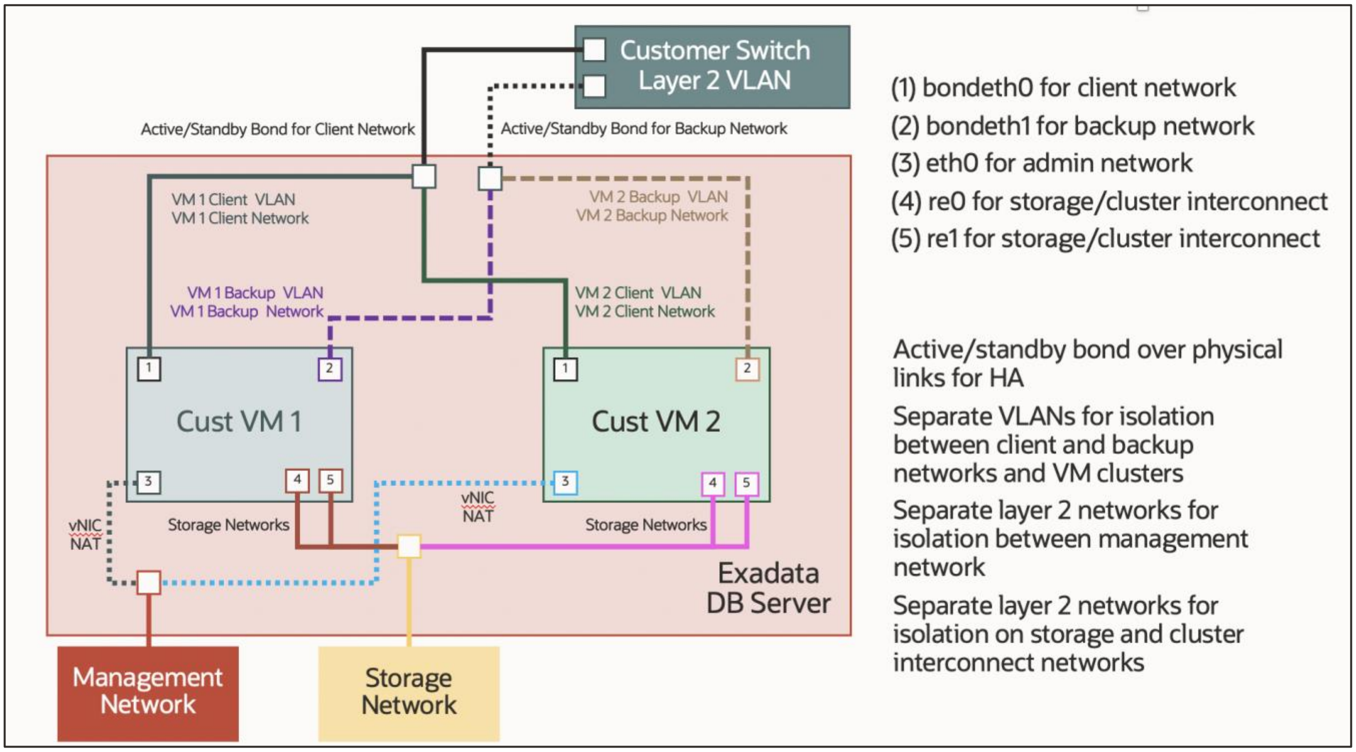
Customer Switch
Layer 2 VLAN
Active/Standby Bond for Client Network
Active/Standby Bond for Backup Network
VM 1 Client VLAN
VM 1 Client Network
VM 2 Backup VLAN
VM 2 Backup Network
VM 1 Backup VLAN
VM 1 Backup Network
VM 2 Client VLAN
VM 2 Client Network
Cust VM 1
Cust VM 2
1
2
3
4
5
vNIC
NAT
Storage Networks
Exadata
DB Server
Management
Network
Storage
Network
(1) bondeth0 for client network
(2) bondeth1 for backup network
(3) eth0 for admin network
(4) re0 for storage/cluster interconnect
(5) re1 for storage/cluster interconnect
Active/standby bond over physical links for HA
Separate VLANs for isolation between client and backup networks and VM clusters
Separate layer 2 networks for isolation between management network
Separate layer 2 networks for isolation on storage and cluster interconnect networks

Figure 3: VM Cluster Network Isolation

The Control Plane Server accesses the Oracle Cloud Infrastructure (OCI) control plane via public Internet. The Control Plane Server reaches the Internet via a layer 2 Ethernet connection to a customer-managed switch. The customer provides time services (NTP), name resolution (DNS) for Internet hostnames, and routing for the Control Plane Server connection to the OCI control plane. The Control Plane Server does not require inbound TCP connections, and only requires outbound connections to Oracle IP addresses on TCP port 443, described in the Control Plane Server Networking section of this document. Customers may and should impose network access rules to deny inbound access to the Control Plane Server and to only permit outbound access to required Oracle endpoints. The minimum required bandwidth for the connection from the CPS to OCI control Plane is 50 Mbps for downloads and 10 Mbps for uploads.

The Exadata Database (DB) Server is connected to a customer managed layer 2 switch via 10Gb or 25Gb Ethernet. The customer has access to customer virtual machines (customer VM) via a pair (client and backup) of layer 2 (tagged VLAN) network connections to the customer VM that are implemented as virtual network interface cards (vNICs). The physical network connections are implemented for high availability in an active/standby configuration.

The customer VM accesses Exadata Storage via a private, non-routed interconnect network via SR-IOV mapped interfaces, shown in yellow. Each physical Exadata Database Server and Storage Server has an HA (active/standby) connection to a pair of redundant storage networking switches. The following CIDR describes the standard IP addressing for the storage network configuration: 100.107.0.0/24. If those IP addresses conflict with existing IP addresses, then customers can override this CIDR block with an arbitrary customer-supplied IP address range.

Oracle cloud automation accesses the customer VM via a NAT address on the management network implemented on a vNIC in the Exadata Database Server, shown in red. Oracle cloud automation access to the customer VM is controlled via token based ssh. Temporary and unique ssh key pairs are generated by Oracle cloud automation to access the customer VM for each customer-initiated 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 customer VM, such as `oracle`, `opc`, `grid`, or `root`. The temporary private keys used by the automation are stored in encrypted files on in the ExaDB-C@C hardware in the customer's 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 `root` account can access the keys, but Oracle operator named accounts cannot directly access the keys. Oracle operator named accounts can be permitted to assume the `root` identity or use `sudo` to gain access to root privileges on the infrastructure. The Operator Access Control[54] service

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

can be applied to the ExaDB-C@C service to permit customers to control when Oracle operators can gain access to the ExaDB-C@C infrastructure and Autonomous Database Dedicated VMs, and when Oracle operators can gain `root` access on those components.

The customer's OCI Identity and Access Management (IAM) controls govern if and how a customer OCI identity can execute Oracle cloud automation functionality against the customer VM and databases. The customer VM has detective access controls implemented though the Oracle Linux audit system, including detection of `ssh` access by cloud automation. Customers have control to block cloud automation `ssh` access at layers 3 and 4 via firewall configuration in the customer VM; however, this will break cloud automation functionality that must access the customer VM via `ssh`. This functionality includes:

- ASM disk group resize
- Local storage resize
- Customer VM memory resize
- Database patching
- Grid Infrastructure patching
- Customer VM OS patching

Oracle cloud automation does not need network access the customer VM to perform OCPU scaling, and OCPU scaling functionality will function normally when customers block Oracle cloud automation network access to the customer VM. Oracle cloud automation access may be temporarily restored by the customer to permit the subset of functionality that requires `ssh` access to the customer VM.

ExaDB-C@C Service Delivery

Figure 4 depicts examples of the TCP ports and protocols used to deliver the ExaDB-C@C service.[55]

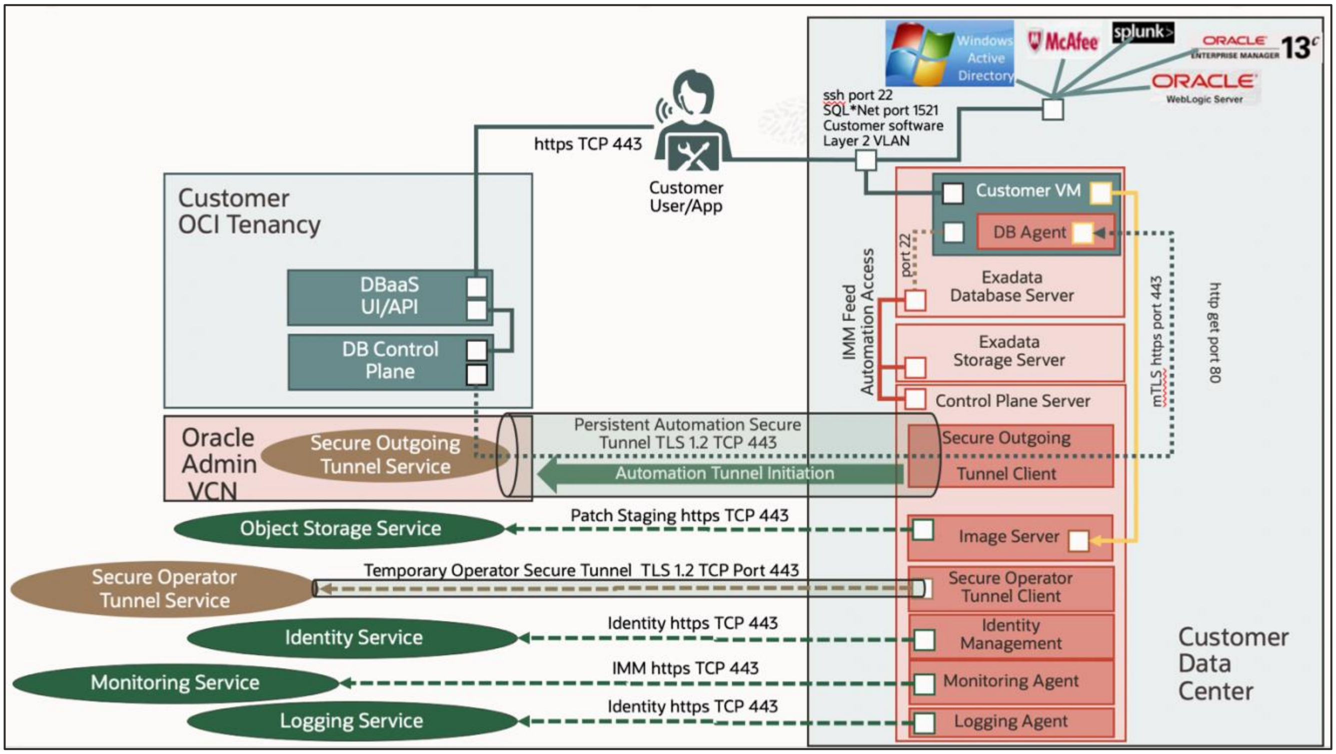

Figure 4: ExaDB-C@C Service Ports and Protocols

Important components of remote service delivery include the following:

