ORACLE

Exadata Database Service on Dedicated Infrastructure Security Controls

A Technical Summary for Security Approvers and Developers

April 17, 2026 | Version 2.44

PURPOSE STATEMENT

This document provides an overview of features and enhancements included in Exadata Releases 25.2.5.0.0.251214 and 24.1.19.0.0.251214. It is intended solely to help you assess the business benefits of upgrading to Exadata release 25.2.5.0.0.251214 and 24.1.19.0.0.251214 and plan your IT projects.

This paper describes the security controls built into the Oracle Exadata Database Service on Dedicated Infrastructure (ExaDB-D) in Oracle Cloud Infrastructure (OCI), Oracle AI Database@Azure, Oracle AI Database@Google Cloud, and Oracle AI Database@AWS) to help you evaluate them for your use cases. These controls follow industry best practices to protect your data and mission-critical workloads. If your current security standards differ, this paper suggests alternative controls so you can update or adjust your policies.

DISCLAIMER

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

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

TABLE OF CONTENTS

LIST OF IMAGES

LIST OF TABLES

INTRODUCTION

ExaDB-D delivers Exadata as a managed cloud service in OCI and partner data centers. You get all Exadata features, OCI orchestration, and Oracle support. The service helps you secure your data in dedicated compute and storage servers in your chosen cloud provider's data center. You control:

- Networks that can access your database
- Credentials that can authenticate your VMs and databases

You have root-level and SYS-level access to your virtual machines and databasesYou can set security policies, install agents, forward logs, and manage identities to help you comply with regulations. Oracle operates the service control plane and Exadata Infrastructure under Oracle Corporate Security Practices. The service's security controls help to enforce the shared responsibility model so you and Oracle can work together to support, protect, and audit your Oracle AI Database. The service encrypts your application data in flight to your Oracle AI Database and your Oracle AI Database data at rest.

ROLES AND RESPONSIBILITIES

This section describes the shared responsibility model for ExaDB-D. ExaDB-D in OCI provides the basis of the responsibility model between you and Oracle. Additions for Multicloud show how the responsibility model evolves to include the cloud service provider (CSP).

ExaDB-D in OCI

ExaDB-D follows a shared responsibility model in which you and Oracle each manage specific aspects of the system:

Your responsibilities include securing, monitoring, and managing your:

- OCI tenancy
- Virtual machines (VMs)
- Databases running on those VMs

Oracle's responsibilities include securing, monitoring, and managing:

- Physical servers (Exadata Database and Storage Servers)
- Internal network switches
- Power Distribution Units (PDUs)
- The OCI region that delivers your service

Oracle monitors and responds to issues within its responsibility, including:

- Infrastructure security and access control
- Monitoring and maintenance of Exadata compute, storage, and network hardware and software
- Event monitoring and maintenance for Auto Service Request Qualified Engineered Systems Products

Oracle does not monitor components that fall outside its responsibility, such as your:

- Flash Cache usage
- VM security and access logs
- Oracle CRS, ASM, and Database
- Software running in your VM

Oracle staff are not authorized to access your VMs and databases, save certain support exceptions detailed in Exception Workflows for Oracle Access to Your VM.

Detailed breakdowns of roles and responsibilities are shown in Table 1 and ExaDB-D on Dedicated Infrastructure - Explanation of Cloud Operations Service (KB60969).

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

WORK FUNCTION	ORACLE MANAGED INFRASTRUCTURE		YOUR SERVICES	
	Oracle Cloud Operations	Your Staff	Oracle Cloud Operations	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 ExaDB-D on Dedicated Infrastructure documentation	Software updates of your Oracle AI 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 infrastructure or subscription issues	Submit SRs via My Oracle Support (MOS)	Response & Resolution of SR	Submit SRs via My Oracle Support (MOS)

Additions for Multicloud

Multicloud adds your CSP to the responsibility matrix. Your CSP provides physical data center control and Oracle controls access to the ExaDB-D equipment. Table 2 shows the roles and responsibilities for Oracle, your CSP, and your staff at supporting and operating Multicloud.

Table 2: Roles and responsibilities for Multicloud

Work Function	Oracle Responsibility	CSP 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

Work Function	Oracle Responsibility	CSP 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

ARCHITECTURE OVERVIEW

This section provides an architecture overview for ExaDB-D. ExaDB-D in OCI shows how Oracle delivers the ExaDB-D service in OCI data centers. Additions for Multicloud show how Oracle extends the architecture to deliver the service in your CSP data center.

ExaDB-D in OCI

Figure 1 shows the ExaDB-D architecture. The service is deployed on Exadata Database Servers and Storage Servers in a 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 client and backup Virtual Cloud Networks (VCNs). You can optionally connect to resources in your data centers using FastConnect or site-to-site VPN. An RDMA over Converged Ethernet (RoCE) network isolates your Exadata Storage and Real Application Cluster (RAC) traffic using VLAN technology.

Oracle Cloud Infrastructure supports identity federation with:

- Oracle Identity Cloud Service
- Microsoft Active Directory (via Active Directory Federation Services (AD FS))
- Microsoft Azure Active Directory
- Okta
- Security Assertion Markup Language (SAML) 2.0 protocol compatible services

You use HTTPS connections to OCI interfaces to manage your service, such as:

- Web User Interface (Web UI): for ad hoc actions via OCI Console
- OCI Cloud Shell (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/REST API: for application integration
- OCI Terraform Provider with documentation provided by HashiCorp

You control cloud automation functionality, such as creating databases and scaling OCPUs, with OCI Identity and Access Management (IAM). OCI Audit provides you with a record of these actions.

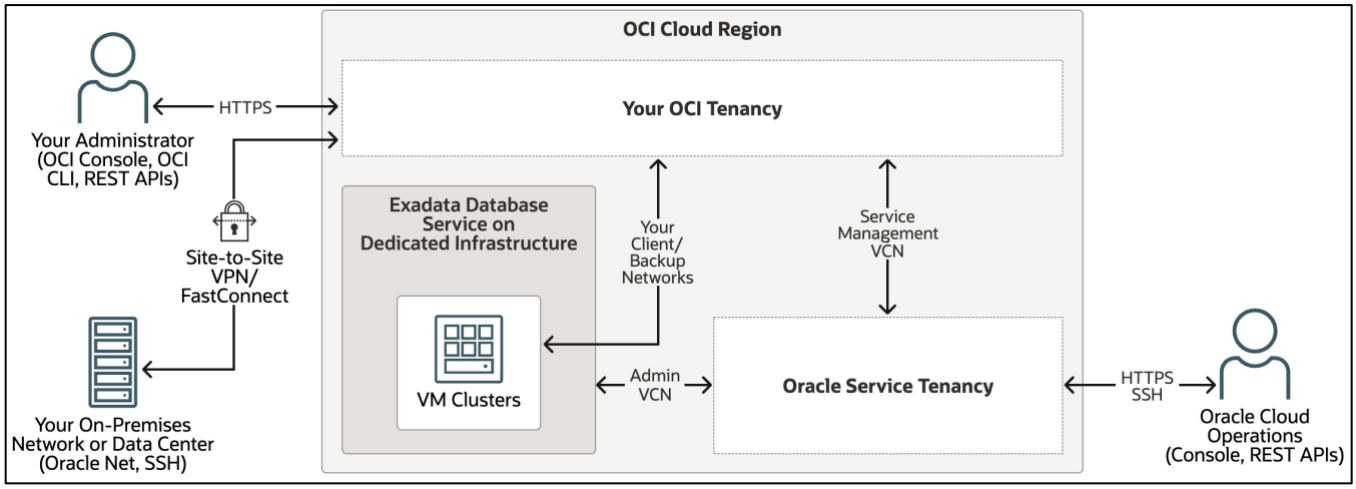

Figure 1: ExaDB-D architecture

The control plane sends the commands to the necessary components through Oracle management networks in response to your management actions, as follows:

Database operations:

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

VM operations:

- Token-based SSH from control plane 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

You can perform some management functionality by accessing the VMs and databases directly using compatible services and tools. See Reference Guides for ExaDB-D for details. You should use OCI interfaces when available to reduce complexity and operational burden, and to improve auditability.

Oracle Cloud Operations manages the infrastructure using HTTPS and SSH from Oracle service tenancies. HTTPS and SSH access are authenticated by FIPS 140-2 Level 3 hardware MFA devices. Authorization is based on Oracle's least-privilege, default-deny access control practices. Access to Oracle VPNs is required to access Oracle service tenancies. Commercial Cloud Operations staff may manage services from outside Oracle facilities.

