ORACLE

Exadata Database Service on Cloud@Customer Security Controls

A Technical Summary for Security Approvers and Developers

April 17, 2026 | Version 2.37

PURPOSE STATEMENT

This document provides an overview of security features and enhancements you can use with Exadata Cloud Releases 25.2.6.0.0.260117 and 25.1.13.0.0.260117. It is intended solely to help you assess the business benefits of upgrading to 25.2.6.0.0.260117 and 25.1.13.0.0.260117 and to plan your IT projects.

Exadata Database Service on Cloud@Customer (ExaDB-C@C) requires that you allow the infrastructure to make outbound connections from your data center to the OCI endpoints used by the service and Oracle to:

- Choose the staff that maintain the infrastructure
- Provide identity management services for that staff
- Use Oracle-provided software and hardware to access to the infrastructure
- Perform all infrastructure maintenance, including periodic superuser (`root`) access
- Access Oracle-managed components necessary to maintain the service and resolve issues

ExaDB-C@C lets you choose a control model for Oracle staff shell access to the infrastructure:

- Oracle-controlled: access granted after Oracle approves access
- Customer-controlled: access granted after you approve access with Operator Access Control

This paper describes the security controls built into ExaDB-C@C to help you evaluate them for your use cases. These controls follow industry best practices to protect your data and mission-critical workloads. If your current security standards differ, this paper suggests alternative controls so you can update or adjust your policies.

DISCLAIMER

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

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

TABLE OF CONTENTS

LIST OF IMAGES

LIST OF TABLES

INTRODUCTION

ExaDB-C@C delivers Exadata as a managed cloud service in your data center. You get all Exadata features, OCI orchestration, and Oracle support. The service helps you secure your data in the ExaDB-C@C rack on your premises. You control

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

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

ROLES AND RESPONSIBILITIES

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

Your responsibilities include securing, monitoring, and managing your:

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

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

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

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

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

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

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

Oracle staff are not authorized to access your VMs and databases, except in specific support cases described in Exception Workflows for Oracle Access to Your VM.

Detailed breakdowns of roles and responsibilities are provided in Table 1 and Exadata Database Service on Cloud at Customer (ExaDB-C@C) - Explanation Of Cloud Operations Service (KB40460).

Table 1: Roles and responsibilities

WORK FUNCTION	ORACLE-MANAGED INFRASTRUCTURE		YOUR SERVICES	
	Oracle Cloud Operations	Your Staff	Oracle Cloud Operations	Your Staff
Monitoring	Infrastructure, control plane, hardware faults, availability, capacity	Provide network access to support Oracle infrastructure log collection and monitoring	Infrastructure availability to support your monitoring of your services	Monitoring of your 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 your 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 your VMs	Provide network access to support cloud automation delivery	Provide running and accessible VM	Snapshots / Backup & Recovery of your IaaS and PaaS data using Oracle native or third-party capability
Cloud Support	Response & Resolution of SRs related to infrastructure or subscription issues	Submit SRs via MOS	Response & Resolution of SR	Submit SRs via Support Portal

ARCHITECTURE OVERVIEW

Figure 1 shows the ExaDB-C@C architecture. The service is deployed Exadata Database Servers and Storage Servers in a Oracle rack in your data center. You can use your rack with approval from Oracle. The rack contains all the components of a standard Exadata Database Machine, plus 2 control plane servers (CPS) in a highly available (active/standby) configuration. The CPS connects the Exadata rack to the control plane so that you and Oracle can manage the service. You choose the OCI region that delivers your service and control network access from the CPS to OCI management endpoints. An RDMA over Converged Ethernet (RoCE) network isolates your Exadata Storage and Real Application Cluster (RAC) traffic using VLAN technology.

Oracle Cloud Infrastructure supports identity federation with:

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

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

- Web User Interface (Web UI): for ad hoc actions via OCI Console
- OCI Cloud Shell (Cloud Shell): a browser-based Linux shell within the OCI Console
- OCI Command-Line Interface (OCI CLI): command-line interface for scripting and automation
- OCI SDK/REST API: for application integration
- OCI Terraform Provider with documentation provided by HashiCorp

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

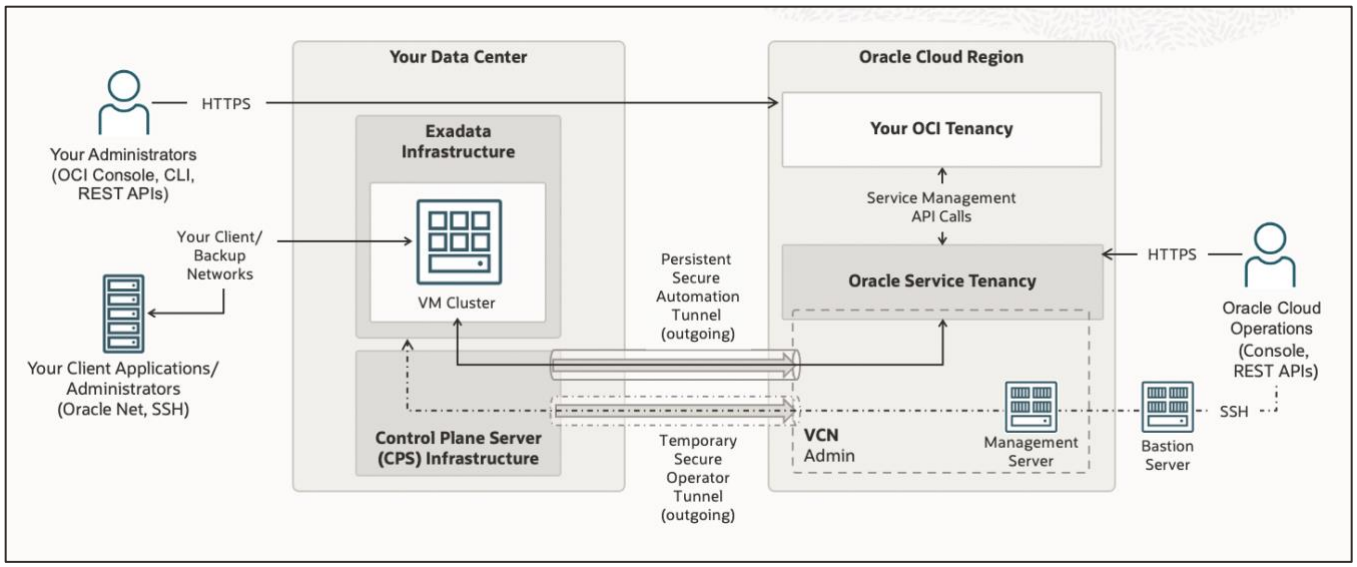

Figure 1: ExaDB-C@C architecture

The control plane sends commands to the necessary components through the Persistent Secure Automation Tunnel, as follows:

Database operations:

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

VM operations:

- Token-based SSH from CPS processes to service accounts
- Secured by temporary keys managed by the control plane and delivered via agent software in the VM
- Transported over the management network

Infrastructure operations:

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

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

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

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

SECURITY CONTROLS

ExaDB-C@C helps you protect your databases from unauthorized access. You control the physical access to the Exadata hardware, and logical access to your OCI tenancy, VMs, databases, and data. Oracle controls logical infrastructure access, and you can use Operator Access Control to control Oracle staff shell access to the ExaDB-C@C infrastructure.

Your authentication and authorization controls (Figure 2) include credentials for:

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

Your encryption controls include:

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

Your network security controls include:

- Switch and firewall network security controls for ExaDB-C@C infrastructure access to your OCI region (Figure 6)
- Switch and firewall network security controls to your VMs and databases (Figure 6)
- Network access rules in your VM operating system and Oracle Connection Manager

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

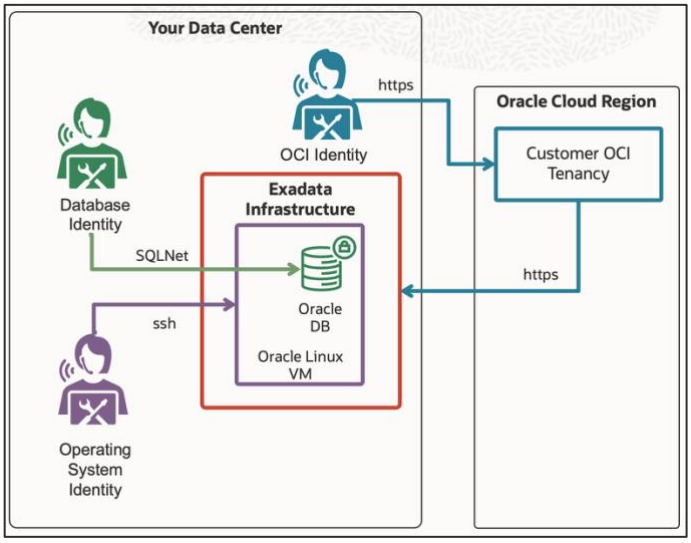

Figure 2: Your OCI, database, and operating system identities

Database Security Controls

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

Database Authentication

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

Network Encryption

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

Data at Rest Encryption

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

- PKCS#12 wallet
- Oracle Key Vault
- Compatible third-party HSM

Oracle TDE is engineered to be highly performant. It automatically leverages special instructions in Intel CPUs (AES-NI) to accelerate cryptographic operations. In addition, TDE tablespace encryption works seamlessly with Exadata Hybrid Columnar Compression (EHCC) and Smart Scan technology. With TDE, sensitive user data remains encrypted throughout the database, whether it is in tablespace storage files, temporary or undo tablespaces, or other files such as redo logs. In addition, TDE can encrypt entire database backups. Data Pump and Oracle Recovery Manager (RMAN) both integrate with TDE encrypted data. Oracle AI Database 26ai integrates the cryptographic algorithms necessary to help protect your database against quantum attacks. For further information on Oracle TDE, consult the Advanced Security Guide for your Oracle AI Database version. The Oracle TDE FAQ provides answers to common architecture and implementation questions.

Encryption Key Management with PKCS#12 Wallet

The TDE MEK is stored outside of the database, by default in a PKCS#12-compliant container called a 'wallet'. The wallet is stored in a shared file system accessible by your ExaDB-C@C VMs. Oracle Databases 18c and later allow you to upload your own, externally generated encryption keys (called Bring-Your-Own-Key, BYOK) into the shared wallet, maintaining separation of duties between the database administrators and key custodians.