- Customer access to Oracle Cloud Infrastructure (OCI) tenancy
- Customer control of access to OCI user interfaces and APIs
- OCI Database Control Plane access to ExaDB-C@C for remote automation delivery
- Secure Outgoing Tunnel Service to connect ExaDB-C@C to OCI region
- OCI Object Storage Service to deliver software updates for ExaDB-C@C components
- Infrastructure monitoring
- Identity management for Oracle Cloud Ops Staff
- Temporary secure tunnel service for Oracle Operator Access (reverse `ssh` tunnel)

The ExaDB-C@C service requires software deployed in the customer VM to communicate with the Oracle control plane. Implementation details for the processes, user ids, and network communication ports implemented in the ExaDB-C@C customer VM are published in the Exadata Database Service on Cloud@Customer Security Guide.[56]

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; customers may not access the ADB-D VM per the ADB-D service definition; OpCtl may be used by the customer to control Oracle access to the ADB-D VM

[55] Service endpoints are abbreviated for the clarity of the drawing; reference

Table 2: Required outbound URL access for ExaDB-C@Cand https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-network-requirements.html#GUID-F06BD75B-E971-48ED-8699-E1004D4B4AC1 for a comprehensive list of URL endpoints

[56] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html#GUID-519A41E4-A97D-476E-B4BA-745C3486C779

- A second persistent Secure Outgoing Tunnel Service is used to access ADB-D-specific endpoints for the purposes of delivering ADB-D service functionality
- A second temporary Secure Operator Tunnel Service is established to an ADB-D-specific endpoint to permit Oracle ADB-D support operators `ssh` access to the ADB-D VM

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

Customer VM Default Users, Security Settings, and Processes and Certificates

Customer VM Default Users

The ExaDB_C@C service includes several user accounts regularly manage the components deployed in the ExaDB-C@C customer VM. In all Exadata Cloud@Customer machines, Oracle uses and recommends SSH based login only. No Oracle user or processes use password-based authentication system. The Guest VM Default Users[57] product documentation indicates all the operating system users that are deployed as part of the service. The service includes 5 privileged service account users:

- `root`: Linux requirement, used sparingly to run local privileged commands. root is also used for some processes like Oracle Trace File Analyzer Agent and ExaWatcher.
- `grid`: Owns Oracle Grid Infrastructure software installation and runs Grid Infastructure processes.
- `oracle`: Owns Oracle database software installation and runs Oracle Database processes.
- `opc`:
  - Used by Oracle Cloud automation for automation tasks.
  - Has the ability to run certain privileged commands without further authentication (to support automation functions).
  - Runs the local agent, also known as “DCS Agent” that performs lifecycle operations for Oracle Database and Oracle Grid Infastructure software (patching, create database, and so on).
- `dbmadmin`:
  - The dbmadmin user is used for Oracle Exadata Database Machine Command-Line Interface (DBMCLI) utility.
  - The dbmadmin user should be used to run all services on the database server. For more information, see Using the DBMCLI Utility.

Note, security scanning tools that assess user accounts separately from service accounts should consider that the `root`, `grid`, `oracle`, `opc`, and `dbmadmin` accounts are service accounts rather than interactive user accounts. Customers may use the `opc` account to access the customer VM for system administration purposes and to configure customer-specific authentication (e.g., LDAP) or privileged access management (PAM) software that is compatible with the ExaDB-C@C customer VM.

Oracle recommends using the service with the user names, user ids (UID), group names, and group id (GID) deployed in the deployed configuration. Changing the Oracle Home user (`oracle`) or Grid Infrastructure user (`grid`) after install is not supported and will cause service exceptions.[58]

Customer VM Default Security Settings

In addition to all the Exadata features explained in Security Features of Oracle Exadata Database Machine,[59] the ExaDB-C@C customer VM includes the following security configuration settings that can be referenced from the ExaDB-C@C Security Guide Guest VM Default Security Settings[60] product documentation:

- Implementing password aging and complexity policies
- Defining account lockout and session timeout policies
- Restricting remote root access
- Restricting network access to certain accounts
- Implementing login warning banner

These settings include:

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

[58] https://docs.oracle.com/en/database/oracle/oracle-database/19/cwwin/about-the-oracle-home-user-for-the-oracle-grid-infrastructure-installation.html

[59] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/security.html

[60] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html#GUID-E8850A77-C206-4127-83C4-B678E9EBF911

- `PermitRootLogin` value in `/etc/ssh/sshd_config`, which permits or denies the root user to login through `SSH`.
  - By default, `PermitRootLogin` is set to without-password.
  - It is recommended to leave this setting to permit the subset of cloud automation that uses this access path (for example, customer VM OS patching) to function. Setting `PermitRootLogin` to no will disable this subset of cloud automation functionality.
- `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`.
  - Defaults to `hard maxlogins 10` and it is the recommended secure value.
- `ssh-macs`: Specifies the available Message Authentication Code (MAC) algorithms.
- The MAC algorithm is used in protocol version 2 for data integrity protection.
  - Defaults to `hmac-sha1`, `hmac-sha2-256`, `hmac-sha2-512` for both server and client.
  - Secure recommended values: `hmac-sha2-256`, `hmac-sha2-512` for both server and client.
- `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.
  - Defaults to `-M 99999`, `-m 0`, `-W 7`
  - `--strict_compliance_only -M 60`, `-m 1`, `-W 7`
  - Secure recommended values: `-M 60`, `-m 1`, `-W 7`

Note, the shell timeout settings for the service account users include the time required for automation that uses token-based ssh access to function. This includes long running tasks like ASM rebalances that happen as part of an Exadata storage resize. Operating system security scanning tools should be configured to recognize these longer shell timeouts as the required implementation to support these aspects of how the service is delivered.

Oracle recommends that customers allow the security configuration settings deployed in the customer VM to minimize customer operational burden of testing, validating, and maintaining customizations and to avoid the risk of a security configuration change causing a service exception.

Customer VM Default Processes and Certificates

The ExaDB-C@C service includes processes used to run Oracle database, Oracle Real Application Clusters, Oracle Trace File Analyzer (TFA), Exawatcher, and Management Server, as described in the Guest VM Default Processes[61] documentation. The Guest VM Default Port Matrix Table[62], reproduced as Table 3 below, indicates the interfaces, ports, and processes of the software that listens on ports in the customer VM, and the certificate authority (CA) where certificates are applicable.

Oracle recommends that customer security scanners should be configured to allow the use of the Oracle-signed certificates listening on the stated ports as these certificates are integrated into the service and managed by Oracle. Allowing the use of Oracle managed certificates within the service minimizes customer operational burden of managing certificates and reduces the risk of a service exception due to certificate expirations and certificate authority conflicts.

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[63]	N/A
		1521	Oracle TNS listener[64]	Oracle signed, customers may add

[61] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html#GUID-519A41E4-A97D-476E-B4BA-745C3486C779

[62] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html#GUID-93DD9F98-AC6F-4538-AE78-13399C1C02A7

[63] https://docs.oracle.com/en/operating-systems/oracle-linux/openssh/openssh-ConfiguringOpenSSHServer.html

[64] https://docs.oracle.com/en/database/oracle/oracle-database/19/netag/configuring-and-administering-oracle-net-listener.html

		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).	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[65]	customer-controlled certificates
		5000	Oracle Trace File Analyzer[66] Collector	Oracle signed
		7879	Jetty Management Server.[67] Application server engine that is used internally by Oracle Exadata System Software, in particular Management Server (MS).[68]	Oracle signed
	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 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 signed, customers may add customer-controlled certificates
Bridge on backup VLAN	bondeth1	7879	Jetty Management Server	Oracle signed

[65] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-secure-sockets-layer-authentication.html#GUID-6AD89576-526F-4D6B-A539-ADF4B840819F

[66] https://docs.oracle.com/en/database/oracle/oracle-database/19/atnms/managing-and-configuring-tfa.html

[67] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmso/application-server-update-management-server.html

[68] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmso/management-server-database-servers.html

Oracle Clusterware[69,70] 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 signed
		Dynamic Port: 9000-65500 Ports are controlled by the configured ephemeral range in the operating system and are dynamic.	System Monitor service (osysmond) Cluster Logger service (ologgerd) Cluster Health Monitor[71] uses system monitor (osysmond) and cluster logger (ologgerd) services to collect diagnostic data.	Oracle signed
	clib1/clre1	5054	Oracle Grid Interprocess communication	N/A
		7879	Jetty Management Server	Oracle signed
Cluster nodes use these interfaces to access storage cells (ASM disks). However, the IP/ports 7060/7070 attached to the	stib0/stre0	7060	dbcs-admin Cloud agent for handling database lifecycle operations[72]	Oracle signed
		7070	dbcs-agent	Oracle signed

[69] https://docs.oracle.com/en/database/oracle/oracle-database/19/cwadd/introduction-to-oracle-clusterware.html#GUID-7612C5C2-AC7C-4311-97B2-CF189268969A

[70] https://docs.oracle.com/en/database/oracle/oracle-database/19/rilin/port-numbers-and-protocols-of-oracle-components.html

