ORACLE

Exadata Cloud@Customer Security Controls

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

February 8, 2021 | Version 1.01

PURPOSE STATEMENT

This document provides an overview of features and enhancements included in release 19.2.13.0.0.200428. It is intended solely to help you assess the business benefits of upgrading to 19.2.13.0.0.200428 and to plan your I.T. projects.

This document details security and control features of Oracle's Gen 2 Exadata Cloud@Customer (ExaC@C) service delivered through the Gen 2 Oracle Cloud Infrastructure (OCI) control plane. It is intended solely to help you assess the security features and controls of Exadata Cloud@Customer.

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

Exadata Cloud@Customer provides Oracle's public Exadata Cloud Service at a customer's data center using Oracle-owned and managed infrastructure located at a customer's data center. This document highlights compliance, security, access control, and auditing features of Exadata Cloud@Customer that help protect against unauthorized system access and use.

COMPLIANCE

The operational compliance standards of Exadata Cloud@Customer with the OCI control plane are governed by Oracle internal support processes and procedures. Exadata Cloud@Customer has gained attestations of compliance (AoC) from the following standards:

- ISO 27001
- Health Insurance Portability and Accountability Act (HIPAA)
- PCI DSS

ORACLE GLOBAL SECURITY POLICY

Oracle's security policies cover the management of security for both Oracle's internal operations and the services, including the Exadata Cloud@Customer 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 follows the security practices published at https://www.oracle.com/corporate/security-practices/corporate/. The published content includes the following detail:

- Objective – help protect the confidentiality, integrity, and availability of both Oracle and customer data
- Human resources security
- Access control
- Network communications security
- Data security
- Laptop and mobile device security
- Physical and environmental security

When Oracle is working on customer site or systems at customer direction, Oracle consultants and support staff will observe customer practices as agreed to between Oracle and the customer.

ROLES AND RESPONSIBILITIES

Exadata Cloud@Customer is jointly managed by the customer and Oracle. The Exadata Cloud@Customer deployment is divided into 2 areas of responsibility:

- Customer managed services: components that the customer can access as part of their subscription to Exadata Cloud@Customer
  - 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

Customers control and monitor access to customer services, including network access to their VMs (via layer 2 VLANs and firewalls implemented in the customer VM), authentication to access the VM, and authentication to access databases running in the VMs. 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 details the division of roles and responsibilities for Oracle and the customer.

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	Provide network access to support Oracle infrastructure log collection and monitoring	Infrastructure availability to support customer monitoring of customer services	Monitoring of Customer OS, Databases, Apps
Incident Management & Resolution	Incident Management and Remediation Spare Parts and Field Dispatch	Onsite Diagnostic Assistance (e.g., network troubleshooting)	Support for any incidents related to the underlying platform	Incident Management and resolution for Customer's Apps
Patch Management	Proactive patching of Hardware, IaaS/PaaS control stack	Provide network access to support patch delivery	Staging of available patches (e.g., Oracle DB patch set)	Patching of tenant instances Testing
Backup & Restoration	Infrastructure and Control Plane backup and recovery, recreate customer VMs	Provide network access to support cloud automation delivery	Provide running and customer accessible VM	Snapshots / Backup & Recovery of customer's IaaS and PaaS data using Oracle native or 3rd party capability
Cloud Support	Response & Resolution of SR' related to infrastructure or subscription issues	Submit SRs via MOS	Response & Resolution of SR	Submit SRs via Support Portal

EXADATA CLOUD@CUSTOMER SERVICE ARCHITECTURE

Figure 1 shows the architecture block diagram the Gen 2 Exadata Cloud@Customer service.

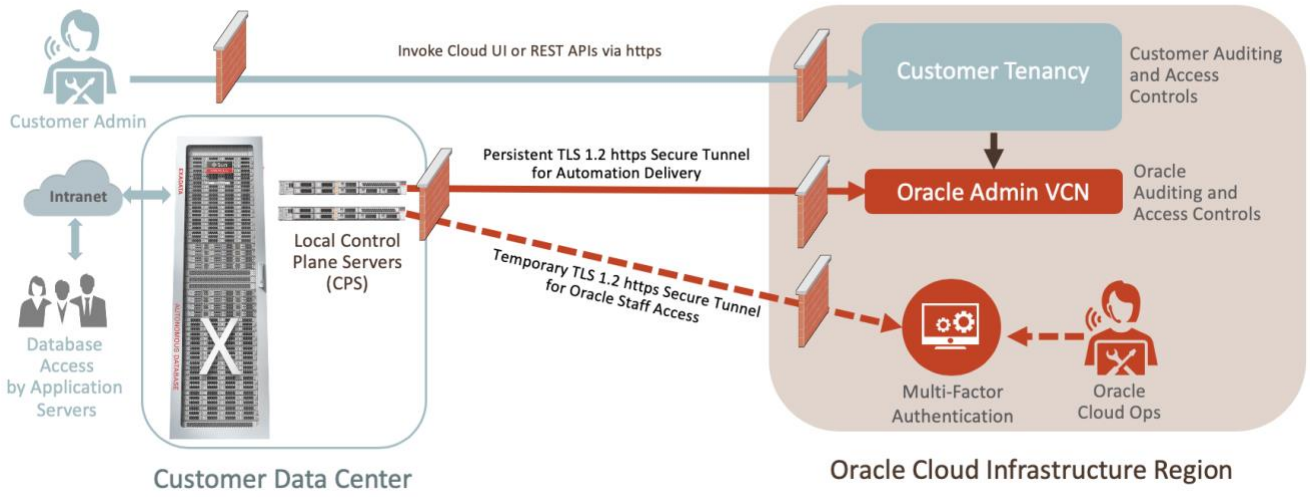

Figure 1: Architecture block diagram for Oracle Exadata Cloud@Customer

The Exadata Cloud@Customer service is deployed in an Exadata Cloud@Customer rack in a data center of the customer's choice. The Exadata Cloud@Customer rack contains all of the components of a standard Exadata Database Machine, plus 2 Control Plane Servers (CPS) in a highly available (HA) configuration that connect to an OCI region.

