ORACLE

Oracle Operator Access Control

How you control Oracle staff access to resources supporting your services

Jan 13, 2026, Version 3.10

Public

Purpose

This document provides an overview of features and enhancements included in Oracle Operator Access Control.[1] 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, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

[1] https://docs.oracle.com/en-us/iaas/operator-access-control/index.html

Table of Contents

List of Images

List of Tables

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. It supports Exadata Cloud@Customer, Compute Cloud@Customer, and Autonomous Database Dedicated.[2]

Architecture

ExaDB-C@C runs in your data center, using a standard Exadata Database Machine and two Control Plane Servers (CPS). CPS connect your Exadata to Oracle Cloud, so both you and Oracle can manage the system. Figure 1 shows the architecture block diagram.

You control database access through your own network, 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 and API Access Control.[3,4] You control which endpoints the CPS accesses.

For more on security, review:

- Exadata Cloud@Customer Security Controls[5]
- Exadata Cloud@Customer Security Guide[6]
- Security Features in Autonomous Database[7]
- Securing Compute Cloud@Customer[8]

[2] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-49AE3FAF-95E3-4D7D-B950-9FC52C4B5FA9

[3] https://docs.oracle.com/en-us/iaas/oracle-api-access-control/doc/overview-of-api-access-control.html

[4] https://www.youtube.com/watch?v=-kzyH4LzP3c

[5] https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/exadata-cloud-at-customer-security-controls.pdf

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

[7] https://docs.oracle.com/en-us/iaas/autonomous-database/doc/security-features-adb-d.html

[8] https://docs.oracle.com/en-us/iaas/compute-cloud-at-customer/ccc/securing_compute_cloud_customer.htm

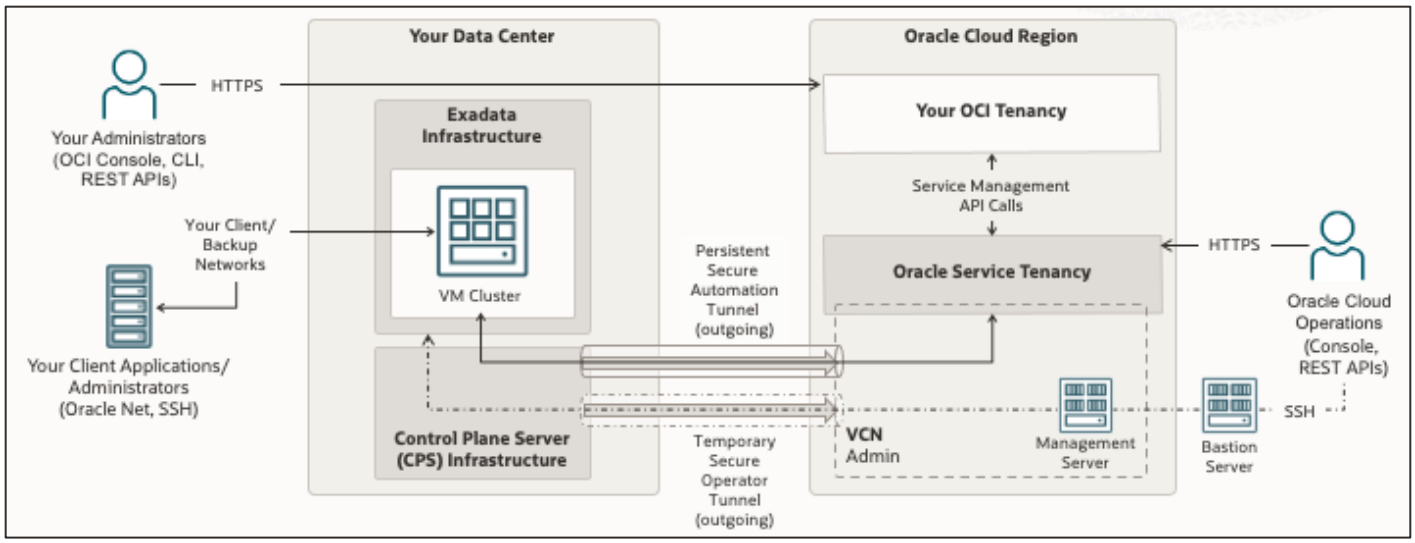

Figure 1: Gen 2 ExaDB-C@C Network Architecture

When you use Operator Access Control:

- Oracle staff remote shell accounts are removed from Oracle-managed components.
- 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.
- Action Enforcement[9] controls privilege limits.
- Commands and keystrokes are reported to your OCI Logging service and syslog server.[10]

Figure 2 shows major components in the Operator Access Control SSH access flow:

- Oracle staff authenticate to Oracle Cloud Network Attach (OCNA) 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[11]
  - Oracle geographic control controls, as set in the Consensus Assessment Initiative Questionnaire[12]
- Staff authenticate to Bastion and Management servers with FIPS 140-2 level 3 hardware MFA.
- 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.

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,[13] Human Resources

[9] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-F0334C90-AB4B-429F-AA51-8FD7508BB241

[10] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-6526ADE1-C664-4600-A62B-5993EA25134E

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

[12] https://www.oracle.com/a/ocom/docs/oci-corporate-caiq.pdf

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

Security,[14] and Information Asset Classification[15] practices. Oracle Export Restrictions, Prohibited End Users[16] indicates countries and persons that may not access Oracle Cloud Services.

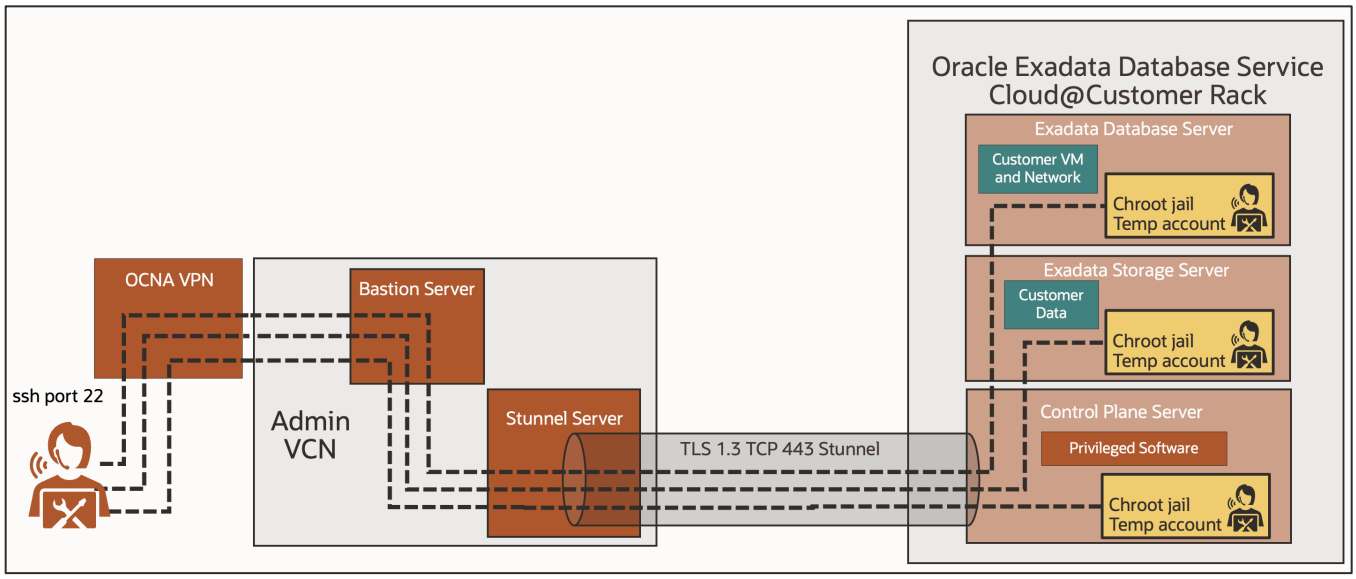

Figure 2: Operator Access Control Access Architecture

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 apply policies that govern the rules by which a system can be accessed
- Configure notifications and logging per your standards
- Respond to Access Requests in a timely manner
- Monitor Oracle staff commands and keystrokes for security and audit purposes
- Revoke or deny access to infrastructure as your business and security needs dictate

Preventive Security Controls

Preventive 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.

