Oracle OCI Exadata Database Service on Dedicated Infrastructure Security Controls

ORACLE

Exadata Database Service on Dedicated Infrastructure Security Controls

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

May 14, 2025 | Version 2.32

PURPOSE STATEMENT

This document provides an overview of features and enhancements included in Exadata release 25.1.2.0.0.250213.1.[1] It is intended solely to help you assess the business benefits of upgrading to Exadata release 25.1.2.0.0.250213.1 and to plan your I.T. projects.

This document summarizes the security and control features of Oracle's Oracle Cloud Infrastructure (OCI) Exadata Database Service on Dedicated Infrastructure (ExaDB-D) in OCI regions and Oracle Database services in multicloud.[2,] It is intended for customer security staff chartered at evaluating adoption of ExaDB-D. Security staff chartered with evaluating ExaDB-D should also review the following documentation:

- Oracle Cloud Infrastructure Security Architecture[3]
- Oracle Cloud Infrastructure Security Guide[4]
- Oracle Corporate Security Practices[5]
- Exadata Database Service on Dedicated Infrastructure Security Guide[6]
- Security Features in Autonomous Database[7]
- Security and Authentication in Oracle Autonomous Database[8]
- Oracle Cloud Infrastructure Security Testing Policies[9]
- Oracle Cloud Services Contracts[10]
- Oracle Data Processing Agreement[11]
- Oracle Cloud Services Agreement[12]

The ExaDB-D service is delivered the same by Oracle in OCI data centers and partner cloud service provider (CSP) data centers (e.g., OD@Azure, OD@Google, and OD@AWS) save the exceptions called out in Oracle Multicloud. These exceptions include physical control of the ExaDB-D infrastructure, control plane and remote management connectivity, and the networking implementation that connects the ExaDB-D client virtual cloud network (VCN) to the partner cloud service provider network (e.g., Azure Virtual Network).

---

[1] https://support.oracle.com/knowledge/Oracle%20Database%20Products/2333222_1.html
[2] https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/Content/multicloud/Oraclemulticloud.htm
[3] https://www.oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf
[4] https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_guide.htm
[5] https://www.oracle.com/corporate/security-practices/
[6] https://docs.oracle.com/en-us/iaas/exadatacloud/exacs/ecs-security-guide.html
[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-authentation-autonomous-database.html
[9] https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm
[10] https://www.oracle.com/corporate/contracts/cloud-services/
[11] https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf
[12] https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#online

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.

TABLE OF CONTENTS

LIST OF IMAGES

LIST OF TABLES

INTRODUCTION

Exadata Database Service on Dedicated Infrastructure (ExaDB-D) provides Oracle's Exadata Database Machine as a service in an Oracle Cloud Infrastructure (OCI) data center. The advantage of ExaDB-D is that the customer gains the features and functionality the Exadata Database Machine plus the orchestration and management tools of OCI and Oracle Cloud Ops support for infrastructure maintenance.

ExaDB-D is the right database service for use cases where customers seek to gain the operational and financial value of a cloud service with the availability, performance, and functionality, and security of the Exadata Database Machine.

The ExaDB-D 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-D service delivery model, this paper describes the security controls of ExaDB-D as compensating measures for edge cases where customer approved security standards may differ from the ExaDB-D model. The intent of this paper is to describe the controls such that they may be used by customer security teams to grant exceptions to historical standards and to create future standards based on these controls.

The ExaDB-D service is available in OCI,[13] Azure,[14,15] and Google Cloud Provider[16,17] data centers. The Oracle Database@Azure FAQ[18] and Oracle Database@Google FAQ[19] provide commonly requested information about the services

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 Oracle Cloud Compliance Documentation[20] for relevant detail about a specific standard for ExaDB-D. 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.

You may request compliance documents from an Oracle sales representative, and you may access them directly from their OCI Cloud Console.[21]

The frameworks and standards that the ExaDB-D service in OCI is delivered to includes the following:

- C5
- CSA STAR Level 2
- Canada Protected B
- DESC (UAE)
- DoD IL5
- ENS High
- FSI (Korea)
- FedRAMP High – JAB ATO
- G-Cloud Marketplace
- GxP
- HIPAA
- HITRUST CSF
- Héberge des Données de Santé (HDS)
- IRAP
- ISMAP
- ISMS
- ISO/ EC 20000-1
- ISO/IEC 27001
- ISO/IEC 27017
- ISO/IEC 27018
- ISO/IEC 27701
- ISO/IEC 9001
- MeitY
- NCSC
- NISC
- PCI DSS
- SAMA
- SOC 1
- SOC 2
- SOC 3
- Saudi Arabian National Cybersecurity Authority
- Three Ministries
- UK Cyber Essentials
- UK Security and Data Protection Toolkit

ORACLE CONTRACTS

The Oracle Data Processing Agreement[22] describes how Oracle controls, protects, and processes data related to Oracle services, including ExaDB-D, such as

- Cross Border Data Transfers

---

[13] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecscm/exa-service-desc.html#GUID-D35869C4-7F3F-423A-A498-1E74A4BD5F0C
[14] https://learn.microsoft.com/en-us/azure/oracle/oracle-db/provision-oracle-database
[15] https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/Content/database-for-azure/intro.htm
[16] https://cloud.google.com/oracle/database/docs/create-instances
[17] https://docs.oracle.com/en/solutions/deploy-oracle-database-at-google-cloud/index.html#GUID-DF76B414-E4A9-47E6-AF55-248F89D77A22
[18] https://www.oracle.com/cloud/azure/oracle-database-at-azure/faq/
[19] https://www.oracle.com/cloud/google/oracle-database-at-google-cloud/faq/
[20] https://www.oracle.com/cloud/compliance/#attestations
[21] https://docs.oracle.com/en-us/iaas/Content/ComplianceDocuments/Concepts/compliancedocsoverview.htm
[22] https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf

- Security and Confidentiality
- Audit Rights
- Incident Management and Breach Notification

The Oracle Cloud Services Agreement[23] 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[24] provides an index to Oracle's security, compliance, privacy, and commercial contracts.

ORACLE CORPORATE SECURITY POLICIES

Oracle's security policies cover the management of security for both Oracle's internal operations and the services, including the ExaDB-D 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. Oracle's published Corporate Security Practices[25] including the following information:

- Objectives[26] – help protect the confidentiality, integrity, and availability of both Oracle and customer data
- Human resources security[27]
- Access control[28]
- Network communications security[29]
- Data security[30]
- Laptop and mobile device security[31]
- Physical and environmental security[32]
- Supply Chain Security and Assurance[33]

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[34] 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[35] 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

---

[23] https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#online
[24] https://www.oracle.com/trust/
[25] https://www.oracle.com/corporate/security-practices/corporate/
[26] https://www.oracle.com/corporate/security-practices/corporate/objectives.html
[27] https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
[28] https://www.oracle.com/corporate/security-practices/corporate/access-control.html
[29] https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html
[30] https://www.oracle.com/corporate/security-practices/corporate/data-protection/
[31] https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html
[32] https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
[33] https://www.oracle.com/corporate/security-practices/corporate/supply-chain/
[34] https://www.oracle.com/corporate/security-practices/assurance/vulnerability/disclosure.html
[35] https://www.oracle.com/security-alerts/#CVEOtherDocs

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-D, 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 FOR EXADB-D IN OCI

ExaDB-D is jointly managed by the customer and Oracle. The ExaDB-D deployment is divided into 2 areas of responsibility:

- Customer managed services: components that the customer can control as part of their subscription to ExaDB-D
  - 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
- Oracle managed cloud control plane services
  - Customer web UI and API interfaces
  - Publicly accessible services and endpoints, such as OCI cloud services
  - Privately accessible endpoints, such as OCI Fast Connect
  - OCI cloud automation for the purposes of orchestrating OCI cloud services

Customers control and monitor access to customer services, including network access to their VMs via OCI Virtual Cloud Networks (VCN),[36] OCI Network Security Lists,[37] OCI VCN Flow Logs,[38] authentication to access the VM via token-based `ssh`,[39] and authentication to access databases running in the VMs via Oracle database authentication methods[40]. 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. The Exadata Database on Dedicated Infrastructure Service Description[41] and Exadata Database Service on Dedicated Infrastructure - Explanation of Cloud Operations Service (Doc ID 2875973.1)[42] provides further detail.

Table 1: Roles and Responsibilities for ExaDB-D in OCI

WORK FUNCTION	ORACLE MANAGED INFRASTRUCTURE		CUSTOMER MANAGED SERVICES	
	Oracle Cloud Ops	Customer	Oracle Cloud Ops	Customer
Monitoring	Infrastructure, Control Plane, Hardware Faults, Availability, Capacity	Not Appliable	Infrastructure availability to support customer monitoring of customer services	Monitoring of Customer OS, Databases, VMs, and Apps
Incident Management & Resolution	Incident Management and Remediation Spare Parts and Field Dispatch	Not Appliable	Support for any incidents related to the underlying platform	Incident Management and resolution for Customer's Apps

[36] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/overview.htm
[37] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/securitylists.htm#Security_Lists
[38] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/vcn_flow_logs.htm
[39] https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/exaconnectingDB.htm
[40] https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/exaconnectingDB.htm
[41] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecscm/exa-service-desc.html
[42] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2875973.1

Patch Management	Proactive patching of Hardware, IaaS control software, hypervisor, and any applicable Oracle-managed infrastructure components	Not Appliable	Staging of available patches (e.g., Oracle DB patch set) per Maintaining an Exadata Database Service on Dedicated Infrastructure[43] documentation	Patching of tenant instances Testing
Backup & Restoration	Infrastructure and Control Plane backup and recovery, recreate customer VMs	Not Appliable	Provide running and customer accessible VM	Snapshots / Backup & Recovery of customer's IaaS data using Oracle native or 3rd party capability
Cloud Support	Response & Resolution of SR related to infrastructure or subscription issues	Submit SRs via My Oracle Support (MOS)	Response & Resolution of SR	Submit SRs via My Oracle Support (MOS)

CONSIDERATIONS WHEN MAKING CHANGES TO THE SERVICE SOFTWARE

ExaDB-D 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.[44] 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,[45] Oracle Software Security Assurance,[46] and the Exadata Cloud@Customer Security Features.[47] 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-D SERVICE ARCHITECTURE

The ExaDB-D service is deployed across Exadata Database Server and Storage Server racks in an OCI data center of the customer's choice. The ExaDB-D racks contain all the components of a standard Exadata Database Machine, plus networking hardware to support OCI VCNs. The physical Exadata rack and networking infrastructure may be shared among multiple tenants (customers). The Exadata Database Servers and Exadata Storage Servers are dedicated to a single tenant (customer).

The customer's database data is secured in the ExaDB-D Database Servers and Storage Servers in the OCI data center, and all customer access to customer databases is made via network connections (VCNs) the customer permits to access the VMs and databases in the ExaDB-D 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` in the customer VM operating system, `SYS` in the Oracle database) to customer VMs and databases, and the customer can act with those credentials to secure the VM and database to help address policy and regulatory requirements. This includes, and is not limited to, installing agents,

[43] https://docs.oracle.com/en-us/iaas/Content/Database/Concepts/examaintenance.htm
[44] https://support.oracle.com/knowledge/Oracle%20Cloud/1593827_1.html
[45] https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html
[46] https://www.oracle.com/corporate/security-practices/assurance/
[47] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html

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-D Compute VM operating system and Oracle database.

Customers deploy and manage ExaDB-D and database services using the Oracle Cloud Infrastructure Console and REST APIs. The customer controls access to the cloud automation's management functionality via the OCI Identity and Access Management (IAM)[48] service, and the OCI Audit[49] 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. The customer controls network access to the ExaDB-D customer VM and database services running on the ExaDB-D service via OCI Virtual Cloud Networks.[50] Oracle controls network access the ExaDB-D infrastructure for cloud automation and for Oracle staff with a need to maintain the service.

