Oracle OCI Exadata Database Service on Dedicated Infrastructure Security Controls

ORACLE

Exadata Database Service on Dedicated Infrastructure Security Controls

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

April 12, 2023 | Version 2.19

PURPOSE STATEMENT

This document provides an overview of features and enhancements included in Exadata release 20.1.13.0.0.210817. It is intended solely to help you assess the business benefits of upgrading to Exadata release 20.1.13.0.0.210817 and to plan your I.T. projects.

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

- Oracle Cloud Infrastructure Security Architecture[1]
- Oracle Cloud Infrastructure Security Guide[2]
- Oracle Corporate Security Practices[3]
- Exadata Database Service on Dedicated Infrastructure Security Guide[4]

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.

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

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

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

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

TABLE OF CONTENTS

LIST OF IMAGES

LIST OF TABLES

INTRODUCTION

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

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

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

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[5] for relevant detail about a specific standard for ExaDB-D. Please note that this information is subject to change and may be updated frequently, is provided "as-is" and without warranty and is not incorporated into contracts.

You may request compliance documents from an Oracle sales representative, and you may access them directly from their OCI Cloud Console.[6]

ORACLE CORPORATE SECURITY POLICIES

Oracle's security policies cover the management of security for both Oracle's internal operations and the services, including the ExaDB-D service, Oracle provides to its customers, and apply to all Oracle personnel, such as employees and contractors. These policies are aligned with the ISO/IEC 27002:2013 (formerly known as ISO/IEC 17799:2005) and ISO/IEC 27001:2013 standards and guide all areas of security within Oracle. Oracle's published Corporate Security Practices[7] including the following information:

- Objectives[8] – help protect the confidentiality, integrity, and availability of both Oracle and customer data
- Human resources security[9]
- Access control[10]
- Network communications security[11]
- Data security[12]
- Laptop and mobile device security[13]
- Physical and environmental security[14]
- Supply Chain Security and Assurance[15]

---

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

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

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

[8] https://www.oracle.com/corporate/security-practices/corporate/objectives.html

[9] https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html

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

[11] https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html

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

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

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

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

ROLES AND RESPONSIBILITIES

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

- Customer managed services: components that the customer can control as part of their subscription to ExaDB-D
  - Customer accessible virtual machines (VM)
  - Customer accessible database services
- Oracle managed infrastructure: hardware that is owned and operated by Oracle to run customer accessible services
  - Power Distribution Units (PDUs)
  - Out of band (OOB) management switches
  - Storage networking switches
  - Exadata Storage Servers
  - Physical Exadata Database Servers
- Oracle managed cloud control plane services
  - Customer web UI and API interfaces
  - Publicly accessible services and endpoints, such as OCI cloud services
  - Privately accessible endpoints, such as OCI Fast Connect
  - OCI cloud automation for the purposes of orchestrating OCI cloud services

Customers control and monitor access to customer services, including network access to their VMs via OCI Virtual Cloud Networks (VCN),[16] OCI Network Security Lists,[17] OCI VCN Flow Logs,[18] authentication to access the VM via token-based `ssh`,[19] and authentication to access databases running in the VMs via Oracle database authentication methods[20]. Oracle controls and monitors access to Oracle-managed infrastructure components. Oracle staff are not authorized to access customer services, including customer VMs and databases. Table 1 summarizes the division of roles and responsibilities for Oracle and the customer. The Exadata Database on Dedicated Infrastructure Service Description[21] and Exadata Database Service on Dedicated Infrastructure - Explanation of Cloud Operations Service (Doc ID 2875973.1)[22] provides further detail.

Table 1: Roles and Responsibilities

WORK FUNCTION	ORACLE MANAGED INFRASTRUCTURE		CUSTOMER MANAGED SERVICES	
	Oracle Cloud Ops	Customer	Oracle Cloud Ops	Customer
Monitoring	Infrastructure, Control Plane, Hardware Faults, Availability, Capacity	Not Appliable	Infrastructure availability to support customer monitoring of customer services	Monitoring of Customer OS, Databases, VMs, and Apps
Incident Management & Resolution	Incident Management and Remediation Spare Parts and Field Dispatch	Not Appliable	Support for any incidents related to the underlying platform	Incident Management and resolution for Customer's Apps
Patch Management	Proactive patching of Hardware, IaaS control software, hypervisor, and any applicable Oracle-	Not Appliable	Staging of available patches (e.g., Oracle DB patch set) per Maintaining an Exadata Database Service on Dedicated	Patching of tenant instances Testing

[16] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/overview.htm
[17] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/securitylists.htm#Security_Lists
[18] https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/vcn_flow_logs.htm
[19] https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/exaconnectingDB.htm
[20] https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/exaconnectingDB.htm
[21] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecscm/exa-service-desc.html
[22] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2875973.1

	managed infrastructure components		Infrastructure[23] documentation	
Backup & Restoration	Infrastructure and Control Plane backup and recovery, recreate customer VMs	Not Appliable	Provide running and customer accessible VM	Snapshots / Backup & Recovery of customer's IaaS data using Oracle native or 3rd party capability
Cloud Support	Response & Resolution of SR related to infrastructure or subscription issues	Submit SRs via My Oracle Support (MOS)	Response & Resolution of SR	Submit SRs via My Oracle Support (MOS)

EXADB-D SERVICE ARCHITECTURE

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

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

Customers deploy and manage ExaDB-D and database services using the Oracle Cloud Infrastructure Console and REST APIs. The customer controls access to the cloud automation's management functionality via the OCI Identity and Access Management (IAM)[24] service, and the OCI Audit[25] service provides the customer with a record of all customer-initiated management actions invoked via the OCI Console or OCI REST endpoints, such as creating or deleting databases. The customer controls network access to the ExaDB-D customer VM and database services running on the ExaDB-D service via OCI Virtual Cloud Networks.[26] Oracle controls network access the ExaDB-D infrastructure for cloud automation and for Oracle staff with a need to maintain the service.