SSH Authentication

By default, your service infrastructure 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 the `~/.ssh/authorized_keys`

[14] https://www.oracle.com/corporate/security-practices/corporate/human-resources-security/#awareness

[15] https://www.oracle.com/corporate/security-practices/corporate/information-assets-classification/

[16] https://www.oracle.com/corporate/security-practices/corporate/governance/global-trade-compliance/

file. All actions and keystrokes are logged per user. When the Access Request ends, Operator Access Control deletes all related accounts.

Action Enforcement

Operator Access Control Action Enforcement[17] uses Oracle Linux chroot jail[18] and other security software to restrict what administrative commands can do. This includes accessible file systems and files, and wrapper code that:

- Prevents direct access to system commands and utilities
- Limits the arguments the operator can send to those system commands and utilities

A chroot jail changes the apparent root directory for a running process and its children. It allows you to run a program with a root directory other than /. The program cannot see or access files outside the designated directory tree. This limits the directory access of a potential attacker. The chroot jail locks down a given process and any user ID that it is using so that all they see is the directory in which the process is running. To the process, it appears that the directory in which it is running is the root directory. See the Oracle Linux Security Guide[19] for detail.

Operator Access Control Actions translate Oracle Linux permissions on the target system. 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 five different Actions for ExaDB-C@C:

- Control Plane Server Only
- System Diagnostics
- System Maintenance with Restart Privileges
- System Maintenance with Hypervisor access / VM Control Privileges
- Full System Access

Operator Access Control Actions documentation[20] details the controls for each Action, summarized below.

Control Plane Server Only

Control Plane Server Only,[21] identified as `INFRA_CPS_ONLY`, 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

ACTION NAME	ACTION IDENTIFIER	OPERATOR PRIVILEGES

[17] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-B62E1B69-8B2F-4ACC-8454-65F5983D8E41

[18] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/security-ImplementingOracleLinuxSecurity.html#ol7-s3-syssec

[19] https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-implement-sec.html#ol7-s3-syssec

[20] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-533A688A-FC75-43A8-B7DF-6481D781C872

[21] https://docs.oracle.com/en-us/iaas/operator-access-control/doc/overview-of-operator-access-control.html#GUID-EBA5FE64-26E6-4709-8804-3E1B61123E7D

Control Plane Server (CPS) Only	`INFRA_CPS_ONLY`	**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
		  • 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,[22] identified as `INFRA_DIAG`, is designed for diagnosing any issue in the ExaDB-C@C infrastructure layer. In cases where Oracle Cloud Ops only has a need to perform diagnostics access, Oracle Cloud Ops will ask for `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:

[22] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-D461D65B-CEC9-4720-9433-28BBC75F5CDE

- 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

ACTION NAME	ACTION IDENTIFIER	OPERATOR PRIVILEGES

System Diagnostics	`INFRA_DIAG`	**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
		  • 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
		• **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,[23] 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

[23] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-F02B41E2-D939-4599-AA18-50168D12585D

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 ExaDB-C@C system offline.
  - 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.
  - 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

ACTION NAME	ACTION IDENTIFIER	OPERATOR PRIVILEGES
System Maintenance with Restart Privileges	`INFRA_UPDATE_RESTART`	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
  - 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
  - **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,[24] 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 in the ExaDB-C@C database 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.
  - 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.