Network Block Diagram for ExaDB-D in OCI

Figure 1 summarizes the network architecture block diagram for ExaDB-D, and the Oracle Exadata Database Service on Dedicated Infrastructure Technical Architecture[51] product documentation provides further detail. Customer accessible and controlled components are shown in blue. Oracle managed components dedicated to the specific customer (single tenant) are shown in red. Oracle managed infrastructure that is shared among OCI tenants is shown in green. The ExaDB-D Database (DB) Servers and Storage Servers shown in red, are interconnected via an isolated layer 2 management network, also shown in red. There is no direct network access from the management network to the customer client and backup networks.

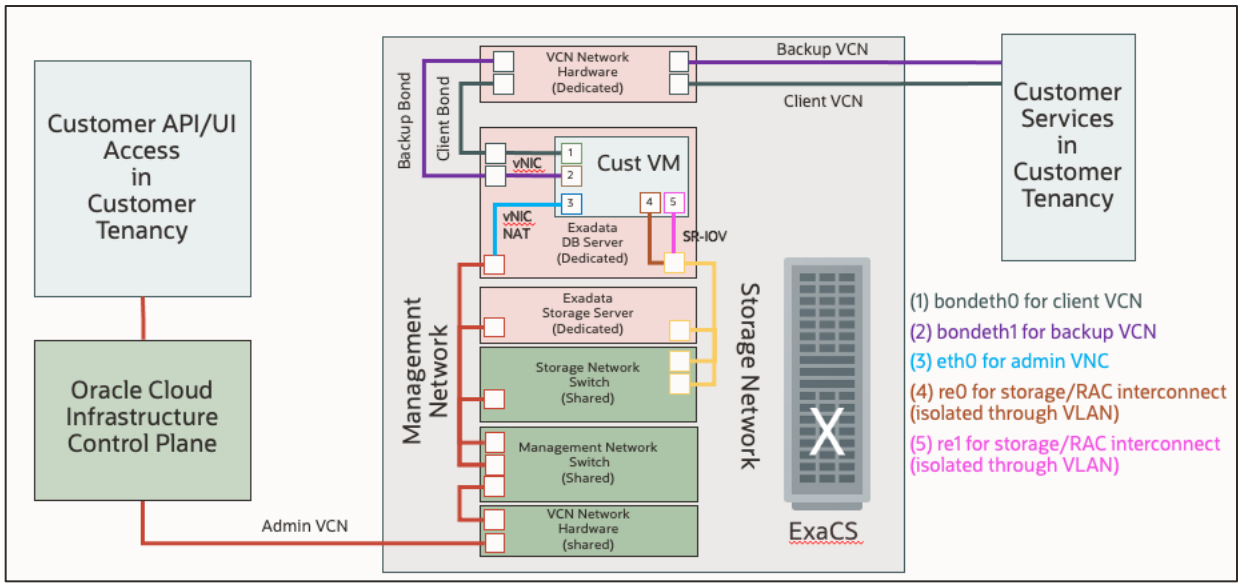

Figure 1: Network Architecture block diagram for Oracle Exadata Database Service on Dedicated Infrastructure

The Exadata Database Server is connected to the OCI networking infrastructure via specialized VCN networking hardware, shown in green for the Oracle-managed infrastructure (shared among customers/tenants), and red for customer services (dedicated to a customer/tenant). The customer has access to customer virtual machines (customer VM) via the client and backup networks implemented as OCI VCNs and mapped to the customer VM as vNIC interfaces. The physical network connections are implemented for high availability in an active/standby configuration that is managed by Oracle Cloud Operations. In the event of a physical network link failure, Oracle Cloud Operations will perform the necessary recovery steps to reinstate the network connection. This can lead to short network outages in some cases.

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 a Highly Available (HA) (active/standby) connection to a pair of redundant storage networking switches.

---

[48] https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm
[49] https://docs.oracle.com/en-us/iaas/Content/Audit/Concepts/auditoverview.htm
[50] https://www.oracle.com/cloud/networking/virtual-cloud-network/
[51] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecsid/

A subset of Oracle cloud automation functionality accesses the customer VM via a NAT address on the management VCN implemented on a vNIC in the Exadata Database Server, shown in blue. 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 is stored in memory Oracle cloud automation software running in the ExaDB-D hardware in the customer's data center and discarded after the action is completed. Likewise, the cloud automation software removes the temporary public key from the service account when the action is completed.

The port matrix describing running processes, TCP port numbers, and userids for running processes deployed in the customer VM is published in the Security Guide for Oracle Exadata Database Service on Dedicated Infrastructure Security Guide.[52] This guide describes security for an Exadata Cloud Infrastructure and includes information about the best practices for securing the Exadata Cloud Infrastructure.

Customer Access to ExaDB-D Services

Customers access Oracle databases (DB) running on ExaDB-D via an OCI VCN connection from customer endpoints to the databases running in the customer VM using standard Oracle database connection methods, such as Oracle Net on TCP port 1521. Customer's access the VM running the Oracle databases via standard Oracle Linux methods, such as token based `ssh` on TCP port 22.[53]

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 hosted in the OCI control plane. Customers do not have to manage the infrastructure layer as Oracle performs infrastructure management to support the 99.95% service uptime published in the Oracle PaaS and IaaS Public Cloud Pillar Documentation.[54] Customers are not authorized to directly access ExaDB-D infrastructure, load monitoring agents, or directly pull or push files to the Oracle managed infrastructure in the ExaDB-D service.

The customer's OCI Identity and Access Management (IAM) controls govern if and how a customer 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:

- Database patching
- Grid Infrastructure patching
- Customer VM OS patching
- Oracle managed infrastructure quarterly patching (used to validate CRS restarts in the customer VM)
- Add Database Server Infrastructure
- Add VM Cluster Node
- Delete VM Cluster Node
- Add Storage Server

Oracle cloud automation access may be temporarily restored by the customer to permit the subset of functionality required to access the customer VM and customer databases. 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.

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

Customer VM Default Users

The ExaDB-D service includes several user accounts regularly manage the components deployed in the ExaDB-D service customer VM. In all ExaDB-D service machines, Oracle uses and recommends SSH based login only. No Oracle user or

[52] https://docs.oracle.com/en-us/iaas/exadatacloud/exacs/ecs-security-guide.html
[53] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecscm/ecs-connect-to-service-instance.html#GUID-53DE1ED5-96D9-4F7F-B57F-4EF8D01FCDCB
[54] https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf

processes use password-based authentication system. The Guest VM Default Users[55] 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 Infrastructure 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 Infrastructure 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-D 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.[56]

Customer VM Default Security Settings

In addition to all the Exadata features explained in Security Features of Oracle Exadata Database Machine,[57] the ExaDB-D customer VM includes the following security configuration settings that can be referenced from the ExaDB-D Security Guide Guest VM Default Security Settings[58] 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:

- `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.

---

[55] https://docs.oracle.com/en-us/iaas/exadatacloud/doc/ecs-security-guide.html#GUID-84E782CD-10B8-47A1-A3AF-1DDEE82A6C06

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

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

[58] https://docs.oracle.com/en-us/iaas/exadatacloud/doc/ecs-security-guide.html#GUID-3A150605-1DC9-401F-9201-C0E73ABE817E

- 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-D 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[59] documentation. The Guest VM Default Port Matrix Table[60], reproduced as Table 2 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 2: 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[61]	N/A
		1521 Optionally, customers can assign a SCAN listener port (TCP/IP) in the range between 1024 and 8999. Default is 1521. Note: TNS listener opens dynamic ports after initial contact to	Oracle TNS listener[62] Receives incoming client connection requests and manages the traffic of these requests to the database server. Supports Oracle Native Network Encryption (NNE)	Oracle self-signed; customers may add customer-controlled certificates

[59] https://docs.oracle.com/en-us/iaas/exadatacloud/doc/ecs-security-guide.html#GUID-3A150605-1DC9-401F-9201-C0E73ABE817E

[60] https://docs.oracle.com/en-us/iaas/exadatacloud/doc/ecs-security-guide.html#GUID-3A150605-1DC9-401F-9201-C0E73ABE817E

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

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

		well known ports (1521, 1525).	and TLS/SSL as transport layer security authentication[63]	
		5000	Oracle Trace File Analyzer[64] Collector	Oracle self-signed
		7879	Jetty Management Server.[65] Application server engine that is used internally by Oracle Exadata System Software, in particular Management Server (MS).[66]	Oracle self-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 self-signed; customers may add customer-controlled certificates
	bondeth0:2	1521 Optionally, customers can assign a SCAN listener port (TCP/IP) in the range between 1024 and 8999. Default is 1521.	Oracle TNS Listener	Oracle self-signed; customers may add customer-controlled certificates
Bridge on backup VLAN	bondeth1	7879	Jetty Management Server	Oracle self-signed
	clib0/clre0	1525	Oracle TNS listener Oracle Clusterware running on each cluster node communicates	N/A

[63] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-secure-sockets-layer-authentication.html#GUID-6AD89576-526F-4D6B-A539-ADF4B840819F
[64] https://docs.oracle.com/en/database/oracle/oracle-database/19/atnms/managing-and-configuring-tfa.html
[65] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmso/application-server-update-management-server.html
[66] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmso/management-server-database-servers.html

Oracle Clusterware[67,68] running on each cluster node communicates through these interfaces.			through these interfaces.	
		3260	Synology DSM iSCSI	N/A
		5054	Oracle Grid Interprocess Communication	N/A
		7879	Jetty Management Server	Oracle self-signed
		Dynamic Port: 9000-65500 Ports are controlled by the configured ephemeral range in the operating system and are dynamic.	System Monitor service (osysmond) Cluster Logger service (ologgerd) Cluster Health Monitor[69] uses system monitor (osysmond) and cluster logger (ologgerd) services to collect diagnostic data.	Oracle self-signed
	clib1/clre1	5054	Oracle Grid Interprocess communication	N/A
		7879	Jetty Management Server	Oracle self-signed
Cluster nodes use these interfaces to access storage cells (ASM disks).	stib0/stre0	7060	dbcs-admin Cloud agent for handling database lifecycle operations[70]	Oracle self-signed
		7070	dbcs-agent	Oracle self-signed

[67] https://docs.oracle.com/en/database/oracle/oracle-database/19/cwadd/introduction-to-oracle-clusterware.html#GUID-7612C5C2-AC7C-4311-97B2-CF189268969A
[68] https://docs.oracle.com/en/database/oracle/oracle-database/19/rilin/port-numbers-and-protocols-of-oracle-components.html
[69] https://docs.oracle.com/en/database/oracle/oracle-database/19/atnms/understanding-cluster-health-monitor-services.html
[70] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html#GUID-519A41E4-A97D-476E-B4BA-745C3486C779

However, the IP/ports 7060/7070 attached to the storage interfaces are used to access DBCS agent from the Control Plane server.			Cloud agent for handling database lifecycle operations[71]	
	stib1/stre1	7060	dbcs-admin	Oracle self-signed
		7070	dbcs-agent	Oracle self-signed
Control Plane server to domU	eth0	22	sshd	N/A
Loopback	lo	22	sshd	N/A
		2016	Oracle Grid Infrastructure	N/A
		6100	Oracle Notification Service (ONS),[72] 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[73]	Customer-controlled or Oracle signed

[71] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/ecccm/ecc-secguide.html#GUID-519A41E4-A97D-476E-B4BA-745C3486C779
[72] https://docs.oracle.com/en/database/oracle/oracle-database/19/cwadd/introduction-to-oracle-clusterware.html
[73] https://docs.oracle.com/en/cloud/paas/data-safe/admds/create-oracle-data-safe-onpremises-connector1.html

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:

- 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

The OCI Terraform Provider[74] may be used to deploy and manage ExaDB-D. Documentation for the Hashicorp Terraform software is available from Hashicorp.[75]

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

- DBaaS UI/API sends request to DB Control Plane via https
- DB Control Plane sends the request via REST API to the ExaDB-D Admin VCN
  - 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 a secure connection (mTLS) between the OCI control plane and each DB Agent; this mTLS connection is implemented through the private interconnect network in the ExaDB-D rack; the port matrix for software processes running in the customer VM is published in the Exadata Database Service on Dedicated Infrastructure 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 `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-memory 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 to the required endpoint (e.g., Exadata Storage Server, Exadata Database Server)

Oracle manages and controls the private `ssh` tokens used to manage infrastructure and customer VM components. These tokens are stored and protected in the OCI control plane. The infrastructure tokens are unique and only provide access to infrastructure components (e.g., Exadata Storage Servers, physical Exadata Database Server, Storage Network switch), and do not provide access to customer VMs or databases. The customer VM tokens are unique to the specific management action and only provide access to the customer VM.

