Exadata Cloud@Customer Security Controls

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

February 2, 2022 | Version 2.14

PURPOSE STATEMENT

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

This document summarizes the security and control features of Oracle's Gen 2 Exadata Cloud@Customer (ExaC@C) service[1] delivered through the Gen 2 Oracle Cloud Infrastructure (OCI) control plane, and is intended for customer security staff chartered at evaluating adoption of ExaC@C, which requires the customer to accept the following service delivery requirements:

- Oracle chooses the staff that are authorized to connect to the ExaC@C infrastructure
- Oracle is the identity provider for the staff accessing the ExaC@C infrastructure
- Oracle staff authorized to access the ExaC@C infrastructure will use Oracle provided software and hardware to gain access to the infrastructure

Security staff chartered with evaluating ExaC@C should also review the following related documentation that describes additional controls available with Oracle Operator Access Control (OpCtl) and the Oracle Cloud Infrastructure control plane:

- Exadata Cloud@Customer Security Guide[2]
- Oracle Cloud Infrastructure Security Architecture[3]
- Oracle Cloud Infrastructure Security Guide[4]
- Oracle Cloud Infrastructure Security Testing Policies[5]
- Oracle Operator Access Control Tech Brief[6]
- Oracle Operator Access Control product documentation[7]
- Oracle Cloud Services Contracts[8]
- Oracle Data Processing Agreement[9]
- Oracle Corporate Security Practices[10]

DISCLAIMER

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

[1] https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/gen2-exacc-ds.pdf

[2] https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/exadata/doc/exacc-secguide.html

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

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

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

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

[7] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-7CF13993-DB16-485A-A9FA-399E0049740B

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

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

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

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 (ExaC@C) 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. The advantage of ExaC@C is that the customer retains physical control of the ExaC@C hardware by locating it in a data center of their choice while still receiving the efficiency and automation of the Oracle Cloud Infrastructure (OCI) control plane and OCI Cloud Ops staff support for infrastructure maintenance.

ExaC@C is the right database service for use cases where customers seek to gain the operational and financial value of a cloud implementation while honoring policy, legal, and regulatory requirements dictated to mission critical applications and highly regulated industries. For example, ExaC@C is ideal for banking and financial services applications, energy utilities, and defense, and any other application where risk management is a key pillar of application success. Customers operating in these industries and interested in pursuing a cloud strategy must ensure that their chosen cloud provider has comprehensive support of these capabilities within their standardized service offering.

The ExaC@C 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 ExaC@C service delivery model, ExaC@C includes the security controls described in this paper as compensating measures for edge cases where customer approved security standards may differ from the ExaC@C 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 https://www.oracle.com/cloud/compliance/#attestations to access relevant detail about a specific standard. 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.

ExaC@C is operated in compliance from the following standards:

- ISO 27001
- System and Organization Controls 1 (SOC 1)
- System and Organization Controls 2 (SOC 2)
- System and Organization Controls 3 (SOC 3)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)

Customers may request compliance documents from an Oracle sales representative, and customers may access them directly from their OCI Cloud Console. Instructions for accessing compliance documents are published at https://docs.oracle.com/en-us/iaas/Content/ComplianceDocuments/Concepts/compliancedocsoverview.htm.

ORACLE COPORATE SECURITY PRACTICES

Oracle’s security practices cover the management of security for both Oracle’s internal operations and the services, including the ExaC@C 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[11] including the following information:

- Objective[12] – help protect the confidentiality, integrity, and availability of both Oracle and customer data
- Human resources security[13]
- Access control[14]
- Network communications security[15]
- Data security[16]
- Laptop and mobile device security[17]
- Physical and environmental security[18]
- Supply Chain Security and Assurance[19]

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

ExaC@C is jointly managed by the customer and Oracle. The ExaC@C deployment is divided into 2 areas of responsibility:

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

[11] https://www.oracle.com/corporate/security-practices/corporate/
[12] https://www.oracle.com/corporate/security-practices/corporate/objectives.html
[13] https://www.oracle.com/corporate/security-practices/corporate/human-resources-security.html
[14] https://www.oracle.com/corporate/security-practices/corporate/access-control.html
[15] https://www.oracle.com/corporate/security-practices/corporate/network-communications-security.html
[16] https://www.oracle.com/corporate/security-practices/corporate/data-protection/
[17] https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html
[18] https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html
[19] https://www.oracle.com/corporate/security-practices/corporate/supply-chain/

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

EXAC@C SERVICE ARCHITECTURE

Figure 1 shows the architecture block diagram the Gen 2 ExaC@C service.

