Oracle OCI Exadata Database Service on Dedicated Infrastructure Security Controls

ORACLE

Exadata Database Service on Dedicated Infrastructure Security Controls

A Technical Summary for Security Approvers and Developers

December 8, 2025 | Version 2.42

PURPOSE STATEMENT

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

This document summarizes the security features of the Oracle Exadata Database Service on Dedicated Infrastructure (Exadata Database Service) in Oracle Cloud Infrastructure (OCI) and Oracle Multicloud.[2] It is intended for security staff evaluating Exadata Database Service. Links to other documentation you should also consult are provided throughout the document. Oracle delivers the Exadata Database Service similarly in OCI and partner cloud service provider (CSP) environments, such as Oracle Database@Azure, Oracle Database@Google Cloud, and Oracle Database@AWS. The Oracle Multicloud section of this document lists exceptions in physical infrastructure control, remote management access, and network configuration.

[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

DISCLAIMER

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

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

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

TABLE OF CONTENTS

LIST OF IMAGES

LIST OF TABLES

INTRODUCTION

Exadata Database Service provides Exadata as a managed cloud service in OCI and partner data centers. You get all Exadata features, OCI orchestration, and Oracle support. This paper describes the security controls built into service. These controls follow industry best practices to protect customer data and mission-critical workloads. If your current security standards differ, this paper suggests alternative controls so you can update or adjust your policies.

ROLES AND RESPONSIBILITIES

Exadata Database Service follows a shared responsibility model where you and Oracle each manage specific aspects of the system. Responsibilities are separated as follows:

Your services:

- Virtual machines (VM)
- Databases running within them

Oracle managed infrastructure:

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

Oracle managed cloud control plane:

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

You are responsible for securing, monitoring, and managing access to your VMs and databases. You manage authentication to your VMs and Oracle Databases using standard operating system and database tools.[3] Oracle controls and monitors access to Oracle-managed infrastructure components. Oracle staff are not authorized to access your VMs and databases, save certain support exceptions detailed in Exception Workflows - Oracle Access to VM. Detailed breakdowns of roles and responsibilities are provided in Table 1, Exadata Database on Dedicated Infrastructure Service Description,[4] and Exadata Database Service on Dedicated Infrastructure - Explanation of Cloud Operations Service (Doc ID 2875973.1).[5]

Table 1: Roles and Responsibilities for Exadata Database Service in OCI

WORK FUNCTION	ORACLE MANAGED INFRASTRUCTURE		YOUR SERVICES	
	Oracle Cloud Ops	Your Staff	Oracle Cloud Ops	Your Staff
Monitoring	Infrastructure, Control Plane, Hardware Faults, Availability, Capacity	Not Appliable	Infrastructure availability to support you monitoring your services	Monitoring of 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 your 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[6] documentation	Software updates of your Oracle Database, Grid Infrastructure, and VM operating system Testing
Backup & Restoration	Infrastructure and Control Plane backup and recovery, recreate VMs	Not Appliable	Provide running and customer accessible VM	Snapshots / Backup & Recovery of your data using Oracle native or 3rd party capability
Cloud Support	Response & Resolution of SR related to	Submit SRs via My Oracle Support (MOS)	Response & Resolution of SR	Submit SRs via My Oracle Support (MOS)

[3] https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/exaconnectingDB.htm
[4] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecscm/exa-service-desc.html
[5] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2875973.1
[6] https://docs.oracle.com/en-us/iaas/Content/Database/Concepts/examaintenance.htm

	infrastructure or subscription issues			

EXADATA DATABASE SERVICE ARCHITECTURE

Exadata Database Service is deployed on Exadata Database and Storage Servers in an OCI data center you choose. Physical Exadata Database and Storage Servers are dedicated to your services. Physical power and network infrastructure are shared. Your data is stored on Exadata Storage Servers and accessed through your VCNs and VLAN-isolated storage networks. You have root-level and SYS-level access to your virtual machines and databases. You can set security policies, which gives you the ability to comply with regulations, install agents, forward logs, and manage identities.

Figure 1 illustrates the network architecture for Exadata Database Service.[7] In the diagram:

- Blue indicates components you control
- Red indicates components dedicated to your services and controlled by Oracle
- Green indicates shared components controlled by Oracle

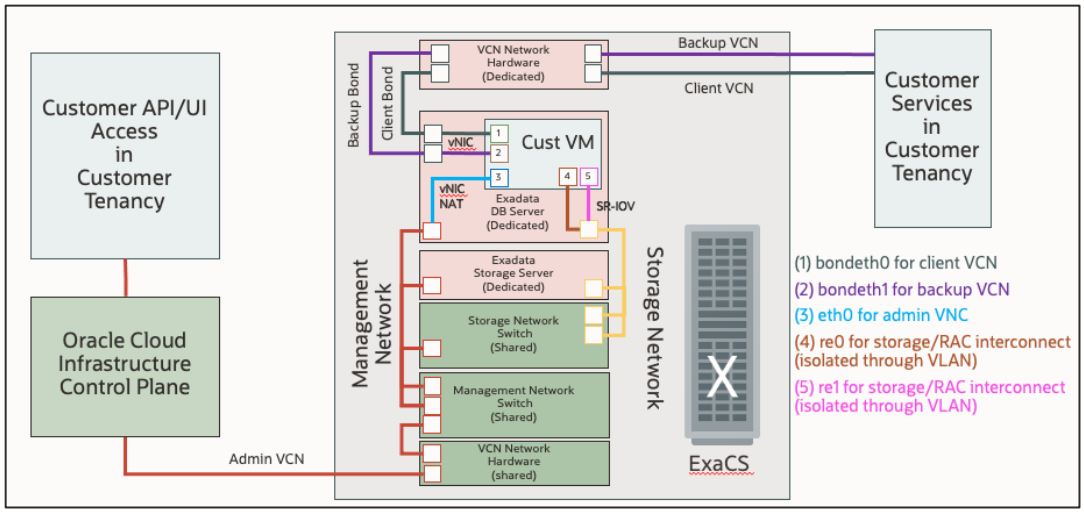

Figure 1: Network Architecture block diagram for Oracle Exadata Database Service on Dedicated Infrastructure

Dedicated Exadata Database and Storage Servers (red) are interconnected with an isolated 100GbE storage network (yellow). Communication between the components is implemented as RDMA over Converged Ethernet (RoCE). Different Exadata Database Service deployments are isolated with VLAN tags. Latency-sensitive network operations are serviced with high-priority network channels.

Exadata Database Servers connect to OCI networking using specialized hardware. vNICs connect the VMs to the client and backup networks. For resilience, physical connections are configured in an active-standby setup at the hypervisor. In the case of a link failure, Oracle will automatically restore connectivity. Short interruptions might occur during recovery.

The VM connects to the storage network using SR-IOV mapped interfaces (yellow). Each Exadata server connects to redundant storage switches in a high-availability (HA) configuration. Users and applications connect to databases through the client or backup network using standard Oracle protocols, such as Oracle Net over TCP port 1521. Shell Access to the VMs is through token-based `ssh` on TCP port 22, following standard Oracle Linux procedures.[8] Customers can access the Exadata Database Service VM Console[9] for exceptional maintenance and support conditions.

A subset of Oracle cloud automation functionality accesses the VM through NAT address on a vNIC on an isolated management network (/31 CIDR, blue). Software automation accesses the VM with temporary and just-in-time credentials, as follows:

---

[7] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecsid/
[8] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecscm/ecs-connect-to-service-instance.html#GUID-53DE1ED5-96D9-4F7F-B57F-4EF8D01FCDCB
[9] https://docs.oracle.com/en/learn/exadb-serial-console-connection/index.html

- Temporary and unique `ssh` key pair is generated by Oracle cloud automation for the specific management action.
- Public `ssh` key is added to the `~/.ssh/authorized_keys` files of the necessary service account in the VM, (e.g., `oracle`, `opc, grid`, or `root`) by the dbcs-agent on port 7070.[10]
- Private `ssh` key is secured in the infrastructure.
- Software automation uses the temporary `ssh` key to perform the required function.
- Temporary `ssh` key pair is deleted.

OCI Audit service records APIs that initiate cloud automation access to your VM. Oracle Linux audit logs in your VM record cloud automation access. You can forward these logs to compatible systems.[11]

CUSTOMIZATION AND THIRD-PARTY SOFTWARE

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

Oracle will not provide technical support for non-Oracle software. This includes installation, testing, certification, and error resolution. The supplier of the custom/third party software is responsible for any technical support for it. Oracle recommends that all non-Oracle software be certified by the vendor for use in an Oracle Linux and/or Exadata environment and thorough testing is performed in the target environment by you. Details for third party software support on Exadata Database Service are published on My Oracle Support document, "Installing Third Party Software on Exadata Components (Doc ID 1593827.1)."[12]

If a problem arises, Oracle Support will help diagnose it through the Oracle Service Request (SR) process. Depending on the issue, Oracle may recommend reverting the change. In some cases, particularly those involving third-party software, Oracle may request that the issue be reproduced without the third-party components, following its standard support policies.[13] Oracle support is included with your database service subscription at no additional charge.

Oracle recommends using the service as delivered. The design of Exadata Database Service incorporates oversight from Oracle Corporate Security Architecture[14] and Oracle Software Security Assurance.[15] Exadata Database Service security features are described in the Exadata Database Service Dedicated Security Guide.[16] Following the prescribed service design helps reduce the need for extensive testing, validation, and troubleshooting of changes.