Encryption Key Management with Oracle Key Vault

You can use Oracle Key Vault (OKV) to store your TDE MEK for your ExaDB-C@C databases. OKV provides continuous online key management to all TDE-enabled databases and encrypted GoldenGate trail files. It also provides the capability to ingest externally generated keys (BYOK). You can use the OKV Persistent Master Encryption Key Cache to enable databases to be operational if the OKV server is unavailable. See Migration of File based TDE to OKV for Gen 2 ExaDB-C@C Using REST for more detail.

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

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

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

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

Database Backup Encryption

ExaDB-C@C automation supports backups to:

- Both cloud storage and Exadata storage
- Cloud storage only
- Zero Data Loss Recovery Appliance (ZDLRA) only

ExaDB-C@C encrypts database backups with the same master key used for the Transparent Data Encryption wallet encryption, as described in the ExaDB-D Security Guide. The encryption key is not stored with the backup. You are responsible for backing up and restoring your TDE master encryption key. When you use the Zero Data Loss Recovery

Appliance, backups of encrypted tablespaces, and redo describing changes to these tablespaces, are encrypted. The TDE-encrypted data blocks are encrypted on the database, Recovery Appliance storage, tape devices, and replicated appliances, and when transferred through any network connections.

Preventing Database Administrators from Accessing User Data with SQL

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

Mitigating SQL Injection Attacks

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

SQL Firewall helps to address the following three use cases:

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

SQL Firewall offers the following benefits:

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

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

Database Security Monitoring and Management

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

Oracle Data Safe

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

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

Oracle Data Safe Technical Architecture shows an on-premises connector deployed on your servers to connect databases running on ExaDB-C@C to the Data Safe service. The Data Safe FAQ provides answers to commonly asked questions about Oracle Data Safe. There is no additional cost to use Data Safe so long as you do not exceed one million audit records per database in a month.

Oracle Database Security Assessment Tool

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

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

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

VM Security Controls

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

Minimal package installation and enabled services:

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

Secure configuration:

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

Secure access methods:

- Accessing Database Servers via SSH using strong cryptographic ciphers
- Weak ciphers are disabled by default
- Accessing diagnostics via Exadata MS Web UI (HTTPS)

Auditing and logging:

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

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

Exadata software version 22.1.4.0.0.221020 and newer supports Microsoft Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) for authentication to your VMs. You configure AD and LDAP using the Linux System Security Services Daemon (SSSD). SSSD support is enabled in conjunction with an Exadata-specific security profile using the Linux `authselect` utility on Oracle Linux 8. Oracle Exadata System Software maintains the existing SSSD configuration details during system updates.

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

VM Default Security Settings

The ExaDB-C@C VM is deployed with security settings aligned to industry standards and Oracle best practices. These configurations help to enforce access control, reduce operational risks, and support automated lifecycle management. Key settings include:

- Password aging and complexity
- Account lockout and session timeout policies
- Deny direct root login via SSH

Technical configurations include:

- `PermitRootLogin` value in `/etc/ssh/sshd_config`, which permits or denies the root user to log in through SSH
  - Default: PermitRootLogin is set to without-password
  - Recommendation: keep default to permit cloud automation capabilities like OS patching
- `session-limit`: Sets the hard `maxlogins` parameter in `/etc/security/limits.conf`, which is the maximum number of logins for all users. This limit does not apply to a user with `uid=0`
  - Default: `hard maxlogins 10`
  - Recommendation: keep default
- `ssh-macs`: Specifies the available Message Authentication Code (MAC) algorithms
- The MAC algorithm is used in protocol version 2 for data integrity protection
  - Default: hmac-sha1, hmac-sha2-256, hmac-sha2-512 for both server and client
  - Recommendation: keep default
- `password-aging`: Sets or displays the current password aging for interactive user accounts
  - `-M`: Maximum number of days a password may be used
  - `-m`: Minimum number of days allowed between password changes
  - `-W`: Number of days warning given before a password expires
  - Default: `-M 99999`, `-m 0`, `-W 7`
  - Recommendation: for strict compliance `-M 60`, `-m 1`, `-W 7`

Shell timeouts are configured to allow long-running automation tasks (e.g., ASM rebalance). These values are part of the service configuration and should be allowed by security scanning tools.

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

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

VM Default Users

Each ExaDB-C@C VM includes standard privileged service accounts used by Oracle software to deliver and maintain the service. Token-based SSH login is required. Password-based SSH login is disabled. Service accounts include:

- `root`: required by Linux; used for software updates and some background processes (e.g., Oracle Trace File Analyzer Agent and ExaWatcher)
- `grid`: owns, runs, and maintains the Oracle Grid Infrastructure software and processes
- `oracle`: owns, runs, and maintains the Oracle Database software and processes
- `opc`: used by Oracle cloud automation
  - Performs automation tasks
  - Can run certain privileged commands
  - Runs control plane agent software (DBCS Agent and DBCS Admin) for service lifecycle operations
- `dbmadmin`: used with the DBMCLI tool to manage core Exadata features.

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

You must retain the deployed usernames, userids, group names, and group ids. Changing the Oracle Home user (`oracle`) or Grid Infrastructure user (`grid`) after install is not supported and will cause service exceptions.

VM File Integrity Monitoring

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

VM Backup Encryption

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

Cloud Automation Access to Your VM

Cloud automation software accesses your databases and VM two ways:

- REST API call to the DBCS agent using mTLS on port 7060/7070 through the storage network
- Secure login to your VM as a privileged user using token-based SSH through the management network

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

Your VM includes the Oracle Linux packet filtering software as an additional data protection control to block network access to the VM. Blocking SSH access from the control plane will break the following service functionality:

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

OCPU scaling does not require SSH access to the VM and will continue to function if you block cloud automation access to the VM at the network layer.

Controlling Oracle Services and Support Staff Access to Your VM

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

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

When you use Delegate Access Control:

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

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

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

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

Figure 3 shows the Delegate Access Control approval and access workflow. Delegate Access Control uses the same delivery mechanics as Operator Access Control and is included in the scope of the Operator Access Control PCI-DSS attestation of compliance (AoC).

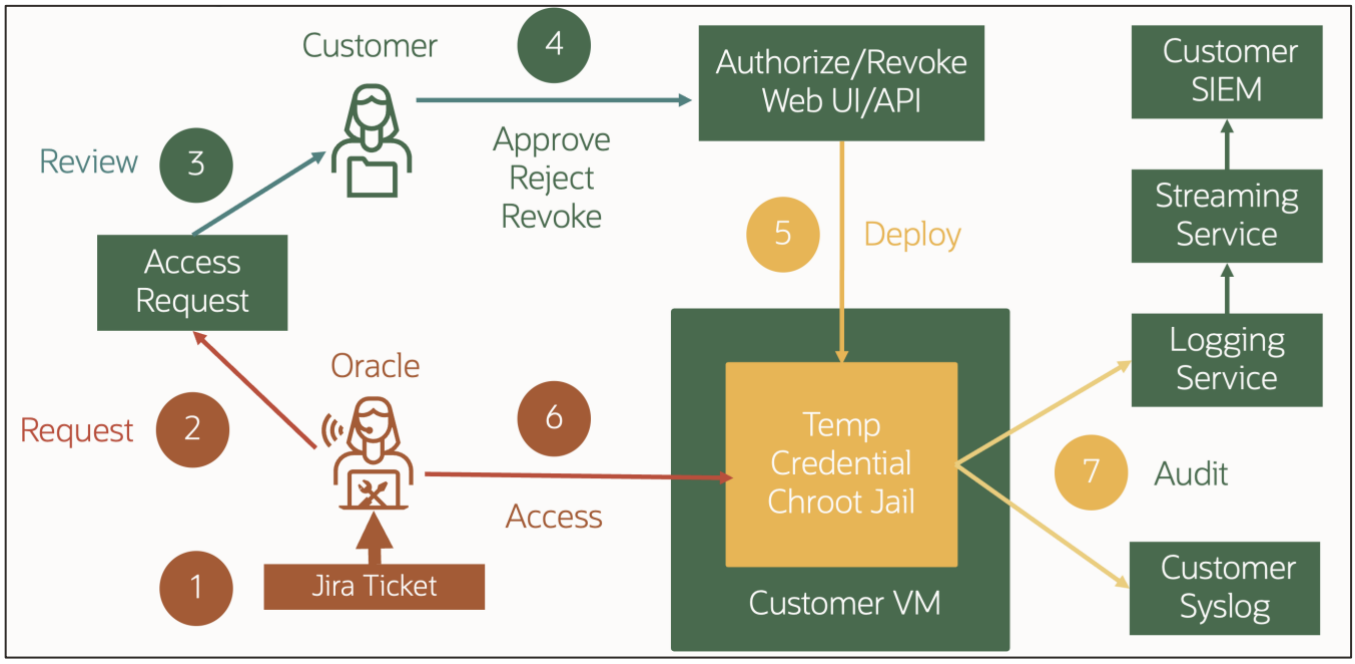

Figure 3: Delegate Access Control approval workflow

Network Security Controls

You can use your on-premises network security controls and OCI security features with ExaDB-C@C. This section summarizes these controls.

Controlling Your On-premises Networks

You can use your network security controls with the ExaDB-C@C client and backup networks. Your controls must allow the ExaDB-C@C service to function, including:

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

Your Oracle Grid Infrastructure network traffic flows through the internal storage network of ExaDB-C@C and is not affected by your client and backup network controls. You must allow the ExaDB-C@C infrastructure to access OCI services, as described in the appendix of this document. You can isolate these network connections from your client and backup networks. See the Network Architecture Diagram in the Technical Appendix of this document for more details.

Controlling OCI Networks

You can use compatible OCI network security controls with your ExaDB-C@C service, including:

- FastConnect or site-to-site VPN, to connect your ExaDB-C@C infrastructure to OCI (Figure 7)
- Transit Routing and Network Security Lists to help control ExaDB-C@C infrastructure access to OCI services.
- VCN Flow Logs to monitor traffic volume to network endpoints in Transit VCNs
- Network Firewall in your Transit VCN to allow access to URLs and IP addresses supporting ExaDB-C@C
- Service Gateway in your Transit VCN to provide access to OCI services without exposing traffic to the internet

Private Service Access (PSA) is not supported for ExaDB-C@C management connections. Implementing PSA for ExaDB-C@C management connections will cause service exceptions.

