Oracle® Operator Access Control

Oracle Operator Access Control Configuration and Administration Guide

F32988-21
May 2024

Oracle Operator Access Control Oracle Operator Access Control Configuration and Administration Guide,

F32988-21

Primary Authors: Douglas Williams, Nirmal Kumar

Contributing Authors: Behkam Aminzadeh, Harish Prabhakara, Harsha Srikanth Karna, Jeffrey Wright, Joydip Kundu, Kiran Viswanatham, Kris Bhanushali, Krishna Chander, Lok Liu, Mathew Steinberg, Prasanna Ramamurthi, Ramkumar Krishnan

Contents

1

Overview of Oracle Operator Access Control

Learn how to control, audit, and revoke access of Oracle service staff to your infrastructure by using Oracle Operator Access Control.

- What is Oracle Operator Access Control?
  Oracle Operator Access Control enables you to grant, audit, and revoke the access Oracle has to your Exadata Infrastructure, Exadata Infrastructure hosting an Oracle Autonomous Database on Exadata Cloud@Customer, and Autonomous Exadata VM Cluster (client virtual machines deployed on Oracle Autonomous Database on Exadata Cloud@Customer) administered by Oracle, and to obtain audit reports of all actions taken by a human operator, in a near real-time manner.
- Terms Associated with Operator Access Control
  Learn about what terms are used with Operator Access Control.
- What Control Options Does Oracle Operator Access Control Provide?
  You create policies that specify which set of Actions operators can perform on your infrastructure.
- Enforcement of Actions in Operator Access Control
  Learn about enforcing controls on the operations an Oracle operator can perform in your environment.
- Limits for Operator Access Control
  Operator Access Control is a solution designed for auditing and compliance of Oracle access, not a general purpose compliance solution.
- Customer Tenancy Job Roles for Operator Access Control
  To establish operator access control, you set up access control policies, and establish user groups responsible for managing and monitoring access to your infrastructure.
- Forwarding Operator Access Control Audit Logs to SIEM Systems
  You can choose to forward Operator Access Control audit logs directly from Exadata Cloud@Customer to the security information and event management (SIEM) systems in your data center.

What is Oracle Operator Access Control?

Oracle Operator Access Control enables you to grant, audit, and revoke the access Oracle has to your Exadata Infrastructure, Exadata Infrastructure hosting an Oracle Autonomous Database on Exadata Cloud@Customer, and Autonomous Exadata VM Cluster (client virtual machines deployed on Oracle Autonomous Database on Exadata Cloud@Customer) administered by Oracle, and to obtain audit reports of all actions taken by a human operator, in a near real-time manner.

Oracle Operator Access Control for Exadata Cloud@Customer

Oracle Exadata Cloud@Customer service is a shared responsibility system:

- You are responsible for actions in your virtual machines, and day-to-day management of databases and applications that run on your virtual machines.

- Oracle is responsible for the infrastructure components: power, bare-metal operating system, hypervisors, Exadata Storage Servers, and other aspects of the infrastructure environment.

However, if you have regulatory requirements to audit and control all aspects of your system management, then the shared responsibility model creates a problem. You have to prove to your regulators that you are in complete control of your systems, and you are operating your systems in compliance with those compliance regulations.

How can you control and audit all actions performed on infrastructure components by any operator or any software on your systems? How can you maintain the same level of audits and access control to your systems, and provide the audit records required for internal or external regulatory audits across your systems? To solve this problem, Oracle provides Oracle Operator Access Control as the solution to restrain Oracle operators' unfettered access to your systems.

Operator Access Control for Oracle Autonomous Database on Exadata Cloud@Customer

Operator Access Control has been expanded to provide controls for client virtual machines deployed on Oracle Autonomous Database on Exadata Cloud@Customer. Similar to Operator access control for Exadata Cloud@Customer Infrastructure, customers may now impose Oracle operator access controls on their Autonomous Virtual Machine clusters deployed on Exadata Cloud@Customer.

The delivery of the Autonomous Database on dedicated infrastructure (both in OCI and Cloud@Customer) is based on the tenet that the customer is the "user" of the database and Oracle is the "manager". By "manage" we mean the typical database admin or DBA tasks such as the following:

- Provisioning Autonomous Database resources
- Backing up databases
- Recovering a database
- Patching and upgrading
- Scaling
- Monitoring service health
- Auditing
- Alerts and Notifications

The customer has no access to the client operating system, sys/system access to their container databases, or access to system logs. And, the customer is limited to monitoring application health and performance and security of applications at all levels. Oracle operators, on the other hand, being the manager has complete, unrestrained access to all components including root access to hypervisor and client VMs.

The shared responsibility model for Autonomous database poses several operational challenges to regulated customers who are required to retain control of all data and infrastructure regardless of vendor and deployment model (on-premise, hosted, or cloud). Regulated customers undergo their own compliance scrutiny and formulate their own security guidelines that may take years to harden and put into practice.

This is especially true of Oracle's enterprise customers that are highly regulated and run their most critical systems, their most security-sensitive applications on Oracle. To

solve this problem, Oracle provides Oracle Operator Access Control as the solution to restrain Oracle operators' unfettered access to your systems.

Oracle Operator Access Control for Oracle Cloud Infrastructure

Oracle Operator Access Control is a compliance audit system that enables you to maintain close management and audit trails of all actions that an Oracle operator performs on the infrastructure.

Oracle Operator Access Control enables you to do the following:

- Grant access to your infrastructure, including who can access the infrastructure, when the system can be accessed, and how long Oracle personnel can access the system.
- View and save a near real-time report of all actions an Oracle operator performs on your system.
- Limit access, including limiting what actions an Oracle operator can perform on your system.
- Revoke access, including the access that you have granted previously.

Operator Access Control for Compute Cloud@Customer

The Compute Cloud@Customer infrastructure is based on the tenet that the customer is the 'user' of VMs and services they create and run on the infrastructure and Oracle is the 'manager' of the infrastructure itself. By 'manage' we mean typical tasks such as upgrading, patching, and monitoring for the infrastructure components.

The customer has no access to infrastructure virtual or bare-metal OS instances on infrastructure components nor management software that runs on these instances. Oracle Ops, on the other hand, being the manager, has complete, unrestrained access to all components including root access to hypervisor and Control Plane Servers.

This model poses several operational challenges to regulated customers who are required to retain control of all data and infrastructure regardless of vendor and deployment model (on-premises, hosted, or cloud) Regulated customers undergo their own compliance scrutiny and formulate their own security guidelines that may take years to harden and put into practice. This is especially true of Oracle's enterprise customers that are highly regulated and run their most critical systems, their most security-sensitive applications on Oracle.

Operator Access Control has been extended to support these customer compliance objectives and enable them to bring their mission-critical databases to Oracle Cloud such that customers are ultimately in control of access to their dedicated systems.

Terms Associated with Operator Access Control

Learn about what terms are used with Operator Access Control.

Operator: An Oracle employee that is a member of an operators group (Ops group) tenancy in Oracle Cloud Infrastructure (OCI). For example, an operator can be an Oracle employee in the `Exadata Cloud@Customer_ops` group or the `ExaCS_ops` group. The Ops group tenancy is a set of tenancies in OCI that are permitted to administer operation controls. The Ops groups, and the operators that are members of these groups, do not have any default privilege other than the ability to request access to infrastructure. The groups and membership in the operator groups is strictly controlled by Oracle.

User: An OCI user of the tenancy on whose Exadata Cloud@Customer system the controls are placed.

Exadata Infrastructure Layer: Multiple physical or operating system layers of the Exadata system. Currently, defined as Control Plane Server, Host, Guest VM, cell servers, switches, and `ILOM`.

Action: A named, predefined set of commands, files, or networks that can be accessed on a given layer. Oracle defines actions.

Operator Control: A customer-defined entity, which contains a grouping of pre-approved actions, and actions that require explicit approval from the approval-group to allow access. The approver group is a standard IAM user group that lists the set of users who have permissions to approve or revoke access.

Operator Attributes: In certain cases, the operator control can define criteria for the operators that are permitted to access the infrastructure.

Assignment of Operator Control: This is the process by which an Exadata Cloud@Customer system is attached to a named operator control. At any given point in time, only one operator control can be enforced on an Exadata Cloud@Customer system. The assignment can be permanent or for a specific duration. If an operator control is not assigned to an Exadata Cloud@Customer system, then the Exadata Cloud@Customer system runs with a default operator control that permits all access required for diagnostics and maintenance.

Access Request: Access request is the process by which an operator requests permission to access an identified Exadata infrastructure. The Exadata infrastructure is identified by OCID. The request identifies the action that the operator requires.

Access Request Approve/Reject: Access approve/reject is the process by which a competent user as determined by the operator control deployed on the Exadata infrastructure can grant or reject an access request.

Access Request Revoke: A competent user can revoke an access request at any given point in time. This removes the sessions of the operator connected to the Exadata infrastructure based on this access request immediately.

Access Request In Review: Acknowledge a Raised Oracle Operator Access Request and tell the requester that the access request is being reviewed.

What Control Options Does Oracle Operator Access Control Provide?

You create policies that specify which set of Actions operators can perform on your infrastructure.

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. When you grant permissions through an Action, every action an Oracle operator performs is logged. You can audit the logs as part of your MAC constraint requirements policy.

A **policy** is a set of actions that you specify to implement mandatory access control (MAC) constraints on the ability of Oracle operators to perform maintenance on your systems. To define your policies, these are a list of specific access controls that you can enforce through Actions:

1. Configure operator controls for management of Oracle operators:
   - Operator controls to restrict access profiles on a given resource type in your tenancy. For example, you can set up separate policies for resources such as your virtual machine (VM), the Oracle infrastructure database server, the control plane server, or the InfiniBand network. In addition, you can configure polices to associate access controls to a group of resources in your tenancy.
   - Configure an administrator group of users associated with each operator control. Members of these groups can approve, change, or deny access requests on a resource where you have deployed an operator control.
   - Configure Actions for access to resources that you define as preapproved, without requiring either configuring a group of administrative users to control access.
2. Specify mandatory request authorization before permitting any access to resources. For example:
   - When a set of actions are marked as **pre-approved**, any access request specifying only a subset of such actions will be automatically approved, and Oracle staff can access infrastructure components.
   - When an access policy is not set to **pre-approved**, Oracle staff are denied access to compartments until you explicitly grant access requests.
3. Revoke access to your infrastructure that you have previously granted:
   - Automatic time limits revoke any access that you grant on a resource. When you grant an access request, an Oracle operator is granted a unique user ID for the access you grant for a limited time. When that time limit is reached, all Oracle access to your system related to the approved access request is revoked. If more time is needed, then an Oracle operator can submit an extension request.
   - Revoke access manually that was already granted to a resource before the access you previously granted has expired.
4. Audit all actions a human operator performs on your resources:
   - All keyboard entries and commands run by the human actor are audited. You obtain full access to all Linux audit logs.