SERVICE LIFECYCLE MANAGEMENT

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

- Web User Interface (web UI): for ad hoc actions via OCI Console
- Oracle Cloud Shell: a browser-based Linux shell within the OCI Console
- OCI Command Line Interface (OCI CLI): command line interface for scripting and automation
- OCI SDK/RESTAPI: for application integration
- OCI Terraform Provider[17] by Hashicorp[18]

If an OCI 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 VM
- Secured by mTLS

---

[10] https://docs.oracle.com/en-us/iaas/exadatacloud/doc/ecs-security-guide.html
[11] https://docs.oracle.com/en/learn/ocilogs-log-shipper/index.html
[12] https://support.oracle.com/knowledge/Oracle%20Cloud/1593827_1.html
[13] https://support.oracle.com/knowledge/Oracle%20Cloud/1593827_1.html
[14] https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html
[15] https://www.oracle.com/corporate/security-practices/assurance/
[16] https://docs.oracle.com/en-us/iaas/exadatacloud/doc/ecs-security-guide.html
[17] https://docs.oracle.com/en-us/iaas/Content/API/SDKDocs/terraform.htm
[18] https://registry.terraform.io/providers/hashicorp/oci/latest/docs

- Transported over the storage network

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 VM
- Transported over the management network

Infrastructure operations:

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

Quarterly Software Updates

Oracle Software Security Assurance Practices[19] and Oracle Software Security Assurance[20] standards control Oracle software development. Oracle implements segregation of duties[21] for development, test, quality assurance, and deployment of software. Reference the following documentation for details:

- Oracle Critical Patch Updates for Security Alerts and Bulletins[22]
- My Oracle Support Document 2333222.1 for Exadata Cloud Software Versions[23]
- Oracle Cloud Infrastructure Maintenance documentation[24] for infrastructure updates
- Exadata Cloud Infrastructure System documentation[25] for 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. You can schedule maintenance during a period that will have the least impact on your users. OCI interfaces provide full control and visibility over when quarterly maintenance will be applied and functionality to reschedule maintenance when required.[26]

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

Monthly Infrastructure Security Scanning and Updates

Oracle performs monthly infrastructure security scans and updates[27] to Exadata Database Service infrastructure in accordance with Oracle corporate security standards. These standards align with and support various industry standards, including PCI-DSS, and government security standards, including FedRAMP High and ISO/IEC 27001. Oracle performs updates to infrastructure online, with no reboot, and designed to have no impact to applications. Oracle applies monthly security updates to Storage Servers in a rolling manner, also designed to have no impact to applications. You may schedule monthly security maintenance at a specific time during the month, albeit in a single maintenance window. Oracle will publish

---

[19] https://www.oracle.com/corporate/security-practices/assurance/
[20] https://www.oracle.com/corporate/security-practices/assurance/
[21] https://www.oracle.com/corporate/security-practices/corporate/access-control.html
[22] https://www.oracle.com/security-alerts/
[23] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2333222.1
[24] https://docs.oracle.com/en-us/iaas/exadatacloud/exacs/exa-conf-oracle-man-infra.html#GUID-C4301E26-E809-438F-96D7-9C6BB02FEA7F
[25] https://docs.oracle.com/en-us/iaas/exadatacloud/exacs/ecs-patch-update.html
[26] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecscm/ecs-patch-update.html#GUID-37442222-8D97-49FD-8CB3-B08B0F539E09
[27] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecscm/exa-conf-oracle-man-infra.html#GUID-1C03DC65-3210-41F6-88FC-7AA7BE7870BB

a schedule for monthly maintenance at least one week prior to start of the maintenance period. You may reschedule if required.

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

Oracle Infrastructure Monitoring

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

- Infrastructure security and access control
- Exadata Compute, Storage, and Network infrastructure hardware and software[28] monitoring and maintenance
- Auto Service Request Qualified Engineered Systems Products[29] event monitoring and maintenance

Your Exadata Database Service automatically sends Infrastructure Monitoring Metrics (IMM) to monitoring systems in the OCI control plane. These are 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

Security Testing and Scanning of Your VM

You may test the security of Exadata Database Service in accordance with Oracle Cloud Testing Policies.[30] You may use OpenSCAP[31] to scan the VM for compliance. You may use third-party scanning tools to scan your VMs. Your use of third-party scanning tools should be designed and implemented for the Exadata Database Service software distribution and configuration. In some cases, arbitrary benchmarks may flag security issues on the Exadata Database Service VM that may not be a material risk for the Exadata Database Service. You may reference My Oracle Support Note, "Responses to common Exadata security scan findings (Doc ID 1405320.1)"[32] to learn more about how common benchmarks may be adjusted to work with Exadata. If the Exadata Database Service VM is modified to comply with a benchmark, you should these modifications to validate that they do not compromise Exadata Database Service functionality. Automated software updates, including operating system, Oracle Database, and Grid Infrastructure updates may revert your changes and should be tested prior to production deployment.

PREVENTIVE CONTROLS

Oracle designed the Exadata Database Service to protect your database data from unauthorized access. The Exadata Database Service separates access control duties between you and Oracle, as follows:

- You control access to your OCI tenancy, VMs, databases, and data
- Oracle controls access to Oracle-managed infrastructure components

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

Authentication and authorization controls

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

Data encryption controls

[28] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2875973.1
[29] https://docs.oracle.com/cd/E37710_01/doc.41/e37287/toc.htm
[30] https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm
[31] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-scap-sec.html.
[32] https://support.oracle.com/knowledge/Oracle%20Database%20Products/1405320_1.html

- Oracle Native Network Encryption or TLS/SSL for application to database network encryption[33]
- Transparent Database Encryption (TDE) for user tablespace[34] data encryption at rest

Network controls

- OCI VCNs and Security Lists to control layers 2 and 3 access to VMs[35]
- Zero-trust Packet Routing to control layers 2 and 3 access to VMs[36]
- Network access rules implemented in the VM operating system[37] and Oracle Database[38]
- Temporary Delegate Access Control networks and bastion servers to allow Delegate Access Control credentials to authenticate to the VM

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

Database Security Controls

Exadata Database Service can deploy all the Oracle Database security controls included in the Oracle Database software, compatible OCI services, and compatible key management systems, such as:

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

Database Authentication

You can configure Oracle Database authentication with Centrally Managed Users,[39] including password authentication, Kerberos authentication, [40] or public key infrastructure (PKI) authentication. With centrally managed users, customers can manage the authorization for Active Directory users to access Oracle Databases. Oracle Database allows multifactor authentication (MFA) configuration for native users in the form of either push notifications through Oracle Mobile Authenticator (OMA) or Cisco Duo, or certificate-based authentication.[41] You can implement MFA by existing external authentication methods for human users with OCI IAM, MS-EI, and RADIUS.

Oracle Native Network Encryption, TLS/SSL, and mTLS

---

[33] Exadata Database Service automation configures Oracle Native Network Encryption; Oracle strongly recommends that customers preserve this control
[34] Exadata Database Service automation configured Oracle Transparent Data Encryption (TDE); Oracle strongly recommends that customers preserve this control
[35] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecscm/ecs-network-setup.html#GUID-40900E3C-8730-46E7-8F4C-9301ED0CEFF6
[36] https://docs.oracle.com/en/cloud/paas/base-database/zpr/index.html#articletitle
[37] https://docs.oracle.com/en/operating-systems/oracle-linux/8/firewall/firewall-AboutPacketFilteringFirewalls.html
[38] https://docs.oracle.com/en/database/oracle/oracle-database/19/netag/configuring-oracle-connection-manager.html#GUID-AF8A511E-9AE6-4F4D-8E58-F28BC53F64E4
[39] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/integrating_mads_with_oracle_database.html#GUID-9739D541-FA9D-422A-95CA-799A4C6F488D
[40] https://support.oracle.com/knowledge/Oracle%20Cloud/2621025_1.html
[41] https://docs.oracle.com/en/database/oracle/oracle-database/23/dbseg/configuring-authentication.html#GUID-10E4F568-0FA3-4F82-99AA-14FB2947469C

Exadata Database Service encrypts data in flight from the client to the Oracle Database instance with Oracle Native Network Encryption (NNE). NNE is automatically configured for databases created by the Exadata Database Service automation. The Oracle Database instance is configured to request encrypted connections from applications,[42] and implement an encrypted connection for capable applications. If an application cannot support an encrypted connection, the Oracle Database instance will permit the application to connect without encryption. The service automation does not provide interfaces to configure TLS/SSL for Oracle Database connections. You can configure TLS/SSL and mTLS using operating system tools deployed in the VM.[43] Documentation for Oracle Native Network Encryption and TLS/SSL are published in the Security Guide for each Oracle Database version.[44]

Oracle Transparent Data Encryption

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

- PKCS#12 wallet
- OCI Vault
- Oracle Key Vault
- Azure Key Vault for Oracle Database@Azure
- Compatible third-party HSM

Oracle TDE is engineered to be highly performant. It automatically leverages special instructions in Intel CPUs (AES-NI) to accelerate cryptographic operations. In addition, TDE tablespace encryption works seamlessly with Exadata Hybrid Columnar Compression (EHCC) and Smart Scan technology. With TDE, sensitive user data remains encrypted throughout the database, whether it is in tablespace storage files, temporary or undo tablespaces, or other files such as redo logs. In addition, TDE can encrypt entire database backups. Data Pump and Oracle Recovery Manager (RMAN) both integrate with TDE encrypted data. Details for the TDE implementation on Exadata Database Service are shown in the Exadata Database Machine Cryptographic Services[45] documentation. For further information on Oracle TDE, consult the Advanced Security Guide for the Oracle Database version you are running. The Oracle TDE FAQ[46] provides answers to common Oracle TDE architecture and implementation questions.

Oracle TDE for Exadata Database Service with PKCS#12 Wallet

The TDE MEK is stored outside of the database, by default in a PKCS#12 compliant container called a 'wallet'. 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.

Oracle TDE for Exadata Database Service with OCI Vault

Exadata Database Service works with OCI Vault, letting you manage TDE keys outside of the VM for stronger security. With OCI Vault, you 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

---

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

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

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

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

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

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

Oracle TDE for Exadata Database Service with Oracle Key Vault

You can migrate your Exadata Database Service databases to Oracle Key Vault (OKV).[47] OKV provides continuous online key management to all TDE-enabled databases and encrypted GoldenGate trail files. It also provides the capability to ingest externally generated keys (BYOK). Instructions for using operating system methods to migrate TDE Master Keys to OKV are published in Managing Encryption Keys on External Devices product documentation[48] and Migration of File based TDE to OKV for Exadata Database Service Using Automation via REST (Doc ID 2924192.1).[49] You can use the OKV Persistent Master Encryption Key Cache[50] to enable databases to be operational if the OKV server is unavailable.