Additional OCI Security Controls

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

Controlling Which Networks Can Authenticate to Your Tenancy Resources

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

Denying Specific API Actions in Your Tenancy

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

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

Controlling Your Administrators' Use of Privileged APIs

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

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

Before a privileged API can be invoked, the user intending to invoke the API must raise an Access Request with their OCI identity, and a different OCI identity must approve the Access Request. Figure 4 shows the API Access Control approval workflow. See API Access Control at the Oracle Learning Center for more details. API Access Control is included with no additional charge.

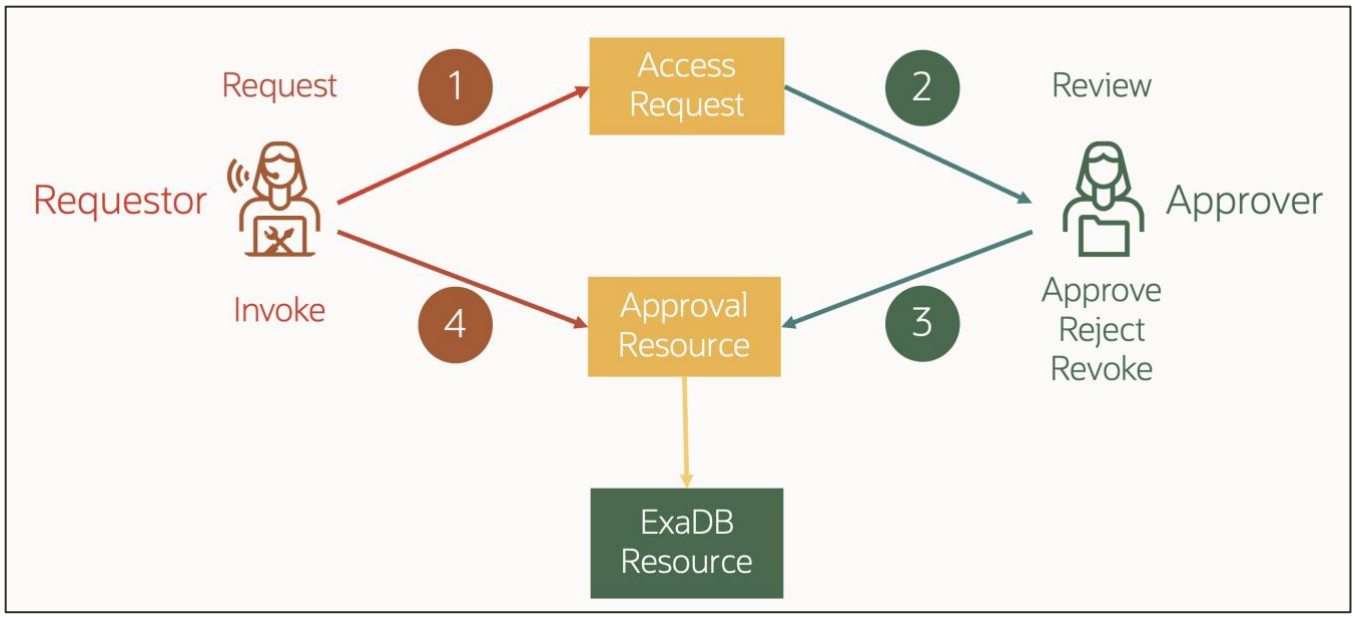

Figure 4: API Access Control approval workflow

Ransomware Recovery

Zero Data Loss Recovery Appliance (ZDLRA) is engineered for database ransomware protection. It has four key technology pillars:

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

Recovery Appliance has Resiliency and Recoverability from Cyber-Attacks. It is designed to be fault-isolated from the production database. If a cyber-attack hits the production database, the Recovery Appliance is not compromised. Oracle recommends using ZDLRA to help protect Oracle databases from ransomware.

Oracle Infrastructure Security Controls

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

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

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

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

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

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

OCNA access:

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

Bastion host access:

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

ExaDB-C@C management server and infrastructure access:

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

Figure 5 shows how Oracle Cloud Operations staff access ExaDB-C@C infrastructure components.

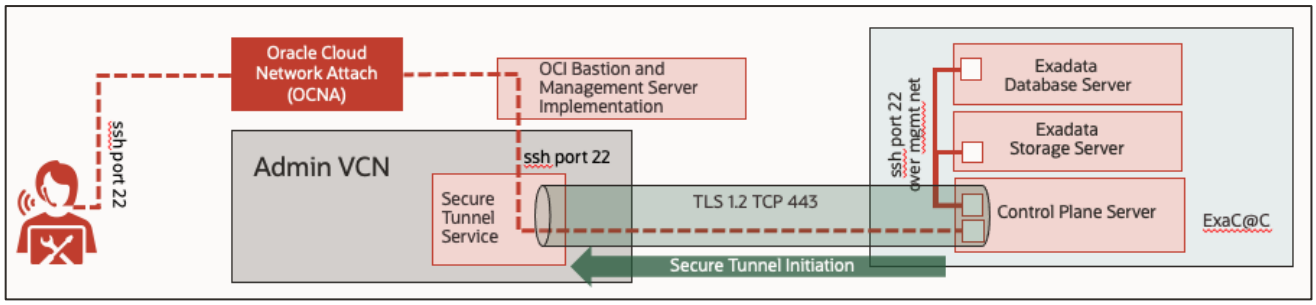

Figure 5: Cloud Operations shell access to ExaDB-C@C Infrastructure

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

Controlling Oracle Staff Shell Access to Your Infrastructure

Running mission-critical or highly regulated workloads in the cloud is challenging because of the shared responsibility model. In this approach, the cloud provider manages the infrastructure, while you oversee your virtual machines, applications, and databases. If you are accountable for every action taken on your environment, including those by cloud provider staff on your dedicated infrastructure, Oracle Operator Access Control helps you address this oversight need. It's designed for organizations where risk management is vital: banking, financial services, energy, defense, and any environment requiring strict operational control. You can use it with ExaDB-C@C and Autonomous Database Dedicated (ADB-D)

Operator Access Control is a privileged access management (PAM) service you integrate with your change management processes and systems to:

- Control when and how much access Oracle staff have to ExaDB-C@C infrastructure and ADB-D VMs
- Observe and record Oracle operator commands and keystrokes Oracle staff execute on ExaDB-C@C infrastructure
- Terminate Oracle operator connections at your discretion

These controls are a standard part of the ExaDB-C@C service and are available at no extra cost. When you use Operator Access Control, access is:

- Granted after it is requested by Oracle and approved by you

- Implemented with unique temporary accounts specific to the work request and traceable to individual persons
- Limited to explicitly approved components related to a stated and specific work request
- Limited to the duration of the work request
- Automatically revoked after the task is completed or a timeout is reached

Operator Access Control Action Enforcement controls privilege limits for Oracle operators. Operator Access Control Audit Logs are traceable to an individual person. Oracle can provide Oracle staff identity details when required for investigations or compliance purposes.

You can revoke Oracle operator access. Operator Access Control revocation:

- Terminates SSH sessions
- Terminates processes started by temporary accounts
- Removes temporary accounts from ExaDB-C@C infrastructure and ADB-D VM

You must monitor and respond to Operator Access Control Access Requests around the clock (24x7x365) to support the ExaDB-C@C service. Use OCI Events and Notifications to automatically alert your staff when new requests occur. You can integrate systems like Splunk or ServiceNow to streamline your response process.

If you can't monitor and respond to every request, or if automated approval meets your needs, use Operator Access Control's preapproval feature. Preapproval gives you temporary, just-in-time access and full audit logs, without requiring staff to approve each request in OCI. This reduces operational burden and lowers the risk of delays causing bigger issues or outages. Configure preapproval for maintenance windows to streamline updates. Selectively pre-approve lower privileges while requiring explicit approval for higher privileges to help you balance risk and operational efficiency.

You can integrate Operator Access Control audit logs with compatible third-party software products. This includes sending audit logs to your syslog server and integrating the OCI Logging service with Splunk. See the Operator Access Control product documentation and Operator Access Control Tech Brief for detail.

AUDITING AND LOGGING

ExaDB-C@C provides auditing and logging for your services and Oracle-managed infrastructure. The service separates monitoring duties as follows:

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

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

Database Audit Logging

ExaDB-C@C provides comprehensive audit logging for the database with Oracle AI Database Unified Audit. You can send these audit records to your syslog server or compatible security information event management (SIEM) system. Oracle publishes documentation for configuring, managing, and monitoring of Oracle AI Database audit logs in the Oracle AI Database Security Guide for each database version. See Oracle AI Database Unified Audit: Best Practice Guidelines for more detail.

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

VM Audit Logging

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

OCI Audit Logging

OCI Audit automatically records calls to all supported Oracle Cloud Infrastructure public application programming interface (API) endpoints as log events. All services support logging by Audit. Object Storage service supports logging for bucket-related events, but not for object-related events. Log events recorded by Audit include API calls made by the OCI Console,

Command-Line Interface (CLI), Software Development Kits (SDK), your own custom clients, and other Oracle Cloud Infrastructure services. Information in the logs includes:

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

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

Oracle Infrastructure Audit Logging

Oracle is responsible for recording, analyzing, and responding to infrastructure audit logs. Infrastructure audit logs for ExaDB-C@C X8 and earlier hardware include the following:

ILOM:

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

Physical Exadata Database Server:

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

Exadata Storage Server:

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

Storage Network Switch:

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

Audit logs for ExaDB-C@C X8M and later hardware include the following:

ILOM:

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

Physical Exadata Database Server:

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

Exadata Storage Server:

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

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

Operator Access Control and Delegate Access Control Audit Logging

Operator Access Control and Delegate Access Control Logs provide you with command and keystroke logs for Oracle staff shell access. Oracle Linux auditd generates these logs. You can send these logs to your local SIEM system and your OCI Logging service. You can forward these logs to compatible systems and process them with compatible technology. Both services provide API and OCI Console interfaces that generate human-readable HTML files. These files summarize keystroke (TTY) and command records to show you the operations done and order of operations. The services redact sensitive information, such as user passwords, from the log files.

INCIDENT RESPONSE

You and Oracle work together to secure and monitor access to ExaDB-C@C components. If either party detects an unauthorized action, that party can take responsive action immediately, prior to notifying the other party. If you detect an unauthorized action, notify Oracle of the action and response using the Oracle Service Request (SR) process.

Your Responsive Controls

You can take any responsive action on any services or equipment you control. This includes terminating Operator and Delegate Access Control Access Requests, network connections into your VM, and network connections between the CPS and OCI resources. Your databases should continue to function normally if you terminate connections between the CPS and OCI. Oracle's responsive controls include terminating connections at Bastion hosts in OCI, revoking access to Oracle-managed ExaDB-C@C infrastructure, and disconnecting ExaDB-C@C infrastructure from the control plane.