     You can request an audit of a specific Oracle human operator on your system.

> **Note:**
>
> The human operator's identity is not available to you as an Oracle customer. However, the Oracle Operator Access Control system maintains service records of the human operator, so that Oracle can correlate the human operator with a specific access request that you have granted for service on your tenancy. If you suspect malicious action, and require an audit, then Oracle can use that request to review all actions of the specific human operator who performed the actions permitted by an access request.

Enforcement of Actions in Operator Access Control

Learn about enforcing controls on the operations an Oracle operator can perform in your environment.

What is Action Enforcement?

Operator Access Control, **Actions** limit the privileges the operator has in running commands, accessing resources, and changing the state of the system.

An Action defines the permissions, resource, and system change access an Oracle operator is granted to perform a given range of tasks for specific administrative functions on a Exadata infrastructure in an environment managed using Operator Access Control. The commands an Action permits can be Oracle Linux commands, or cell server commands.

Resources for which an Action grants access are files and network. System changes correspond to a state change in the operating system, or to a state change in the software running on those systems. The state change is a consequence of restarts or configuration modifications.

Action enforcement is based on approved **Access Requests**, which set up a time-limited policy of which changes you want to enable an Oracle operator to implement, as defined by a set of Actions granted to operators. Every access request creates a temporary user credential in the Exadata infrastructure. The policy of access that you define is based on the Actions you approve in the Access Request, which is attached to the temporary user created.

The Action enforcements are typically a function of the operating system. An Action enforcement policy is created for an instance of the operating system, such as in all hosts, cell servers, and Control Plane Servers. The Actions granted with a policy are removed after the Access Request becomes invalid, either because the Access Request is closed, because the administration task is completed, revoked, or expired.

Action enforcement can be applied to different infrastructure, such as an operating system, to other software, such as `cellcli`.

Operator Access Control Actions: Exadata Infrastructure

Actions define the operations an operator can perform on Exadata Cloud@Customer infrastructure that are limited to host, cell server, and Control Plane Servers.

Actions are applicable to the Exadata Cloud@Customer infrastructure as a whole. Actions control the Oracle operator actions on multiple layers of Exadata Cloud@Customer. The layers controlled in the current version are cell servers, Management Domain (host), and the Control Plane Servers. The actions are

organized by the requirements, which leads to the request of actions and the critical impact these actions potentially generate.

The actions translate Oracle Linux permissions on the target Exadata Cloud@Customer system. The permissions are categorized into file system privileges, command execution privileges, and `su` or `sudo` privileges. The actions are categorized by the nature of the change that can be effected by the operator on the Exadata Cloud@Customer system.

- Action: Control Plane Server (CPS) Only
  Control Plane Server (CPS) Only, which is identified as `INFRA_CPS_ONLY` is intended to be used for diagnosing and resolving CPS issues only. Oracle staff are prevented from accessing components beyond the CPS, including cell servers and host operating system (Dom0).
- Action: System Diagnostics
  System Diagnostics, which is identified as `INFRA_DIAG` is intended to be used for diagnosing any issue in the Exadata Cloud@Customer infrastructure layer.
- Action: System Maintenance with Restart Privileges
  System Maintenance with Restart Privileges, which is identified as `INFRA_UPDATE_RESTART` is intended to be used for operator access scenarios that require a system configuration change, or a restart of the system.
- Action: System Maintenance with Data access / VM Control Privileges
  System Maintenance with Data access / VM control Privileges, which is identified as `INFRA_HYPERVISOR` is intended to be used for diagnostics and maintenance scenarios where VM management on the host is required.
- Action: Full System Access
  Full System Access, which is identified as `INFRA_FULL` permits access to the root accounts on the infrastructure components.

Action: Control Plane Server (CPS) Only

Control Plane Server (CPS) Only, which is identified as `INFRA_CPS_ONLY` is intended to be used for diagnosing and resolving CPS issues only. Oracle staff are prevented from accessing components beyond the CPS, including cell servers and host operating system (Dom0).

Table 1-1 Actions Enabled with INFRA_CPS_ONLY

Action Name	Control Plane Server (CPS) Only
Action Identifier	`INFRA_CPS_ONLY`

Table 1-1 (Cont.) Actions Enabled with INFRA_CPS_ONLY

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` – `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`

Table 1-1 (Cont.) Actions Enabled with INFRA_CPS_ONLY

	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`

Action: System Diagnostics

System Diagnostics, which is identified as `INFRA_DIAG` is intended to be used for diagnosing any issue in the Exadata Cloud@Customer infrastructure layer.

The diagnosis involves reading logs, running diagnostics, and monitoring commands. This action is also intended to fix issues with diagnostics agents in the Exadata Cloud@Customer system. The fix involves restarting diagnostic daemons with potentially modified parameters.

> **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 diagnostic commands such as `top` and `netstat`.
- On cell servers, it additionally allows the operator to run `cellcli` commands to obtain diagnostic information.
- The operator to access the manage the cloud orchestration infrastructure on the Control Plane Server with the capability to restart all daemons on the Control Plane Server.

Table 1-2 Actions Enabled with INFRA_DIAG

Action Name	System Diagnostics
Action Identifier	`INFRA_DIAG`

Table 1-2 (Cont.) Actions Enabled with INFRA_DIAG

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` – `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`

Table 1-2 (Cont.) Actions Enabled with INFRA_DIAG

- `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:**

Table 1-2 (Cont.) Actions Enabled with INFRA_DIAG

	– **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`

Action: System Maintenance with Restart Privileges

System Maintenance with Restart Privileges, which is identified as `INFRA_UPDATE_RESTART` is intended to be used for operator access scenarios that require a system configuration change, or a restart of the system.

The `INFRA_UPDATE_RESTART` scenarios are typically for maintenance. However, there can be diagnostics scenarios where this action is also 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 (host, cell server), to restart specific sub-systems, such as the network, and to restart cell disks.

> **Caution:**
>
> Be aware that System Maintenance with Restart Privileges action permits restarts of infrastructure components (database servers, storage servers, and control plane servers) and prevents access to customer VMs, customer data, and the infrastructure audit service.

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 Exadata Cloud@Customer system offline.
- Allows the operators to change the 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 cell servers.
- Permits the Oracle operator to access the manage the cloud orchestration infrastructure on the Control Plane Server, with the capability to restart all daemons on the Control Plane Server.

Inheritance: All privileges of System Diagnostics

Table 1-3 Actions Enabled with INFRA_UPDATE_RESTART

Action Name	System Maintenance with Restart Privileges
Action Identifier	`INFRA_UPDATE_RESTART`

Table 1-3 (Cont.) Actions Enabled with INFRA_UPDATE_RESTART

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 of 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`

Table 1-3 (Cont.) Actions Enabled with INFRA_UPDATE_RESTART

- 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.

Table 1-3 (Cont.) Actions Enabled with INFRA_UPDATE_RESTART

- /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/

Action: System Maintenance with Data access / VM Control Privileges

System Maintenance with Data access / VM control Privileges, which is identified as INFRA_HYPERVISOR is intended to be used for diagnostics and maintenance scenarios where VM management on the host is required.

System Maintenance with Data access / VM Control Privileges action is intended to be used for diagnostics and maintenance scenarios where VM management on the host is required. Any data on the Guest VM is treated as customer data. As VM management involves the ability to access the VM data, this action potentially exposes data risk. However, this action does not give any access to the TDE keys of the data stored in cell 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, Mem) allocated.

> **Note:**
>
> System Maintenance with Data access/ VM control privileges prevents access to the infrastructure audit subsystem.

System Maintenance with Data Access / 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 host.
- Inherits the privileges from the "System Maintenance with Restart Privileges" action.

- Does not allow the operator to change the operating system parameters of the host or cell servers. However, this allows the operator to shut down the Guest VM and significantly change the configuration of the Guest VM.

Inheritance: All privileges of System Maintenance with Restart.

Table 1-4 Actions Enabled with INFRA_HYPERVISOR

Action Name	System Maintenance with Data access / VM control Privileges
Action Identifier	`INFRA_HYPERVISOR`

Table 1-4 (Cont.) Actions Enabled with INFRA_HYPERVISOR

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 – `lspci` – `imageinfo` – `imagehistory` – `ethtool` – `sosreport` – `reboot` – `sundiag.sh` – `ipmitool`

Table 1-4 (Cont.) Actions Enabled with INFRA_HYPERVISOR

- `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/`

Table 1-4 (Cont.) Actions Enabled with INFRA_HYPERVISOR

- **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/

Action: Full System Access

Full System Access, which is identified as INFRA_FULL permits access to the root accounts on the infrastructure components.

Full System Access action is intended to be used when full access to the Exadata Cloud@Customer infrastructure is required. Access is always limited to non-Guest VM layers. Full access here means the root privileges on every operating system instance in the Exadata Cloud@Customer system, other than Guest VMs.

> **Note:**
>
> Full System Access action permits the operator to become the root user on the infrastructure. This allows the operator to access and modify any memory register, any file, any device, and the audit subsystem.

Table 1-5 Actions Enabled with INFRA_FULL

Action Name	Full System Access
Action Identifier	`INFRA_FULL`
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`

Operator Access Control Actions: Autonomous VM Cluster

Besides Full System Access, use the limited access cages, Diagnostics and Maintenance, to view logs and perform service-related tasks.

- Action: Autonomous Exadata VM Cluster Full System Access
  Autonomous Exadata VM Cluster Full System Access, which is identified as `AVM_FULL` is to be used rarely if none of the lower access privileges can solve the issue.
- Action: Autonomous Exadata VM Cluster System Diagnostics
  Autonomous Exadata VM Cluster System Diagnostics, which is identified as `AVM_SYS_DIAG` is to be used to view logs.
- Action: Autonomous Exadata VM Cluster System Maintenance
  Autonomous Exadata VM Cluster System Maintenance, which is identified as `AVM_SYS_MAINT` is to be used to do service related changes.

Action: Autonomous Exadata VM Cluster Full System Access

Autonomous Exadata VM Cluster Full System Access, which is identified as `AVM_FULL` is to be used rarely if none of the lower access privileges can solve the issue.

Autonomous Exadata VM Cluster Full System Access action is intended to be used when full access to the Guest VMs is required. Full access here means the `root` privileges to the Guest VMs.

> **Note:**
>
> Full System Access action poses extreme availability and data exposure risks, which can be persistent. The action also provides ability to bar export of audit logs from the system.

