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

June 11, 2025 | Version 2.34

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 IT projects.

This document summarizes the security and control features of the Oracle Exadata Database Service on Dedicated Infrastructure (ExaDB-D) within Oracle Cloud Infrastructure (OCI) and Oracle Multicloud[2], deployments. It is intended for customer security teams evaluating the adoption of ExaDB-D. Security teams evaluating ExaDB-D should also consult 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]

Oracle delivers the ExaDB-D service consistently across both OCI data centers and partner cloud service provider (CSP) environments, such as OD@Azure, OD@Google, and OD@AWS. However, Oracle Multicloud outlines key exceptions—specifically in areas like physical infrastructure control, control plane and remote management access, and the network configuration that links the ExaDB-D client virtual cloud network (VCN) to the partner cloud's 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

Purpose Statement 2

Disclaimer 3

Introduction 5

ExaDB-D Service Architecture 6

- Roles and Responsibilities 6
- Network Block Diagram 7
- Customer Access to OCI Interfaces 8
- Customer Access to Databases and VMs 9
- Oracle Infrastructure Monitoring 9
- Quarterly Software Updates 10
- Security Scanning 10
  - Customer Security Scanning and Testing of Customer VM 10
  - Monthly Oracle-Managed Infrastructure Security Scanning and Maintenance 11

Preventive Controls 11

- Data Security Controls 12
  - Oracle Native Network Encryption 13
  - Oracle Transparent Data Encryption 13
  - Oracle Database Vault 15
  - Oracle Data Safe 15
  - Oracle Database Security Assessment Tool (DBSAT) 16
  - Service Termination and Data Destruction 16
- VM Security Controls 16
  - Customer VM Default Users 17
  - Customer VM Default Security Settings 17
  - Customer VM Default Processes and Certificates 18
  - VM Console Access via OCI Control Plane 21
  - Cloud Automation Access to Customer VM 22
  - Oracle Delegate Access Control 22
  - Third-Party Software on ExaDB-D Customer VM 23
  - Considerations when Making Changes to the Service Software 23
- Infrastructure Software Security and Access Controls 24
  - Software Security Controls 24
  - Oracle Access Control for Infrastructure Components 24

Detective Controls (Logging and Auditing) 25

- Customer Audit Logging 25
  - OCI Audit Logging 26
  - Database Audit Logging 26
  - VM Audit Logging 26
  - File Integrity Monitoring 26
- Oracle Infrastructure Audit Logging 27

Responsive Controls 27

- Oracle Incident Response 28
- 15-Minute Service Response Time for Critical Issues 28

Commercial Reference Information 29

- Compliance 29
- Oracle Corporate Security Policies 29
- Vulnerability Disclosure 30
- Oracle Data Processing Agreement 30
- Oracle Cloud Services Agreement 30
- Security and Service Logs 31
  - Oracle Management of Security Event Logs 31
  - Consensus Assessment Initiative Questionnaire (CAIQ) Related to Security Logs 31

1-Year Minimum Security Log Retention 32
99.95% Monthly Uptime Service Level Agreement (SLA) 32
60-Day Access Period After Service Termination 32
Exception Workflows - Oracle Access to Customer VM 33
VM is Controlled by Delegate Access Control 33
Service Exception Before Customer Could Log into Customer VM 33
Service Exception After Customer Could Log into Customer VM 33
Oracle Multicloud 34
Oracle Multicloud Architecture 35
Roles and Responsibilities for Oracle Multicloud 37
OD@Azure Supplement 38
Deployment and Operation 38
API Access 40
IP Address and Routing Control 40
Database and VM Access 42
Summary 42

LIST OF IMAGES

Figure 1: Network Architecture block diagram for Oracle Exadata Database Service on Dedicated Infrastructure 8
Figure 2: Oracle Network Encryption, Database Vault, and Transparent Data Encryption 13
Figure 3: Cloud Operations Staff Access to ExaDB-D Infrastructure Components 25
Figure 4: Multicloud Architecture 35
Figure 5: OD@Azure overview 38
Figure 6: OD@Azure availability domains 39
Figure 7: OD@Azure architecture diagram 40
Figure 8: Customer access to Azure interfaces 40
Figure 9: OD@Azure networking, single availability zone 41
Figure 10: OD@Azure networking, multiple availability zones 41

LIST OF TABLES

Table 1: Roles and Responsibilities for ExaDB-D in OCI 7
Table 2: Default Port Matrix for Guest VM Services 18
Table 3: Roles and Responsibilities for Oracle Multicloud 37

INTRODUCTION

The Exadata Database Service on Dedicated Infrastructure (ExaDB-D) delivers the Oracle Exadata Database Machine as a managed cloud service in Oracle Cloud Infrastructure (OCI) data centers. Customers benefit from the full capabilities of Exadata combined with OCI orchestration tools and support from Oracle staff. ExaDB-D is ideal for customer who want the performance, availability, and security of Exadata and the operational and financial benefits of a cloud service.

Exadata Database Service on Dedicated Infrastructure (ExaDB-D) delivers Oracle's Exadata Database Machine as a service within 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.

This paper describes the security controls built into the ExaDB-D service delivery model. These controls reflect industry best practices and are designed to protect customer data and mission-critical workloads. If your current security standards differ, this paper suggests alternate controls so you can update or make exceptions to existing policies.

EXADB-D SERVICE ARCHITECTURE

ExaDB-D is deployed using Exadata Database Server and Storage Servers located in an Oracle Cloud Infrastructure (OCI) data center selected by the customer. While the physical power and networking infrastructure may be shared across tenants, the Exadata Database and Storage Servers are dedicated to a single customer.

Customer data remains on dedicated servers and is accessed via VCNs configured by the customer and storage networks, which are isolated by VLAN technology. Customers retain full control of credential they use to access their virtual machines and databases. With `root`-level (OS) and `SYS`-level (database) privileges, customers can enforce their own security policies and meet regulatory obligations. This may include installing agents, forwarding logs, configuring identity management, or other security configuration.

Customers deploy and manage ExaDB-D and database services using the Oracle Cloud Infrastructure Console and REST APIs.

They control access to cloud automation management functions through the OCI Identity and Access Management (IAM) [13] service. The OCI Audit[14] 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. Customers control network access to the ExaDB-D customer VM and database services running on the ExaDB-D service via Virtual Cloud Networks,[15] layer 3 and 4 network security controls,[16] Zero-Trust packet routing.[17]

Oracle controls network access the ExaDB-D infrastructure for cloud automation and for Oracle staff with a need to maintain the service in accordance with Oracle Access Control[18] practices.

Roles and Responsibilities

ExaDB-D follows a shared responsibility model, with Oracle and the customer each managing specific aspects of the system. Responsibilities are separated as follows:

Customer managed components:

- Virtual machines (VM)
- Databases running within them

Oracle managed infrastructure:

- Physical servers (Exadata database and storage servers)
- Storage networking switches
- Out of band (OOB) management switches
- Power Distribution Units (PDUs)

Oracle managed cloud control plane:

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

Customers are responsible for securing and managing access to their VMs and databases using OCI features like Virtual Cloud Networks (VCN),[19] Network Security Lists,[20] and VCN Flow Logs.[21] They also manage token-based `ssh` and authentication to their VMs and Oracle database authentication.[22]

---

[13] https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm
[14] https://docs.oracle.com/en-us/iaas/Content/Audit/Concepts/auditoverview.htm
[15] https://www.oracle.com/cloud/networking/virtual-cloud-network/
[16] https://docs.public.content.oci.oraclecloud.com/en-us/iaas/exadatacloud/doc/ecs-network-setup.html#GUID-8D325542-24CB-41C9-B0FF-73B2EFC4911D
[17] https://docs.oracle.com/en-us/iaas/Content/zero-trust-packet-routing/overview.htm
[18] https://www.oracle.com/corporate/security-practices/corporate/access-control.html
[19] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/overview.htm
[20] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/securitylists.htm#Security_Lists
[21] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/vcn_flow_logs.htm
[22] https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/exaconnectingDB.htm

Oracle controls and monitors access to Oracle-managed infrastructure components. Oracle staff are not authorized to access customer services, including customer VMs and databases, save certain support exceptions detailed in Exception Workflows - Oracle Access to Customer VM.

A detailed breakdown of roles and responsibilities is provided in Table 1, the Exadata Database on Dedicated Infrastructure Service Description[23] and Exadata Database Service on Dedicated Infrastructure - Explanation of Cloud Operations Service (Doc ID 2875973.1).[24]

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
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[25] 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)

Network Block Diagram

Figure 1 illustrates the network architecture for ExaDB-D. For more detail, refer to the Exadata Database Service on Dedicated Infrastructure Technical Architecture[26] documentation. In the diagram:

- Blue indicates customer-controlled components
- Red shows Oracle-managed components dedicated to a single customer
- Green represents shared Oracle-managed infrastructure

[23] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecscm/exa-service-desc.html
[24] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2875973.1
[25] https://docs.oracle.com/en-us/iaas/Content/Database/Concepts/examaintenance.htm
[26] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecsid/

The ExaDB-D Database and Storage Servers are connected through an isolated Layer 2 management network. This management network is entirely separate from the customer's client and backup networks—there is no direct connectivity between them.