See Oracle Cloud Infrastructure Security Architecture for more information about how Oracle secures it's cloud for multitenant consumption.

Additions for Multicloud

Multicloud runs Oracle AI Database workloads in Azure, Google Cloud, and AWS data centers. All Exadata hardware for 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.

Figure 2 shows the Multicloud architecture. Three additional components bring ExaDB-D to the CSP data center:

- OCI Child Site: location in CSP data center containing the ExaDB-D equipment
- Private connectivity: network integration connecting your CSP application networks with your ExaDB-D networks
- OCI-Controlled Network: network integration connecting the Child Site to the OCI control plane

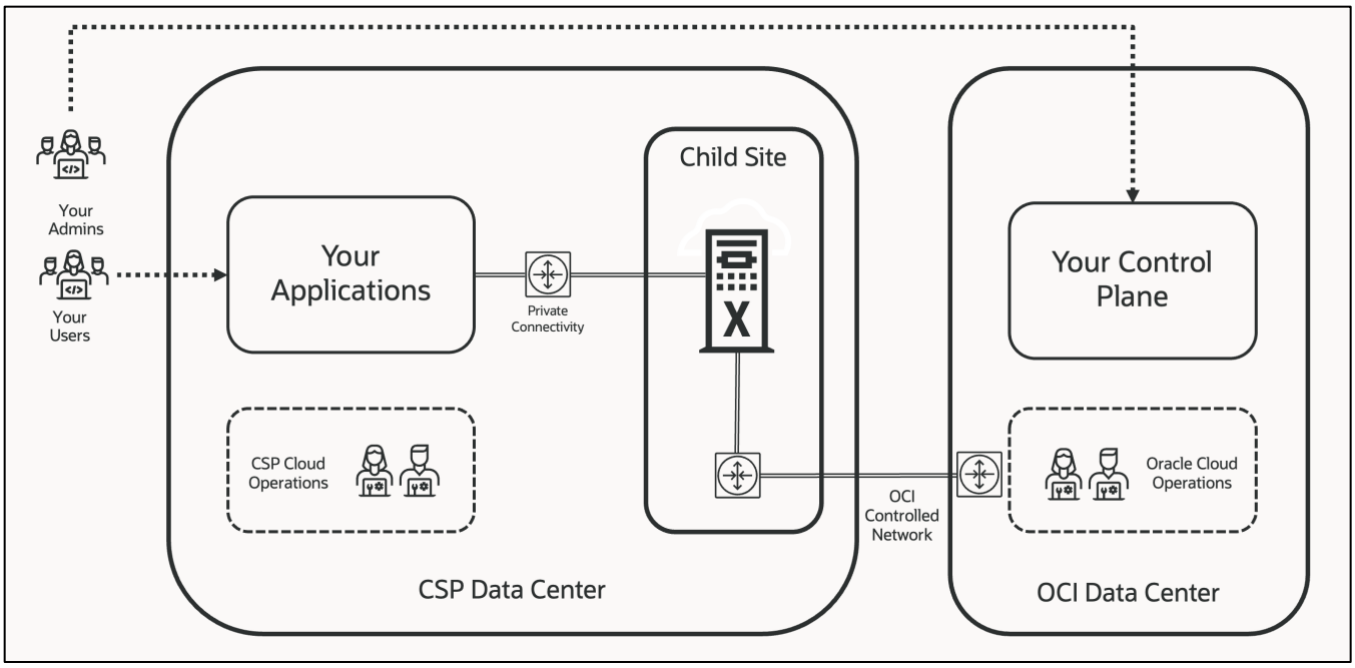

Figure 2: Multicloud architecture

OCI Child Site

The Oracle AI Database services are deployed in an OCI Child Site in the CSP data center. Multicloud racks contain all the components of a standard ExaDB-D 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 apply to the Oracle cages in the Child Site. Logical security for the Child Site follows the standards of the ExaDB-D 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 ExaDB-D 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 ExaDB-D components in response to your CSP and OCI APIs
- CSP staff use their credentials to access CSP equipment
- Oracle staff use their credentials to access Oracle equipment

The Multicloud ExaDB-D is deployed in a subnet within your CSP network. Automation creates a corresponding OCI VCN with a matching subnet and IP CIDR range to your CSP network. The cluster runs in your OCI subnet using VNICs assigned private IPs. These private IPs are also reserved in your 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 3 shows the implementation in Oracle AI Database@Azure. Oracle implements the service similarly with other CSPs.

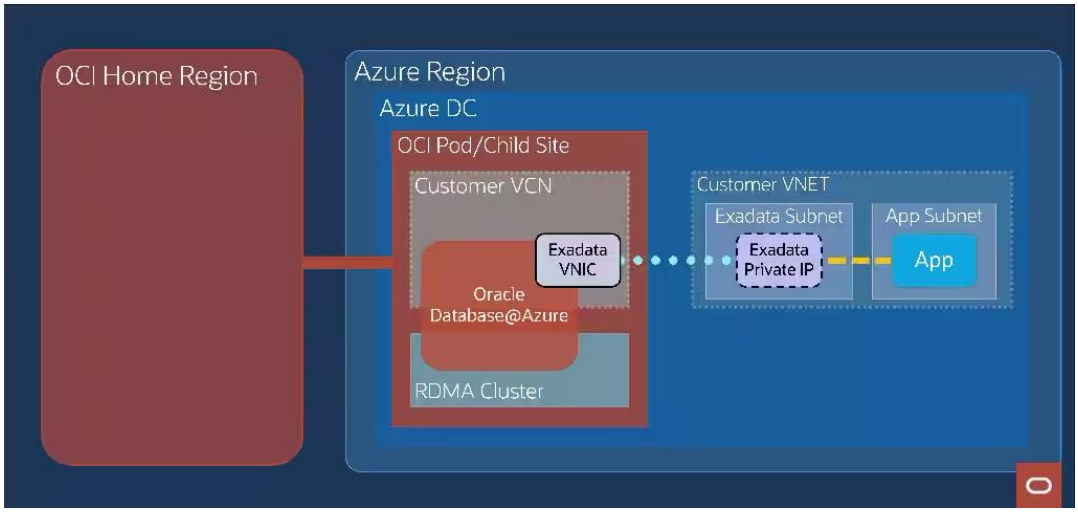

Figure 3: Oracle AI Database@Azure private connectivity

When an application or user in your 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 AI Database instance. The direct private network link helps to prevent the application, user, and database network traffic from leaving CSP data center. Figure 9, Figure 10, and Figure 11 in the technical appendix of this document 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 ExaDB-D networks. You can apply CSP network security controls to your CSP networks and OCI network security controls to your ExaDB-D networks.

OCI Controlled Network

The private OCI controlled network connects the Child Site to the OCI control plane. This network provides access for:

- API and console driven lifecycle management
- Oracle support staff shell and API 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 for Multicloud resources, the calls use federated identity for authentication with downstream OCI APIs. When 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 control plane to create and manage database instances. Figure 4 shows the integration of Azure interfaces calling OCI APIs to manage Oracle AI Database@Azure. Oracle implements the service similarly for other CSPs.