The customer's database data is secured in the on-premises Exadata Cloud@Customer rack, and all access to customer databases is made via network connections (intranet) the customer permits to access the VMs and databases in the Exadata Cloud@Customer 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, SYS) to customer VMs and databases, and the customer can act with those credentials to secure the VM and database to help address local 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 Exadata Cloud@Customer Compute VM operating system and Oracle database.

The OCI region performs remote delivery of the Exadata Cloud@Customer service, including customer-controlled cloud automation for database and system management and infrastructure maintenance and support. The customer controls access to the cloud automation's management functionality via the OCI Identity and Access Management (IAM) Service, and the OCI Audit 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. Oracle controls network access from the OCI region to the Control Plane Server, and operator access to perform infrastructure maintenance and support.

Control Plane Server Networking

The Exadata Cloud@Customer service requires no inbound TCP connection for service delivery, support, or management purposes. The Exadata Cloud@Customer service requires outbound TCP connections on port 443 to Oracle endpoints for the purposes of remote service delivery and management to the following Oracle services:

- OCI Persistent Secure Tunnel Service for Automation Delivery
  - Delivery of Cloud Automation via REST API calls
- OCI Temporary Secure Tunnel Service for Operator Access
  - Oracle operator access to Oracle managed components
- OCI Monitoring Service
  - Infrastructure Monitoring Metrics (e.g., hardware component health, intrusion detection, etc.)
- OCI Object Storage Service
  - Delivery of software updates
- OCI Identity Service
  - Authentication and authorization to access infrastructure components

The simplest configuration is for the customer to permit outbound https access to the Internet (TCP/443 for 0.0.0.0/* IP range) for faster deployment and service activation, easier management, and future service expansion.

Exadata Cloud@Customer supports IP address filtering. Specific Oracle services in a specific OCI region need to be whitelisted, as indicated by the OSN CIDR's for public IP address that are described at https://docs.cloud.oracle.com/iaas/tools/public_ip_ranges.json. Future Exadata Cloud@Customer features may require CPS access to other OCI service endpoints, and the IP addresses of OCI services may change within the scope of the IP addresses listed in the aforementioned document. To accommodate future service releases and service maintenance, customers should permit outbound CPS access to all of the OCI IP addresses listed in the OSN CIDR for their region.

Exadata Cloud@Customer supports http proxy (e.g., corporate proxy, passive proxy) to manage connections from the CPS to OCI endpoints. An http proxy adds deployment complexity, and maintenance to support future Exadata Cloud@Customer releases that may require access to additional OCI endpoints. Should customers choose to selectively permit access to URLs for specific OCI services, customers may need to update their permitted URLs when Oracle adds new features and services to Exadata Cloud@Customer.

The most restrictive access for Exadata Cloud@Customer Control Plane Server to OCI access is to enable access to 5 endpoints in a specific region: Identity Service, Object Storage Service, Monitoring Service, persistent secure tunnel service for Cloud Automation Delivery, and temporary secure operator tunnel service to provide Oracle Cloud Ops staff access to ExaC@C infrastructure. The public URLs for Identity Service, Object Storage Service, and Monitoring Service and detailed at the following documentation links:

- Identity Service (https://docs.cloud.oracle.com/en-us/iaas/api/#/en/identity/20160918/)
- Object Storage Service (https://docs.cloud.oracle.com/en-us/iaas/api/#/en/objectstorage/20160918/)
- OCI Monitoring Service (https://docs.cloud.oracle.com/en-us/iaas/api/#/en/monitoring/20180401/)
- OCI Persistent Secure Tunnel Service for Automation Delivery: https://wss.exacc.<oci_region>.oci.oraclecloud.com
- OCI Temporary Secure Tunnel Services for Operator Access: https://mgmthe1.exacc.<oci_region>.oci.oraclecloud.com and https://mgmthe2.exacc.<region>.oci.oraclecloud.com

The OCI Persistent Secure Tunnel Service for Automation Delivery is used for remote delivery of Cloud Automation commands (REST API calls, exclusively). This service is limited to Exadata Cloud@Customer and not part of OCI's public services. The URLs for this service are specific to the OCI region configured to manage the Exadata Cloud@Customer infrastructure.

The OCI Temporary Secure Tunnel Service for Operator Access is used exclusively for Oracle Operator Access (ssh) to Oracle Managed Exadata Cloud@Customer Infrastructure. This service is limited to Exadata Cloud@Customer, not part of OCI's public services. The URLs for this service are specific to the OCI region configured to permit Oracle Operator Access to the Exadata Cloud@Customer infrastructure. The OCI Temporary Secure Tunnel Service is the only path by which an Oracle Operator can use an ssh connection to gain access to the Exadata Cloud@Customer infrastructure.

The certificates for the TLS connectivity are managed by Oracle exclusively and rotated every 90 days. Customers are not permitted to manage the certificates or inspect the traffic contained in the secure connections.

The CPS requires a customer provided DNS for IP address resolution, and NTP server for clock synchronization.

Customer Access to Exadata Cloud@Customer Services

Customers access Oracle databases (DB) running on Exadata Cloud@Customer via a layer 2 (tagged VLAN) connection from customer equipment to the databases running in the customer VM using standard Oracle database connection methods, such as Oracle Net on port 1521. Customer's access the VM running the Oracle databases via standard Oracle Linux methods, such as token based ssh on 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 software in a tenancy designed with security in mind and hosted in the Oracle Cloud Infrastructure. Customers do not have to manage the infrastructure layer as Oracle maintains a 99.95% uptime SLO. Customers are not authorized to directly access Exadata Cloud@Customer infrastructure, load monitoring agents, or directly pull or push files to the Oracle managed infrastructure in the Exadata Cloud@Customer service.

