ORACLE

Operator Access Control

How you control Oracle staff access to your service infrastructure

June 16, 2026, Version 3.15
Copyright © 2026, Oracle and/or its affiliates
Public

Purpose statement

This document provides an overview of features and enhancements included in Oracle Operator Access Control. It is intended solely to help you assess the business benefits of using Operator Access Control and to plan your I.T. projects.

Disclaimer

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

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, timing, and pricing 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.

Copyright © 2026, Oracle and/or its affiliates / Public

ORACLE

Table of contents

Introduction **4**

Roles and Responsibilities **5**

Architecture **5**

Security Controls **8**

SSH Authentication 8

Network Isolation 8

Enforcement of Privilege Limits 8

Control Plane Server Only 9

System Diagnostics 10

System Maintenance with Restart 13

System Maintenance with Data Access / VM Control 16

Full System Access 19

Audit **20**

Revoking Access **20**

Cloud Interfaces and Notification **21**

Concept of Operations **21**

Access Request Process Flow 22

Oracle Staffing Updates 22

Your Approval Policies 23

Implications for Service Quality and Availability 23

Failure Recovery 23

Security Incident Reporting and Communication 23

Summary **24**

Copyright © 2026, Oracle and/or its affiliates / Public

List of figures

Figure 1: Gen 2 ExaDB-C@C network architecture 5
Figure 2: ExaDB-D in OCI network architecture diagram 6
Figure 3: ExaDB-D in Azure, AWS, and Google Cloud network architecture 6
Figure 4: Operator Access Control SSH access for ExaDB-C@C 7
Figure 5: Operator Access Control SSH access for ExaDB-D 8
Figure 6: Operator Access Control Operational Flow 22

List of tables

Table 1: Control Plane Server Only Privileges 9
Table 2: System Diagnostics Privileges 11
Table 3: System Maintenance with Restart Privileges 14
Table 4: System Maintenance with Data Access / VM Control Privileges 17
Table 5: Full System Access Privileges 20

Introduction

Cloud computing shifts some control from your in-house systems to your cloud provider. Now, you share responsibility for security, privacy, and operations. Regulations may require you to manage and monitor cloud provider staff access. Oracle Operator Access Control provides this oversight. It allows you to:

- Decide when Oracle staff connect
- Approve privileges
- Monitor and record activity
- Revoke access at any time

The service is included at no extra cost and applies to shell access by Oracle staff, not automated tools. Operator Access Control supports the following services:

- Exadata Database Service Dedicated in OCI, AWS, Azure, and Google Cloud
- Exadata Cloud@Customer
- Compute Cloud@Customer
- Autonomous Database Dedicated on Exadata Cloud@Customer and Exadata Database Service Dedicated

Operator Access Control is a FedRAMP authorized service, and it is included in Oracle's PCI-DSS and SOC-2 compliance programs. You can access Oracle compliance documents from your OCI Console and your Oracle sales representative.

For more on security, refer to the following:

- Exadata Cloud@Customer Security Controls
- Exadata Cloud@Customer Security Guide
- Exadata Database Service Dedicated Security Controls
- Exadata Database Service Dedicated Security Guide
- Security Features in Autonomous Database
- Securing Compute Cloud@Customer

Copyright © 2026, Oracle and/or its affiliates / Public

Roles and Responsibilities

When you control Oracle staff access with Operator Access Control, Oracle has the responsibility to:

- Issue an Operator Access Control access requests to you when they need to access infrastructure
- Perform work after you approve their access request
- Provide Oracle employee personal information when required

You have the responsibility to:

- Create and assign operator controls that govern the rules by which a system can be accessed
- Configure notifications and logging services per your standards
- Respond to access requests in a timely manner
- Monitor Oracle staff commands and keystrokes for security and audit purposes
- Approve, reject, or revoke access to infrastructure as your business and security needs dictate

In the event of a security incident, you and Oracle have the responsibility to work together per Oracle Information Security Incident Response.

Architecture

Exadata Database Cloud Services are based on the Exadata Database Machine. You control access to your databases and virtual machines through your own networks, credentials, and policies. You have full administrative access to your virtual machines and databases. You can set security policies, install agents, forward logs, and manage identities to meet regulatory needs. Cloud automation and lifecycle management come from your selected OCI region, with all actions logged by OCI Audit. You control when and how cloud automation operates through OCI IAM Policy and API Access Control.

The Exadata Cloud@Customer (ExaDB-C@C) architecture uses two Control Plane Servers (CPS) to connect an Exadata rack in your data center to the OCI control plane. You can control Oracle's access to the entire rack with Operator Access Control, including database servers, storage servers, CPS, power distribution units, and network switches. Figure 1 shows the architecture diagram for ExaDB-C@C.

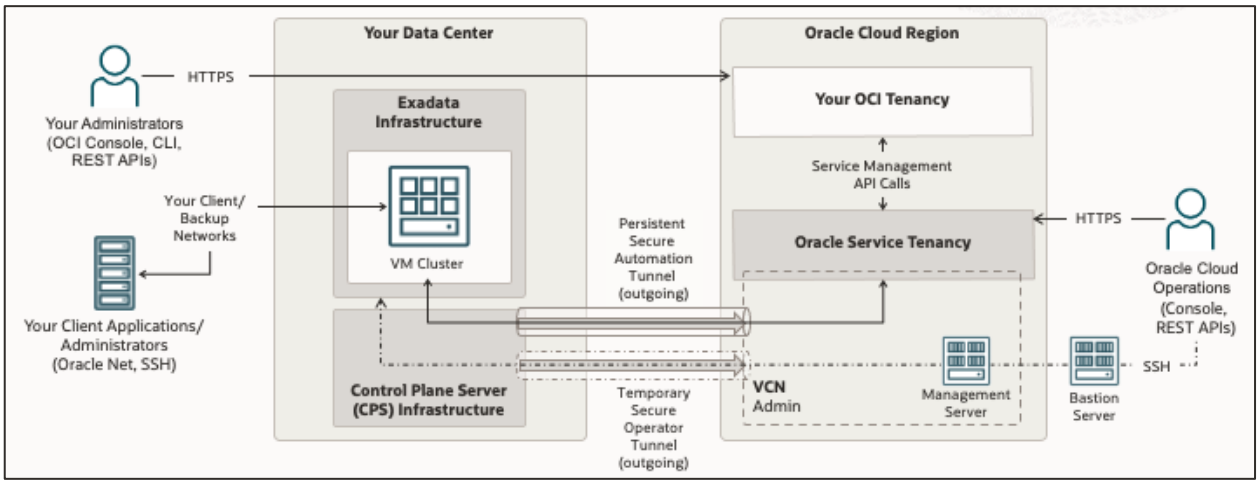

Figure 1: Gen 2 ExaDB-C@C network architecture

Exadata Database Service Dedicated (ExaDB-D) in OCI, AWS, Azure, and Google Cloud dedicates Exadata Database and Storage servers to your service. You share physical racks, power distribution units, and specialized networking hardware with other tenants. You can control Oracle's access to the database servers and storage servers dedicated to your service with Operator Access Control. Oracle controls access to the shared components, such as racks, power distribution units, and networking hardware. Figure 2 shows the architecture diagram for ExaDB-D in OCI. Figure 3 shows the architecture diagram for ExaDB-D in Azure, AWS, and Google Cloud.