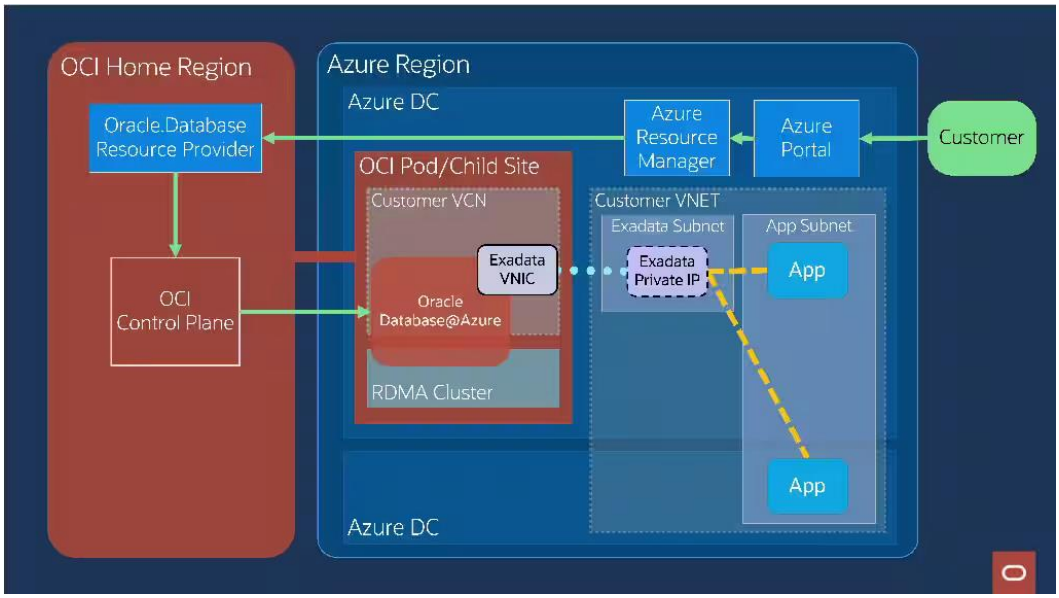

Figure 4: Integration of Multicloud Interfaces

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. Your databases and VMs should continue to function if there are disruptions to the OCI controlled network. A disruption to the OCI controlled network will cause a temporary disruption in API-driven service lifecycle management and Oracle monitoring and maintenance of the Child Site.

SECURITY CONTROLS

ExaDB-D helps you protect your database data from unauthorized access. You control logical access to your OCI tenancy, VMs, databases, and data. Oracle controls logical infrastructure access. Physical access control depends on where you deploy your service:

- ExaDB-D in OCI: Oracle controls data center and physical equipment access
- Multicloud: CSP controls data center access and Oracle controls physical equipment access to Oracle equipment inside the CSP data center

Your authentication and authorization controls include credentials for:

- Access OCI Console, APIs, and services
- VM operating systems and database administration accounts
- Database user to access databases and database data

Your encryption controls include:

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

Your network security controls include:

- Network Security Groups and Security Lists to control layers 2 and 3 access to your VMs
- Zero-trust Packet Routing to control layers 2 and 3 access to your VMs
- Network access rules implemented in the VM operating system and Oracle Connection Manager
- Private Service Access to control which services your VCNs can access and which credentials can be used from your networks

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

Database Security Controls

You can Oracle AI Database security features, compatible OCI services, and compatible key management systems with ExaDB-D. This section provides a summary of commonly used software, services, and key management systems.

Database Authentication

You can configure authentication for Oracle AI Database with Centrally Managed Users, including password authentication, Kerberos authentication, or public key infrastructure (PKI) authentication. With Centrally Managed Users, you can manage the authorization for Active Directory users to access Oracle AI Databases. Oracle AI 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. You can implement MFA by existing external authentication methods for human users with OCI IAM, MS-EI, and RADIUS.

Network Encryption

ExaDB-D encrypts data in flight from the client to the Oracle AI Database instance with Oracle Native Network Encryption (NNE) by default. The Oracle AI Database instance requests encrypted connections from applications and establishes encrypted connections for capable applications. If an application cannot support an encrypted connection, the Oracle AI Database instance will permit the application to connect without encryption. You can change this setting as your requirements dictate. The service automation does not provide OCI interfaces to configure Oracle TCPS (TLS/SSL) for Oracle AI Database connections. You can configure TCPS (TLS/SSL) and mTLS using operating system tools deployed in the VM. See Oracle Native Network Encryption and TCPS (TLS/SSL) in the Security Guide for your Oracle AI Database version for more details.

Data at Rest Encryption

ExaDB-D 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 AI Database@Azure
- AWS Key Management Service for Oracle AI Database@Azure
- Google Cloud Platform Key Management Service for Oracle AI Database@Google Cloud
- 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. Oracle AI Database 26ai integrates the cryptographic algorithms necessary to help protect your database against quantum attacks. For further information on Oracle TDE, consult the Advanced Security Guide for your Oracle AI Database version. The Oracle TDE FAQ provides answers to common architecture and implementation questions.

Encryption Key Management with PKCS#12 Wallet

The TDE MEK is stored outside of the database, by default in a PKCS#12 compliant container called a ‘wallet’. The wallet is stored in a shared file system accessible by your ExaDB-D VMs. Oracle AI Databases 18c and later allow you to upload your 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.

Encryption Key Management with OCI Vault

You can use OCI Vault to store your TDE MEK. 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

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

Encryption Key Management with Oracle Key Vault

You can use Oracle Key Vault (OKV) to store your TDE MEK for your ExaDB-D databases. 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). You can use the OKV Persistent Master Encryption Key Cache to enable databases to be operational if the OKV server is unavailable. See Migration of file-based TDE to OKV for Exadata Database Service Using Automation via REST (KB79439) for more detail.

Encryption Key Management with Azure Key Vault

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

Encryption Key Management with AWS Key Management Service

Oracle ExaDB-D on Dedicated Infrastructure on Oracle AI Database@AWS supports integration with AWS Key Management Service (KMS). This capability allows users to manage Transparent Data Encryption (TDE) master encryption keys (MEKs) using AWS customer managed keys.

Encryption Key Management with Google Cloud Key Management

ExaDB-D on Oracle AI Database@Google Cloud supports integration with Google Cloud Platform's Key Management Service (KMS). This allows users to manage Transparent Data Encryption (TDE) master encryption keys (MEKs) using GCP Customer-Managed Encryption Keys (CMEKs).

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

Oracle AI Database is compatible with PKCS#11 compatible key management devices. Third-party key management and HSM vendors have used this interface to implement TDE key management for Oracle AI Databases. Reference My Oracle Support (MOS) note Oracle TDE Support With 3rd Party HSM Vendors (KB593570) for implementation and support details.

Integrating an external key manager requires you to install PKCS#11 libraries on your ExaDB-D 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 AI 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.

Database Backup Encryption

All backups are encrypted with the same master key used for the Transparent Data Encryption wallet encryption. The encryption key is not stored with the backup. You are responsible for backing up and restoring your TDE master encryption key. When you use the Autonomous Recovery Service, backups of encrypted tablespaces, and redo describing changes to these tablespaces, are encrypted. 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.

Preventing Database Administrators from Accessing User Data with SQL

Oracle Database Vault helps to both protect application data from database administrator access and address privacy and regulatory requirements. You can deploy controls to block database administrator access to application data and control sensitive operations inside the database using trusted path authorization. You can 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 for your database version.

Mitigating SQL Injection Attacks

Oracle SQL Firewall provides real-time protection against common database attacks by restricting database access to only authorized SQL statements or connections for a designated user. It mitigates risks from SQL injection attacks, anomalous access, and credential theft or abuse, preventing or detecting potential SQL injection attacks. You can use SQL Firewall to control which SQL statements are allowed to be processed by the database. In addition, SQL Firewall can use session context data such as IP address to restrict database connections. Unauthorized SQL and database connection can be logged and blocked.

SQL Firewall helps to address the following three use cases:

- Provide real-time protection by restricting database access to only authorized SQL statements and database connections
- Mitigate SQL injection attacks, anomalous access, and credential theft/abuse risks
- Enforce trusted database connection paths

SQL Firewall offers the following benefits:

- Inspects all incoming database connections and SQL statements, including those from PL/SQL
- You decide whether you want to block unauthorized SQL or only log it
- Evaluates the complete SQL and the processing context
- Blocks connections that do not come from trusted IP addresses, operating system user names, or program names
- Enables you to build an allow-list policy for each database user of SQL statements that a typical database user performs, and then detects, blocks, and logs any unexpected SQL

See the SQL Firewall product documentation for more details. SQL Firewall is available starting in database version 26ai.

Database Security Monitoring and Management

You can use software and services compatible with the Oracle AI Database and ExaDB-D to monitor and manage your database security posture. Oracle provides security monitoring and management tools for your ExaDB-D databases, including Oracle Data Safe and Oracle AI Database Security Assessment Tool (DBSAT).

Oracle Data Safe

Oracle Data Safe is an OCI cloud service that helps you:

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

Data Safe Architecture shows implementation details. The Data Safe FAQ provides answers to commonly asked questions about Data Safe. There is no additional cost to use Data Safe so long as you do not exceed one million audit records per database in a month.

Oracle Database Security Assessment Tool

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

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.

Controlling VM Cluster Access to Exadata Storage

ASM-scoped Security controls which Oracle Automatic Storage Management (ASM) clusters and Oracle AI 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 Exadata Database Machine and Compliances with PCI-DSS V3.2 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.