[71] https://docs.oracle.com/en/database/oracle/oracle-database/19/atnms/understanding-cluster-health-monitor-services.html

[72] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html#GUID-519A41E4-A97D-476E-B4BA-745C3486C779

storage interfaces are used to access DBCS agent from the Control Plane server.			Cloud agent for handling database lifecycle operations[73]	
	stib1/stre1	7060	dbcs-admin	Oracle signed
		7070	dbcs-agent	Oracle 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),[74] part of Oracle Grid Infrastructure 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.	N/A
		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[75]	Customer-controlled or Oracle signed

Customer Access to OCI Interfaces

The customer accesses cloud automation services in their OCI tenancy via an https connection on port 443 to the OCI Control Plane. The OCI Control Plane provides the following management interfaces:

[73] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html#GUID-519A41E4-A97D-476E-B4BA-745C3486C779

[74] https://docs.oracle.com/en/database/oracle/oracle-database/19/cwadd/introduction-to-oracle-clusterware.html

[75] https://docs.oracle.com/en/cloud/paas/data-safe/admds/create-oracle-data-safe-onpremises-connector1.html

- Web User Interface (web UI) – typically for ad hoc actions
- Oracle Cloud Shell - Linux shell directly in the Oracle Cloud Infrastructure Console
- OCI Command Line Interface (OCI CLI) – typically for programmatic actions from an operating system shell
- REST API (OCI software development kit, OCI SDK) – typically for application integration
- Terraform – for infrastructure as code

Access to OCI management interfaces is controlled by the customer via OCI Identity and Access Management (IAM). If a customer managed identity is authorized to perform a requested action, then the action is delivered to the appropriate ExaDB-C@C components as follows:

- DBaaS UI/API sends request to DB Control Plane via https
- DB Control Plane sends the request via REST API to a proxy service (CPS Proxy) via the Persistent Secure Tunnel Service Admin VCN
- TLS 1.2 Persistent Secure Tunnel Service in the OCI Admin VCN and the CPS delivers REST API request to the CPS proxy running on the CPS in the ExaDB-C@C rack
- The CPS proxy issues commands to ExaDB-C@C components:
    - Actions that require access to Database Services in the customer VM are sent to the DB Agent running in any or all the customer VMs (e.g., up to 4 VMs in a half rack) via secure connection between the OCI control plane and each DB Agent; this mTLS connection is implemented through the private interconnect network in the ExaDB-C@C rack and ports are detailed in the Exadata Database Service on Cloud@Customer Security Guide[76]
    - Actions that require access to the customer VM are executed via token-based `ssh` over the internal management network implemented as a NAT address on the customer VM that is accessible from the Exadata Database Server; the public `ssh` keys are temporary, generated for the purpose of the customer-invoked management action, and are stored in the `authorized_keys` files of the `oracle`, `opc`, `grid`, and/or `root` users in the customer VM; the private `ssh` keys are temporary, generated for the purpose of the customer-invoked management action, and stored in encrypted files by the Oracle cloud automation software running in the Exadata hardware stored in the customer's data center
    - Actions that require access to infrastructure components are issued via token-based `ssh` over the internal management network from the CPS to the required endpoint (e.g., Exadata Storage Server, Exadata Database Server)

Infrastructure Monitoring

Oracle monitors and generates alerts if it is actionable by Oracle as indicated in Gen 2 Exadata Database Cloud At Customer - Explanation Of Cloud Operations Service (Doc ID 2707015.1).[77] Oracle monitors the infrastructure layer, which includes Exadata Compute (Dom0), Exadata Cell, Network Switches and Control Plane Server (CPS) via the Exadata Database Machine alerting mechanism. Additional monitoring is implemented for node availability, disk utilization, network devices, etc..

Oracle does not monitor performance metrics which are not actionable by Oracle, such as Flash Cache usage, IO usage, etc.. Oracle does not monitor Guest VM, CRS, ASM, Database and any additional software running on the Guest OS. It is customer's responsibility to monitor Guest VM, CRS/ DB, etc..

The ExaDB-C@C infrastructure components report their Infrastructure Management Metrics (IMM) to the CPS, and the CPS relays this information to Oracle for processing. The IMM connection is implemented via https with endpoint specific the OCI region used to manage the ExaDB-C@C service.

Oracle Support performs monitoring and maintenance of the ExaDB-C@C implementation as follows:

- Automated monitoring on Oracle Cloud@Customer infrastructure components sends Infrastructure Monitoring Metrics (IMM) via an infrastructure monitoring utility deployed on the CPS to the OCI Telemetry Service endpoint
    - Chassis temperature, drive status, etc.
    - Details for all monitoring data are published at Auto Service Request Qualified Engineered Systems Products[78]
- Automated monitoring on application and security logs sends application and security logs to the Oracle-managed OCI Logging service endpoint

[76] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html#GUID-519A41E4-A97D-476E-B4BA-745C3486C779

[77] https://support.oracle.com/knowledge/Oracle%20Cloud/2707015_1.html

[78] https://docs.oracle.com/cd/E37710_01/doc.41/e37287/toc.htm

- Oracle Support analyzes monitoring data, determines which events require correction, creates support tickets, and assigns support tickets to OCI support staff
- After being assigned a ticket, Cloud Ops support staff are dispatched to perform required support actions

Quarterly Software Updates

Details for how Oracle and customers work together to perform Exadata Database Service on Cloud@Customer software updates are published in the Maintaining an Exadata Database Service on Cloud@Customer Service[79] documentation. My Oracle Support Document 2333222.1, Exadata Cloud Software Versions[80] provides information about current and historical software versions available for ExaDB-C@C.

Quarterly bundle patches for the Oracle database, Grid Infrastructure, and customer VM operating system are staged to the CPS from OCI object storage by Oracle. The quarterly software updates are listed for the customer in the cloud automation user interfaces, and application of those patches is controlled by the customer via OCI tools and policies. Patches are accessed for application via outbound http (port 80) connections from the customer VM to the Image Server running on the CPS. Customers control what identities can apply software updates to ExaDB-C@C resources using OCI Policies.[81]

Quarterly patch bundles and software updates for ExaDB-C@C infrastructure components are deployed by Oracle cloud automation. Customers control if the update is applied as a rolling upgrade to one component at a time or if all components are taken offline and updated at the same time using OCI interfaces.[82] Customers control when quarterly software updates are applied by Oracle using OCI interfaces.[83] Quarterly patch bundles and software updates are applied via API access by Oracle identities that are controlled by Oracle IAM Policies. Oracle operator shell access is not required or used for quarterly software updates unless an exception condition is detected in the precheck or apply processes. Customers using Operator Access Control will only receive an Access Request if an exception condition is detected during the patch precheck or apply process.

Monthly Security Scans and Updates

Security maintenance,[84] performed alongside the quarterly maintenance, is executed in months when important security updates are needed and includes fixes for vulnerabilities with CVSS scores greater than 7.

Security maintenance, when needed, is scheduled to be applied during a 21-day window that begins after the 15th of each month. Customers will receive notification of the proposed schedule at least 7 days before the start of the monthly maintenance window and can reschedule monthly maintenance to another date in the window if desired. Monthly security maintenance contains fixes for all security vulnerabilities identified during the previous month's scans. Updates to database servers are applied online via Ksplice technology, while updates to storage servers are applied in a rolling fashion.

For more information about the CVE release matrix, see Exadata Database Machine and Exadata Storage Server Supported Versions (Doc ID 888828.1).[85]

Scan results are secured internally at Oracle and are not shared publicly or with customers for security reasons. Oracle's Software Security Assurance Practices[86] detail how Oracle handles and communicates software vulnerabilities.

[79] https://docs.oracle.com/en-us/iaas/Content/Database/Concepts/examaintenance.htm

[80] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2333222.1

[81] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-policy-details.html#GUID-523EBAE0-C17F-435A-97A6-374DE2F94747

[82] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-config-infra-maintenance.html#GUID-1E61C3AE-FD67-4B22-9D26-04F0D352BF22

[83] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-config-infra-maintenance.html#GUID-19B3645B-854A-488C-B149-CB3D827548D7

[84] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-vw-maint-hist.html#GUID-A2008207-3683-424F-9279-F632BF4C9076

[85] https://support.oracle.com/epmos/faces/DocumentDisplay?id=888828.1

[86] https://www.oracle.com/corporate/security-practices/assurance/

Software Update Security Controls

All software updates are controlled by Oracle Software Security Assurance Practices.[87] The initial software deployment packages and all software updates managed by Oracle for the ExaDB-C@C service are signed and encrypted prior to delivery to the service. The ExaDB-C@C service automatically checks these software updates for a valid signature, and if the detected signature is invalid the software update is rejected and an alert is sent to Oracle. Oracle Software Security Assurance[88] standards apply to ExaDB-C@C software. Oracle implements segregation of duties[89] for software development, software test and quality assurance, and deployment of software ExaDB-C@C components.

PREVENTIVE CONTROLS

The ExaDB-C@C service is designed to protect customer services and database data from unauthorized access. The ExaDB-C@C service separates duties between the customer and Oracle. The customer controls access to customer services, databases, and database data. Oracle controls access to Oracle-managed infrastructure components.

Customer Access Controls

The customer controls access to their VMs, databases, and data via 3 types of controls:

- Authentication
  - Credentials for customer identities to access OCI services,[90] customer VM operating system and databases,[91] and database data[92]
  - Temporary Delegate Access Control[93] credentials for customers to control Oracle support and services staff access to the customer VM
- Network
  - Layer 2 VLANs to access customer VMs[94]
  - Network access rules implemented in the customer VM operating system[95] and Oracle database[96]
  - Temporary Delegate Access Control networks and bastion servers to allow Delegate Access Control credentials to authenticate to the customer VM
- Encryption
  - Application to database encryption[97]
  - Database to storage encryption[98]

The ExaDB-C@C software does not provide interfaces for customers to configure firewalls, disable network interfaces, or disable cloud automation software agents running in the customer VM. Customers with exceptional security requirements may implement such controls using operating system tools; however, this action will disable cloud automation functionality that accesses the customer VM. Customers will need to remove these controls and enable cloud automation software agents using operating system tools to restore cloud automation functionality that accesses the customer VM.