Copyright © 2026, Oracle and/or its affiliates / Public

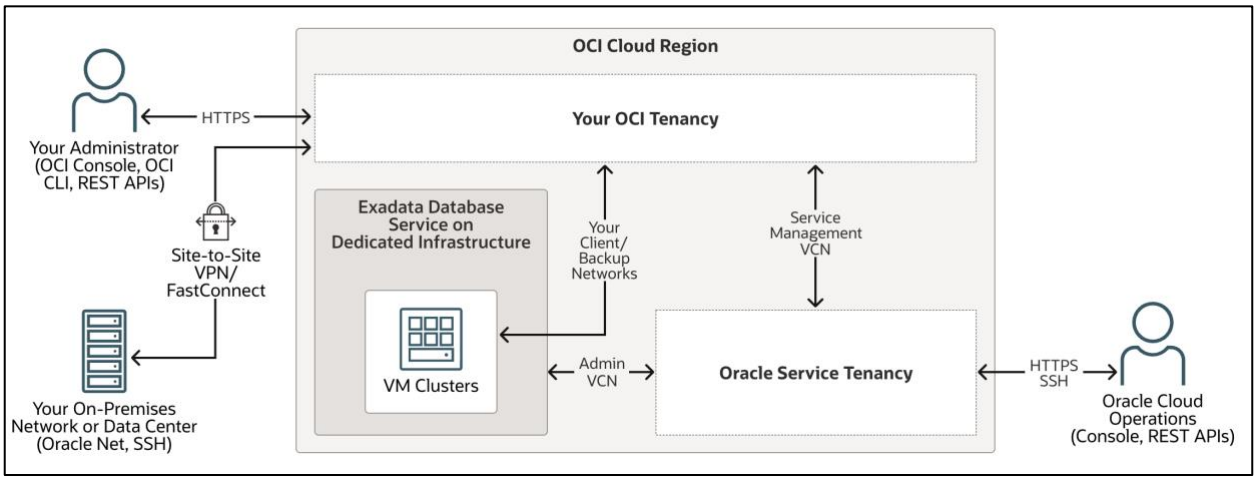

Figure 2: ExaDB-D in OCI network architecture diagram

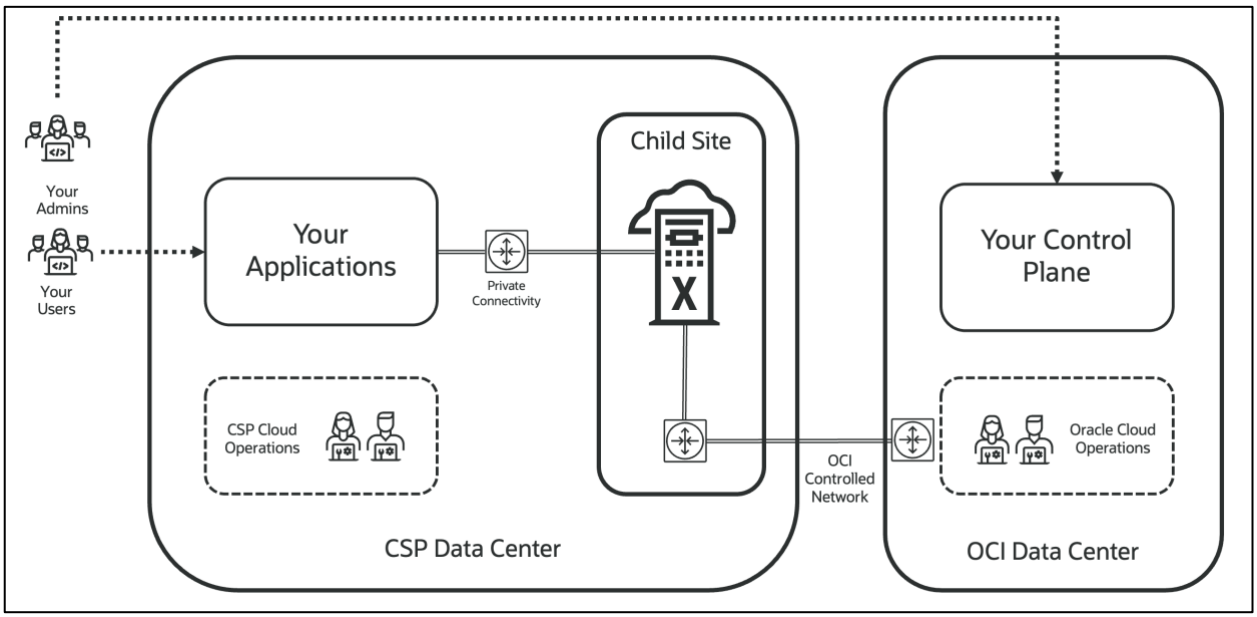

Figure 3: ExaDB-D in Azure, AWS, and Google Cloud network architecture

Independent of Operator Access Control, Oracle controls for Oracle staff access to Oracle-managed infrastructure. Oracle corporate identity management and permissions services control authorization. Authorization checks include job code and training records. Oracle least-privileged access model follows Oracle Access Control, Human Resources Security, and Information Asset Classification practices. General security controls for infrastructure access include the following:

Oracle Cloud Network Attach (OCNA) VPN 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:

- Requires OCNA access
- Entitlement granted based on job-code and training records
- 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

Copyright © 2026, Oracle and/or its affiliates / Public

Service infrastructure access:

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

Oracle uses globally deployed staff in a follow-the-sun model to support commercial cloud services. These staff can work from non-Oracle locations. Oracle controls staff supporting government services based on applicable frameworks.