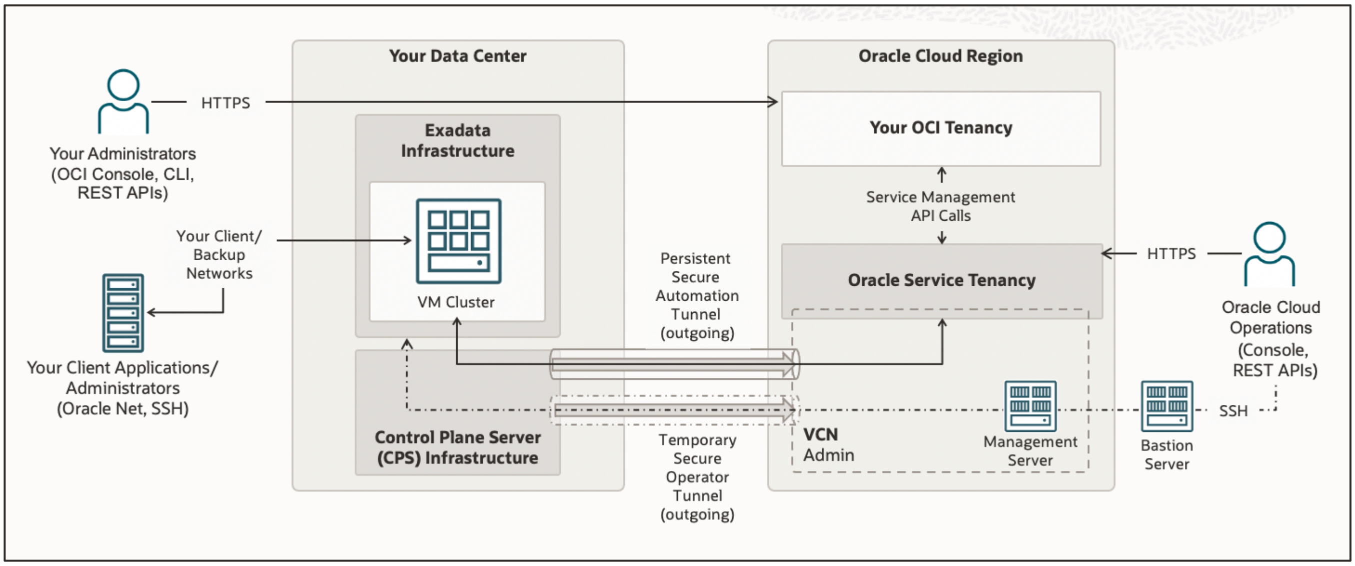
Your Administrators (OCI Console, CLI, REST APIs)
HTTPS
Your Data Center
Exadata Infrastructure
VM Cluster
Control Plane Server (CPS) Infrastructure
Your Client/ Backup Networks
Your Client Applications/ Administrators (Oracle Net, SSH)
Persistent Secure Automation Tunnel (outgoing)
Temporary Secure Operator Tunnel (outgoing)
Oracle Cloud Region
Your OCI Tenancy
Service Management API Calls
Oracle Service Tenancy
VCN Admin
Management Server
Bastion Server
HTTPS
SSH
Oracle Cloud Operations (Console, REST APIs)

Figure 1: Architecture block diagram for Oracle ExaC@C

The ExaC@C service is deployed in an ExaC@C rack in a data center of the customer's choice. The ExaC@C 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 ExaC@C rack, and all access to customer databases is made via network connections (intranet) the customer permits to access the VMs and databases in the ExaC@C 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 ExaC@C Compute VM operating system and Oracle database.

The OCI region performs remote delivery of the ExaC@C 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 ExaC@C service requires no inbound TCP connection for service delivery, support, or management purposes. The ExaC@C service requires outbound TCP connections on port 443 to Oracle endpoints for the purposes of remote service delivery and management. These endpoints are shown in Table 2: Required outbound URL access for ExaC@C, and in the Network Requirements for Oracle Exadata Cloud@Customer section[20] of the Exadata Cloud@Customer product documentation.[21]

If you are using IP address filtering based firewall rules, due to the dynamic nature of cloud interfaces, you must allow traffic with all the relevant IP CIDR ranges associated with your OCI region as identified by https://docs.oracle.com/en-us/iaas/tools/public_ip_ranges.json.

ExaC@C 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 ExaC@C releases that may require access to additional OCI endpoints. Should you choose to selectively permit access to URLs for specific OCI services, you may need to update you permitted URLs when Oracle adds new features and services to ExaC@C. Customer https, challenge proxy, and traffic inspection are not supported.

The ExaC@C 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 ExaC@C and not part of OCI's public services. The URLs for this service are specific to the OCI region configured to manage the ExaC@C infrastructure.

The ExaC@C Secure Tunnel Service for Remote Operator Access is used exclusively for Oracle Operator Access (ssh) to Oracle Managed ExaC@C Infrastructure and ADB-D resources when applicable. This service is limited to ExaC@C, 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 ExaC@C infrastructure. The OCI Temporary Secure Tunnel Service is the path by which an Oracle Operator can use an ssh connection to gain access to the ExaC@C infrastructure and ADB-D services when applicable.

The certificates for the TLS connectivity are managed by Oracle exclusively and rotated every 6 months. 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, NTP server for clock synchronization, and routing to OCI service URLs.

The minimum bandwidth requirements for the Control Plane Server internet connection to OCI are 50/10 mbs download/upload.

[20] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/eccad/eccpreparing.html#GUID-F06BD75B-E971-48ED-8699-E1004D4B4AC1

[21] https://docs.oracle.com/en/engineered-systems/exadata-cloud-at-customer/eccad/index.html

Table 2: Required outbound URL access for ExaC@C

DESCRIPTION/PURPOSE	OPEN PORT	CERTIFICATE AUTHORITY	LOCATION REPLACE *OCI_REGION* WITH YOUR REGION
Persistent Outgoing Tunnel Service for cloud automation Delivery	443 outbound	Oracle Self-Signed	https://wss.exacc.*oci_region*.oci.oraclecloud.com
Persistent Outgoing Tunnel Service for Autonomous Database Dedicated (ADB-D) cloud automation Delivery	443 outbound	Oracle Self-Signed	https://wsshe.adbd-exacc.*oci_region*.oci.oraclecloud.com
Temporary Secure Tunnel Service for remote Oracle operator access supporting ExaC@C Infrastructure	443 outbound	Oracle Self-Signed	https://mgmthe1.exacc.*oci_region*.oci.oraclecloud.com https://mgmthe2.exacc.*oci_region*.oraclecloud.com
Temporary Secure Tunnel Service for remote Oracle operator access for ADB-D resources	443 outbound	Oracle Self-Signed	https://mgmthe.adbd-exacc.*oci_region*.oci.oraclecloud.com
Object Storage Service to retrieve system updates	443 outbound	DigiCert	https://objectstorage.*oci_region*.oraclecloud.com https://swiftobjectstorage.*oci_region*.oraclecloud.com
Monitoring Service to record and process Infrastructure Monitoring Metrics (IMM)	443 outbound	DigiCert	https://telemetry-ingestion.*oci_region*.oraclecloud.com
Identity Service for name resolution of Oracle operators	443 outbound	DigiCert	https://identity.*oci_region*.oraclecloud.com
Logging Service for application and security logs	443 outbound	DigiCert	https://frontend.logging.*oci_region*.oracleiaas.com https://controlplane.logging.*oci_region*.oracleiaas.com

Customer Access to ExaC@C Services

Customers access Oracle databases (DB) running on ExaC@C 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 ExaC@C infrastructure, load monitoring agents, or directly pull or push files to the Oracle managed infrastructure in the ExaC@C service.