Table 1-6 Actions Enabled with AVM_FULL

Action Name	Full System Access
Action Identifier	`AVM_FULL`
Operator Privileges	**Linux User Privilege**: Non-root **Can su to `root`**: yes **Chroot caged**: 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

Action: Autonomous Exadata VM Cluster System Diagnostics

Autonomous Exadata VM Cluster System Diagnostics, which is identified as `AVM_SYS_DIAG` is to be used to view logs.

Autonomous Exadata VM Cluster System Diagnostics action is intended to be used to view logs. A read-only profile, which allows non-privileged read-only access to the system. This action is used to determine possible issues with the operating system and the software running on it. Most of the non-root commands would be available in this mode. No privileged commands are available in this action. Operators are not allowed to `sudo` as `oracle`, `opc`, or `grid` but will have a white-listed set of commands they can run as that dynamic operator user.

Table 1-7 Actions Enabled with AVM_SYS_DIAG

Action Name	Autonomous Exadata VM Cluster System Diagnostics
Action Identifier	`AVM_SYS_DIAG`
Scope	Guest VM

Table 1-7 (Cont.) Actions Enabled with AVM_SYS_DIAG

Operator Privileges	**Linux User Privilege**: Non-root **Can su to root, oracle, opc, grid**: No **Chroot caged**: Yes **Directories Readable**: • `/proc` • `/sys` • `/tmp` • `/usr/lib64` • `/usr/bin` • `/usr/etc` • `/usr/include` • `/usr/lib` • `/usr/libexec` • `/usr/local` • `/usr/share` • `/opt/nessus` • `/usr/java` • `/var` • `/u01` • `/u02` • `/acfs01` • `/opt/oracle/dcs/log` • `/opt/oracle.ExaWatcher/archive` **Directories Writable**: `/tmp` **Restricted application log readable locations**: • `/etc/oratab` • `/opt/oracle/dcs/log` • `/opt/oracle/dcs/idempotencytoken_`*`jobid`*`_db` • `/u02/oracle.ahf` • `/u02/app/oracle/diag/rdbms` • `/opt/oracle.ExaWatcher/archive` **Config files readable**: • `/etc/oratab` • `/opt/oracle/dcs/idempotencytoken_`*`jobid`*`_db` • `/etc/hosts` **Egress network access**: None **Blacklisted operating system commands**: • `dd` • `kdumpctl` • `ipcrm` • `ipcmk` **List of commands executable**: `ls`, `cat`, and `tail` commands are supported in the locations where `opctl` dynamic user does not have read access

Limit Operator's Access to a Specific Customer-Approved Autonomous Container Database (ACD)

Restrict access to a specific ACD in an autonomous VM cluster in the diagnostics and maintenance cages.

Operators can specify if they need:

- SSH-only access to the autonomous VM cluster without SQL access to the ACDs. In this case, all SQL access to the ACDs will be blocked.
- SSH access to the autonomous VM cluster and SQL access to the ACDs. If they select both, they must select one or more ACDs.

The customer receives an approval request with the details that the operators are requesting access to. That way, the customer can be assured that the operators will have access to the right ACD. Once the customer approves the access request, the operators will get SQL access to only the ACDs they have been approved for.

The `Request Reason` attribute will display which ACDs the operators are requesting access to.

Action: Autonomous Exadata VM Cluster System Maintenance

Autonomous Exadata VM Cluster System Maintenance, which is identified as `AVM_SYS_MAINT` is to be used to do service related changes.

Autonomous Exadata VM Cluster System Maintenance action is intended to be used to do service related changes. This action is used to start and stop services, and run service health checks. Most of the service related commands are available in this mode. Operator will have access to the logs, but not allowed to `su` to `oracle`, `opc`, or `grid`.

Table 1-8 Actions Enabled with AVM_SYS_MAINT

Action Name	Autonomous Exadata VM Cluster System Maintenance
Action Identifier	`AVM_SYS_MAINT`
Scope	Guest VM

Table 1-8 (Cont.) Actions Enabled with AVM_SYS_MAINT

Operator Privileges	**Linux User Privilege**: Non-root **Can su to root, oracle, opc, grid**: No **Chroot caged**: Yes **Directories readable**: • /proc • /sys • /tmp • /usr/lib64 • /usr/bin • /usr/etc • /usr/include • /usr/lib • /usr/libexec • /usr/local • /usr/share • /opt/nessus • /usr/java • /var • /u01 • /u02 • /acfs01 • /opt/oracle/dcs/log • /opt/oracle.ExaWatcher/archive **Directories writable**: None **Restricted application log readable locations**: • /etc/oratab • /opt/oracle/dcs/log • /opt/oracle/dcs/idempotencytoken_*jobid*_db • /u02/oracle.ahf • /u02/app/oracle/diag/rdbms • /opt/oracle.ExaWatcher/archive **Config files readable**: • /etc/oratab • /etc/crontab • /opt/oracle/dcs/idempotencytoken_jobid_db • /etc/hosts **Egress network access**: None **Blacklisted operating system commands**: • dd • kdumpctl • ipcrm • ipcmk **Command aliases**: {"job_manager" : "/var/opt/oracle/adbd/apps/job_manager/job_manager.py", "backup_api" : "/var/opt/oracle/bkup_api/bkup_api", "service_driver" : "/var/opt/oracle/pylib/DBAAS/service_driver.py"} **List of commands executable**: Execution of service related commands are available as is but without switching to oracle or grid user. Execution of

Table 1-8 (Cont.) Actions Enabled with AVM_SYS_MAINT

scripts are supported through aliases without switching to `oracle` or `grid` user.

Refer to the examples provided below.

- `crsctl status resource adbd_archive_log_ilkzdar1`
- `crsctl check cluster -all`
- `crsctl stat res -t`
- `crsctl stat res ora.asm -t`
- `srvctl status service -db ilkzdar1_cdg1hw`
- `srvctl status database -d hr5zxn5l_cdg1bg`
- `srvctl status instance -i hr5zxn5l1 -d hr5zxn5l_cdg1bg`
- `tfactl blackout add -targettype host -timeout 2h -reason "Testing maint cage" -c`
- `dgmgrl`
- `asmcmd lsdsk -p`
  (Not allowed due to possible access to system console)
- `sysresv`
  (Not allowed due to options to remove ipc resources)
- SQL*Plus is restricted to selected queries. Switching to `oracle` or `grid` is not supported.

```
opctl_avm_maint_user01@atpd-exa-suzzm1:~$ execsql
ORACLE_UNQNAME is required.Check /etc/oratab
opctl_avm_maint_user01@atpd-exa-suzzm1:~$
```

```
opctl_avm_maint_user01@atpd-exa-suzzm1:~$ cat /etc/
oratab | grep -v '^\s*$\|^\s*\#'
ownwdhci_iad2pn:/u02/app/oracle/product/19.0.0.0/
db1916_0_wc139_cl_atksxzha_096_0105:Y +ASM1:/u02/app/
19.0.0.0/grid1916_0_wc140_cl_atksxzha_096_1334:Y
ay5sq1qf_iad2bp:/u02/app/oracle/product/19.0.0.0/
db1916_0_wc141_cl_atksxzha_096_0214:Y
dhb2br6k_iad22z:/u02/app/oracle/product/19.0.0.0/
db1916_0_wc142_cl_atksxzha_096_0416:Y
v001zhgm_iad2zs:/u02/app/oracle/product/19.0.0.0/
db1916_0_wc143_cl_atksxzha_096_0419:Y
drmgiyo6_iad277:/u02/app/oracle/product/19.0.0.0/
db1916_0_wc138_cl_atksxzha_096_0033:Y
fflilzax_iad2km:/u02/app/oracle/product/19.0.0.0/
db1916_0_wc145_cl_atksxzha_096_0411:Y
gytjhr9o_iad2tt:/u02/app/oracle/product/19.0.0.0/
db1916_0_wc144_cl_atksxzha_096_0411:Y
dqk29prh_iad2hc:/u02/app/oracle/product/19.0.0.0/
db1916_0_wc146_cl_atksxzha_096_0416:Y
utynogge_iad2p8:/u02/app/oracle/product/19.0.0.0/
db1916_0_wc147_cl_atksxzha_096_1213:Y
my06yvoe_iad2km:/u02/app/oracle/product/19.0.0.0/
db1916_0_wc149_cl_atksxzha_096_1218:Y
nfcteuzf_iad2j9:/u02/app/oracle/product/19.0.0.0/
db1916_0_wc148_cl_atksxzha_096_1216:Y
opctl_avm_maint_user01@atpd-exa-suzzm1:~$
```

```
opctl_avm_maint_user01@atpd-exa-suzzm1:~$ execsql
utynogge_iad2p8
```

```
SQL*Plus: Release 19.0.0.0.0 - Production on Thu Oct 6
06:32:11 2022 Version 19.16.0.1.0 Copyright (c) 1982,
```

Table 1-8 (Cont.) Actions Enabled with AVM_SYS_MAINT

	2020, Oracle. All rights reserved. Last Successful login time: Thu Oct 06 2022 06:29:09 +00:00 Connected to: Oracle Database 19c EE Extreme Perf Release 19.0.0.0.0 - Production Version 19.16.0.1.0 SQL> SELECT INSTANCE_NAME, STATUS, DATABASE_STATUS FROM V$INSTANCE; INSTANCE_NAME STATUS DATABASE_STATUS ---------------- ------------ ----------------- utynogge1 OPEN ACTIVE SQL> SELECT sys_context('userenv','instance_name') FROM dual; SYS_CONTEXT('USERENV','INSTANCE_NAME') -- ------------------------ utynogge1 SQL> !whoami SP2-0738: Restricted command "! (HOST)" not available SQL> !ls -ltr SP2-0738: Restricted command "! (HOST)" not available SQL> Scripts to be run as below with aliases. • /var/opt/oracle/adbd/apps/job_manager/job_manager.py --get_status adbd_archive_log_ilkzdar1 To be run as: job_manager --get_status adbd_archive_log_ilkzdar1 • /var/opt/oracle/pylib/DBAAS/service_driver.py --dbname=hr5zxn5l_cdg1bg To be run as: service_driver --dbname=hr5zxn5l_cdg1bg • /var/opt/oracle/bkup_api/bkup_api --dbname ilkzdar1 list jobs To be run as: backup_api --dbname ilkzdar1 list jobs

Limit Operator's Access to a Specific Customer-Approved Autonomous Container Database (ACD)

Restrict access to a specific ACD in an autonomous VM cluster in the diagnostics and maintenance cages.

Operators can specify if they need:

- SSH-only access to the autonomous VM cluster without SQL access to the ACDs. In this case, all SQL access to the ACDs will be blocked.
- SSH access to the autonomous VM cluster and SQL access to the ACDs. If they select both, they must select one or more ACDs.