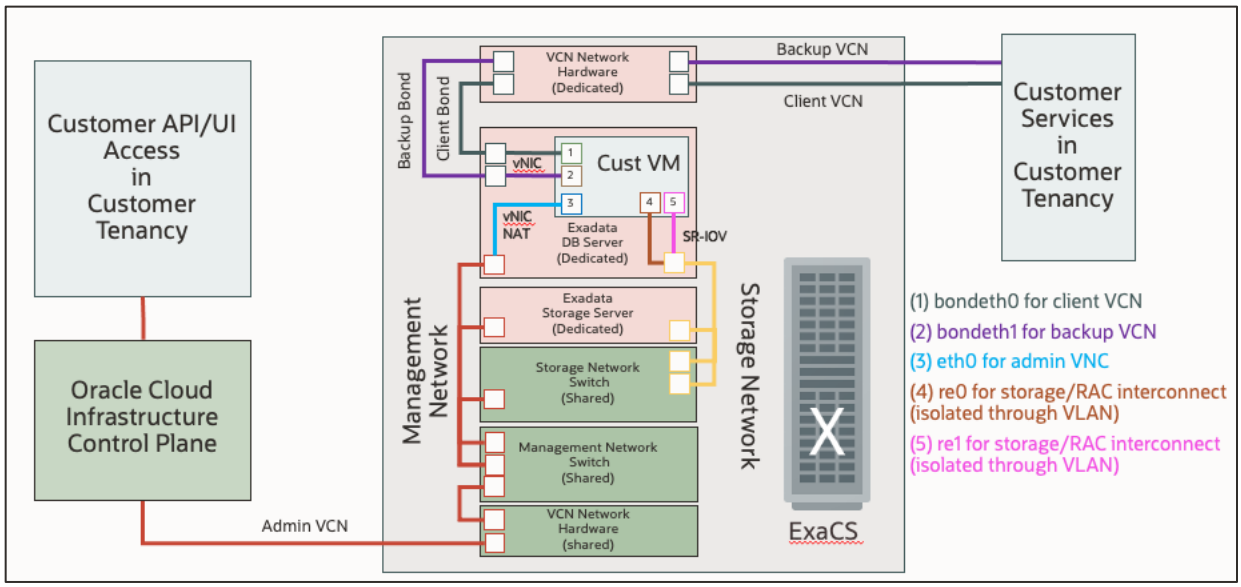

Figure 1: Network Architecture block diagram for Oracle Exadata Database Service on Dedicated Infrastructure

Oracle connects the Exadata Database Servers to OCI networking using specialized hardware. Shared infrastructure components appear in green, while those dedicated to the customer appear in red. Customers access their VMs over OCI Virtual Cloud Networks (VCNs), with interfaces mapped as vNICs. For resilience, these physical connections are configured in an active/standby setup managed by Oracle Cloud Operations. In case of a link failure, Oracle will automatically restore connectivity. Short interruptions might occur during recovery.

The customer VM connects to Exadata Storage via a private, non-routable interconnect using SR-IOV mapped interfaces (yellow). Each Exadata server connects to redundant storage switches in a high-availability (HA) configuration.

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`, as follows:

1. Temporary and unique `ssh` key pairs are generated by Oracle cloud automation to access the customer VM for each customer-initiated management action
2. Public `ssh` 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, (e.g., `oracle`, `opc`, `grid`, or `root`)
3. Software automation uses the temporary `ssh` keys to perform the required function
4. Temporary `ssh` keys are deleted

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.[27]

Customer Access to OCI Interfaces

Customers interact with ExaDB-D cloud automation via HTTPS (port 443) connections to OCI interfaces. The OCI control plane offers several interfaces for managing ExaDB-D:

- Web User Interface (web UI): for ad hoc actions via OCI Console
- Oracle Cloud Shell: a browser-based Linux shell within the Console
- OCI Command Line Interface (OCI CLI): command line interface for scripting and automation
- OCI SDK/RESTAPI: for application integration

[27] https://docs.oracle.com/en-us/iaas/exadatacloud/exacs/ecs-security-guide.html

Additionally, the OCI Terraform Provider[28] may be used to deploy and manage ExaDB-D. Terraform documentation is provided by Hashicorp.[29]

Access to management interfaces is controlled by the customer's OCI Identity and Access Management (IAM) policies. Customers may use OCI Network Sources[30] to limit authentication to their tenancy resources from IP addresses they control. If a customer-managed identity is authorized to perform a requested action, then the control plane sends the commands to the necessary components as follows:

Database operations:

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

Customer VM operations:

- Token-based ssh from control plane processes to service accounts
- Secured by temporary keys managed by the control plane and delivered via agent software in the customer VM
- Transported over the client or admin network

Infrastructure operations:

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

Customer Access to Databases and VMs

Customers connect to databases running on ExaDB-D through Oracle Cloud Infrastructure (OCI) Virtual Cloud Networks (VCNs) using standard Oracle protocols, such as Oracle Net over TCP port 1521. Access to the virtual machines (VMs) hosting these databases is managed using token-based SSH on TCP port 22, following standard Oracle Linux procedures.[31]

Infrastructure management tasks, such as OCPU scaling or creating VM clusters, are performed by customers through Oracle cloud automation tools, which are hosted in the OCI control plane.

Oracle Infrastructure Monitoring

Oracle monitors the ExaDB-D infrastructure to detect and respond to issues that fall within Oracle's operational responsibility, such as:

- Infrastructure security and access control
- Exadata Compute, Storage, and Network infrastructure hardware and software[32] monitoring and maintenance
- Auto Service Request Qualified Engineered Systems Products[33] event monitoring and maintenance

Infrastructure Monitoring Metrics (IMM) are automatically sent to monitoring systems in the OCI control plane, triaged by Oracle support, and assigned to support staff for resolution when required.

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

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

Customers are responsible for monitoring customer services (e.g., Guest VM, Oracle Cluster Services, Oracle database).

---

[28] https://docs.oracle.com/en-us/iaas/Content/API/SDKDocs/terraform.htm
[29] https://registry.terraform.io/providers/hashicorp/oci/latest/docs
[30] https://docs.oracle.com/en-us/iaas/Content/Identity/Tasks/managingnetworksources.htm
[31] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecscm/ecs-connect-to-service-instance.html#GUID-53DE1ED5-96D9-4F7F-B57F-4EF8D01FCDCB
[32] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2875973.1
[33] https://docs.oracle.com/cd/E37710_01/doc.41/e37287/toc.htm

Quarterly Software Updates

All software updates are controlled by Oracle Software Security Assurance Practices.[34] Oracle Software Security Assurance[35] standards apply to ExaDB-D software. Oracle implements segregation of duties[36] for software development, software test and quality assurance, and deployment of software ExaDB-D components.

Reference the following documentation for software update details:

- Oracle Critical Patch Updates for Security Alerts and Bulletins[37]
- My Oracle Support Document 2333222.1 for Exadata Cloud Software Versions[38]
- Oracle Cloud Infrastructure Maintenance documentation[39] for infrastructure updates
- Exadata Cloud Infrastructure System documentation[40] for customer VM, Grid Infrastructure, and Oracle database software updates

Oracle stages quarterly software updates for the Oracle database, Grid Infrastructure, and Linux operating system in OCI Object Storage. These updates are listed in OCI interfaces when they are available. Customers control when and how updates are applied via OCI interfaces.[41]

Oracle minimizes the impact of quarterly maintenance on customer applications using rolling maintenance operations, preserving database availability throughout the update process. Rolling maintenance reboots each database server, one at a time, with at most one server offline at any time. Applications designed for high availability automatically and transparently migrate their database connections between available database instances without disruption, eliminating the need for scheduling downtime. Storage server updates are also applied in a rolling manner.

Customers fully control quarterly maintenance schedules and can schedule maintenance during a period which will have the least impact on their business users. OCI interfaces provide full control and visibility over when quarterly maintenance will be applied and functionality to reschedule maintenance should unexpected business issues occur.

Security Scanning

Customer Security Scanning and Testing of Customer VM

Customers may use OpenSCAP[42] to scan the customer VM for compliance.

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)"[43] 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.[44]

---

[34] https://www.oracle.com/corporate/security-practices/assurance/
[35] https://www.oracle.com/corporate/security-practices/assurance/
[36] https://www.oracle.com/corporate/security-practices/corporate/access-control.html
[37] https://www.oracle.com/security-alerts/
[38] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2333222.1
[39] https://docs.oracle.com/en-us/iaas/exadatacloud/exacs/exa-conf-oracle-man-infra.html#GUID-C4301E26-E809-438F-96D7-9C6BB02FEA7F
[40] https://docs.oracle.com/en-us/iaas/exadatacloud/exacs/ecs-patch-update.html
[41] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecscm/ecs-patch-update.html#GUID-37442222-8D97-49FD-8CB3-B08B0F539E09
[42] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-scap-sec.html.
[43] https://support.oracle.com/knowledge/Oracle%20Database%20Products/1405320_1.html
[44] https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm

Monthly Oracle-Managed Infrastructure Security Scanning and Maintenance

Oracle performs a monthly infrastructure security scan and applies security updates to ExaDB-D infrastructure to Oracle managed components remain in compliance with Oracle corporate security standards. These standards align with and support various industry standards, including PCI-DSS, and government security standards, including FedRAMP High and ISO/IEC 27001.