Physical Network Implementation

Figure 2 describes the physical network implementation for ExaC@C deployed in the Exadata rack. The customer accessible and controlled components are shown in blue, and the Oracle managed components are shown in red. The ExaC@C infrastructure components are interconnected via an isolated layer 2 management network, also shown in red. There is no direct network access from the management or storage networks to the customer client and backup networks, and the Exadata Database Server does not have an IP address configured (plumbed) to access the client or backup networks.

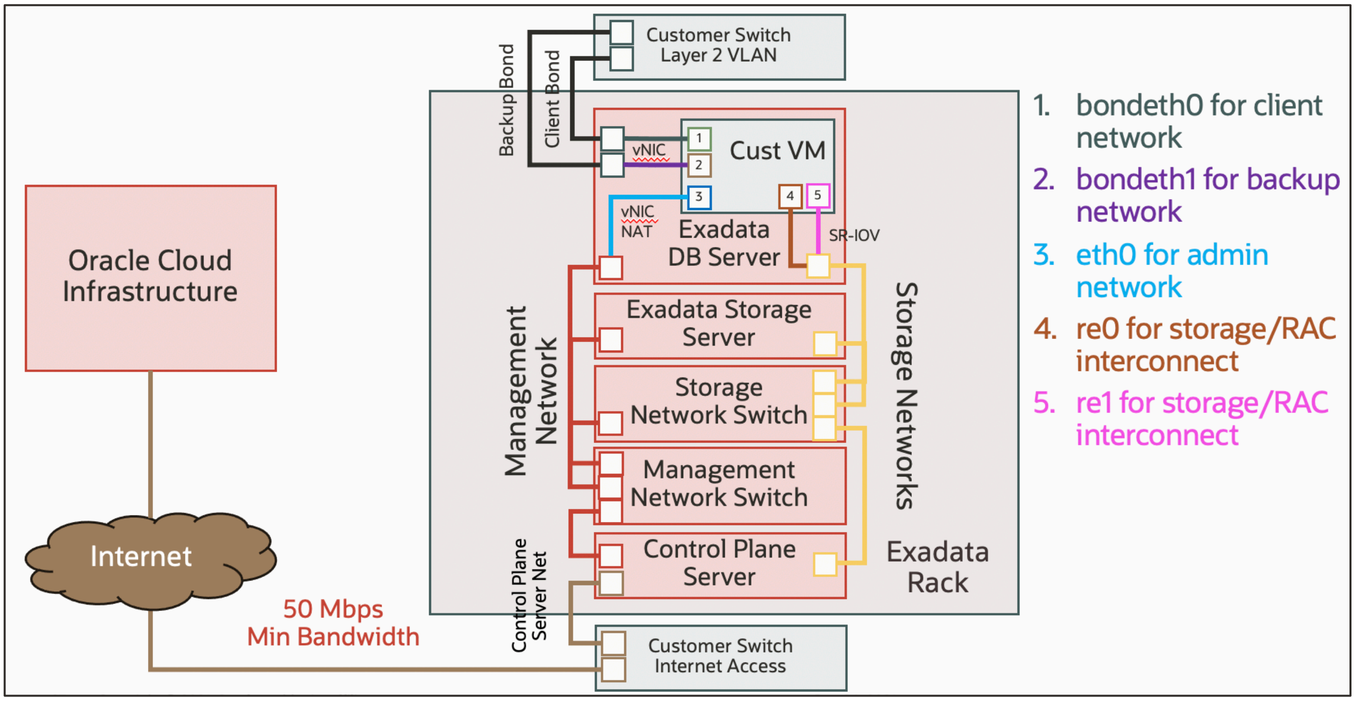

Figure 2: ExaC@C Physical Network Implementation

Figure 3 details the network isolation between different Virtual Machine Clusters (VM Clusters) deployed on the same ExaC@C 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 preventive control against in-VM executed methods to access cached data from other VMs.