Customers may use OCI Network Sources[77] to control authentication to their tenancy to be allowed from IP addresses they control.

Oracle Infrastructure Monitoring

Oracle monitors and generates alerts if it is actionable by Oracle as indicated in "Oracle Support Document 2875973.1 (Exadata Database Service on Dedicated Infrastructure - Explanation Of Cloud Operations Service)."[78] Oracle monitors the infrastructure layer, which includes Exadata Compute (Dom0), Exadata Storage Servers, and Network Switches 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 or any additional software running on the Guest OS. It is customers responsibility to monitor Guest VM, CRS/ DB, etc..

---

[74] https://docs.oracle.com/en-us/iaas/Content/API/SDKDocs/terraform.htm
[75] https://registry.terraform.io/providers/hashicorp/oci/latest/docs
[76] https://docs.oracle.com/en-us/iaas/exadatacloud/exacs/ecs-security-guide.html
[77] https://docs.oracle.com/en-us/iaas/Content/Identity/Tasks/managingnetworksources.htm
[78] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2875973.1

The ExaDB-D infrastructure components report their Infrastructure Management Metrics (IMM) to monitoring servers in the OCI control plane. Oracle Support performs monitoring and maintenance of the ExaDB-D implementation as follows:

- Automated monitoring on Oracle Cloud Service infrastructure components sends Infrastructure Monitoring Metrics (IMM) to monitoring servers in the OCI control plane
  - Chassis temperature, drive status, etc.
  - Details for all monitoring data are published at Auto Service Request Qualified Engineered Systems Products[79]
- 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 authorized and dispatched to perform required support actions

Quarterly Software Updates

Standard quarterly bundle patches for the Oracle database, Grid Infrastructure, and customer VM operating system are staged to 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 directly from OCI Object Storage managed by Oracle. Quarterly patch information is available from Oracle Critical Patch Updates, Security Alerts and Bulletins.[80] My Oracle Support Document 2333222.1, Exadata Cloud Software Versions[81] provides information about current and historical software versions available for ExaDB-D. Oracle Cloud Infrastructure Maintenance documentation[82] describes the infrastructure update process, and the Patch and Update Exadata Cloud Infrastructure System documentation[83] describes the customer-managed update process for the customer VM, Grid Infrastructure, and Oracle database software.

Software updates for infrastructure components are deployed by Oracle cloud automation and Oracle staff, as required by the specific software updates. When possible, updates are applied to the running system, and without downtime, using tools like Linux ksplice. If an update requires a component restart, which is typical in a quarterly patch event, Oracle performs the component restart in a Real Application Cluster (RAC) rolling fashion to ensure service availability during the update 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. The Configuring Oracle-Managed Infrastructure Maintenance product documentation[85] details how maintenance is scheduled and performed for ExaDB-D.

---

[79] https://docs.oracle.com/cd/E37710_01/doc.41/e37287/toc.htm
[80] https://www.oracle.com/security-alerts/
[81] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2333222.1
[82] https://docs.oracle.com/en-us/iaas/exadatacloud/exacs/exa-conf-oracle-man-infra.html#GUID-C4301E26-E809-438F-96D7-9C6BB02FEA7F
[83] https://docs.oracle.com/en-us/iaas/exadatacloud/exacs/ecs-patch-update.html
[84] https://docs.oracle.com/en-us/iaas/exadatacloud/exacs/exa-conf-oracle-man-infra.html#GUID-A2008207-3683-424F-9279-F632BF4C9076
[85] https://docs.oracle.com/en-us/iaas/Content/Database/Concepts/examaintenance.htm

Software Update Security Controls

All software updates are controlled by Oracle Software Security Assurance Practices.[86] Oracle Software Security Assurance[87] standards apply to ExaDB-D software. Oracle implements segregation of duties[88] for software development, software test and quality assurance, and deployment of software ExaDB-D components.

PREVENTIVE CONTROLS

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

Customer Access Controls

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

- User Authentication
  - Credentials to access OCI services
  - Credentials to customer VM operating systems and database administration accounts
  - Credentials for database users to access databases and database data
- Network Access
  - OCI VCNs and Security Lists to control layer 2 and 3 access to customer VMs[89]
  - Zero-trust Packet Routing to control layer 2 and 3 access to customer VMs[90]
  - Network access rules implemented in the customer VM operating system[91] and Oracle database[92]
  - Temporary Delegate Access Control networks and bastion servers to allow Delegate Access Control credentials to authenticate to the customer VM
- Database Encryption
  - Application to database encryption[93]
  - Transparent Database Encryption (TDE) for user tablespaces[94]

The ExaDB-D 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, customers should take care to allow cloud automation functionality that accesses the customer VM.

Customer Access Control for ExaDB-D Services

Customers perform management actions via OCI automation by making an https connection to the Oracle Cloud Control Plane in the OCI region chosen by the customer. The customer is authenticated using their OCI Identity and Access Management (IAM)[95] credentials, and customer actions are controlled via OCI IAM permissions configured by the customer

---

[86] https://www.oracle.com/corporate/security-practices/assurance/
[87] https://www.oracle.com/corporate/security-practices/assurance/
[88] https://www.oracle.com/corporate/security-practices/corporate/access-control.html
[89] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecscm/ecs-network-setup.html#GUID-40900E3C-8730-46E7-8F4C-9301ED0CEFF6
[90] https://docs.oracle.com/en/cloud/paas/base-database/zpr/index.html#articletitle
[91] https://docs.oracle.com/en/operating-systems/oracle-linux/8/firewall/firewall-AboutPacketFilteringFirewalls.html
[92] https://docs.oracle.com/en/database/oracle/oracle-database/19/netag/configuring-oracle-connection-manager.html#GUID-AF8A511E-9AE6-4F4D-8E58-F28BC53F64E4
[93] ExaDB-D automation configures Oracle Native Network Encryption; Oracle strongly recommends that customers preserve this control
[94] ExaDB-D automation configured Oracle Transparent Data Encryption (TDE); Oracle strongly recommends that customers preserve this control
[95] https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm

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 appropriate ExaDB-D components by Oracle-controlled service VCNs.

Customers and database applications access databases running on the ExaDB-D via OCI VNICs attached to the customer VM. Access to databases and operating system is made via customer managed credentials.[96]

Customer Controls for Data Security

ExaDB-D is designed to help secure data for customer-authorized use, and to help protect data from unauthorized use, which includes preventing access to customer data by Oracle Cloud Ops staff members. Security measures designed to protect against unauthorized access to ExaDB-D 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
- 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
- Customer can control Oracle support and services staff access to customer VM via Delegate Access Control[97]
- Customer can install monitoring agents and security controls of their choice on the customer VM operating system if these agents don't modify the Linux kernel or interfere with Exadata operation[98]
- Network connections to the Oracle database are designed to be encrypted by Oracle Native Network Encryption, which is automatically configured to be requested by the database by cloud automation
- Oracle user tablespace database data is protected by Oracle Transparent Data Encryption (TDE) keys
  - Automatically configured by cloud automation and stored in password protected, PKCS12 wallet file stored in the file system of the customer VM
  - Customer controls access to TDE encryption keys via the wallet password
  - Customer can secure the TDE master key to the OCI Vault[99] service
  - Customer can move the TDE master key to an external key store, such as Oracle Key Vault
- Oracle Database Vault[100] may be configured by customers to revoke user data access privileges from database administrator accounts
- 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)[101] prior to scanning the customer VM; customer security scanning/testing must adhere to Oracle Cloud Testing Policy[102]
- 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

Figure 2 demonstrates Oracle network encryption, Oracle TDE, and Oracle Database Vault.

---

[96] https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/exaconnectingDB.htm
[97] https://docs.oracle.com/en-us/iaas/delegate-access-control/doc/overview-of-delac.html
[98] Oracle does not test or support 3rd party software with ExaDB-D; customers should check with 3rd party providers to ensure the 3rd party provider has tested and validated their software with ExaDB-D and that the 3rd party provider can support their software on ExaDB-D
[99] https://www.oracle.com/security/cloud-security/key-management/
[100] Oracle Database vault is included with Enterprise Edition Extreme Performance subscription, and is not included with a Bring Your Own License (BYOL) subscription
[101] https://support.oracle.com/rs?type=doc&id=1405320.1
[102] https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm

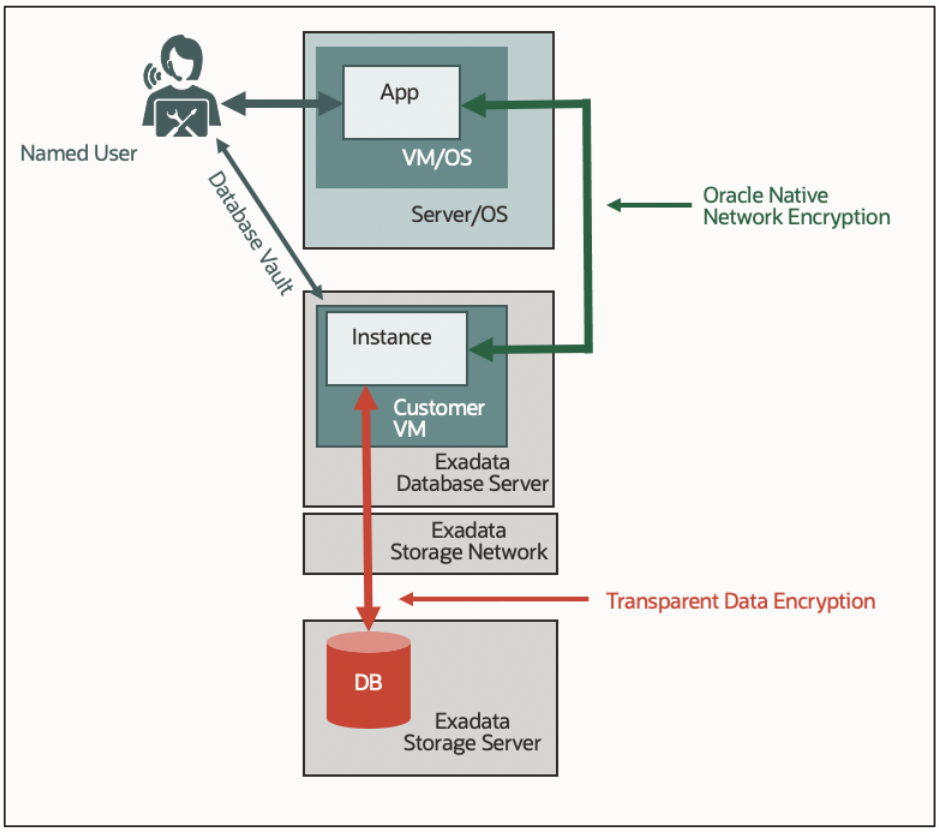

Figure 2: Controls to protect data in flight, from DBA accounts, and at rest

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-D 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. The cloud automation configured the Oracle database software to request an encrypted connection if the application is able to support an encrypted connection. If an application cannot support an encrypted connection, the software will permit the application to connect without encryption. Documentation for Oracle Native Network Encryption and TLS/SSL is published in the Security Guide for each Oracle Database version.[103] ExaDB-D 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.[104]

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[105] published for each database version.