Oracle Incident Response Process

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

"Oracle's Security Incident Management Policy defines requirements for reporting and responding to information security events and incidents. This policy authorizes the Oracle Chief Security Officer organization to provide overall direction for security event and incident preparation, detection, investigation, resolution and forensic evidence handling across Oracle's Lines of Business (LoB). This policy does not apply to availability issues (outages) or to physical security events.

The Integrated Cyber Center (ICC) is the entity responsible for centralized coordination of security incident response, customer trust and security communications matters.

LoB incident response programs must:

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

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

If Oracle determines a security incident involving assets managed by Oracle has occurred, Oracle will promptly notify impacted customers or other third parties in accordance with its contractual and regulatory responsibilities as defined in the Data Processing Agreement for Oracle Services. Information about malicious attempts, suspected incidents and incident history are not shared externally."

15-Minute Service Response Time for Critical Issues

Oracle Cloud Hosting and Delivery Policies describe Oracle's 15-minute service response time for critical issues, including security incidents:

"5.3.1 Severity 1 (Critical Outage)

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

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

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

SOFTWARE SECURITY AND UPDATES

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

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

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

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

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

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

Development and debug tools to inspect your data are not installed on ExaDB-C@C infrastructure. Oracle signs and encrypts software updates prior to transmission from OCI to ExaDB-C@C infrastructure to help prevent tampering.

SECURITY TESTING AND SCANNING

Security Testing and Scanning of Your VM

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

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

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

Security Testing and Scanning of Oracle-Managed Infrastructure

Oracle requires security analysis and testing on Oracle products.

Oracle performs monthly infrastructure security scans and updates to ExaDB-C@C infrastructure to remain in compliance with Oracle corporate security standards. These standards align with and support various industry standards, including PCI-DSS, and government security standards, including FedRAMP High and ISO/IEC 27001. Oracle performs updates to infrastructure online, with no reboot, and designed to have no impact on compatible applications. Oracle applies monthly security updates to Storage Servers in a rolling manner, also designed to have no impact to applications. You may schedule monthly security maintenance at a specific time during the month, albeit in a single maintenance window. Oracle will publish a schedule for monthly maintenance at least one week prior to start of the maintenance period. You may reschedule if required. You are not permitted to access infrastructure components directly, nor can you install monitoring agents or transfer files to Oracle-managed infrastructure.

CUSTOMIZATION AND THIRD-PARTY SOFTWARE

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

Oracle will not provide technical support for non-Oracle software. This includes installation, testing, certification, and error resolution. The supplier of the custom/third-party software is responsible for any technical support for it. Oracle recommends that all non-Oracle software be certified by the vendor for use in an Oracle Linux and/or Exadata environment and thorough testing is performed in the target environment by you. Details for third-party software support on ExaDB-C@C are published on My Oracle Support document, Installing Third-Party Software on Exadata Components (KB144164).

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

Compatible Service Modifications

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

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

Required Service Configuration

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

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

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

Shell timeouts are configured to allow long-running automation tasks (e.g., ASM rebalance). These values are part of the service configuration and should be allowed by security scanning tools.

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

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

SERVICE TERMINATION AND DATA DESTRUCTION

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

DEVICE AND DATA RETENTION

Oracle Customer Data and Device Retention for (DDR) Oracle Cloud at Customer is an optional add-on service for ExaDB-C@C. Oracle DDR permits you to retain eligible hardware items that may contain your sensitive, confidential, or classified data (Retained Hardware) that have been removed from the ExaDB-C@C. For purposes of DDR, Retained Hardware refers to the following components of Exadata database servers, storage servers, and CPS.

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

EXCEPTION WORKFLOWS FOR ORACLE ACCESS TO YOUR VM

ExaDB-C@C includes exception cases where a failure in your VM requires Oracle staff to access your VM to resolve the issue as described in the ExaDB-D Security Guide. The process and technical controls that govern how Oracle staff can access your VM depend on the following:

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

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

VM is Controlled by Delegate Access Control

If you implement Delegate Access Control and subscribe to Oracle Cloud Customer Support and Oracle Cloud Operation, then Oracle Cloud Support and Cloud Operations support staff will issue a Delegate Access Control Access Request to you. After your approval, the Oracle support staff will access the VM using a unique, temporary, just-in-time credential deployed for least-privileged access controlled by Action Enforcement to do the work. The Oracle Linux audit service will provide command/keystroke logs to you via OCI Logging service. You can send the Oracle Linux audit logs to your syslog server.

VM is Accessible by You

If you can access your VM, then you share your VM access with Oracle staff using remote collaboration technology (e.g., Zoom, Webex, Skype, etc.). This access is controlled by the SR process:

- You open a Service Request (SR) indicating the failure

- You or Oracle open a shared session and indicate session information in the SR
- You and Oracle access the shared session information from the SR
- You access the VM using your credentials
- You either enter commands to resolve the issue as instructed by Oracle staff, or you permit the Oracle staff to control the keyboard entry for the VM session
- You update the SR with diagnostics information
- Oracle staff update the SR with resolution information

VM is not Accessible by You

If you cannot access your VM, or the VM is not accessible via remote login from infrastructure networks (e.g., VM is crashed), then specific process and technical controls can permit Oracle staff to access your VM from the infrastructure. This access is controlled by you and Oracle through the Oracle Service Request (SR) process, and Operator Access Control (if implemented):

- If you are willing to permit Oracle Cloud Operations to access your VM without direct supervision, then you open a Service Request (SR) with the following language:
  - SR Title:
    - SR granting Oracle explicit permission to access a Guest VM of ExaCC with VM Name <insert VM Name as listed under the DB Server detail page→ Resources→ Virtual Machines>
  - SR Content:
    - We are opening this SR to grant explicit permission to Oracle to access our Guest VM in order for support to help resolve the issue described in SR# 1-xxxxxxxx. We acknowledge that by providing this permission, we understand that Oracle will have access to all files and memory that are part of the Guest VM. In addition, we also agree that the customer security team has authorized Oracle to have access to the customer Guest VM in order to resolve the issue described in the above SR.
    - DB Server OCID: <insert OCID of DB Server hosting the VM here>
    - VM Name: <insert VM Name as listed under the DB Server detail page→ Resources→ Virtual Machines>
- If you require Oracle to offer a shared screen to permit direct supervision of the Oracle Cloud Operations access, you open a Service Request (SR) with the following language
  - SR Title:
    - SR granting Oracle explicit permission to access a Guest VM of ExaCC with VM Name <insert VM Name as listed under the DB Server detail page→ Resources→ Virtual Machines>
  - SR Content:
    - We are opening this SR to grant explicit permission to Oracle to access our Guest VM in a shared screen session in order for support to help resolve the issue described in SR# 1-xxxxxxxx. We acknowledge that by providing this permission, we understand that Oracle will have access to all files and memory that are part of the Guest VM. This permission to access our VM is contingent on our representative being able to monitor in real-time via a screen-sharing session all activities performed by Oracle. In addition, we also agree that the customer security team has authorized Oracle to have access to the customer Guest VM via this shared screen session in order to resolve the issue described in the above SR.
    - DB Server OCID: <insert OCID of DB Server hosting the VM here>
    - VM Name: <insert VM Name as listed under the DB Server detail page→ Resources→ Virtual Machines>
- If you implement Operator Access Control, Oracle will open an Operator Access Control Access Request to resolve the issue; you must approve the Operator Access Control Access request to permit Oracle staff access to the appropriate system components
- Operator Access Control provides command and keystroke logging in near real time (<60 seconds) to your syslog server and/or the OCI Logging service in your tenancy

With you and Oracle both accessing the shared session, Oracle will work to resolve the issue. Appropriate technical processes will be determined on a case-by-case basis and specific to the failure mode indicated in the SR.

SUMMARY

With ExaDB-C@C, you control the security features throughout the VM. Oracle AI Database encryption encrypts data, and you retain control of the encryption keys. Oracle AI Database security features control authentication and access to data in

the database, and you retain control of credentials and authorization. Oracle Linux authentication features control access to the VM, and you retain control of credentials and authorization.

Security and auditing features throughout the Oracle-managed components of ExaDB-C@C help to prevent unauthorized actions on the infrastructure components of ExaDB-C@C. Security measures include named user access authenticated by FIPS 140-2 Level 3 hardware MFA devices for Oracle-managed infrastructure components. Auditing and logging are implemented throughout the stack, and applicable audit logs are available to you through VM, Oracle Database, OCI services, and the Oracle Service Request (SR) process.

The combined security and auditing postures of your and Oracle's components separate duties and deliver the benefit of a high-security on-premises deployment with the ease of use and economics of the cloud. You and Oracle Cloud Operations work together to configure system security and help prevent unauthorized access to and theft of your data. In the ExaDB-C@C deployment model, you gain the security of an on-premises deployment with the benefits of cloud economics, agility, and scale.

TECHNICAL APPENDIX

Network Architecture Diagram

Figure 6 shows the ExaDB-C@C Network Architecture. Figure 7 shows how to use a site-to-site VPN or FastConnect with a Transit VCN. The CPS accesses OCI through your switches, routers, and proxy servers. Table 2 and Network Requirements for ExaDB-C@C show the URLs required for service delivery. Access to URLs is outbound on port 443 only. You can impose network access rules to deny inbound access to the CPS and to only permit outbound access to required Oracle endpoints. The service supports `http` proxy (e.g., corporate proxy, passive proxy) to manage connections from the CPS to OCI endpoints. ExaDB-C@C does not support challenge proxies or SSL decryption (traffic inspection). You may need to update your permitted URLs when Oracle adds new features to the service. If you use IP address filtering, you must allow traffic to all the relevant IP CIDR ranges associated with your OCI region.