Oracle Transparent Data Encryption and Azure Key Vault

Oracle Database@Azure subscribers can use Azure Key Vault (AKV) Managed HSM, AKV Premium and AKV Standard for managing TDE MEKs.[51] This integration allows applications, Azure services, and databases to use a centralized key management solution for enhanced security and simplified key lifecycle management.

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

Oracle Database is compatible with PKCS#11 compatible key management devices.[52] 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)[53] for implementation and support details.

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

HSM vendors can self-certify their devices to provide root of trust to Oracle Key Vault. They should refer to “Vendor Instructions for Integrating an HSM as the Root of Trust for Oracle Key Vault” in the Oracle Key Vault Root of Trust HSM Configuration Guide.[54]

ASM-scoped Security

ASM-scoped Security[55] controls which Oracle Automatic Storage Management (Oracle ASM) clusters and Oracle Database clients can access specific grid disks on storage cells. Oracle Exadata System Software uses keys to identify clients and determine access rights to the grid disks. Exadata Storage Servers enforce access rights. Cloud automation software automatically configures ASM-scoped security and necessary keys to permit all the VMs in a VM cluster to access the Exadata storage (ASM disk groups) assigned to that VM cluster and to deny access to other VM clusters. See the Oracle

---

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

[48] https://docs.oracle.com/en-us/iaas/exadatacloud/doc/managing-encryption-keys-on-external-devices.html#GUID-627C83FC-D8A3-4BF2-80F6-70B11DED0C43

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

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

[51] https://docs.oracle.com/en-us/iaas/exadatacloud/doc/azure-key-vault-integration-for-oracle-database-at-azure.html

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

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

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

[55] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/configuring-data-security-exadata-storage-servers.html#GUID-A513D1D7-10BA-40D1-8F69-B5C86C5ECE59

Exadata Database Machine and Compliances with PCI-DSS V3.2[56] paper for an example of ASM-scoped security in the context of hosting in-scope and out-of-scope VM clusters on the same Exadata Database Machine.

Oracle Database Vault

Oracle Database Vault helps to both protect application data from database administrator access and address privacy and regulatory requirements. You can deploy controls to block database administrator access to application data and control sensitive operations inside the database using trusted path authorization. Oracle Database Vault helps to secure existing database environments transparently, eliminating costly and time-consuming application changes. Documentation for Oracle Database Vault is published in the Oracle Database Vault Administrator's Guide[57] for each database version.

Database Backup Encryption

All backups are encrypted with the same master key used for the Transparent Data Encryption wallet encryption.[58] The encryption key is not stored with the backup. When you use the Autonomous Recovery Service,[59] backups of encrypted tablespaces, and redo describing changes to these tablespaces, are encrypted.[60] The TDE-encrypted data blocks are encrypted on the database, Recovery Appliance storage, tape devices, and replicated appliances, and when transferred through any network connections.

Oracle Data Safe

Oracle Data Safe[61] helps you to:

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

The Data Safe FAQ[62] provides answers to commonly asked questions about Data Safe. The Oracle Data Safe Technical Architecture[63] provides more detail. There is no additional cost to use Data Safe so long as you do not exceed one million audit records per database in a month.

Oracle Database Security Assessment Tool

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

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

---

[56] https://www.oracle.com/assets/exadata-pci-dss-compliance-wp-3157442.pdf
[57] 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
[58] https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/exadatacloud/doc/ecs-security-guide.html
[59] https://docs.oracle.com/en-us/iaas/recovery-service/index.html
[60] 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
[61] https://docs.oracle.com/en-us/iaas/data-safe/index.html
[62] https://www.oracle.com/security/database-security/data-safe/faq/
[63] https://docs.oracle.com/en/solutions/oracle-data-safe-for-on-prem-database/index.html#GUID-07534FC6-3B10-48E5-BD49-C011D55D1070

DBSAT goes beyond simple configuration checking, examining user accounts, privilege and role grants, authorization control, separation of duties, fine-grained access control, data encryption and key management, auditing policies, and OS file permissions. DBSAT applies rules to quickly assess the current security status of a database and produce findings in all the areas above. For each finding, DBSAT recommends remediation activities that follow best practices to reduce or mitigate risk. By applying the comprehensive measurements and compensating controls described by DBSAT, you can help reduce data exposure risk throughout their enterprise. Oracle DBSAT is available for download from Oracle.[64]

VM Security Controls

The Exadata Database Service VM is deployed with a security-hardened operating system that includes the following:[65]

Minimal package installation and enabled services:

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

Secure configuration:

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

Secure access methods:

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

Auditing and logging:

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

Access to the VM is implemented via token-based `ssh`.[66] You use your OCI credentials to add your specified public keys to the `/home/oracle/opc/.ssh/authorized_keys` file. Your staff with access to the private keys associated with the installed public keys can gain access to the VM as the `opc` user via token-based `ssh`. Oracle cloud automation does not integrate with external key management systems; however, you can manage `ssh` keys using technology compatible with Oracle Linux-consult with applicable PAM providers for details. You can control add `ssh` key functionality with API Access Control[67] so that an OCI identity seeking to add an `ssh` key must get approval from a different OCI identity.

As of Exadata software version 22.1.4.0.0.221020, you can implement Microsoft Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) for authentication to your VMs. You can configure AD and LDAP using standard operating system tools. You can configure the Linux System Security Services Daemon (SSSD) to facilitate access to your VM using LDAP to provide identity services. Oracle Exadata System Software contains the Linux packages to support SSSD, which you may configure according to your specific requirements. The SSSD support is enabled in conjunction with an Exadata-specific security profile using the Linux `authselect` utility on Oracle Linux 8. Oracle Exadata System Software maintains the existing SSSD configuration details during system updates.[68]

---

[64] https://www.oracle.com/database/technologies/security/dbsat.html
[65] https://docs.oracle.com/en-us/iaas/exadatacloud/doc/ecs-security-guide.html#GUID-07B48561-96E7-435A-8C84-0861A02C1464
[66] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecscm/ecs-connecting-to-service-inst.html#GUID-53DE1ED5-96D9-4F7F-B57F-4EF8D01FCDCB
[67] https://docs.oracle.com/en-us/iaas/oracle-api-access-control/index.html
[68] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmso/linux-sssd-support.html

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

VM Default Users

Each Exadata Database Service 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.[69] 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[70] tool to manage core Exadata features.

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

Oracle recommends retaining the deployed usernames, userids, group names, and group ids. Changing the Oracle Home user (`oracle`) or Grid Infrastructure user (`grid`) after install is not supported and will cause service exceptions.[71]

VM Default Security Settings

The Exadata Database Service VM is deployed with security settings that align with industry standards and Oracle best practices.[72,73] 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
- `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.

---

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

[70] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmmn/using-dbmcli-utility1.html

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

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

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

- -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.

VM Default Processes and Certificates

Exadata Database Service 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).[74] The services and ports are detailed in Table 2. The table indicates the network interface, port number, process description, and certificate authority (CA) for each process. Oracle recommends that you configure security scanners to accept the Oracle CA and Oracle self-signed certificates for Oracle-managed services. These certificates and CAs are built into the service and managed by Oracle to secure the delivery of lifecycle management operations. Accepting them reduces the risk of certificate -related service issues and minimizes operational burden.

Table 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[75]	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[76] 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[77]	Oracle self-signed; customers may add customer-controlled certificates
		5000	Oracle Trace File Analyzer[78] Collector	Oracle self-signed

[74] https://docs.oracle.com/en-us/iaas/exadatacloud/doc/ecs-security-guide.html#GUID-3A150605-1DC9-401F-9201-C0E73ABE817E
[75] https://docs.oracle.com/en/operating-systems/oracle-linux/openssh/openssh-ConfiguringOpenSSHServer.html
[76] https://docs.oracle.com/en/database/oracle/oracle-database/19/netag/configuring-and-administering-oracle-net-listener.html
[77] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-secure-sockets-layer-authentication.html#GUID-6AD89576-526F-4D6B-A539-ADF4B840819F
[78] https://docs.oracle.com/en/database/oracle/oracle-database/19/atnms/managing-and-configuring-tfa.html

		7879	Jetty Management Server.[79] Application server engine that is used internally by Oracle Exadata System Software, in particular Management Server (MS).[80]	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[81,82] running on each cluster node communicates through these interfaces.	clib0/clre0	1525	Oracle TNS listener Oracle Clusterware running on each cluster node communicates through these interfaces.	N/A
		3260	Synology DSM iSCSI	N/A
		5054	Oracle Grid Interprocess Communication	N/A

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

		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[83] 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[84]	Oracle self-signed
		7070	dbcs-agent Cloud agent for handling database lifecycle operations[85]	Oracle self-signed
	stib1/stre1	7060	dbcs-admin	Oracle self-signed
		7070	dbcs-agent	Oracle self-signed
Control Plane server to domU	eth0	22	sshd	N/A
Loopback	lo	22	sshd	N/A
		2016	Oracle Grid Infrastructure	N/A

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

		6100	Oracle Notification Service (ONS),[86] 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[87]	Customer-controlled or Oracle signed

VM Console Access via OCI Control Plane

You access your VM console with a token-based `ssh` tunnel through the control plane to the hypervisor console of the VM.[88,89] Access is controlled in 3 steps:

1. Your 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. Your `ssh` credentials create an `ssh` connection from your device or OCI cloud shell to the VM console
3. You log into to the VM console using your username and password; typically, the `root` user

The cloud shell console connection is automatically terminated 24 hours after it is created. You must reauthenticate to OCI to reestablish the console connection. You can terminate the console connection at any time using the OCI console or API interfaces. You can control the VM console connection with API Access Control[90] so that an OCI identity seeking to enable VM console access must get approval from a different OCI identity.