[24] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-931033E2-23F6-4975-8B6D-39C4243C9596

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

ACTION NAME	ACTION IDENTIFIER	OPERATOR PRIVILEGES

System Maintenance with Data Access / VM Control Privileges	`INFRA_HYPERVISOR`	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
- 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

- **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,[25] 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 access of the ExaDB-C@C 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 ExaDB-C@C system, other than your VM. You should expect `INFRA_FULL` Access Requests for diagnostics related to driver software and hardware devices, as 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

ACTION NAME	ACTION IDENTIFIER	OPERATOR PRIVILEGES
Full System Access	`INFRA_FULL`	**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

[25] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-65E3E007-1F3D-4871-BDFB-20C876DE1C17

		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

Detective Security Controls

Detective controls reveal Oracle staff actions, including commands run and keystrokes entered. Operator Access Control logs this activity using Oracle Linux auditd[26,27] on infrastructure components, with records that include timestamps and user information. Hypervisor logs are collected independently of staff access. You can review all logs using two interfaces:

- OCI Logging Service[28]
- Direct send of audit logs in syslog format to your IP address or hostname of your syslog server[29]

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[30] and send Operator Access Control audit log information to your compatible endpoints. Oracle publishes tutorials on how to stream OCI Logs to Splunk.[31,32] The Control Plane Server connects to your syslog server and delivers audit logs over secure TCP only. Operator Access Control does not support UDP connections to syslog servers. You can use the OCI Console and API to generate and download a human-readable HTML formatted file containing the Oracle Linux audit records for a specific Operator Access Control Access Request.[33]

Responsive Security Controls

Responsive controls stop Oracle staff access. You can revoke an Access Request to:

- Terminate SSH connections
- Terminate processes and child processes started by temporary accounts
- Remove temporary accounts

You will need to approve a subsequent Access Request for Oracle to complete maintenance work.

---

[26] https://docs.oracle.com/en/operating-systems/oracle-linux/8/auditing/configuring_and_using_auditing.html

[27] https://docs.oracle.com/en/learn/ol-auditd/#introduction

[28] https://docs.oracle.com/en-us/iaas/Content/Logging/Concepts/loggingoverview.htm.

[29] https://docs.oracle.com/en/cloud/paas/operator-access-control/exops/overview-of-operator-access-control.html#GUID-6526ADE1-C664-4600-A62B-5993EA25134E

[30] https://docs.oracle.com/en-us/iaas/Content/Streaming/Concepts/streamingoverview.htm

[31] https://docs.oracle.com/en/solutions/logs-stream-splunk/index.html#GUID-8D87CAA4-CD41-4E90-A333-5B04E23DBFAA

[32] https://blogs.oracle.com/cloud-infrastructure/announcing-the-oracle-cloud-infrastructure-logging-plugin-for-splunk

[33] https://docs.oracle.com/en-us/iaas/operator-access-control/doc/managing-access-requests.html#GUID-B52FA4FA-95C8-4719-AB43-0D6574E8B179

Concept of Operations

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 deny) the access.
5. Temporary credentials are created and delivered.
6. Oracle staff log in with MFA.
7. Actions are audited, with logs sent to your OCI Logging service and syslog server.
8. You monitor progress using compatible tools.
9. You revoke access when required

At any time, you can communicate with Oracle via Operator Interaction.[34] Every message is logged as part of the request record.

For process details and demonstration, see:

- Process Flow for Operator Access Control (Operator Access Control) (Doc ID 2788316.2)[35]
- Operator Access Control Demonstration Video[36]

[34] https://docs.oracle.com/en-us/iaas/operator-access-control/doc/managing-access-requests.html