VM Security Controls

Your ExaDB-D VM is deployed with a security-hardened operating system that includes the following:

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 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

You access your VM with token-based SSH. 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. 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 the Add SSH key functionality with API Access Control so that an OCI identity seeking to add an SSH key must get approval from a different OCI identity.

Exadata software version 22.1.4.0.0.221020 and newer supports Microsoft Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) for authentication to your VMs. You configure AD and LDAP using the Linux System Security Services Daemon (SSSD). 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.

Oracle cloud automation secure login via token-based SSH is not compatible with Kerberos authentication. Oracle cloud automation functionality that accesses your VM with SSH will fail if you implement Kerberos authentication in the VM and require additional challenges to authenticate to the privileged user accounts (`root`, `oracle`, `grid`, `opc`, and `dbmadmin`). You can use Kerberos authentication for Oracle database users.

VM Default Security Settings

The ExaDB-D VM is deployed with security settings that align with industry standards and Oracle best practices. 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.
  - `-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.

`PermitRootLogin=without-password` is required for some cloud automation capabilities. If you set `PermitRootLogin=no`, those actions will fail, and you will need to set `PermitRootLogin=without-password` for those actions to complete. You can manage `PermitRootLogin` to you standards using operating system tools.

You should retain the deployed settings to reduce testing and maintenance effort, and to avoid service disruption risk caused by configuration changes.

VM Default Users

Each ExaDB-D VM includes privileged service accounts used by Oracle to deliver and maintain the service. Token-based SSH login is required. Password-based SSH login is disabled. 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 AI 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 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 ExaDB-D software.

You must retain 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

VM File Integrity Monitoring

ExaDB-D includes Oracle Linux Advanced Intrusion Detection Environment (AIDE) 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. The time to report changes is dependent on the system checks (usually at least once a day) that you configure in `/etc/aide.conf`. The configuration file defines which files and directories are monitored by AIDE, and how logging and output are handled. See Oracle Linux: Advanced Intrusion Detection Environment (AIDE) Usage and HOWTO KB385603 for more information.

VM Backup Encryption

Oracle backs up images of your VMs to components in your ExaDB-D infrastructure rack to help recover from physical database server failure. Oracle encrypts these backups and controls backup encryption keys. Oracle can restore these images when the components in the rack storing these backups are available.

Cloud Automation Access to Your 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 ports 7060 and 7070
- Secure login to VM as a privileged user (`root`, `opc`, `grid`, `oracle`) via token-based SSH

The control plane generates a temporary and unique SSH key pair for each management action. The public key is added to the `~/.ssh/authorized_keys` files of the necessary service account in the VM by the DBCS agent. The private key is stored in the control plane infrastructure. The control plane discards the private key and removes the temporary key after the action completes.

The VM provides the Oracle Linux packet filtering software 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 function if you block cloud automation access to the VM at the network layer.

Controlling Oracle Services and Support Staff Access to Your VM

You can use Delegate Access Control to subscribe your VMs to database maintenance and support services, and control and monitor access by service provider staff. You can subscribe to 5 different services:

- Oracle AI Database Cloud Customer Support – support services for your database and Oracle Linux technology that are included at no additional charge
- Oracle AI Database Cloud Operations Support – support services for cloud automation software deployed in your VM that are included at no additional charge
- Oracle-Managed software updates for Database Cloud Services – support services for updating your VM software that are included at no additional charge
- Oracle Engineered Systems Deployment and Infrastructure Support – assisted patching and troubleshooting for your services that are negotiated separately
- Strategic Customers Program for DB Cloud Platforms – custom support services that are negotiated separately

When you use Delegate Access Control:

- Oracle staff access your VM only after you approve
- Action Enforcement restricts access to approved components related to the work request

- Access is temporary, just-in-time, and automatically revoked after a set time
- Command and keystroke logs are traceable to an individual person
- Oracle can provide personal information when required for executed commands and keystrokes

You can terminate access at any time. When you terminate access, Delegate Access Control:

- Terminates SSH connections and Bastion hosts
- Terminates Linux processes started by the temporary account
- Removes temporary credentials

Figure 5 shows the Delegate Access Control approval and access workflow. Delegate Access Control uses the same delivery mechanics as Operator Access Control, and is included in the scope of the Operator Access Control PCI-DSS attestation of compliance (AoC).

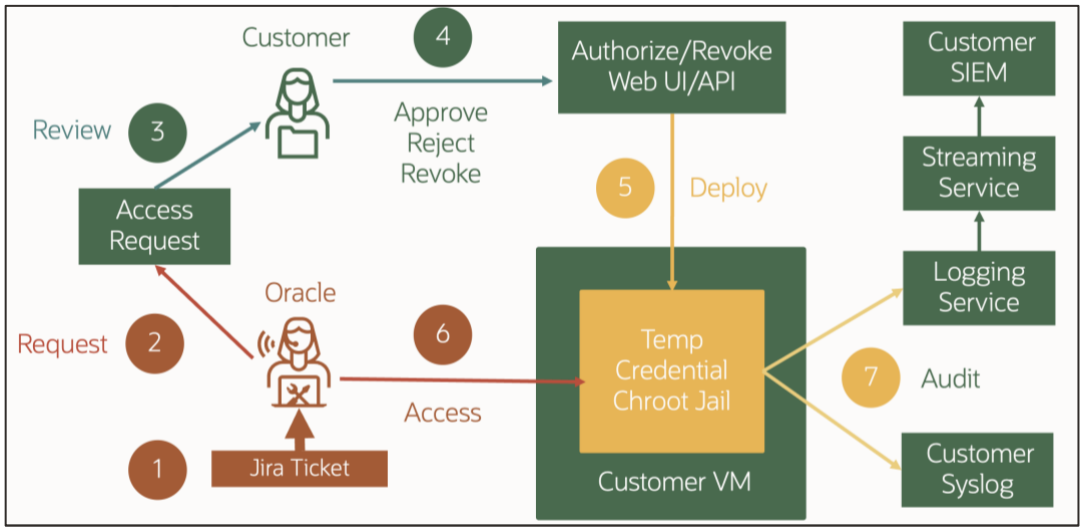

Figure 5: Delegate Access Control approval workflow

Network Security Controls

You can use OCI network security features with ExaDB-D, including:

- Network Security Lists and Security Groups
- Zero-trust packet routing
- Private Service Access (PSA)
- VCN Flow Logs

This section summarizes these controls.

Controlling IP Addresses, Ports and Protocols with Firewall Features

You can use Network Security Groups and Security Lists, virtual firewall features that control traffic at the packet level, with your ExaDB-D service. The product documentation provides ways to implement the security rules. Your network security controls must allow the ExaDB-D network requirements, such as:

- 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

The suggested security rules are general and designed for ease of implementation. You can further restrict network access to your minimum requirements if you do not need the full access provided by the suggested rules.

Controlling IP Addresses, Ports, and Protocols with Declarative Natural Language

You can use Zero Trust Packet Routing (ZPR) with ExaDB-D to help prevent unauthorized access to data by managing network security policy separately from the underlying network architecture. You use an easily understood and intent-based

policy language, security administrators to define specific access pathways for data. Traffic that is not explicitly allowed by policy cannot travel the network, improving security while simplifying the work of security, network, and audit teams.

Controlling Which Credentials can be Used From Your Networks

You can use Private Service Access (PSA) instead of a Service Gateway with your ExaDB-D service for granular, per-service network access controls. PSA uses a private IP from your network as the path to reach an OCI service API, rather than the public IP for that API. In-tenancy credentials are enforced when accessing a service through a PSA, blocking cross-tenancy credential use and cross-tenancy Object Storage PAR access.

You must create the following PSAs to support ExaDB-D:

- Database Service: Used for resource principal authentication and access to your service metadata
- Identity and Access Management Data Plane API: Used for service authentication
- Object Storage Service API: Used for software updates and custom image downloads
- Functions Service Invocation: Used for service monitoring
- OCI Monitoring Ingestion: Used for service monitoring
- Logging Ingestion API: Used for service monitoring

You must also create a network security rule to allow inbound access to your subnet on port 443 from the network that you configured your PSA on.

Additional OCI Security Controls

OCI provides other security services to support your ExaDB-D service. This section provides a summary of commonly used controls.