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

Cloud Automation Access to VM

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

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

The VM provides the Oracle Linux packet filtering software[91] as an additional data protection control to block network to the VM. Blocking `ssh` access from the control plane will break the following service functionality:

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

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

Delegate Access Control

You can use Delegate Access Control[92] to subscribe your VMs to database maintenance and support services, and control and monitor access by service provider staff. You can subscribe to 4 types of Delegate Access Control services:

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

Delegate Access Control preventive controls include:

- Oracle staff access only after your approval of a specific work request
- Access is limited to approved components related for each work request
- Access is temporary, just-in-time, and automatically revoked after a set time
- You control when Oracle staff can access your services
- Software uses Oracle Linux `chroot` jails[93] to enforce of privilege limits

Delegate Access Control detective controls include:

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

Delegate Access Control responsive controls include:

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

---

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

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

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

Figure 2 shows the Delegate Access Control approval and access workflow. The Delegate Access Control demonstration video[94] provides more detail. Delegate Access Control uses the same delivery mechanics as Operator Access Control[95] and is included in the scope of the Operator Access Control PCI-DSS attestation of compliance (AoC).

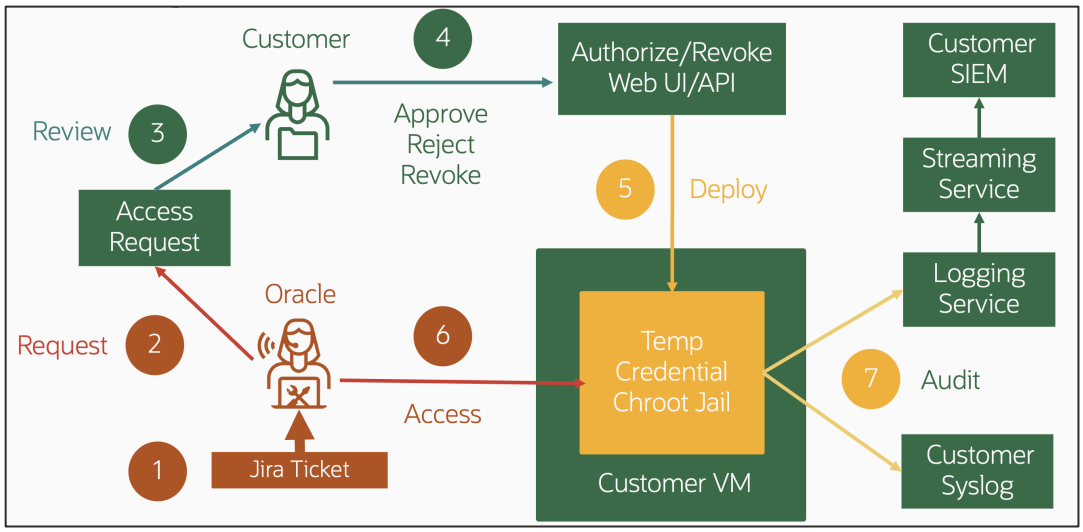

Figure 2: Delegate Access Control approval workflow

Network Security Controls

You can use OCI network security features with Exadata Database Service, including:

- Virtual Cloud Networks (VCN)[96]
- Network Security Lists[97]
- Zero-trust packet routing (ZPR)[98]
- VCN Flow Logs[99]

Network Security Groups and Security Lists are virtual firewall features that control traffic at the packet level. Ways to implement the security rules are provided in the product documentation. [100] Zero-trust Packet Routing 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. VCN Flow Logs show details about traffic that passes through a VCN.

Your network security controls must allow the Exadata Database Service network requirements.[101] The requirements include:

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

---

[94] https://www.youtube.com/watch?v=fwKtfp3aNuk
[95] https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/oracle-operator-access-control-tech-brief.pdf
[96] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/overview.htm
[97] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/securitylists.htm#Security_Lists
[98] https://www.oracle.com/security/cloud-security/zero-trust-packet-routing/
[99] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/vcn_flow_logs.htm
[100] https://docs.public.content.oci.oraclecloud.com/en-us/iaas/exadatacloud/doc/ecs-network-setup.html#GUID-660464D2-2DB3-408C-85E2-1438E6C4BF91
[101] https://docs.public.content.oci.oraclecloud.com/en-us/iaas/exadatacloud/doc/ecs-network-setup.html

Network Sources and API Access Control

OCI Network Sources[102] and API Access Control help you to control how OCI services, and API and Console functionality can be used with your services. Network sources controls where your services can be accessed from. API Access Control enforces separation of duties for privileged Exadata Database Service APIs. These controls are optional security enhancements and included in your service at no additional charge.

OCI Network Sources limits authentication to your tenancy resources to connections initiating from specific IP addresses, such as your proxy that allows egress from your corporate VPN. If you implement a site-to-site VPN or FastConnect from your data center to an OCI region, you can route OCI Console and API connections through an OCI Transit VCN.[103] This gives your on-premises network private access to Oracle services, so that your on-premises hosts can use their private IP addresses and the traffic does not go over the public internet.

API Access Control enforces a multi-identity approval workflow for privileged OCI Console and API functionality. Before a privileged API can be invoked, the user intending to invoke the API must raise an Access Request with their OCI identity, and a different OCI identity must approve the Access Request. Figure 3 shows the API Access Control approval workflow. Watch the API Access Control demonstration video[104] and see API Access Control at the Oracle Learning Center[105] for more details.

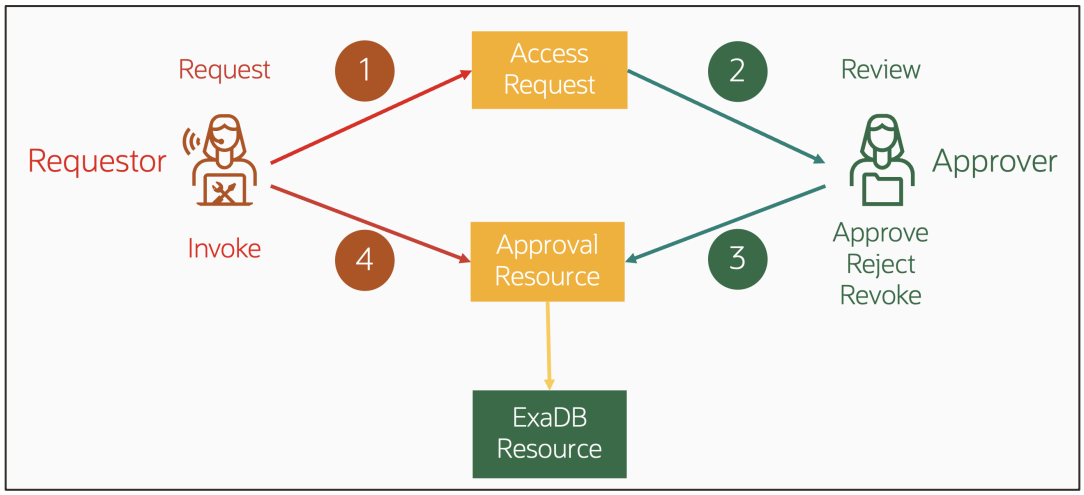

Figure 3: API Access Control approval workflow

Software Development and Delivery Security Controls

Exadata Database Service delivers the enterprise-class security features of Exadata Database Machine[106] as a cloud service. Software security for Exadata Database Service includes:

- Software development performed under Oracle Software Security Assurance[107] practices
- Security architecture performed under Oracle Corporate Security Architecture[108] practices
- Development and debug tools to inspect customer data are not installed on Exadata Database Service infrastructure

[102] https://docs.oracle.com/en-us/iaas/Content/Identity/Tasks/managingnetworksources.htm
[103] https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/transitroutingoracleservices.htm
[104] https://www.youtube.com/watch?v=-kzyH4LzP3c&feature=youtu.be
[105] https://docs.oracle.com/en/learn/exadb-cc-api-access-control/
[106] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/toc.htm
[107] https://www.oracle.com/corporate/security-practices/assurance/
[108] https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html

Oracle Access Controls for Infrastructure Components

Oracle exclusively manages infrastructure security and availability as outlined in the Oracle PaaS and IaaS documentation.[109] Oracle Corporate Security Practices[110] cover the management of security for Oracle internal operations and cloud services. These apply to all Oracle personnel, such as employees and contractors. These policies are aligned with the ISO/IEC 27002:2022(formerly known as ISO/IEC 17799:2005) and ISO/IEC 27001:2022 standards and guide all areas of security within Oracle. Oracle implements an automated HR joiner/mover/leaver processes whereby authorization to access infrastructure is consistent with updates to employee job code, training records, and employment status. Oracle further controls Oracle cloud operations access per Oracle Access Control Practices[111] with a least privilege, default deny approach where access is provided for:

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

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

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

Figure 4 shows how Oracle Cloud Operations (Cloud Ops) staff access infrastructure components to manage the Exadata Database Service infrastructure.