Monthly security maintenance[45] is performed on database server infrastructure online, with no reboot, and no impact to your applications. Monthly updates are applied to storage servers in a rolling manner, also with no impact to your applications. Monthly security maintenance can also be scheduled at a specific time during the month, albeit in a single maintenance window. Oracle will publish a schedule for monthly maintenance at least one week prior to start of the maintenance period, and you can reschedule if required.

Customers are not permitted to access infrastructure components directly, nor can they install monitoring agents or transfer files to Oracle-managed infrastructure.

PREVENTIVE CONTROLS

The ExaDB-D service is designed to protect customer database data from unauthorized access. The ExaDB-D service separates access control duties between the customer and Oracle, as follows:

- The customer controls access to customer services, VMs, databases, and database data
- Oracle controls access to Oracle-managed infrastructure components

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

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 layers 2 and 3 access to customer VMs[46]
- Zero-trust Packet Routing to control layers 2 and 3 access to customer VMs[47]
- Network access rules implemented in the customer VM operating system[48] and Oracle database[49]
- 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[50]
- Transparent Database Encryption (TDE) for user tablespaces[51]

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

---

[45] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecscm/exa-conf-oracle-man-infra.html#GUID-1C03DC65-3210-41F6-88FC-7AA7BE7870BB

[46] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecscm/ecs-network-setup.html#GUID-40900E3C-8730-46E7-8F4C-9301ED0CEFF6

[47] https://docs.oracle.com/en/cloud/paas/base-database/zpr/index.html#articletitle

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

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

[50] ExaDB-D automation configures Oracle Native Network Encryption; Oracle strongly recommends that customers preserve this control

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

may implement such controls using operating system tools; however, customers should take care to allow cloud automation functionality that accesses the customer VM.

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)[52] credentials, and customer actions are controlled via OCI IAM permissions configured by the customer for specific resources. If the customer user is authorized to perform the requested management action on the target resource, then the requested command is sent to the 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.[53]

Data Security Controls

ExaDB-D helps to secure customer data for authorized use and blocks unauthorized access, including from Oracle Cloud Ops staff. Security measures include controls for:

- Authentication and access for named and privileged database users (for example, `SYS`, `SYSTEM`)
- Authentication and access for named and privileged VM users (for example, `root`, `opc`, `oracle`, `grid`)
- VM audit logging
- Oracle support staff access to customer VMs through Delegate Access Control[54]
- Monitoring agents and security controls that do not modify the Linux kernel or affect Exadata operation[55]
- Encryption of network connections to Oracle databases
- Encryption of Oracle database data at rest with Oracle Transparent Data Encryption (TDE)
- Optional Oracle Database Vault[56] to restrict privileges of database administrator accounts
- Customer-installed scanning agents on VMs (see Responses to common Exadata security scan findings My Oracle Support Doc ID 1405320.1[57] and Oracle Cloud Testing Policy[58])
- Customer-installed monitoring agents and security tools on VMs, provided they do not alter the Linux kernel or interfere with Exadata operation

Customers may store their TDE Master Encryption Key storage in any of the following:

- A Password protected PKCS12 wallet file stored in the VM file system
- The OCI Vault59 service
- An external key store, such as Oracle Key Vault

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

---

[52] https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm
[53] https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/exaconnectingDB.htm
[54] https://docs.oracle.com/en-us/iaas/delegate-access-control/doc/overview-of-delac.html
[55] 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
[56] Oracle Database vault is included with Enterprise Edition Extreme Performance subscription, and is not included with a Bring Your Own License (BYOL) subscription
[57] https://support.oracle.com/rs?type=doc&id=1405320.1
[58] https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm
[59] https://www.oracle.com/security/cloud-security/key-management/

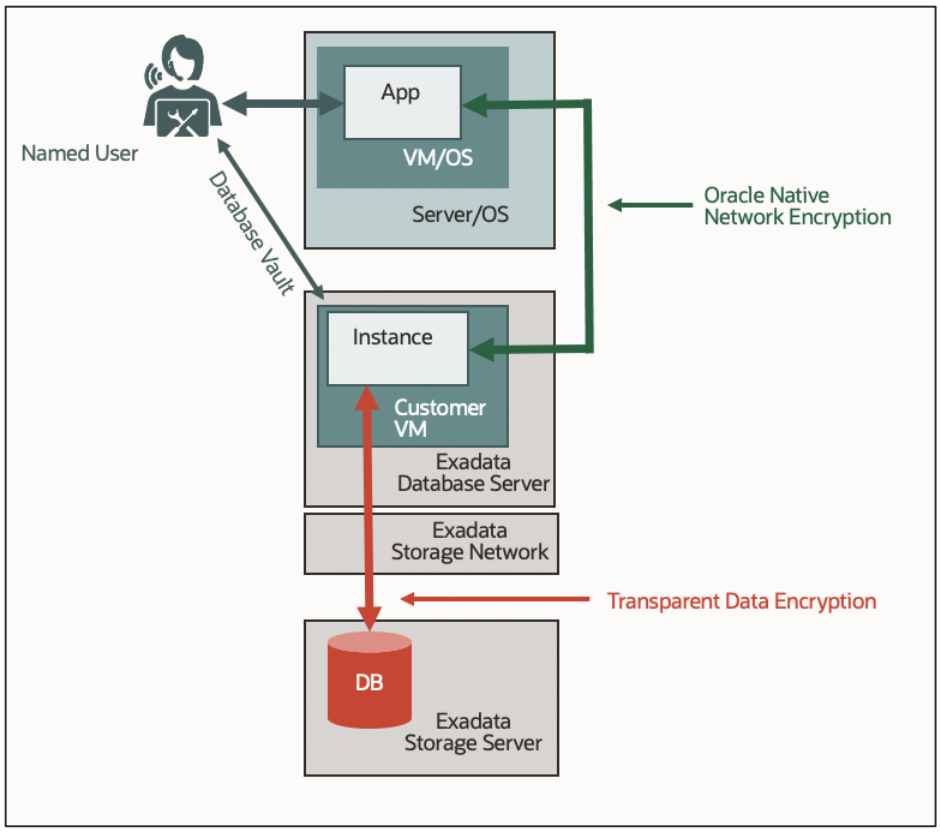

Figure 2: Oracle Network Encryption, Database Vault, and Transparent Data Encryption

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 can 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.[60] 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.[61]

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[62] provides answers to common Oracle TDE architecture and implementation questions.

---

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

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

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

Details for the TDE implementation on ExaDB-D are shown in the Exadata Database Machine Cryptographic Services[63] 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 works with Oracle Cloud Infrastructure (OCI) Vault and Oracle Key Vault (OKV), letting customers manage TDE keys outside of the VM for stronger security. With OCI Vault, customers get:

- Separate hardware to manage TDE Master Encryption Keys
- Reliable, durable, and fully managed key storage
- Hardware security modules (HSMs) certificated to FIPS 140-2 Level 3
- Automated TDE key rotation and audit features to help meet compliance requirements

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)[64], 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 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)."[65]

---

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

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

[65] https://support.oracle.com/knowledge/Oracle%20Cloud/2924192_1.html

Customers have the option to use the OKV Persistent Master Encryption Key Cache[66] 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[67] documentation.

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

Oracle Database is compatible with PKCS#11 compatible key management devices.[68]

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)[69] 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.[70]

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[71] published for each database version.

Oracle Data Safe

Oracle Data Safe[72] 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

---

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

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

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

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

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

[71] 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

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

- 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[73] 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[74] 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

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.[75]

Service Termination and Data Destruction

Customers may terminate their ExaDB-D instance as part of ExaDB-D Lifecycle Management Operations.[76] 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.[77] 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.[78] Customers may obtain secure erase certifications from Oracle by opening a My Oracle Support (MOS) request.

VM Security Controls

Access to the customer VM is implemented via token-based `ssh`.[79] 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

---

[73] https://docs.oracle.com/en/solutions/oracle-data-safe-for-on-prem-database/index.html#GUID-07534FC6-3B10-48E5-BD49-C011D55D1070
[74] https://www.oracle.com/security/database-security/data-safe/faq/
[75] https://www.oracle.com/database/technologies/security/dbsat.html
[76] https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/examanagingDBsystem.htm
[77] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/exadata-secure-erase.html#GUID-6C9FD30C-FF88-4ABA-9249-93E183784B0D
[78] https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization
[79] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecscm/ecs-connecting-to-service-inst.html#GUID-53DE1ED5-96D9-4F7F-B57F-4EF8D01FCDCB

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[80] are executed as image updates using the Exadata Database Machine image update process,[81] 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.

Customer VM Default Users

Each ExaDB-D customer VM includes standard privileged service accounts used by Oracle to deliver and maintain the service. Token-based SSH login is required; password-based SSH login is disabled.[82] Service accounts include:

- `root`: required by Linux; used for privilege used for software updates and some background processes (e.g., Oracle Trace File Analyzer Agent and ExaWatcher)
- `grid`: owns, runs, and maintains the Oracle Grid Infrastructure software and processes
- `oracle`: owns, runs, and maintains the Oracle database software and processes
- `opc`: used by Oracle cloud automation
  - Performs automation tasks
  - Can run certain privileged commands
  - Runs control plane agent software (DBCS Agent and DBCS Admin) for service lifecycle operations
- `dbmadmin`: used with the DBMCLI[83] tool to manage core Exadata features.