Controlling Which Networks Can Authenticate to Your Tenancy Resources

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 a Transit VCN. This gives your on-premises network private access to Oracle services, so your on-premises hosts can use their private IP address and the traffic does not go over the public internet.

Denying Specific API Actions in Your Tenancy

IAM Deny policies introduce deny statements that simplify policy management, enabling easier restriction of resource access. Only members of the default administrator group in the default domain can enable deny policies through a guided workflow in the Console. During setup, the following default root-level policy restricts who can manage deny statements, ensuring that only the tenancy administrator who enabled IAM deny is allowed to write deny policies, along with members of the default administrators group. Members of the default administrator group in the default domain are always exempt from a deny policy to ensure continued access at the highest level.

To help control risk, administrators can enable notifications for deny policy changes. While deny policies enhance security and flexibility, they must be managed carefully, because administrators in child compartments can use deny policies to block parent access. Deny policies take precedence over allow policies

Controlling Your Administrators' Use of Privileged APIs

API Access Control adds a mandatory approval workflow for privileged APIs. When enabled on Cloud Exadata Infrastructure, it extends protection to its associated Cloud VM Clusters and Container Database by enforcing a multi-identity approval workflow for privileged OCI Console and API functionality, including:

- Deleting databases, VM Clusters, and infrastructure
- Updates to Database, Grid infrastructure, and operating system software
- Data Guard switchover
- Creating a VM console connection
- Adding SSH keys to VMs

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 6 shows the API Access Control approval

workflow. See API Access Control at the Oracle Learning Center for more details. API Access Control is included with no additional charge.

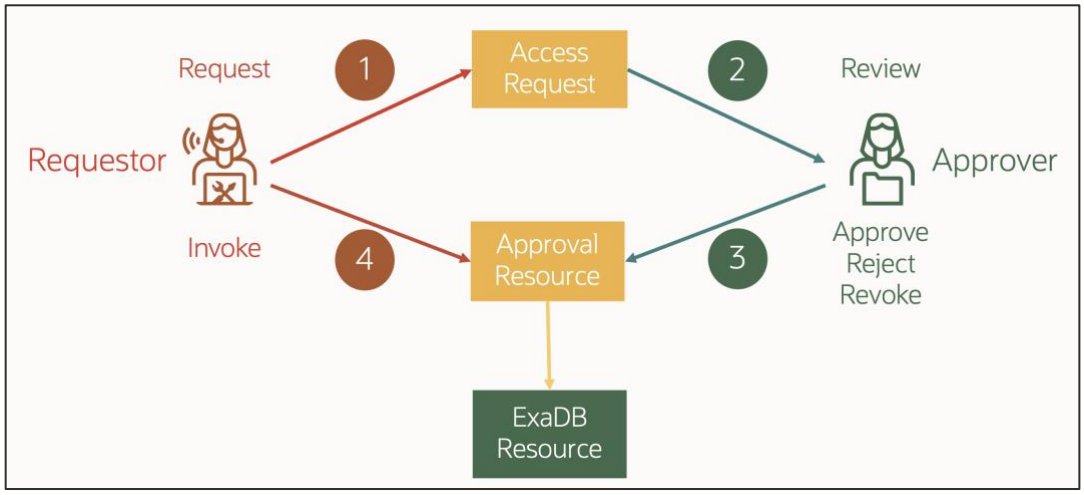

Figure 6: API Access Control approval workflow

Ransomware Recovery

Oracle Database Autonomous Recovery Service (Recovery Service) is a fully managed, standalone, and centralized database protection service for Oracle AI Databases deployed in OCI, Multicloud, and on-premises. It is engineered for database ransomware protection. It has four key technology pillars:

- Database Protection includes real-time transaction protection and end-to-end ransomware protection and immutability
- Recovery Assurance includes continuous backup validation, database protection monitoring, as well as high-speed, fast database restore capabilities through a dedicated network
- Resilient Architecture built on a compute and storage servers foundation, which stems from Oracle Exadata engineered systems design methodology; the user model has a separation of duties; the roles for databases, the Recovery Appliance, and for any related appliances are segregated from each other; no one user can access other systems which they are not privileged to do so
- Immutable Backups prevents the backups themselves on a compromised system to be purged or deleted by internal processes or external users

Recovery Service has resiliency and recoverability from cyber-attacks. It is designed to be fault-isolated from the production database. If a cyber-attack hits the production database, Recovery Service is not compromised. Oracle recommends using Recovery Service to help protect Oracle AI Databases from ransomware.

Oracle Infrastructure Security Controls

Oracle exclusively manages infrastructure security and availability as outlined in the Oracle PaaS and IaaS documentation. Oracle Corporate Security Practices 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 process whereby authorization to access infrastructure is consistent with updates to employee job code, training records, and employment status. Oracle further controls Cloud Operations access per Oracle Access Control with a least-privilege, default-deny approach where access is provided for:

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

Cloud Operations staff access and support service infrastructure components, including:

- Power Distribution Units (PDUs)
- Out-of-band (OOB) management switches

- Storage Network switches
- Exadata Storage Servers
- Physical Exadata Database Servers

Oracle controls for Cloud Operations staff access to ExaDB-D infrastructure include:

OCNA access:

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

Bastion host access:

- Entitlement granted based on job-code and training records
- Requires OCNA access
- Isolated to privileged admin VCNs in the region hosting the service
- Authentication by FIPS 140-2 Level 3 hardware MFA devices
- Connection logging and monitoring traceable to named users

ExaDB-D management server and infrastructure access:

- Entitlement granted based on job-code and training records
- Requires Bastion host access
- Authentication by FIPS 140-2 Level 3 hardware MFA devices
- Connection logging and monitoring traceable to named users

Figure 7 how Oracle Cloud Operations staff access ExaDB-D infrastructure components.

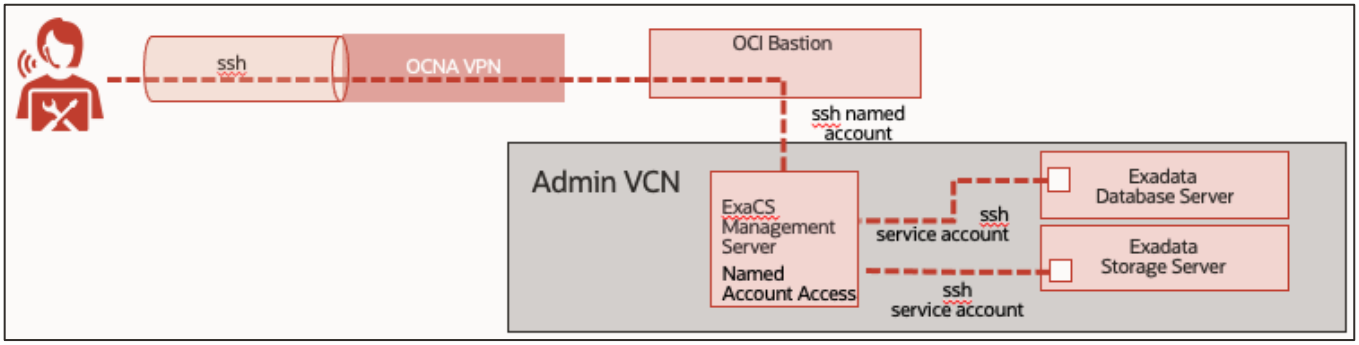

Figure 7: Cloud Operations shell access to ExaDB-D infrastructure

Oracle's commercial Cloud Operations staff work globally in a follow-the-sun model, providing 24/7 support. Commercial Cloud Operations staff may manage services from outside Oracle facilities.

AUDITING AND LOGGING

ExaDB-D provides 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.

You can send your audit logs to compatible technology. See Ingest Oracle Cloud Infrastructure Logs into Third-Party SIEM Platforms using Log Shippers for implementation details. Monitoring your audit logs is not part of Oracle's responsibility, and Oracle does not monitor your audit logs. You can request access to applicable Oracle infrastructure audit log information from Oracle via the Oracle service request (SR) process. Operator Access Control and Delegate Access Control audit logs are available to you and Oracle.

Database Audit Logging

ExaDB-D provides comprehensive audit logging for the database with Oracle AI Database Unified Audit. You can send these audit records to your syslog server or compatible security information event management (SIEM) system. Oracle publishes

documentation for configuring, managing, and monitoring of Oracle AI Database audit logs in the Oracle AI Database Security Guide for each database version. See Oracle AI Database Unified Audit: Best Practice Guidelines for more detail.