[87] https://www.oracle.com/corporate/security-practices/assurance/

[88] https://www.oracle.com/corporate/security-practices/assurance/

[89] https://www.oracle.com/corporate/security-practices/corporate/access-control.html

[90] https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm

[91] https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/exadata/doc/ecc-connecting-to-exacc-system.html

[92] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-privilege-and-role-authorization.html#GUID-89CE989D-C97F-4CFD-941F-18203090A1AC

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

[94] https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/exadata/doc/ecc-setting-up-the-network.html

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

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

[97] ExaDB-C@C automation configures Oracle Native Network Encryption; customers may override this control; Oracle strongly recommends that customers preserve this control

[98] ExaDB-C@C automation configured Oracle Transparent Data Encryption (TDE); Oracle strongly recommends that customers preserve this control

Customer Access Control for ExaDB-C@C Services

Customers perform management actions via OCI automation by making an https connection to the Oracle Public Cloud Control Plane in the OCI region chosen by the customer. The customer is authenticated using their OCI Identity and Access Management (IAM) credentials, and customer actions are controlled via OCI IAM permissions configured by the customer for specific resources. If the customer user is authorized to perform the requested management action on the target resource, then the requested command is sent to the local Control Plane Servers (CPS) via the Persistent Secure Tunnel Service for delivery into the appropriate ExaDB-C@C components.

Customers and database applications access databases running on the ExaDB-C@C via a layer 2 (tagged VLAN) network connection hosted in the customer VM. Access to databases and operating system is made via customer managed credentials.

Customer Controls for Data Security

Oracle ExaDB-C@C is designed to help secure data for legitimate customer use and to help protect data from unauthorized access, which includes preventing access to customer data by Oracle Cloud Ops staff members. Security measures designed to protect against unauthorized access to ExaDB-C@C infrastructure, customer VMs, and Oracle database data include the following:

- Customer retains control over named and privileged (e.g., `sys`, `system`) user authentication and access to customer database
- Customer retains control over named and privileged (e.g., `root`, `opc`, `oracle`, `grid`) user authentication and access to customer VM
- Customer can control Oracle support and services staff access to customer VM via Delegate Access Control[99]
- Access to customer VM is logged by the customer VM operating system, these logs are available to the customer, and the customer can send these logs to other security information event management (SIEM) systems of their choice
- Customers can install scanning agents on the customer VM for the purposes of detecting malware; customers should review Responses to common Exadata security scan findings (My Oracle Support Doc ID 1405320.1)[100] prior to scanning the customer VM; customer security scanning/testing must adhere to Oracle Cloud Testing Policy[101]
- Customer can install monitoring agents and security controls of their choice on the customer VM operating system if these agents don't taint the Linux kernel or interfere with Exadata operation
- Network connections to the Oracle database are designed to be encrypted by Oracle Native Network Encryption, which is automatically configured by cloud automation
- Oracle database data is encrypted at rest by Oracle Transparent Data Encryption (TDE)
  - Automatically configured by cloud automation and stored in password-protected, PKCS#12 wallet file stored in an ASM Cluster File System (ACFS)[102] hosted on the Exadata Storage that is accessible from the customer VM
  - Customer controls access to TDE encryption keys via the wallet password
  - Customer can move the TDE master key to an external key store, such as Oracle Key Vault
- Oracle Database Vault[103] may be configured to help protect user data access from database administrators

Figure 5 shows compensating controls within the Oracle Database that protect customer data access from people or software that can gain access to infrastructure and customer VM components:

- Oracle Native Network Encryption[104]
- Oracle Database Vault[105]
- Oracle Transparent Database Encryption (TDE)[106]

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

[100] https://support.oracle.com/rs?type=doc&id=1405320.1

[101] https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm

[102] https://docs.oracle.com/en/database/oracle/oracle-database/19/ostmg/overview-acfs-advm.html

[103] https://docs.oracle.com/en/database/oracle/oracle-database/19/dvadm/introduction-to-oracle-database-vault.html#GUID-0C8AF1B2-6CE9-4408-BFB3-7B2C7F9E7284

[104] Included with Enterprise Edition Extreme Performance subscription and with Bring Your Own License (BYOL) subscription

[105] Included with Enterprise Edition Extreme Performance subscription, not included with Bring Your Own License (BYOL) subscription

[106] Included with Enterprise Edition Extreme Performance subscription and with Bring Your Own License (BYOL) subscription

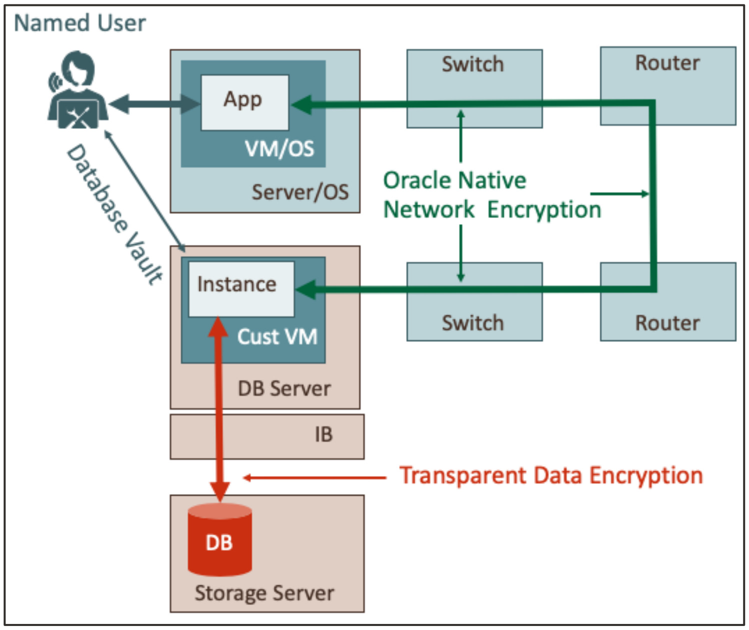

Figure 5: Controls to Protect Data in Flight and at Rest

Oracle Native Network Encryption

Oracle Native Network Encryption encrypts data in flight between the application and the Oracle database instance and is automatically configured for databases created via the ExaDB-C@C automation. When Oracle Native Network Encryption is enabled, access to infrastructure components that can observe IP and Ethernet packets does not provide access to customer data because the data is encrypted. Documentation for Oracle Native Network Encryption and TLS/SSL is published in the Security Guide for each Oracle Database version. For example, for Oracle database 19c, see https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-network-data-encryption-and-integrity.html#GUID-7F12066A-2BA1-476C-809B-BB95A3F727CF. ExaDB-C@C cloud automation does not provide interfaces to configure TLS/SSL for Oracle database connections. Customers may configure TLS/SSL using the operating system tools deployed in the customer VM.

Oracle Database Vault

Oracle Database Vault security controls are designed to help protect application data from database administrator access and help 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. Customers are responsible for configuring and managing Oracle Database Vault via Oracle database software methods. Documentation for Oracle Database Vault is published in the Oracle Database Vault Administrator's Guide[107] published for each database version.

Oracle Transparent Data Encryption and Oracle Key Vault

Oracle Transparent Data Encryption (TDE) encrypts user tables and tablespaces in the Oracle database. The encryption is transparent to authorized applications and users because the database automatically encrypts data before it is written to storage and automatically decrypts it when reading from storage. Authorized applications that store and retrieve data in the database only see the decrypted (or "plaintext") data. TDE prevents privileged operating system users, network and storage administrators (or someone masquerading as them) from bypassing the database controls to access the data directly. Authorized database users and applications do not need to present the decryption key when they process encrypted data. Instead, the database enforces the access control rules described in the previous chapters and denies access if the user is not authorized to see the data.

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.

[107] 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

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.

TDE uses a two-tier key architecture comprising of data encryption keys that are encrypted with a master encryption key. That master encryption key is stored outside of the database, by default in a PKCS#12 compliant container called a 'wallet' in an ACFS file system which provides a shared wallet location that is accessible to both instances of the RAC-enabled databases. Furthermore, 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. Customers may choose to migrate their ExaDB-C@C databases to Oracle Key Vault (OKV)[108], the only key management solution for your Oracle database estate that provides continuous key availability by adding up to 16 OKV nodes to a key management cluster that can span geographically distributed data centers and the Oracle Cloud Infrastructure (OCI). Oracle Key Vault 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).

For further information on Oracle TDE, consult the Advanced Security Guide for the Oracle database version you are running

The Oracle TDE FAQ[109] provides answers to common Oracle TDE architecture and implementation questions.

Oracle supports customers using Oracle Key Vault (OKV) as an external key store for databases running on ExaDB-C@C. ExaDB-C@C is integrated with OKV[110] so that customers can use cloud automation interfaces to migrate TDE keys to OKV and rotate TDE keys. Instructions for using operating system methods to migrate TDE Master Keys to OKV are published in My Oracle Support Document 2823650.1 (Migration of File based TDE to OKV for Exadata Database Service on Cloud at Customer Gen2[111]) and Oracle Cloud Automation can be used to automate the process of migrating TDE Master Keys to OKV and rotating them.[112]

Customers have the option to use the OKV Persistent Master Encryption Key Cache[113] to enable databases to be operational if the OKV server is unavailable.

Details for the TDE implementation on ExaDB-C@C are shown in the Exadata Database Machine Cryptographic Services[114] documentation.

Oracle Transparent Data Encryption and Third-Party Hardware Security Modules (HSM)

Oracle Database is compatible with PKCS#11 compatible key management devices.[115]

Oracle Database leverages PKCS#11, an open key management standard, to interface with external key managers. 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)[116] for implementation and support details.