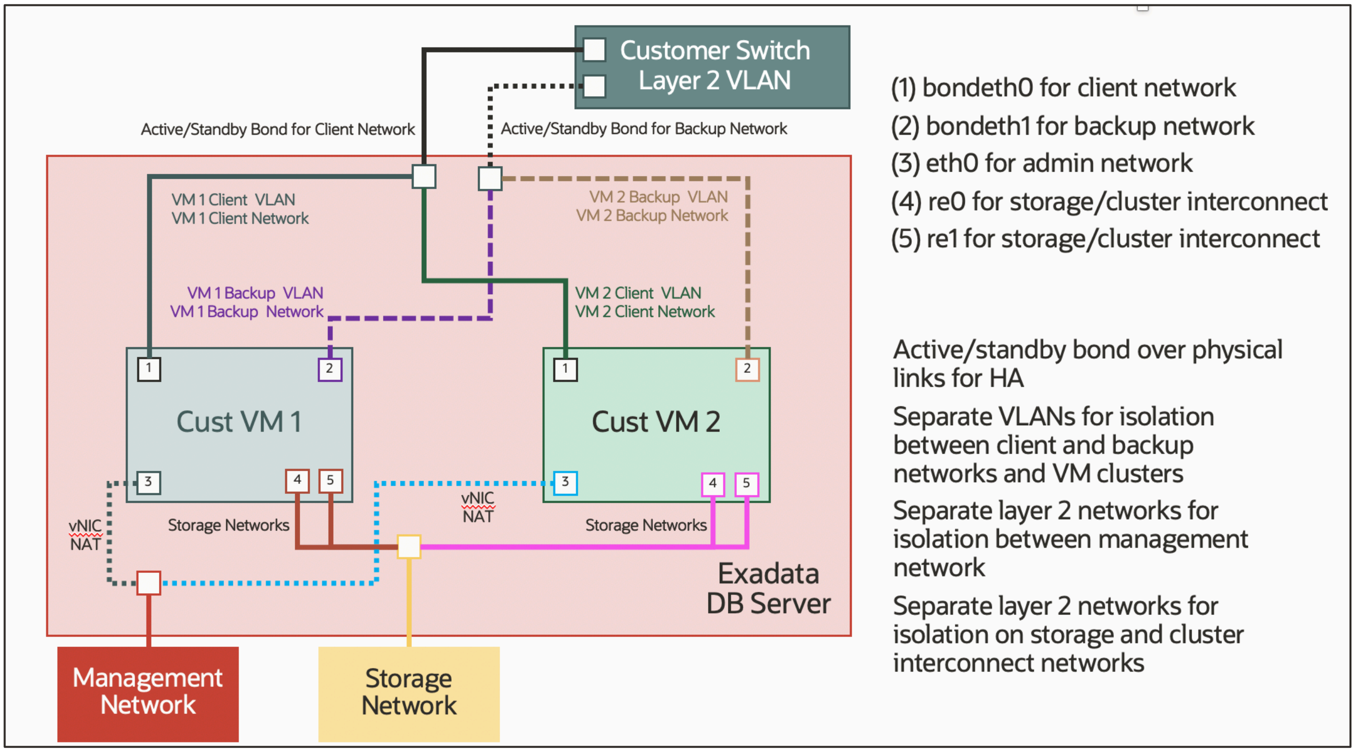
Customer Switch
Layer 2 VLAN
Active/Standby Bond for Client Network
Active/Standby Bond for Backup Network
VM 1 Client VLAN
VM 1 Client Network
VM 2 Backup VLAN
VM 2 Backup Network
VM 1 Backup VLAN
VM 1 Backup Network
VM 2 Client VLAN
VM 2 Client Network
1
2
Cust VM 1
3
4
5
1
2
Cust VM 2
3
4
5
vNIC
NAT
vNIC
NAT
Storage Networks
Storage Networks
Exadata
DB Server
Management
Network
Storage
Network
(1) bondeth0 for client network
(2) bondeth1 for backup network
(3) eth0 for admin network
(4) re0 for storage/cluster interconnect
(5) re1 for storage/cluster interconnect
Active/standby bond over physical links for HA
Separate VLANs for isolation between client and backup networks and VM clusters
Separate layer 2 networks for isolation between management network
Separate layer 2 networks for isolation on storage and cluster interconnect networks

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, and routing 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 layer 2 switch via 10Gb or 25Gb Ethernet. 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 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. 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 are stored in memory Oracle cloud automation software running in the ExaC@C 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 private keys are controlled such that `root` account can access the keys, but Oracle operator named accounts cannot directly access the keys. Oracle operator named accounts can be permitted to assume the `root` identity or use `sudo` to gain access to root privileges. The Operator Access Control service can be used to manage the ExaC@C service to permit customers to control when Oracle operators can gain `root` access or `root` privileges.

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 I the customer VM; however, this will break cloud automation functionality that must access the customer VM via ssh. This functionality includes:

- ASM disk group resize
- Local storage resize
- Customer VM memory resize
- Database patching
- Grid Infrastructure patching
- Customer VM OS 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. Oracle cloud automation access may be temporarily restored by the customer to permit the subset of functionality that requires `ssh` access to the customer VM.

ExaC@C Service Delivery

Figure 4 depicts the TCP ports and protocols used to deliver the ExaC@C service.