[35] https://support.oracle.com/epmos/faces/DocumentDisplay?id=2788316.2

[36] https://www.youtube.com/watch?v=ZCLMs_kgSr4

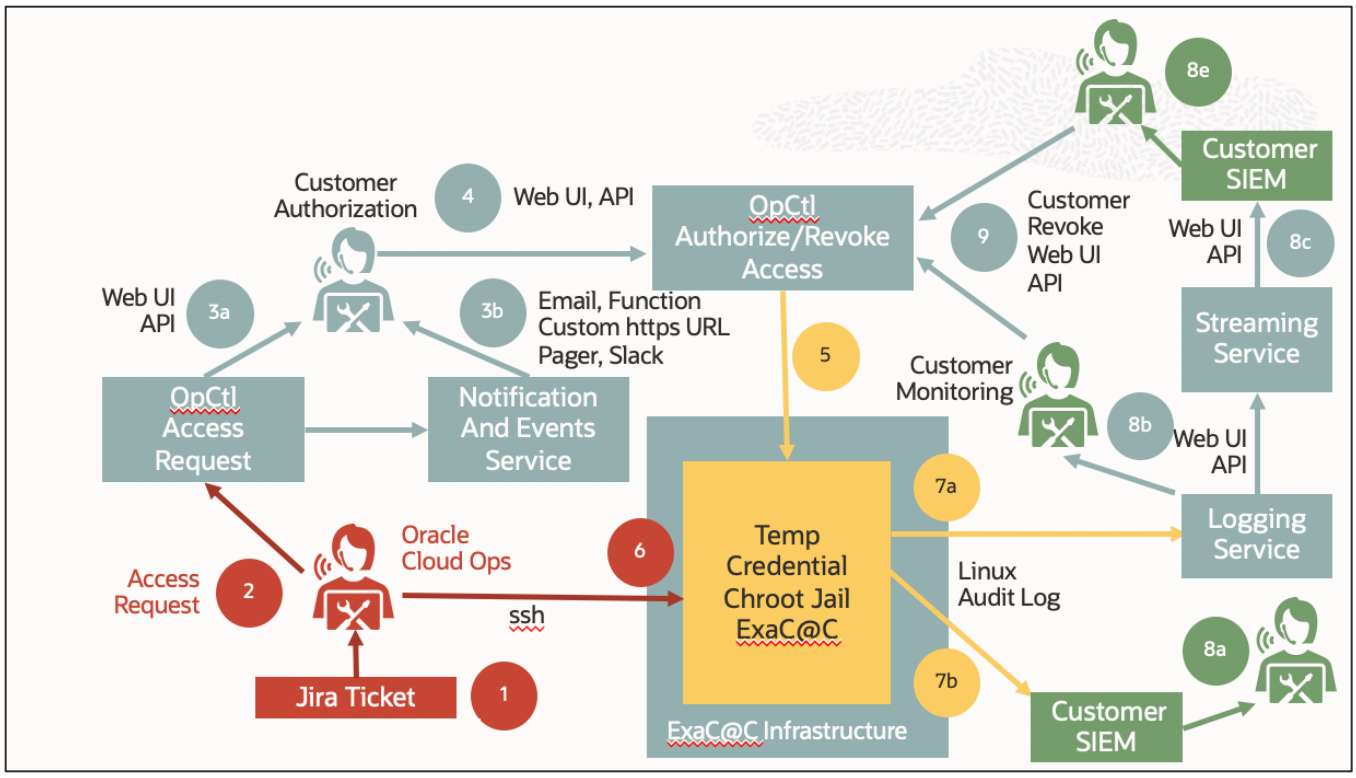

Figure 3: Operator Access Control Operational Flow

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.
- 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.

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 ExaDB-C@C infrastructure. To help ensure service quality during planned maintenance, you can pre-approve all system access profiles during maintenance windows.[37] 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. Reference Common Exclusions in the Oracle PaaS and IaaS Public Cloud Services Pillar Document[38] for detail.

If you cannot respond in15 minutes or less, you can reduce risks service quality and availability risks by pre-approving access.[39] 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 standard service exclusions[40] when you pre-approve access.