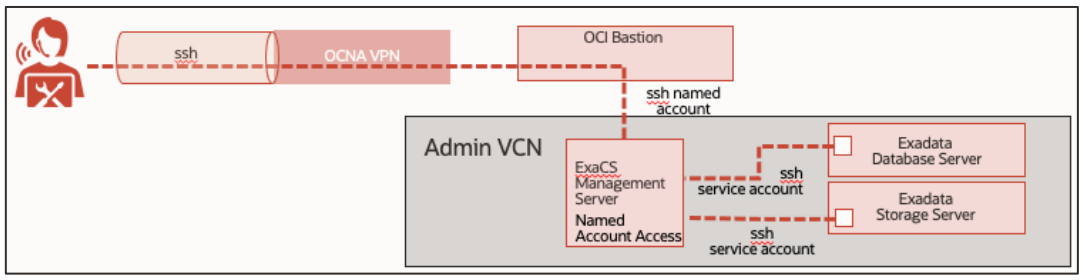

Figure 4: Cloud Operations Staff Access to Exadata Database Service Infrastructure Components

Oracle controls Oracle Cloud Ops staff access to Exadata Database Service infrastructure, as follows:

OCNA access:

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

Bastion server access:

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

Management server access:

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

[109] https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf
[110] https://www.oracle.com/corporate/security-practices/corporate/
[111] https://www.oracle.com/corporate/security-practices/corporate/access-control.html

Exadata Database Service infrastructure access:

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

DETECTIVE CONTROLS

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

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

Oracle is not authorized to access your audit logs. You may request access to applicable Oracle infrastructure audit log information from Oracle via the Oracle service request (SR) process. Your audit rights are described in the Oracle Data Processing Agreement (DPA).[112]

Customer Service Audit Logging

Exadata Database Service provides four capabilities for auditing and logging:

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

You can send these audit logs to compatible technology. See Ingest Oracle Cloud Infrastructure Logs into Third-Party SIEM Platforms using Log Shippers[113] for implementation details.

OCI Audit Logging

OCI Audit[114] automatically records calls to all supported Oracle Cloud Infrastructure public application programming interface (API) endpoints as log events. All services support logging by Audit. Object Storage service supports logging for bucket-related events, but not for object-related events. Log events recorded by Audit include API calls made by the Oracle Cloud Infrastructure Console, Command Line Interface (CLI), Software Development Kits (SDK), your own custom clients, and other Oracle Cloud Infrastructure services. Information in the logs includes:

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

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

Database Audit Logging

Exadata Database Service provides comprehensive audit logging for the database with Oracle Database Unified Audit.[115] You can send these audit records to your syslog server[116] or compatible security information event management (SIEM) system.

---

[112] https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf
[113] https://docs.oracle.com/en/learn/ocilogs-log-shipper/index.html#introduction
[114] https://docs.oracle.com/en-us/iaas/Content/Audit/Concepts/auditoverview.htm
[115] https://www.oracle.com/database/technologies/security/db-auditing.html
[116] https://support.oracle.com/knowledge/Oracle Cloud/2652319_1.html

See the OCI solution playbook for streaming to SIEM[117] for an example. Oracle publishes documentation for configuring, managing, and monitoring of Oracle Database audit logs in the Oracle Database Security Guide[118] for each database version.

VM Audit Logging

The Oracle Linux audit log service (`auditd`)[119] records actions executed by operating system credentials. You can configure `auditd` per your standards, including sending the Oracle Linux audit log to a remote log server.[120] See the Oracle Linux Security Guide[121] for more detail. You can integrate the Oracle Linux audit logs into the OCI Log Analytics service.[122]

File Integrity Monitoring

Exadata Database Service includes the Oracle Linux Advanced Intrusion Detection Environment (AIDE)[123,124] to check file and directory integrity. AIDE is a small, yet powerful, intrusion detection tool automatically installed with the Linux Operating System, that uses predefined rules to check file and directory integrity. It is meant to protect the system internally, by providing a layer of protection against viruses, rootkits, malware, and detection of unauthorized activities. It is an independent static binary for simplified client/server monitoring configurations. AIDE runs on demand, and the time to report changes is dependent on the system checks (usually at least once a day). You can change the configuration in `/etc/aide.conf`. The configuration file is controls which files and directories are monitored by AIDE, and how logging and output are handled.

Oracle Infrastructure Audit Logging

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

ILOM:

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

Physical Exadata Database Server:

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

Exadata Storage Server:

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

Storage Network Switch:

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

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

ILOM:

- syslog

---

[117] https://docs.oracle.com/en/solutions/oci-aggregate-logs-siem/#GUID-601E052A-8A8E-466B-A8A8-2BBBD3B80B6D

[118] 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

[119] https://docs.oracle.com/en/learn/ol-auditd/

[120] https://support.oracle.com/knowledge/Oracle%20Cloud/2652319_1.html

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

[122] https://blogs.oracle.com/ateam/post/harnessing-the-power-of-linux-logs-in-oci-logging-analytics-om

[123] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmso/aide.html

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

- 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.[125] Infrastructure audit logs are accessible by Oracle security staff.

RESPONSIVE CONTROLS

You and Oracle work together to secure and monitor access to Exadata Database Service components. If either party detects an unauthorized action, that party can take responsive action immediately, prior to notifying the other party. If you detect an unauthorized action, you should notify Oracle of the action and response using the Oracle Service Request (SR) process. You may take any responsive action on any services you control. This includes terminating network connections into the VM and Oracle Database. Oracle's responsive controls include terminating connections at Bastion Servers in OCI and revoking access to Oracle-managed Exadata Database Service infrastructure resources.

Oracle Incident Response

Oracle Incident Response[126] describes how Oracle responds to security incidents, shown below.

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

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

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

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

15-Minute Service Response Time for Critical Issues

Oracle Cloud Hosting and Delivery Policies[127] describes Oracle's 15-minute service response time for critical issues, including security incidents, shown below:

---

[125] https://www.oracle.com/contracts/docs/ocloud_hosting_delivery_policies_3089853.pdf
[126] https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html
[127] https://www.oracle.com/contracts/docs/ocloud_hosting_delivery_policies_3089853.pdf

"5.3.1 Severity 1 (Critical Outage)

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

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

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

COMMERCIAL REFERENCE INFORMATION

This section summarizes Oracle public commercial content related to common security questions for Exadata Database Service. Reference the Oracle Trust Center[128] for an index to Oracle's security, compliance, privacy, and commercial contract documents.

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[129] for relevant detail about a specific standard for Exadata Database Service. 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 your OCI Cloud Console.[130]

The frameworks and standards that the Exadata Database Service in OCI is delivered to includes:

- 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

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

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

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

- UK Cyber Essentials
- UK Security and Data Protection Toolkit

Oracle Corporate Security Policies

Oracle Corporate Security Practices[131] help to protect the confidentiality, integrity, and availability of Oracle and customer data. These practices cover the management of security for Oracle's internal operations and cloud services, and apply to all Oracle personnel, such as employees and contractors. These policies are aligned with the ISO/IEC 27002:2022 (formerly known as ISO/IEC 17799:2005) and ISO/IEC 27001:2022 standards and guide all areas of security within Oracle. These practices include:

- Objectives[132]
- Human resources security[133]
- Access control[134]
- Network communications security[135]
- Data security[136]
- Laptop and mobile device security[137]
- Physical and environmental security[138]
- Supply Chain Security and Assurance[139]

Vulnerability Disclosure

As a matter of policy, Oracle will not provide additional information about the specifics of vulnerabilities beyond what is provided in the Critical Patch Update, Security Alert notification, pre-installation notes, readme files, and FAQs.[140] Oracle provides all customers with the same information to protect all customers equally. Oracle will not provide advance notification or "insider information" on Critical Patch Update or Security Alerts to individual customers. Oracle does not develop or distribute active exploit code (or "proof of concept code") for vulnerabilities in Oracle products.

The Oracle Critical Updates, Security Alerts, and Bulletins[141] 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 Exadata Database Service, 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[142] describes how Oracle controls, protects, and processes data, such as:

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

---

[131] https://www.oracle.com/corporate/security-practices/corporate/
[132] https://www.oracle.com/corporate/security-practices/corporate/objectives.html
[133] https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
[134] https://www.oracle.com/corporate/security-practices/corporate/access-control.html
[135] https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html
[136] https://www.oracle.com/corporate/security-practices/corporate/data-protection/
[137] https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html
[138] https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
[139] https://www.oracle.com/corporate/security-practices/corporate/supply-chain/
[140] https://www.oracle.com/corporate/security-practices/assurance/vulnerability/disclosure.html
[141] https://www.oracle.com/security-alerts/#CVEOtherDocs
[142] https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf

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

Oracle Cloud Services Agreement

The Oracle Cloud Services Agreement[143] provides information about how your data is processed in Oracle Cloud Services, such as:

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

Important Cloud Services Agreement information is shown below.

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

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

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

Oracle Management of Security Event Logs

Oracle Communications and Operations Management[144] describes how Oracle controls and manages security log information related to Oracle services, shown below:

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

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

Consensus Assessment Initiative Questionnaire (CAIQ) Related to Security Logs

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

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

Oracle Consensus Assessment Initiative Questionnaire (CAIQ)[145] provides detail about how Oracle manages security logs, shown below:

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

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

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

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

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

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

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

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

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

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

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

One-Year Minimum Security Log Retention

The Oracle Cloud Hosting and Delivery Policies[146] publication describes Oracle security log processing and retention, shown below:

"1.14 Security Logs

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

99.95% Monthly Uptime Service Level Agreement (SLA)

The Oracle PaaS and IaaS Public Cloud Services Pillar Document[147] describes Oracle service credit remediation in cases where Oracle services are not delivered to 99.95% uptime, shown below:

---

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

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

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

"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[148] describes the access period after service termination whereby you can retrieve your data from the service, shown below:

"6.1 Termination of Oracle Cloud Services

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

Exception Workflows - Oracle Access to VM

Exadata Database Service support includes exception cases where a failure in the VM requires Oracle staff to access your VM to resolve the issue. The process and technical controls that govern how Oracle staff can access your VM depend on the following:

- Is the VM controlled by Delegate Access Control?
- Did the service exception occur before you could access the VM?
- Did the service exception occur after you could access into the VM?

The processes and technology controls for these cases are described in the following sections.

VM is Controlled by Delegate Access Control

If you have implemented Delegate Access Control[149] and subscribed to Oracle Cloud Customer Support and Oracle Cloud Operation, then Oracle Database cloud support and Oracle cloud operations support staff will issue a Delegate Access Control Access Request to you. After your approval, the Oracle support staff will access the VM using a unique, temporary, just-in-time credential deployed for least-privileged access implemented with Linux chroot jails to do the work. The Oracle Linux audit service will provide command/keystroke logs to you via OCI Logging service. You can send the Oracle Linux audit logs to a syslog server.