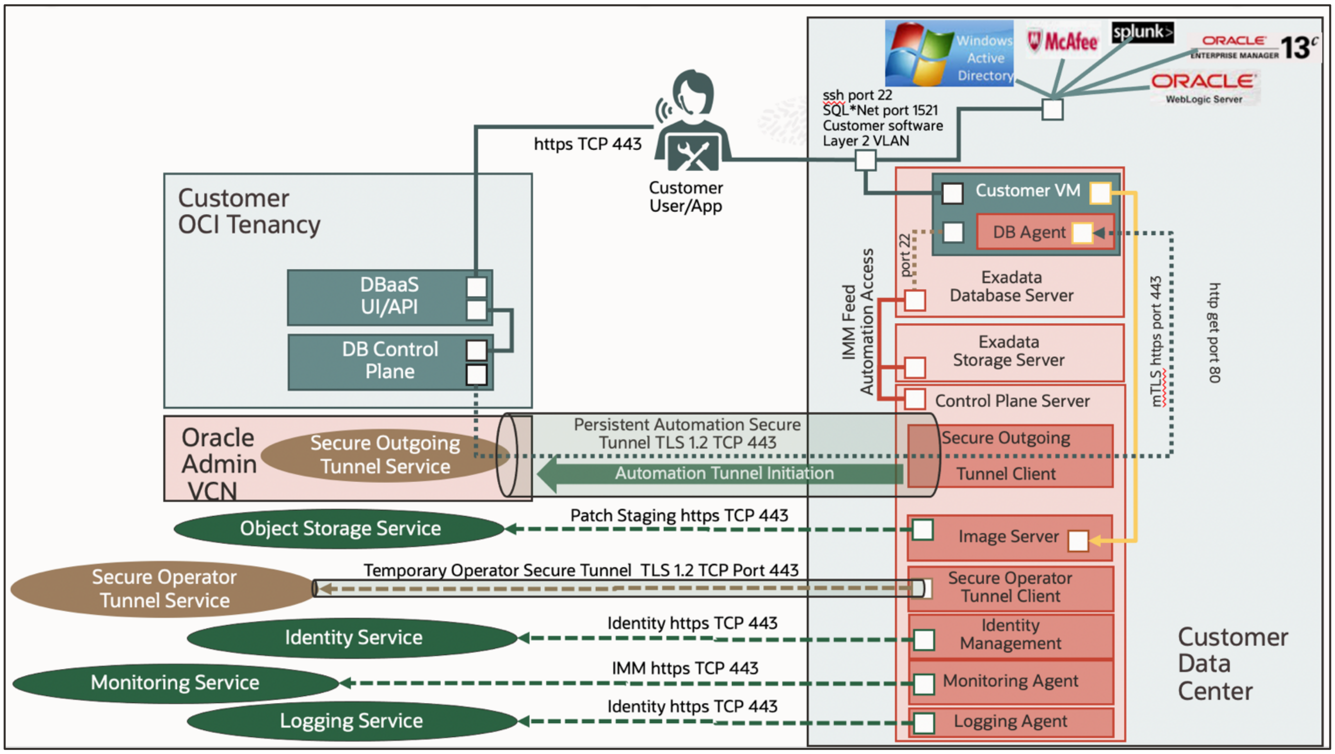

Figure 4: ExaC@C Service Ports and Protocols

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 ExaC@C for remote automation delivery
- Secure Outgoing Tunnel Service to connect ExaC@C to OCI region
- OCI Object Storage Service to deliver software updates for ExaC@C components
- Infrastructure monitoring
- Identity management for Oracle Cloud Ops Staff
- Temporary (ephemeral) secure tunnel service for Oracle Operator Access (reverse ssh tunnel)

ADB-D services may be run on the ExaC@C service. When ADB-D services are deployed, the following updates are applied to the ExaC@C service:

- The Customer VM becomes the ADB-D VM, and Oracle retains control to log into the ADB-D VM (token-based ssh as a named user) to support the ADB-D service; customers may not access the ADB-D VM per the ADB-D service definition
- A second Secure Outgoing Tunnel Service is established to an ADB-D-specific endpoint for the purposes of delivering ADB-D service functionality
- A second Secure Operator Tunnel Service is established to an ADB-D-specific endpoint to permit Oracle ADB-D support operators ssh access to the ADB-D 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
- Terraform – 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 ExaC@C 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 in the OCI Admin VCN and the CPS delivers REST API request to the CPS proxy running on the CPS in the ExaC@C rack
- The CPS proxy issues commands to ExaC@C 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 ExaC@C 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 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/or `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 from the CPS to the required endpoint (e.g., Exadata Storage Server, Exadata Database Server)

Infrastructure Monitoring

The ExaC@C 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 ExaC@C service.

Oracle Support performs monitoring and maintenance of the ExaC@C 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 to the OCI Telemetry Service endpoint
  - 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
- Automated monitoring on application and security logs sends application and security logs to the Oracle-managed OCI Logging service endpoint
- 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

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.

PREVENTIVE CONTROLS

The ExaC@C service is designed to isolate and protect customer services and database data from unauthorized access. The ExaC@C 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[22], customer VM operating system and databases[23], and database data[24]
- Network
  - Layer 2 VLANs to access customer VMs[25]
  - Network access rules implemented in the customer VM operating system[26] and Oracle database[27]
- Encryption
  - Application to database encryption[28]
  - Database to storage encryption[29]

Customer Access Control for ExaC@C 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

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

[23] https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/exadata/doc/ecc-connecting-to-exacc-system.html

[24] https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-privilege-and-role-authorization.html#GUID-89CE989D-C97F-4CFD-941F-18203090A1AC

[25] https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/exadata/doc/ecc-setting-up-the-network.html

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

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

[28] ExaC@C automation configures Oracle Native Network Encryption; customers may override this control; Oracle strongly recommends that customers preserve this control

[29] ExaC@C automation configured Oracle Transparent Data Encryption (TDE); Oracle strongly recommends that customers preserve this control

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 ExaC@C components.

Customers and database applications access databases running on the ExaC@C 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 ExaC@C 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 ExaC@C 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 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 encrypted by Oracle Native Network Encryption, which is automatically configured by cloud automation
- Oracle database data is encrypted 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, such as Oracle Key Vault
- Oracle Database Vault[30] may be configured to help protect user data access from database administrators

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[31]
- Oracle Database Vault[32]
- Oracle Transparent Database Encryption (TDE)[33]

[30] https://docs.oracle.com/en/database/oracle/oracle-database/19/dvadm/introduction-to-oracle-database-vault.html#GUID-0C8AF1B2-6CE9-4408-BFB3-7B2C7F9E7284

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

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

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

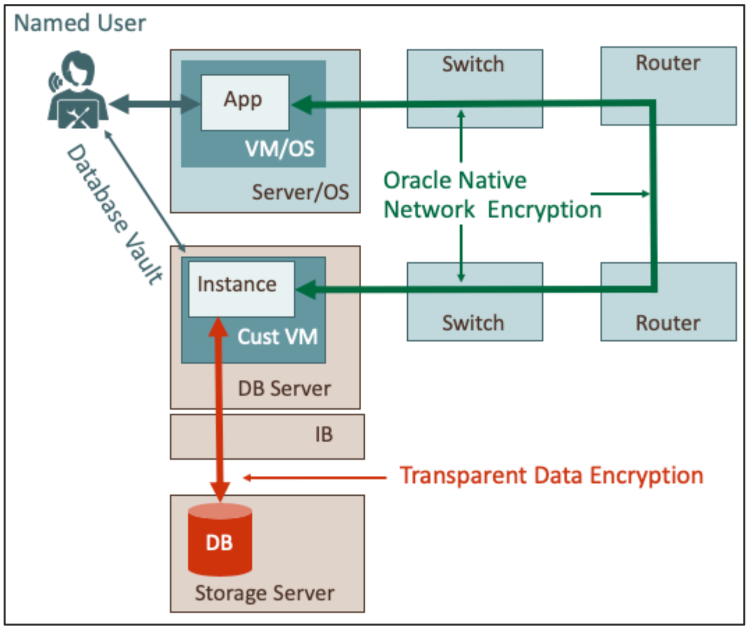

Figure 5: Controls to protect data in flight, while processing, and at rest

Oracle Native Network Encryption

Oracle Native Network Encryption encrypts data in flight between the application and the Oracle database instance and is automatically configured for databases created via the ExaC@C 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 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 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 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 user tables and tablespaces the Oracle database. The encryption is transparent to authorized applications and users because the database automatically encrypts data before it is written to storage and automatically decrypts it when reading from storage. Authorized applications that store and retrieve data in the database only see the decrypted (or "plaintext") data. TDE prevents privileged operating system users, network and storage administrators (or someone masquerading as them) from bypassing the database controls to access the data directly. Authorized database users and applications do not need to present the decryption key when they process encrypted data. Instead, the database enforces the access control rules described in the previous chapters and denies access if the user is not authorized to see the data.