Security scanning tools should classify these accounts as service accounts. Customers may use the `opc` account for administrative purposes, including configuring LDAP or PAM software compatible with the ExaDB-D software.

Oracle recommends retaining the deployed usernames, userids, group names, and group ids. Changing the Oracle Home user (`oracle`) or Grid Infrastructure user (`grid`) after install is not supported and will cause service exceptions.[84]

Customer VM Default Security Settings

The ExaDB-D customer VM is deployed security settings designed to align with industry standards and Oracle best practices.[85,86] These configurations help enforce access control, reduce operational risks, and support automated lifecycle management. Key settings include:

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

Technical configurations include:

- `PermitRootLogin` value in `/etc/ssh/sshd_config`, which permits or denies the root user to login through SSH.
  - Default: PermitRootLogin is set to without-password.
  - Recommendation: keep default to permit cloud automation capabilities like OS patching
- `session-limit`: Sets the hard `maxlogins` parameter in `/etc/security/limits.conf`, which is the maximum number of logins for all users. This limit does not apply to a user with `uid=0`.
  - Default: `hard maxlogins 10`
  - Recommendation: keep default

---

[80] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-update-exacc-system.html
[81] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmmn/updating-exadata-software.html#GUID-E6090FA9-13B4-4BEF-A28D-73BDC3729C58
[82] https://docs.oracle.com/en-us/iaas/exadatacloud/doc/ecs-security-guide.html#GUID-84E782CD-10B8-47A1-A3AF-1DDEE82A6C06
[83] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmmn/using-dbmcli-utility1.html
[84] https://docs.oracle.com/en/database/oracle/oracle-database/19/cwwin/about-the-oracle-home-user-for-the-oracle-grid-infrastructure-installation.html
[85] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/security.html
[86] https://docs.oracle.com/en-us/iaas/exadatacloud/doc/ecs-security-guide.html#GUID-3A150605-1DC9-401F-9201-C0E73ABE817E

- `ssh-macs`: Specifies the available Message Authentication Code (MAC) algorithms.
- The MAC algorithm is used in protocol version 2 for data integrity protection.
  - Default: hmac-sha1, hmac-sha2-256, hmac-sha2-512 for both server and client
  - Recommendation: keep default
- `password-aging`: Sets or displays the current password aging for interactive user accounts.
  - `-M`: Maximum number of days a password may be used.
  - `-m`: Minimum number of days allowed between password changes.
  - `-W`: Number of days warning given before a password expires.
  - Default: `-M 99999`, `-m 0`, `-W 7`
  - Recommendation: for strict compliance `-M 60`, `-m 1`, `-W 7`

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

Customer VM Default Processes and Certificates

ExaDB-D customer VMs run Oracle software processes that support database operations, including Oracle Database, Oracle Real Application Clusters (RAC), Oracle Trace File Analyzer (TAF), Exawatcher, and Exadata Management Server (MS).[87] The services and ports are detailed in as Table 2. The table identifies the network interface, port number, process description, and certificate authority (CA) for each process. Oracle recommends configuring security scanners to accept the Oracle CA and Oracle self-signed certificates for Oracle-managed services. These certificates and CAs are built into the service and managed by Oracle to secure the delivery of lifecycle management operations. Accepting them reduces the risk of certificate -related service issues and minimizes operational burden.

Table 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[88]	N/A
		1521 Optionally, customers can assign a SCAN listener port (TCP/IP) in the range between 1024 and 8999. Default is 1521. Note: TNS listener opens dynamic ports after initial contact to well-known ports (1521, 1525).	Oracle TNS listener[89] Receives incoming client connection requests and manages the traffic of these requests to the database server. Supports Oracle Native Network Encryption (NNE) and TLS/SSL as transport layer security authentication[90]	Oracle self-signed; customers may add customer-controlled certificates

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

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

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

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

		5000	Oracle Trace File Analyzer[91] Collector	Oracle self-signed
		7879	Jetty Management Server.[92] Application server engine that is used internally by Oracle Exadata System Software, in particular Management Server (MS).[93]	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
Oracle Clusterware[94,95] running on each cluster node communicates through these interfaces.	clib0/clre0	1525	Oracle TNS listener Oracle Clusterware running on each cluster node communicates through these interfaces.	N/A

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

		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[96] 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). However, the IP/ports 7060/7070 attached to the storage interfaces are used to access DBCS agent from the Control Plane server.	stib0/stre0	7060	dbcs-admin Cloud agent for handling database lifecycle operations[97]	Oracle self-signed
		7070	dbcs-agent Cloud agent for handling database lifecycle operations[98]	Oracle self-signed
	stib1/stre1	7060	dbcs-admin	Oracle self-signed
		7070	dbcs-agent	Oracle self-signed

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

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),[99] 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[100]	Customer-controlled or Oracle signed

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.[101,102] 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 create an `ssh` connection from a customer device or OCI cloud shell to the VM console
3. Customer logs into to VM console using a username and password; typically `root`

---

[99] https://docs.oracle.com/en/database/oracle/oracle-database/19/cwadd/introduction-to-oracle-clusterware.html
[100] https://docs.oracle.com/en/cloud/paas/data-safe/admds/create-oracle-data-safe-onpremises-connector1.html
[101] https://docs.oracle.com/en-us/iaas/releasenotes/changes/9cee8331-1a56-494c-9bcc-f0dab3eea1b4/
[102] https://docs.oracle.com/en-us/iaas/exadata/doc/ecc-manage-vm-clusters.html#GUID-34F8308B-480A-4DAE-A158-2B4856E41A90

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.

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[103] 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.

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).[104]

Customers have control to block cloud automation `ssh` access at layers 3 and 4 via firewall configuration in the customer VM, but this will break cloud automation functionality that must access the customer VM via `ssh`. These include:

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

If these functions are needed, customers can temporarily restore access. Note that OCPU scaling does not require `ssh` access to the VM and will continue to work even when cloud automation is blocked at the network layer.

Oracle Delegate Access Control

Oracle Delegate Access Control[105] is an optional privileged access management (PAM) service integrated with ExaDB-D that enables 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,[106] 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

---

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

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

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

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

- 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

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 features include the following:

- Oracle staff access only after customer approval of a specific work request
- Access is limited to approved components related for each work request
- Access is temporary and automatically revoked after a set time
- Customers control when Oracle staff can access their services
- Software enforcement of privilege limits

Delegate Access Control detective security control features include the following:

- Customer notification when Oracle staff need to access the customer VM
- Command and keystroke logs traceable to an individual person

Delegate Access Control responsive security control features include the following:

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

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).[107]

Considerations when Making Changes to the Service Software

ExaDB-D provides customers with privileged access to their environments, including `root` access to guest operating systems and `SYSDBA` access to Oracle databases. This level of control allows customers to make configuration changes, but such changes may lead to exceptions or issues elsewhere in the stack over time.

If a problem arises, Oracle Support will help diagnose it through the Oracle Service Request (SR) process. Depending on the issue, Oracle may recommend reverting the change. In some cases, particularly those involving third-party software, Oracle

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

may request that the issue be reproduced without the third-party components, following its standard support policies.[108] Oracle support is included with your database service subscription at no additional charge.

Oracle recommends using the service as delivered. The design of ExaDB-D incorporates oversight from Oracle Corporate Security Architecture Oversight[109] and Oracle Software Security Assurance.[110] The service security features are described in the Exadata Database Service Dedicated Security Guide.[111] Following the prescribed service design helps reduce the need for extensive testing, validation, and troubleshooting of changes.

Infrastructure Software Security and Access Controls

Oracle exclusively manages infrastructure security and availability as outlined in the Oracle PaaS and IaaS documentation.[112]

Software Security Controls

ExaDB-D is based on the Exadata Database Machine and delivers the enterprise-class security features of Exadata Database Machine[113] 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 the service
- 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[114]
- Security architecture performed under Oracle Corporate Security Architecture[115]

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.