Service Exception Before You Could Access the VM

If your service has an exception before you could access the service, you can authorize Oracle staff to access your 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:

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

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

- As per the security policy associated with Exadata Database Service, Oracle personnel are prohibited to access customer domU[150] without customer's explicit permission. For Oracle to comply with this policy, Oracle staff must - get customer permission to access domU 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 you respond "yes" in the SR, then Oracle will temporarily adjust process and security controls to permit Oracle staff to access the VM. Oracle staff access to the VM will be authorized until the SR is closed or you direct Oracle to cease access in the SR.

Service Exception After Customer Accessed the VM

If your service has an exception after you could access the service, you can authorize Oracle staff to access your VM 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

If you are willing to permit Oracle Cloud Ops to access the VM without direct supervision, then you open a Service Request (SR) with the following language:

- SR Title:
  - SR granting Oracle explicit permission to access a Guest VM of Exadata Database Service 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 your security team has authorized Oracle to have access to your 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 you require Oracle to offer a shared screen to permit direct supervision of the Oracle cloud ops access, you open a Service Request (SR) with the following language:

- SR Title:
  - SR granting Oracle explicit permission to access a Guest VM of Exadata Database Service 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 your security team has authorized Oracle to have access to your 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 you create the new SR and Oracle receives the new SR, then Oracle will temporarily adjust process and security controls to permit Oracle staff to access the VM. Oracle staff access to the VM will be authorized until the SR is closed or you direct Oracle to cease access in the SR.

---

[150] domU is an Oracle term for the VM deployed in the Exadata Database Service. This term is required as part of the process controls that govern Oracle staff access to the VM in the Exadata Database Service.

SERVICE TERMINATION AND DATA DESTRUCTION

You can terminate your Exadata Database Service.[151] Oracle Exadata System Software includes the Secure Eraser utility,[152] which securely erases data on hard drives, flash devices, persistent memory, and internal USBs. It also resets ILOM to factory settings. Secure Eraser sanitizes all content, not only user data (Oracle Database data stored in the service), but also operating system, Oracle Exadata System Software, and user configurations. The Exadata Secure Eraser automatically detects the hardware capabilities of each storage device and selects the best erasure method supported. Cryptographic erasure is used whenever possible to provide better security and faster speed. The cryptographic erasure method used by Secure Eraser is designed to comply with the NIST SP-800-88r1 standard.[153] You can obtain secure erase certifications from Oracle by opening a My Oracle Support (MOS) Service Request (SR). Hardware used for ExaDB-D services implements cryptographic erase.

Oracle may move ExaDB-D infrastructure hardware between Oracle data centers. Prior to moving the hardware, Oracle will perform an Exadata Secure Erase on the infrastructure components to prevent your data from leaving an Oracle data center. Oracle will destroy all media that bore your data at hardware end-of-life.

STORAGE MEDIA HARDWARE HANDLING AND DESTRUCTION

Oracle Information and Assets Classification[154] practices apply to the storage media in your ExaDB-D service. Oracle performs storage media hardware maintenance and destruction is designed to comply with PCI DSS, ISO 27001, and CSA STAR. Relevant controls include:

ISO 27001 controls:

- *A.8.3.2 – Disposal of media: requires that media be disposed of securely when no longer required, using formal procedures.*
- *A.8.3.3 – Physical media transfer: requires traceability and protection of media during transport.*
- *A.11.2.7 – Secure disposal or re-use of equipment: equipment (including disks) must be verified to ensure all sensitive data is removed prior to reuse or destruction.*

PCI DSS control *9.4.7 Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following:*

- *The electronic media is destroyed.*
- *The cardholder data is rendered unrecoverable so that it cannot be reconstructed.*
- *9.4.7.a Examine the media destruction policy to verify that procedures are defined to destroy electronic media when no longer needed for business or legal reasons in accordance with all elements specified in this requirement.*
- *9.4.7.b Observe the media destruction process and interview responsible personnel to verify that electronic media with cardholder data is destroyed via one of the methods specified in this requirement*.

CSA STAR controls:

- *DCS-01.1, Are policies and procedures for the secure disposal of equipment used outside the organization's premises established, documented, approved, communicated, enforced, and maintained?*
- *DCS-01.2, Is a data destruction procedure applied that renders information recovery information impossible if equipment is not physically destroyed?*

You may download ISO 27001 and PCI DSS compliance documents from your OCI tenancy: Identity and Security->Compliance. Oracle's public web pages host the Oracle CAIQ for CSA STAR.[155]

You will be notified of storage media hardware physical access and replacement for your service by the following measures:

---

[151] https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/examanagingDBsystem.htm
[152] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/exadata-secure-erase.html#GUID-6C9FD30C-FF88-4ABA-9249-93E183784B0D
[153] https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization
[154] https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification/#data-management
[155] https://www.oracle.com/a/ocom/docs/oci-corporate-caiq.pdf

- Oracle will issue an ExaDB-D customer notification (CN) to your staff subscribed to CNs.
- Your Oracle ASM Alert Log will indicate storage media offline/online status changes and ASM disk lifecycle events.
- Your Oracle ASM Audit Log will indicate ASM disk lifecycle events, including dropping and adding ASM disks.
- Your Oracle Linux operating system logs will indicate changes in storage device (ASM disks) status.

Oracle classifies ExaDB-D disk and flash media as sensitive assets that require strict handling and destruction procedures. The following requirements apply:

- Access Control: A two-person verification process is required to access these parts.
- Onsite Handling: Parts must not leave the data center under any circumstances.
- Destruction: Parts must be destroyed within the data center premises using Oracle-approved destruction methods (e.g., shredding, degaussing).
- Documentation: The destruction process and verification must be documented, with records retained for compliance and audit purposes.

ORACLE MULTICLOUD

Oracle Multicloud[156] runs Oracle Database workloads in Azure, Google Cloud, and AWS data centers. The Oracle Multicloud database service benefits from the simplicity, security, and low latency of a single operating environment within the cloud provider network. All Exadata hardware for Oracle Multicloud is physically located in the cloud provider data centers and connected to the cloud provider services with cloud provider networks. Oracle manages the infrastructure through Oracle-controlled networks. These networks integrate the Multicloud infrastructure with the OCI management networks.

Roles and Responsibilities for Oracle Multicloud

Table 3 describes the roles and responsibilities for Oracle, cloud services provider, and your 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	Your Responsibility
Monitoring	Infrastructure, Control Plane, Hardware Faults, Availability, Capacity	Infrastructure availability to support customer monitoring of customer service Provide Oracle hardware service technician access to CSP data center Provide Oracle hardware service technician escort to Oracle hardware cages	Monitoring of operating systems, databases, and applications
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 your applications
Patch Management	Proactive patching of Hardware, IaaS/PaaS control stack, Staging of available patches (e.g., Oracle DB patch set)		Patching of you tenant instances

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

Work Function	Oracle Managed Infrastructure Responsibility	Cloud Services Provider Managed Infrastructure Responsibility	Your Responsibility
Backup & Restoration	Infrastructure and Control Plane Backup and recovery	Onsite Diagnostic Assistance (e.g., network troubleshooting, power, cooling	Snapshots/Backup & Recovery of your resources and data using Oracle native backups or 3rd party solutions.
Cloud Support	Response and Resolution	Response & Resolution	Submit SRs via Support Portal

Oracle Multicloud Architecture

Figure 5 shows the Oracle Multicloud architecture. This architecture provides you with all the functionality of the Exadata Database Service in OCI plus additional functionality to deliver the service in your cloud service provider's data center. This functionality includes:

- OCI Child Site: cages in the CSP data center containing the Exadata Database Service equipment
- Private connectivity: network integration connecting your application networks with your Exadata Database Service networks
- OCI-Controlled Network: network integration connecting the Child Site to the OCI control plane
- Cloud Console and API-Driven Lifecycle Management Controls: to help you secure and operate your service
- Additional OCI services: to help you optimize your security posture and operations

The following sections describe the security posture of these components and OCI services you can use to help you secure and monitor your implementation.

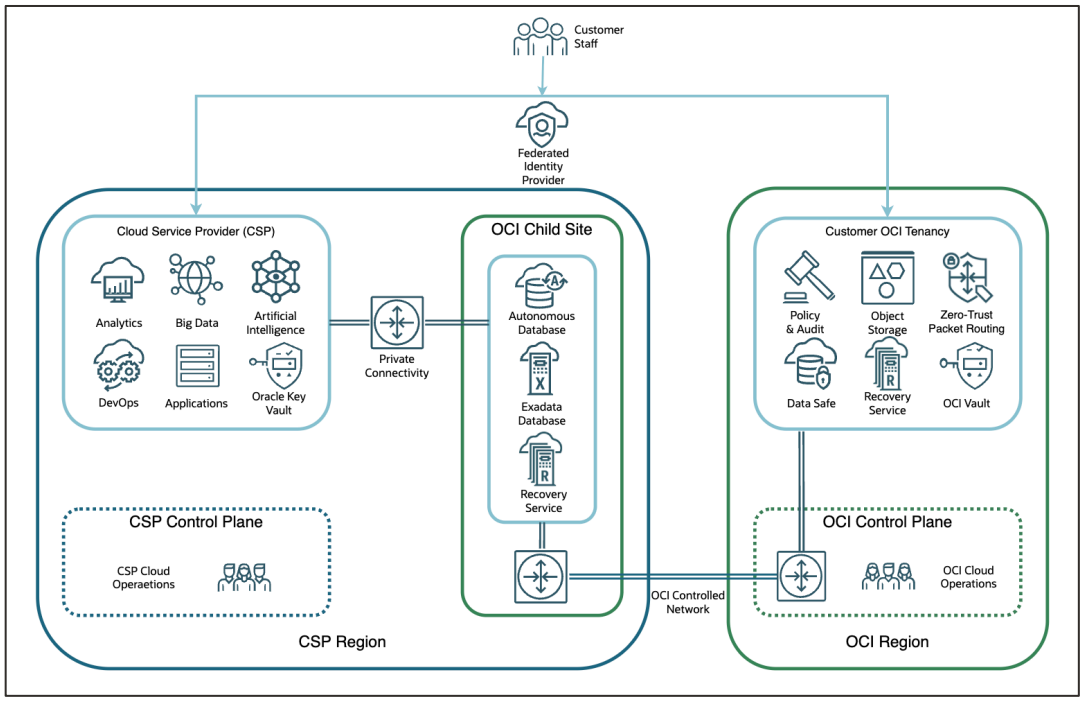

Figure 5: Multicloud Architecture

OCI Child Site

The Oracle Database services are deployed in an OCI Child Site in the CSP data center. The Multicloud racks contain all the components of a standard Exadata Database Service in OCI. Physical control duties are separated as follows:

- CSP controls access to the CSP building
- Oracle controls access to the Oracle cages that secure the hardware inside the Child Site

Oracle Global Physical Security Controls[157] apply to the Oracle cages in the Child Site. Logical security for the Child Site follows the standards of the Exadata Database Service in OCI data centers. Check with your CSP to learn more about their physical security controls applicable to Multicloud.