The customer receives an approval request with the details that the operators are requesting access to. That way, the customer can be assured that the operators will have access to the right ACD. Once the customer approves the access request, the operators will get SQL access to only the ACDs they have been approved for.

The `Request Reason` attribute will display which ACDs the operators are requesting access to.

Operator Access Control Actions: Compute Cloud@Customer

Occasionally, authorized operators need to access resources to upgrade Compute Cloud@Customer, troubleshoot or help resolve an issue.

- Action: Compute Cloud@Customer Infrastructure Full Access
  Compute Cloud@Customer Infrastructure Full Access is identified as `CCC_SYS_ADMIN_FULL_ACCESS`.

Action: Compute Cloud@Customer Infrastructure Full Access

Compute Cloud@Customer Infrastructure Full Access is identified as `CCC_SYS_ADMIN_FULL_ACCESS`.

Table 1-9 Actions Enabled with CCC_SYS_ADMIN_FULL_ACCESS

Action Name	Full System Access
Action Identifier	`CCC_SYS_ADMIN_FULL_ACCESS`
Operator Privileges	**Linux User Privilege**: Non-root **Can su to `root`**: yes **Chroot caged**: No **Directories Readable**: All **Files Readable**: All **Directories Writeable**: All **Files Writeable**: All **List of commands executable**: All **Can su into:** `root` through `sudo` and execute all commands as the `root` user

Limits for Operator Access Control

Operator Access Control is a solution designed for auditing and compliance of Oracle access, not a general purpose compliance solution.

Operator Access Control only audits authorized users created in the context of an access request associated with an Oracle Operator Access control. The following is a list of examples of compliance audit and control actions that Operator Access Control does not address.

- Operator Access Control controls only the layers that Oracle owns. For example, Operator Access Control controls access to the physical Exadata Database Server and Exadata Storage Server.
- Operator Access Control does not control automation actions, including the actions that are run as `root`, or other high privileged automation users, including proxy-based automation access.
- Operator Access Control only offers controls at the level of defined Actions. The Actions themselves control access to an application at the operating system level.
- Operator Access Control is not a general auditing service. It only audits authorized users created in the context of an access request associated with an Operator Control.
- Operator Access Control only controls different layers in the Exadata Cloud@Customer systems. It doesn't offer controls on external entities of Oracle Cloud Infrastructure, such as switches, or other control plane software.

Customer Tenancy Job Roles for Operator Access Control

To establish operator access control, you set up access control policies, and establish user groups responsible for managing and monitoring access to your infrastructure.

- Operator Control Creation for Policy Administrators
  Policy administrators are the users who have permissions to set up operator control policies (called Operator Control).
- How Operator Access Requests Are Approved
  See how you can manage operator control approvals by setting up an Identity and Access Management (IAM) regime using Oracle Operator Access Control policies.
- How Operator Access is Audited
  Learn how logs are captured and how you can audit operator activities.

Operator Control Creation for Policy Administrators

Policy administrators are the users who have permissions to set up operator control policies (called Operator Control).

To create operator access control over your infrastructure, the first step is to create Operator Control policy administrators that develop and create the set of operator controls that you want to use for your tenancy fleet administrators.

Typically, when you create operator controls, you divide the Exadata infrastructure into access control groups based on multiple dimensions:

- Business Critical: Critical systems, less critical systems, development systems
- Security or Compliance: Systems with specific compliance needs and others
- User Groups: Which user groups (usually with fleet administrator role) you want to make responsible for a set of Exadata systems

Some examples of the user groups responsible for a set of Exadata systems:

- Vertical departments, whose applications depend on a set of Exadata systems.
- Systems shared across several departments, for which an IT department is responsible for administration.

Typically, you create compartments on your infrastructure based on criteria of criticality, regulatory compliance, and user group management, because compartments form the logical administrative boundaries in Oracle Cloud Infrastructure. Usually, each compartment has a user group that is granted management privileges on the compartment. For this reason, your Policy Administrator should create as many operator controls as there are compartments holding Exadata infrastructures.

In addition to specific operator controls for compartments, you must also create an additional policy, called `DEFAULT_OPERATOR_CONTROL`, that you can use to create new sets of Exadata systems in new compartments, for which you can create a different set of administrative users.

Related Topics

- Understanding Compartments

How Operator Access Requests Are Approved

See how you can manage operator control approvals by setting up an Identity and Access Management (IAM) regime using Oracle Operator Access Control policies.

Tenancy administrators for Operator Controls for an Oracle Cloud system are members of the operator control administrator group for Operator Controls. You receive operator control requests for access to Oracle Cloud Infrastructure. To support your regulatory compliance requirements, you can govern access to your infrastructure. You can specify that some actions are always in the status **auto-approved**, and specify that other actions must receive approval before Oracle can perform system maintenance operations in your tenancy. When you grant access to your system, that access is automatically limited to a standard time duration. You can also specify that operations must take place within a specific timeframe that you specify.

Example 1-1 Operator Controls for an Oracle Cloud Infrastructure IAM policy

You can set fine-grained controls on the permissions that you grant on your system.

For example, suppose you have two groups of Exadata Cloud systems in a compartment for which you are the tenancy administrator. As part of your IAM policy, you have created two separate sets of Exadata systems: The first group of systems has all Operator Policy configurations set to **pre-approved**, and the second group of systems has no Operator Policy configured to **pre-approved**.

You have also created two groups of users: `PRE_APPROVED_POLICY_USERS`, and `EXPLICIT_APPROVED_POLICY_USERS`. The Operator Control groups are identified by the tagging you provide: Namespace `optctl` has two Operator Control groups. One is identified by the tag `pre-approved-exacc`. The second group is identified by the tag `explicit-approved-exacc`. So, broadly, you have a set of servers where all actions are **pre-approved**, and a set of servers where no actions are **pre-approved**.

Next, In your compartment, suppose you have established a set of Exadata Cloud resources, each of which represents a level of actions permitted:

- `system_diag` specifies permissions for actions to diagnose any issue in the Exadata Cloud@Customer infrastructure layer, such as reading logs, running diagnostic and monitoring commands. You grant members of this policy the `INFRA_DIAG` action.
- `system_main` specifies permissions for actions to perform system diagnostics and maintenance, but also the option to restart the system. You grant members of this policy the `INFRA_UPDATE_RESTART` action, but the authorization is set **specify authorization**.
- `system_all` grants full system administration privileges permissions on the system, including unrestricted use of `sudo`. You grant members of this policy the `INFRA_FULL` action. You have no policy group created with this Action.

For the resources where you have set up the `system_diag` policy, you have marked as **pre-approved** all administration activities permitted by that action. You have specified that members of the group `PRE_APPROVED_POLICY_USERS` is granted access to use `system_diag` with **pre-approved** status in the tenancy

Next, suppose an Oracle operator with `PRE_APPROVED_POLICY_USERS` group membership requests access to a server, but requests the action `INFRA_UPDATE_RESTART` because a maintenance action requires a restart. The Oracle operator must still request access for the Action that permits an operator to restart the system as part of a maintenance action. You

grant access to the `system_main` policy, but all actions that require this policy access require approval.

Note that at any point in time, as an administrator, regardless of existing group memberships or approval, you can revoke the access to the operator. If you remove an Oracle operator from the group membership, then the operator will have no access to the system.

How Operator Access is Audited

Learn how logs are captured and how you can audit operator activities.

> **Note:**
>
> The audit logs are collected using the `auditd` subsystem in the Linux kernel. To add Operator Access Control rules to collect the logs, you must reboot the Exadata system after assigning an Operator Control the first time. You need not reboot the Exadata system for the subsequent assignments.

Extent of Audit Logs Captured

Operator Access Control service logs the actions performed by the operator on a controlled system. The logs are captured for two broad categories.

- Lifecycle event logs
- Command logs

The first being lifecycle events and the second being commands run by the operator on the target hosts.

Lifecycle Event Logs

Operator Access Control service captures login and logout events only for the Operator Access Control service authorized users and it does not capture automation login events.

Command Logs

Operator Access Control service captures all commands run by the authorized users on a shell. It captures the command input without any redaction and it does not capture the command output. It also captures all shell commands run using shell scripts.

For example, Operator Access Control service captures the following command:

```
netstat -an | grep 8080
```

Additionally, the commands run using the shell script `searchlog.sh` in this case are also captured.

```
./searchlog.sh -process "cellservice"
```

The command logs include commands run by a user even after an `su` has been done. For example, after logging in, if the authorized user *`auth_user_123`* runs the following commands, then Operator Access Control service captures all of these commands.

```
su - celladmin
tail -n 10 /var/log/messages
```

Keyboard Logging

Additionally, the command logs can also be captured in the keyboard log format. Keyboard logging captures every keystroke the operators type on their computers. It does not serve a lot of practical purposes to capture keyboard logging, however, there are cases where regulatory requirements need to capture keystroke logging.

Items Not Logged

Operator Access Control service does not log automation commands or lifecycle events. While this service logs all commands issued to the shell either directly or through invocation of shell scripts, it does not log actions performed by the binary executables. Hence if an operator logs into the cell server and then gets into a `cellcli` shell, the logs will be limited to capturing the `cellcli` shell commands alone. Operator Access Control service does not log commands run inside the `cellcli`.

Format of Audit Logs

The audit logs are formatted as JSON text. Audit logs are categorized into two parts — the raw data and the interpreted data. The raw data is not comprehensible outside the context of a Linux machine where the log was captured. For example, the raw data does not refer to Linux user names, rather it refers to internal identifiers instead. Mapping the identifier to user can only be done on the Linux machine where the log was captured.

In addition to the interpretation, the format also sets the context by providing the "access request ID" in the logs.

Lifecycle Event Logs

The following two examples give the format of the audit log for lifecycle events. The examples show a **login** and a **logout** event. The username used for this login is "USERNAME".