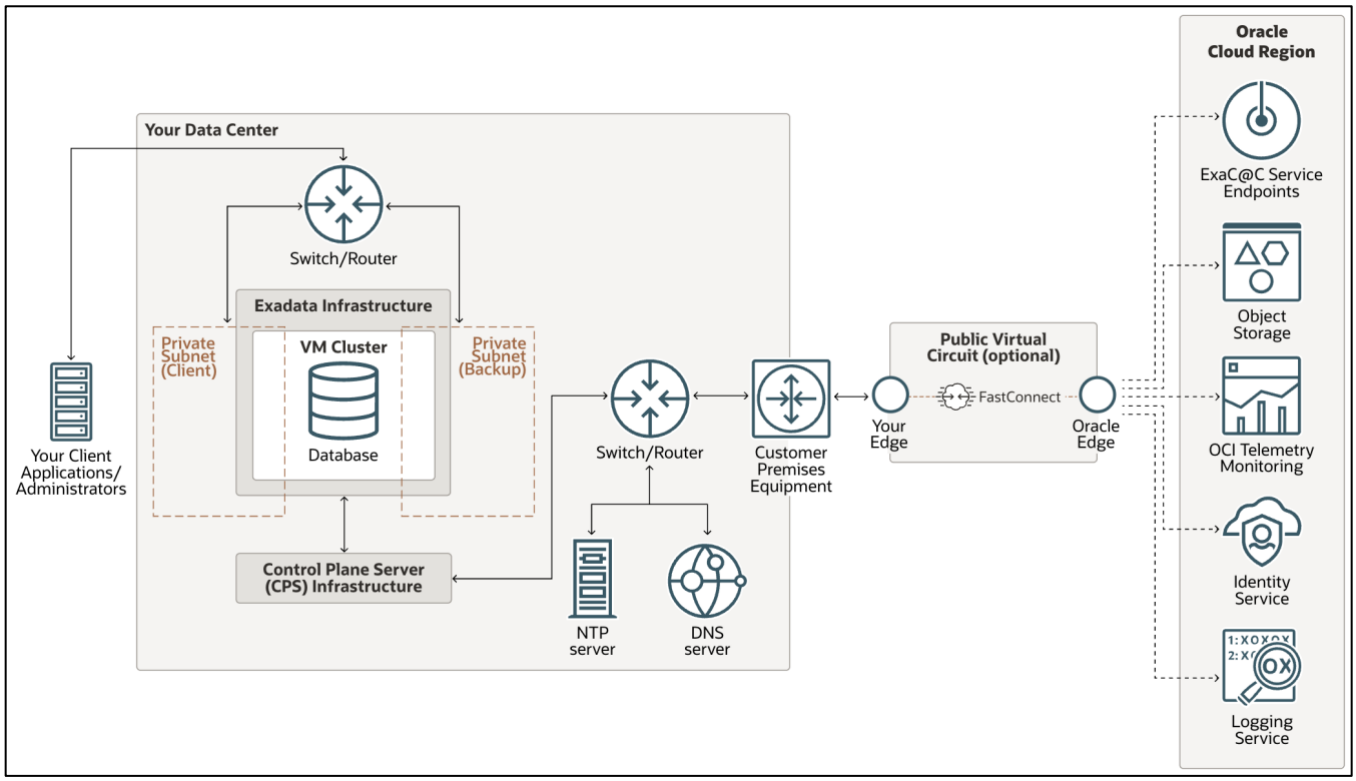

Figure 6: ExaDB-C@C network architecture

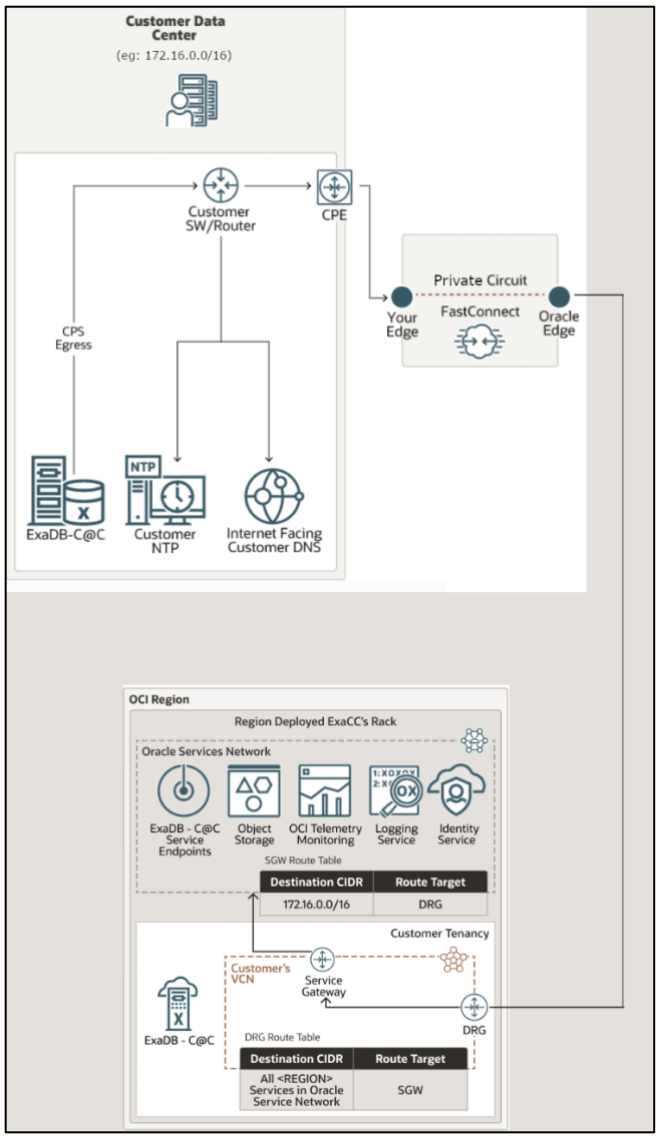

Figure 7: CPS networking with Transit VCN

Table 2: Required URLs for service delivery

DESCRIPTION/PURPOSE	TLS VERSION	CERTIFICATE AUTHORITY	LOCATION (REPLACE *OCI_Region* WITH YOUR REGION)
Persistent Outgoing Tunnel Service for cloud automation Delivery	1.3	DigiCert	https://wss.exacc.*oci_region*.oci.oraclecloud.com
Persistent Outgoing Tunnel Service for ADB-D cloud automation Delivery	1.3	DigiCert	https://wsshe.adbd-exacc.*oci_region*.oci.oraclecloud.com
Temporary Secure Tunnel Service for remote Oracle operator access supporting ExaDB-C@C Infrastructure	1.2	DigiCert	https://mgmthe1.exacc.*oci_region*.oci.oraclecloud.com https://mgmthe2.exacc.*oci_region*.oci.oraclecloud.com

Temporary Secure Tunnel Service for remote Oracle operator access for ADB-D resources	1.3	DigiCert	https://mgmthe.adbd-exacc.*oci_region*.oci.oraclecloud.com
Object Storage Service to retrieve system updates	1.2	DigiCert	https://objectstorage.*oci_region*.oraclecloud.com https://swiftobjectstorage.*oci_region*.oraclecloud.com https://*.objectstorage.oci_region.oci.customer-oci.com
Monitoring Service to record and process Infrastructure Monitoring Metrics	1.2	DigiCert	https://telemetry-ingestion.*oci_region*.oraclecloud.com
Identity Service for name resolution of Oracle operators	1.2	DigiCert	https://identity.*oci_region*.oraclecloud.com https://auth.*oci_region*.oraclecloud.com
Logging Service for application and security logs	1.2	Oracle PKISVC CrossRegion Intermediate r2[1]	https://frontend.logging.ad1.oci_region.oracleiaas.com https://frontend.logging.ad2.oci_region.oracleiaas.com https://frontend.logging.ad3.oci_region.oracleiaas.com https://controlplane.logging.ad1.*oci_region*.oracleiaas.com https://controlplane.logging.ad2.*oci_region*.oracleiaas.com https://controlplane.logging.ad3.*oci_region*.oracleiaas.com
Resource Principal based authentication and ADB-D service delivery	1.2	DigiCert	https://database.*oci_region*.oraclecloud.com
VM serial console	1.2	DigiCert	https://console1.exacc.*oci_region*.oci.oraclecloud.com https://console2.exacc.*oci_region*.oci.oraclecloud.com
Monitoring Service to record and process Infrastructure Monitoring Metrics resources	1.2	DigiCert	https://ingestion.logging.region.oci.oraclecloud.com
Metering and Monitoring	1.2	DigiCert	https://*.functions.oci_region.oci.oraclecloud.com

Network Interface Diagram

Figure 8 shows the network interface diagram. The components you control are shown in blue. The components that Oracle controls are shown in red. An isolated layer 2 management network interconnects the infrastructure components (red). There is no direct network access from the management or storage networks to your client and backup networks. Nominally, the Exadata Database Server does not have an IP address configured (plumbed) on your client or backup networks. The ExaDB-C@C control plane software temporarily configures IP addresses on the Exadata Database Server to perform network validation checks on the Client and Backup networks when you create a VM Cluster Network resource.

You connect the Exadata Database Server client and backup network ports to your Layer 2 switch using 10Gb or 25Gb Ethernet. You control the VLAN tags for these networks. The Exadata Database Server host operating system implements highly available network connections for the VM with an active/standby configuration. You can optionally implement LACP.

Your VMs access Exadata Storage through a private, non-routed interconnect network with SR-IOV mapped interfaces (yellow). Each physical Exadata Database Server and Storage Server has an HA (active/standby) connection to redundant storage networking switches. The default storage network configuration is 100.107.0.0/24. You can override this CIDR block if required.

ADB-D services may be run on the ExaDB-C@C service. When ADB-D services are deployed:

[1] PKISVC CrossRegion Intermediate r2 is an Oracle Cloud Infrastructure Certificate Authority (CA) managed by Oracle for Oracle cloud control plane services, such as internal logging systems used by ExaDB-C@C

- 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
- You may not access the ADB-D VM per the ADB-D service definition
- ADB-D configures a second persistent Secure Outgoing Tunnel Service to ADB-D-specific management endpoints
- ADB-D configures a separate temporary Secure Operator Tunnel Service to ADB-D-specific endpoint for remote SSH access to the ADB-D VM

Oracle enforces separation of duties between ExaDB-C@C infrastructure operations and ADB-D operations.