---

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

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

[105] 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

Oracle Transparent Data Encryption

ExaDB-D service uses Oracle Transparent Data Encryption (TDE) to protect data at rest for its databases. TDE is a two-tier key architecture comprising of data encryption and master encryption keys. The data encryption keys protect table and tablespaces but are wrapped by a single database master encryption key. The master key is separated from encrypted data and are stored outside of the database. The TDE master key may be stored in an Oracle Wallet, a PKCS#12 standard-based key storage file.

For further information on Oracle TDE, consult the Advanced Security Guide for the Oracle database version you are running. The Oracle TDE FAQ[106] provides answers to common Oracle TDE architecture and implementation questions.

Details for the TDE implementation on ExaDB-D are shown in the Exadata Database Machine Cryptographic Services[107] documentation.

Oracle TDE for ExaDB-D with OCI Vault 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.

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.

ExaDB-D is integrated with Oracle Cloud Infrastructure (OCI) Vault service and Oracle Key Vault (OKV). Customers can create and manage TDE keys with OCI Vault or Oracle Key Vault instead of the Oracle Wallet stored in the customer VM as an added measure of separation for systems that require that enhanced security posture. OCI Vault has the following benefits:

- Control and manage TDE master keys in a separate hardware implementation from the database service
- TDE keys are stored in a highly available, durable, and managed service
- TDE keys are protected by hardware security modules (HSM) that meet Federal Information Processing Standards (FIPS) 140-2 Security Level 3 security certification
- Automation to rotate TDE keys and audit their cryptographic operations to meet compliance and regulatory needs

To manage ExaDB-D TDE keys, customers should first access the Vault service and create encryption keys. The encryption key algorithm you use must be AES-256. Next, customers should ensure the required IAM policy is set for you to manage keys in Vault. Once these prerequisite steps are complete, customers can create Exadata databases protected by customer managed keys. Only databases after Oracle Database 11g release 2 (11.2.0.4) are supported.

Customers may choose to migrate their ExaDB-D databases to Oracle Key Vault (OKV)[108], the only key management solution for their Oracle database estate that provides continuous key availability by adding up to 16 OKV nodes to a key

---

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

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

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

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).

Oracle supports customers using Oracle Key Vault (OKV) as an external key store for databases running on ExaDB-D. Instructions for using operating system methods to migrate TDE Master Keys to OKV are published at "Migration of File based TDE to OKV for ExaDB-D Using Automation via REST (Doc ID 2924192.1)."[109]

Customers have the option to use the OKV Persistent Master Encryption Key Cache[110] to enable databases to be operational if the OKV server is unavailable.

Details for the TDE implementation on ExaDB-D are shown in the Exadata Database Machine Cryptographic Services[111] documentation.

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

Oracle Database is compatible with PKCS#11 compatible key management devices.[112]

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)[113] for implementation and support details.

Integrating an external key manager requires the installation of PKCS#11 libraries on the ExaDB-D 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 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.[114]

Controls for Cloud Automation Access to Customer VM

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

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

The customer VM provides the Oracle Linux packet filtering software[115] as an additional data protection control to block network to the customer VM. The Oracle Linux firewall, `iptables` or `firewalld`, can be configured to block control plane access at layers 3 (IP) and 4 (TCP port). Customers may configure the operating system firewall to help address their specific security requirements.

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

---

[109] https://support.oracle.com/knowledge/Oracle%20Cloud/2924192_1.html
[110] https://docs.oracle.com/en/database/oracle/key-vault/21.7/okvag/security_objects.html#GUID-27DA6A5A-E405-4394-BD0D-C2B213391426
[111] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/exadata-security-features.html#GUID-FA8A2A69-AEFC-4FE3-959A-A6E584BD1F4F
[112] https://docs.oracle.com/en/database/oracle/oracle-database/19/asoag/introduction-to-transparent-data-encryption.html#GUID-2D6C5B27-8E6A-4EF7-AABF-B0FB031C8374
[113] https://support.oracle.com/knowledge/Oracle%20Database%20Products/2310066_1.html
[114] https://docs.oracle.com/en/database/oracle/key-vault/21.3/okvhm/index.html#Oracle%C2%AE-Key-Vault
[115] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-implement-sec.html#ol7-firewall-sec

Oracle cloud automation secure login via token-based `ssh` is not compatible with Kerberos authentication, and parts of the Oracle cloud automation functionality may cease to function if customers implement Kerberos authentication in the customer VM. Oracle does not support customers configuring Kerberos operating system authentication in the customer VM because this action breaks the cloud automation. Customers may configure Kerberos authentication for Oracle database user authentication. For details, please see Oracle Support Document 2621025.1 (Does ExaCC VM's Support Kerberos Authentication).[116]

Controls for Customer Staff Access to Customer VM

Access to the customer VM is implemented via token-based `ssh`.[117] 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. 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 integrate with customer key management systems, and customers can manage `ssh` keys using technology compatible with Oracle Linux.

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-D. ExaDB-D does not provide cloud automation support for this configuration. Customers can configure AD and LDAP by directly accessing the ExaDB-D customer VM to implement AD and LDAP. Customers should note that the ExaDB-D customer VM updates[118] are executed as image updates using the Exadata Database Machine image update process,[119] 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.

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.[120,121] Access is controlled in 3 steps:

1. Customer OCI IAM credentials create a console connection, which includes deploying temporary bastion servers, 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.

Controls for Protecting Against Theft of Data

User tablespace data in ExaDB-D databases is protected 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. Reference NSA guidelines[122] and NIST standards[123] for further detail.

---

[116] https://support.oracle.com/knowledge/Oracle%20Cloud/2621025_1.html
[117] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecscm/ecs-connecting-to-service-inst.html#GUID-53DE1ED5-96D9-4F7F-B57F-4EF8D01FCDCB
[118] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-update-exacc-system.html
[119] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmmn/updating-exadata-software.html#GUID-E6090FA9-13B4-4BEF-A28D-73BDC3729C58
[120] https://docs.oracle.com/en-us/iaas/releasenotes/changes/9cee8331-1a56-494c-9bcc-f0dab3eea1b4/
[121] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-manage-vm-clusters.html#GUID-34F8308B-480A-4DAE-A158-2B4856E41A90
[122] https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm
[123] https://www.nist.gov/publications/advanced-encryption-standard-aes

Oracle's Corporate Security Practices[124] cover the management of security for Oracle's internal operations and the cloud services, including ExaDB-D, 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 Delegate Access Control

Customers can use Oracle Delegate Access Control[125] 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[126] service, to control when Oracle professional services staff can access the customer VM, the privileges 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[127] 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[128] includes functionality that supports an on-premises connector deployed on customer-controlled servers to facilitate connecting databases running on ExaDB-D to connect to the OCI Data Safe service in an OCI region. The Data Safe FAQ[129] provides answers to commonly asked questions about Data Safe.

Oracle Database Security Assessment Tool (DBSAT)

The Oracle Database Security Assessment Tool 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 is designed to enable customers to quickly find:

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

---

[124] https://www.oracle.com/corporate/security-practices/corporate/
[125] https://docs.oracle.com/en-us/iaas/delegate-access-control/doc/overview-of-delac.html
[126] https://www.oracle.com/contracts/docs/oracle-engineered-systems-deployment-and-infrastructure-support.pdf
[127] https://docs.oracle.com/en-us/iaas/data-safe/index.html
[128] https://docs.oracle.com/en/solutions/oracle-data-safe-for-on-prem-database/index.html#GUID-07534FC6-3B10-48E5-BD49-C011D55D1070
[129] https://www.oracle.com/security/database-security/data-safe/faq/

DBSAT analyzes information in 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 DBSAT is available for download from Oracle.[130]

Oracle Controls for Cloud Operations Access to Infrastructure Components

Oracle Access Control Practices[131] restrict access to Oracle staff with a need to know and need to access ExaDB-D infrastructure, and include the following details:

- Authorization to access ExaDB-D 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-D infrastructure components, which include the following equipment:

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

Figure 3 shows how Oracle Cloud Operations (Cloud Ops) staff access infrastructure components to manage the ExaDB-D infrastructure.

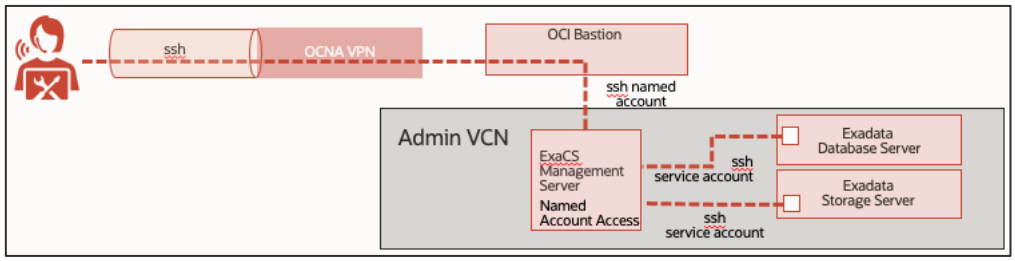

Figure 3: Cloud Operations Staff Access to ExaDB-D Infrastructure Components

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
- Access to Bastion and Management servers for the purposes of ssh access to ExaDB-D infrastructure
  - Access to ExaDB-D management servers is implemented as a tunnel through the Bastion server isolated to OCI privileged administrative VCN located in the OCI region hosting the service
  - Connections through Bastion servers are logged and monitored by Oracle
- Login to management servers dedicated to managing ExaDB-D infrastructure as a named user via ssh using MFA implemented with a FIPS 140-2 Level 3 hardware token (Yubikey)
  - Access to the management server is controlled based on Oracle's published least privileged access policies[132]
  - Connections to the ExaDB-D infrastructure are logged and monitored by Oracle
- Log into the ExaDB-D infrastructure using the required service account using token-based ssh
  - Command execution is traceable to a specific named user via audit logging implemented in the ExaDB-D infrastructure

[130] https://www.oracle.com/database/technologies/security/dbsat.html
[131] https://www.oracle.com/corporate/security-practices/corporate/access-control.html
[132] https://www.oracle.com/corporate/security-practices/corporate/access-control.html

- Connections to infrastructure components are logged and monitored by Oracle

Oracle Process Access Controls

Oracle's Access Control[133] security practice restricts access to Oracle staff with a need to know and need to access ExaDB-D infrastructure, and include the following policies:

- Authorization to access ExaDB-D infrastructure 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

Exadata Infrastructure Software Security and Controls

ExaDB-D is based on the Exadata Database Machine and delivers the enterprise-class security features of Exadata Database Machine[134] in an on-premises cloud model. Security features of ExaDB-D include the following:

- Software deployed on ExaDB-D 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-D infrastructure
- Non-essential operating system tools and packages are not installed on ExaDB-D infrastructure
- Software development performed under Oracle Software Security Assurance[135]
- Security architecture performed under Oracle Corporate Security Architecture[136]

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.