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

With TDE, sensitive user data remains encrypted throughout the database, whether it is in tablespace storage files, temporary or undo tablespaces, or other files such as redo logs. In addition, TDE can encrypt entire database backups. Data Pump and Oracle Recovery Manager (RMAN) both integrate with TDE encrypted data.

TDE uses a two-tier key architecture comprising of data encryption keys that are encrypted with a master encryption key. That master encryption key is stored outside of the database, by default in a PKCS#12 compliant container called a 'wallet' in 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)[34], 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 TDE-enabled databases and encrypted GoldenGate trail files. It also provides the capability to ingest externally generated keys (BYOK).

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

- TDE for Oracle Database 19c[35]
- TDE for Oracle Database 18c[36]
- TDE for Oracle Database 12.2.0.1[37]
- TDE for Oracle Database 12.1.0.2[38]
- TDE for Oracle Database 11.2.0.4[39]

The Oracle TDE FAQ[40] 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

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

The customer VM provides the Oracle Linux packet filtering software[41] as a compensating control for customers to control network access to the customer VM, including blocking control plane software access. Customers may use Oracle Linux operating system administration tools to configure packet filtering software. ExaC@C automation does not include functionality or interfaces to configure Oracle Linux packet filtering software.

Customers do not have direct access to the infrastructure components for the purposes of determining source IP addresses for packet filtering software 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. For details, please see Oracle Support

[34] https://docs.oracle.com/en/database/oracle/key-vault/21.2/okvag/okv_intro.html#GUID-0D169EB8-C355-459A-9ABD-325CA5B46DD0
[35] https://docs.oracle.com/en/database/oracle/oracle-database/19/asoag/introduction-to-transparent-data-encryption.html#GUID-62AA9447-FDCD-4A4C-B563-32DE04D55952
[36] TDE for Oracle Database 18c
[37] TDE for Oracle Database 12.2.0.1
[38] TDE for Oracle Database 12.1.0.2
[39] TDE for Oracle Database 11.2.0.4
[40] https://www.oracle.com/database/technologies/faq-tde.html
[41] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-implement-sec.html#ol7-firewall-sec

Document 2621025.1 (Does ExaCC VM's Support Kerberos Authentication) can be found at: https://mosemp.us.oracle.com/epmos/faces/DocumentDisplay?id=2621025.1.

Microsoft Active Directory (AD) authentication for the customer VM is not supported on Exadata.

LDAP is not compatible with the Exadata software implemented in the customer VM on the ExaC@C service. Oracle does not support customers configuring Microsoft Active Directory for user authentication to the customer VM in the ExaC@C service.

Controls for Customer Staff Access to Customer VM

Access to the customer VM is implemented via token-based ssh[42]. 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.

Controls for Protecting Against Theft of Data

Data stored in user tables and tablespaces in databases running on ExaC@C is encrypted 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 ExaC@C 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 Data Safe

Oracle Data Safe[43] 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.

To learn more about how you can use Data Safe to better secure your Exadata Cloud-at-Customer environment, visit https://www.oracle.com/security/database-security/data-safe.

[42] https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/exadata/doc/ecc-connecting-to-exacc-system.html

[43] https://docs.oracle.com/en-us/iaas/data-safe/doc/oracle-data-safe-overview.html

Oracle Database Security Assessment Tool (DBSAT)

The Oracle Database Security Assessment Tool (DBSAT)[44] 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's standard security policies and practices restrict access to Oracle staff with a need to know and need to access ExaC@C infrastructure, and include the following details:

- Authorization to access ExaC@C infrastructure 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
- Oracle access control policy is published at https://www.oracle.com/corporate/security-practices/corporate/access-control.html

Oracle Cloud Operations Staff are authorized to access and support ExaC@C infrastructure components, which include the following equipment:

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

Figure 6 shows how Oracle Cloud Operations (Cloud Ops) staff access infrastructure components to manage the ExaC@C.