Oracle Access Control for Infrastructure Components

Oracle Corporate Security Practices[116] cover the management of security for Oracle internal operations and cloud services, and apply to all Oracle personnel, such as employees and contractors. These policies are aligned with the ISO/IEC 27002:2022(formerly known as ISO/IEC 17799:2005) and ISO/IEC 27001:2022 standards and guide all areas of security within Oracle. Oracle Access Control Practices[117] 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 comply 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

---

[108] https://support.oracle.com/knowledge/Oracle%20Cloud/1593827_1.html
[109] https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html
[110] https://www.oracle.com/corporate/security-practices/assurance/
[111] https://docs.oracle.com/en-us/iaas/exadatacloud/doc/ecs-security-guide.html
[112] https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf
[113] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/toc.htm
[114] https://www.oracle.com/corporate/security-practices/assurance/
[115] https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html
[116] https://www.oracle.com/corporate/security-practices/corporate/
[117] https://www.oracle.com/corporate/security-practices/corporate/access-control.html

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

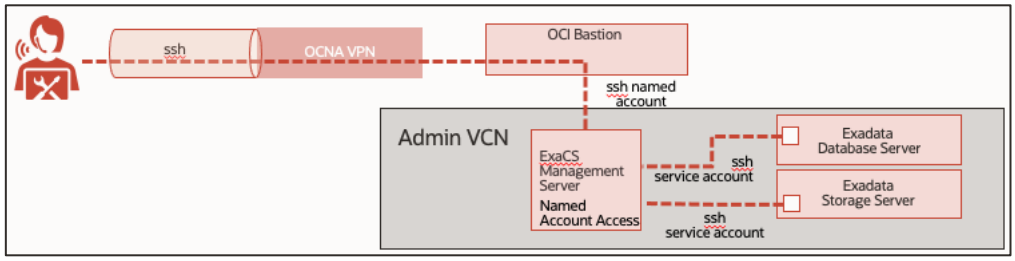

Figure 3: Cloud Operations Staff Access to ExaDB-D Infrastructure Components

Oracle controls Oracle Cloud Ops staff access to ExaDB-D infrastructure as follows:

OCNA access:

- Entitlement granted based on job-specific entitlements
- Authenticated with FIPS 140-2 Level 3 hardware MFA

Bastion and management server access:

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

Management server access:

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

ExaDB-D infrastructure access:

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

Oracle Access Control[118] practices restrict ExaDB-D infrastructure access to staff with a verified need, and includes these key policies:

- Support staff with appropriate job codes and training-enforced by technical controls-are authorized for access.
- Automated HR processes update access permissions based on changes to employee roles, training, or employment status

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).[119]

Customer Audit Logging

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

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

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

- OCI Audit Service:[120] 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:[121] audit logs for database actions initiated via a customer's Oracle database credential
- Customer VM operating system audit log:[122] audit logs for actions initiated on a customer VM via an operating system credential

OCI Audit Logging

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 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[123] 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.

Database Audit Logging

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[124] for each database version.

VM Audit Logging

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.[125] Customers may integrate the Oracle Linux audit logs into the OCI Log Analytics service.[126]

File Integrity Monitoring

Customers may use the Oracle Linux Advanced Intrusion Detection Environment (AIDE)[127] 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

---

[120] https://docs.oracle.com/en-us/iaas/Content/Audit/Concepts/auditoverview.htm
[121] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/introduction-to-auditing.html#GUID-94381464-53A3-421B-8F13-BD171C867405
[122] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-implement-sec.html#ol7-audit-sec
[123] https://docs.cloud.oracle.com/iaas/Content/Audit/Concepts/auditoverview.htm.
[124] 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
[125] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-audit-sec.html
[126] https://blogs.oracle.com/ateam/post/harnessing-the-power-of-linux-logs-in-oci-logging-analytics-om
[127] https://support.oracle.com/knowledge/Oracle%20Linux%20and%20Virtualization/2616282_1.html

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). When AIDE is installed, you can change the configuration in `/etc/aide.conf`. The configuration file is used to decide which files and directories are monitored by AIDE, and how logging and output are handled.

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.[128] 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[129] practices.

RESPONSIVE CONTROLS

The customer and Oracle work together to secure and monitor access to customer services, databases, database data, VMs, and infrastructure. Should either party detect an unauthorized action, that party can take responsive action immediately and prior to notifying the other party, depending on security policy and the details and circumstances of the unexpected action.

---

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

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

If the customer detects an unauthorized action, the customer should notify Oracle of the action and response via the Oracle Service Request process.

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, and customers may use Delegate Access Control[130] 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.

Oracle Incident Response

The Oracle Incident Response[131] publication describes how Oracle responds to security indents, as summarized below.

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

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

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

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

15-Minute Service Response Time for Critical Issues

The Oracle Cloud Hosting and Delivery Policies[132] publication describes Oracle's 15-minute service response time for critical issues, including security incidents, summarized below:

"5.3.1 Severity 1 (Critical Outage)

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

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

Oracle will use reasonable efforts to respond to Severity 1 service requests within fifteen (15) minutes. Throughout the period during which Oracle is working to address a Severity 1 service request, You agree to make available Your technical contact 24x7. Oracle will work 24x7 until the Severity 1 service request is resolved, a reasonable work-around is put in place, an approved action plan is in place or the Customer's 24x7 contact is no longer available. You must provide Oracle with a

[130] https://docs.oracle.com/en-us/iaas/delegate-access-control/doc/overview-of-delac.html
[131] https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html
[132] https://www.oracle.com/contracts/docs/ocloud_hosting_delivery_policies_3089853.pdf

technical contact during this 24x7 period to assist with data gathering, testing, and applying fixes. You are required to propose this severity classification with great care, so that valid Severity 1 situations obtain the necessary resource allocation from Oracle."

COMMERCIAL REFERENCE INFORMATION

This section summarizes Oracle public commercial content related to common security questions for the Exadata Database Service on Dedicated Infrastructure in Oracle Cloud Infrastructure, Azure, Google Cloud Provider, and Amazon Web Services. The Oracle Trust Center[133] provides an index to Oracle's security, compliance, privacy, and commercial contract documents for more detail.

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[134] 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.[135]

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 Corporate Security Policies

Oracle Corporate Security Practices[136] cover the management of security for Oracle's internal operations and cloud services, and apply to all Oracle personnel, such as employees and contractors. These policies are aligned with the ISO/IEC 27002:2022 (formerly known as ISO/IEC 17799:2005) and ISO/IEC 27001:2022 standards and guide all areas of security within Oracle. These practices include:

---

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

[134] https://www.oracle.com/cloud/compliance/#attestations

[135] https://docs.oracle.com/en-us/iaas/Content/ComplianceDocuments/Concepts/compliancedocsoverview.htm

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

- Objectives[137] – help protect the confidentiality, integrity, and availability of both Oracle and customer data
- Human resources security[138]
- Access control[139]
- Network communications security[140]
- Data security[141]
- Laptop and mobile device security[142]
- Physical and environmental security[143]
- Supply Chain Security and Assurance[144]

Vulnerability Disclosure

As a matter of policy, Oracle will not provide additional information about the specifics of vulnerabilities beyond what is provided in the Critical Patch Update or Security Alert notification, the pre-installation notes, the readme files, and FAQs[145] Oracle provides all customers with the same information to protect all customers equally. Oracle will not provide advance notification or "insider information" on Critical Patch Update or Security Alerts to individual customers. 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[146] page lists announcements of security fixes made in Critical Patch Update Advisories, Security Alerts and Bulletins, and it is updated when new Critical Patch Update Advisories, Security Alerts and Bulletins are released. Oracle will issue Security Alerts for vulnerability fixes deemed too critical to wait for distribution in the next Critical Patch Update, and a history of these alerts is maintained on the Critical Updates, Security Alerts, and Bulletins page.

Cloud customers, including ExaDB-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.

Oracle Data Processing Agreement

The Oracle Data Processing Agreement for Oracle Services[147] describes how Oracle controls, protects, and processes data, such as:

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

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

Oracle Cloud Services Agreement

The Oracle Cloud Services Agreement[148] provides information about customer data is processed in Oracle Cloud Services, such as:

- Ownership Rights and Restrictions

---

[137] https://www.oracle.com/corporate/security-practices/corporate/objectives.html
[138] https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
[139] https://www.oracle.com/corporate/security-practices/corporate/access-control.html
[140] https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html
[141] https://www.oracle.com/corporate/security-practices/corporate/data-protection/
[142] https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html
[143] https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
[144] https://www.oracle.com/corporate/security-practices/corporate/supply-chain/
[145] https://www.oracle.com/corporate/security-practices/assurance/vulnerability/disclosure.html
[146] https://www.oracle.com/security-alerts/#CVEOtherDocs
[147] https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf
[148] https://www.oracle.com/corporate/contracts/cloud-services/contracts.html#online

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

Security and Service Logs

This section provides details about how Oracle service teams manage security logs.

Oracle Management of Security Event Logs

Oracle Communications and Operations Management[149] describes how Oracle controls and manages security log information related to Oracle services, summarized below:

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

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

Consensus Assessment Initiative Questionnaire (CAIQ) Related to Security Logs

Oracle Consensus Assessment Initiative Questionnaire (CAIQ)[150] provides detail about how Oracle manages security logs, summarized below:

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

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

...

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

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

...