DETECTIVE CONTROLS (LOGGING AND AUDITING)

ExaDB-D 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).[137]

Customer Audit Logging

ExaDB-D provides three capabilities for auditing and logging of customer actions:

- OCI Audit Service:[138] 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:[139] audit logs for database actions initiated via a customer's Oracle database credential
- Customer VM operating system audit log:[140] audit logs for actions initiated on a customer VM via an operating system credential

The OCI 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

---

[133] https://www.oracle.com/corporate/security-practices/corporate/access-control.html
[134] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/toc.htm
[135] https://www.oracle.com/corporate/security-practices/assurance/
[136] https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html
[137] https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf
[138] https://docs.oracle.com/en-us/iaas/Content/Audit/Concepts/auditoverview.htm
[139] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/introduction-to-auditing.html#GUID-94381464-53A3-421B-8F13-BD171C867405
[140] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-implement-sec.html#ol7-audit-sec

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 OCI Audit[141] 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. Note, OCI Audit logs are stored in the compartment of the target resource where the API was invoked.

Oracle database auditing tracks changes made to the Oracle database by database users and non-database users. Customers can 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[142] for each database version.

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`, `opc`, and named users configured by the customer. Customers can 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.[143] Customers may integrate the Oracle Linux audit logs into the OCI Log Analytics service.[144]

Customer Security Scanning of Customer VM

Customers may use OpenSCAP[145] to scan the customer VM for compliance.

Customers may use the Oracle Linux Advanced Intrusion Detection Environment (AIDE)[146] 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-D software distribution and configuration. In some cases, arbitrary benchmarks can flag security issues on the ExaDB-D customer VM that may not be a material risk due to compensating controls on the ExaDB-D 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)”[147] at to learn more about how common benchmarks may be adjusted to work with Exadata. If the ExaDB-D 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-D 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 of the ExaDB-D customer VM must be done in accordance with Oracle Cloud Testing Policies.[148]

---

[141] https://docs.cloud.oracle.com/iaas/Content/Audit/Concepts/auditoverview.htm.
[142] 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
[143] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-audit-sec.html
[144] https://blogs.oracle.com/ateam/post/harnessing-the-power-of-linux-logs-in-oci-logging-analytics-om
[145] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-scap-sec.html.
[146] https://support.oracle.com/knowledge/Oracle%20Linux%20and%20Virtualization/2616282_1.html
[147] https://support.oracle.com/knowledge/Oracle%20Database%20Products/1405320_1.html
[148] https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm

Customer Use of Third-Party Software on ExaDB-D Customer VM

Customers have control to install third party software, including scanning software, on the ExaDB-D 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-D are published on My Oracle Support Installing Third Party Software On Exadata Components (Doc ID 1593827.1).[149]

Oracle Infrastructure Audit Logging

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

- ILOM
  - `syslog`
  - ILOM syslog redirected to the syslog of the physical infrastructure component
- Physical Exadata Database Server
  - `/var/log/messages`
  - `/var/log/audit.log`
  - `/var/log/secure`
  - `/var/log/xen/xend.log`
- Exadata Storage Server
  - `/var/log/messages`
  - `/var/log/audit.log`
  - `/var/log/secure`
- Storage Network Switch
  - `/var/log/messages`
  - `/var/log/audit.log`
  - `/var/log/secure`
  - `/var/log/opensm.log`

Oracle retains the following audit logs for ExaDB-D 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 at least 1 year.[150] 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[151] 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

[149] https://support.oracle.com/knowledge/Oracle%20Cloud/1593827_1.html
[150] https://www.oracle.com/contracts/docs/ocloud_hosting_delivery_policies_3089853.pdf
[151] https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html

prior to notifying the other party, depending on security policy and the details and circumstances of the unexpected action. If the customer detects an unauthorized action, the customer should notify Oracle of the action and response via the Oracle Service Request process. Oracle will notify the customer of confirmed unauthorized actions and Oracle responses per Oracle's Incident Response Policy.[152]

The customer may take any responsive action on any services they control. This includes terminating network connections into the customer VM and into the customer-controlled Oracle database.

Customers may use Delegate Access Control[153] to control and terminate Oracle staff access to customer VMs.

Oracle's responsive controls may include terminating connections at Bastion Servers in OCI and revoking access to Oracle-managed ExaDB-D infrastructure resources.

SERVICE TERMINATION AND DATA DESTRUCTION

Customers may terminate their ExaDB-D instance as part of ExaDB-D Lifecycle Management Operations.[154] Terminating an Exadata Database Service on Dedicated Infrastructure resource permanently deletes it and any databases running on it. The terminate service functionality is implemented as Exadata Database Machine Secure Erase.[155] 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.[156] Customers may obtain secure erase certifications from Oracle by opening a My Oracle Support (MOS) request.

EXCEPTION WORKFLOWS - ORACLE ACCESS TO CUSTOMER VM

The ExaDB-D 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.

VM is Controlled by Delegate Access Control

If a customer has implemented Delegate Access Control[157] and subscribed to Oracle Cloud Customer Support and Oracle Cloud Operation then Oracle database cloud support or Oracle cloud operations support staff will issue a Delegate Access Control Access Request to the customer. After approval, the Oracle support staff will access the VM via a unique,temporary, just-in-time credential deployed for least-privileged acesss implemented via Linux chroot jails to do the work. The Oracle Linux audit service will provide command/keystroke logs to the customer via OCI Logging service. The customer can optionally send the Oracle Linux audit logs to a syslog server they control.

Service Exception Before Customer Could Log Into Customer VM

If a customer service has an exception prior to the customer accessing the service, the customer can authorize Oracle staff to access the customer service by responding "yes" to Oracle's ask for access in the Service Request (SR) related to the service exception. The use cases for this method include failure for a VM to be created by cloud automation.

Oracle staff will ask for authorization in an existing SR by entering the following information:

---

[152] https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html
[153] https://docs.oracle.com/en-us/iaas/delegate-access-control/doc/overview-of-delac.html
[154] https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/examanagingDBsystem.htm
[155] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/exadata-secure-erase.html#GUID-6C9FD30C-FF88-4ABA-9249-93E183784B0D
[156] https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization
[157] https://docs.oracle.com/en-us/iaas/delegate-access-control/doc/overview-of-delac.html

- As per the security policy associated with ExaCC service, Oracle personnel are prohibited to access customer DomU without customer's explicit permission. For Oracle to comply with this policy, Oracle staff must - get customer permission to access DomU[158] by asking the following question.
- "In order for us to resolve the issue described in this SR, we need customer's explicit permission allowing us to login to customer DomU. By giving us explicit permission to access DomU, you are confirming that there is no confidential data that is stored in customer DomU or associated databases and customer security team is authorizing Oracle to have access to customer DomU in order for Oracle to help fix this issue. Do I have your explicit permission to access DomU?"

If the customer responds "yes" in the SR, then Oracle process and security controls will be temporarily adjusted to permit Oracle staff access to the customer VM. Oracle staff access to the customer VM will be authorized until the SR is closed or the customer directs Oracle to cease access in the SR.

Service Exception After Customer Could Log Into Customer VM

If a customer service has an exception after to the customer accesses the service, the customer can authorize Oracle staff to access the customer service by opening a new SR to authorize access.

The use cases for this method include the following:

- Errors that cause a VM to fail to boot
- Errors that cause customer `ssh` to VM to fail or lost customer credentials
- Other support error conditions

For the customer to authorize Oracle to access the customer VM, the customer must open a new SR with the following language:

- 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 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>

[158] DomU is an Oracle term for the customer VM deployed in the ExaDB-D service. This term is required as part of the process controls that govern Oracle staff access to the customer VM in the ExaDB-D service.

After the customer creates the new SR and Oracle receives the new SR, then Oracle process and security controls will be adjusted to permit Oracle staff to access the customer VM.

DATA PROCESSING AGREEMENT AUDIT

As part of the ExaDB-D 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[159] provides detail about how customers may request an audit and how the audit will be processed.

ORACLE DELEGATE ACCESS CONTROL

The Oracle Delegate Access Control[160] service is a privileged access management (PAM) service that enables ExaDB-D 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,[161] 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-D subscription
- Strategic Customers Program for DB Cloud Platforms – custom support services that are negotiated separately from the ExaDB-D 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 login to the customer VM to meet the same standards applied to customer staff accessing customer managed systems. For example, Delegate Access Control is ideal for banking and financial services applications, energy utilities, and defense, and any other application where risk management is a key pillar of application success.

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

---

[159] https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf
[160] https://docs.oracle.com/en-us/iaas/delegate-access-control/doc/overview-of-delac.html
[161] https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/oracle-operator-access-control-tech-brief.pdf

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

COMMERCIAL REFERENCE INFORMATION FOR SERVICE DELIVERY

This section summarizes Oracle public content with respect to the following aspects of the Exadata Database Service Dedicated (in Oracle Cloud Infrastructure, Azure, Google Cloud Provider, and Amazon Web Services) and Exadata Database Service on Dedicated Infrastructure:

- Oracle Incident Response - the process if a security event is expected
- Oracle security monitoring, including Exadata Database Service
- Consensus Assessment Initiative Questionnaire (CAIQ) related to security logging
- 1-Year minimum security log retention
- 99.95% uptime service level agreement reference
- 15 minute response time for critical issue reference
- 60 day access period after service termination

Oracle Incident Response

Reference Oracle Incident Response[162] publication.

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

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

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

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

Oracle Management of Security Event Logs

Reference Oracle Communications and Operations Management.[163]

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

Oracle policy requires that Lines of Business monitor logs for security event investigation and forensic purposes. Identified anomalous activities must feed into the security event management processes for the Line of Business owning that system.

---

[162] https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html
[163] https://www.oracle.com/corporate/security-practices/corporate/communications-operations-management.html

Access to security logs is provided on the basis of need-to-know and least privilege. Where possible, log files are protected by strong cryptography in addition to other security controls, and access is monitored. Logs generated by internet-accessible systems are required to be relocated to systems that are not internet-accessible."

Consensus Assessment Initiative Questionnaire (CAIQ) Related to Security Logs

Reference Oracle Consensus Assessment Initiative Questionnaire (CAIQ).[164]

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

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

...

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

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

...

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

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

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

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

...

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

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

- *Restricting access to log configuration capabilities to individuals with privileged access*
- *Encrypting log data in transit*
- *Classifying log records in accordance with the Information Protection Policy*
- *Continuously monitoring log data with automated tools"*

1-Year Minimum Security Log Retention

Reference page 8 of Oracle Cloud Hosting and Delivery Policies.[165]

"1.14 Security Logs

Oracle logs certain security-related activities on operating systems, applications, databases and network devices. Systems are configured to log default security activities, access to information or programs, system events such as alerts, console messages, and system errors. Oracle reviews logs for security event investigation and forensic purposes. Identified anomalous activities feed into the security event management process. Security logs are stored within the Security Information and Event

---

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

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

Management system (or equivalent system) in a native, unaltered format and retained in accordance with Oracle's internal policies. Security logs are retained online for a minimum of 1 year. These logs are retained and used by Oracle for our internal security operations."

99.95% Monthly Uptime Service Level Agreement (SLA)

Reference page 53 of PaaS and IaaS Public Cloud Services Pillar Document.[166]

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

Monthly Uptime Percentage: Service Credit Percentage

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

15-Minute Service Response Time for Critical Issues

Reference page 15 of Oracle Cloud Hosting and Delivery Policies.[167]

"5.3.1 Severity 1 (Critical Outage)

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

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

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

60-Day Access Period After Service Termination

Reference page 17 of Oracle Cloud Hosting and Delivery Policies.[168]

"6.1 Termination of Oracle Cloud Services

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

---

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

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

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

ORACLE MULTICLOUD

Oracle Multicloud[169] runs Oracle Database workloads in Azure, Google Cloud Provider, and Amazon Web services data centers. All Exadata hardware for Oracle Multicloud is physically located in the cloud provider data centers and connected to the cloud provider services via cloud provider networks. Oracle manages the infrastructure via Oracle-controlled networks that integrate the infrastructure into the OCI infrastructure management networks, and customers manage the database services they subscribe to. The Oracle Multicloud database service benefits from the simplicity, security, and low latency of a single operating environment within thin cloud provider network.