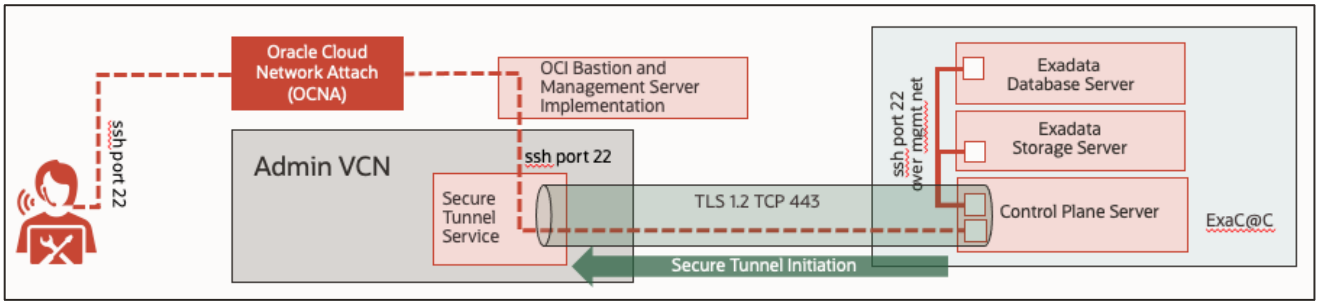

Figure 6: Cloud Operations Staff Access to ExaC@C Infrastructure Components

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

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

- Access through Bastion and Management servers for the purposes of proxied `ssh` tunnel access to ExaC@C infrastructure
  - Access through Management and Bastion servers 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 ExaC@C 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 published at https://www.oracle.com/corporate/security-practices/corporate/access-control.html
  - Connections to the ExaC@C infrastructure are logged and monitored by Oracle
- Login to ExaC@C infrastructure as a named user via ssh tunnel using MFA implemented with a FIPS 140-2 Level 3 hardware token (Yubikey)
  - Command execution is traceable to a specific named user via audit logging implemented in the ExaC@C infrastructure
  - Connections to infrastructure components are logged and monitored by Oracle
- Assume the identity of a service account or use sudo to gain service account authorization to perform management tasks
  - Command execution is traceable to a specific named user via logging at Bastion server and CPS
  - Connections to infrastructure components are monitored by Oracle to ensure authorized actions are performed and unauthorized actions are terminated

Exadata Infrastructure Software Security

ExaC@C 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 ExaC@C include the following:

- Software deployed on ExaC@C infrastructure is limited to the minimum software components to run customer services
- Development and debug tools to inspect customer data are not installed on ExaC@C infrastructure
- Non-essential operating system tools and packages are not installed on ExaC@C infrastructure
- Software development performed under Oracle Software Security Assurance[45]
- Security architecture performed under Oracle Corporate Security Architecture[46]

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

ExaC@C 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 Oracle Data Processing Agreement (DPA) audit rights at https://www.oracle.com/a/ocom/docs/corporate/data-processing-agreement-062619.pdf.

Customer Audit Logging

ExaC@C provides 3 areas for auditing and logging of customer actions

- OCI Audit Service[47]: 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[48]: audit logs for database actions initiated via a customer's Oracle database credential

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

[46] https://www.oracle.com/corporate/security-practices/corporate/governance/security-architecture.html

[47] https://docs.oracle.com/en-us/iaas/Content/Audit/Concepts/auditoverview.htm

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

- Customer VM operating system audit log[49]: 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`, `grid`, `opc`, and named users configured by the customer. Customers may 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.

Customer Security Scanning of Customer VM

Customers may use OpenSCAP to scan the customer VM for security vulnerabilities. Details on how to use OpenSCAP are published at https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-scap-sec.html.

Customers may use the Oracle Linux Advanced Intrusion Detection Environment (AIDE) to check file and directory integrity. AIDE is a small, yet powerful, intrusion detection tool automatically installed with the Linux Operating System, that uses predefined rules to check file and directory integrity. It is meant to protect the system internally, by providing a layer of protection against viruses, rootkits, malware, and detection of unauthorized activities. It is an independent static binary for simplified client/server monitoring configurations. 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. Details for how to use AIDE are published at https://support.oracle.com/knowledge/Oracle%20Linux%20and%20Virtualization/2616282_1.html.

Customers have control to install third party software, including scanning software, on the ExaC@C 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

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

testing is performed in the target environment by the customer. Third party providers. Details for third party software support on ExaC@C are published at https://support.oracle.com/knowledge/Oracle%20Cloud/1593827_1.html.

Customer security testing ExaC@C customer VM must be done in accordance with Oracle Cloud Testing Policies, published at https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_testing-policy.htm.

Oracle Audit Logging

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

- ILOM
  - `syslog`
  - ILOM `syslog` redirected to the `syslog` of the physical infrastructure component
- Physical Exadata Database Server
  - `/var/log/messages`
  - `/var/log/audit.log`
  - `/var/log/secure`
  - `/var/log/xen/xend.log`
- Exadata Storage Server
  - `/var/log/messages`
  - `/var/log/audit.log`
  - `/var/log/secure`
- Storage Network Switch
  - `/var/log/messages`
  - `/var/log/audit.log`
  - `/var/log/secure`
  - `/var/log/opensm.log`

Oracle retains the following audit logs for ExaC@C X8M and later hardware:

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

The retention period for Oracle infrastructure audit logs is 13 months. Infrastructure audit logs are accessible by Oracle security staff. In the event of a suspect security incident, Oracle and customer staff will work together to respond and resolve the issue per Oracle Incidence response policy, published at https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html.

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 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 ExaC@C resources.

SERVICE TERMINATION

Customers may terminate their ExaC@C instance as part of ExaC@C Lifecycle Management Operations.[50] Terminating an Exadata Cloud Service resource permanently deletes it and any databases running on it. The terminate service functionality is implemented as Exadata Database Machine Secure Erase.[51] The Exadata Secure Eraser automatically detects the hardware capability of a storage device and picks the best erasure method supported by the device. Cryptographic erasure is used whenever possible to provide better security and faster speed. The cryptographic erasure method used by Secure Eraser is fully compliant with the NIST SP-800-88r1 standard.

EXCEPTION WORKFLOWS - ORACLE ACCESS TO CUSTOMER VM

The ExaC@C 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 how Oracle staff can access the customer VM depend on if the customer VM can be accessed by the customer, or if the customer VM is not accessible by the customer. The processes and technology implementation to for these cases are described in the following sections.