Integrating an external key manager requires the installation of PKCS#11 libraries on the ExaDB-C@C customer VM which, in the case of third-party solutions are, developed, tested, and provided to the customer by the vendor. 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

[108] https://docs.oracle.com/en/database/oracle/key-vault/21.2/okvag/okv_intro.html#GUID-0D169EB8-C355-459A-9ABD-325CA5B46DD0

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

[110] https://docs.oracle.com/en-us/iaas/exadata/doc/manage-encryption-keys-on-external-devices.html#GUID-B1EE94A4-2852-4376-949D-25E6E286B932

[111] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2823650.1

[112] https://docs.oracle.com/en-us/iaas/exadata/doc/manage-encryption-keys-on-external-devices.html#GUID-B1EE94A4-2852-4376-949D-25E6E286B932

[113] https://docs.oracle.com/en/database/oracle/key-vault/21.7/okvag/security_objects.html#GUID-27DA6A5A-E405-4394-BD0D-C2B213391426

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

[115] https://docs.oracle.com/en/database/oracle/oracle-database/19/asoag/introduction-to-transparent-data-encryption.html#GUID-2D6C5B27-8E6A-4EF7-AABF-B0FB031C8374

[116] https://support.oracle.com/knowledge/Oracle%20Database%20Products/2310066_1.html

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.[117]

Controls for Cloud Automation Access to Customer VM

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

- Secure login to customer VM as a privileged user (`root`, `opc`, `oracle`) via token-based `ssh`
- REST API call to Oracle software agent running in customer VM via mTLS authentication; port matrix and software processes are published in the Exadata Database Service on Cloud@Customer Security Guide[118]

The customer VM provides the Oracle Linux packet filtering software[119] as a compensating control for customers to control network access to the customer VM, including blocking control plane software access. Customers may use Oracle Linux operating system administration tools to configure packet filtering software. ExaDB-C@C automation does not include functionality or interfaces to configure Oracle Linux packet filtering software.

Customers do not have direct access to the infrastructure components for the purposes of determining source IP addresses for packet filtering software configuration, and for testing customer VM firewall configuration for the purposes of blocking control plane access to customer VM. Customers should use the Oracle SR process to request Cloud Ops support to determine the necessary firewall rules, and to validate that the customer VM firewall configuration blocks control plane access as required.

Oracle cloud automation secure login via token-based `ssh` is not compatible with Kerberos authentication, and Oracle cloud automation functionality may cease to function if customers implement Kerberos authentication in the customer VM to control service accounts. For details, please see Oracle Support Document 2621025.1 (Does ExaCC VM's Support Kerberos Authentication).[120]

As of Exadata software version 22.1.4.0.0.221020, Microsoft Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) authentication to the customer VM can be implemented by customers on ExaDB-C@C. ExaDB-C@C does not provide cloud automation support for this configuration. Customers can configure AD and LDAP by directly accessing the ExaDB-C@C customer VM to implement AD and LDAP. Customers should note that the ExaDB-C@C customer VM updates[121] are executed as image updates like how the Exadata Database Machine image update process,[122] and that customers should test and validate how their AD or LDAP implementation is affected by the image update process. Customers should plan for the possibility of needing to temporarily disable or remove AD or LDAP during a patch cycle, and then reinstate AD or LDAP following the patch if the implementation of AD or LDAP is not compatible with the image update process.

Controls for Customer Staff Access to Customer VM

SSH Access to the Customer VM via Client Network

Access to the customer VM is implemented via token-based `ssh`.[123] Customers use their OCI Cloud Tenancy credentials and controls to add customer-specified public keys to the `/home/oracle/opc/.ssh/authorized_keys` file of the `opc` user as described in the Accessing an Exadata Database Service on Cloud@Customer Instance[124] documentation. Customer staff with access to the private keys associated with the installed public keys can gain access to the customer VM via token-based `ssh`. Oracle cloud automation does not

[117] https://docs.oracle.com/en/database/oracle/key-vault/21.3/okvhm/index.html#Oracle%C2%AE-Key-Vault

[118] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html

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

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

[121] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-update-exacc-system.html

[122] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmmn/updating-exadata-software.html#GUID-E6090FA9-13B4-4BEF-A28D-73BDC3729C58

[123] https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/exadata/doc/ecc-connecting-to-exacc-system.html

[124] https://docs.oracle.com/en/cloud/cloud-at-customer/exadata-cloud-at-customer/exacc/connect-ssh.html#GUID-C5DAB5B8-1FFA-4122-9181-189561F6E0F1

integrate with customer key management systems, and customers can manage ssh keys using technology compatible with Oracle Linux.

VM Console Access via OCI Control Plane

Access to the customer VM console is implemented via token-based ssh tunnel through the control plane to the hypervisor console of the customer VM.[125,126] Access is controlled in 3 steps:

1. Customer 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. Customer ssh credentials are use to create an ssh connection from a customer 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 the customer VM console using the username and password permitted to authenticate to the customer VM operating system console, typically the root user; this password is controlled by the customer

The cloud shell console connection is automatically terminated 24 hours after it is created, and customers must reauthenticate to OCI to reestablish the console connection. Customers may terminate the console connection at any time using the OCI console or API interfaces.

Figure 6 describes the steps to create the console connection for an ssh connection on port 443 to an OCI endpoint. The workflow is as follows:

1. Customer 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 the customer OCI user is authorized by IAM Policy to create the VM console connection
3. Cloud automation software injects the customer 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 the customer data center to the OCI endpoint that supports the VM console ssh tunnel

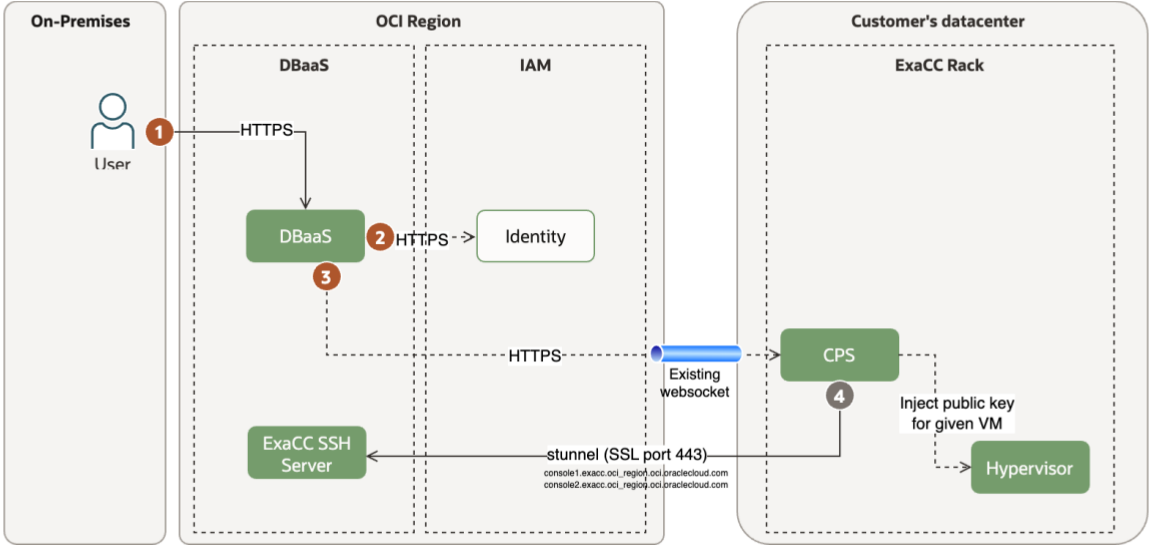

Figure 6: Workflow block diagram to create ssh tunnel to VM console

Figure 7 describes the steps to establish an ssh connection from a customer device to the VM console. The workflow is as follows:

1. Customer initiates 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

[125] https://docs.oracle.com/en-us/iaas/releasenotes/changes/9cee8331-1a56-494c-9bcc-f0dab3eea1b4/

[126] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-manage-vm-clusters.html#GUID-34F8308B-480A-4DAE-A158-2B4856E41A90

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

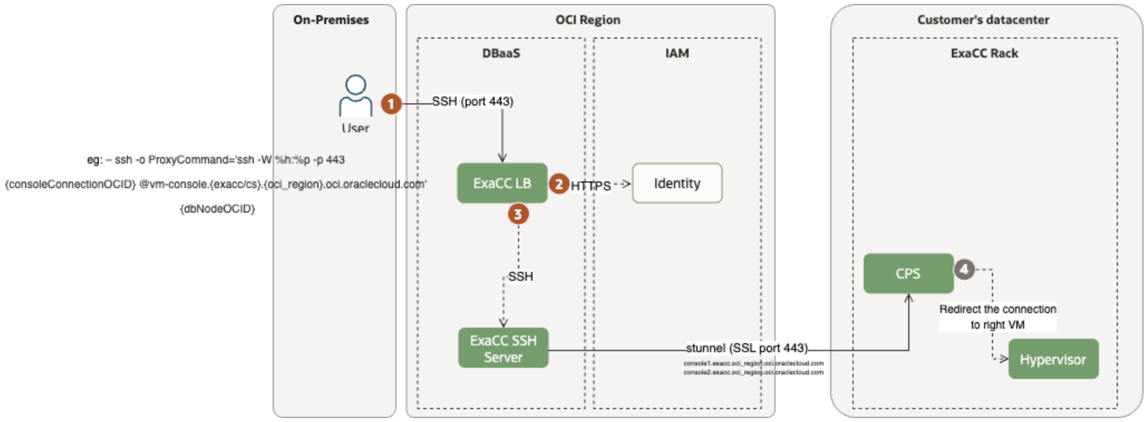
On-Premises
OCI Region
Customer's datacenter
DBaaS
IAM
ExaCC Rack
User
1
SSH (port 443)
eg: – ssh -o ProxyCommand='ssh -W %h:%p -p 443
{consoleConnectionOCID} @vm-console.{exacc/cs}.{oci_region}.oci.oraclecloud.com'
{dbNodeOCID}
ExaCC LB
2
HTTPS
Identity
3
SSH
ExaCC SSH Server
stunnel (SSL port 443)
console1.exacc.oci_region.oci.oraclecloud.com
console2.exacc.oci_region.oci.oraclecloud.com
CPS
4
Redirect the connection to right VM
Hypervisor