Customers may use the OCI Federated Identity Provider (IdP)[170] to can control how their staff authenticate to their Cloud Service Provider (CSP) tenancy and OCI tenancy for API and console driven lifecycle management of the Exadata Database Service, Recovery Service, and Autonomous Database Service.

Customers may optionally federate their database authentication with Centrally Managed Users,[171] including password authentication, Kerberos authentication, or public key infrastructure (PKI) authentication. With centrally managed users, customers can manage the authorization for Active Directory users to access Oracle databases.

Customers control authentication to their Oracle Database Service VMs using their privileged access management (PAM) software compatible with the Oracle Database VM - consult with applicable PAM providers for details. Customers may also use the token-based SSH access feature included in the Oracle Database Service.[172]

Customers may optionally use Delegate Access Control[173] to subscribe to Oracle support services, such as Database Cloud Services Support, Cloud Operations Support, and Engineered Systems Deployment and Infrastructure Support (ESDIS). Oracle Database and Cloud Operations support are included at no additional charge, and ESDIS may be purchased separately with fees based on the scope of services.

Customers may optionally use Operator Access Control[174] to control Oracle Autonomous Database Operations staff access to the Autonomous Database Service Dedicated VMs for your Autonomous Databases.

The Oracle database services are deployed in an OCI Child Site in the CSP data center. Duties are separated such that CSP staff control access to the CSP building for Oracle staff, and Oracle staff control access to the Oracle cages that secure the hardware inside of the OCI Child Site. The CSP physical data center security helps to control Oracle access to the OCI Child Site.

Figure 4 shows the Oracle Multicloud architecture where Oracle and the CSP work together to provide customers with API and console access to deploy private connectivity between their CSP network hosting their applications and the Oracle Database Service Virtual Cloud Network (VCN).

---

169 https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/Content/multicloud/Oraclemulticloud.htm
170 https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/federation.htm
171 https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/integrating_mads_with_oracle_database.html#GUID-9739D541-FA9D-422A-95CA-799A4C6F488D
172 https://docs.oracle.com/en-us/iaas/exadatacloud/doc/ecs-connect-to-service-instance.html
173 https://docs.oracle.com/en-us/iaas/delegate-access-control/doc/overview-of-delac.html
174 https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/oracle-operator-access-control-tech-brief.pdf

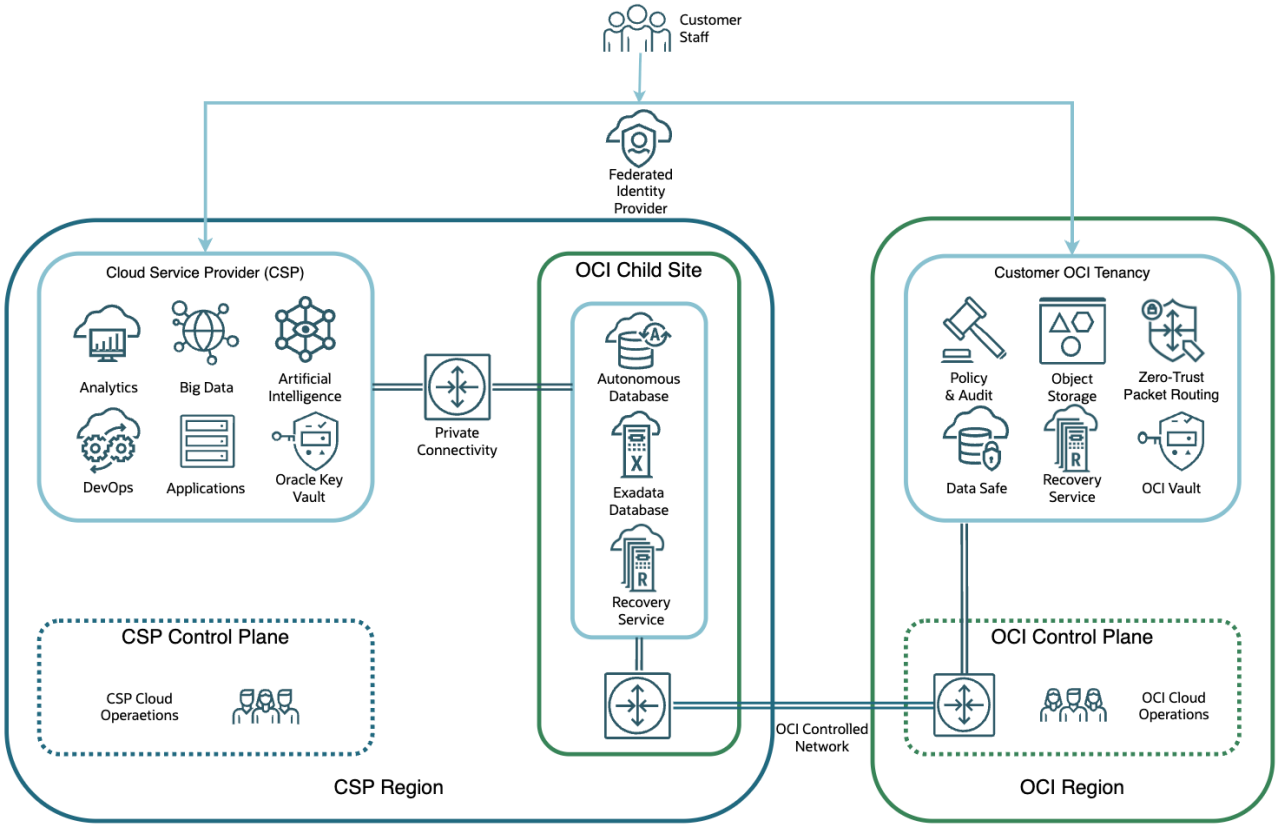

Figure 4: Multicloud Architecture

This private connectivity is deployed and managed in response to customer Federated IdP credentials that deploy the Oracle Database Service. Maintenance and support access for the hardware that implements the connectivity to route packets between the CSP network and the OCI VCN is separated between CSP and Oracle staff such that

- CSP cloud operations staff retain service credentials for Azure networking hardware and
- Oracle cloud operations staff retain credentials for Oracle networking hardware.

Oracle controls Oracle cloud operations access per Oracle's Access Control Practices[175] via least privilege, default deny approach where access is provided for

- those with a need-to-know,
- the least privileges to do the work,
- and a separation of duties to help prevent conflicts of interest.

Inside the CSP tenancy and network, customers will need to provide access to their database services and VM on the TNS lister port they configure for your service and for ssh access on port 22. The Oracle database service is configured to request encrypted connections from applications[176] and implement an encrypted connection for capable applications. In addition to the well-known Oracle database security features[177] and Exadata Database Service Security features,[178] customers may also store their Oracle Transparent Data Encryption (TDE)[179] Master Encryption Key (MEK) in

[175] https://www.oracle.com/corporate/security-practices/corporate/access-control.html
[176] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-network-data-encryption-and-integrity.html#GUID-42863092-227B-437C-AFFA-623BE6AEA0EA
[177] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/toc.htm
[178] https://docs.oracle.com/en-us/iaas/exadatacloud/doc/ecs-security-guide.html
[179] https://docs.oracle.com/en/database/oracle/oracle-database/19/asoag/introduction-to-transparent-data-encryption.html#GUID-B0870B12-E6AD-4254-B4B3-D6A15A637975

- a PKCS#12 compliant wallet[180] stored on an ACFS file system accessible to the VM cluster,
- an Oracle Key Vault (OKV) appliance[181] that you deploy in your CSP tenancy,
- OCI Vault[182] service running in the OCI region in supporting your Oracle Database service

All backups are encrypted with the same master key used for the Transparent Data Encryption wallet encryption.[183] The encryption key is not stored with the backup. When you use the Autonomous Recovery Service,[184] backups of encrypted tablespaces, and redo describing changes to these tablespaces, are encrypted.[185] The TDE-encrypted data blocks are secured on the protected database, Recovery Appliance storage, tape devices, and replicated appliances, and when transferred through any network connections.

The Oracle Database Service provides comprehensive audit logging of the database and VM access via Oracle Database Unified Audit[186] and Oracle Linux auditd.[187] Customers may send these audit records to their syslog server[188] or compatible security information event management (SIEM) system that they control; see the OCI solution playbook for streaming to SIEM[189] for an example.

Customers control database service lifecycle management via OCI Identity and Access Management (IAM).[190] IAM provides authorization control for which staff can perform which actions on which resources, and OCI Audit[191] provides a comprehensive audit record of the identity, action, and resource for lifecycle management actions. To deliver the service to the CSP Child Site, Oracle implements an OCI controlled network private to the Oracle control plane. This Oracle-controlled management network provides access for

- API and console driven lifecycle management functionality
- Oracle support staff shell access to infrastructure components when necessary
- Delegate Access Control shell access to your VMs when customers approve Oracle to access their VMs
- Access to OCI services that customers may consume to help you secure and run their business

Important OCI services that customers may use include the following:

- OCI Vault to store the TDE MEK - OCI Vault lets customers store and manage encryption keys and secrets to securely access resources,
- Oracle Data Safe to help understand data sensitivity, evaluate data risks, mask sensitive data, implement and monitor security controls, assess user security, monitor user activity, and manage Oracle Database 23ai SQL Firewall—all in a single, unified console,
- Oracle Database Autonomous Recovery Service - a fully managed data protection service for Oracle databases running on OCI, Microsoft Azure, and Google Cloud. Unique, automated capabilities protect Oracle Database changes in real time, validate backups without production database overhead, and enable fast, predictable recovery to any point in time,
- Zero Trust Packet Routing (ZPR) – to help prevent unauthorized access to data using an intent-based policy language, security administrators can define specific access pathways for data. Traffic that is not explicitly allowed

---

[180] https://docs.oracle.com/en/database/oracle/oracle-database/23/dbtde/introduction-to-transparent-data-encryption.html#GUID-769EC29B-0107-40FE-9A9D-BF81A4BBD0E9
[181] https://docs.oracle.com/en/solutions/deploy-key-vault-database-at-azure/index.html#GUID-F2B87C73-9C1E-4A59-98B2-43CD01279AB3
[182] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecscm/manage-databases.html#GUID-AC5FB30C-3F93-44EA-9653-2C8DA235986A
[183] https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/exadatacloud/doc/ecs-security-guide.html
[184] https://docs.oracle.com/en-us/iaas/recovery-service/index.html
[185] https://docs.oracle.com/en/engineered-systems/zero-data-loss-recovery-appliance/23.1/amagd/data-encryption-techniques.html#GUID-3E1A521B-3B51-4D1F-BF88-27BBE41A4B03
[186] https://www.oracle.com/database/technologies/security/db-auditing.html
[187] https://docs.oracle.com/en/learn/ol-auditd/
[188] https://support.oracle.com/knowledge/Oracle Cloud/2652319_1.html
[189] https://docs.oracle.com/en/solutions/oci-aggregate-logs-siem/#GUID-601E052A-8A8E-466B-A8A8-2BBBD3B80B6D
[190] https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm
[191] https://docs.oracle.com/en-us/iaas/Content/Audit/Concepts/auditoverview.htm

by policy cannot travel the network, improving security while simplifying the work of security, network, and audit teams,

- Object Storage – for low cost database backups and database service software updates and custom Oracle Home images.