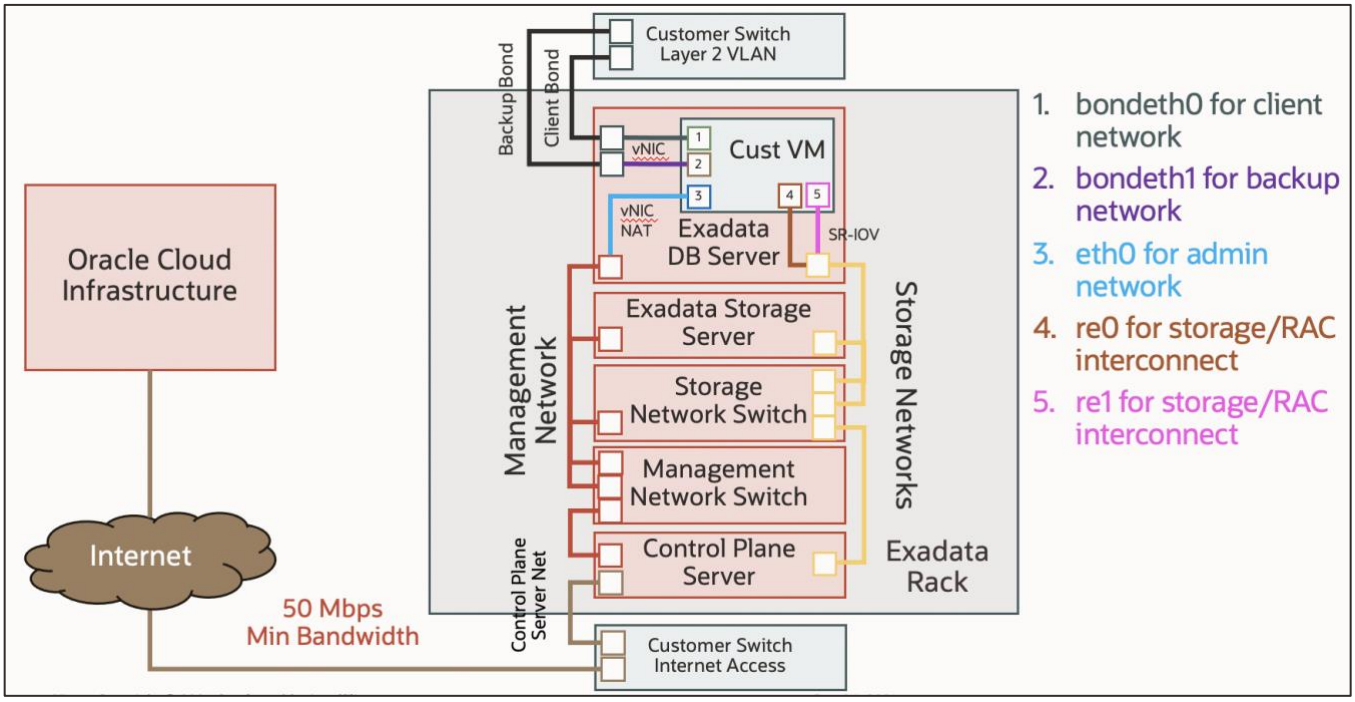

Figure 8: ExaDB-C@C network interfaces

VM Cluster Network Isolation

Figure 9 shows the network isolation between different Virtual Machine Clusters (VM Clusters) deployed on the same Exadata Database Server (DB Server). VMs share physical links for their client (network 1) and backup (network 2) networks. You can specify different VLAN tags for different networks on different VM clusters to isolate network access. Software automatically configures VLANs to isolate the storage networks of each VM Cluster (networks 4 and 5). The /30 vNIC admin network (network 3) isolates admin networks of different VMs on the same Exadata DB Server. The Exadata Database Server does not route between different admin networks. CPU cores are pinned to specific VMs to help prevent in-VM methods from accessing CPU-cached data from other VMs. You can reference Oracle Database Machine and Compliance with PCI DSS V3.2 to see an example of VM cluster network isolation and how it can help you to operate in compliance with PCI DSS.

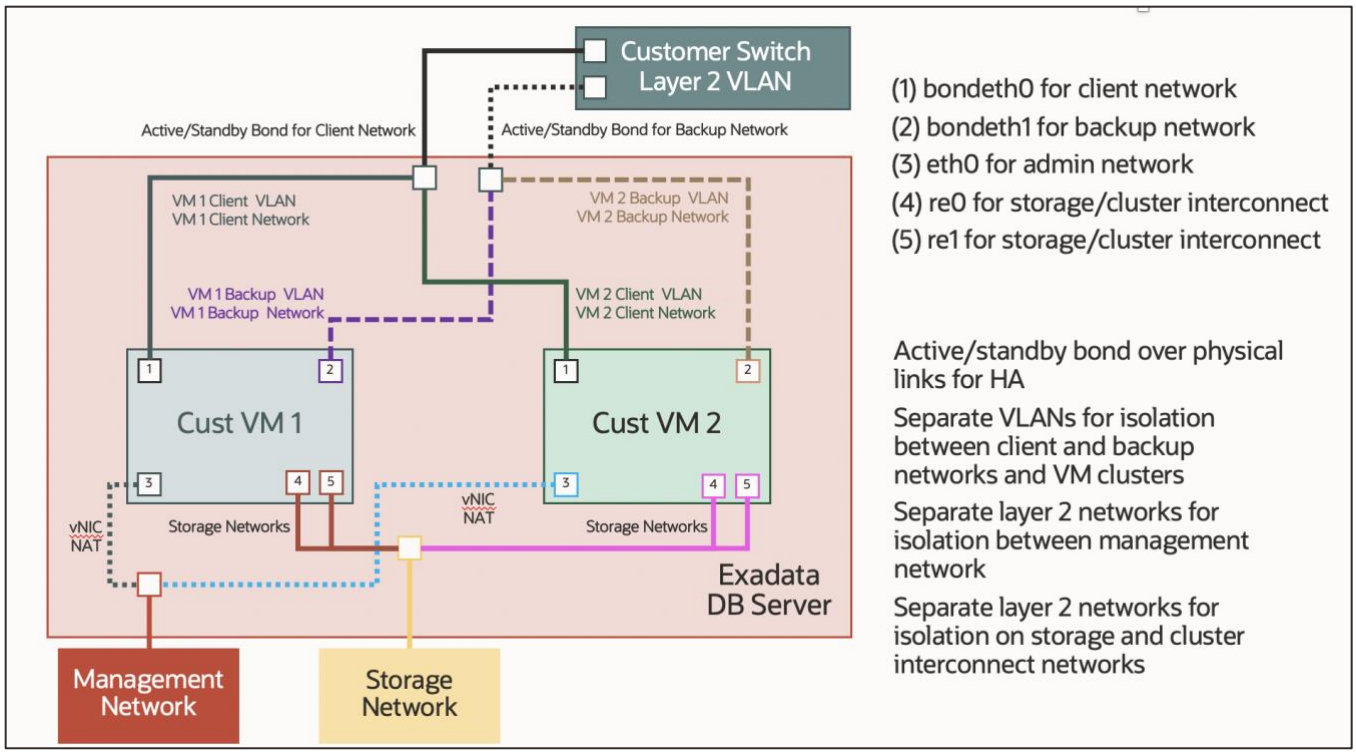

Figure 9: VM Cluster network isolation

Control Plane Software Communication

Figure 10 shows how software processes communicate between the on-premises rack and OCI. The Persistent Secure Tunnel Service for Automation Delivery transmits cloud automation commands (REST API calls) and returns minimal diagnostics to assess service availability. The Secure Tunnel Service for Remote Operator Access provides temporary Oracle operator access (SSH) to Oracle-managed Infrastructure and ADB-D resources when applicable. These services are limited to ExaDB-C@C and not part of OCI's public services. Connections to OCI services are temporary and configured just-in-time when they are required for service functionality, such as downloading software updates from object storage, authenticating resource and service principals, and transmitting monitoring and logging records.

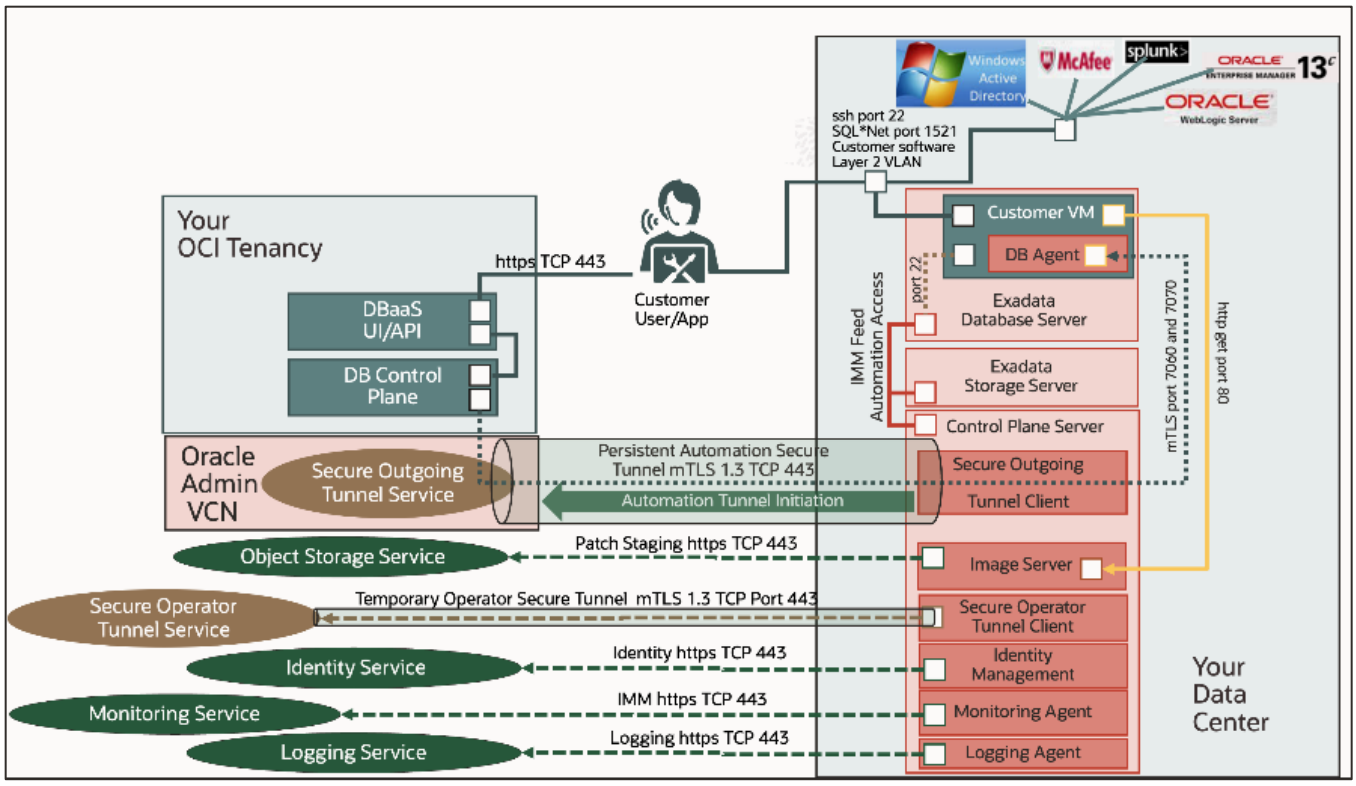

Figure 10:ExaDB-C@C Infrastructure access to OCI services

Oracle manages TLS and mTLS certificates for the connectivity from infrastructure to OCI exclusively. Oracle rotates client certificates for the Persistent Secure Tunnel Service on a 6-month schedule. Oracle rotates client certificates for the Secure Tunnel Service for Remote Operator Access on a 15-day schedule. Client certificates are unique to each ExaDB-C@C infrastructure. The subject alternate name (SAN) of the certificates includes the ExaDB-C@C infrastructure Oracle Cloud Identity (OCID).