Figure 7: Workflow block diagram to establish an ssh connection via port 443 to an OCI endpoint

Figure 8 describes the steps to create a VM console connection and establish an ssh connection using the OCI Cloud Shell. Note, this process uses system generated and protected temporary ssh keys to rather than user-supplied ssh keys. The workflow is as follows:

1. Customer 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. Customer OCI IAM user invokes Cloud Shell extension
4. OCI IAM validates the customer 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 to inject the public key and create the SSH connection tunnel
7. CPS Creates ssh connection and Cloud Shell connects to the serial console

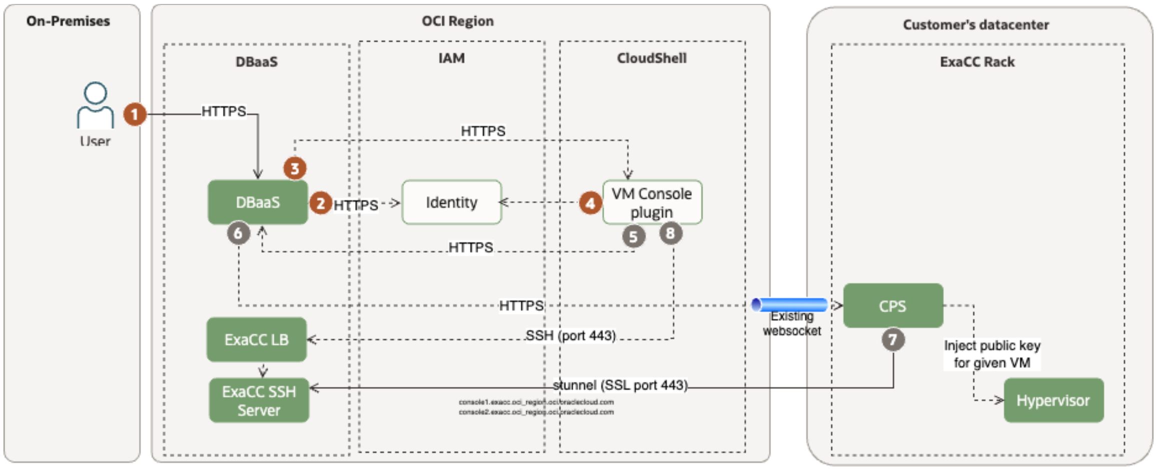

Figure 8: Workflow block diagram to establish an ssh connection to the VM console using the OCI Cloud Shell

Figure 9 shows the workflow to terminate a VM console connection

1. Customer 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

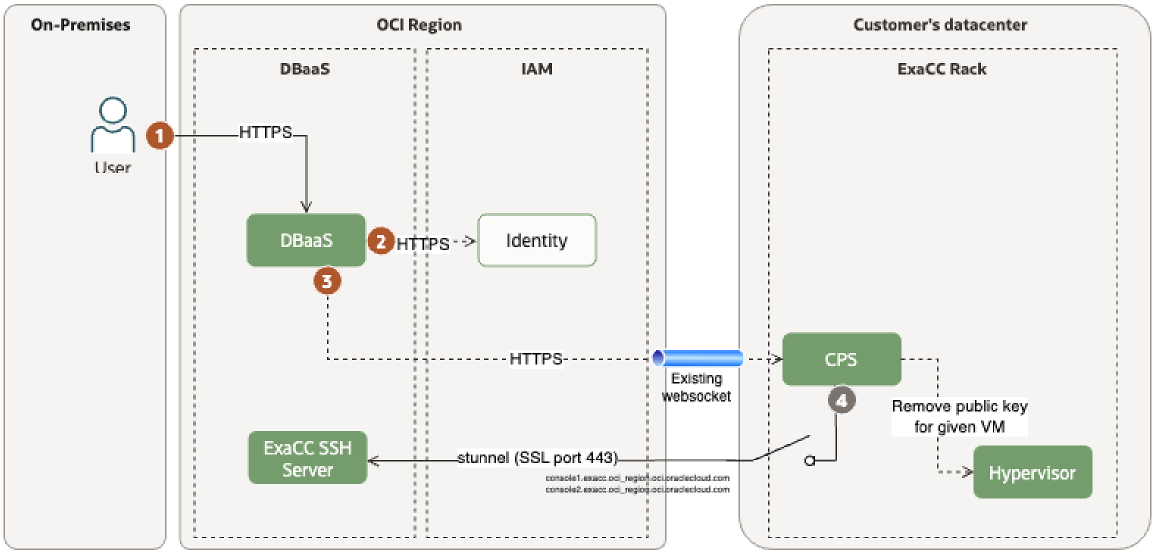

Figure 9: Workflow block diagram to terminate a VM console ssh connection

Controls for Protecting Against Theft of Data

Data stored in user tables and tablespaces in databases running on ExaDB-C@C is encrypted by Oracle Transparent Data Encryption (TDE). Theft of encrypted data is of limited use, due to the technical difficulty of decrypting the data. The United States Department of Defense (DoD) and National Security Agency (NSA) endorse AES encryption standards to secure data.

Oracle Corporate Security Practices[127] cover the management of security for both Oracle's internal operations and the services, including the ExaDB-C@C service, Oracle provides to its customers, 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.

Privileged Access Management with Operator Access Control and Delegate Access Control

Operator Access Control (OpCtl) [128] is a privileged access management (PAM) service that customers may use to manage Oracle staff can access ExaDB-C@C infrastructure and ADB-D VMs. OpCtl works by revoking all remotely accessible login accounts from the ExaDB-C@C infrastructure and ADB-D VMs, and then deploying unique temporary credentials into specific components for Oracle staff after the customer approves an OpCtl Access Request. The Operator Access Control Tech Brief[129] provides detail for customer security staff evaluating the OpCtl for ExaDB-C@C and ADB-D.

Customers can use OpCtl to control when Oracle staff can remotely log into ExaDB-C@C infrastructure and ADB-D VMs, and when Oracle staff can gain root access to ExaDB-C@C Infrastructure and ADB-D on ExaDB-C@C VMs. OpCtl also provides full command/keystroke logging to customers and customer control to terminate Oracle connections. OpCtl is included in the scope of the Oracle Cloud Infrastructure PCI-DSS Attestation of Compliance (AoC).

Customers can use Oracle Delegate Access Control (DaCtl),[130] to subscribe to Oracle Database Cloud Customer Support and Oracle Database Cloud Operations Support services. Via Delegate Access Control, customers can control when Oracle support staff can gain access to the customer VM, the privileges Oracle support staff have when accessing the customer VM, and get full command/keystroke audit logs recorded during access to the customer VM. These support services are included at no additional charge as part of a subscription to OCPUs for Oracle Database Cloud Services. Delegate Access Control is based on the Operator Access Control technology and is included in the Operator Access Control scope of the Oracle Cloud Infrastructure PCI-DSS AoC.

Customers can use Delegate Access Control to subscribe to add-on services, such as the Oracle Engineered System Infrastructure Deployment and Support[131] service, to control when Oracle professional services staff can access the customer VM, the privileges

[127] https://www.oracle.com/corporate/security-practices/corporate/

[128] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html

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

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

[131] https://www.oracle.com/contracts/docs/oracle-engineered-systems-deployment-and-infrastructure-support.pdf

Oracle professional services staff have when accessing the customer VM and get full command/keystroke audit logs recorded during access to the customer VM. Add-on services may be tailored to meet specific goals and needs, and these services are scoped and charged based on these goals and needs.

Oracle Data Safe

Oracle Data Safe[132] is a security cloud service that is included with your Exadata Cloud at Customer subscription. Data Safe helps you:

- 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

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 Data Safe Technical Architecture[133] includes functionality that supports an on-premises connector deployed on customer-controlled servers to facilitate connecting databases running on ExaDB-C@C to connect to the OCI Data Safe service in an OCI region.

Oracle Database Security Assessment Tool (DBSAT)

The Oracle Database Security Assessment Tool (DBSAT)[134] is a stand-alone command line tool that accelerates the assessment and regulatory compliance process by collecting relevant types of configuration information from the database and evaluating the current security state to provide recommendations on how to mitigate the identified risks.

DBSAT is provided at no additional cost and enables customers to quickly find

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

DBSAT analyzes information on the database and listener configuration to identify configuration settings that may unnecessarily introduce risk. 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, customers can reduce data exposure risk throughout their enterprise.

Oracle Controls for Cloud Operations Access to Infrastructure Components

Oracle Access Control Practices[135] restrict access to Oracle staff with a need to know and need to access ExaDB-C@C infrastructure, and include the following details:

- Authorization to access ExaDB-C@C infrastructure and is limited to specific support staff whose job codes and training records are in compliance with Oracle policies; technical security measures enforce this policy
- Automated HR joiner/mover/leaver processes ensure authorization to access customer infrastructure is consistent with updates to employee job code, training records, and employment status

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

- Power Distribution Units (PDUs)

[132] https://docs.oracle.com/en-us/iaas/data-safe/index.html

[133] https://docs.oracle.com/en/solutions/oracle-data-safe-for-on-prem-database/index.html#GUID-07534FC6-3B10-48E5-BD49-C011D55D1070

[134] https://www.oracle.com/database/technologies/security/dbsat.html

[135] https://www.oracle.com/corporate/security-practices/corporate/access-control.html

- Out of band (OOB) management switches
- Storage Network switches
- Exadata Storage Servers
- Physical Exadata database servers

Figure 10 shows how Oracle Cloud Operations (Cloud Ops) staff access infrastructure components to manage the ExaDB-C@C.