When you apply Operator Access Control to your infrastructure, it establishes baseline authentication and isolation control by removing accounts accessible to Oracle staff through SSH and SSH network access. Following:

- Oracle requests access over HTTPS with Oracle credentials.
- Your approve access over HTTPS with your credentials.
- Requesting staff get a unique, just in time, temporary, and least-privileged account.
- Requesting staff get temporary, just in time SSH network access to approved components
- Action Enforcement controls privilege limits.
- Commands and keystrokes are reported to your OCI Logging service and syslog server.

Figure 4 shows the SSH access flow for ExaDB-C@C:

- Oracle staff authenticate to OCNA VPN with FIPS 140-2 level 3 hardware MFA.
- Oracle scans their end-user device and allows access if device meets Oracle endpoint requirements, including virus scanning and device configuration.
- Staff authenticate to the Bastion and Management server with FIPS 140-2 level 3 hardware MFA.
- Software automation establishes the temporary security operator tunnel.
- Their SSH session is forwarded through the temporary secure operator tunnel.
- They authenticate to their temporary accounts with FIPS 140-2 level 3 hardware MFA.
- Operator Access Control removes temporary accounts and network access when the request expires, the operator closes it, or you terminate it.

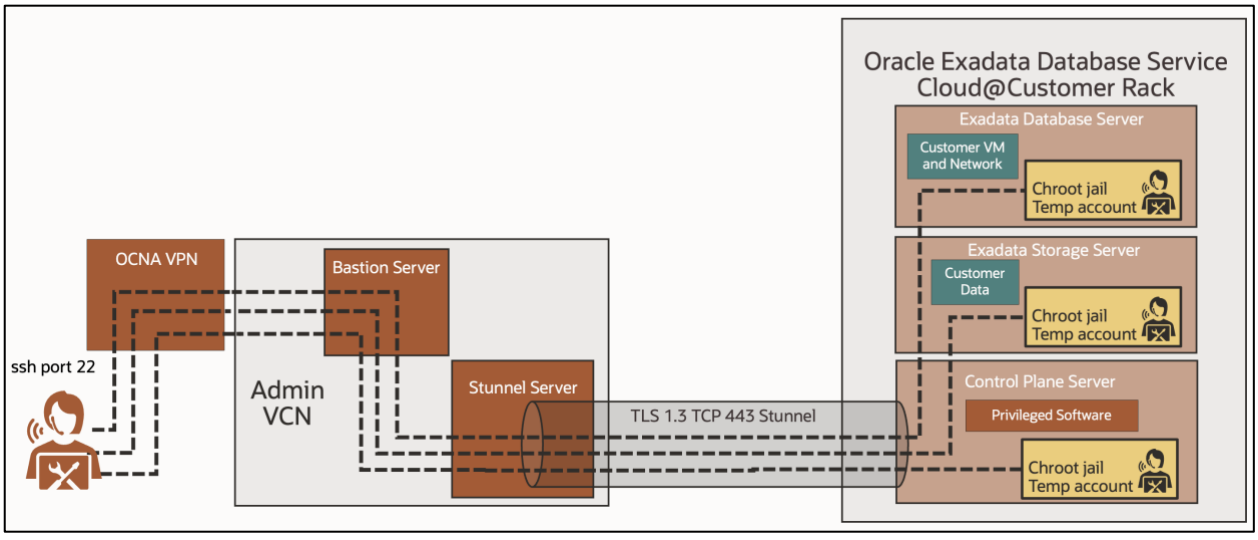

Figure 4: Operator Access Control SSH access for ExaDB-C@C

Figure 5 shows the SSH access flow for ExaDB-D in OCI, Azure, AWS, and Google Cloud:

- Oracle staff authenticate to OCNA VPN with FIPS 140-2 level 3 hardware MFA.
- Oracle scans their end-user device and allows access if device meets Oracle endpoint requirements, including virus scanning and device configuration.
- Staff authenticate to Bastion and Management server with FIPS 140-2 level 3 hardware MFA.
- They SSH from the Management Server to the target infrastructure.
- They authenticate to their temporary accounts with FIPS 140-2 level 3 hardware MFA.
- Operator Access Control removes temporary accounts and network access when the access request expires, the operator closes it, or you terminate it.

Copyright © 2026, Oracle and/or its affiliates / Public

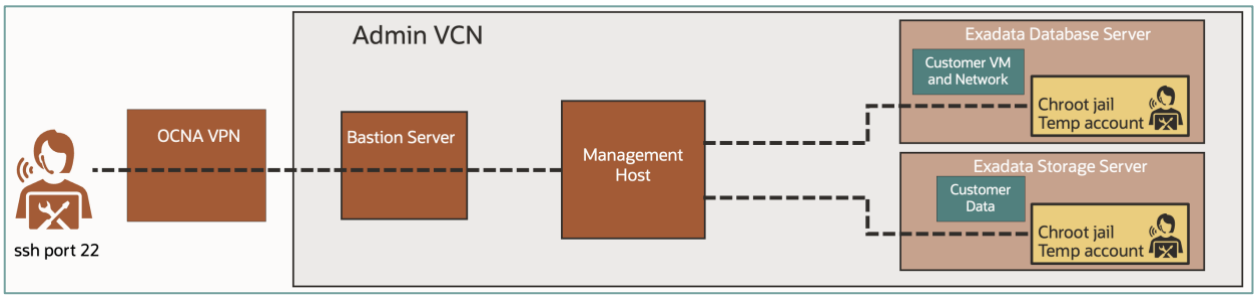

Figure 5: Operator Access Control SSH access for ExaDB-D

Security Controls

Security controls limit what Oracle staff can do, such as when they can log into the infrastructure, how long they can access the infrastructure, the commands they can run, and the files and devices they can access. Operator Access Control does this with authentication controls, network isolation controls, and controls to enforce privilege limits.

SSH Authentication

By default, the service infrastructure you control does not have interactive shell accounts. When you approve an access request, Operator Access Control creates a temporary account for the Oracle staff member and adds their SSH public key, secured with their hardware MFA device. Each staff member receives their own temporary account if more people need access. Action Enforcement prevents these accounts from viewing or changing their ~/.ssh/authorized_keys file. All commands and keystrokes are logged per user. When the access request ends, Operator Access Control deletes all related accounts and their files, and all processes started by those accounts.