Example 1-2 Login Event Log

```
{
"layer": "CPS",
"req_auth_id": "1",
"srchost": "dhcp-10-191-235-63.vpn.example.com",
"res": "success'",
"desthost": "10.191.235.63",
"pid": "89736",
"tty": "/dev/pts/2",
"host": "scaqae08dv0605m",
"time": "Thu Oct 29 03:20:22 2020",
"raw_data": "type=USER_LOGIN msg=audit(10/29/2020 03:20:22.091:10777414) :
pid=89736 uid=root auid=USERNAME ses=75141 msg='op=login id=USERNAME
exe=/usr/sbin/sshd hostname=dhcp-10-191-235-63.vpn.example.com
addr=10.191.235.63 terminal=/dev/pts/2 res=success' \n",
"event": "login",
```

```
"loginid": "USERNAME"
}
```

Example 1-3 Logout Event Log

```
{
"layer": "CPS",
"req_auth_id": "1",
"srchost": "dhcp-10-191-235-63.vpn.example.com",
"res": "success'",
"desthost": "10.191.235.63",
"pid": "90456",
"tty": "ssh",
"host": "scaqae08dv0605m",
"time": "Thu Oct 29 03:20:35 2020",
"raw_data": "type=USER_LOGOUT msg=audit(10/29/2020
03:20:35.855:10777438) : pid=90456 uid=root auid=USERNAME ses=75142
msg='op=login id=USERNAME exe=/usr/sbin/sshd
hostname=dhcp-10-191-235-63.vpn.example.com addr=10.191.235.63
terminal=ssh res=success' \n",
"event": "logout",
"loginid": "USERNAME"
}
```

Command Logs

The command logs are more elaborate. They provide information about the command, the parameters of the command the effective user executing the command. The commands also have a hierarchy in the sense that a shell script execution will first have a `bash -c` logged and then the script commands.

Example 1-4 Command Execution

```
{
"layer": "CPS",
"req_auth_id": "1",
"title": "ls\u0000/",
"raw_data": "type=PROCTITLE msg=audit(10/29/2020
03:20:29.418:10777424) : proctitle=ls / \ntype=PATH
msg=audit(10/29/2020 03:20:29.418:10777424) : item=1 name=/lib64/ld-
linux-x86-64.so.2 inode=1182648 dev=f9:00 mode=file,755 ouid=root
ogid=root rdev=00:00 nametype=NORMAL \ntype=PATH msg=audit(10/29/2020
03:20:29.418:10777424) : item=0 name=/usr/bin/ls inode=1189225
dev=f9:00 mode=file,755 ouid=root ogid=root rdev=00:00 nametype=NORMAL
\ntype=CWD msg=audit(10/29/2020 03:20:29.418:10777424) : cwd=/
\ntype=EXECVE msg=audit(10/29/2020 03:20:29.418:10777424) : argc=2
a0=ls a1=/ \ntype=SYSCALL msg=audit(10/29/2020
03:20:29.418:10777424) : arch=x86_64 syscall=execve success=yes exit=0
a0=0xfff6d0 a1=0xff42d0 a2=0xfff960 a3=0x7ffc1dd337e0 items=2
ppid=90474 pid=90764 auid=USERNAME uid=USERNAME gid=USERNAMg
euid=USERNAME suid=USERNAME fsuid=USERNAME egid=USERNAMg sgid=USERNAMg
fsgid=USERNAMg tty=pts2 ses=75141 comm=ls exe=/usr/bin/ls key=(null)
\n",
"args": [],
```

```
"rec_id": "10777424",
"tty": "pts2",
"host": "scaqae08dv0605m",
"time": "Thu Oct 29 03:20:29 2020",
"loginid": "USERNAME"
}
```


The field title provides the command that was executed. The raw data provides much more information.

Frequency of Collection

Operator Access Control service collects the logs as and when the events happen, timestamps, and pushes the logs to the logging service periodically. It attempts to push the logs in every 30 second intervals.

Accessing Audit Logs

You can access audit logs through the logging service. For more information, see Logging Overview.

The JSON shown in section 2 is available in the logging service. Use your tenancy to access the logging service. The logs are posted to the compartment on which the Operator Control was created. The logs are tagged to the Operator Control.

Retention Policies of Audit Logs

The audit logs are retained in the user tenancy and therefore Operator Access Control service does not control the lifetime of audit logs. You can control control the duration of retention period. However, if this service could not push the logs to user tenancy, then it will try to retain the logs to the extent allowed by Exadata configurations. The retention period is considerable, that is, running into days or longer.

Forwarding Operator Access Control Audit Logs to SIEM Systems

You can choose to forward Operator Access Control audit logs directly from Exadata Cloud@Customer to the security information and event management (SIEM) systems in your data center.

To improve your security management, you can transmit audit logs to the OCI Logging service and to the SIEM systems in your data centers. To transmit these audit logs to SIEM systems, syslog over TCP is used.

- Deploying a Syslog Server in Your Data Center
  To receive audit logs from Exadata Cloud@Customer, deploy a Syslog server in your data center. The Syslog server can be of your choice. Most Linux systems ship with `rsyslog`.
- Example Syslog Server Configuration
  To see how you can configure a Syslog server of your choice, use this example.
- Testing Connectivity Between CPS and the Syslog Server
  Ensure that you have provided a valid IP address or host name for the Syslog server.

- Example of Audit Logs
  As an administrator, see examples of the audit logs received securely from the Control Plane Server.

Deploying a Syslog Server in Your Data Center

To receive audit logs from Exadata Cloud@Customer, deploy a Syslog server in your data center. The Syslog server can be of your choice. Most Linux systems ship with `rsyslog`.

You can forward audit logs to only one Syslog server for each target Exadata Cloud@Customer system. Oracle supports secure communication only, and uses TLS for transmission security. The Control Plane Server connects with the Syslog server, and delivers all audit logs over secure TCP. To establish trust between the Control Plane Server and the Syslog server, use a PEM format Syslog server CA certificate file. The file extension must be `.pem`, `.cer`, or `.crt`. For more information about configuration, see Example Syslog Server Configuration.

The log contains elements already described in the chapter Managing and Searching Logs with Operator Access Control. The format is ensured to be compatible with `syslog` and `audit-d` log parsers. See the example audit log.

Sending audit logs to SIEM systems is on a best effort basis. While the Control Plane Server retries sending logs on network failures, packets can drop silently on thresholds. In such cases, the logs surfacing through the OCI Logging service are the reference.

> **Note:**
>
> To forward audit logs, you must assign at least one Operator Control to the Exadata Cloud@Customer system indefinitely (ALWAYS ASSIGNED).

Related Topics

- Assign Operator Control
  To assign policies to control human access to infrastructures and databases, complete this procedure.

Example Syslog Server Configuration

To see how you can configure a Syslog server of your choice, use this example.

Before you attempt to configure the Syslog server, you must be prepared to do the following:

1. Open a network port for receiving remote logs.

> **Note:**
>
> Egress rules for the Syslog server should be open for Syslog Port. For Example, if the 6514 port is used for Syslog, then the Egress Security rule should be in place to allow traffic to reach Syslog from Autonomous VM Cluster.

2. Enable encryption on the Syslog server for remote communication.
3. (Optional) Generate and transfer a root certificate for secure communication.

> **Note:**
>
> The example given below is for configuring a `rsyslog` server (v 8.24) on a machine with Oracle Linux 7. The configuration is generally available at `/etc/rsyslog.conf`. Only the relevant sections are covered in this example.

For this example, the listening port is `10514`. There are multiple sources available on the Internet to assist you with encrypting Syslog traffic. A good reference is Encrypting Syslog Traffic with TLS (SSL) [short version] — rsyslog 8.18.0.master documentation.

```
# rsyslog configuration file (8.24.0 - /etc/rsyslog.conf - Oracle Linux 7)
# For more information see /usr/share/doc/rsyslog-*/rsyslog_conf.html
# If you experience problems, then see http://www.rsyslog.com/doc/
troubleshoot.html

#### MODULES $ModLoad imuxsock # provides support for local system logging
(e.g. via logger command)# Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 10514

...# certificate files
$DefaultNetstreamDriverCAFile /var/gnutls1/ca.pem
$DefaultNetstreamDriverCertFile /var/gnutls1/cert.pem
$DefaultNetstreamDriverKeyFile /var/gnutls1/key.pem$ModLoad imtcp # load TCP
listener$InputTCPServerStreamDriverMode 1 # run driver in TLS-only mode
$InputTCPServerStreamDriverAuthMode anon # client is NOT authenticated
#$InputTCPServerStreamDriverAuthMode x509/name # client is NOT authenticated
$InputTCPServerRun 10514 # start up listener at port 10514
...
```

Testing Connectivity Between CPS and the Syslog Server

Ensure that you have provided a valid IP address or host name for the Syslog server.

The Syslog server must be able to receive logs from a Syslog client, and it must be reachable from Exadata Cloud@Customer. To confirm your configuration, use this procedure.

1. To validate that the Syslog server can receive logs, run the `nc` command towards the Syslog server and Syslog port from any host in your network having access to the Syslog server.

   ```
   nc syslog server host syslog port
   ```

2. To ensure the path between Exadata Cloud@Customer and the Syslog server is valid, ping the Exadata Cloud@Customer Control Plane Server IP address. To obtain the Control Plane Server (CPS) IP address, contact your network administrator.

Related Topics

- Assign Operator Control
  To assign policies to control human access to infrastructures and databases, complete this procedure.

Example of Audit Logs

As an administrator, see examples of the audit logs received securely from the Control Plane Server.

When you transmit logs to the Syslog server, many headers and the JSON formatting are omitted. The following examples show the nature of data shipped through Syslog.

Example 1-5 1

```
Apr 12 07:38:22 scaqar05dv0511m opctl: type=USER_LOGIN
msg=audit(04/12/2021 07:38:05.752:1742859) :
pid=65327
uid=root
auid=830916abb78e4157b9e45b641e34fcf6 ses=32770
msg='op=login id=830916abb78e4157b9e45b641e34fcf6
exe=/usr/sbin/sshd
hostname=localhost.localdomain
addr=127.0.0.1
terminal=/dev/pts/3 res=success'
```

Example 1-6 2

```
Apr 12 07:38:22 scaqar05dv0511m opctl: type=USER_LOGOUT
msg=audit(04/12/2021 07:38:08.802:1742867) :
pid=65327
uid=root
auid=830916abb78e4157b9e45b641e34fcf6
ses=32770
msg='op=login
id=830916abb78e4157b9e45b641e34fcf6 exe=/usr/sbin/sshd
hostname=?
addr=?
terminal=/dev/pts/3 res=success'
```

Related Topics

- Managing and Searching Logs with Operator Access Control
  Learn to enable logs to view the list of Operator Controls created and in use in a compartment. Also, to monitor operator activities in a cage.

2

Managing Infrastructure Access with Operator Access Control

Learn how to create, assign, approve, revoke, and control other infrastructure access operations on Oracle Cloud@Customer Exadata infrastructure and Compute Cloud@Customer infrastructure.