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

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

---

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

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

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

The Oracle Cloud Hosting and Delivery Policies[151] publication describes Oracle security log processing and retention, summarized below:

"1.14 Security Logs

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

99.95% Monthly Uptime Service Level Agreement (SLA)

The Oracle PaaS and IaaS Public Cloud Services Pillar Document[152] describes Oracle service credit remediation in cases where Oracle services are not delivered to 99.95% uptime, summarized below:

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

Monthly Uptime Percentage: Service Credit Percentage

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

60-Day Access Period After Service Termination

Oracle Cloud Hosting and Delivery Policies[153] describes the access period after service termination whereby customers can retrieve their data from the service, summarized below:

"6.1 Termination of Oracle Cloud Services

For a period of 60 days after the end of the Services Period for the Oracle Cloud Services or, if applicable, the 60 day period following Your termination of Cloud Services that You consume in a Pay as You Go model, following the end of their

---

[151] https://www.oracle.com/contracts/docs/ocloud_hosting_delivery_policies_3089853.pdf
[152] https://www.oracle.com/contracts/docs/paas_iaas_pub_cld_srvs_pillar_4021422.pdf
[153] https://www.oracle.com/contracts/docs/ocloud_hosting_delivery_policies_3089853.pdf

associated Services Period, Oracle will make available, via secure protocols and in a structured, machine-readable format, Your Content residing in the Oracle Cloud Services, or keep the service system accessible, for the purpose of data retrieval by You. At the end of the Services Period Your right to use such Services expires, except as otherwise permitted under the terms of the Oracle agreement, Your Order and the Service Specifications applicable to Your Oracle Cloud Services."

Exception Workflows - Oracle Access to Customer VM

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 cannot be accessed 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[154] 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 access 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:

- As per the security policy associated with ExaDB-D 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[155] 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 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:

---

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

[155] 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.

- SR Title:
  - SR granting Oracle explicit permission to access a Guest VM of ExaDB-D 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 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 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 ExaDB-D 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 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 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>

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.

ORACLE MULTICLOUD

Oracle Multicloud[156] 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)[157] to 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 federate their database authentication with Centrally Managed Users,[158] 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.

---

[156] https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/Content/multicloud/Oraclemulticloud.htm

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

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

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.[159]

Customers may use Delegate Access Control[160] 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[161] 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.

Oracle Multicloud Architecture

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).

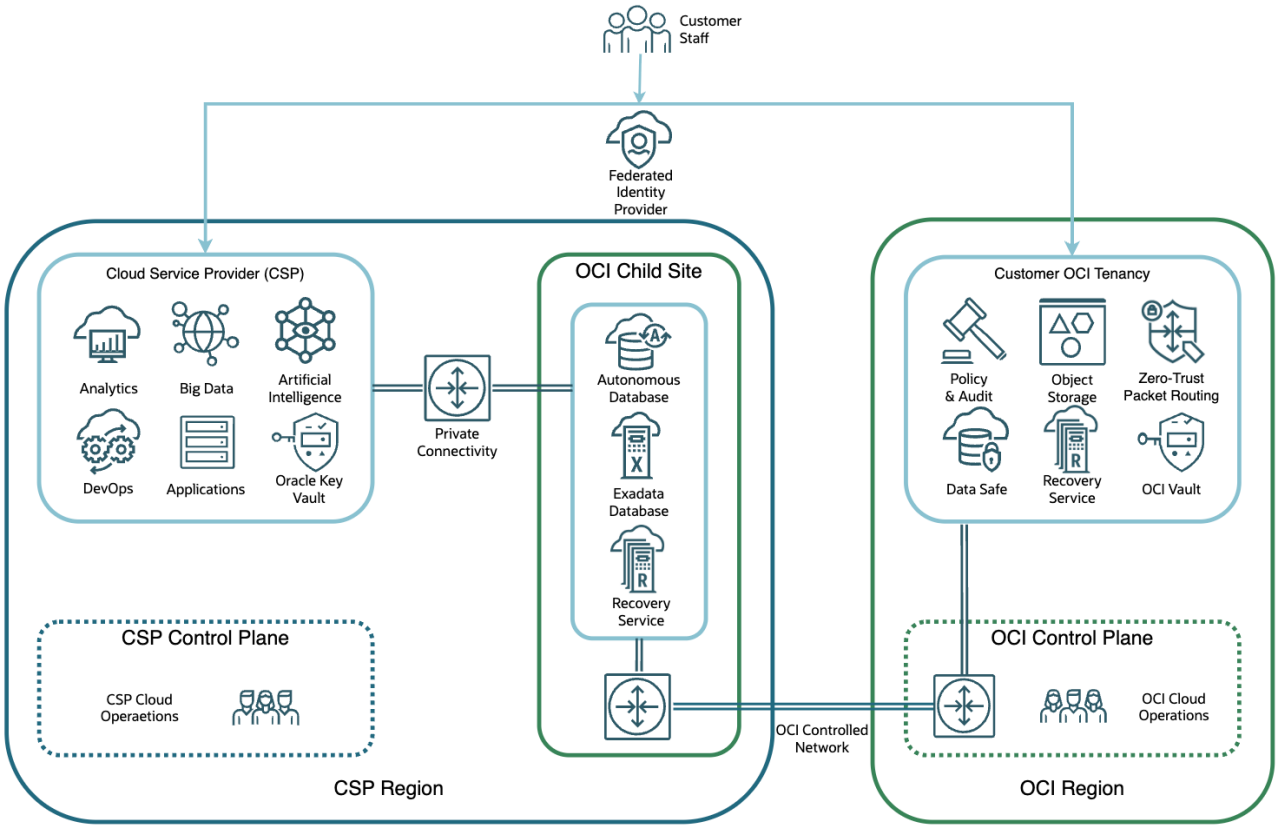

Figure 4: Multicloud Architecture

[159] https://docs.oracle.com/en-us/iaas/exadatacloud/doc/ecs-connect-to-service-instance.html
[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

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 Access Control Practices[162] via a least privilege, default deny approach where access is provided for:

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

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,[163] and implement an encrypted connection for capable applications. In addition to the well-known Oracle database security features[164] and Exadata Database Service Security features,[165] customers may also store their Oracle Transparent Data Encryption (TDE)[166] Master Encryption Key (MEK) in the following:

- A PKCS#12 compliant wallet[167] stored on an ACFS file system accessible to the VM cluster
- An Oracle Key Vault (OKV) appliance[168] deploy in the CSP tenancy,
- An OCI Vault[169] service running in the OCI region in supporting the Oracle Database service

All backups are encrypted with the same master key used for the Transparent Data Encryption wallet encryption.[170] The encryption key is not stored with the backup. When customers use the Autonomous Recovery Service,[171] backups of encrypted tablespaces, and redo describing changes to these tablespaces, are encrypted.[172] 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[173] and Oracle Linux auditd.[174] Customers may send these audit records to their syslog server[175] or compatible security information event management (SIEM) system that they control. See the OCI solution playbook for streaming to SIEM[176] for an example.

---

[162] https://www.oracle.com/corporate/security-practices/corporate/access-control.html
[163] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-network-data-encryption-and-integrity.html#GUID-42863092-227B-437C-AFFA-623BE6AEA0EA
[164] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/toc.htm
[165] https://docs.oracle.com/en-us/iaas/exadatacloud/doc/ecs-security-guide.html
[166] https://docs.oracle.com/en/database/oracle/oracle-database/19/asoag/introduction-to-transparent-data-encryption.html#GUID-B0870B12-E6AD-4254-B4B3-D6A15A637975
[167] https://docs.oracle.com/en/database/oracle/oracle-database/23/dbtde/introduction-to-transparent-data-encryption.html#GUID-769EC29B-0107-40FE-9A9D-BF81A4BBD0E9
[168] https://docs.oracle.com/en/solutions/deploy-key-vault-database-at-azure/index.html#GUID-F2B87C73-9C1E-4A59-98B2-43CD01279AB3
[169] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecscm/manage-databases.html#GUID-AC5FB30C-3F93-44EA-9653-2C8DA235986A
[170] https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/exadatacloud/doc/ecs-security-guide.html
[171] https://docs.oracle.com/en-us/iaas/recovery-service/index.html
[172] 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
[173] https://www.oracle.com/database/technologies/security/db-auditing.html
[174] https://docs.oracle.com/en/learn/ol-auditd/
[175] https://support.oracle.com/knowledge/Oracle Cloud/2652319_1.html
[176] https://docs.oracle.com/en/solutions/oci-aggregate-logs-siem/#GUID-601E052A-8A8E-466B-A8A8-2BBBD3B80B6D

Customers control database service lifecycle management via OCI Identity and Access Management (IAM).[177] IAM provides authorization control for which staff can perform which actions on which resources, and OCI Audit[178] 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
- Oracle support staff shell access to infrastructure components when necessary
- Delegate Access Control shell access to customer VMs when customers approve Oracle to access their VMs
- Access to OCI services that customers may consume to help them secure and run their business

Important OCI services that customers may use include the following:

- OCI Vault to store the TDE MEK[179] - OCI Vault lets customers store and manage encryption keys and secrets to securely access resources
- Oracle Data Safe[180] - helps customers to 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[181] - 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)[182] – helps to 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 by policy cannot travel the network
- Object Storage[183] – 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

[177] https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm
[178] https://docs.oracle.com/en-us/iaas/Content/Audit/Concepts/auditoverview.htm
[179] https://docs.oracle.com/en-us/iaas/exadatacloud/doc/manage-databases.html#GUID-E322F1CC-46C9-47A1-8A4E-921432B25287
[180] https://docs.oracle.com/en-us/iaas/data-safe/index.html
[181] https://docs.oracle.com/en-us/iaas/recovery-service/index.html
[182] https://www.oracle.com/security/cloud-security/zero-trust-packet-routing/
[183] https://docs.oracle.com/en/database/oracle/oracle-database/23/bkupr/bkupr_object_storage.html

Work Function	Oracle Managed Infrastructure Responsibility	Cloud Services Provider Managed Infrastructure Responsibility	Customer Managed Services Responsibility
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 Supplement

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.