VM Default Processes and Certificates

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

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

Table 3 shows the network interface, port number, process description, and certificate authority (CA) for each process. Oracle recommends that you configure security scanners to accept the Oracle CA and Oracle self-signed certificates for Oracle-managed services. These certificates and CAs are built into the service and managed by Oracle to secure the delivery of lifecycle management operations. Accepting them reduces the risk of service issues and minimizes operational burden.

Table 3: Default port matrix for guest VM services

TYPE OF INTERFACE	NAME OF INTERFACE	PORT	PROCESS RUNNING	CERTIFICATE AUTHORITY
Bridge on client VLAN	bondeth0	22	`sshd`	N/A
		1521 Optionally, you can assign a SCAN listener port (TCP/IP) in the range between 1024	Oracle TNS listener Receives incoming client connection requests and manages the traffic	Oracle self-signed; you may add you certificates

		and 8999. Default is 1521. Note: TNS listener opens dynamic ports after initial contact to well-known ports (1521, 1525).	of these requests to the Database Server. Supports Oracle Native Network Encryption (NNE) and TCPS (TLS/SSL) as transport layer security authentication	
		5000	Oracle Trace File Analyzer Collector	Oracle self-signed
		7879	Jetty Management Server. Application server engine that is used internally by Oracle Exadata System Software, in particular Management Server (MS).	Oracle self-signed
	bondeth0:1	1521/2484 Optionally, you can assign a SCAN listener port (TCP/IP) in the range between 1024 and 8999. Default is 1521.	Oracle TNS Listener	Oracle self-signed; you can add your certificates
	bondeth0:2	1521/2484 Optionally, you can assign a SCAN listener port (TCP/IP) in the range between 1024 and 8999. Default is 1521.	Oracle TNS Listener	Oracle self-signed; you can add your certificates
Bridge on backup VLAN	bondeth1	7879	Jetty Management Server	Oracle self-signed
Oracle Clusterware running on each cluster node communicates through these interfaces.	clib0/clre0	1525	Oracle TNS listener Oracle Clusterware running on each cluster node communicates through these interfaces.	N/A
		3260	Synology DSM iSCSI	N/A

		5054	Oracle Grid Interprocess Communication	N/A
		7879	Jetty Management Server	Oracle self-signed
		Dynamic Port: 9000-65500 Ports are controlled by the configured ephemeral range in the operating system and are dynamic.	System Monitor service (`osysmond`) Cluster Logger service (`ologgerd`) Cluster Health Monitor uses system monitor (osysmond) and cluster logger (ologgerd) services to collect diagnostic data.	Oracle self-signed
	clib1/clre1	5054	Oracle Grid Interprocess communication	N/A
		7879	Jetty Management Server	Oracle self-signed
Cluster nodes use these interfaces to access storage cells (ASM disks). However, the IP/ports 7060/7070 attached to the storage interfaces are used to access DBCS agent from the CPS.	stib0/stre0	7060	`dbcs-admin` Cloud agent for handling database lifecycle operations	Oracle self-signed
		7070	`dbcs-agent` Cloud agent for handling database lifecycle operations	Oracle self-signed
	stib1/stre1	7060	`dbcs-admin`	Oracle self-signed
		7070	`dbcs-agent`	Oracle self-signed
CPS to domU	eth0	22	`sshd`	N/A
Loopback	lo	22	`sshd`	N/A
		2016	Oracle Grid Infrastructure	N/A
		6100	Oracle Notification Service (ONS), part of Oracle Grid Infrastructure	N/A

			The Cluster Synchronization Service (CSS), Event Management (EVM), and Oracle Notification Services (ONS) components communicate with other cluster component layers on other nodes in the same cluster database environment.	
		7879	Jetty Management Server	Oracle signed
		Dynamic Port: 9000-65500	Oracle Trace File Analyzer collector	Oracle signed
Bridge on client VLAN	bondeth0	You control	Optional Oracle Data Safe On-Premises Connector	You certificate or Oracle self-signed certificate

VM Serial Console Access

You can access your VM serial console (serial console) through a token-based SSH tunnel. The service provides serial console access in three steps:

1. Create a serial console connection using your OCI IAM credentials (the control plane deploys temporary components to support the SSH proxy tunnel)
2. Connect using SSH over port 443 from your device (or Cloud Shell) to the OCI endpoint for the serial console tunnel
3. Sign in to the serial console with your OS credentials (typically `root`)

Software automatically terminates the Cloud Shell serial console connection after 24 hours. You must reauthenticate to OCI to reestablish the serial console connection. You may terminate the serial console connection at any time using the OCI Console or API interfaces.

Figure 11 shows the steps to create the serial console connection for an SSH connection on port 443 to an OCI endpoint:

1. User requests a serial console connection; payload includes an SSH public key for the serial console endpoint
2. Control plane performs authorization check
3. Control plane sends SSH public key to the serial console endpoint
4. CPS connects outbound to the SSH server endpoint to support inbound SSH to the serial console endpoint

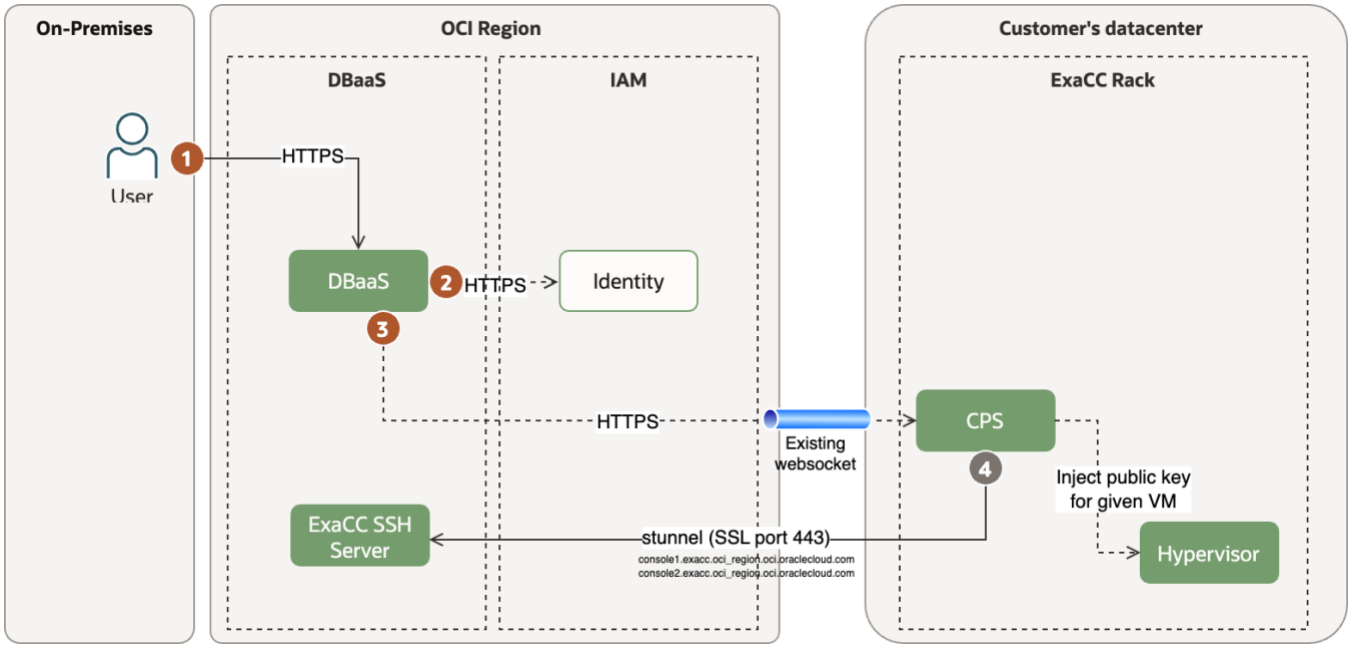

Figure 11: Create SSH tunnel to serial console workflow diagram

Figure 12 shows the steps to establish an SSH connection from your device to the serial console:

1. User connects on port 443 with the SSH connection string provided by control plane
2. Username for the connection is associated with the requesting user's IAM username
3. Control plane associates the SSH target with the ExaDB-C@C virtual machine
4. Control plane performs authorization check for the user to connect to the serial console
5. Control plane forwards the SSH connection through the temporary SSH tunnel to the CPS
6. CPS forwards the SSH connection to the virtual machine serial console running on the hypervisor

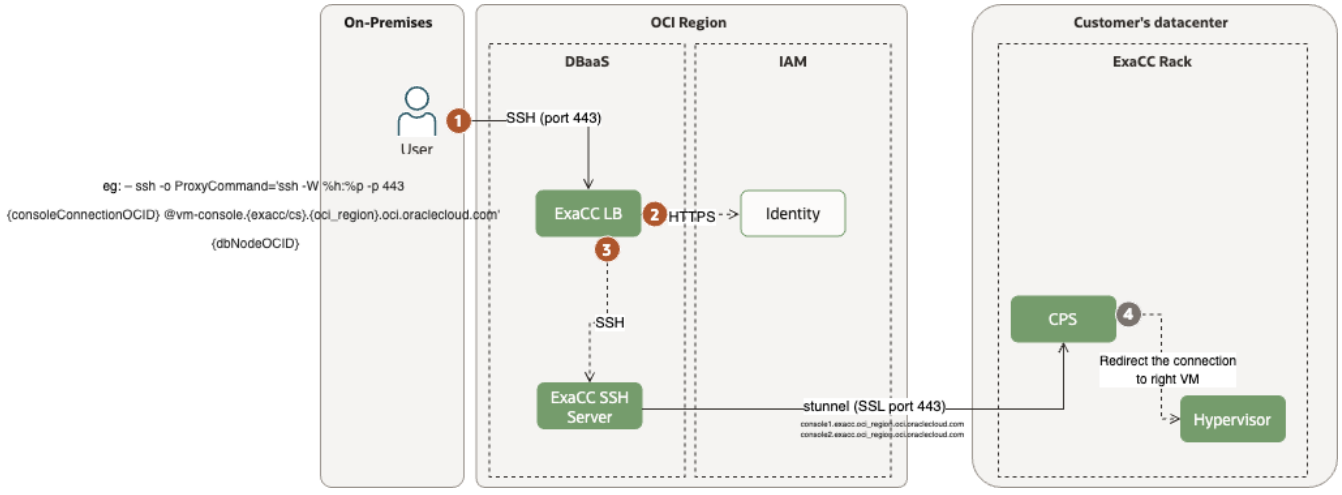

Figure 12: Establish ssh connection via port 443 to an OCI endpoint workflow diagram