Network Isolation

By default, the service infrastructure you control does not permit SSH network access for Oracle operators. When you approve an access request, Operator Access Control allows temporary SSH network access for the Oracle staff. For ExaDB-C@C, Operator Access Control creates temporary Bastion hosts for each operator and establishes the temporary security operator tunnel shared among the operators. For ExaDB-D, the Management server temporarily allows the approved named users SSH access to the IP addresses on the approved components with mandatory security controls enforced by the operating system kernel. Operator Access Control removes network access when the access request expires, the operator closes it, or you terminate it.

Enforcement of Privilege Limits

Operator Access Control Actions enforce privilege limits. An Action places constraints on what an Oracle operator is permitted to do on infrastructure managed by Oracle. These constraints include control over running operating system shell commands, running and Oracle scripts. Actions also place constraints on the ability of Oracle operators to run binaries, shell scripts, and Perl or Python scripts that are beyond the scope of the function defined by the Action. Operator Access Control Actions translate Oracle Linux permissions on the target system. Oracle Linux chroot jail and other security software work together to:

- Restrict accessible file systems and files
- Prevent direct access to system commands and utilities
- Limit the arguments the operator can send to those system commands and utilities

Permissions are categorized into file system privileges, command execution privileges, and su or sudo privileges. Actions are grouped by the nature of the change they can affect. Operator Access Control provides the following Actions for Exadata Database Cloud Services:

- Control Plane Server Only (ExaDB-C@C only)
- System Diagnostics

Copyright © 2026, Oracle and/or its affiliates / Public

- System Maintenance with Restart
- System Maintenance with Hypervisor access / VM Control
- Full System Access

The following sections summarize these privileges.

Control Plane Server Only

Control Plane Server Only, identified as `INFRA_CPS_ONLY`, applies to ExaDB-C@C only. It is designed for routine diagnosis and maintenance of the ExaDB-C@C control plane functionality while preventing access to the data plane components of the ExaDB-C@C service. `INFRA_CPS_ONLY` access prevents access to the `root` account and other privileged software accounts on the Control Plane Server to prevent access to or disruption of customer services, including customer VMs, customer databases, and customer network resources. `INFRA_CPS_ONLY` permits limited diagnostics, software updates, and restarts of the Control Plane Servers.

Table 1 details the privileges for Control Plane Server Only.

Table 1: Control Plane Server Only Privileges

OPERATOR PRIVILEGES

Linux User Privilege: Non-root
Can su to root: No
chroot jail: Yes
Can su into: None
sudo user + command list: Limited to the list provided above
Cell server privileges: No
Host operating system (dom0): No
Network Privileges: No
List of executable commands:
These commands can be run directly from the Bash prompt.
• Alias:
  • sudols
  • sudocp
  • sudocat
  • sudotail
  • sudohead
  • sudovi
  • sudorm
  • systemctl
  • reboot
  • ifconfig
  • lsof
  • docker
  • ipmitool
  • dbmcli
  • traceroute
  • tcptraceroute
  • journalctl
  • exacloud

Copyright © 2026, Oracle and/or its affiliates / Public

    - du
    - imageinfo
    - imagehistory
    - arping
    - curl
    - tcpdump
    - crontab
    - sundiag.sh
    - sosreport
    - ethtool
- Special commands supported:
    - rootexec /root/alarm_detail.sh
    - rootexec /root/alerthistory.sh
    - rootexec /root/blackout.sh
    - rootexec /root/quarantine_ack.sh
    - rootexec /root/stateless_ack.sh
    - rootexec /root/stateless_alert.sh
    - rootexec /etc/keepalived/manual-switchover.sh

Directories and files with explicit Read and Write access:

- Read and Write:
    - /u01/
    - /opt/oci/exacc/
- Read-Only:
    - /var/log/
    - /opt/oracle.cellos/
    - /usr/local/nessus/results/
    - /opt/nessus/var/nessus/logs/

Special Operator Access Control commands:

Cage commands to view or modify (read, read/write) files or directories mentioned above:

- sudols
- sudocp
- sudocat
- sudotail
- sudohead
- sudovi
- sudorm

Can su into: None

sudo user + command list: Limited to the list provided above

Cell server privileges: No

Host operating system (dom0): No

Network Privileges: No

System Diagnostics

System Diagnostics, identified as `INFRA_DIAG`, is designed for diagnosing any issue in the infrastructure layer. In cases where Oracle Cloud Ops only has a need to perform diagnostics access, Oracle Cloud Ops will ask for

Copyright © 2026, Oracle and/or its affiliates / Public

INFRA_DIAG privileges. In cases where Oracle Cloud Ops knows there is a need for an action that cannot be performed with INFRA_DIAG, then Oracle Cloud Ops will ask for the necessary privileges, including INFRA_FULL. Cases that need INFRA_FULL for the purposes of diagnostics include diagnostics of Oracle Linux kernel functionality, such as device drivers, and hardware/firmware fault diagnosis.

–

Table 2 details the privileges of System Diagnostics. Note:

- System Diagnostics Action poses no customer data exposure risks and low availability risks.
- System Diagnostics Action allows:
  - The operator to use `cat, grep,` and so on to read log files of the operating system, infrastructure software, and cloud orchestration software.
  - The operator to run Oracle Linux diagnostics commands such as `top` and `netstat`.
  - The operator to run `cellcli` commands on Exadata Storage Servers to obtain diagnostic information.
  - The operator to access and manage the cloud orchestration infrastructure on the Control Plane Server with capability to restart all daemons on the Control Plane Server.

Table 2: System Diagnostics Privileges

OPERATOR PRIVILEGES

Oracle Linux user privilege: Non-root.
 	
Can su to root: No
 	
chroot jail: Yes
 	
Can su into:
 	
• Cell: cellmonitor
• Host: dbmmonitor
• Control Plane Server:
  • ecra
  • exawatcher
  • dbmsvc
Execute as root:
 	
• cat
• head
• tail
• cp for files inside /var/log/*
• [CPS]: systemctl
 	
Cell Server Privileges: Act as cell monitor.
 	
Network Privileges: Can SSH into all hosts, cell servers, and Control Plane Servers. The user name is the same across all of these.
 	