Physical Network Implementation

Figure 2 describes the physical network implementation for Exadata Cloud@Customer. The customer accessible and controlled components are shown in blue, and the Oracle managed components are shown in red. The Exadata Cloud@Customer infrastructure components, shown in red, are interconnected via an isolated layer 2 management network, also shown in red. There is no direct network access from the management network to the customer client and backup networks.

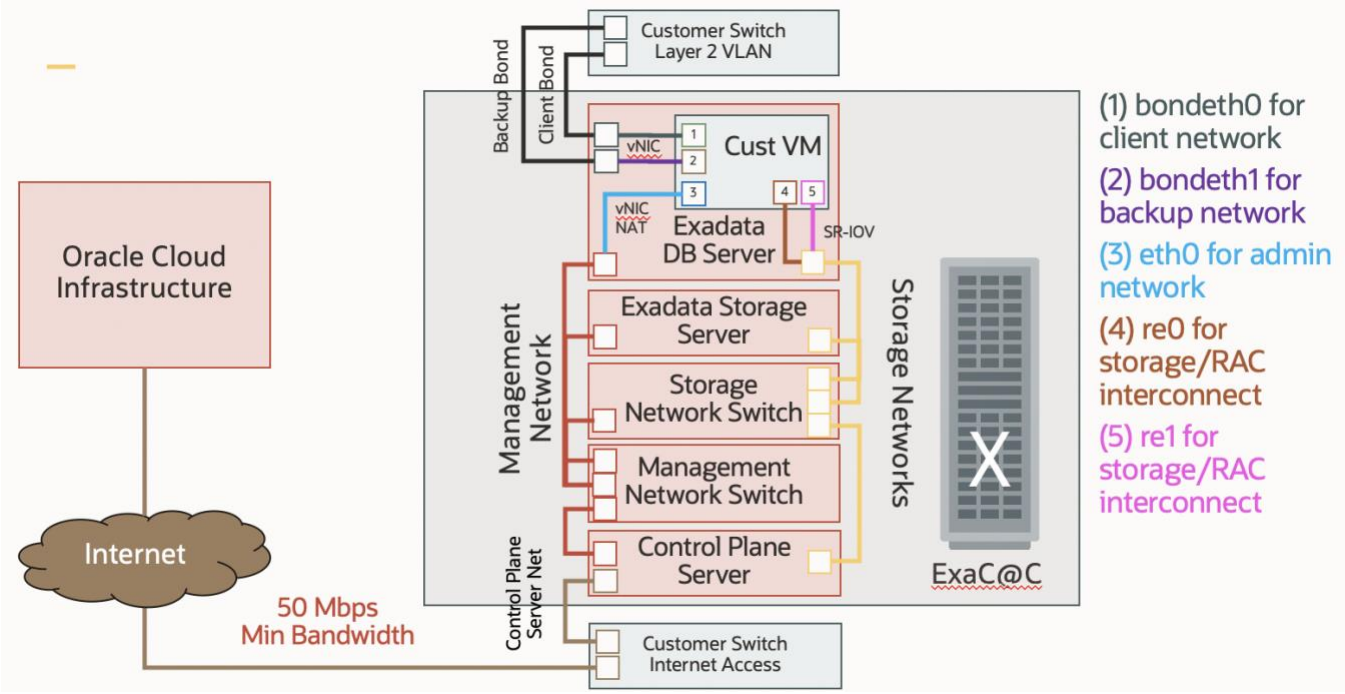

Figure 2: Exadata Cloud@Customer Physical Network Implementation

Figure 3 details the network isolation between different Virtual Machine Clusters (VM Clusters) deployed on the same Exadata Cloud@Customer Exadata Database Server (DB Server). When multiple VM clusters are configured, the customer controls the VLAN tags and IP networking configuration of each VM cluster, and the same physical links are shared for the client (indicated as network 1) and backup (indicated as network 1) networks for each VM on the same Exadata DB Server. Customers can specify different VLAN tags for different networks on different VM clusters to isolate network access into the VM cluster. The back-end storage networks of each VM cluster (networks 4 and 5) are isolated via layer 2 controls in the Converged Ethernet implementation that supports the back-end storage network, so there is no method for different VMs on the same Exadata Database Server to access each other via the back-end storage network. The vNIC/NAT admin network access (network 3) is implemented as an isolated /30 network so that there is no method for different VMs on the same Exadata DB Server to access one another on the admin network.

In addition to the network isolation, CPU cores are pinned to specific VMs on a given Exadata Database Server as a preventative control against in-VM executed methods to access cached data from other VMs.