- Create Operator Control
  To create an Operator Control using the Oracle Cloud Console, you open the console in a browser, select **Create Operator Control**, and specify the compartment, user, and permissions that you want to grant.
- View Operator Control Details
  To view the details of an Operator Control, use this procedure.
- Run Assignment Validation
  To validate the Operator Control assignment, use this procedure.
- Assign Operator Control
  To assign policies to control human access to infrastructures and databases, complete this procedure.
- Enable Notifications
  Learn to enable notifications for approvers when an access request is raised.
- Edit Operator Control
  To change the compartment, user, permissions, and other control settings for an Operator Control, you can use the Edit Operator Control option.
- Remove Operator Control
  The contents of the Operator Controls are visible even after you remove them. However, you cannot edit or assign them again.
- Add Tags to Operator Control
  If you want to make an Operator Control easier to find, or to track resources used for specific purposes, you can add tags.
- Update Operator Control Assignment
  To change the duration of an Operator Control assignment, edit the Operator Control configuration.
- Remove Operator Control Assignment
  To remove an Operator Control assignment, complete this procedure on the system where you want to remove the assignment.
- Filter Operator Control Assignments by State
  To review the assignment states, you can filter the Assignments based on the workflow state of the request.
- Filter Operator Control by Compartment
  To find Operator Controls specific to an individual compartment, you can use List Scope to filter Operator Controls by compartment.

- Filter Operator Control by State
  Filter Operator Controls by selecting a state from the list of states of the operator control action.
- Filter Operator Control by Resource Type
  To filter Operator Controls by resource types, complete this procedure.
- Move Operator Control to Another Compartment
  To relocate an Operator Control to another compartment, use this procedure.
- Move Operator Control Assignment to Another Compartment
  To relocate an Operator Control Assignment to another compartment, use this procedure.

Create Operator Control

To create an Operator Control using the Oracle Cloud Console, you open the console in a browser, select **Create Operator Control**, and specify the compartment, user, and permissions that you want to grant.

You specify operator controls to define operator attributes of Oracle operators who can access your Oracle Cloud Infrastructure system, what access privileges they are granted, and which users and groups on your compartment are empowered to grant or revoke Oracle operator access to the infrastructure on which the compartment resides.

Before you can create an Operator Control, you must have an operator attribute account that grants you privileges to create Operator Controls on the tenancy and compartment that you want to manage, and you must have created administrative users and groups on your compartment that have the privilege to grant or revoke access requests for infrastructure maintenance.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. Click **Create Operator Control**.
   The Create Operator Control window opens.
4. In the **Compartment** field, select a compartment where you want to create the Operator Control.
   To find the compartment in the tenancy, you can search for a string in the compartment name. For example, if there are three compartments in the tenancy with `Dbaas-region` in the compartment name, then entering the search phrase "`DBaaS-region`" returns all three of those compartments.
5. In the **Operator Control Name** field, enter an Operator Control name to which you want to grant access to your compartment. For the Description field that is associated with that Operator Control name, provide information that explains the purpose of this control, and other access information that you require for regulatory compliance.
6. In the **Resource Type** section, choose resource type: **Exadata Infrastructure**, **Autonomous Exadata VM Cluster**, or **Compute Infrastructure**.
7. In the **Deployment Platform** section, you can select either **Cloud@Customer** or **Oracle Cloud** if you have chosen the resource type **Autonomous Exadata VM Cluster**. If you have chosen **Exadata Infrastructure** or **Compute Infrastructure** as the resource type, then **Cloud@Customer** is the only option available.

8. In the Approval Requirements section, provide information regarding the access control that you want to grant to the operator:
   - **Choose Pre-Approval Mode**: Select one of the following:
     - **PRE-APPROVE ALL ACTIONS** Select this mode to auto-approve access requests to Oracle operators to perform system maintenance operations. You can revoke this approval mode at any time.
     - **SELECT ACTIONS TO PRE-APPROVE** Select this mode to choose particular actions that you want to grant automatically. If you select this option, then the Pre-Approved Actions list appears. To view and select actions from the Pre-Approved Actions list, click the arrow keys on the right side of the field, and select the actions that you want to approve. Note that each operator action has a risk profile associated with it, which informs you if your system can encounter a performance impact during a maintenance operation.
   - **Requires Second approval:** Choose **Yes** if you want a second approval for the Access Request using this Operator Control.

   > **Note:**
   >
   > - A banner is displayed on the Access Request details page indicating that this Access Request requires 2 approvals to move to the **Approved** state.
   > - A banner is displayed if there are any pending approvals.
   > - If any of the two users reject the Access Request, then the Access Request is moved to the **Rejected** state.
   > - If one user approves the Access Request now (**Approve Now**) and the other user approves it for later (**Approve Later**), then **Approve Later** takes precedence.

9. In the field **Groups allowed to approve access to resources governed by this Operator Control**, click the arrow keys on the right side of the field to add groups whose members you want to be able to approve or revoke Oracle operator maintenance requests on your system. Approval groups are not compatible with Identity Domains.

   Select **Use IAM Policy** to permit the Operator Access Control service to authorize users based on IAM Policy rules to approve any access requests. You must select USE IAM Policy to support Identity Domains.

   Prior to choosing the **Use IAM Policy** option, you must have written a policy to grant approval permissions to access requests for the groups in different identity domains.

   For more information, see Managing Access to Resources.

10. (Optional) In the field **Message to Operator**, you can choose to enter a message that is displayed to the Oracle operator at the time of an access request. Use this option to provide information to the Oracle operator. For example, you can specify that an Oracle operator must perform an action before an access request is approved, or perform an action before beginning a pre-approved operation.

11. (Optional) To specify additional features, select **Show Advanced Options**. In the **Tag Namespace** field, consider adding a **tag namespace** (an identifying text string applied to a set of compartments), or tagging the control with an existing tag namespace.
    For more information, see Overview of Tagging.

12. When you have completed and reviewed your selections, click **Create**. The Operator Control is created.
13. **Save as Stack:**
    Stack is a collection of Oracle Cloud Infrastructure resources corresponding to a given Terraform configuration. Each stack resides in the compartment you specify, in a single region; however, resources on a given stack can be deployed across multiple regions. For more information, see stack.

    While creating Operator Control, you can save resource configuration as a stack. Use the stack to configure and manage the resource through the Resource Manager service. For requirements and recommendations for Terraform configurations used with Resource Manager, see Resource Manager.

View Operator Control Details

To view the details of an Operator Control, use this procedure.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. From the list of Operator Controls, click the name of the Operator Control that you want to edit.
4. In the **Operator Control Information** section, you can verify the **Resource Type** for which you have created the Operator Control.
   You can also verify if notifications have been configured or not in the **Notifications Information** section. If you have not configured notifications, then a warning banner is displayed.
   a. Click **Configure**.
      Configure notifications dialog is displayed.
   b. In the **Configure notifications** dialog, enter valid email addresses, and then click **Create**.

Run Assignment Validation

To validate the Operator Control assignment, use this procedure.

Assignment validation performs the following actions:

- Validates Syslog connectivity if Syslog is configured.
- Checks for the maintenance window.
- Creates a test access request for the assigned resource and runs a set of test commands on it. Additionally, you will be able to validate the approval workflow. Also, you can verify if you received a notification when the test access request was created. This helps you verify the Notifications setup.
- Closes the test access request created earlier upon the successful run of the test commands. And, you will be able to download the audit log report for the test access request.
- Displays whether the assignment validation has succeeded or failed with an appropriate message

During this process, a test access request is created with a default action based on the resource type. You can also have an option to choose a different action.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. Click **Assignments**.
4. In the list of Assignments, find the assignment you want to run assignment validation.
5. On the Assignment details page, click the **Assignment validation** tab.
   The **Assignment validation** and **Stages Completed** sections include details of the assignment validation run.
6. Click **Run assignment validation**.
7. On the Run assignment validation dialog, select an action.
   Operator Access Control creates a cage for the action selected.
8. Click **Run assignment validation**.
9. Upon clicking **Run assignment validation**, Operator Access Control will prompt you to approve the access request.
10. Click the link on the banner and approve the access request.
    Upon completing assignment validation, Operator Access Control displays an appropriate message indicating whether the assignment validation has succeeded or failed.

Assign Operator Control

To assign policies to control human access to infrastructures and databases, complete this procedure.

> **Note:**
>
> Ensure that the person or entity doing the assignment has the privilege to use the Exadata infrastructures. If not, then create the following IAM policy:
>
> ```
> use exadata-infrastructures in tenancy or compartment
> ```

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. From the list of Operator Controls, click the name of the Operator Control that you want to assign.
4. In the Operator Control details page, click **Assign Operator Control**.
5. Under **Assignment Compartment**, select the compartment where you want the assignment resource to reside.
6. The **Operator Control Information** section displays the name and OCID of the Operator Control and the Resource Type and Deployment Platform for which this Operator Control was created. Based on the Resource Type, the corresponding resources are listed for selection in the **Assignment Information** section.

7. In the Assign Operator Control page, under **Assignment Information**, make the following selections:
   a. Select an Exadata Cloud@Customer system in the compartment. If the Exadata Cloud@Customer system is not in the current compartment, then click **Change Compartment** to choose the compartment where the Exadata Cloud@Customer system resides.
   b. Choose the duration for which you want to assign the operator control access:
      i. (Default) **ALWAYS ASSIGNED** - Operator Control is assigned to the system indefinitely.

      > **Note:**
      >
      > You must assign at least one Operator Control to the Exadata Cloud@Customer system indefinitely.

      ii. **ASSIGNED FOR A SPECIFIED DURATION** - Operator Control is assigned to the system for a specific period.
      From the calendar controls, select the time period in which you want to assign the access.

      > **Note:**
      >
      > You can assign an Operator Control for a specific duration only when you have assigned at least one Operator Control to the Exadata Cloud@Customer system indefinitely (**ALWAYS ASSIGNED**).

8. (Optional) In the **DESCRIPTION** field, enter a description of the operator control access.
9. (Optional) In the Audit Log Forwarding section enter the following details.

   > **Note:**
   >
   > Audit Log forwarding is available only when you choose the **ALWAYS ASSIGNED** option.

   a. Select the **Forward audit logs** check box.
   b. Enter the IP address or hostname of the Syslog server in the **Syslog server address (IP or host)** field.
   c. Enter the port number in the **Syslog server port** field.
   d. (Optional) Choose a certificate authority (CA) certificate file, or paste the content of the certificate file.

> **Note:**
>
> If the certificate is not provided, then the Syslog server should offer a well-known certificate for communication.

10. Select the **Auto-approve access requests during the maintenance window** check box.
While Exadata Cloud@Customer infrastructure is being patched, there may be a delay in approving your access request. Selecting this option helps you get automatic approval during Exadata Cloud@Customer scheduled maintenance window.

    When Oracle Cloud Operations raise an access request, Operator Access Control needs to check if the infrastructure is in maintenance mode or not to auto-approve the request.