List of executable commands:
 	
• Control Plane Server (Alias): These commands can be run directly from the Bash prompt.
  • systemctl
  • reboot
  • ifconfig
  • lsof
  • docker
  • ipmitool
  • dbmcli
  • traceroute
  • tcptraceroute

Copyright © 2026, Oracle and/or its affiliates / Public

        - journalctl
        - exacloud
        - du
        - imageinfo
        - imagehistory
        - arping
        - curl
        - tcpdump
        - crontab
        - sundiag.sh
        - sosreport
        - ethtool
    - Cell server (Alias): These commands can be run directly from the Bash prompt.
        - cellcli - read-only commands
        - sundiag.sh
        - sosreport
        - lspci
        - imageinfo
        - imagehistory
    - Host (Alias): These commands can be run directly from the Bash prompt.
        - dbmcli - read-only commands
        - sundiag.sh
        - sosreport
        - virsh - only list options
        - xm - only list options
        - docker
        - podman
        - imageinfo
        - imagehistory

Directories and files with explicit Read and Write access:

- Control Plane Server:
    - Read and Write: /u01/
    - Read-Only:
        - /var/log/
        - /opt/oci/exacc/exacloud/log/
        - /opt/oracle.cellos/
        - /usr/local/nessus/results/
        - /opt/nessus/var/nessus/logs/
    - Special Operator Access Control commands: Cage commands to view or modify (read, read/write) files or directories mentioned above.
        - sudols
        - sudocp
        - sudocat
        - sudotail
        - sudohead
        - sudovi
        - sudorm

Copyright © 2026, Oracle and/or its affiliates / Public

- Host:
    - Read and Write: None
    - Read-Only: /var/log/
    - Special Operator Access Control commands: Cage commands to view or modify (read, read/write) files or directories mentioned above.
        - sudols
        - sudocp
        - sudocat
        - sudotail
        - sudohead

The following directories are mapped in a read-write mode for the tools to run; however, Oracle operators are not granted direct access to them.

- /var
- /opt/oracle

- Cell server:
    - Read and Write: None
    - Read Only: /var/log/
    - Special Operator Access Control commands: Cage commands to view or modify (read, read/write) files or directories mentioned above.
        - sudols
        - sudocp
        - sudocat
        - sudotail
        - sudohead

The following directories are mapped in a read-write mode for the tools to run; however, Oracle operators are not granted direct access to them.

- /var
- /opt/oracle

System Maintenance with Restart

System Maintenance with Restart, identified as `INFRA_UPDATE_RESTART`, is designed for operator access scenarios that require a system configuration change, or a restart of the system. `INFRA_UPDATE_RESTART` scenarios are typically for maintenance. However, there can be diagnostics scenarios where this action is required. System configuration changes involve network configuration changes, hardware configuration changes, operating system configuration changes such as mounts, inodes, ulimits, or cloud orchestration software configuration changes. System restart entitles the Oracle operator to restart the operating system (Exadata Database Server, Exadata Storage Server), to restart specific sub-systems, such as the network, and to restart cell disks.

Table 3 details System Maintenance with Restart privileges. Note:

- Be aware that System Maintenance with Restart Privileges Action can create significant service availability risk to the system. However, it does not expose any data to risk.
- System Maintenance with Restart Privileges action:
    - Permits the Oracle operator to perform system maintenance activities with `root` privileges. The operator cannot become `root` but can run maintenance commands as `root`.
    - Does not allow the operator to change the audit parameters or access the audit logs; however, the action allows the operator to take the whole system offline.

Copyright © 2026, Oracle and/or its affiliates / Public

- Allows the operators to change configuration of the operating system through permanent changes. For example, the Oracle operator is permitted to change `/etc/` parameters.
- Permits the Oracle operator to start daemon processes, and to manage the cell disks using the `cell admin` privilege of `cellcli` on Exadata Storage Servers.
- For ExaDB-C@C only, permits the Oracle operator to access the manage the cloud orchestration infrastructure on the Control Plane Server, with capability to restart all daemons on the Control Plane Server.

Inheritance: All privileges of System Diagnostics

Table 3: System Maintenance with Restart Privileges

OPERATOR PRIVILEGES

Same as System Diagnostics privilege + the following:
 	
Can su to root: No
 	
chroot jail: Yes
 	
Can su into:
 	
• exawatcher
• dbmsvc
• dbmadmin
• dbmmonitor on the host
 	
Execute as root:
 	
• restart
• ip
• ifconfig
• lspci
 	
Cell server privileges: celladmin in cell server
 	
Network Privileges: Can SSH into all hosts, cell servers, and Control Plane Servers. The user name is the same across all these layers
 	
List of executable commands:
 	
• Control Plane Server (Alias): These commands can be run directly from the Bash prompt.
  • systemctl
  • reboot
  • ifconfig
  • lsof
  • docker
  • ipmitool
  • dbmcli
  • traceroute
  • tcptraceroute
  • journalctl
  • exacloud
  • du
  • imageinfo
  • imagehistory
  • arping
  • curl
  • tcpdump
  • crontab

Copyright © 2026, Oracle and/or its affiliates / Public

        - sundiag.sh
        - sosreport
        - ethtool
    - Cell server (Alias): These commands can be run directly from the Bash prompt.
        - reboot
        - sundiag.sh
        - cellcli - all commands
        - lspci
        - imageinfo
        - imagehistory
        - ethtool
        - ipmitool
        - ipmitool_interactive (same as ipmitool, can be used when tty is required)
    - Host (Alias): These commands can be run directly from the Bash prompt.
        - reboot
        - dbmcli - all commands
        - sundiag.sh
        - virsh - only list options
        - xm - only list options
        - docker
        - podman
        - imageinfo
        - imagehistory
        - ethtool
        - sosreport

Directories and files with explicit Read and Write access:

- Control Plane Server:
    - Read and Write: /u01/
    - Read-Only:
        - /var/log/
        - /opt/oci/exacc/exacloud/log/
        - /opt/oracle.cellos/
        - /usr/local/nessus/results/
        - /opt/nessus/var/nessus/logs/
    - Special Operator Access Control commands: Cage commands to view or modify (read, read/write) files or directories mentioned above.
        - sudols
        - sudocp
        - sudocat
        - sudotail
        - sudohead
        - sudovi
        - sudorm
- Host:
    - Read and Write: None

Copyright © 2026, Oracle and/or its affiliates / Public

- Read-Only: /var/log/
- Special Operator Access Control commands: Cage commands to view or modify (read, read/write) files or directories mentioned above.
    - sudols
    - sudocp
    - sudocat
    - sudotail
    - sudohead

The following directories are mapped in a read-write mode for the tools to run; however, Oracle operators are not granted direct access to them.