Network Block Diagram

Figure 1 summarizes the network architecture block diagram for ExaDB-D, and the Oracle Exadata Database Service on Dedicated Infrastructure Technical Architecture[27] product documentation provides further detail. Customer accessible and controlled components are shown in blue. Oracle managed components dedicated to the specific customer (single tenant) are shown in red. Oracle managed infrastructure that is shared among OCI tenants is shown in green. The ExaDB-D Database (DB) Servers and Storage Servers shown in red, are interconnected via an isolated layer 2 management network, also shown in red. There is no direct network access from the management network to the customer client and backup networks.

[23] https://docs.oracle.com/en-us/iaas/Content/Database/Concepts/examaintenance.htm
[24] https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm
[25] https://docs.oracle.com/en-us/iaas/Content/Audit/Concepts/auditoverview.htm
[26] https://www.oracle.com/cloud/networking/virtual-cloud-network/
[27] https://docs.oracle.com/en/engineered-systems/exadata-cloud-service/ecsid/

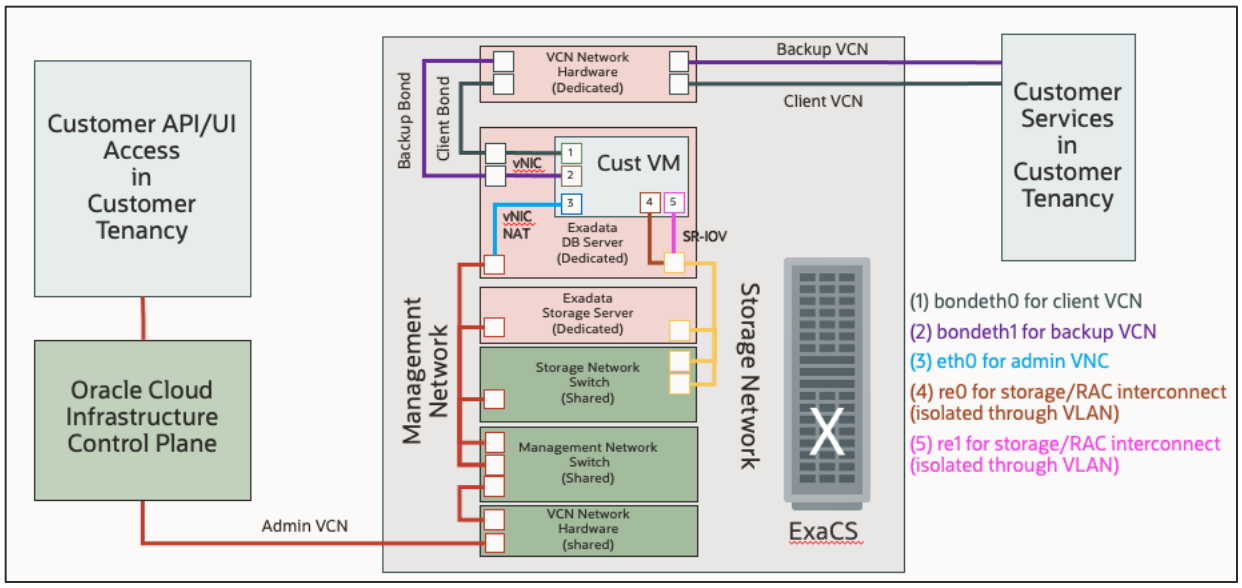

Figure 1: Network Architecture block diagram for Oracle Exadata Database Service on Dedicated Infrastructure

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

The customer VM accesses Exadata Storage via a private, non-routed interconnect network via SR-IOV mapped interfaces, shown in yellow. Each physical Exadata Database Server and Storage Server has a Highly Available (HA) (active/standby) connection to a pair of redundant storage networking switches.

A subset of Oracle cloud automation functionality accesses the customer VM via a NAT address on the management VCN implemented on a vNIC in the Exadata Database Server, shown in blue. Oracle cloud automation access to the customer VM is controlled via token based `ssh`. Temporary and unique `ssh` key pairs are generated by Oracle cloud automation to access the customer VM for each customer-initiated management action. The public key is injected by the cloud automation through the DBCS agent into the `~/.ssh/authorized_keys` files of the necessary service account in the customer VM, such as `oracle`, `opc, grid`, or `root`. The temporary private keys used by the automation is stored in memory Oracle cloud automation software running in the ExaDB-D hardware in the customer's data center and discarded after the action is completed. Likewise, the cloud automation software removes the temporary public key from the service account when the action is completed.

The port matrix describing running processes, TCP port numbers, and userids for running processes deployed in the customer VM is published in the Security Guide for Oracle Exadata Database Service on Dedicated Infrastructure Security Guide.[28] This guide describes security for an Exadata Cloud Infrastructure and includes information about the best practices for securing the Exadata Cloud Infrastructure.

Customer Access to ExaDB-D Services

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

Actions to manage infrastructure components, such as OCPU scaling and creating a Virtual Machine (VM) Cluster, are executed by the customer utilizing the cloud automation hosted in the OCI control plane. Customers do not have to manage the infrastructure layer as Oracle performs infrastructure management to support the 99.95% service uptime published in the Oracle PaaS and IaaS

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

Public Cloud Pillar Documentation.[29] Customers are not authorized to directly access ExaDB-D infrastructure, load monitoring agents, or directly pull or push files to the Oracle managed infrastructure in the ExaDB-D service.