Case 1: Customer Can Access the Customer VM

If the customer VM is accessible by the customer, then Oracle staff are not permitted to access to the customer VM from the Oracle managed infrastructure components. Instead, customer staff are required to access the customer VM using customer credentials, and then customer staff can share access to the customer VM using shared-screen technology (e.g., zoom, webex, skype, etc.). This access is controlled by the SR process as follows:

- Customer opens a Service Request (SR) indicating the failure
- Customer or Oracle opens a shared session and indicates session information in the SR[52]
- Oracle and customer staff access shared session information from the SR
- Customer accesses the customer VM using customer credentials
- Customer either enters commands to resolve the issue as instructed by Oracle staff, or customer permits the Oracle staff to control the keyboard entry for the VM session
- Customer updates the SR with diagnostics information
- Oracle staff update the SR with resolution information

[50] https://docs.oracle.com/en/cloud/cloud-at-customer/exadata-cloud-at-customer/exacc/delete-exadata-service-instance.html
[51] https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/exadata-secure-erase.html#GUID-6C9FD30C-FF88-4ABA-9249-93E183784B0D
[52] Customers using Operator Access Control should reference the Operator Access Control Tech Brief at https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/oracle-operator-access-control-tech-brief.pdf for additional customer controls and process updates for exception processing with Operator Access Control

Case 2: Customer Cannot Access the Customer VM

If the customer cannot access the customer VM, then specific process and technical controls can permit Oracle staff to access the customer VM from the infrastructure. This access is controlled by the SR process as follows:

- Customer opens a Service Request (SR) with the following language:
  - SR Title: "*SR granting Oracle explicit permission to access DomU of ExaCC with serial number AKXXXXXXXXX*"
  - SR Content: "*We are opening this SR to grant explicit permission to Oracle to access our DomU in order for support to help resolve issue described in SR# XXXXXXXX. We acknowledge that by providing this permission, we understand that Oracle will have access to ALL FILES in DomU and agree that there are no confidential files stored in any of the file systems in DomU. In addition, we also agree that customer security team has authorized Oracle to have access to customer DomU in order to resolve the issue described in the above SR.*"
- Oracle or customer will open a shared session and provide shared session information in the SR[53]
- With Oracle and customer both accessing the shared session, Oracle will use specific service accounts in the infrastructure to access customer VM and resolve issue; appropriate technical processes will be determined on a case-by-case basis and specific to the failure mode indicated in the SR

DATA PROCESSING AGREEMENT AUDIT

As part of the ExaC@C service, customers may audit Oracle's compliance with its obligations under this Data Processing Agreement (DPA) up to once per year. In addition, to the extent required by Applicable Data Protection Law, the customer or the customer's Regulator may perform more frequent audits. The Data Processing Agreement for Oracle Services[54] provides detail about how customers may request an audit and how the audit will be processed.

DEVICE AND DATA RETENSION

Oracle Customer Data and Device Retention for (DDR) Oracle Cloud at Customer[55] is an optional add-on service for ExaC@C. Oracle DDR permits the customer to retain eligible hardware items that may contain sensitive, confidential, or classified customer data (Retained Hardware) that have been removed from the ExaC@C hardware system placed onsite in the customer's data center for the customer's ExaC@C subscription.

For purposes of DDR, Retained Hardware refers to the following:

- Hard disk drives (HDD)
- Solid-state drives (SSD)
- Persistent memory (PMEM) components

ORACLE OPERATOR ACCESS CONTROL

An impediment to bringing a class of applications supporting mission critical and highly regulated workloads to a cloud platform is the shared responsibility model inherent to a cloud platform. In this model, the cloud service provider retains control to manage a subset of the system, such as the infrastructure (cloud provider tenancy), and the customer retains control to manage another part of the system, such as virtual machines, applications, and databases (customer tenancy). For mission critical and highly regulated workloads, the customer may have the responsibility to control the actions any person takes when accessing the any part of the system, including the actions by the cloud provider staff in the cloud provider

[53] Customers using Operator Access Control should reference the Operator Access Control Tech Brief at https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/oracle-operator-access-control-tech-brief.pdf for additional customer controls and process updates for exception processing with Operator Access Control.

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

[55] https://www.oracle.com/assets/customer-data-device-retention-sd-4419287.pdf

tenancy. To meet these requirements, Oracle customers can use Oracle Operator Access Control (OpCtl)[56] with Exadata Cloud@Customer (ExaC@C) and Autonomous Database Dedicated (ADB-D) on ExaC@C.

OpCtl is an Oracle Cloud Infrastructure (OCI) Privileged Access Management (PAM) service for ExaC@C. OpCtl provides the customer interfaces to

- Control when and how much access Oracle staff have to ExaC@C infrastructure
- Observe and record Oracle operator commands and keystrokes Oracle staff execute on ExaC@C infrastructure
- Terminate Oracle operator connections at the customer's discretion

These controls are a standard part of the ExaC@C service and are available at no extra cost to Oracle customers.

OpCtl is the right feature for use cases where customers need to control Oracle Cloud Ops staff login to infrastructure to meet the same standards applied to customer staff accessing customer managed systems. For example, OpCtl is ideal for banking and financial services applications, energy utilities, and defense, and any other application where risk management is a key pillar of application success.

OpCtl preventive security control features include the following:

- Oracle staff access only when authorized by the customer and only for a specific Oracle work request
- Oracle staff access is limited to explicitly approved components related to a stated and specific work request
- Oracle staff access is temporary, and is automatically revoked after the authorized task is completed or a timeout is reached
- Customer control over when Oracle staff can access infrastructure
- Software enforcement of privilege escalation by Oracle staff

OpCtl detective security control features include the following:

- Customer notification when Oracle staff need to access infrastructure
- Command and keystroke logging for actions taken by Oracle staff
- Commands and keystrokes are traceable to an individual person
- Customer security monitoring of all commands and keystrokes entered by Oracle staff
- Oracle-supplied record of the Oracle staff identity to the customer when required for any command executed
- Oracle security staff monitoring of all Oracle Cloud Ops staff activities

OpCtl responsive security control features include the following:

- Customer control to terminate Oracle staff access and all processes started by Oracle staff at any time
- Oracle security staff control to terminate Oracle staff access and all processes started by Oracle staff at any time

A complete description of the OpCtl service for ExaC@C Infrastructure is available from the Operator Access Control product documentation.[57]

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

[57] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-7CF13993-DB16-485A-A9FA-399E0049740B

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 ExaC@C service ensure that Oracle Cloud Operations staff only perform authorized actions on the infrastructure components of ExaC@C. 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 ExaC@C service, and customers do not access Oracle managed infrastructure to consume ExaC@C Service. In the ExaC@C 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 2222
Author: [OPTIONAL]
Contributing Authors: [OPTIONAL]