You can use Database Vault to protect the Oracle AI Database Unified Audit Trail from database administrators.

VM Audit Logging

The Oracle Linux audit log service (`auditd`) records actions executed by operating system credentials in your VMs. You can configure `auditd` per your standards, including sending the Oracle Linux audit log to a remote log server. You can integrate the Oracle Linux audit logs into the OCI Log Analytics service.

OCI Audit Logging

OCI Audit 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

Audit events have a header ID, target resources, timestamp of the recorded event, request parameters, and response data. You can view events logged by the OCI Audit service by using the OCI Console, API, or the SDK for Java. Data from events can help you 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. You can forward these logs to compatible systems.

Network Traffic Logging

You can use VCN Flow Logs to capture network traffic information to support monitoring and security needs. VCN flow logs show details about traffic that passes through a VCN help you audit traffic. You can use capture filters to evaluate and select traffic to include in the flow log and leverage the Logging service to send log information to a specified log group.

Oracle Infrastructure Audit Logging

Oracle is responsible for recording, analyzing, and responding to infrastructure audit logs.

Infrastructure audit logs for ExaDB-D 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`

Infrastructure audit logs for ExaDB-D X8M and later hardware include the following:

ILOM:

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

Physical Exadata Database Server:

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

Exadata Storage Server:

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

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

INCIDENT RESPONSE

You and Oracle work together to secure and monitor access to ExaDB-D 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, notify Oracle of the action and response using the Oracle Service Request (SR) process.

Your Responsive Controls

You may take any responsive action on any services you control. This includes terminating network connections into your VM and Oracle AI Database.

Oracle Incident Response Process

Oracle Incident Response describes how Oracle responds to security incidents, shown below:

"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 describes Oracle's 15-minute service response time for critical issues, including security incidents, shown below:

"5.3.1 Severity 1 (Critical Outage)

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

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

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

SOFTWARE SECURITY AND UPDATES

Oracle Software Security Assurance Practices govern Oracle software development. Oracle implements segregation of duties for development, test, quality assurance, and deployment of software. Reference the following documentation for details:

- Oracle Critical Patch Updates for Security Alerts and Bulletins
- Exadata Database Service Software Versions
- Configure Oracle-Managed Infrastructure Maintenance
- Patch and Update an ExaDB-D System
- ExaDB-D Interim Software Updates

Oracle stages software updates for your Oracle AI Database, Grid Infrastructure, and your Linux operating system in OCI Object Storage. These updates are listed in OCI interfaces when they are available. You control when your staff can apply these updates. You schedule quarterly infrastructure updates during a period that will have the least impact on your users. OCI interfaces provide full control and visibility over when Oracle applies quarterly infrastructure. You can reschedule maintenance when required.

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.

You can find which CVEs are covered by which Critical Patch Update Advisory or Security Alert in the Oracle Map of CVE to Advisory/Alert. You can identify the CVEs resolved by a software release for your VM or Exadata Infrastructure by:

- Accessing your VM Cluster Updates (OS) or Update History and record the software version (e.g., 24.1.18.0.0.251115)
- Accessing Exadata Database Machine and Exadata Storage Software Supported Versions (KB153930)
- Finding your software version and downloading the CVE Release Matrix

Development and debug tools to inspect your data are not installed on ExaDB-D infrastructure.

SECURITY TESTING AND SCANNING

Security Testing and Scanning of Your VM

You can test the security of ExaDB-D in accordance with Oracle Cloud Testing Policies. Your service includes OpenSCAP to scan the VM for compliance.

You can use third-party scanning tools to scan your VMs. Your third-party scanning tools and benchmarks should be compatible with the ExaDB-D software distribution and configuration. In some cases, arbitrary benchmarks flag security

issues on the ExaDB-D VM that are not a material risk. See responses to common Exadata security scan findings (FAQ3926) to learn more about how common benchmarks may be adjusted to work with Exadata.

Security Testing and Scanning of Oracle-Managed Infrastructure

Oracle requires security analysis and testing on Oracle products.

Oracle performs monthly infrastructure security scans and updates to ExaDB-D infrastructure to remain in compliance with Oracle corporate security standards. These standards align with and support various industry standards, including PCI-DSS, and government security standards, including FedRAMP High and ISO/IEC 27001. Oracle performs updates to infrastructure online, with no reboot, and designed to have no impact on compatible 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 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.

CUSTOMIZATION AND THIRD-PARTY SOFTWARE

ExaDB-D provides you with privileged access to your environments, including `root` access to guest operating systems and `SYSDBA` access to Oracle AI Databases. This level of control allows you to make configuration changes and install 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 ExaDB-D are published on My Oracle Support document, Installing Third-Party Software on Exadata Components (KB144164).

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. Oracle support is included with your database service subscription at no additional charge.

Compatible Service Modifications

You may modify certain aspects of your VM to comply with your security standards, including:

- Firewall/packet filtering services, provided you allow cloud automation functionality
- Login banner
- `sudo` log file, operating system audit logs, and sending audit logs to remote log servers
- Password aging, complexity, history, and expiration
- `systemd` journal upload and send to remote syslog server
- Configure system-wide crypto policy MACs
- Configure `fs.suid_dumpable`

Required Service Configuration

You must preserve certain aspects of your VM to support service operation, including:

- `exec` permission on `/tmp`, `/dev/`, `/var/tmp`, and `/var/log`
- `exec` and `suid` on `/dev/shm`
- Deployed `crontab` configuration
- Deployed `sudo` configuration
- Deployed shell timeouts
- Deployed `umask`
- Deployed `net.ipv4.conf.all.rp_filter` configuration
- Deployed dot file access
- `rds` kernel module
- Cryptographic library configuration
- Deployed usernames, userids, group names, and group ids

Your VM `pam.d` configuration includes `[default=die]` for auth failure, which functions like `required` and `requisite`.

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.

`PermitRootLogin=without-password` is required for some cloud automation capabilities. If you set `PermitRootLogin=no`, those actions will fail, and you will need to set `PermitRootLogin=without-password` for those actions to complete. You can manage `PermitRootLogin` to you standards using operating system tools.

If you modify your VM to comply with a benchmark, you should test these modifications and validate they do not compromise service functionality prior to production deployment. Automated operating system, Oracle AI Database, and Grid Infrastructure updates can revert your changes. Oracle recommends using the service as delivered. Following the prescribed service design helps reduce the need for extensive testing, validation, and troubleshooting of changes.

SERVICE TERMINATION AND DATA DESTRUCTION

You can terminate your ExaDB-D. Termination invokes the Exadata Secure Eraser utility, 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 AI 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. Hardware used for ExaDB-D supports cryptographic erase. The cryptographic erasure method used by Secure Eraser is designed to comply with the NIST SP-800-88r1 standard. You can obtain secure erase certifications from Oracle by opening a My Oracle Support (MOS) Service Request (SR).

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 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. See Consensus Assessment Initiative Questionnaire (CAIQ) v4.0 for Oracle Cloud Infrastructure (OCI) for more detail.

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

- 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

EXCEPTION WORKFLOWS FOR ORACLE ACCESS TO YOUR VM

ExaDB-D support includes break-glass 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 implement Delegate Access Control and subscribe to Oracle Cloud Customer Support and Oracle Cloud Operation, then Oracle Cloud Support and 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 controlled by Action Enforcement 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 your syslog server.

VM is Accessible by You

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:

- As per the security policy associated with ExaDB-D, Oracle personnel are prohibited to access customer domU[1] 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.

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

VM is not Accessible by You

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 staff 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 ExaDB-D with VM Name <insert VM Name as listed under the DB Server detail page→ Resources→ Virtual Machines>
- SR Content:
  - We are opening this SR to grant explicit permission to Oracle to access our Guest VM for support to help resolve the issue described in SR# 1-xxxxxxxx. We acknowledge that by providing this permission, we understand that Oracle will have access to all files and memory that are part of the Guest VM. In addition, we also agree that 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 Oracle staff access, you open a Service Request (SR) with the following language:

- SR Title:
  - SR granting Oracle explicit permission to access a Guest VM of ExaDB-D with VM Name <insert VM Name as listed under the DB Server detail page→ Resources→ Virtual Machines>
- SR Content:
  - We are opening this SR to grant explicit permission to Oracle to access our Guest VM in a shared screen session for support to help resolve the issue described in SR# 1-xxxxxxxx. We acknowledge that by providing this permission, we understand that Oracle will have access to all files and memory that are part of the Guest VM. This permission to access our VM is contingent on our representative being able to monitor in real-time via a screen-sharing session all activities performed by Oracle. In addition, we also agree that 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.