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

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

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

Customer Access to OCI Interfaces

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

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

The OCI Terraform Provider[30] may be used to deploy and manage ExaDB-D. Documentation for the Hashicorp Terraform software is available from Hashicorp.[31]

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

- DBaaS UI/API sends request to DB Control Plane via https
- DB Control Plane sends the request via REST API to the ExaDB-D Admin VCN
  - Actions that require access to Database Services in the customer VM are sent to the DB Agent running in any or all the customer VMs (e.g., up to 4 VMs in a half rack) via a secure connection (mTLS) between the OCI control plane and each DB Agent; this mTLS connection is implemented through the private interconnect network in the ExaDB-D rack; the port matrix for software processes running in the customer VM is published in the Exadata Database Service on Dedicated Infrastructure Security Guide[32]
  - Actions that require access to the customer VM are executed via token-based `ssh` over the internal management network implemented as a NAT address on the customer VM that is accessible from the Exadata Database Server; the public `ssh` keys are temporary, generated for the purpose of the customer-invoked management action, and are stored in the `authorized_keys` files of the `oracle`, `opc`, `grid`, and `root` users in the customer VM; the private `ssh` keys are temporary, generated for the purpose of the customer-invoked management action, and stored in-memory by the Oracle cloud automation software running in the Exadata hardware stored in the customer's data center
  - Actions that require access to infrastructure components are issued via token-based `ssh` over the internal management network to the required endpoint (e.g., Exadata Storage Server, Exadata Database Server)

[29] https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf

[30] https://docs.oracle.com/en-us/iaas/Content/API/SDKDocs/terraform.htm

[31] https://registry.terraform.io/providers/hashicorp/oci/latest/docs

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

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

Oracle Infrastructure Monitoring

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

- Automated monitoring on Oracle Cloud Service infrastructure components sends Infrastructure Monitoring Metrics (IMM) to monitoring servers in the OCI control plane
  - Chassis temperature, drive status, etc.
  - Details for all monitoring data are published at Auto Service Request Qualified Engineered Systems Products[33]
- Oracle Support analyzes monitoring data, determines which events require correction, creates support tickets, and assigns support tickets to OCI support staff
- After being assigned a ticket, Cloud Ops support staff are authorized and dispatched to perform required support actions

Details related to monitoring data are published in Oracle Support Document 2875973.1 (Exadata Database Service on Dedicated Infrastructure - Explanation Of Cloud Operations Service).[34]

Software Updates

Standard quarterly bundle patches for the Oracle database, Grid Infrastructure, and customer VM operating system are staged to OCI Object Storage by Oracle. The quarterly software updates are listed for the customer in the cloud automation user interfaces, and application of those patches is controlled by the customer via OCI tools and policies. Patches are accessed directly from OCI Object Storage managed by Oracle. Quarterly patch information is available from Oracle Critical Patch Updates, Security Alerts and Bulletins.[35] My Oracle Support Document 2333222.1, Exadata Cloud Software Versions[36] provides information about current and historical software versions available for ExaDB-D. Oracle Cloud Infrastructure Maintenance documentation[37] describes the infrastructure update process, and the Patch and Update Exadata Cloud Infrastructure System documentation[38] describes the customer-managed update process for the customer VM, Grid Infrastructure, and Oracle database software.

Software updates for infrastructure components are deployed by Oracle cloud automation and Oracle staff, as required by the specific software updates. When possible, updates are applied to the running system, and without downtime, using tools like Linux ksplice. If an update requires a component restart, which is typical in a quarterly patch event, Oracle performs the component restart in a Real Application Cluster (RAC) rolling fashion to ensure service availability during the update process.

Security maintenance,[39] performed alongside the quarterly maintenance, is executed in months when important security updates are needed and includes fixes for vulnerabilities with CVSS scores greater than 7.

Security maintenance, when needed, is scheduled to be applied during a 21-day window that begins after the 15th of each month. Customers will receive notification of the proposed schedule at least 7 days before the start of the monthly maintenance window and can reschedule monthly maintenance to another date in the window if desired. Monthly security maintenance contains fixes for all security vulnerabilities identified during the previous month's scans. Updates to database servers are applied online via Ksplice technology, while updates to storage servers are applied in a rolling fashion. The Configuring Oracle-Managed Infrastructure Maintenance product documentation[40] details how maintenance is scheduled and performed for ExaDB-D.

---

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

[34] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2875973.1

[35] https://www.oracle.com/security-alerts/

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

[37] https://docs.oracle.com/en-us/iaas/exadatacloud/exacs/exa-conf-oracle-man-infra.html#GUID-C4301E26-E809-438F-96D7-9C6BB02FEA7F

[38] https://docs.oracle.com/en-us/iaas/exadatacloud/exacs/ecs-patch-update.html

[39] https://docs.oracle.com/en-us/iaas/exadatacloud/exacs/exa-conf-oracle-man-infra.html#GUID-A2008207-3683-424F-9279-F632BF4C9076

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

PREVENTIVE CONTROLS

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

Customer Access Controls

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

- User Authentication
  - Credentials to access OCI services
  - Credentials to customer VM operating systems and database administration accounts
  - Credentials for database users to access databases and database data
- Network Access
  - OCI VCNs and Security Lists to control layer 2 and 3 access to customer VMs
  - Network access rules implemented in the customer VM operating system and Oracle database
- Database Encryption
  - Application to database encryption[41]
  - Transparent Database Encryption (TDE) for user tablespaces[42]

Customer Access Control for ExaDB-D Services

Customers perform management actions via OCI automation by making an https connection to the Oracle Cloud Control Plane in the OCI region chosen by the customer. The customer is authenticated using their OCI Identity and Access Management (IAM)[43] credentials, and customer actions are controlled via OCI IAM permissions configured by the customer for specific resources. If the customer user is authorized to perform the requested management action on the target resource, then the requested command is sent to the appropriate ExaDB-D components by Oracle-controlled service VCNs.