Private Connectivity

Your CSP credentials deploy the private connectivity between the CSP network and Exadata Database Service network. Maintenance and support access for the networking hardware is separated between CSP and Oracle staff such that:

- CSP service-principals access CSP components in response to your CSP APIs
- OCI service-principals access Exadata Database Service components in response to your CSP and OCI APIs
- CSP cloud operations staff use their credentials to access CSP equipment
- Oracle cloud operations staff use their credentials to access Oracle equipment

The Multicloud database cluster is deployed in a subnet within the CSP network. Automation creates a corresponding OCI virtual cloud network (VCN) with a matching subnet and IP CIDR range to the CSP network. The cluster runs in the OCI subnet using VNICs assigned private IPs. These private IPs are also reserved in the CSP subnet. Direct CSP to OCI connectivity in the CSP datacenter maps each private IP in the CSP network to its corresponding VNIC in the VCN. Figure 6 shows the implementation in Oracle Database@Azure. Oracle implements the service similarly with other CSPs.

When an application or user in CSP network connects to a database using the assigned private IP address, a virtual networking service routes the packets through the private connectivity to an 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 CSP data center. Figure 7, Figure 8, and Figure 9 show the networking for Multicloud in Azure, AWS, and Google Cloud.

For any CSP, you control access to your databases (TNS Listener port) and VMs (ssh port 22) from your CSP and Exadata Database Service networks. You can apply CSP network security controls to your CSP networks. You can apply OCI network security controls to your Exadata Database Service networks.

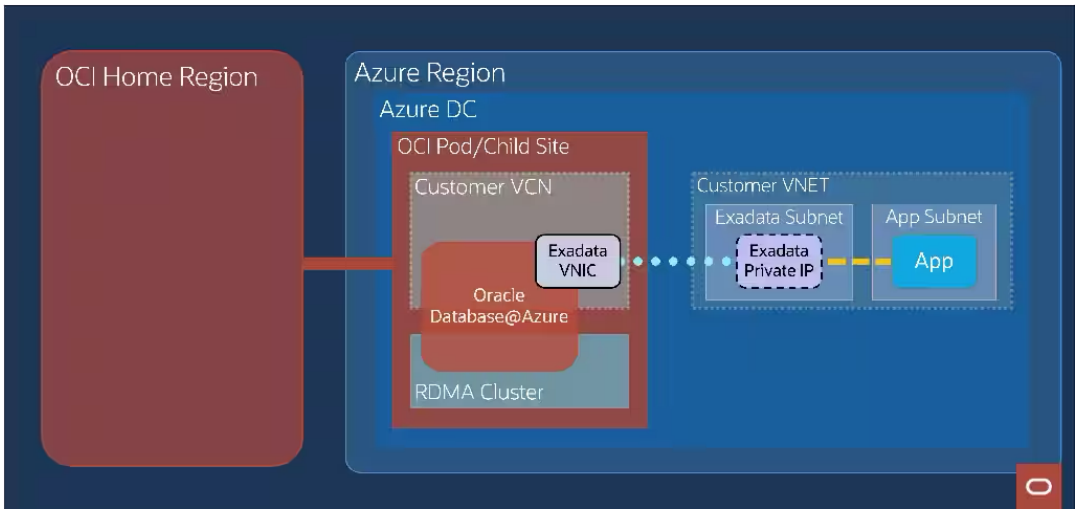

Figure 6: Oracle Database@Azure architecture diagram

[157] https://www.oracle.com/corporate/security-practices/corporate/governance/global-physical-security.html