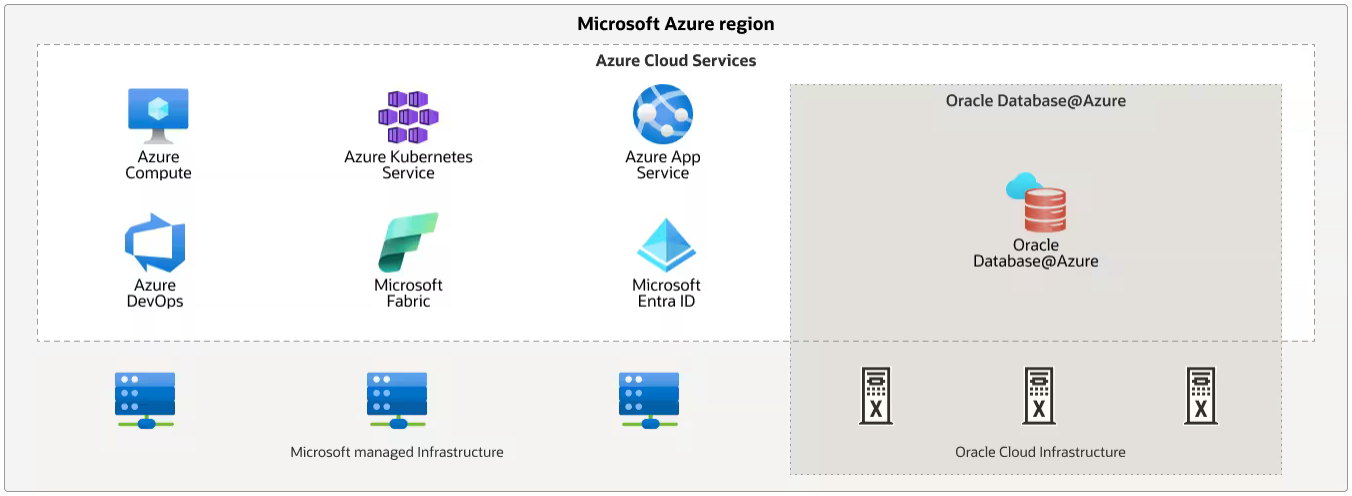

Figure 5: OD@Azure overview

Deployment and Operation

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.[184] 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.

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

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.

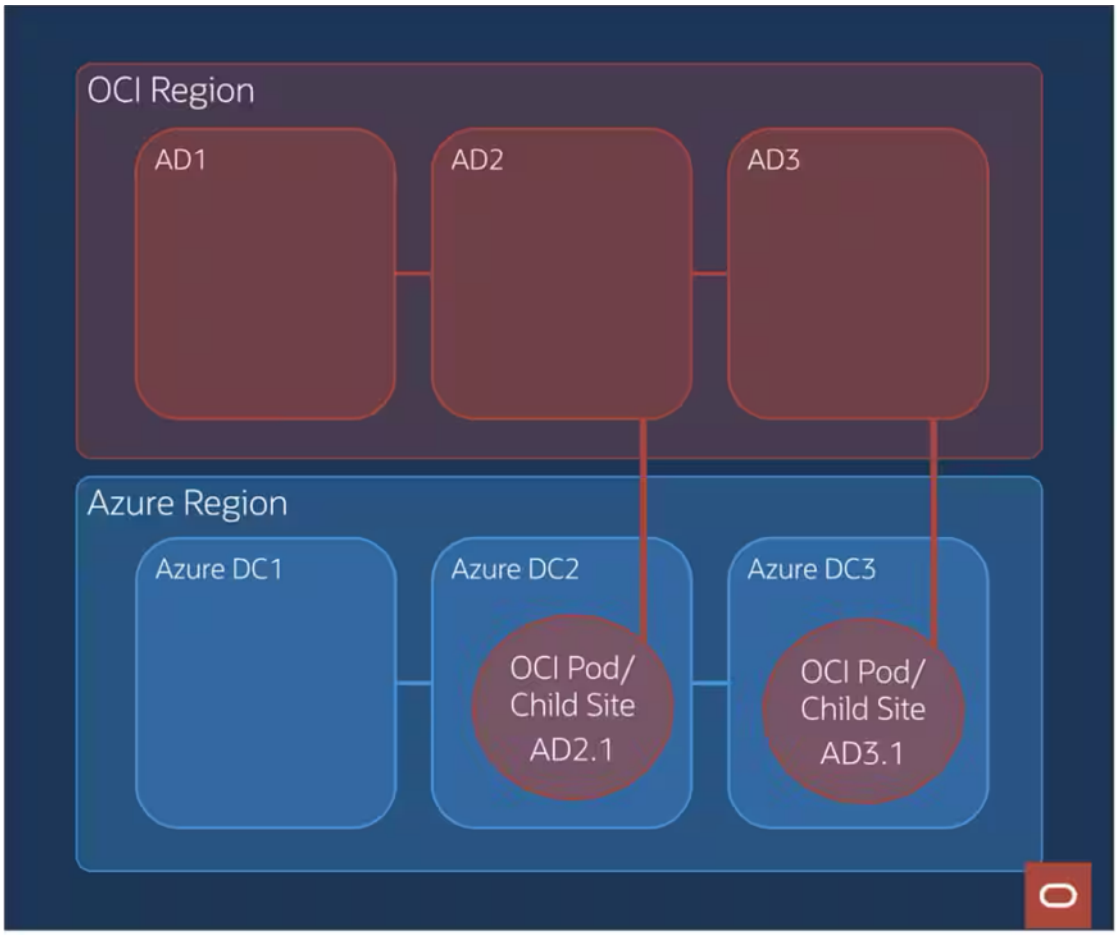

Figure 6: OD@Azure availability domains

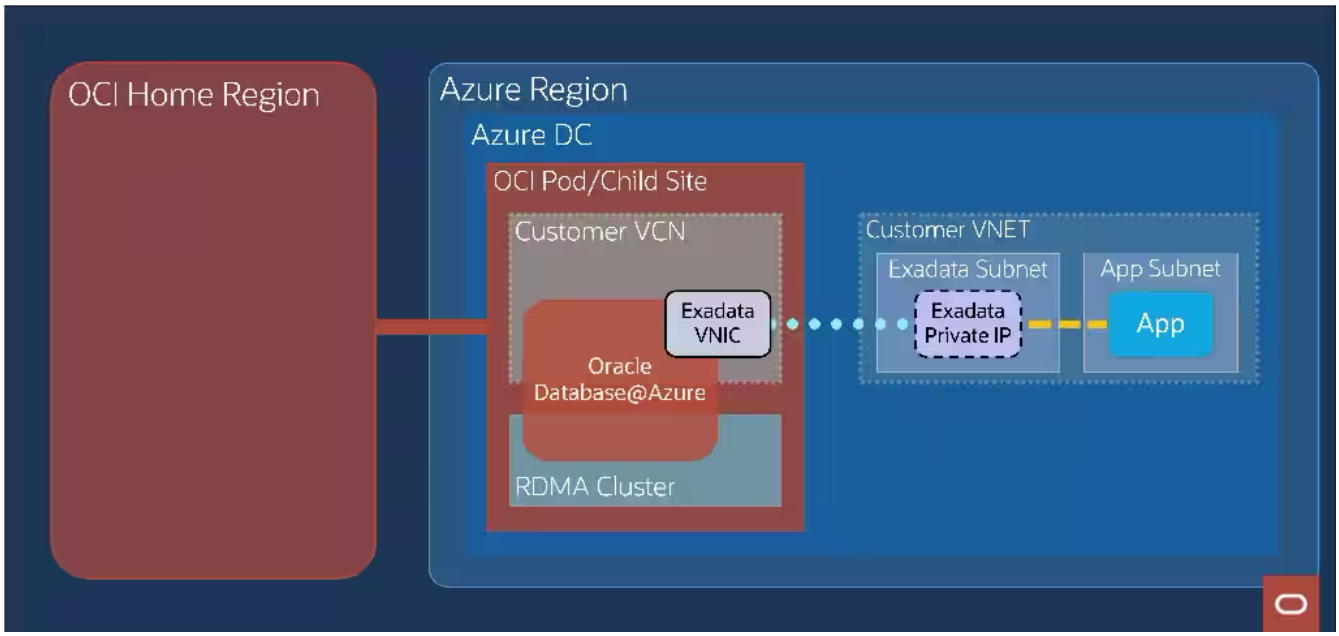

Figure 7: OD@Azure architecture diagram

API Access

Customers use the Azure console to create Exadata infrastructure and VM clusters, then use OCI interfaces to create Exadata database instances. The Azure console calls Azure Resource Manager, which routes API requests to the OD@Azure Resource Provider. The resource provider handles translation, authorization, authentication, and interacts with the Exadata Database control plane to create and manage database instances.

Federation between Microsoft Entra ID and OCI Identity and Access Management (IAM) lets customers continue using Entra ID for identity management. When customers make API calls to OD@Azure resources, the calls use federated identity for authentication with downstream OCI APIs.