Customers and database applications access databases running on the ExaDB-D via OCI VNICs attached to the customer VM. Access to databases and operating system is made via customer managed credentials.[44]

Customer Controls for Data Security

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

- Customer retains control over named and privileged (e.g., `SYS`, `SYSTEM`) user authentication and access to customer database
- Customer retains control over named and privileged (e.g., `root`, `opc`, `oracle`, `grid`) user authentication and access to customer VM
- Access to customer VM is logged by the customer VM operating system, these logs are available to the customer, and the customer can send these logs to other security information event management (SIEM) systems of their choice
- Customer can install monitoring agents and security controls of their choice on the customer VM operating system if these agents don't modify the Linux kernel or interfere with Exadata operation[45]
- Network connections to the Oracle database are designed to be protected by Oracle Native Network Encryption, which is automatically configured by cloud automation
- Oracle user tablespace database data is protected by Oracle Transparent Data Encryption (TDE) keys

---

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

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

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

[44] https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/exaconnectingDB.htm

[45] Oracle does not test or support 3rd party software with ExaDB-D; customers should check with 3rd party providers to ensure the 3rd party provider has tested and validated their software with ExaDB-D and that the 3rd party provider can support their software on ExaDB-D

  - Automatically configured by cloud automation and stored in password protected, PKCS12 wallet file stored in the file system of the customer VM
  - Customer controls access to TDE encryption keys via the wallet password
  - Customer can secure the TDE master key to the OCI Vault[46] service
- Oracle Database Vault,[47] a feature of the Oracle database software, may be configured by customers to help protect user data access from database administrators

Controls to Protect Data in Flight, While Processing, and at Rest

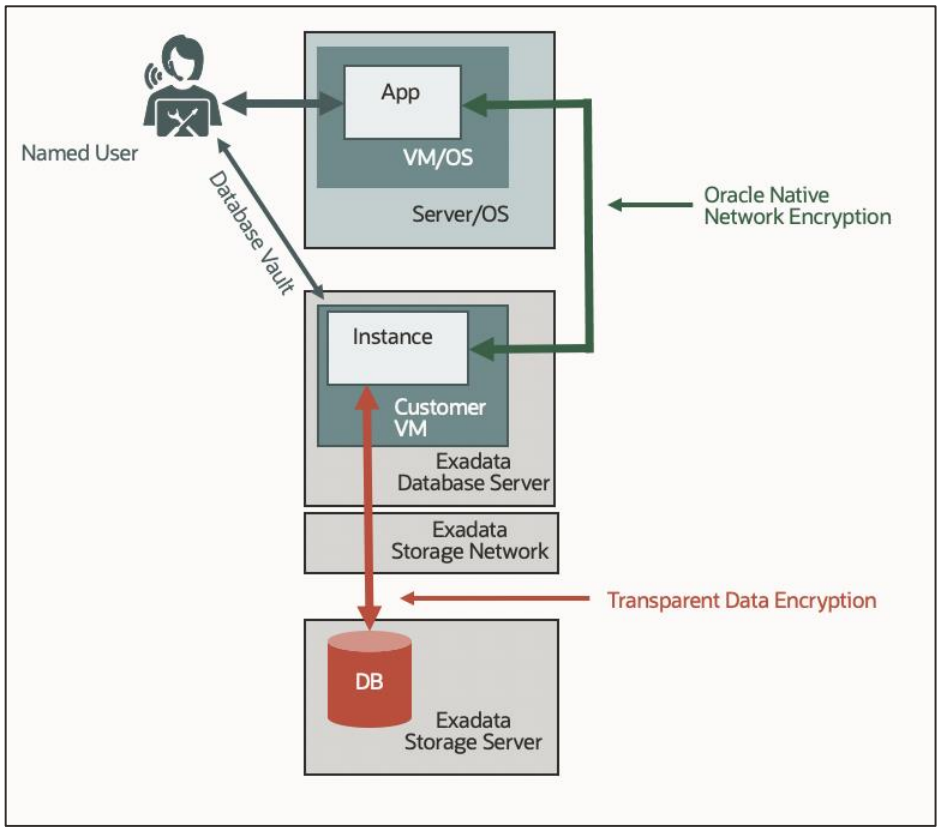

Figure 2 shows additional controls within the Oracle Database that protect customer data access from people or software that can gain access to infrastructure and customer VM components:

- Oracle Native Network Encryption[48]
- Oracle Database Vault[49]
- Oracle Transparent Database Encryption (TDE)[50]

[46] https://www.oracle.com/security/cloud-security/key-management/
[47] Oracle Database vault is included with Enterprise Edition Extreme Performance subscription, and is not included with a Bring Your Own License (BYOL) subscription
[48] Included with Enterprise Edition Extreme Performance subscription and with Bring Your Own License (BYOL) subscription
[49] Included with Enterprise Edition Extreme Performance subscription, not included with Bring Your Own License (BYOL) subscription
[50] Included with Enterprise Edition Extreme Performance subscription and with Bring Your Own License (BYOL) subscription