- /var
- /opt/oracle
- /home/dbmadmin

- Cell Server:
    - Read and Write: None
    - Read Only: /var/log/
    - Special Operator Access Control commands: Cage commands to view or modify (read, read/write) files or directories mentioned above.
        - sudols
        - sudocp
        - sudocat
        - sudotail
        - sudohead

The following directories are mapped in a read-write mode for the tools to run; however, Oracle operators are not granted direct access to them.

- /var
- /opt/oracle
- /home/celladmin/

System Maintenance with Data Access / VM Control

System Maintenance with Data Access / VM Control, identified as `INFRA_HYPERVISOR`, is designed for diagnostics and maintenance scenarios where VM management on the Exadata Database Server is required. Any data on the customer VM is treated as customer data. As VM management involves the ability to access the VM data, this action potentially exposes data risk. However, all customer data created by service automation is encrypted with TDE and this action does not give any access to the TDE keys of the data stored in Exadata Storage Servers. VM management is required in cases where there are problems with the VM software infrastructure or where a VM configuration needs to be modified. Configuration involves the external aspect of the VMs such as the networks attached, disks attached, or resources (CPU, Memory) allocated.

Table 4 details System Maintenance with Data Access / VM Control privileges. Note:

- System Maintenance with VM Control Privileges action poses significant data risks and availability risks to the customer. The data risks are exposed because the customer VM file systems are accessible through access of VM disks. The availability risks are exposed because the VMs can be controlled by the operator.
- System Maintenance with VM Control Privileges Action:
    - Allows the operator to perform Xen/KVM management commands with `root` privileges. The operator cannot become `root`. This action is applicable only to the Exadata Database Server.
    - Inherits the privileges from the "System Maintenance with Restart Privileges" action.

Copyright © 2026, Oracle and/or its affiliates / Public

- Does not allow the operator to change operating system parameters of Exadata Database Servers or Exadata Storage Servers. However, this allows the operator to shut down the customer VM and significantly change the configuration of the customer VM.
- Does not allow the operator to change the configuration of the Oracle Linux Audit service

Inheritance: All privileges of System Maintenance with Restart.

Table 4: System Maintenance with Data Access / VM Control Privileges

OPERATOR PRIVILEGES

Same as "System Maintenance with Restart" privileges + the following:
 	
Oracle Linux user privilege: Non-root.
 	
Can su to root: No
 	
chroot jail: Yes
 	
Can su into: celladmin in cell server
 	
Execute as root:
 	
• /usr/sbin/xm
• /usr/sbin/xentop
• /usr/sbin/virsh
 	
Cell Server Privileges: celladmin
 	
Network Privileges: Can SSH into all hosts, cell servers, and Control Plane Servers. The user name is the same across all of these.
 	
List of executable commands:
 	
• Control Plane Server (Alias): These commands can be run directly from the Bash prompt.
  • systemctl
  • reboot
  • ifconfig
  • lsof
  • docker
  • ipmitool
  • dbmcli
  • traceroute
  • tcptraceroute
  • journalctl
  • exacloud
  • du
  • imageinfo
  • imagehistory
  • arping
  • curl
  • tcpdump
  • crontab
  • sundiag.sh
  • sosreport
  • ethtool
• Cell server (Alias): These commands can be run directly from the Bash prompt.
  • cellcli - all commands

Copyright © 2026, Oracle and/or its affiliates / Public

        - lspci
        - imageinfo
        - imagehistory
        - ethtool
        - sosreport
        - reboot
        - sundiag.sh
        - ipmitool
        - ipmitool_interactive (same as ipmitool, can be used when tty is required)
    - Host (Alias): These commands can be run directly from the Bash prompt.
        - dbmcli - all commands
        - sundiag.sh
        - virsh - all options
        - xm - all options
        - virsh_interactive - all options (same as virsh, can be used when tty is required)
        - xm_interactive - all options (same as xm, can be used when tty is required)
        - xentop - all options
        - vm_maker - all options
        - docker
        - docker_interactive (same as docker, can be used when tty is required)
        - podman
        - podman_interactive (same as podman, can be used when tty is required)
        - imageinfo
        - imagehistory
        - ethtool
        - sosreport
        - ipmitool
        - ipmitool_interactive (same as ipmitool, can be used when tty is required)
        - ops_console.sh

Directories and files with explicit Read and Write access:

- Control Plane Server:
    - Read and Write: /u01/
    - Read-Only:
        - /var/log/
        - /opt/oci/exacc/exacloud/log/
        - /opt/oracle.cellos/
        - /usr/local/nessus/results/
        - /opt/nessus/var/nessus/logs/
    - Special Operator Access Control commands: Cage commands to view or modify (read, read/write) files or directories mentioned above.
        - sudols
        - sudocp
        - sudocat
        - sudotail
        - sudohead
        - sudovi
        - sudorm

Copyright © 2026, Oracle and/or its affiliates / Public

- Host:
    - Read and Write: None
    - Read-Only: /var/log/
    - Special Operator Access Control Commands: Cage commands to view or modify (read, read/write) files or directories mentioned above.
        - sudols
        - sudocp
        - sudocat
        - sudotail
        - sudohead

The following directories are mapped in a read-write mode for the tools to run; however, Oracle operators are not granted direct access to them.

- /var
- /opt/oracle
- /home/dbmadmin

- Cell server:
    - Read and Write: None
    - Read Only: /var/log/
    - Special Operator Access Control commands: Cage commands to view or modify (read, read/write) files or directories mentioned above.
        - sudols
        - sudocp
        - sudocat
        - sudotail
        - sudohead

The following directories are mapped in a read-write mode for the tools to run; however, Oracle operators are not granted direct access to them.

- /var
- /opt/oracle
- /home/celladmin/
- /usr/sbin/xm
- /usr/sbin/xentop
- /usr/sbin/virsh

Exadata Storage Server Privileges: `celladmin`

Network Privileges: Can `SSH` into all Exadata Database Server Infrastructure, Exadata Storage Servers and Control Plane Servers. The user name is same across all of these.