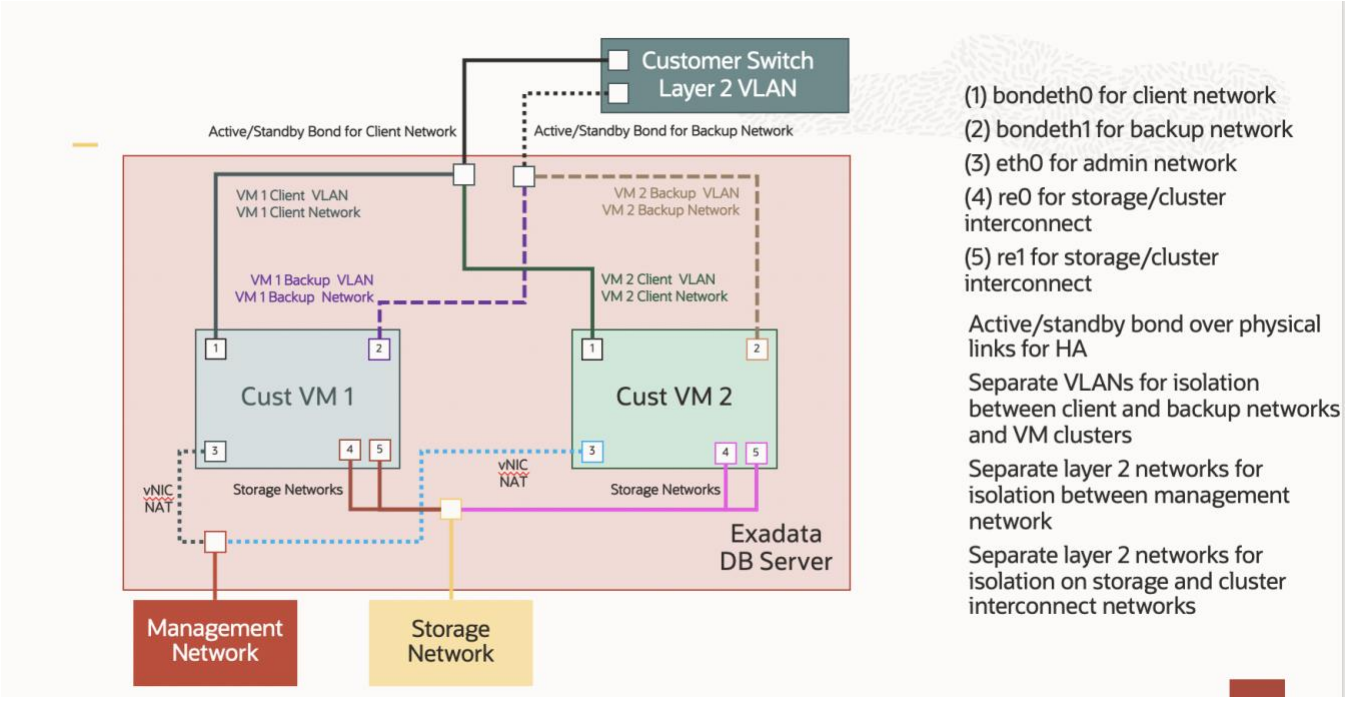

Figure 3: VM Cluster Network Isolation

The Control Plane Server accesses the Oracle Cloud Infrastructure (OCI) control plane via public Internet. The Control Plane Server reaches the Internet via a layer 2 Ethernet connection to a customer-managed switch. The customer provides time services (NTP), name resolution (DNS) for Internet hostnames (e.g., oracle.com), and routing (default gateway) for the Control Plane Server connection to the OCI control plane. The Control Plane Server does not require inbound TCP connections, and only requires outbound connections to Oracle IP addresses on TCP port 443, described in the Control Plane Server Networking section of this document. Customers may and should impose network access rules to deny inbound access to the Control Plane Server and to only permit outbound access to required Oracle endpoints. The minimum required bandwidth for the connection from the CPS to OCI control Plane is 50 Mbps for downloads and 10 Mbps for uploads.

The Exadata Database (DB) Server is connected to a customer managed switch via 10Gb or 25Gb Ethernet, shown in blue. The customer has access to customer virtual machines (customer VM) via a pair (client and backup) of layer 2 (tagged VLAN) network connections to the customer VM that are implemented as virtual network interface cards (vNICs). The physical network connections are implemented for high availability in an active/standby configuration.

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 an HA (active/standby) connection to a pair of redundant storage networking switches. The following CIDR describes the standard IP addressing for the storage network configuration: 100.107.0.0/24. If those IP addresses are in conflict with existing IP addresses, then customers can override this CIDR block with an arbitrary customer-supplied IP address range.

Oracle Cloud Automation accesses the customer VM via a NAT address on the management network implemented on a vNIC in the Exadata Database Server, shown in red. Oracle Cloud Automation access to the customer VM is controlled via token based ssh. Public keys for Oracle Cloud Automation access are stored in the authorized keys files of the oracle, opc, and root users of the customer VM. The private keys used by the automation are stored and protected by the Oracle Cloud Automation software running in the Exadata Cloud@Customer hardware in the customer's data center.

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 may further control access via the management network and Oracle Cloud Automation keys by blocking network access (firewall rules, disabling network interface) and by revoking the credentials used by the Oracle Cloud Automation (remove the public keys from the authorized keys files). 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, such as customer VM operating system patching. 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.

Exadata Cloud@Customer Service Delivery

Figure 4 describes the TCP ports and protocols used to deliver the Exadata Cloud@Customer service. Important components of remote service delivery include

- Customer access to Oracle Cloud Infrastructure (OCI) tenancy
- Customer control of access to OCI user interfaces and APIs
- OCI Database Control Plane access to Exadata Cloud@Customer for remote automation delivery
- Secure Outgoing Tunnel Service to connect Exadata Cloud@Customer to OCI region
- OCI Object Storage Service to deliver software updates for Exadata Cloud@Customer components
- Infrastructure monitoring
- Identity management for Oracle Cloud Ops Staff
- Temporary (ephemeral) secure tunnel service for Oracle Operator Access (reverse ssh tunne)