Roles and Responsibilities for Oracle Multicloud

Table 3 describes the roles and responsibilities for Oracle, cloud services provider, and customer staff at supporting and operating Oracle Multicloud.

Table 3: Roles and Responsibilities for Oracle Multicloud

Work Function	Oracle Managed Infrastructure Responsibility	Cloud Services Provider Managed Infrastructure Responsibility	Customer Managed Services Responsibility
Monitoring	Infrastructure, Control Plane, Hardware Faults, Availability, Capacity	Infrastructure availability to support customer monitoring of customer service	Monitoring of Customer OS, Databases, Apps
Incident Management & Response	Incident Management and Remediation Spare Parts and Field Dispatch	Onsite Diagnostic Assistance (e.g., network troubleshooting, power, cooling	Incident Management and resolution for Customer's Apps
Patch Management	Proactive patching of Hardware, IaaS/PaaS control stack, Staging of available patches (e.g., Oracle DB patch set)		Patching of tenant instances
Backup & Restoration	Infrastructure and Control Plane Backup and recovery	Onsite Diagnostic Assistance (e.g., network troubleshooting, power, cooling	Snapshots/Backup & Recovery of customer resources using Oracle native backups or 3rd party solutions.
Cloud Support	Response and Resolution	Response & Resolution	Submit SRs via Support Portal

OD@Azure Details

The OD@Azure service is deployed across Exadata Database Server and Storage Server racks in an Azure data center of the customer's choice. The OD@Azure racks contain all the components of a standard Exadata Database Machine, plus networking hardware. The physical Exadata rack and networking infrastructure may be shared among multiple tenants (customers). The Exadata Database Servers and Exadata Storage Servers are dedicated to a single tenant (customer). Figure 5 shows an overview diagram of the OD@Azure service.

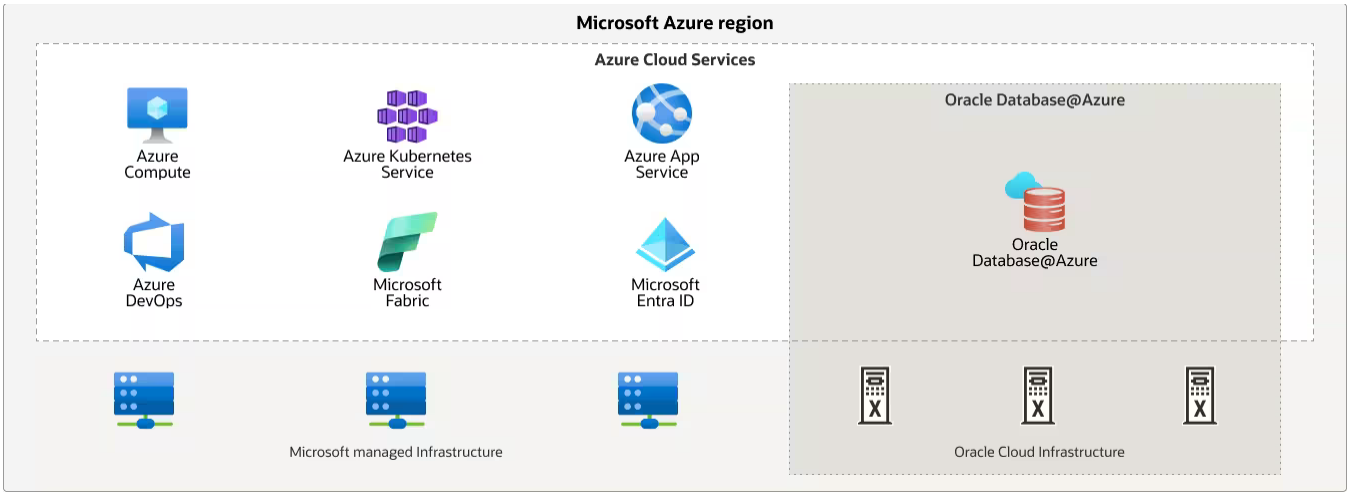

Figure 5: OD@Azure overview

Customers deploy and manage OD@Azure and database services using the Azure Console, Oracle Cloud Infrastructure Console and REST APIs. The customer controls access to the cloud automation's management functionality via the Azure Entra ID and OCI Identity and Access Management (IAM) services, and the Azure Audit and OCI Audit services provides the customer with a record of all customer-initiated management actions invoked via the Azure/OCI Console or Azure/OCI REST endpoints, such as creating or deleting databases. The customer controls network access to the ExaDB-D customer VM and database services running on the OD@Azure service via Azure Virtual Networks and OCI Virtual Cloud Networks. Microsoft and Oracle control network access to the OD@Azure infrastructure for cloud automation and operator shell access. All software updates, security patches, and deployments to OCI are performed the same way as any other OCI region, including the security and operational controls.

An OCI region contains one or three availability domains.[192] Each availability domain can have one or more data center sites with child DC sites acting as an extension of the OCI availability domain fabric. OCI child sites inside Azure data centers and are connected to the OCI region that's closest in terms of physical distance and network distance, as described in Figure 6.

OD@Azure stacks and their key dependencies are entirely hosted in the OCI child sites inside the Azure data centers with the same underlying infrastructure as OCI, offering the same physical network stack, Gen 2 Virtual Network service, off-box virtualization, and RDMA cluster network to power Oracle Exadata Database Service and the Oracle Autonomous Database. Figure 7 shows the OD@Azure architecture. Control plane connectivity for the OD@Azure service is implemented with a direct private network link between the OCI child site in the Azure data center and the Azure network in the same data center.

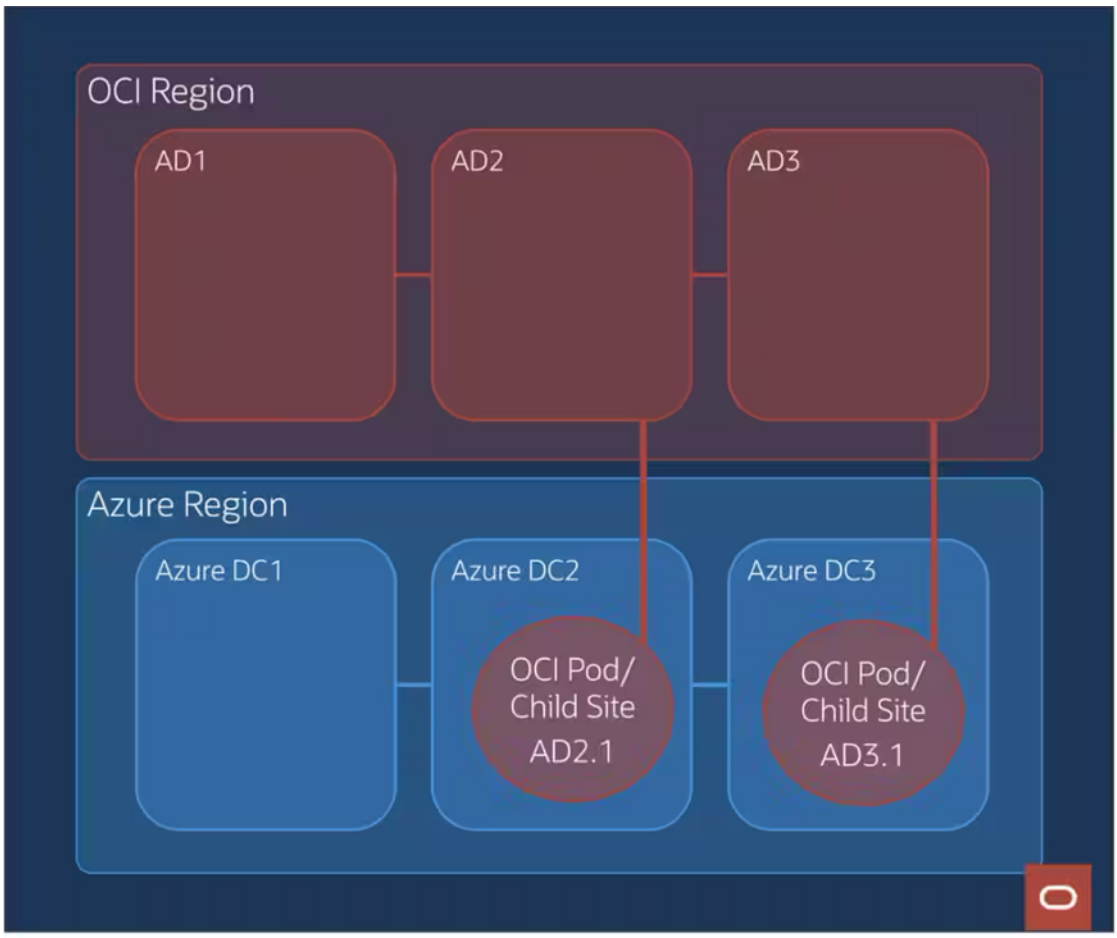

Figure 6: OD@Azure availability domains

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

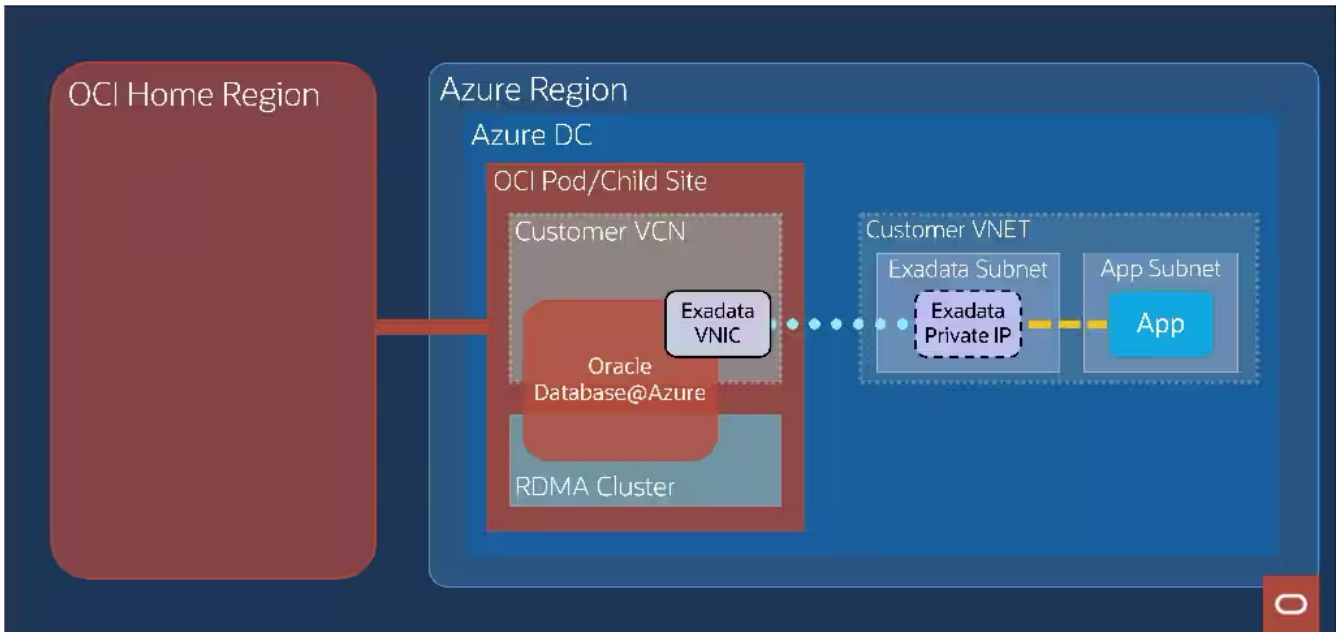

Figure 7: OD@Azure architecture diagram

OD@Azure IP Address and Routing Control Details

The OD@Azure database cluster is created in a subnet in an Azure virtual network (VNET). The cloud automation software creates a backend OCI virtual cloud network (VCN) for the ExaDB-D service with an equivalent subnet using the same IP CIDR range as the subnet in Azure VNET. The database cluster runs in the OCI subnet and using virtual network interface cards (VNICs) within the OCI subnet with necessary private IP assignments. The private IP addresses are reserved on the subnet in Azure VNET. A virtual mapping is created between the private IP in the customer VNET and the VNIC in the backend VCN through direct Azure-OCI connectivity within the Azure datacenter. Figure 8 shows the networking implementation for OD@Azure in a single availability zone, and Figure 9 shows the networking implementation in multiple availability zones.