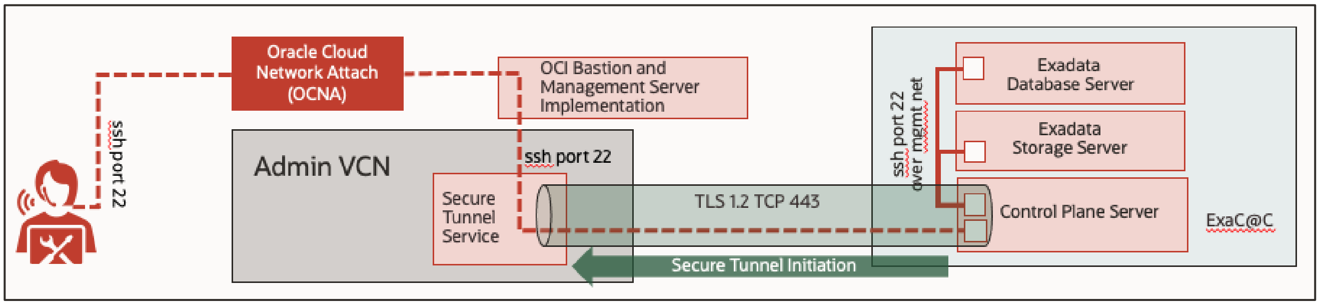

Figure 10: Cloud Operations Staff Access to ExaDB-C@C Infrastructure Components

Oracle controls Oracle Cloud Ops staff access to Cloud Service infrastructure components in the following process:

- Access Oracle Cloud Network Attach (OCNA) using FIPS 140-2 level 3 hardware MFA (Yubikey) based on entitlements specific to job code per Oracle Access Control practices
- Access through Bastion and Management servers for the purposes of proxied `ssh` tunnel access to ExaDB-C@C infrastructure
    - Access through Management and Bastion servers isolated to OCI privileged administrative VCN located in the OCI region hosting the service; entitlements to access and tunnel through Management and Bastion servers controlled by Oracle Access Control practices
    - Connections through Bastion servers are logged and monitored by Oracle
- Login to ExaDB-C@C infrastructure as a named user via `ssh` tunnel using MFA implemented with a FIPS 140-2 Level 3 hardware token (Yubikey)
    - Command execution is traceable to a specific named user via audit logging implemented in the ExaDB-C@C infrastructure
    - Connections to infrastructure components are logged and monitored by Oracle
- Assume the identity of a service account or use `sudo` to gain service account authorization to perform management tasks
    - Command execution is traceable to a specific named Oracle person
    - Connections to infrastructure components are monitored by Oracle

Customers may apply Operator Access Control (OpCtl)[136] to further control Oracle staff access to ExaDB-C@C infrastructure and ADB-D VMs.

Exadata Infrastructure Software Security

ExaDB-C@C is based on the Exadata Database Machine and delivers the enterprise-class security features of Exadata Database Machine in an on-premises cloud model. Security features of ExaDB-C@C include the following:

- Software deployed on ExaDB-C@C infrastructure is limited to the minimum software components to run customer services
- Development and debug tools to inspect customer data are not installed on ExaDB-C@C infrastructure
- Non-essential operating system tools and packages are not installed on ExaDB-C@C infrastructure
- Software development performed under Oracle Software Security Assurance[137]
- Security architecture performed under Oracle Corporate Security Architecture[138]

Details of the Exadata Database Machine security features are available from Oracle at https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/toc.htm.

[136] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html

[137] https://www.oracle.com/corporate/security-practices/assurance/

[138] https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html

DETECTIVE CONTROLS

ExaDB-C@C provides robust detective controls (auditing and logging) for customer services and Oracle managed infrastructure. The customer controls the logging configuration of customer services, and Oracle controls the logging configuration of Oracle managed infrastructure. Oracle is not authorized to access customer service audit logs. The customer may request access to applicable Oracle audit log information via the Oracle service request (SR) process, and customers may view their audit rights in the Oracle Data Processing Agreement (DPA).[139]

Customer Audit Logging of Customer Access

ExaDB-C@C provides 3 areas for auditing and logging of customer actions:

- OCI Audit Service:[140] audit logs for control plane actions (e.g., web UI, OCI CLI, OCI REST API) initiated via a customer's OCI IAM credential
- Oracle database auditing:[141] audit logs for database actions initiated via a customer's Oracle database credential
- Customer VM operating system audit log:[142] audit logs for actions initiated on a customer VM via an operating system credential

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

- 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 Audit service by using the Console, API, or the SDK for Java. Data from events can be used to perform diagnostics, track resource usage, monitor compliance, and collect security-related events. OCI Audit Service[143] documentation.

Oracle database auditing tracks changes made to the Oracle database by database users and non-database users. Customers have the right and responsibility to configure and manage the Oracle database audit log, including sending the audit log a remote log server. Documentation for configuring, managing, and monitoring of Oracle database audit logs is published in the Oracle Database Security Guide for each database version.[144]

The customer VM operating system audit log is implemented as the audit log service for the Oracle Linux (OL) operating system running in the customer VM. The Oracle Linux audit log service records actions executed via operating system credentials, such as `root`, `oracle`, `grid`, `opc`, and named users configured by the customer. Customers may configure the Oracle Linux audit log per their standards, including sending the Oracle Linux audit log to a remote log server. Documentation is published in the Oracle Linux Security Guide[145] for the specific version of the operating system running in the customer VM.

The customer may monitor network access at any point they control, including network access between the CPS and the Internet, network access into the customer VM, and network access from the customer VM to the customer data center.

[139] https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf

[140] https://docs.oracle.com/en-us/iaas/Content/Audit/Concepts/auditoverview.htm

[141] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/introduction-to-auditing.html#GUID-94381464-53A3-421B-8F13-BD171C867405

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

[143] https://docs.cloud.oracle.com/iaas/Content/Audit/Concepts/auditoverview.htm

[144] for 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

[145] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-audit-sec.html

Customer Audit Logging of Oracle Access to Oracle-Managed Resources

Customers may use Oracle Operator Access Control[146] as an additional detective control for Oracle staff access to ExaDB-C@C infrastructure and ADB-D VMs. Operator Access Control provides command and keystroke logging of all commands and keystrokes entered by Oracle staff when they access the ExaDB-C@C infrastructure and ADB-D VM. Operator Access Control audit logs are available via the OCI Logging service and a direct send from the CPS to a customer-specified syslog server. The Operator Access Control Tech Brief[147] provides additional detail.

Customer Security Scanning and Testing of Customer VM

Customers may use OpenSCAP[148] to scan the customer VM for security vulnerabilities.

Customers may use the Oracle Linux Advanced Intrusion Detection Environment (AIDE)[149] 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. It runs on demand, and the time to report changes is dependent on the system checks (usually at least once a day). The utility works by using a number of algorithms (such as, but not limited to, md5, sha1, rmd160, tiger), supports common file attributes and also supports regular expression parsers for file(s) to be included or excluded from the scan.

Customers using third party scanning tools with third party provided benchmarks should take care to update benchmarks to make them compatible with the ExaDB-C@C software distribution and configuration. In some cases, arbitrary benchmarks can flag security issues on the ExaDB-C@C customer VM that may not be a material risk due to compensating controls on the ExaDB-C@C service that the benchmark is not aware of. Customers may reference My Oracle Support Note, "Responses to common Exadata security scan findings (Doc ID 1405320.1)"[150] at to learn more about how common benchmarks may be adjusted to work with Exadata. If the ExaDB-C@C customer VM is modified to comply with a third party or customer designed benchmark these modifications should be tested to validate that they do not compromise ExaDB-C@C software automation. Automated software updates, including operating system, Oracle database, and Grid Infrastructure updates may revert customer changes that are implemented to meet third party provided security benchmarks.

Customer security testing ExaDB-C@C customer VM must be done in accordance with Oracle Cloud Testing Policies.[151]

Customer Use of Third-Party Software on ExaDB-C@C Customer VM

Customers have control to install third party software, including scanning software, on the ExaDB-C@C customer VM. 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. It is highly recommended 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 the customer. Details for third party software support on ExaDB-C@C are published on My Oracle Support Installing Third Party Software On Exadata Components (Doc ID 1593827.1).[152]

Oracle Infrastructure Audit Logging

Audit logging of actions taken in the ExaDB-C@C infrastructure owned by Oracle are the responsibility of Oracle. Oracle maintains the following infrastructure audit logs for ExaDB-C@C X8 and earlier hardware:

- ILOM
  - `syslog`
  - ILOM `syslog` redirected to the `syslog` of the physical infrastructure component
- Physical Exadata Database Server
  - `/var/log/messages`

[146] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html

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

[148] https://support.oracle.com/knowledge/Oracle%20Database%20Products/2793920_1.html

[149] https://support.oracle.com/knowledge/Oracle%20Linux%20and%20Virtualization/2616282_1.html

[150] https://support.oracle.com/knowledge/Oracle%20Database%20Products/1405320_1.html

[151] https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm

[152] https://support.oracle.com/knowledge/Oracle%20Cloud/1593827_1.html

    - `/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`

Oracle retains the following audit logs for ExaDB-C@C X8M and later hardware:

- 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 13 months. Infrastructure audit logs are accessible by Oracle security staff. In the event of a suspect security incident, Oracle and customer staff will work together to respond and resolve the issue per Oracle Incidence Response[153] practices.

RESPONSIVE CONTROLS

The customer and Oracle work together to secure and monitor access to customer services, databases, database data, VMs, and infrastructure. Should either party detect an unauthorized action, that party can take responsive action immediately and prior to notifying the other party, depending on security policy and the details and circumstances around the unauthorized action. If the customer detects an unauthorized action, the customer should notify Oracle of the action and response via the Oracle SR process. Oracle will notify the customer of detected unauthorized actions and Oracle responses.

The customer may take any responsive action on any services or equipment they control. This includes terminating network connections into the customer VM and terminating network connections between the CPS and OCI resources. The database services and databases will continue to function normally if a customer terminates connections between the CPS and OCI resources, and any authorized action that is terminated via this customer response can be restarted.

Customers may use Operator Access Control[154] to terminate Oracle staff access to ExaDB-C@C infrastructure and ADB-D VMs.

Oracle's responsive controls include terminating connections at Bastion Servers in OCI, terminating connections at the CPS, and revoking access to ExaDB-C@C resources.