SUMMARY

With ExaDB-D, you control the security features throughout the VM. Oracle AI Database encryption encrypts data, and you retain control of the encryption keys. Oracle AI 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 ExaDB-D help to prevent unauthorized actions on the infrastructure components of ExaDB-D. Security measures include multi-factor named user authentication and strong authentication with and FIPS 140-2 level 3 compliant token-based SSH access to Oracle-managed infrastructure components. Auditing and logging are implemented throughout the stack, and applicable audit logs are available to you through the Oracle Service Request (SR) process.

ExaDB-D delivers the benefit of a high-security on-premises deployment with the ease-of-use and economics of the cloud. Your staff and Oracle staff work together to implement system security and help prevent unauthorized access to and theft of customer data. In the ExaDB-D deployment model, you gain the security of an on-premises deployment with the benefits of cloud economics, agility, and scale.

TECHNICAL APPENDIX

Network Architecture Diagram

Figure 8 shows the network interface diagram for ExaDB-D. 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

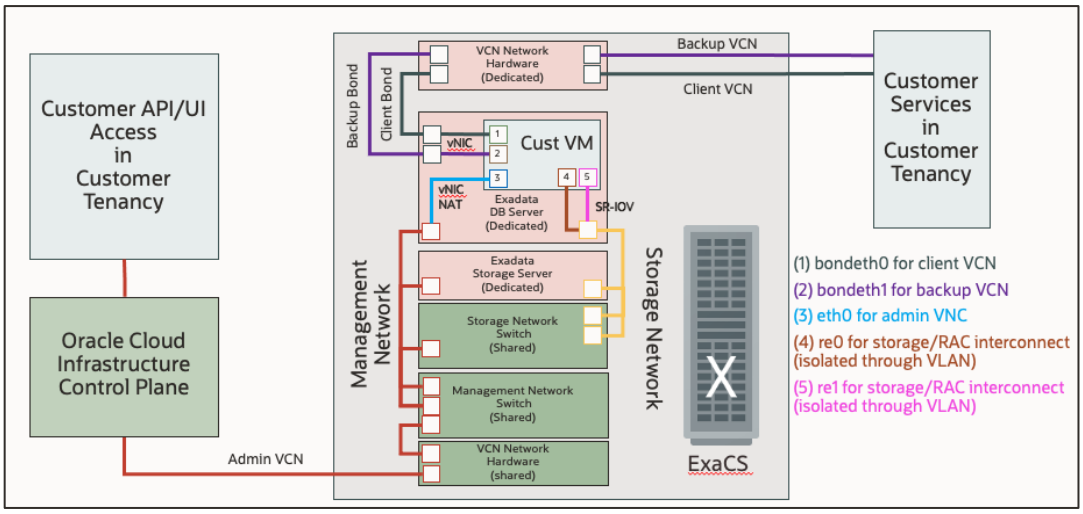

Figure 8: ExaDB-D network architecture

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 ExaDB-D 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. Your users and applications connect to databases through the client or backup network using standard Oracle protocols, such as Oracle Net over TCP port 1521 and TCPS over port 2484. Shell access to the VMs is through token-based SSH on TCP port 22, following standard Oracle Linux procedures. You can access your ExaDB-D VM serial console for exceptional maintenance, support, and software installation conditions.

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

- 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 ports 7060 and 7070.
- 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.

Multicloud Network Architecture Diagrams

This section shows the network diagrams for Oracle AI Database@Azure with multiple availability zones (Figure 9), Oracle AI Database@AWS with a single availability zone (Figure 10), and Oracle AI Database@GCP with a single availability zone (Figure 11). You may deploy any of these services with single or multiple availability zones if the region supports those configurations.

In all cases, your ExaDB-D client and backup networks connect to your CSP networks to support your applications. These networks also support access to OCI services used to deliver the ExaDB-D service. You can apply OCI network security technology to these networks just like you can do so for ExaDB-D in OCI, including:

- Network Security Groups
- Security Lists
- Zero-trust Packet Routing
- Private Service Access