Full System Access

Full System Access, identified as `INFRA_FULL` is designed to diagnose and resolve issues within the core Oracle Linux operating system, Oracle Linux kernel code, and hardware/firmware issues. Full System Access action is used when full (root) access to infrastructure is required, such as access to power distribution units (PDU) and Integrated Lights Out Management (ILOM) console. Access is always limited to non-customer VM layers. Full access means the root privileges on every operating system instance in the system, other than your VMs. You should expect `INFRA_FULL` access requests for diagnostics related to driver software and hardware devices, as

Copyright © 2026, Oracle and/or its affiliates / Public

well as for resolution of issues related to driver software and hardware devices. `INFRA_FULL` access is also required to restart or perform diagnostics and maintenance on infrastructure components that fail to boot.

Table 5 details Full System Access privileges. Note:

- Full System Access Action poses availability and data exposure risks, which can be persistent. The action also provides ability to bar export of audit logs from the system.
- Oracle audit logging via OCI Bastion servers provides a compensating control to mitigate risk of audit log tampering on the ExaDB-C@C infrastructure

Table 5: Full System Access Privileges

OPERATOR PRIVILEGES
Linux User Privilege: Non-root
Can su to root: yes
chroot jail: No
Directories Readable: All
Files Readable: All
Directories Writeable: All
Files Writeable: All
List of commands executable: All
Can su into: root through sudo
sudo user + command list: No restriction
Cell server privileges: root and celladmin
Network Privileges: Can SSH into all hosts, cell servers, and Control Plane Servers. The user name is the same across all of these. Also, connect to root directly on the host, cell server to using exassh

Audit

Audit logs reveal Oracle staff actions, including commands run and keystrokes entered. Operator Access Control logs this activity using Oracle Linux auditd on infrastructure components, with records that include timestamps and user information. Hypervisor logs are collected independently of staff access. You can access audit logs through the following technology:

- OCI Logging service
- Your syslog server (ExaDB-C@C only)
- Operator Activity Audit Log Report

The OCI Logging service typically shows Operator Access Logs within 30 seconds of command execution. You can integrate your OCI Logging service with your OCI Streaming service and send Operator Access Control audit log information to your compatible endpoints. Oracle publishes tutorials on how to send audit logs to third party SIEM systems.

The CPS connects to your syslog server and delivers audit logs over secure TCP only. Operator Access Control does not support UDP connections to syslog servers.

Revoking Access

Revoking an access request stops Oracle staff access by:

- Terminating SSH connections
- Terminating processes and child processes started by temporary accounts
- Removing temporary accounts

Copyright © 2026, Oracle and/or its affiliates / Public

- Removing temporary network access

You must approve a subsequent access request for Oracle to complete maintenance work.

Cloud Interfaces and Notification

You configure and manage Operator Access Control via OCI Console (web UI) or OCI APIs. The OCI Console is a simple, intuitive interface to permit a person to easily interact with Operator Access Control to configure policies, apply policies to infrastructure, and grant, monitor, and revoke access.

OCI APIs provide programmatic access to the same functionality as the OCI Console. You can use OCI APIs to integrate Operator Access Control management into your compatible systems and processes, such as ticketing and change management systems. The OCI Developer Tools documentation shows how to integrate with the OCI API framework. The Oracle A-Team publishes API signing and Postman integration examples, and Oracle Help Center publishes the Identify Cloud Service tutorial.

Operator Access Control publishes access requests to OCI interfaces. You access these interfaces from the OCI Console and OCI API interfaces to learn if you have a pending access request. If you poll access requests, poll frequently (<5 minutes) when you configure explicit approval to avoid process delays.

You can configure push notifications using the OCI Events and OCI Notifications services. Operator Access Control publishes the following events:

- access request – Approve
- access request – Auto Approve
- access request – Create
- access request – Close
- access request – Expire
- access request – Extend
- access request – Reject
- access request – Revoke
- access request Shared Operator – Create
- Assign Operator Control – Create
- Assign Operator Control – Delete
- Assign Operator Control – Update
- Operator – Login
- Operator – Logout
- Operator Control – Create
- Operator Control – Delete
- Operator Control – Update

You can filter Events prior Notifications for processing purposes. Notifications support the following formats:

- Email
- Function
- HTTPs (custom URL)
- Pager duty
- Slack
- SMS

You can integrate Notifications and Events with your compatible change management systems. For example, you can integrate with ServiceNow and You can use a custom URL subscription to integrate with compatible change management systems.

The Operator Access Control access request – Create event includes an attribute for “Approval Required.” You can use this feature to notify to your staff differently for pre-approved and explicit customer approval to help you optimize operations. The Operator Access Control Login and Logout events show when Oracle staff log into and out of the system to help you dynamically adjust your security posture.

Copyright © 2026, Oracle and/or its affiliates / Public

Concept of Operations

You and Oracle work together to support your service infrastructure when you use Operator Access Control. Oracle requests access, including the time and privileges required to do the work. You review and approve access to start immediately or at a future time. This section shows how you and Oracle work together so that you can plan updates to your business processes accordingly.

Access Request Process Flow

Oracle and your team coordinate each Operator Access Control session. The key steps are:

1. Oracle monitoring creates a ticket.
2. Oracle staff request access for the required privileges.
3. You receive and review the request.
4. You approve (or reject) the request.
5. Temporary credentials are created and delivered.
6. Oracle staff log in with MFA.
7. Actions are audited, with logs sent to your configured endpoints.
8. You monitor progress using compatible tools.
9. You revoke access when required

You can communicate with Oracle via Operator Interaction. Every message is logged as part of the request record.