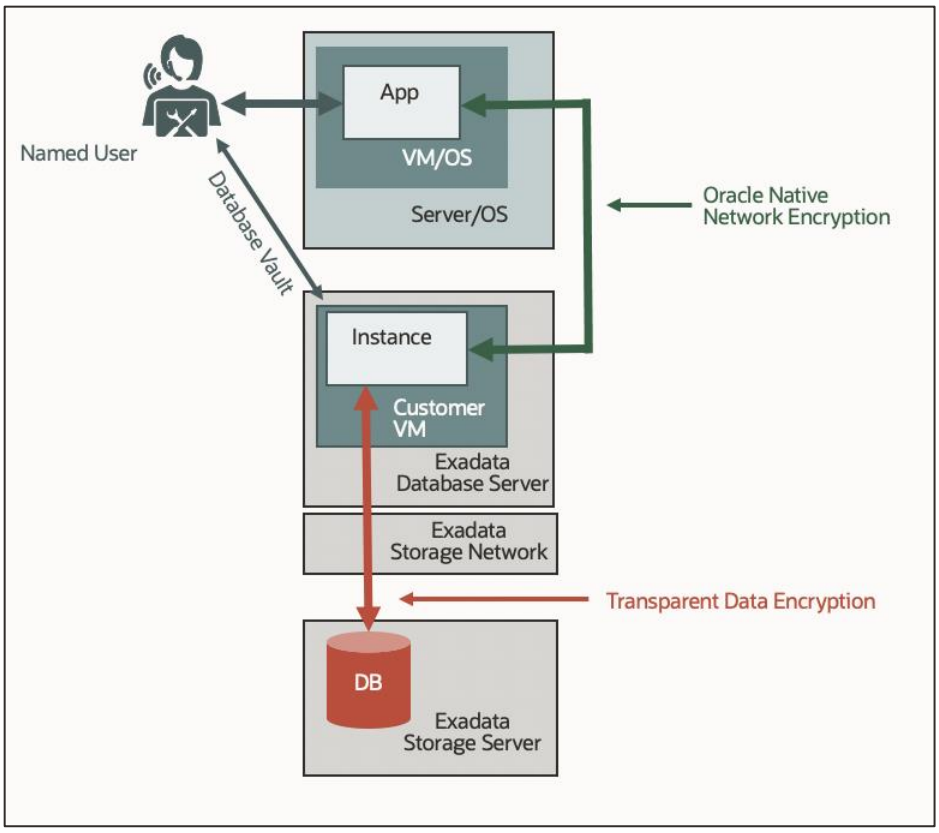

Figure 2: Controls to protect data in flight, while processing, and at rest

Oracle Native Network Encryption

Oracle Native Network Encryption helps to protect data in flight between the application and the Oracle database instance and is automatically configured for databases created via the ExaDB-D automation. When Oracle Native Network Encryption is enabled, access to infrastructure components that can observe network packets does not provide access to customer data because the data is encrypted. Documentation for Oracle Native Network Encryption is published in the Security Guide[51] for each Oracle Database version.

Oracle Database Vault

Oracle Database Vault security controls are designed to help protect application data from database administrator access and help address privacy and regulatory requirements. You can deploy controls to block database administrator access to application data and control sensitive operations inside the database using trusted path authorization. Oracle Database Vault helps to secure existing database environments transparently, eliminating costly and time-consuming application changes. Customers are responsible for configuring and managing Oracle Database Vault via Oracle database software methods. Documentation for Oracle Database Vault is published in the Oracle Database Vault Administrator's Guide[52] published for each database version.

Oracle Transparent Data Encryption and OCI Vault Service

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

---

[51] For Oracle database 19c, see https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-network-data-encryption-and-integrity.html - GUID-7F12066A-2BA1-476C-809B-BB95A3F727CF

[52] For Oracle Database 19c, see https://docs.oracle.com/en/database/oracle/oracle-database/19/dvadm/introduction-to-oracle-database-vault.html#GUID-0C8AF1B2-6CE9-4408-BFB3-7B2C7F9E7284

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

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

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

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

- TDE for Oracle Database 19c[53]
- TDE for Oracle Database 18c[54]
- TDE for Oracle Database 12.2.0.1[55]
- TDE for Oracle Database 12.1.0.2[56]
- TDE for Oracle Database 11.2.0.4[57]

The Oracle TDE FAQ[58] provides answers to common Oracle TDE architecture and implementation questions.

Controls for cloud automation Network Access to Customer VM

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

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

The customer VM provides the Oracle Linux packet filtering software[59] as an additional data protection control to block network to the customer VM. The Oracle Linux firewall, `iptables` or `firewalld`, can be configured to block control plane access at layers 3 (IP) and 4 (TCP port). Customers may configure the operating system firewall to help address their specific security requirements.

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

Oracle cloud automation secure login via token-based `ssh` is not compatible with Kerberos authentication, and parts of the Oracle cloud automation functionality may cease to function if customers implement Kerberos authentication in the customer VM. Oracle does not support customers configuring Kerberos operating system authentication in the customer VM because this action breaks the cloud automation. Customers may configure Kerberos authentication for Oracle database user authentication. For details, please see Oracle Support Document 2621025.1 (Does ExaCC VM's Support Kerberos Authentication).[60]

Controls for Customer Staff Access to Customer VM

---

[53] https://docs.oracle.com/en/database/oracle/oracle-database/19/asoag/introduction-to-transparent-data-encryption.html#GUID-62AA9447-FDCD-4A4C-B563-32DE04D55952

[54] https://docs.oracle.com/en/database/oracle/oracle-database/18/asoag/introduction-to-transparent-data-encryption.html#GUID-62AA9447-FDCD-4A4C-B563-32DE04D55952

[55] https://docs.oracle.com/en/database/oracle/oracle-database/12.2/asoag/configuring-transparent-data-encryption.html#GUID-C5D20EAE-3369-411F-9A7E-13AB14139F1D

[56] https://docs.oracle.com/database/121/ASOAG/configuring-transparent-data-encryption.htm#ASOAG10474

[57] https://docs.oracle.com/cd/E11882_01/network.112/e40393/asotrans.htm#ASOAG600

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

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

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

Access to the customer VM is implemented via token-based `ssh`. Customers use their OCI Cloud Tenancy credentials and controls to add customer-specified public keys to the `/home/oracle/opc/.ssh/authorized_keys` file of the `opc` user. Customer staff with access to the private keys associated with the installed public keys can gain access to the customer VM via token-based `ssh`. Oracle cloud automation does not integrate with customer key management systems, and customers can manage `ssh` keys using technology compatible with Oracle Linux.