Figure 13 shows the steps to create a serial console connection and establish an SSH connection using the Cloud Shell. This process uses system-generated and protected temporary SSH keys rather than user-supplied SSH keys:

1. User requests a serial console connection through Cloud Shell
2. Control plane performs serial console authorization check
3. User invokes Cloud Shell extension
4. Control plane performs Cloud Shell authorization check
5. Control plane generates SSH key pair and the serial console plugin retrieves the keys
6. CPS retrieves the public key and sends it to the hypervisor
7. CPS connects outbound to the SSH server endpoint and Cloud Shell connects inbound to the serial console through the tunnel

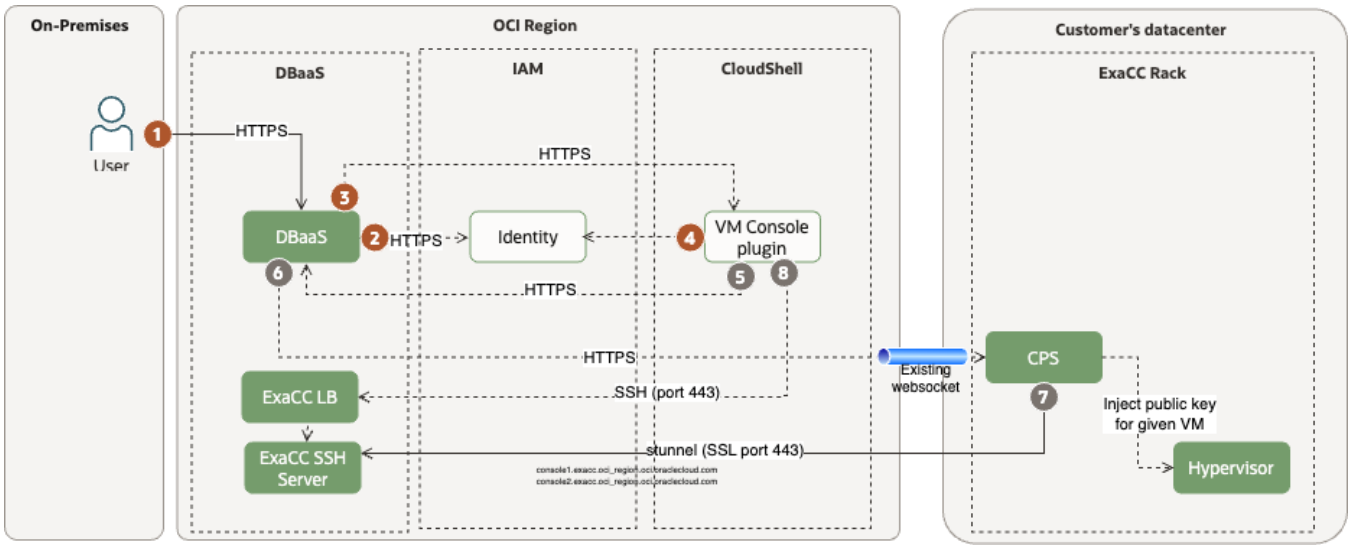

Figure 13: Establish an SSH connection to the serial console using Cloud Shell workflow diagram

Figure 14 shows the workflow to terminate a serial console connection

1. User requests to terminate the serial console connection
2. OCI IAM performs authorization check
3. Control plane sends the termination API through the secure automation tunnel (websocket)
4. CPS terminates the SSH tunnel (stunnel) supporting the serial console connection

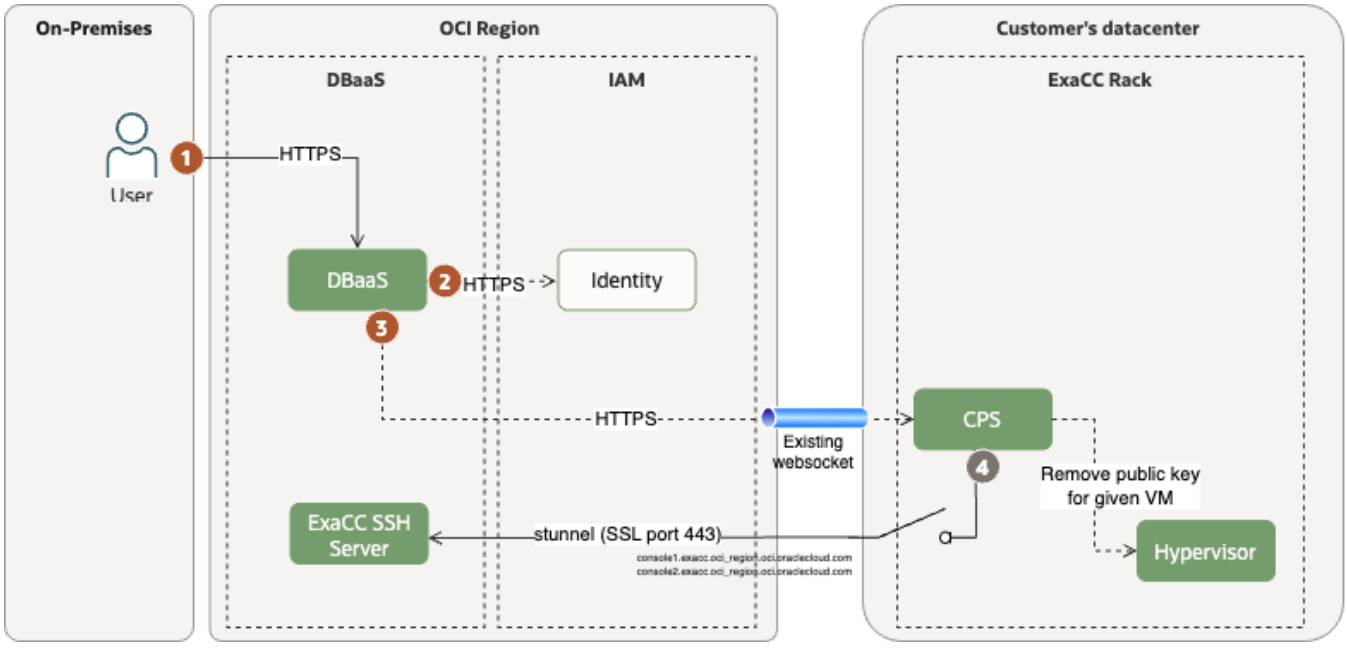

Figure 14: Terminate a serial console SSH connection workflow diagram

You can control the serial console connection with API Access Control so that an OCI identity seeking to enable serial console access must get approval from a different OCI identity.

COMMERCIAL APPENDIX

This section summarizes Oracle public commercial content related to common security questions for ExaDB-C@C. Visit the Oracle Trust Center for an index to Oracle's security, compliance, privacy, and commercial contract documents.

Compliance

Oracle provides information about frameworks for which an Oracle line of business has achieved a third-party attestation or certification for one or more of its services in the form of “attestations.” These attestations can assist in your compliance and reporting, providing independent assessment of the security, privacy and compliance controls of the applicable Oracle cloud services. In reviewing these third-party attestations, it is important that you consider they are generally specific to a certain cloud service and may also be specific to a certain data center or geographic region. You can access Oracle Cloud Compliance 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.

The frameworks and standards ExaDB-C@C is delivered to include:

- 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)
- FedRAMP

You can request compliance documents from an Oracle sales representative and access them directly from your OCI Console. Oracle Cloud Infrastructure and GDPR paper help you meet European Union General Data Protection Regulation (GDPR) requirements with OCI services.

Oracle Corporate Security Policies

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

- Objectives
- Human resources security
- Access control
- Network communications security
- Data security
- Laptop and mobile device security
- Physical and environmental security
- Supply Chain Security and Assurance

Vulnerability Disclosure

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

The Oracle Critical Updates, Security Alerts, and Bulletins page lists announcements of security fixes made in Critical Patch Update Advisories, Security Alerts and Bulletins, and it is updated when new Critical Patch Update Advisories, Security Alerts and Bulletins are released. Oracle will issue Security Alerts for vulnerability fixes deemed too critical to wait for distribution in the next Critical Patch Update, and a history of these alerts is maintained on the Critical Updates, Security Alerts, and Bulletins page.

Oracle Data Processing Agreement

Oracle Data Processing Agreement for Oracle Services describes how Oracle controls, protects, and processes personal information, such as:

- Cross-Border Data Transfers

- Security and Confidentiality
- Audit Rights
- Incident Management and Breach Notification

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

Oracle Cloud Services Agreement

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

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

Important Cloud Services Agreement information is shown below.

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

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

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

Oracle Management of Security Event Logs

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

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

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

Oracle Consensus Assessment Initiative Questionnaire (CAIQ) provides detail about how Oracle manages security logs:

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

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

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

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

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

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

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

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

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

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

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

One-Year Minimum Security Log Retention

Oracle Cloud Hosting and Delivery Policies describes Oracle security log processing and retention, shown below:

"1.14 Security Logs

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

99.95% Monthly Uptime Service Level Objective (SLO)

Service level objectives are engineering objectives for the expected monthly service level of the applicable Oracle PaaS or IaaS public cloud service. Unlike for SLAs, Oracle offers no financial compensation in the event an SLO is missed. Oracle works to meet a Service Level Objective of 99.95% for ExaDB-C@C.

60-Day Access Period After Service Termination

Oracle Cloud Hosting and Delivery Policies describes the 60-day access period after service termination to retrieve your data from the service, shown below:

"6.1 Termination of Oracle Cloud Services

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

CONNECT WITH US

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

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

Exadata Database Service on Cloud@Customer Security Controls
April 2626