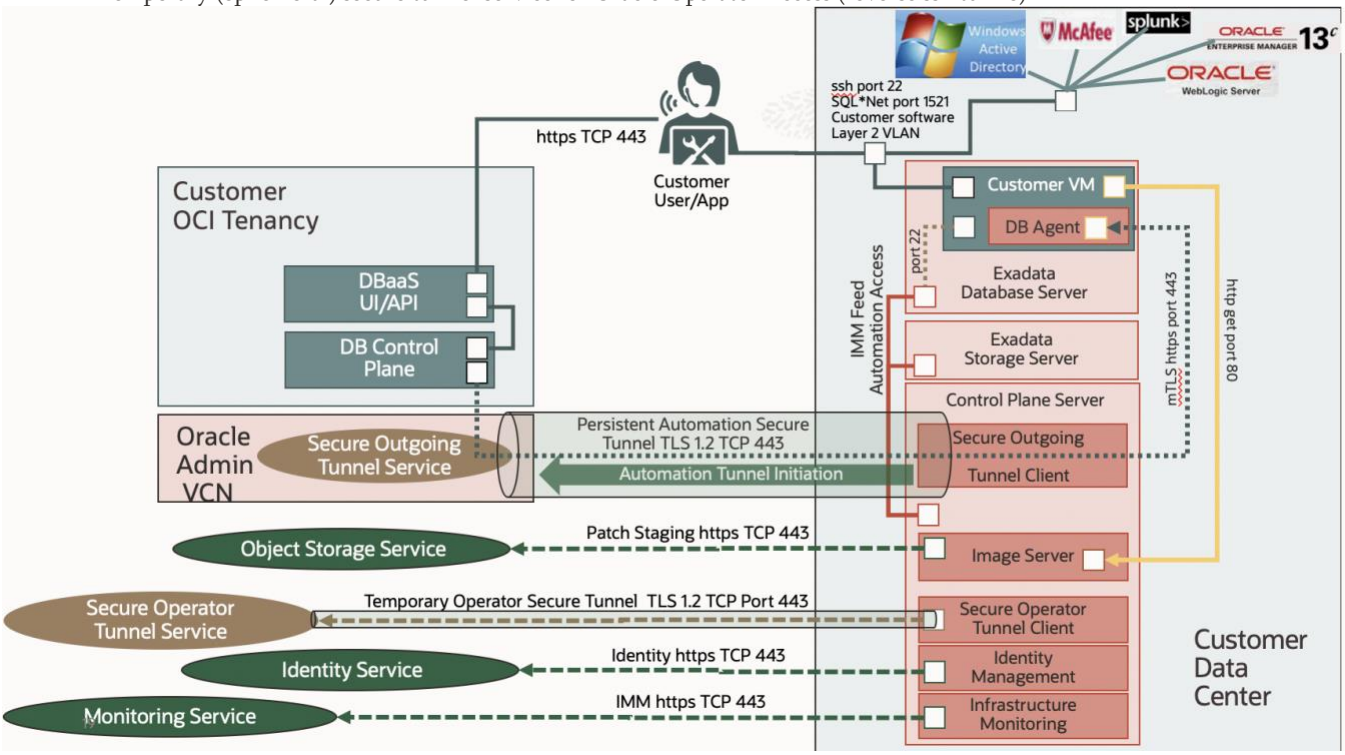

Figure 4: Exadata Cloud@Customer Ports and Protocols

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
- Terraform – typically for infrastructure as code

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 Exadata Cloud@Customer components. as follows:

- DBaaS UI/API sends request to DB Control Plane via https on port 443
- DB Control Plane sends the request via REST API to a proxy service (CPS Proxy) via the Persistent Secure Tunnel Service Admin VCN
- TLS 1.2 Persistent Secure Tunnel Service end in the OCI Admin VCN and the CPS delivers REST API request to the CPS proxy running on the CPS in the Exadata Cloud@Customer rack
- The CPS proxy issues commands to Exadata Cloud@Customer components

  - Actions that require access to Database Services in the customer VM are sent to the DB Agent running in any or all of the customer VMs (e.g., up to 4 VMs in a half rack) via an mTLS (port 443) connection between the OCI control plane and each DB Agent; this mTLS connection is implemented through the private interconnect network in the Exadata Cloud@Customer rack
  - 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 stored in the authorized_keys files of the oracle, opc, and root users in the customer VM; the private ssh keys are stored and protected 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 from the CPS to the required endpoint (e.g., Exadata Storage Server, Exadata Database Server)

Oracle manages and controls the private ssh tokens uses to manage infrastructure and customer VM components. These tokens are stored and protected in the CPS. 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 only provide access to the customer VM, and do not provide access to infrastructure components.

Infrastructure Monitoring

The Exadata Cloud@Customer infrastructure components report their Infrastructure Management Metrics (IMM) to the CPS, and the CPS relays this information to Oracle for processing. The IMM connection is implemented via https with endpoint specific the OCI region used to manage the Exadata Cloud@Customer service.

Oracle Global Support performs monitoring and maintenance of the Exadata Cloud@Customer implementation as follows:

- Automated monitoring on Oracle Cloud@Customer infrastructure components sends Infrastructure Monitoring Metrics (IMM) via an infrastructure monitoring utility deployed on the CPS
  - Chassis temperature, drive status, etc.
  - Details for all monitoring data are published at Auto Service Request Qualified Engineered Systems Products at https://docs.oracle.com/cd/E37710_01/doc.41/e37287/toc.htm
- Oracle Global 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

Software Updates

Standard quarterly bundle patches for the Oracle database, Grid Infrastructure, and customer VM operating system are staged to the CPS from 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 for application via outbound http (port 80) connections from the customer VM to the Image Server running on the CPS.

Standard quarterly patch bundles and 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, Oracle performs the component restart in a rolling fashion to ensure service availability during the update process.

PREVENTATIVE CONTROLS (COMPONENT AND DATA ACCESS)

The Exadata Cloud@Customer service is designed to isolate and protect customer services and database data from unauthorized access. The Exadata Cloud@Customer service separates duties between the customer and Oracle. The customer controls access to customer services, databases, and database data. Oracle controls access to Oracle-managed infrastructure components.