Figure 8 shows the integration of Azure interfaces calling OCI APIs to manage the OD@Azure service.

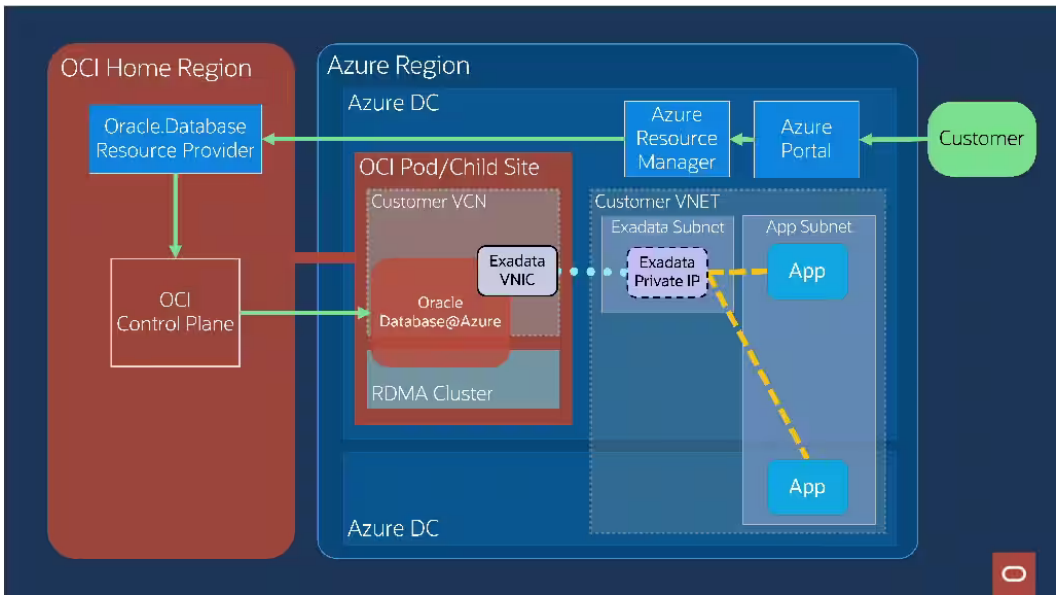

Figure 8: Customer access to Azure interfaces

IP Address and Routing Control

The OD@Azure database cluster is deployed in a subnet within an Azure virtual network (VNET). Automation creates a corresponding OCI virtual cloud network (VCN) with a matching subnet and IP CIDR range. The cluster runs in the OCI

subnet using VNICs assigned private IPs. These private IPs are also reserved in the Azure VNET subnet. Direct Azure-OCI connectivity in the Azure datacenter maps each private IP in the VNET to its corresponding VNIC in the VCN.

Figure 9 shows the networking implementation for OD@Azure in a single availability zone, and Figure 10 shows the networking implementation in multiple availability zones.

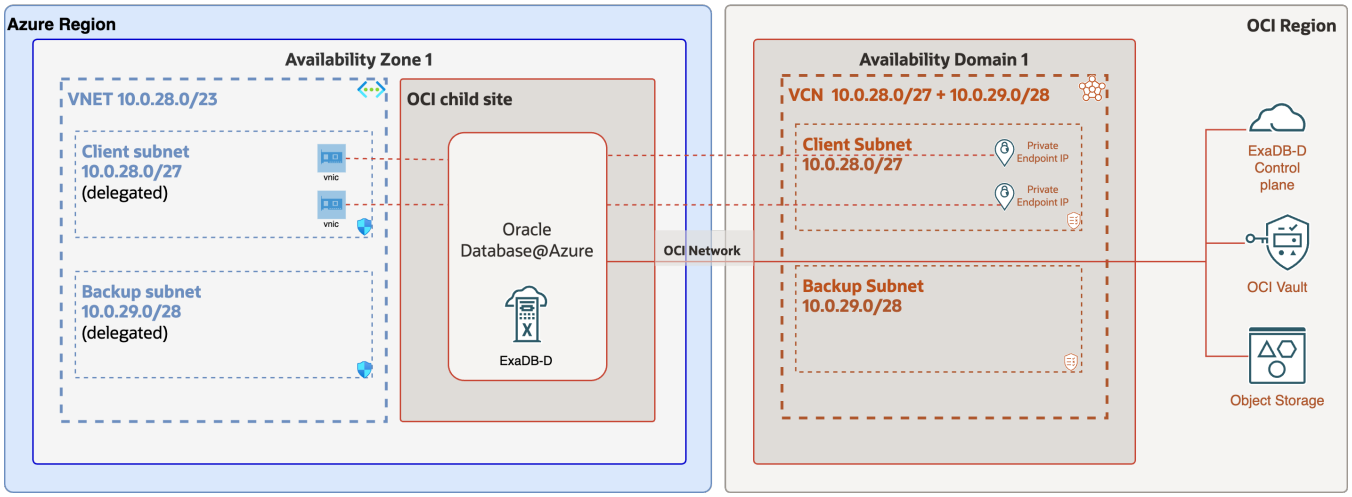

Figure 9: OD@Azure networking, single availability zone

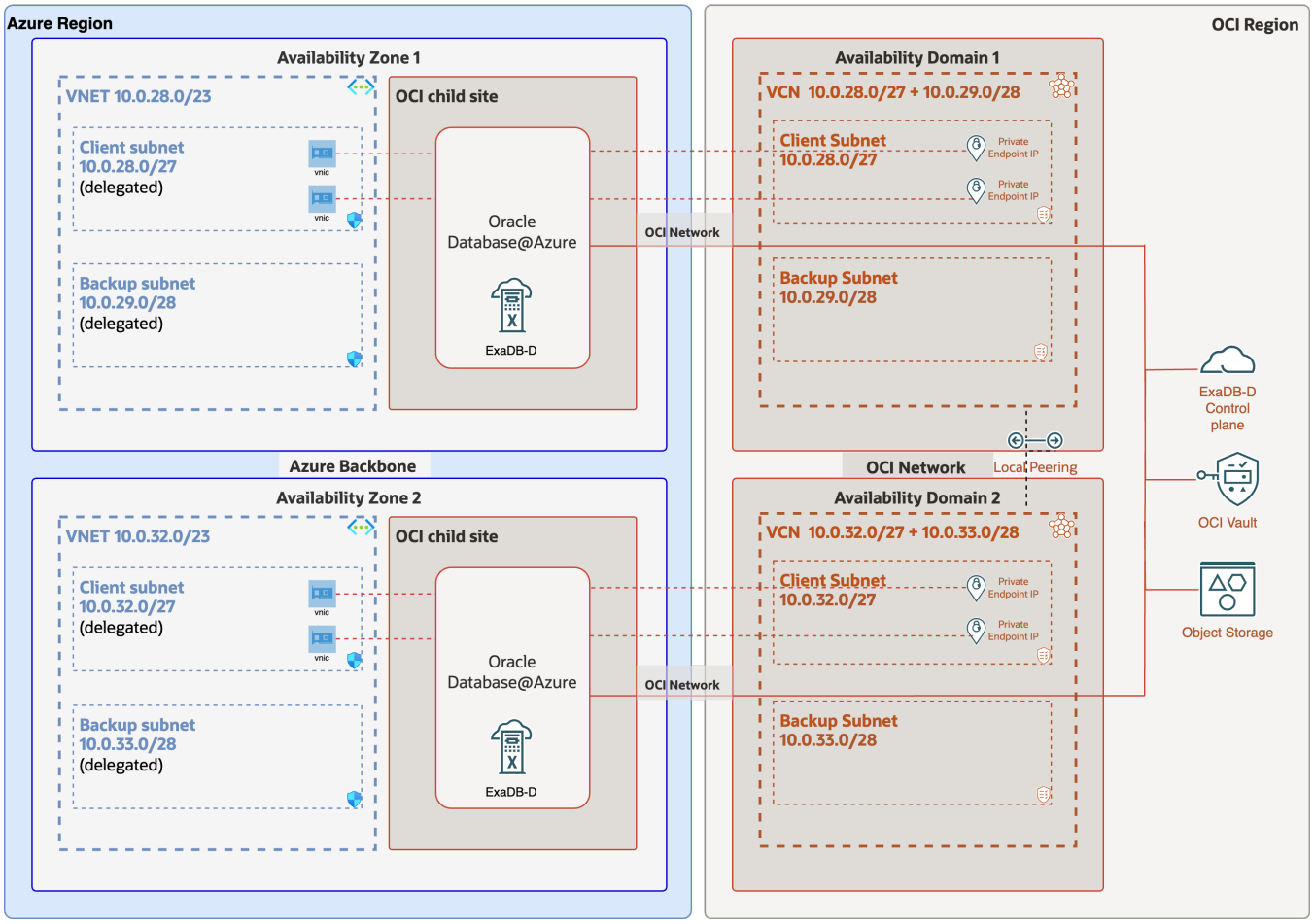

Figure 10: OD@Azure networking, multiple availability zones

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 helps to prevent the application, user, and database network traffic from leaving Azure data center.

Database and VM Access

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,[185] Vault,[186] Oracle Database Autonomous Recovery Service,[187] and customer-developed services within OCI.

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 encrypts 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. 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.

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

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