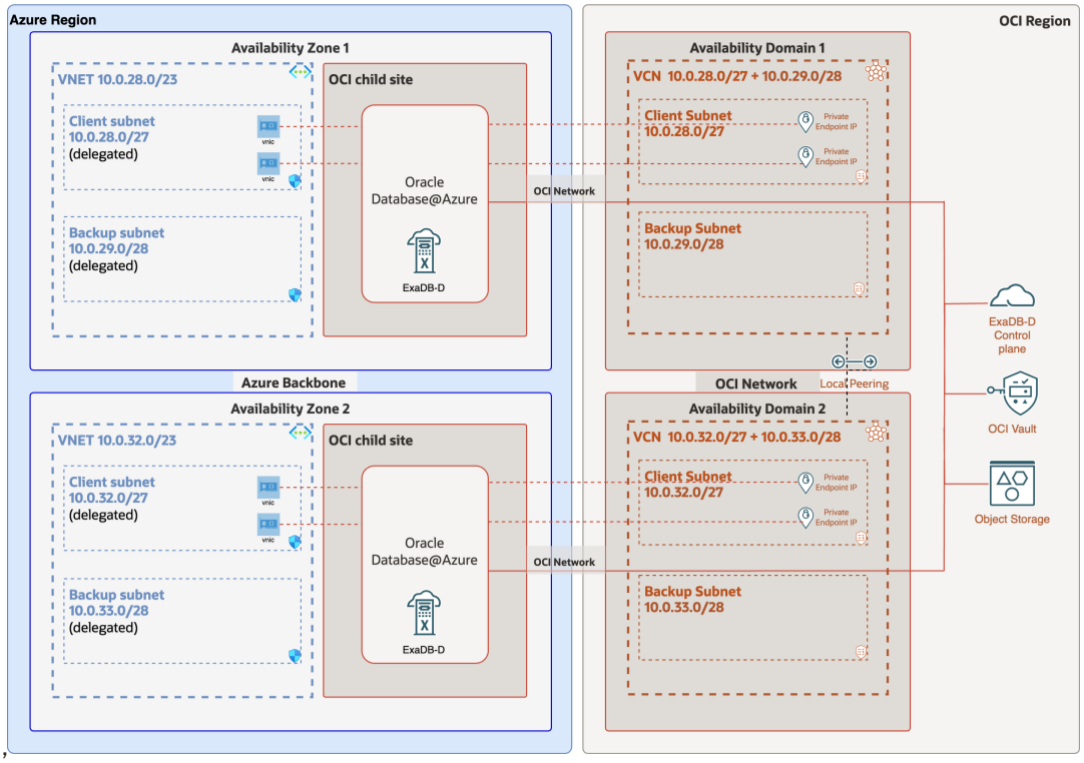

Figure 9: Oracle AI Database@Azure network diagram

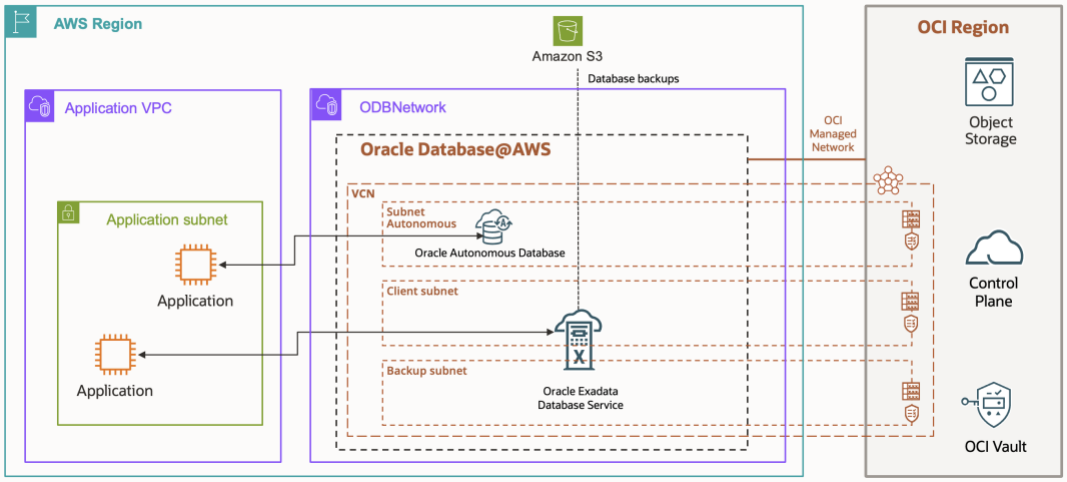

Figure 10: Oracle AI Database@AWS network diagram

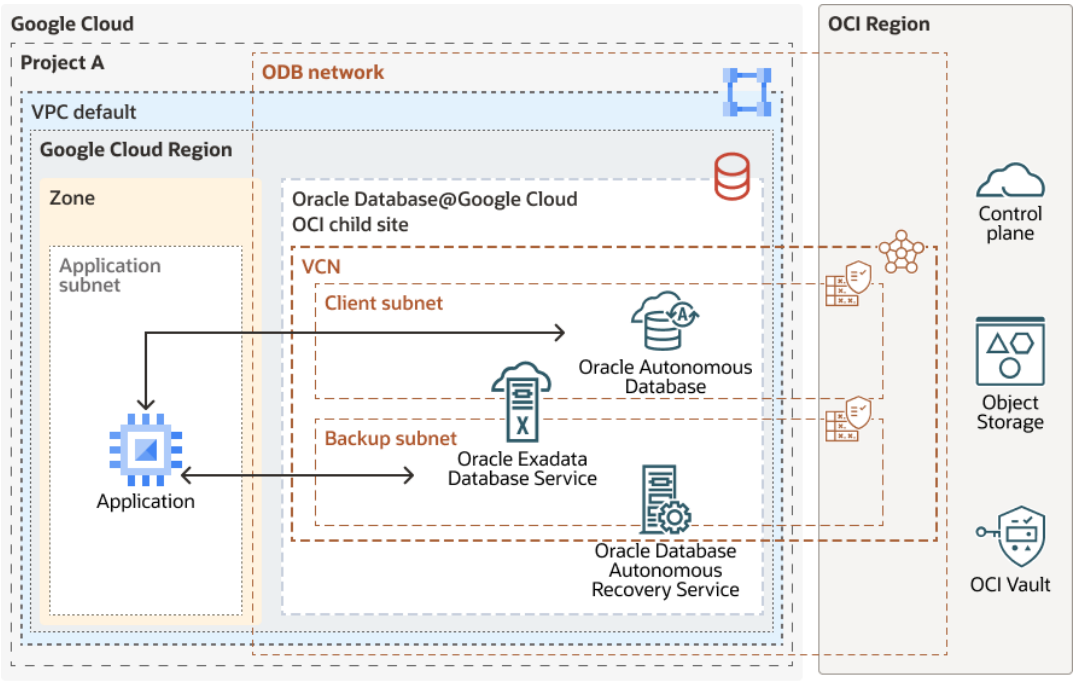

Figure 11: Oracle AI Database@GCP network diagram

VM Default Processes and Certificates

ExaDB-D VMs run Oracle software processes that support database operations, including

- Oracle AI Database, Oracle Real Application Clusters (RAC)
- Oracle Trace File Analyzer (TAF)
- Exawatcher
- Exadata Management Server (MS)

Table 3 shows 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 service issues and minimizes operational burden.

Table 3: Default port matrix for guest VM services

TYPE OF INTERFACE	NAME OF INTERFACE	PORT	PROCESS RUNNING	CERTIFICATE AUTHORITY
Bridge on client VLAN	bondeth0	22	sshd	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 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	Oracle self-signed; customers may add customer-controlled certificates

		TLS/SSL uses port 2484	security authentication	
		5000	Oracle Trace File Analyzer Collector	Oracle self-signed
		7879	Jetty Management Server. Application server engine that is used internally by Oracle Exadata System Software, in particular Management Server (MS).	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 running on each cluster node communicates through these interfaces.	clib0/clre0	1525	Oracle TNS listener Oracle Clusterware running on each cluster node communicates through these interfaces.	N/A
		3260	Synology DSM iSCSI	N/A
		5054	Oracle Grid Interprocess Communication	N/A
		7879	Jetty Management Server	Oracle self-signed

		Dynamic Port: 9000-65500 Ports are controlled by the configured ephemeral range in the operating system and are dynamic.	System Monitor service (osysmond) Cluster Logger service (ologgerd) Cluster Health Monitor 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	Oracle self-signed
		7070	dbcs-agent Cloud agent for handling database lifecycle operations	Oracle self-signed
	stib1/stre1	7060	dbcs-admin	Oracle self-signed
		7070	dbcs-agent	Oracle self-signed
Control Plane server to domU	eth0	22	sshd	N/A
Loopback	lo	22	sshd	N/A
		2016	Oracle Grid Infrastructure	N/A
		6100	Oracle Notification Service (ONS), part of Oracle Grid Infrastructure The Cluster Synchronization Service (CSS), Event Management (EVM), and Oracle Notification Services (ONS) components	N/A

			communicate with other cluster component layers on other nodes in the same cluster database environment.	
		7879	Jetty Management Server	Oracle signed
		Dynamic Port 9000-65500	Oracle Trace File Analyzer collector	Oracle signed
Customer-controlled	Customer-controlled	customer-controlled	Optional Data Safe On-Premises Connector	Customer-controlled or Oracle signed

VM Serial Console Access via OCI Control Plane

You access your VM serial console with a token-based SSH tunnel. You tunnel through the control plane to the hypervisor console of the VM. You control access in 3 steps:

1. Your OCI IAM credentials create a serial console connection, which includes deploying a temporary Bastion host, and 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 serial console using your username and password; typically, the `root` user.

The control plane terminates the console connection 24 hours after creation. 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 serial console with API Access Control.

COMMERCIAL APPENDIX

This section summarizes Oracle public commercial content related to common security questions for ExaDB-D. Visit the Oracle Trust Center 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 for relevant detail about a specific standard for ExaDB-D. This information is subject to change and may be updated frequently, is provided "as-is" and without warranty and is not incorporated into contracts

The frameworks and standards ExaDB-D is delivered to include:

- C5
- CSA STAR Level 2
- Canada Protected B
- DESC (UAE)
- DoD IL5
- ENS High
- FSI (Korea)
- FedRAMP High – JAB ATO
- G-Cloud Marketplace
- GxP
- HIPAA
- HITRUST CSF
- Héberge des Données de Santé (HDS)
- IRAP
- ISMAP
- ISMS
- ISO/ EC 20000-1
- ISO/IEC 27001

- ISO/IEC 27017
- ISO/IEC 27018
- ISO/IEC 27701
- ISO/IEC 9001
- MeitY
- NCSC
- NISC
- PCI DSS
- SAMA
- SOC 1
- SOC 2
- SOC 3
- Saudi Arabian National Cybersecurity Authority
- Three Ministries
- UK Cyber Essentials
- UK Security and Data Protection Toolkit

You can request compliance documents from an Oracle sales representative and access them directly from your OCI Console. See Advisory: Oracle Cloud Infrastructure and the General Data Protection Regulation (GDPR) to help you meet European Union General Data Protection Regulation (GDPR) requirements with OCI services. See FedRAMP Marketplace for FedRAMP details.

Oracle Corporate Security Practices

Oracle Corporate Security Practices 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
- Human Resources Security
- Access Control
- Network Communications Security
- Data Security
- Laptop and Mobile Device Security
- Physical and Environmental Security
- Supply Chain Security and Assurance

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. 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 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.

Oracle Data Processing Agreement

The Oracle Data Processing Agreement for Oracle Services applies to Oracle's Processing of Personal Information (PI) on Your behalf as a Processor for the provision of the Services specified in Your Services Agreement. It describes how Oracle controls, protects, and PI, such as:

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

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

Oracle Cloud Services Agreement

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

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

Important Cloud Services Agreement information is shown below.

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

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

The Oracle Consensus Assessment Initiative Questionnaire (CAIQ) 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

Oracle Cloud Hosting and Delivery Policies 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 describes Oracle service credit remediation in cases where Oracle services are not delivered to 99.95% uptime, shown below:

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

Monthly Uptime Percentage: Service Credit Percentage

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

60-Day Access Period After Service Termination

Oracle Cloud Hosting and Delivery Policies indicates 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."

.

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