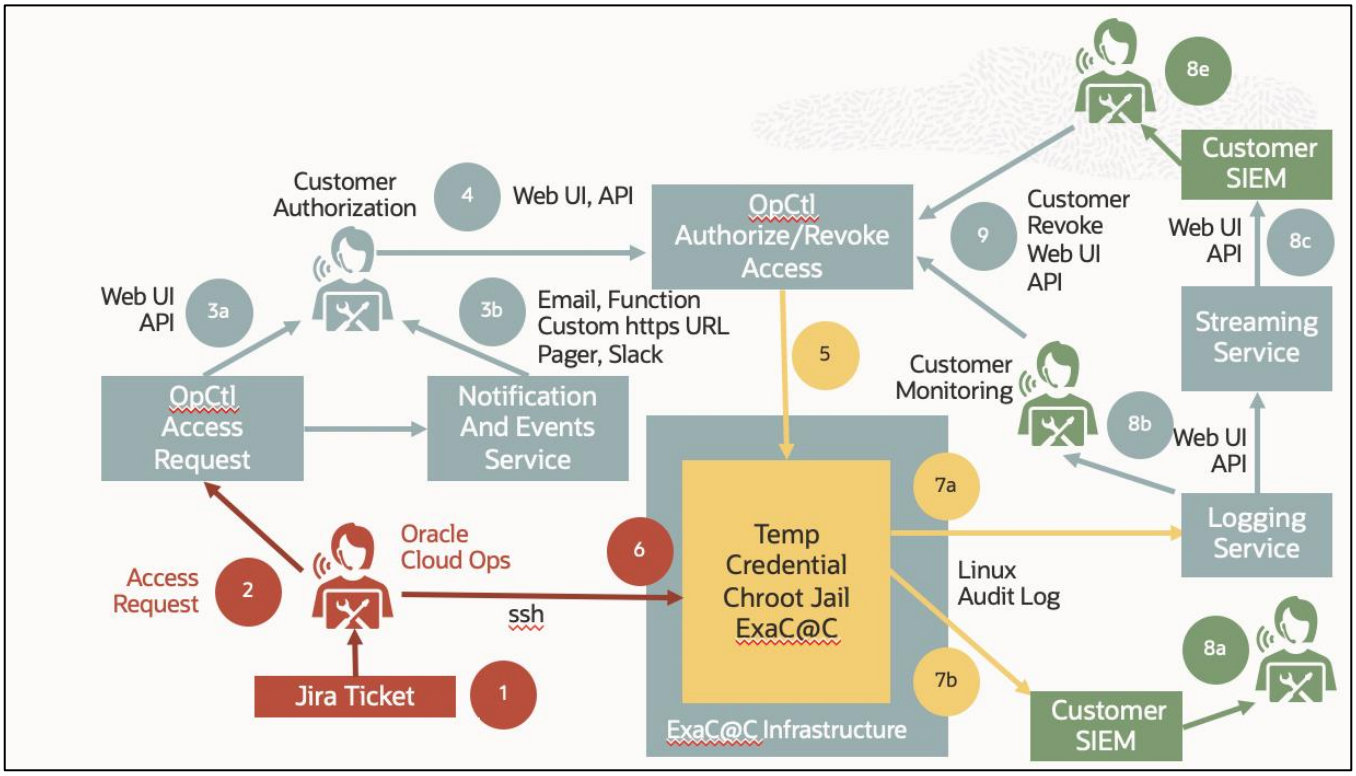

Figure 6: Operator Access Control Operational Flow

Oracle Staffing Updates

Oracle may change staffing for your access request because the work:

- Was approved outside of the shift hours of the requesting staff
- Duration exceeded the staff's shift
- Required additional skills

The same controls support all cases:

- The new staff issues an "Add Shared Operator – Create" request.

Copyright © 2026, Oracle and/or its affiliates / Public

- You receive an “Add Shared Operator – Create” event to inform you of the change.
- A temporary and unique account with the Action Enforcement you approved is given to the new staff.
- The new staff authenticate to the new temporary account.

You can individually identify command and keystroke audit records. If you revoke the access request, Operator Access Control removes all the credentials related to the access request.

Your Approval Policies

Operator Access Control Policies have two approval options for each Action:

- Pre-approved
- Explicit approval

When you pre-approve an Action, the temporary credential is automatically deployed after the access request is created. Pre-approval reduces management effort and improves service quality and availability. When you configure explicit approval, you must approve the access request before the temporary credential is deployed. Explicit approval gives you control of when Oracle can access your infrastructure. Action Enforcement, logging, and revoking access operate identically with pre-approval and explicit approval.

You can selectively pre-approve Actions to balance the risks and benefits of the Action. You can configure time windows with different levels of pre-approval to balance service quality and availability with access control requirements. You can approve access immediately or at a future time to accommodate business and operational needs. You can change pre-approval policies at any time.

You control maintenance windows for your service infrastructure. To help ensure service quality during planned maintenance, you can pre-approve all system access profiles during maintenance windows. When you do this, Oracle staff have immediate access to resolve any unexpected issue or failure. Operator Access Control automatically revokes this type of pre-approved access at the end of the maintenance window.

Implications for Service Quality and Availability

Oracle staff work to support service availability and quality for you. If you configure explicit approval for access, your business processes and technology must ensure timely response and approval. If you respond to an access request in 15 minutes or less, Oracle can maintain service quality and availability. Delaying approval may lead to a service disruption. The disruption may be excluded from service availability calculations. Refer to Common Exclusions in the Oracle PaaS and IaaS Public Cloud Services Pillar Document for detail.

If you cannot respond in15 minutes or less, you can reduce risks service quality and availability risks by pre-approving access. You still realize the benefits of temporary, least-privileged, and just-in-time access, Action Enforcement, command and keystroke logging, and revoking access. There are no exclusions beyond the common service exclusions when you pre-approve access.

Failure Recovery

A highly available (HA) design helps to protects against any single hardware or software component failure in the Operator Access Control service. The Operator Access Control design does not include an alternate human remote shell access method. To recover from Operator Access Control software failure for ExaDB-C@C:

- Oracle contacts you regarding the issue.
- Oracle staff travel to the location of the physical equipment.
- Your staff escort Oracle staff to the physical equipment.
- Oracle staff accesses physical equipment and performs analysis and recovery.

Oracle data center security practices control Oracle staff access to recover from Operator Access Control software failure for ExaDB-D in OCI, AWS, Azure, and Google Cloud.

After restoring Operator Access Control functionality, Oracle performs subsequent remote access through Operator Access Control.

Copyright © 2026, Oracle and/or its affiliates / Public

Security Incident Reporting and Communication

Oracle Incident Response shows how Oracle responds to security incidents. Oracle will respond to information security events when Oracle suspects unauthorized access to Oracle-managed assets. You are responsible for controlling user access and monitoring your services via available tooling and logging. You should report suspected unauthorized access or actions via the Oracle Service Request (SR) process by opening a My Oracle Support (MOS) Security Service Request (SR) and indicating the details of the suspected unauthorized access or actions.

Summary

Operator Access Control helps you meet policy and regulatory requirements for managing Oracle staff access. It integrates closely with your change management tools, SIEM systems, and security teams. To maintain service quality, you must respond promptly to Oracle access requests. Consider pre-approving requests or integrating Operator Access Control with your 24x7 on-call systems to support service availability.

Copyright © 2026, Oracle and/or its affiliates / Public

ORACLE

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

Copyright © 2026, Oracle and/or its affiliates. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.