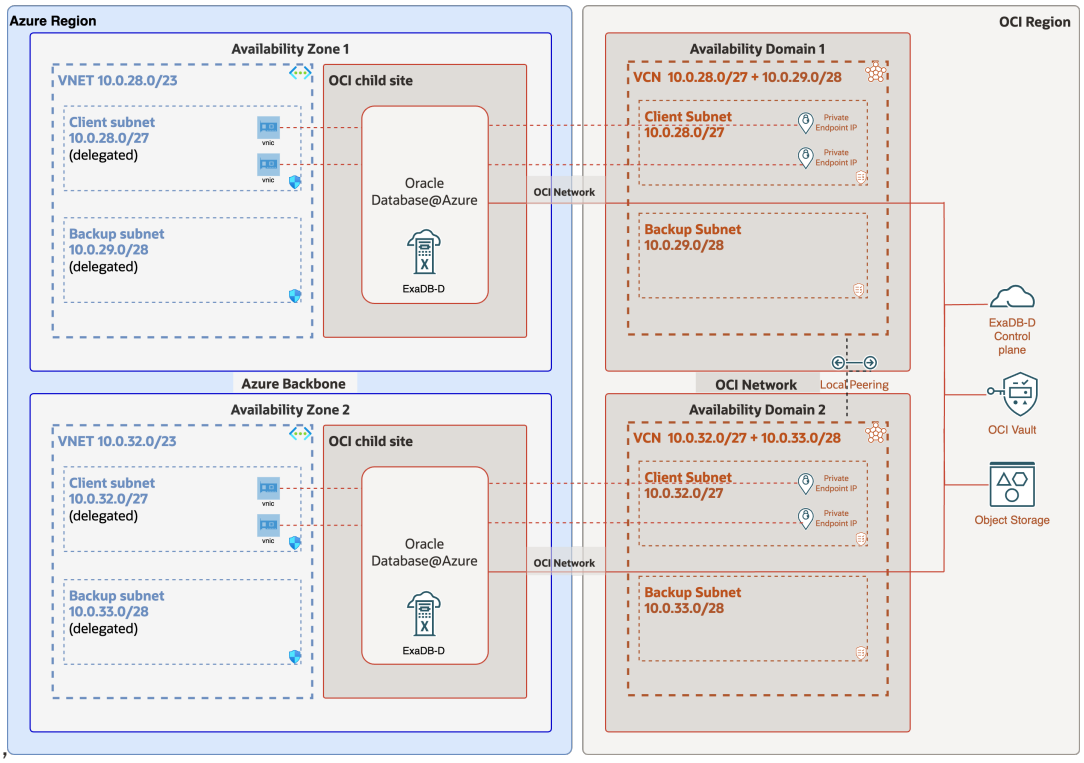

Figure 7: Oracle Database@Azure networking, multiple availability zones

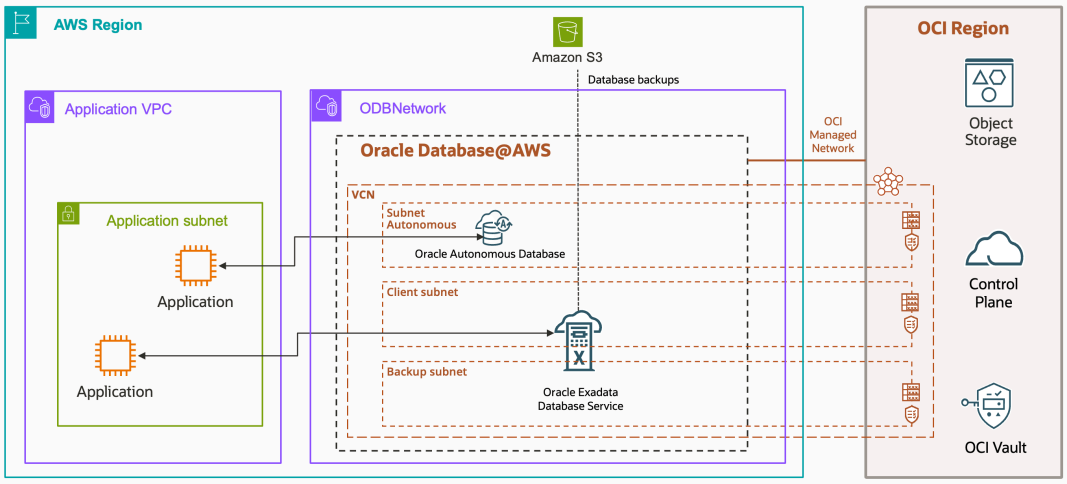

Figure 8: Oracle Database@AWS networking, single availability zone

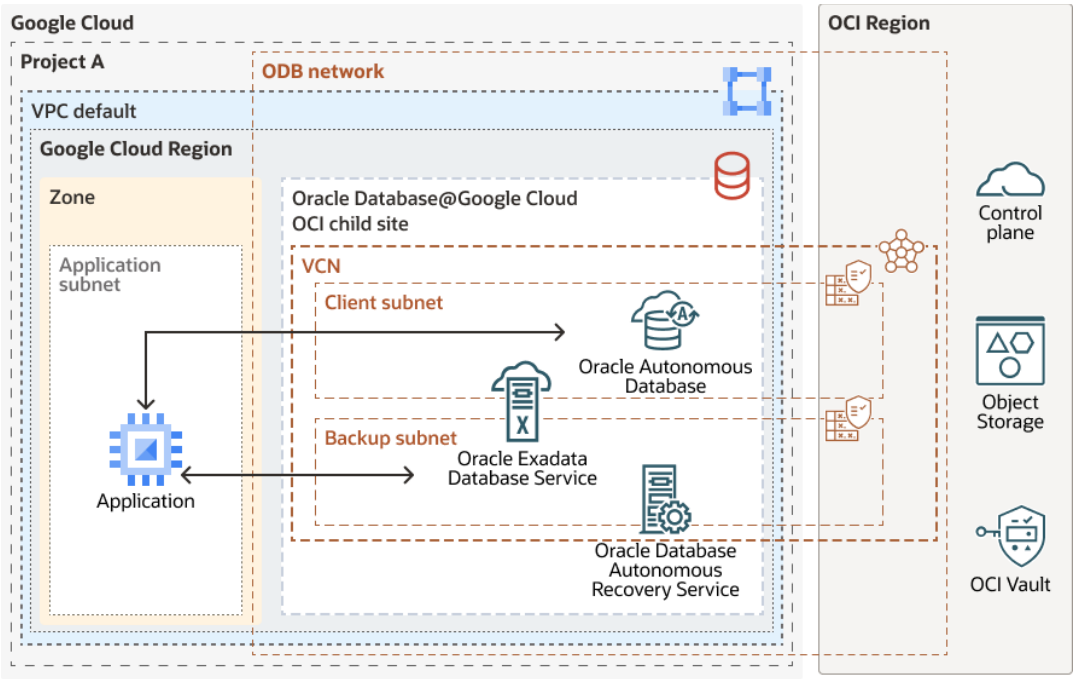

Figure 9: Oracle Database@Google Cloud networking, single availability zone

OCI Controlled Network

Oracle implements an OCI controlled private network from the Child Site to the Oracle control plane to deliver the service. This network provides access for:

- API and console driven lifecycle management
- Oracle support staff shell access to infrastructure components when necessary
- Access to optional OCI services to help you secure and run your business

When you make console or API calls Multicloud resources, the calls use federated identity for authentication with downstream OCI APIs. You use the CSP console to create Exadata infrastructure and VM clusters. The CSP console calls a Resource Manager, which routes API requests to a Resource Provider. The resource provider handles translation, authorization, authentication, and interacts with the Exadata Database control plane to create and manage database instances. Figure 10 shows the integration of Azure interfaces calling OCI APIs to manage the Oracle Database@Azure service. Oracle implements the service similarly for other CSPs.

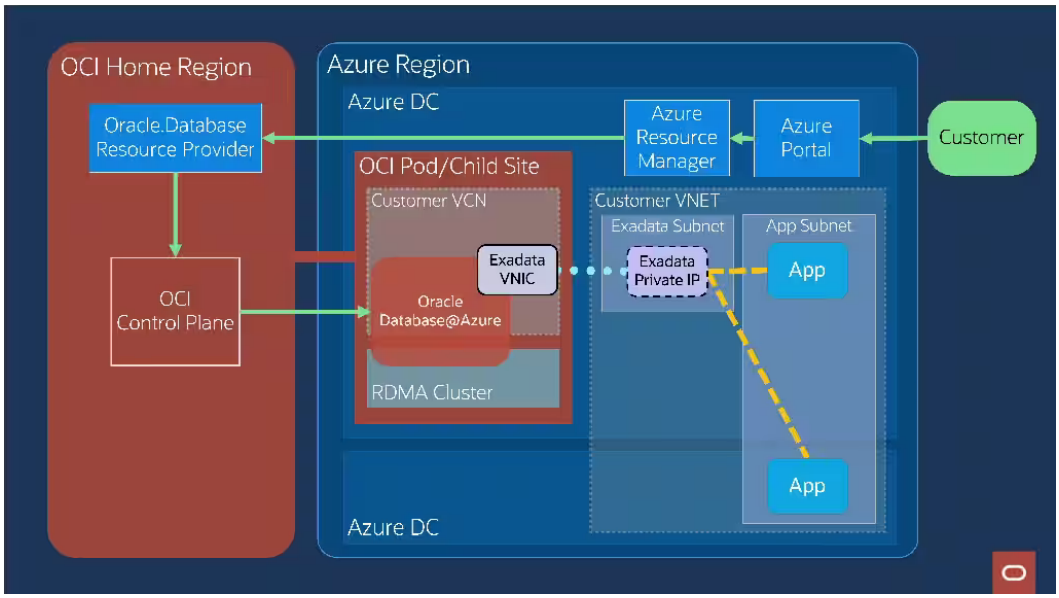

Figure 10: Integration of Multicloud Interfaces

The OCI Controlled network is a shared resource. Oracle exclusively secures, manages, and monitors the OCI controlled network. Access to your databases and VMs is independent of the OCI controlled network, and your databases and VMs should continue to function if there is a disruption to the OCI controlled network. A disruption to the OCI controlled network will cause a temporary disruption in API-driven service lifecycle management, Oracle monitoring, and Oracle access to resolve issues in the Child Site.

Cloud Console and API-Driven Lifecycle Management Controls

You control database service lifecycle using CSP and OCI interfaces. You can use any of the following to help control your staff access to your Multicloud Console and API interfaces:

- OCI Federated Identity Provider (IdP)[158] to authenticate your staff to your OCI tenancy
- OCI IAM Policy to control what your staff can do with OCI interfaces
- OCI Network sources to control what IP addresses can authenticate to your tenancy resources
- OCI Audit for monitoring and compliance
- API Access Control to enforce a separation of duties for privileged database service API functionality

You can also use Multicloud lifecycle management interfaces in your CSP tenancy to manage some aspects of the Multicloud service. Check with your provider for details.

OCI Security Services

You can use OCI services, including security services, with Multicloud. Figure 11 shows an example configuration for your reference. These services integrate with your VMs over the OCI controlled network and include:

- Oracle Data Safe[159] to help you 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[160] 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

158 https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/federation.htm
159 https://docs.oracle.com/en-us/iaas/data-safe/index.html
160 https://docs.oracle.com/en-us/iaas/recovery-service/index.html

- Zero Trust Packet Routing (ZPR)[161] to help prevent unauthorized access to data; using an intent-based policy language, security administrators can define specific access pathways for data; traffic that is not explicitly allowed by policy cannot travel the network
- Delegate Access Control[162] to subscribe to Oracle support services, such as Database Cloud Services Support, Cloud Operations Support, and Engineered Systems Deployment and Infrastructure Support (ESDIS)
- Operator Access Control[163] to control Oracle Autonomous Database Operations staff access to the Autonomous Database Service Dedicated VMs
- API Access Control[164] to enforce a multi-identity approval workflow for privileged OCI Console and API functionality

Your service requires access to OCI Object Storage[165] for low-cost database backups, database service software updates, and custom Oracle Home images. This is included with your Multicloud subscription. You may need separate contracts to enable specific OCI services. Consult with Oracle sales for details.

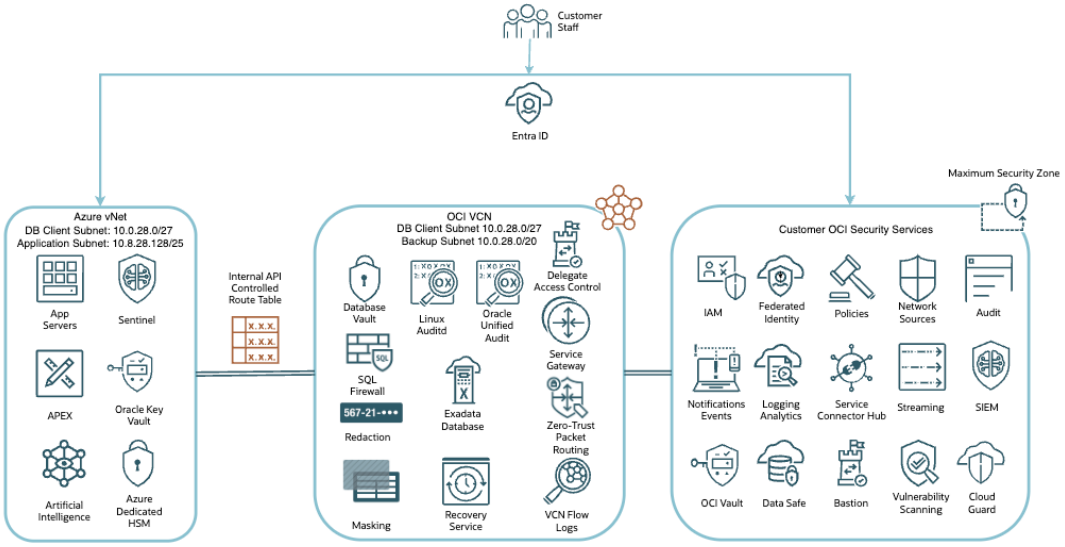

Figure 11: Example end-to-end security control diagram

SUMMARY

With Exadata Database Service, you control the security features throughout the VM. Oracle Database encryption encrypts data, and you retain control of the encryption keys. Oracle Database security features control authentication and access to data in the database, and you retain control of credentials and authorization. Oracle Linux authentication features control access to the VM, and you retain control of credentials and authorization.

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

Exadata Database Service delivers the benefit of a high-security on-premises deployment with the ease-of-use and economics of the cloud. Your staff 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 deployment model, you gain the security of an on-premises deployment with the benefits of cloud economics, agility, and scale.

---

[161] https://www.oracle.com/security/cloud-security/zero-trust-packet-routing/
[162] https://docs.oracle.com/en-us/iaas/delegate-access-control/doc/overview-of-delac.html
[163] https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/oracle-operator-access-control-tech-brief.pdf
[164] https://docs.oracle.com/en-us/iaas/oracle-api-access-control/doc/manage-oracle-api-access-control-resources-using-the-api.html
[165] https://docs.oracle.com/en/database/oracle/oracle-database/23/bkupr/bkupr_object_storage.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