As of Exadata software version 22.1.4.0.0.221020, Microsoft Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) authentication to the customer VM can be implemented by customers on ExaDB-D. ExaDB-D does not provide cloud automation support for this configuration. Customers can configure AD and LDAP by directly accessing the ExaDB-D customer VM to implement AD and LDAP. Customers should note that the ExaDB-D customer VM updates[61] are executed as image updates using the Exadata Database Machine image update process,[62] and that customers should test and validate how their AD or LDAP implementation is affected by the image update process. Customers should plan for the possibility of needing to temporarily disable or remove AD or LDAP during a patch cycle, and then reinstate AD or LDAP following the patch if the implementation of AD or LDAP is not compatible with the image update process.

Controls for Protecting Against Theft of Data

User tablespace data in ExaDB-D databases is protected by Oracle Transparent Data Encryption (TDE). Theft of encrypted data is of limited use, due to the technical difficulty of decrypting the data. The United States Department of Defense (DoD) and National Security Agency (NSA) endorse AES encryption standards to secure data. Reference NSA guidelines[63] and NIST standards[64] for further detail.

Oracle's Corporate Security Practices[65] cover the management of security for Oracle's internal operations and the cloud services, including ExaDB-D, Oracle provides to its customers, and apply to all Oracle personnel, such as employees and contractors. These policies are aligned with the ISO/IEC 27002:2013 (formerly known as ISO/IEC 17799:2005) and ISO/IEC 27001:2013 standards and guide all areas of security within Oracle. Oracle. Oracle security practices are published at.

Oracle Data Safe

Oracle Data Safe[66] is a security cloud service that is included with your Exadata Cloud at Customer subscription. Data Safe helps you:

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

There is no additional cost to use Data Safe so long as you do not exceed one million audit records per database in a month.

Oracle Data Safe Technical Architecture[67] includes functionality that supports an on-premises connector deployed on customer-controlled servers to facilitate connecting databases running on ExaDB-D to connect to the OCI Data Safe service in an OCI region.

Oracle Database Security Assessment Tool (DBSAT)

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

---

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

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

[63] https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm

[64] https://www.nist.gov/publications/advanced-encryption-standard-aes

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

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

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

DBSAT is provided at no additional cost and is designed to enable customers to quickly find:

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

DBSAT analyzes information in the database and listener configuration to identify configuration settings that may unnecessarily introduce risk. DBSAT goes beyond simple configuration checking, examining user accounts, privilege and role grants, authorization control, separation of duties, fine-grained access control, data encryption and key management, auditing policies, and OS file permissions. DBSAT applies rules to quickly assess the current security status of a database and produce findings in all the areas above. For each finding, DBSAT recommends remediation activities that follow best practices to reduce or mitigate risk. By applying the comprehensive measurements and compensating controls described by DBSAT, customers can reduce data exposure risk throughout their enterprise. Oracle DBSAT is available for download from Oracle.[68]

Oracle Controls for Cloud Operations Access to Infrastructure Components

Oracle Cloud Ops staff are not authorized to access customer VMs, databases, or database data under normal operating conditions[69]. Oracle Cloud Operations staff are authorized to access and support ExaDB-D infrastructure components, which include the following equipment:

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

Oracle Technical Controls

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

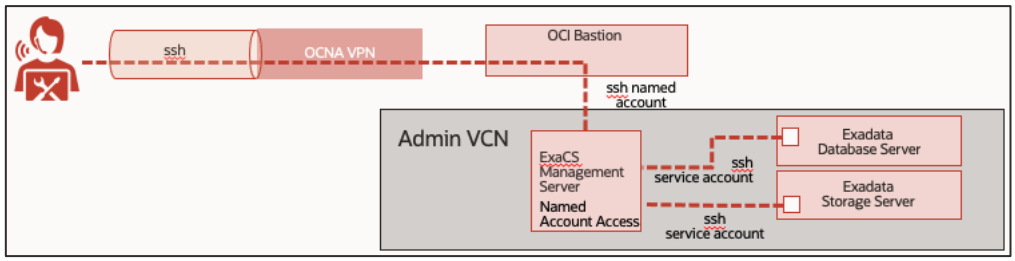

Figure 3: Cloud Operations Staff Access to ExaDB-D Infrastructure Components

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

- Access Oracle Cloud Network Attach (OCNA) using FIPS 140-2 level 3 hardware MFA (Yubikey) based on entitlements specific to job code
- Access to Bastion and Management servers for the purposes of `ssh` access to ExaDB-D infrastructure
  - Access to ExaDB-D management servers is implemented as a tunnel through the Bastion server isolated to OCI privileged administrative VCN located in the OCI region hosting the service
  - Connections through Bastion servers are logged and monitored by Oracle
- Login to management servers dedicated to managing ExaDB-D infrastructure as a named user via `ssh` using MFA implemented with a FIPS 140-2 Level 3 hardware token (Yubikey)
  - Access to the management server is controlled based on Oracle's published least privileged access policies[70]
  - Connections to the ExaDB-D infrastructure are logged and monitored by Oracle
- Log into the ExaDB-D infrastructure using the required service account using token-based `ssh`

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

[69] Exception conditions that can permit Oracle staff to access customer VMs are described in Exception workflows - Oracle Access to Customer VM