Customer Access Controls

The customer controls access to their VMs, databases, and data via 3 types of controls:

- Authentication
  - Credentials to access OCI services, customer VM operating systems databases, and database data
- Network
  - Layer 2 VLANs to access customer VMs
  - Network access rules implemented in the customer VM operating system and Oracle database
- Encryption
  - Application to database encryption[1]
  - Database to storage encryption[2]

Customer Access Control for Exadata Cloud@Customer Services

Customers perform management actions via OCI automation by making an https connection to the Oracle Public Cloud Control Plane in the OCI region chosen by the customer. The customer is authenticated using their OCI Identity and Access Management (IAM) 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 local Control Plane Servers (CPS) via the Persistent Secure Tunnel Service (TLS 1.2) for delivery into the appropriate Exadata Cloud@Customer components.

Customers and database applications access databases running on the Exadata Cloud@Customer via a layer 2 (tagged VLAN) network connection hosted in the customer VM. Access to databases and operating system is made via customer managed credentials.

Customer Controls for Data Security

Oracle Exadata Cloud@Customer is designed to help secure data for legitimate customer use and to help protect data from unauthorized access, which includes preventing access to customer data by Oracle Cloud Ops staff members. Security measures designed to protect against unauthorized access to Exadata Cloud@Customer 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

---

[1] Exadata Cloud@Customer automation configures Oracle Native Network Encryption; customers may override this control

[2] Exadata Cloud@Customer automation configured Oracle Transparent Data Encryption (TDE); Oracle strongly recommends that customers preserve this control

- Customer can install monitoring agents and security controls of their choice on the customer VM operating system as long as these agents don't taint the Linux kernel or interfere with Exadata operation
- Network connections to the Oracle database are designed to be protected by Oracle Advanced Security Network Encryption, which is automatically configured by Cloud Automation
- Oracle database data is protected by Oracle Transparent Data Encryption (TDE) keys
  - Automatically configured by Cloud Automation and stored in password protected, PKCS12 wallet file stored in the file system of the customer VM
  - Customer controls access to TDE encryption keys via the wallet password
  - Customer can move the TDE master key to an external key store
  - Oracle Cloud Ops staff does not have access to TDE encryption keys
- Database Vault may be implemented to help protect user data access from privileged database accounts (e.g., sys, system)

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

Figure 5 shows compensating 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[3]
- Oracle Database Vault[4]
- Oracle Transparent Database Encryption (TDE)[5]

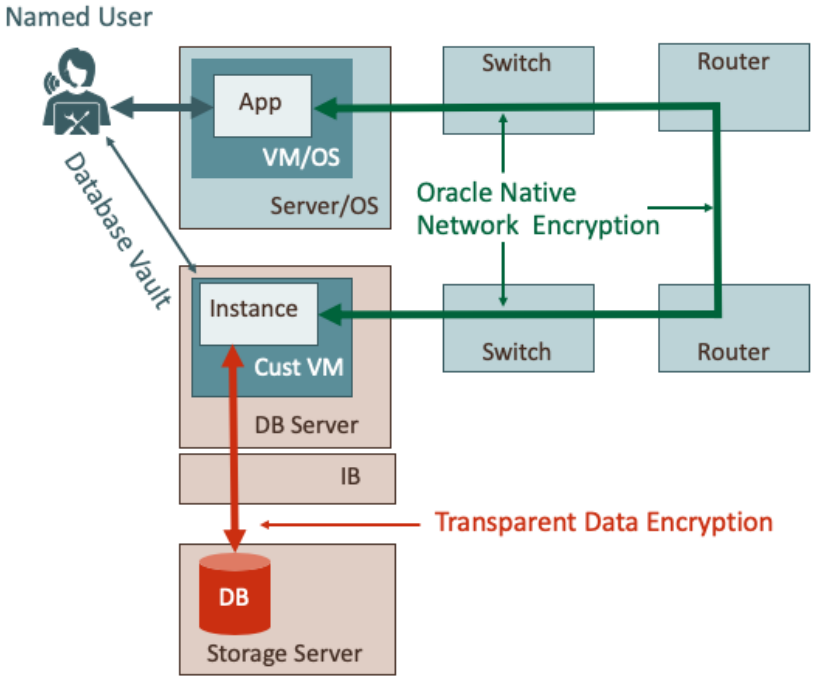

Figure 5: Controls to protect data in flight, while processing, and at rest

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 Exadata Cloud@Customer automation. When Oracle Native Network Encryption is enabled, access to infrastructure components that can observe IP and Ethernet packets does not provide access to customer data because the data is encrypted. Documentation for Oracle Native Network Encryption is published in the Security

[3] Included with Enterprise Edition Extreme Performance subscription, not included with Bring Your Own License (BYOL) subscription

[4] Included with Enterprise Edition Extreme Performance subscription, not included with Bring Your Own License (BYOL) subscription

[5] Included with Enterprise Edition Extreme Performance subscription and with Bring Your Own License (BYOL) subscription

Guide for each Oracle Database version. For example, 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.

Oracle Database Vault

Oracle Database Vault security controls are designed to help protect application data from privileged account access and help address privacy and regulatory requirements. You can deploy controls to block privileged account access (e.g., sys, sysdba, etc.) to application data and control sensitive operations inside the database using trusted path authorization. By blocking privileged account access to data, unauthorized access to customer VM as a privileged account (e.g, root, opc, oracle) that leads to unauthorized access to a database account (e.g., sys, sysdba) does not lead to access to user data. 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 published for each database version. For example, for Oracle Database 19c, see https://docs.oracle.com/en/database/oracle/oracle-database/19/dvadm/introduction-to-oracle-database-vault.html#GUID-0C8AF1B2-6CE9-4408-BFB3-7B2C7F9E7284.