    To fetch the current lifecycle state of the infrastructure, create the following policy:

    ```
    allow any-user to inspect exadata-infrastructures in tenancy where ALL
    { request.principal.type='opctloperatorcontrol' }
    ```

    To fetch the current lifecycle state of Autonomous VM Clusters for Cloud@Customer, create the following policies:

    ```
    allow any-user to inspect autonomous-vmclusters in tenancy where ALL
    { request.principal.type='opctloperatorcontrol' }
    ```

    ```
    allow any-user to inspect autonomous-container-databases in tenancy where
    ALL { request.principal.type='opctloperatorcontrol' }
    ```

    To fetch the current lifecycle state of Autonomous VM Cluster for Public Cloud, create the following policies:

    ```
    allow any-user to inspect cloud-autonomous-vmclusters in tenancy where
    ALL { request.principal.type='opctloperatorcontrol' }
    ```

    ```
    allow any-user to inspect autonomous-container-databases in tenancy where
    ALL { request.principal.type='opctloperatorcontrol' }
    ```

    To fetch the current lifecycle state of the Compute Cloud@Customer infrastructure, create the following policy:

    ```
    allow any-user to inspect ccc-infrastructures in tenancy where ALL
    { request.principal.type='opctloperatorcontrol' }
    ```

11. Click **Assign**. The assignment is listed on the compartment assignment list.
While the assignment is pending, the console displays the state of the assignment as **Updating**. When the operator is assigned to the access request, the state changes to **Accepted**, or **Assigned Failed**. If there is an issue with the access request, then a circle with an exclamation point (!) is displayed next to the assignment state. Click the icon to display details about the issue, and contact Oracle Support.

Enable Notifications

Learn to enable notifications for approvers when an access request is raised.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. From the list of Operator Controls, click the name of the Operator Control that you want to edit.
4. In the **Notification Information** section, click **Configure**.
5. In the **Configure Notifications** page, enter valid email IDs and then click **Create**. Operator Access Control service initiates a call to Notifications Service and Events Service to create Topic, Subscriptions, and Events. When they are being created, you will see an intermittent state of the notification creation process. When the configuration is complete, you will see a message stating that the notification has been created.

By default, the Operator Access Control system sets up event notifications for the following events:

- Access Request Created
- Access Request Approved
- Access Request Expired

You can manually update events or notifications settings any time later. Follow the steps outlined in the following topics to manually configure notifications.

For more information about managing rules, see Managing Rules for Events.

For more information about notification tasks, see Managing Topics and Subscriptions

Edit Operator Control

To change the compartment, user, permissions, and other control settings for an Operator Control, you can use the Edit Operator Control option.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. From the list of Operator Controls, click the name of the Operator Control that you want to edit.
4. In the Operator Control details page, click **Edit Operator Control**.
5. In the Edit Operator Control page, you can edit the following:
    a. Enter a name in the **OPERATOR CONTROL** field.
    b. Enter descriptive text in the **DESCRIPTION** field.
    c. You cannot change the **Resource Type** and **Deployment Platform** after creating an Operator Control.
    d. **CHOOSE PRE-APPROVAL MODE**: Select one of the following:

- **PRE-APPROVE ALL ACTIONS** Select this mode to automatically approve all access requests from Oracle operators to perform system maintenance operations.

  You can revoke this approval mode at any time.

- **SELECT ACTIONS TO PRE-APPROVE** Select this mode to choose particular actions for which you want to grant operator access automatically.

  If you select this option, then the Pre-Approved Actions list appears. To view and select actions from the Pre-Approved Actions list, click the arrow keys on the right side of the field, and select the actions that you want to approve.

  Note that each operator action has a risk profile associated with it, which informs you if your system can encounter a performance impact during a maintenance operation.

> **Note:**
>
> Under **List Scope**, you can select the compartment to which the control applies.

e. **Requires Second approval:** Choose **Yes** if you want a second approval for the Access Request using this Operator Control.

> **Note:**
>
> - A banner is displayed on the Access Request details page indicating that this Access Request requires 2 approvals to move to the **Approved** state.
> - A banner is displayed if there are any pending approvals.
> - If any of the two users reject the Access Request, then the Access Request is moved to the **Rejected** state.
> - If one user approves the Access Request now (**Approve Now**) and the other user approves it for later (**Approve Later**), then **Approve Later** takes precedence.

f. In the field **Groups allowed to approve access to resources governed by this Operator Control**, click the arrow keys on the right side of the field to add groups whose members you want to be able to approve or revoke Oracle operator maintenance requests on your system.

g. (Optional) In the field **Message to Operator**, you can choose to enter a message that is displayed to the Oracle operator at the time that the operator is engaged with an access request.
Use this option to provide information to the Oracle operator. For example, you can specify that an Oracle operator must perform an action before an access request is approved, or perform an action before beginning a preapproved operation.

h. Click **Save**.

Remove Operator Control

The contents of the Operator Controls are visible even after you remove them. However, you cannot edit or assign them again.

> **Note:**
>
> You cannot remove an indefinite assignment (**ALWAYS ASSIGNED**) if there exist one or more windowed assignments (**ASSIGNED FOR A SPECIFIED DURATION**).

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. From the list of Operator Controls, select the one that you want to remove.

   You can also select more than one Operator Control.
4. Click **Remove**.

   You can also choose to click the name of the Operator Control, and then on the details page, click **Remove Operator Control**.
5. In the Remove Operator Control dialog:
   a. Enter the reason for removint the control in the **REMOVAL COMMENTS** field.
   b. Type the word `REMOVE` to confirm.
   c. Click **Remove**.

Add Tags to Operator Control

If you want to make an Operator Control easier to find, or to track resources used for specific purposes, you can add tags.

Applying tags to resources is optional. If you have permissions to create a resource, then you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace. For more information about tagging, see Resource Tags. If you are not sure if you should apply tags, then skip this option (you can apply tags later), or ask your administrator.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. From the list of Operator Controls, select the operator control for which you want to add tags.
4. In the Operator Control details page, click **Add Tags**.

Update Operator Control Assignment

To change the duration of an Operator Control assignment, edit the Operator Control configuration.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. From the list of Operator Controls, click the name of the Operator Control for which you want to update the assignment.
4. In the Operator Control details page, under **Assignments**, find the assignment that you want to update, click the actions button (three dots), and then select **Update Assignment**.
5. In the Update Operator Control Assignment page, you can choose an assignment from one of the following options:
   a. (Default) **ALWAYS ASSIGNED** - Operator Control is assigned to the system indefinitely.

      > **Note:**
      >
      > You must assign at least one Operator Control to the Exadata Cloud@Customer system indefinitely.

   b. **ASSIGNED FOR A SPECIFIED DURATION** - Operator Control is assigned to the system for a specific period.
      From the calendar controls, select the time period for the access.

      > **Note:**
      >
      > You can assign an Operator Control for a specific duration only when you have assigned at least one Operator Control to the Exadata Cloud@Customer system indefinitely (**ALWAYS ASSIGNED**).

   c. (Optional) In the **DESCRIPTION** field, enter a description describing the purpose for the access control, or reason for changing it.
   d. (Optional) In the Audit Log Forwarding section enter the following details.

      > **Note:**
      >
      > Audit logs and Hypervisor logs can be forwarded only when **ALWAYS ASSIGNED** is selected.

      i. Select the **Audit logs** checkbox to forward audit logs.
      ii. Select the **Hypervisor** logs checkbox to forward hypervisor logs. Hypervisor logs provide you the information about the activity that is happening on your hypervisor hosts.

iii. Enter the IP address or hostname of the Syslog server in the **Syslog server address (IP or host)** field.

iv. Enter the port number in the **Syslog server port** field.

v. (Optional) Choose a certificate authority (CA) certificate file, or paste the content of the certificate file.

> **Note:**
>
> If the certificate is not provided, then the Syslog server should offer a well-known certificate for communication.

e. Click **Update**.

Remove Operator Control Assignment

To remove an Operator Control assignment, complete this procedure on the system where you want to remove the assignment.

> **Caution:**
>
> After you remove an Operator Control assignment, the system may be fully accessible to Oracle operators. If you want to continue to maintain more direct control, then consider updating operator controls.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. From the list of Operator Controls, click the name of the Operator Control for which you want to update the assignment.
4. In the Operator Control details page, under **Assignments**, for the assignment that you want to update, click **Actions**, and then select **Remove Assignment**.
5. In the Remove Operator Control Assignment dialog, type the word `REMOVE` to confirm your choice.
6. Click **Remove**.

Filter Operator Control Assignments by State

To review the assignment states, you can filter the Assignments based on the workflow state of the request.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. Click **Assignments**.
4. Under **Filters**, select an Assignment state from the list.

You can perform actions based on the state of the Assignment.

Table 2-1 Actions on Assignments

Assignments	Allowed Action
Assignment in progress	No actions.
Assigned	**Update**, **Move**, or **Remove**.
Failed to assign	**Update**, **Move**, or **Remove**.
Update in progress	No actions.
Delete in progress	No actions.
Failed to delete	**Update**, **Move**, or **Remove**.
Deleted	**Update**, **Move**, or **Remove**.

Filter Operator Control by Compartment

To find Operator Controls specific to an individual compartment, you can use List Scope to filter Operator Controls by compartment.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. Under **List Scope**, select a compartment from the list.

Filter Operator Control by State

Filter Operator Controls by selecting a state from the list of states of the operator control action.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. Under **Filters**, select a state from the list.
   Operator Controls:
   - Any state
   - Created
   - Assigned
   - Unassigned
   - Deleted

   Assignments:
   - Any state
   - Assignment in progress
   - Assigned
   - Failed to assign
   - Update in progress
   - Delete in progress

- Failed to delete
- Deleted

Access Requests:

- Any state
- Raised
- In Review
- Approved for future
- Approved
- Pre-Approved
- Extension Requested
- Rejected
- Revoked
- Completed
- Expired
- In-Process
- Failed to close

Filter Operator Control by Resource Type

To filter Operator Controls by resource types, complete this procedure.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. Under **Filters**, select a **Resource Type** from the list.

Move Operator Control to Another Compartment

To relocate an Operator Control to another compartment, use this procedure.

Moving an Operator Control to a different compartment will not affect associated resources. They remain in their current compartments.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. Click **Operator Controls**.
4. In the list of Operator Controls, click the name of the Operator Control that you want to move.
5. In the Operator Control details page, click **Move Resource**.
6. In the Move Resource to a Different Compartment dialog, choose a new compartment, and then click **Move Resource**.

Move Operator Control Assignment to Another Compartment

To relocate an Operator Control Assignment to another compartment, use this procedure.

Moving an Operator Control Assignment to a different compartment will not affect associated resources. They remain in their current compartments.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. Click **Assignments**.
4. In the list of Operator Control Assignments, click the Actions icon (three dots) for the Operator Control that you want to move, and then click **Move Resource**.
5. In the Move Resource to a Different Compartment dialog, choose a new compartment, and then click **Move Resource**.