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

- Command execution is traceable to a specific named user via audit logging implemented in the ExaDB-D infrastructure
- Connections to infrastructure components are logged and monitored by Oracle

Oracle Process Controls

Oracle's Access Control[71] security practice restricts access to Oracle staff with a need to know and need to access ExaDB-D infrastructure, and include the following policies:

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

Exadata Infrastructure Software Security and Controls

ExaDB-D is based on the Exadata Database Machine and delivers the enterprise-class security features of Exadata Database Machine[72] in an on-premises cloud model. Security features of ExaDB-D include the following:

- Software deployed on ExaDB-D infrastructure is limited to the minimum software components to run customer services
- Development and debug tools to inspect customer data are not installed on ExaDB-D infrastructure
- Non-essential operating system tools and packages are not installed on ExaDB-D infrastructure
- Software development performed under Oracle Software Security Assurance[73]
- Security architecture performed under Oracle Corporate Security Architecture[74]

DETECTIVE CONTROLS (LOGGING AND AUDITING)

ExaDB-D provides robust detective controls (auditing and logging) for customer services and Oracle managed infrastructure. The customer controls the logging configuration of customer services, and Oracle controls the logging configuration of Oracle managed infrastructure. Oracle is not authorized to access customer service audit logs. The customer may request access to applicable Oracle audit log information via the Oracle service request (SR) process, and customers may view their audit rights in the Oracle Data Processing Agreement (DPA).[75]

Customer Audit Logging

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

- OCI Audit Service:[76] audit logs for control plane actions (e.g., web UI, OCI CLI, OCI REST API) initiated via a customer's OCI IAM credential
- Oracle database auditing:[77] audit logs for database actions initiated via a customer's Oracle database credential
- Customer VM operating system audit log:[78] audit logs for actions initiated on a customer VM via an operating system credential

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

- Time the API activity occurred

---

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

- Source of the activity
- Target of the activity
- Type of action
- Type of response

Each log event includes a header ID, target resources, timestamp of the recorded event, request parameters, and response parameters. You can view events logged by the OCI Audit[79] service by using the Console, API, or the SDK for Java. Data from events can be used to perform diagnostics, track resource usage, monitor compliance, and collect security-related events.

Oracle database auditing tracks changes made to the Oracle database by database users and non-database users. Customers can configure and manage the Oracle database audit log, including sending the audit log a remote log server. Documentation for configuring, managing, and monitoring of Oracle database audit logs is published in the Oracle Database Security Guide[80] for each database version.

The customer VM operating system audit log is implemented as the audit log service for the Oracle Linux (OL) operating system running in the customer VM. The Oracle Linux audit log service records actions executed via operating system credentials, such as `root`, `oracle`, `opc`, and named users configured by the customer. Customers can configure the Oracle Linux audit log per their standards, including sending the Oracle Linux audit log to a remote log server. Documentation is published in the Oracle Linux Security Guide.[81]

Customer Security Scanning of Customer VM

Customers may use OpenSCAP[82] to scan the customer VM for compliance.

Customers may use the Oracle Linux Advanced Intrusion Detection Environment (AIDE)[83] to check file and directory integrity. AIDE is a small, yet powerful, intrusion detection tool automatically installed with the Linux Operating System, that uses predefined rules to check file and directory integrity. It is meant to protect the system internally, by providing a layer of protection against viruses, rootkits, malware, and detection of unauthorized activities. It is an independent static binary for simplified client/server monitoring configurations. It runs on demand, and the time to report changes is dependent on the system checks (usually at least once a day). The utility works by using a number of algorithms (such as, but not limited to, md5, sha1, rmd160, tiger), supports common file attributes and also supports regular expression parsers for file(s) to be included or excluded from the scan.

Customers have control to install third party software, including scanning software, on the ExaDB-D customer VM. Oracle will not provide technical support for non-Oracle software. This includes installation, testing, certification, and error resolution. The supplier of the custom/third party software is responsible for any technical support for it. It is highly recommended that all non-Oracle software be certified by the vendor for use in an Oracle Linux and/or Exadata environment and thorough testing is performed in the target environment by the customer and third party providers. Details for third party software support on ExaDB-D are published on My Oracle Support at Installing Third Party Software on Exadata Components (Doc ID 1593827.1).[84]

Customer security testing of the ExaDB-D customer VM must be done in accordance with Oracle Cloud Testing Policies.[85]

Oracle Audit Logging

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

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

---

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

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

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

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

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

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

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

  - `/var/log/audit.log`
  - `/var/log/secure`
  - `/var/log/xen/xend.log`
- Exadata Storage Server
  - `/var/log/messages`
  - `/var/log/audit.log`
  - `/var/log/secure`
- Storage Network Switch
  - `/var/log/messages`
  - `/var/log/audit.log`
  - `/var/log/secure`
  - `/var/log/opensm.log`

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

- ILOM
  - `syslog`
  - ILOM syslog redirected to the syslog of the physical infrastructure component
- Physical Exadata Database Server
  - `/var/log/messages`
  - `/var/log/secure`
  - `/var/log/audit/audit.log`
  - `/var/log/clamav/clamav.log`
  - `/var/log/aide/aide.log`
- Exadata Storage Server
  - `/var/log/messages`
  - `/var/log/secure`
  - `/var/log/audit/audit.log`

The retention period for infrastructure audit logs is 13 months. Infrastructure audit logs are stored in the OCI SIEM service and OCI Logging service and are accessible by the Oracle Incident Management team and OCI security teams. Customers may request access to infrastructure audit logs via the Oracle Service Request (SR) process. If a customer detects suspicious activity, the process is to log a security Service Request, provide applicable logs which will trigger an Oracle Security Operations Center (SOC) engagement. This review is performed by an independent team which works with the customer to investigate events.