Oracle Transparent Data Encryption and Oracle Key Vault

Oracle Transparent Data Encryption (TDE) encrypts data within the database. The encryption is transparent to authorized applications and users because the database automatically encrypts data before it is written to storage and automatically decrypts it when reading from storage. Authorized applications that store and retrieve data in the database only see the decrypted (or "plaintext") data. TDE prevents privileged operating system users, network and storage administrators (or someone masquerading as them) from bypassing the database controls to access the data directly. Authorized database users and applications do not need to present the decryption key when they process encrypted data. Instead, the database enforces the access control rules described in the previous chapters and denies access if the user is not authorized to see the data.

Oracle TDE is engineered to be highly performant. It automatically leverages special instructions in Intel CPUs (AES-NI) to accelerate cryptographic operations. In addition, TDE tablespace encryption works seamlessly with Exadata Hybrid Columnar Compression (EHCC) and Smart Scan technology.

With TDE, sensitive 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 and Data Pump exports and Oracle Recovery Manager (RMAN) and Data Pump both integrate with TDE encrypted data.

TDE uses a two-tier key architecture comprising of data encryption keys that are encrypted with a master encryption key. That master encryption key is stored outside of the database, by default in a PKCS#12 compliant container called a 'wallet' in the /u02 file system on the customer VM operating system which provides a shared wallet location that is accessible to both instances of the RAC-enabled databases. Furthermore, Oracle Databases 18c and later allow customers to upload their own, externally generated encryption keys (called Bring-Your-Own-Key, BYOK) into the shared wallet, maintaining separation of duties between the database administrators and key custodians. Customers may choose to migrate their ExaC@C databases to Oracle Key Vault (OKV), the only key management solution for your Oracle database estate that provides continuous key availability by adding up to 16 OKV nodes to a key management cluster that can span geographically distributed data centers and the Oracle Cloud Infrastructure (OCI). Oracle Key Vault provides continuous online key management to all currently supported, TDE-enabled database releases, as well as encrypted GoldenGate trail files. It also provides the capability to ingest externally generated keys (BYOK). Details for managing TDE are published in the Oracle Database Advanced Security Guide for each database version. For example, for Oracle Database 19c, see https://docs.oracle.com/en/database/oracle/oracle-database/19/asoag/introduction-to-transparent-data-encryption.html

Controls for Cloud Automation Network Access to Customer VM

Oracle Cloud Automation software accesses customer databases and customer VM via 2 access methods

- Secure login to customer VM as a privileged user (root, opc, oracle) via token-based ssh
  - Cloud Automation ssh tokens are generated at service activation and stored and protected in the Control Plane Server located in the Exadata Cloud@Customer infrastructure rack in the customer's data center
  - Customers may block port 22 inbound access to the customer VM; however, this port will need to be temporarily opened for actions that require cloud automation inbound access on port 22 (e.g., memory resize of customer VM)
  - Customers may control Cloud Automation authentication by revoking and reinstating Cloud Automation public keys from the authorized_keys files of the Exdata Cloud@Customer customer VM service accounts using the exacm_keys_patch_file.py tool in the customer VM; however, these keys will need to be temporarily opened for actions that require cloud automation inbound access on port 22 (e.g., memory resize of customer VM)
- REST API call to Oracle DBCS agent running in customer VM via mTLS authentication on port 443
  - Customers should permit inbound access on port 443 to the customer VM so that OCI control plane actions can be sent to the DBCS agent in the customer VM
  - Access to the DBCS agent is protected by mTLS

The customer VM provides the Oracle Linux firewall software as an additional compensating controls to block network to the customer VM. The Oracle Linux firewall, iptables or firewalld, blocks 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, and for testing customer VM firewall configuration for the purposes of blocking control plane access to customer VM. Customers should use the Oracle SR process to request Cloud Ops support to 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 Oracle Cloud Automation functionality may cease to function if customers implement Kerberos authentication in the customer VM. Oracle does not support Cloud Automation with Kerberos configured in the customer VM.

Controls for Customer Staff Access to Customer VM

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/.ssh/authorized_keys and /home/oracle/opc/.ssh/authorized_keys files of the oracle and opc users. 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.

Controls for Protecting Against Theft of Data

Oracle database data in Oracle Exadata Cloud@Customer 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.

Oracle's security policies cover the management of security for both Oracle's internal operations and the services, including the Exadata Cloud@Customer 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. Oracle security practices are published at https://www.oracle.com/corporate/security-practices/corporate/.

Oracle Database Security Assessment Tool (DBSAT)

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

DBSAT is provided at no additional cost and enables 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 on 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 Controls for Cloud Operations Access to Infrastructure Components

Oracle Cloud Ops staff are not authorized to access customer VMs, databases, or database data. Oracle Cloud Operations Staff are authorized to access and support Exadata Cloud@Customer 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 6 shows how Oracle Cloud Operations (Cloud Ops) staff access infrastructure components to manage the Exadata Cloud@Customer.

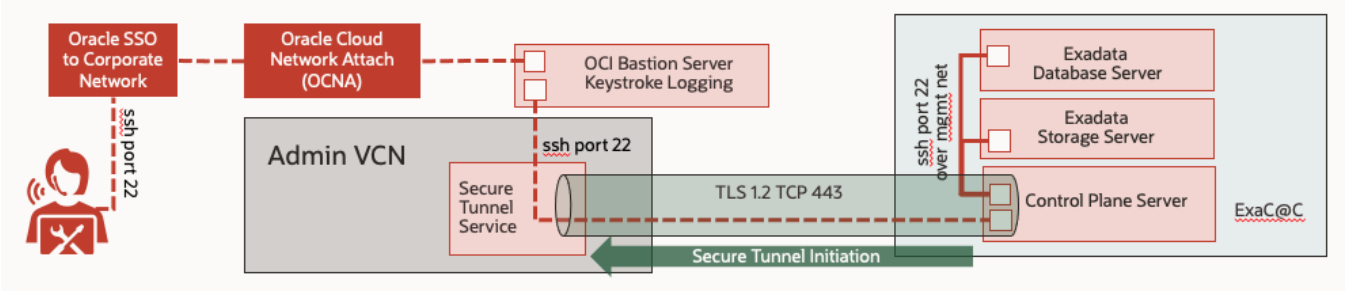

Figure 6: Cloud Operations Staff Access to Exadata Cloud@Customer Infrastructure Components