SERVICE TERMINATION

Customers may terminate their ExaDB-C@C instance as part of ExaDB-C@C Lifecycle Management Operations.[155] Terminating an Exadata Cloud Service resource permanently deletes it and any databases running on it. The terminate service functionality is

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

[154] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html

[155] https://docs.oracle.com/en/cloud/cloud-at-customer/exadata-cloud-at-customer/exacc/delete-exadata-service-instance.html

implemented as Exadata Database Machine Secure Erase.[156] The Exadata Secure Eraser automatically detects the hardware capability of a storage device and picks the best erasure method supported by the device. Cryptographic erasure is used whenever possible to provide better security and faster speed. The cryptographic erasure method used by Secure Eraser is fully compliant with the NIST SP-800-88r1 standard. Customers may obtain secure erase certifications from Oracle by opening a My Oracle Support (MOS) request.

EXCEPTION WORKFLOWS - ORACLE ACCESS TO CUSTOMER VM

ExaDB-C@C service support includes exception cases where a failure in the customer VM requires Oracle staff to access the customer VM to resolve the issue. The process and technical controls that govern how Oracle staff can access the customer VM depend on if the customer VM can be accessed by the customer, or if the customer VM is not accessible by the customer. The processes and technology controls for these cases are described in the following sections.

Customer Can Access the Customer VM or VM Configured with Delegate Access Control

If the customer VM is accessible by the customer or configured with Delegate Access Control, then Oracle staff are not permitted to access to the customer VM from the Oracle managed infrastructure components. Instead, customer staff are required to access the customer VM using customer credentials, and then customer staff can share access to the customer VM using shared-screen technology (e.g., zoom, webex, skype, etc.). This access is controlled by the SR process as follows when a customer is not using Delegate Access Control:

- Customer opens a Service Request (SR) indicating the failure
- Customer or Oracle opens a shared session and indicates session information in the SR
- Oracle and customer staff access shared session information from the SR
- Customer accesses the customer VM using customer credentials
- Customer either enters commands to resolve the issue as instructed by Oracle staff, or customer permits the Oracle staff to control the keyboard entry for the VM session
- Customer updates the SR with diagnostics information
- Oracle staff update the SR with resolution information

The process when a customer uses Delegate Access Control is as follows:

- Customer opens a Service Request (SR) indicating the failure
- Oracle Support staff open a Delegate Access Control Access Request indicating the SR information
- Customer reviews and approves Delegate Access Control Access Request
- Oracle support staff assigned to the Access Request log into customer VM via Delegate Access Control credentials
- Customer monitors work via Delegate Access Control audit logs
- Customer terminates access if customer has cause to terminate access
- Oracle closes Delegate Access Control access request when work is complete, or software automatically closes Delegate Access Control access request when the approved work time duration expires

VM is not Accessible via Remote Login

If the customer cannot access the customer 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 the customer VM from the infrastructure. This access is controlled jointly by the customer and Oracle through the Oracle Service Request (SR) process and the Operator Access Control Technology (if implemented) as follows:

- If a customer is willing to permit Oracle Cloud Ops to access the customer VM without direct customer supervision, then the customer opens 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

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

        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 a customer requires Oracle to offer a shared screen to permit direct customer supervision of the Oracle cloud ops access, the customer opens 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 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 the has implemented Operator Access Control, Oracle will open an Operator Access Control Access Request to resolve the issue; the customer 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 a customer-specified syslog server in the customer's data center and/or the OCI Logging service in the customer's tenancy
- With Oracle and customer 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

DATA PROCESSING AGREEMENT AUDIT

As part of the ExaDB-C@C service, customers may audit Oracle's compliance with its obligations under this Data Processing Agreement (DPA) up to once per year. In addition, to the extent required by Applicable Data Protection Law, the customer or the customer's Regulator may perform more frequent audits. The Data Processing Agreement for Oracle Services[157] provides detail about how customers may request an audit and how the audit will be processed.

DEVICE AND DATA RETENTION

Oracle Customer Data and Device Retention for (DDR) Oracle Cloud at Customer[158] is an optional add-on service for ExaDB-C@C. Oracle DDR permits the customer 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 hardware system placed onsite in the customer's data center for the customer's ExaDB-C@C subscription.

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

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 customer retains control to manage another part of

[157] https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf

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

the system, such as virtual machines, applications, and databases (customer tenancy). For mission critical and highly regulated workloads, the customer 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 in the cloud provider tenancy. To meet these requirements, Oracle customers can use Oracle Operator Access Control[159] (OpCtl) with Exadata Database Service on Cloud@Customer (ExaDB-C@C) and Autonomous Database Dedicated (ADB-D) on ExaDB-C@C.

OpCtl is an Oracle Cloud Infrastructure (OCI) Privileged Access Management (PAM) service for ExaDB-C@C. OpCtl provides the customer 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 to Oracle customers.

OpCtl is the right feature for use cases where customers need to control Oracle Cloud Ops staff login to infrastructure to meet the same standards applied to customer staff accessing customer managed systems. For example, OpCtl 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.

OpCtl preventive security control features include the following:

- Oracle staff access only when authorized by the customer 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
- Customer control over when Oracle staff can access infrastructure
- Software enforcement of privilege escalation by Oracle staff

OpCtl detective security control features include the following:

- Customer notification 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
- Customer security monitoring of all commands and keystrokes entered by Oracle staff
- Oracle-supplied record of the Oracle staff identity to the customer when required for any command executed

OpCtl responsive security control features include the following:

- Customer control to terminate Oracle staff access
- Customer control to terminate processes started by Oracle staff
- Customer control to remove remotely accessible accounts from ExaDB-C@C infrastructure and ADB-D VM

Customers must plan to ensure continuous monitoring (24x7x365) and response to Operator Access Control Access request events[160] for Oracle to support the ExaDB-C@C service. Customers should consider using the OCI Events[161] and Notifications[162] services to automate the process of notifying customer staff for the purposes of processing OpCtl Access Requests. See a Simple Guide to Managing OCI Alarms in ServiceNow[163] for an example of how to do this with ServiceNow.

Customers may integrate OpCtl audit logs into 3rd party software products that are compatible with the OpCtl service. This includes sending OpCtl audit logs to a customer-specified syslog server[164] and integrating the OCI Logging service with Splunk.[165]

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

[160] https://docs.oracle.com/en-us/iaas/operator-access-control/doc/auditing-operator-access-control-lifecycle-events.html#GUID-1C819283-0660-4828-8E11-09D897211436

[161] https://docs.oracle.com/en-us/iaas/Content/Events/Concepts/eventsoverview.htm

[162] https://docs.oracle.com/en-us/iaas/Content/Events/Concepts/eventsoverview.htm

[163] https://www.ateam-oracle.com/post/a-simple-guide-to-managing-oci-alarms-in-servicenow

[164] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-6526ADE1-C664-4600-A62B-5993EA25134E

[165] https://docs.oracle.com/en/solutions/logs-stream-splunk/index.html

A complete description of the OpCtl service for ExaDB-C@C Infrastructure is available from the Operator Access Control[166] product documentation. An overview of the OpCtl service is available in the Operator Access Control Tech Brief.[167]

ORACLE DELEGATE ACCESS CONTROL

The Oracle Delegate Access Control[168] service is a privileged access management (PAM) service that enables Oracle Exadata Database Service on Cloud@Customer customers to subscribe their VM to database maintenance and support services, delegate access to service providers, and control when those service providers can access VM and database resources. Delegate Access Control uses the same delivery mechanics as Operator Access Control, is included in the scope of the Operator Access Control PCI-DSS attestation of compliance (AoC).

Customers 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 customer 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 ExaDB-C@C subscription
- Strategic Customers Program for DB Cloud Platforms – custom support services that are negotiated separately from the ExaDB-C@C subscription

Delegate Access Control allows customers to

- Control when and how much access Oracle support staff have to the customer VM
- Observe and record Oracle support staff commands and keystrokes that are invoked during shell access
- Terminate Oracle support staff connections at the customer's discretion

Delegate Access Control is the right feature for use cases where customers need to control Oracle support staff staff login to the customer VM to meet the same standards applied to customer staff accessing customer managed systems. For example, Delegate Access Cotrol 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.

Delegate Access Control preventive security control features include the following:

- Oracle staff access only when authorized by the customer and only for a specific customer 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
- Customer control over when Oracle staff can access the customer VM
- Software enforcement of privilege escalation by Oracle staff

Delegate Access Control detective security control features include the following:

- Customer notification when Oracle staff need to access the customer VM
- Command and keystroke logging for actions taken by Oracle staff
- Commands and keystrokes are traceable to an individual person
- Customer security monitoring of all commands and keystrokes entered by Oracle staff
- Oracle-supplied record of the Oracle staff identity to the customer when required for any command executed

Delegate Access Control responsive security control features include the following:

- Customer control to terminate Oracle staff access
- Customer control to terminate processes started by Oracle staff
- Customer control to remove remotely accessible accounts from the customer VM

[166] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-7CF13993-DB16-485A-A9FA-399E0049740B

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

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

SUMMARY

Security features throughout the customer VM and customer database are controlled by the customer. Oracle database encryption features encrypt data, and the customer retains control of the encryption keys. Oracle database security features control authentication and access to data in the database, and the customer retains control of this authentication and access. Oracle Linux authentication features control access to the customer's VM, and the customer retains control of this authentication and access.

Security and auditing features throughput the Oracle-managed components of the ExaDB-C@C service ensure that Oracle Cloud Operations staff only perform authorized actions on the infrastructure components of ExaDB-C@C. Security measures include multi-factor named user authentication, strong passwords with rotation schedules, and token-based SSH access to Oracle-managed infrastructure components. Auditing and logging are implemented throughout the stack, and audit logs are available to customers at their request via 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. Customers and Oracle Cloud Operations work together to ensure system security and prevent unauthorized access to and theft of customer data. Oracle Cloud Operations staff does not access customer networks, services, or data to deliver the ExaDB-C@C service, and customers do not access Oracle managed infrastructure to consume ExaDB-C@C Service. In the ExaDB-C@C deployment model, customers 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
November 2424