RESPONSIVE CONTROLS

The customer and Oracle work together to secure and monitor access to customer services, databases, database data, VMs, and infrastructure. Should either party detect an unauthorized action, that party can take responsive action immediately and prior to notifying the other party, depending on security policy and the details and circumstances of the unexpected action. If the customer detects an unauthorized action, the customer should notify Oracle of the action and response via the Oracle Service Request process. Oracle will notify the customer of confirmed unauthorized actions and Oracle responses per Oracle's Incident Response Policy.[86]

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

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

SERVICE TERMINATION AND DATA DESTRUCTION

Customers may terminate their ExaDB-D instance as part of ExaDB-D Lifecycle Management Operations[87]. Terminating an Exadata Database Service on Dedicated Infrastructure resource permanently deletes it and any databases running on it. The terminate service functionality is implemented as Exadata Database Machine Secure Erase.[88] The Exadata Secure Eraser automatically detects the hardware capability of a storage device and picks the best erasure method supported by the device. Cryptographic erasure is used whenever possible to provide better security and faster speed. The cryptographic erasure method used by Secure Eraser is fully

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

[87] https://docs.oracle.com/en-us/iaas/Content/Database/Tasks/examanagingDBsystem.htm

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

compliant with the NIST SP-800-88r1 standard.[89] Customers may obtain secure erase certifications from Oracle by opening a My Oracle Support (MOS) request.

EXCEPTION WORKFLOWS - ORACLE ACCESS TO CUSTOMER VM

The ExaDB-D service does not authorize Oracle staff to access the customer VM under normal operating conditions. There are exception cases where a failure in the customer VM requires Oracle staff access to resolve the issue. The process and technical controls that govern when and how Oracle staff can access the customer VM depend on if the exception occurred before the customer could access the customer VM, or after the customer accessed the customer VM.

Case 1: Service exception before customer could log into customer VM

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

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

- As per the security policy associated with ExaCC service, Oracle personnel are prohibited to access customer DomU without customer's explicit permission. For Oracle to comply with this policy, Oracle staff must - get customer permission to access DomU[90] by asking the following question.
- "In order for us to resolve the issue described in this SR, we need customer's explicit permission allowing us to login to customer DomU. By giving us explicit permission to access DomU, you are confirming that there is no confidential data that is stored in customer DomU or associated databases and customer security team is authorizing Oracle to have access to customer DomU in order for Oracle to help fix this issue. Do I have your explicit permission to access DomU?"

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

Case 2: Service exception after customer could log into customer VM

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

The use cases for this method include the following:

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

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

- If a customer is willing to permit Oracle Cloud Ops to access the customer VM without direct customer supervision, then the customer opens a Service Request (SR) with the following language:
  - SR Title:
    - SR granting Oracle explicit permission to access a Guest VM of ExaCC with VM Name <insert VM Name as listed under the DB Server detail page→ Resources→ Virtual Machines>
  - SR Content:
    - We are opening this SR to grant explicit permission to Oracle to access our Guest VM in order for support to help resolve the issue described in SR# 1-xxxxxxxx. We acknowledge that by providing this permission, we understand that Oracle will have access to all files and memory that are part of the Guest VM. In addition, we also agree that the customer security team has authorized Oracle to have access to the customer Guest VM in order to resolve the issue described in the above SR.
    - DB Server OCID: <insert OCID of DB Server hosting the VM here>
    - VM Name: <insert VM Name as listed under the DB Server detail page→ Resources→ Virtual Machines>

[89] https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization

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

- If a customer requires Oracle to offer a shared screen to permit direct customer supervision of the Oracle cloud ops access, the customer opens a Service Request (SR) with the following language
  - SR Title:
    - SR granting Oracle explicit permission to access a Guest VM of ExaCC with VM Name <insert VM Name as listed under the DB Server detail page→ Resources→ Virtual Machines>
  - SR Content:
    - We are opening this SR to grant explicit permission to Oracle to access our Guest VM in a shared screen session in order for support to help resolve the issue described in SR# 1-xxxxxxxx. We acknowledge that by providing this permission, we understand that Oracle will have access to all files and memory that are part of the Guest VM. This permission to access our VM is contingent on our representative being able to monitor in real-time via a screen-sharing session all activities performed by Oracle. In addition, we also agree that the customer security team has authorized Oracle to have access to the customer Guest VM via this shared screen session in order to resolve the issue described in the above SR.
    - DB Server OCID: <insert OCID of DB Server hosting the VM here>
    - VM Name: <insert VM Name as listed under the DB Server detail page→ Resources→ Virtual Machines>

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

SUMMARY

With Exadata Database Service on Dedicated Infrastructure, security features throughout the customer VM and customer database are controlled by the customer. Oracle database encryption features encrypt data, and the customer retains control of the encryption keys. Oracle database security features control authentication and access to data in the database, and the customer retains control of this authentication and access. Oracle Linux authentication features control access to the customer's VM, and the customer retains control of this authentication and access.

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

Exadata Database Service on Dedicated Infrastructure delivers the benefit of a high-security on-premises deployment with the ease-of-use and economics of the cloud. Customers and Oracle Cloud Operations work together to implement system security and help prevent unauthorized access to and theft of customer data. Oracle Cloud Operations staff does not access customer networks, services, or data to deliver the service, and customers do not access Oracle-managed infrastructure to consume the service. In the Exadata Database Service on Dedicated Infrastructure deployment model, customers gain the security of an on-premises deployment with the benefits of cloud economics, agility, and scale.

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com facebook.com/oracle twitter.com/oracle

Exadata Database Service on Dedicated Infrastructure
Security Controls