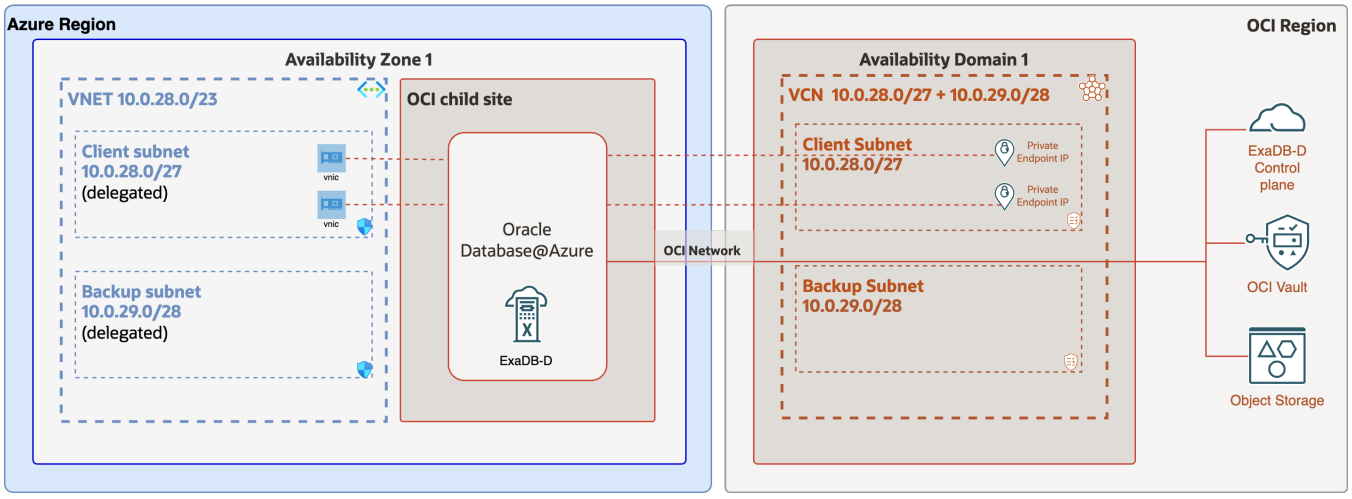

Figure 8: OD@Azure networking, single availability zone

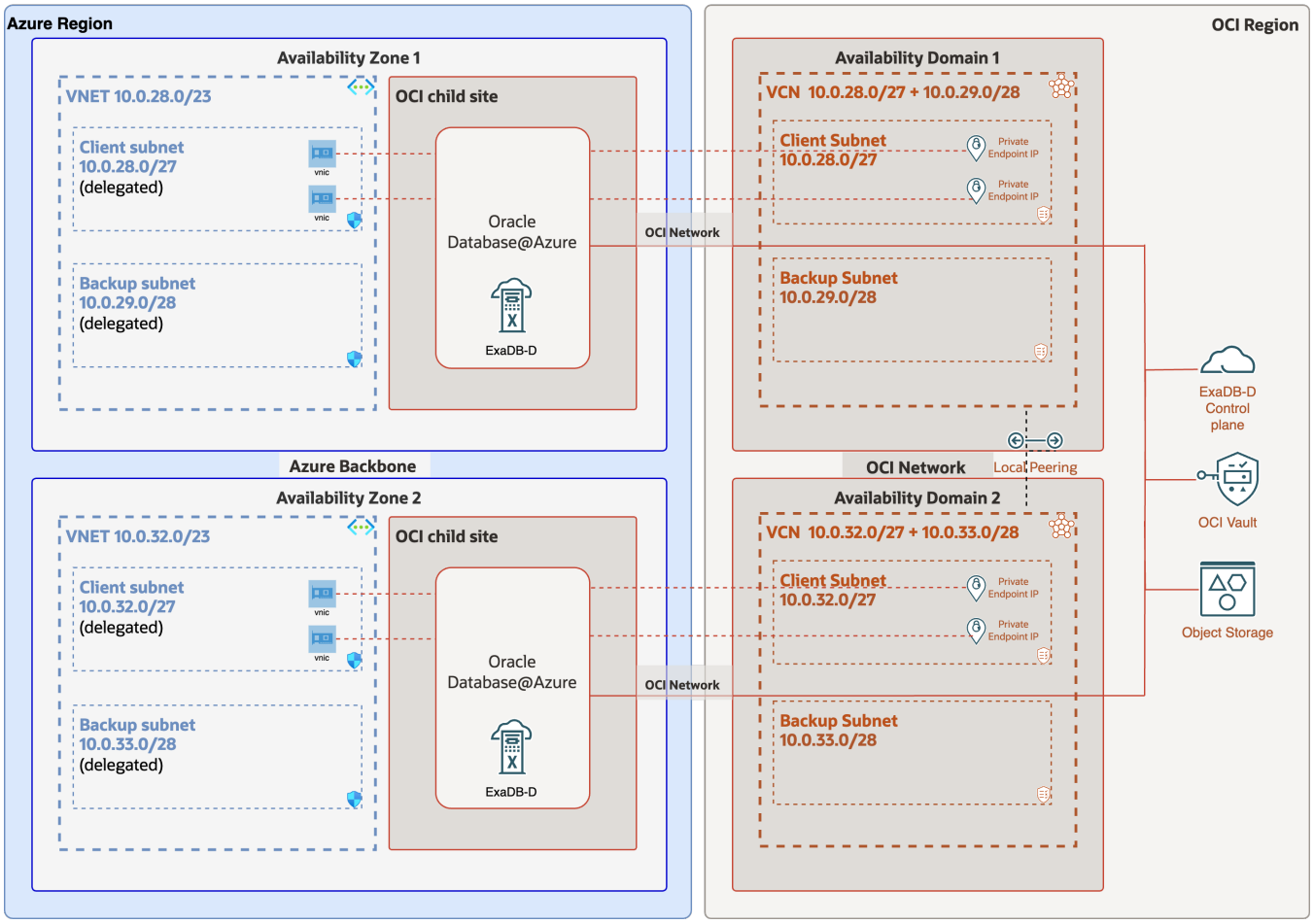

Figure 9: OD@Azure networking, multiple availability zones

When an application or user in Azure VNET connects to a database using the assigned private IP address, the Azure virtual networking service routes the packets through the direct private network connectivity to the edge gateway located inside the child site. The OCI virtual networking service routes the packets from the edge gateway to the servers hosting the Oracle Database instance. The direct private network link prevents the application, user, and database network traffic from leaving Azure data center.

OD@Azure Database Access Details

Customers access Oracle databases (DB) running on OD@Azure via an Azure VNET connection from customer endpoints to the databases running in the customer VM using standard Oracle database connection methods, such as SQLNet on TCP port 1521. Customer's access the VM running the Oracle databases via standard Oracle Linux methods, such as token based SSH on TCP port 22.

Customers may optionally access database services from applications running in OCI VCNs and customers may use OCI services that are integrated with the ExaDB-D service, such as Data Safe,[193] Vault,[194] Oracle Database Autonomous Recovery Service,[195] and customer-developed services within OCI.

[193] https://docs.oracle.com/en-us/iaas/data-safe/index.html
[194] https://docs.oracle.com/en-us/iaas/Content/KeyManagement/home.htm
[195] https://docs.oracle.com/en-us/iaas/recovery-service/doc/about-recovery-service.html

OD@Azure API Access Details

Customers use the Azure console to create the Exadata infrastructure and Exadata VM Cluster resources. Following, customers use OCI interfaces to create an Exadata database instance. The Azure console invokes the Azure Resource Manager which routes the API call to OD@Azure Resource Provider. The resource provider performs the appropriate translation, AuthZ and AuthN, and invokes the Exadata Database control plane, which is responsible for creating and managing the Exadata Database instance. To make the customer experience seamless, a federation is enabled between the Microsoft Entra ID and OCI Identity and Access Management (IAM) service. This integration allows customers to continue using Microsoft Entra ID for identity management. When customers invoke API calls on their OD@Azure resources, the corresponding downstream OCI API calls uses the federated identity for authentication purposes. Figure 10 shows the integration of Azure interfaces calling OCI APIs to manage the OD@Azure service.

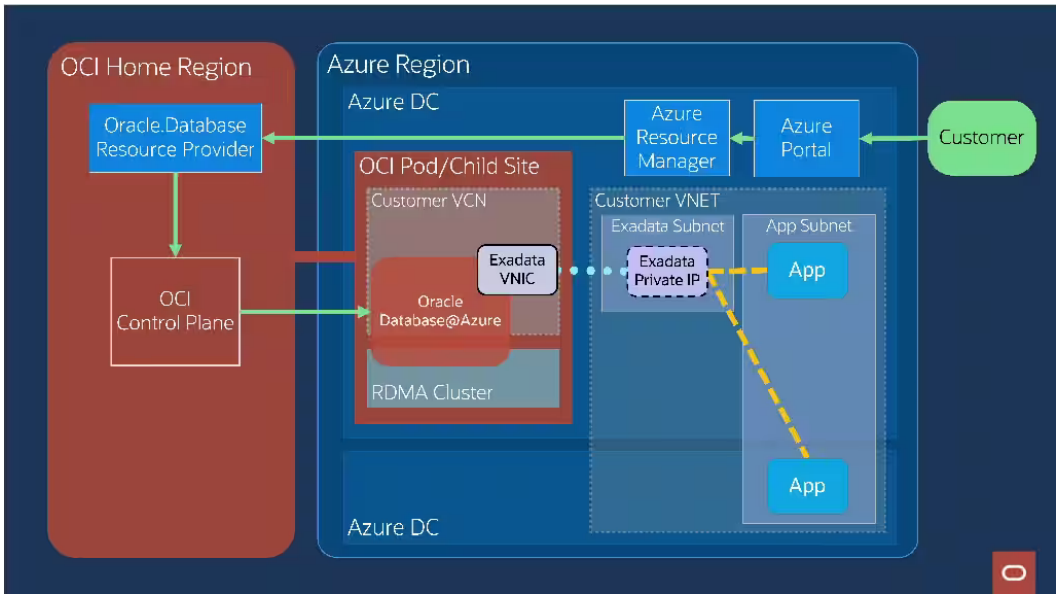

Figure 10: Customer access to Azure interfaces

SUMMARY

With Exadata Database Service on Dedicated Infrastructure, 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 Exadata Database Service on Dedicated Infrastructure help to prevent unauthorized actions on the infrastructure components of ExaDB-D. Security measures include multi-factor named user authentication and strong authentication with and FIPS 140-2 level 3 compliant token-based ssh access to Oracle-managed infrastructure components. Auditing and logging are implemented throughout the stack, and applicable audit logs are available to customers at their request via the Oracle Service Request (SR) process.

Exadata Database Service on Dedicated Infrastructure delivers 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 implement system security and help prevent unauthorized access to and theft of customer data. Oracle Cloud Operations staff does not access customer networks, services, or data to deliver the service, and customers do not access Oracle-managed infrastructure to consume the service. In the Exadata Database Service on Dedicated Infrastructure 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 Dedicated Infrastructure
Security Controls