Oracle controls Oracle Cloud Operations staff access to Cloud@Customer infrastructure components in the following process:

- Login to Oracle corporate network as a named user using Oracle Single Signon (SSO) Login
- Access Oracle Cloud Network Attach (OCNA) based on entitlements specific to job code
- Login to Bastion server as a named user via ssh using multi-factor authentication (MFA) implemented with a FIPS 140-2 compliant one-time password generator of 60-character length from a 36-character set
  - Access to the Bastion server is only available within the OCI privileged administrative VCN
  - All connections to and actions on Bastion servers are logged monitored by Oracle to ensure authorized actions are performed, unauthorized actions are terminated, and an historical record is maintained
- Login to CPS as a named user via ssh using MFA implemented a FIPS 140-2 compliant one-time password generator of 60-character length from a 36-character set
  - Access to the CPS is only available from the Bastion server
  - All connections on the CPS are monitored by Oracle to ensure authorized actions are performed and unauthorized actions are terminated
- Assume the identity of a privileged user to access infrastructure components via token-based ssh
  - All command execution is traceable to a specific named user via logging at Bastion server and CPS
  - ssh tokens for infrastructure access, unique to each customer, are stored and secured in the CPS
  - ssh tokens are rotated every 90 days
  - Access to the infrastructure components are only available from the CPS
  - All connections to infrastructure components are monitored by Oracle to ensure authorized actions are performed and unauthorized actions are terminated

Oracle Process Controls

Oracle's standard security policies and practices restrict access to Oracle staff with a need to know and need to access Exadata Cloud@Customer infrastructure, and include the following details:

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

Exadata Infrastructure Software Security and Controls

Exadata Cloud@Customer is based on the Exadata Database Machine and delivers the enterprise-class security features of Exadata Database Machine in an on-premises cloud model. Security features of Exadata Cloud@Customer include the following:

- Software deployed on Exadata Cloud@Customer infrastructure is limited to the minimum software components to run customer services
- Development and debug tools to inspect customer data are not installed on Exadata Cloud@Customer infrastructure
- Non-essential operating system tools and packages are not installed on Exadata Cloud@Customer infrastructure

Complete details of the Exadata Database Machine security features are available from Oracle at https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/toc.htm.

DETECTIVE CONTROLS (LOGGING AND AUDITING)

Exadata Cloud@Customer provides comprehensive 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 Oracle audit logs via the Oracle service request (SR) process.

Customer Audit Logging

Exadata Cloud@Customer provides 3 areas for auditing and logging of customer actions

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

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

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

Each log event includes a header ID, target resources, timestamp of the recorded event, request parameters, and response parameters. You can view events logged by the Audit 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. OCI Audit Service documentation is published at https://docs.cloud.oracle.com/iaas/Content/Audit/Concepts/auditoverview.htm.

Oracle database auditing tracks changes made to the Oracle database by database users and non-database users. Customers have the right and responsibility to 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 for each database version. For example, for 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.

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 have the responsibility to 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 for the specific version of the operating system running in the customer VM. For example, audit logging for the Oracle Linux 7 distribution is published at https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-audit-sec.html.

The customer may monitor network access at any point they control, including network access between the CPS and the Internet, network access into the customer VM, and network access from the customer VM to the customer data center.

Oracle Audit Logging

Audit logging of actions taken in the Exadata Cloud@Customer infrastructure owned by Oracle are the responsibility of Oracle. Oracle maintains the following infrastructure audit logs:

- 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
  - /var/log/oracle/diag/asm/cell/<hostname>/alert/log.xml
  - /var/log/oracle/diag/asm/cell/<hostname>/trace/ms-odl*.log
- Storage Network Switch
  - /var/log/messages
  - /var/log/audit.log
  - /var/log/secure
  - /var/log/opensm.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 DART 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 determine “Root Cause”.

RESPONSIVE CONTROLS (CONNECTION TERMINATION)

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 around the unauthorized action. If the customer detects an unauthorized action, the customer should notify Oracle of the action and response via the Oracle SR process. Oracle will notify the customer of detected unauthorized actions and Oracle responses.

The customer may take any responsive action on any services or equipment they control. This includes terminating network connections into the customer VM and terminating network connections between the CPS and OCI resources. The database services and databases will continue to function normally if a customer terminates connections between the CPS and OCI resources, and any authorized action that is terminated via this customer response can be restarted.

Oracle’s responsive controls include terminating connections at Bastion Servers in OCI, terminating connections at the CPS, and revoking access to Exadata Cloud@Customer resources.

SUMMARY

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 the Exadata Cloud@Customer service ensure that Oracle Cloud Operations staff only perform authorized actions on the infrastructure components of Exadata Cloud@Customer. Security measures include multi-factor named user authentication, strong passwords with rotation schedules, and token-based SSH access to Oracle-managed infrastructure components. Auditing and logging are implemented throughout the stack, and audit logs are available to customers at their request via the Oracle Service Request (SR) process.

The combined security and auditing postures of customer-managed and Oracle-managed components separate duties and deliver 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 ensure system security and prevent unauthorized access to and theft of customer data. Oracle Cloud Operations staff does not access customer networks, services, or data to deliver the Exadata Cloud@Customer service, and customers do not access Oracle managed infrastructure to consume Exadata Cloud@Customer Service. In the Exadata Cloud@Customer 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 Cloud@Customer
Security Controls
February 2121
Author: [OPTIONAL]
Contributing Authors: [OPTIONAL]