Cloud Interfaces

You configure and manage Operator Access Control via OCI Console[41] (web UI) or OCI APIs.[42] 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[43] documentation shows how to integrate with the OCI API framework. The Oracle A-Team publishes API signing[44] and Postman integration examples.[45,46]

---

[37] https://docs.oracle.com/en-us/iaas/operator-access-control/doc/managing-infrastructure-access.html

[38] https://www.oracle.com/contracts/docs/paas_iaas_pub_cld_srvs_pillar_4021422.pdf

[39] https://docs.oracle.com/en-us/iaas/operator-access-control/doc/managing-infrastructure-access.html#GUID-328FD123-AB5A-4CFA-9606-203D35FC9AB1

[40] https://docs.oracle.com/en-us/iaas/Content/General/Reference/servicelevelobjectives.htm

[41] https://docs.oracle.com/en-us/iaas/Content/GSG/Concepts/console.htm

[42] https://docs.oracle.com/en-us/iaas/api/#/en/operatoraccesscontrol/20200630/

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

[44] https://www.ateam-oracle.com/post/oracle-cloud-infrastructure-oci-rest-call-walkthrough-with-curl

[45] https://www.oracle.com/webfolder/technetwork/tutorials/obe/cloud/idcs/idcs_rest_postman_obe/rest_postman.html

[46] https://www.ateam-oracle.com/post/invoking-oci-application-performance-monitoring-rest-apis-using-postman

Cloud Notification

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[47] and OCI Notification[48] services. Operator Access Control publishes the following events:[49]

- 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 supports 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 use OCI Functions with Notifications to integrate with ServiceNow.[50] You can use a custom URL subscription to integrate with compatible change management systems.[51]

The Operator Access Control createaccessrequest 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.

---

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

[48] https://docs.oracle.com/en-us/iaas/Content/Notification/Concepts/notificationoverview.htm

[49] https://docs.oracle.com/en-us/iaas/operator-access-control/doc/auditing-operator-access-control-lifecycle-events.html

[50] https://www.ateam-oracle.com/post/a-simple-guide-to-managing-oci-alarms-in-servicenow

[51] https://docs.servicenow.com/bundle/rome-it-operations-management/page/product/event-management/task/oracle-cloud-events-integration.html

Integration Test and Validation

You can request Oracle staff to work with you to test Operator Access Control as follows:

- You open an SR and ask Oracle to create an Access Request
- Oracle raises an Access Request
- You approve the Access Request
- Oracle processes the Access Request

Oracle will make a best-effort response to perform the Access Request test to help you validate Access Request processing integration with your systems. The Access Request test performs a predefined set of commands so you can validate logging functionality and integration. Prior to requesting an Access Request test, you need the following:

- ExaDB-C@C infrastructure OCID
- Selection of which Access Request test to perform as a select of one of the following tests: diagnostics, maintenance with restart, maintenance with VM/data access, or full access

The Service Request process is:

- Log into My Oracle Support (MOS) and select “Create Technical SR”
- Enter useful metadata in “Problem Summary”, “Problem Description”
- Under “Where is the Problem?” select the “Cloud” Tab
- In the “Service Type” field enter “Gen 2 Exadata Cloud at Customer”
- For “Problem Type” select “Infrastructure (dom0)” then select “Operator Access Control Test (Limited Availability)”
- Select severity level 2[52]
- Click “Next"
- Provide your target OCID in the OCID field (can be easily copied and pasted from web)
- Click the radio button for the desired test (Diagnostics Access is sufficient for most integration test work)
- Submit the request
- Approve Operator Access Control Access Request
- Monitor Access Request logs (optional)
- Verify completion of Access Request test
- Close SR

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:

- 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.

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

Security Incident Reporting and Communication

Oracle Incident Response[53] 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

[52] A severity 2 service request automatically pages Cloud Ops on-call staff to notify them of the action, and this provides timely response from Oracle for customer validation of Operator Access Control integration; if a severity 3-5 service request is opened, then the Access Request test will receive a longer response time

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

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 consistent ExaDB-C@C availability.