3

Managing Access Requests with Operator Access Control

Learn how to manage Oracle operator access requests to your Oracle Cloud@Customer Infrastructure and Compute Cloud@Customer dedicated infrastructure using Operator Access Control.

- State of an Access Request
  Review the list of states in which an Oracle operator access request can be listed in a status check.
- View the List of Access Requests
  When you receive a notice of an operator access request, you can view the list of all access requests by compartment, and accept or reject an access request.
- Filter Access Requests by State
  To review, approve, update, or revoke Access Requests, you can filter the Access Requests based on the workflow state of the request.
- Filter Access Requests by Resource Type
  To review, approve, update, or revoke Access Requests, you can filter the Access Requests based on the resource type of the request.
- Approve Access Request
  When you approve an access request, you permit access, enable or disable keyboard logging, and provide comments for the action as needed.
- Review Access Request
  To review and acknowledge a Raised Oracle Operator Access Request, use this procedure.
- Request Access for a Future Date and Time
  When you submit an Access Request, you can schedule a future date and time for accessing resources.
- Gather More Information About an Access Request
  If you need clarification of the information in the Access Request for you to approve the Access Request, you can use Operator Access Control to send questions to the Oracle operators working on the Access Request. Oracle operators will answer your question through Operator Access Control interfaces, and you can ask further clarifying questions to get the details you need. To ask for further clarification of details in the Access Request, use the following procedure:
- Download Operator Activity Audit Log Report
  To download audit log reports in HTML format, which contains Operator Activity including the commands and keystrokes entered by the operators, use this procedure.
- Reject Access Request
  To reject an Oracle Operator Access Request that you have previously granted, use this procedure.
- Revoke Access Request
  To revoke access to your tenancy after you have granted access, complete this procedure.

- Approve Extension Request
  When you receive an extension request, you approve an extended duration for the system access.
- Reject Extension Request
  If you receive an Oracle Operator access extension request that you want to reject, then use this procedure.

State of an Access Request

Review the list of states in which an Oracle operator access request can be listed in a status check.

Table 3-1 States of an Access Request

State	Description
RAISED	Operator has submitted an access request, and the approver or the system has not taken any action on the request.
IN-PROCESS	The system is processing the last action taken on the access request.
APPROVED	Approver has approved the access request.
PRE-APPROVED	The system has automatically approved the access request.
EXTENSION REQUESTED	Operator requests an extension of the period of the access request to have sufficient additional time for one or more operators to complete the task.
REJECTED	Approver has rejected the access request.
REVOKED	Approver has revoked the approval on a request. Any operator that may have been accessing the system have been disconnected from the system. No new actions can be taken on the request.
COMPLETED	The maintenance work for which the system access was requested is completed.
EXPIRED	Access request approval time period has expired. The operator cannot access the system without raising and obtaining approval for a new access request.
FAILED TO CLOSE	The system could not close an open access request. The close could have been triggered by REVOKE / COMPLETE / EXPIRE. Contact Oracle support.

View the List of Access Requests

When you receive a notice of an operator access request, you can view the list of all access requests by compartment, and accept or reject an access request.

You can **Approve**, **Reject**, **Approve Extension**, **Reject Extension**, and **Revoke** access requests.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. Click **Access Requests**.

Requests are listed by request ID. The **Resource Name** column displays the resource for which the request was raised. The **Resource Type** column displays the type of the resource (Autonomous Exadata VM Cluster, Exadata Infrastructure). The **State** column lists the status of a request (Raised, In Review, Approved for future, Approved, In-Process, Pre-Approved, Extension Requested, Rejected, Revoked, Completed, Expired, Failed to Close). The **Requested** column displays the date and time of the request.

The **Severity** column displays the severity level (Severity 1 - Complete loss of service for mission-critical operations where work cannot reasonably continue, Severity 2 - Significant or degraded loss of service or resources, Severity 3 - Minor loss of services or resources, Severity 4 - No work being impeded at the time - information is requested or reported) set by the operator. The **Access Request Reason** column displays the reason for the operator request for system access. To view individual requests, you can click a request ID.

Filter Access Requests by State

To review, approve, update, or revoke Access Requests, you can filter the Access Requests based on the workflow state of the request.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. Click **Access Requests**.
4. Under **Filters**, select an Action Request state from the list.
   You can perform actions based on the state of the Access Request.

Table 3-2 Actions on Access Requests

Access Request State	Allowed Action
Raised	**Approve**, **In-Review**, or **Reject**.
In Review	**Approve** or **Reject**.
Approved for future	**Approve** or **Reject**.
Approved	**Revoke**
In-Process	No actions.
Pre-Approved	**Revoke**
Extension Requested	**Approve Extension**, **Reject Extension**, or **Revoke**.
Rejected	No actions.
Revoked	No actions.
Completed	No actions.
Expired	No actions.
Failed to Close	No actions.

Filter Access Requests by Resource Type

To review, approve, update, or revoke Access Requests, you can filter the Access Requests based on the resource type of the request.

1. Log in to your Oracle Cloud Infrastructure tenancy.

2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. Click **Access Requests**.
4. Under **Filters**, select a **Resource Type** from the list.

Approve Access Request

When you approve an access request, you permit access, enable or disable keyboard logging, and provide comments for the action as needed.

> **Note:**
>
> If the user reviewing access requests is not a member of the Administrator User Group for a compartment, or a member of an identity and access management (IAM) user group specifically granted permissions to approve or revoke access on that compartment, then that user must be granted the privileges `inspect identity-providers`, `inspect groups`, and `inspect users` on the compartment before that user can approve or reject access requests.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. Click **Access Requests**.
4. Under **Filters**, select **Raised** from the drop-down list.
5. From the list of Access Requests, click the name of the request that you want to approve.
   You can also select the request and click **Actions** to Approve the access request.

   > **Note:**
   >
   > If you have not configured notifications, then a warning banner is displayed.
   >
   > a. Click **Configure**.
   > Configure notifications dialog is displayed.
   >
   > b. In the **Configure notifications** dialog, enter valid email addresses, and then click **Create**.

6. In the Request ID page, click **Approve**.
7. In the Approve Access Request page, do the following:
   a. To enable keyboard logging, click the box next to that option.
   b. In the comments field, enter additional comments or instructions you want to provide to the operator.
   c. Enter an approval comment.

d. Under **Approval Time**, select either **Approve Now** or **Approve Later**. If you choose to approve later, then select a timezone, **UTC**, or **Browser Timezone**, and then select date and time from the calendar control.

8. Click **Approve**.
In the **Approval information** section of the Access Request details page, you will find information regarding the number of approvals required, the number of approvals received, and the approvers who approved or rejected, as well as when they took action.

Review Access Request

To review and acknowledge a Raised Oracle Operator Access Request, use this procedure.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. Click **Access Requests**.
4. Under **Filters**, select **Raised** from the drop-down list.
5. From the list of Access Requests, click the name of the request that you want to reject.

   You can also click **Action** next to the request, and reject the access request.
6. In the Request ID page, click **In Review**.
7. In the Review Access Request dialog, enter a comment.
8. Click **In Review**.

Request Access for a Future Date and Time

When you submit an Access Request, you can schedule a future date and time for accessing resources.

The Access Request details page shows the scheduled date and time. Even if your request moves to the **Approved** state, you can access resources only at the scheduled date and time.

Gather More Information About an Access Request

If you need clarification of the information in the Access Request for you to approve the Access Request, you can use Operator Access Control to send questions to the Oracle operators working on the Access Request. Oracle operators will answer your question through Operator Access Control interfaces, and you can ask further clarifying questions to get the details you need. To ask for further clarification of details in the Access Request, use the following procedure:

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. Click **Access Requests**.
4. Under **Filters**, for example, select **Raised** from the drop-down list.
5. From the list of Access Requests, click the name of the request that you want to get clarified.
6. In the Request ID page, click the **Operator Interaction** tab.

7. Post your message and click **Send**.

Download Operator Activity Audit Log Report

To download audit log reports in HTML format, which contains Operator Activity including the commands and keystrokes entered by the operators, use this procedure.

> **Note:**
>
> Audit reports are generated automatically or updated periodically.

Audit log reports contain information about the commands and keystrokes entered by operators per session in human-decipherable HTML format. You can download the audit log report for any access that an operator has utilized to access your Exadata infrastructure. The audit log report will be available only if the operator has utilized it to log in to the infrastructure. After the audit log report is generated, it will be available for one year for the customers to download.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. Click **Access Requests**.
4. From the list of access requests, identify the Access Request for which you want the audit log report, then click it.
5. On the access request details page, click **Download Audit Report**.

Reject Access Request

To reject an Oracle Operator Access Request that you have previously granted, use this procedure.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. Click **Access Requests**.
4. Under **Filters**, select **Raised** from the drop-down list.
5. From the list of Access Requests, click the name of the request that you want to reject.

   You can also click **Action** next to the request, and reject the access request.
6. In the Request ID page, click **Reject**.
7. In the Reject Access Request dialog, enter a reason for rejecting the request.
8. Click **Reject**.

Revoke Access Request

To revoke access to your tenancy after you have granted access, complete this procedure.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. Click **Access Requests**.
4. Under **Filters**, select **Pre-Approved** from the drop-down list.
5. From the list of Access Requests, click the name of the request that you want to revoke.

   You can also click **Action** to revoke the access request.
6. In the Request ID page, click **Revoke**.
7. In the Revoke Access Request dialog, enter the explanation for revoking access in the comment field.
8. Click **Revoke**.

Approve Extension Request

When you receive an extension request, you approve an extended duration for the system access.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. Click **Access Requests**.
4. Under **Filters**, select **Extension Requested** from the drop-down list.
5. From the list of Access Requests, click the name of the request that you want to extend duration.
   You can also click the action button to Approve Extension.
6. In the Request ID page, click **Approve Extension**.
7. In the Approve Extension Request page, do the following:
   a. Enter additional comments you want to provide to the operator.
   b. Enter an approval comment.
8. Click **Approve Extension**.
   In the **Approval information** section of the Access Request details page, you will find information regarding the number of approvals required, the number of approvals received, and the approvers who approved or rejected, as well as when they took action.

Reject Extension Request

If you receive an Oracle Operator access extension request that you want to reject, then use this procedure.

Operator Control access expires when an already approved duration elapses. If the Oracle Operator requests an extension to the duration you approved for access to your

infrastructure, and this request is not acceptable, based on your service commitments, or for any other reason, then you can reject that access request.

1. Log in to your Oracle Cloud Infrastructure tenancy.
2. Open the navigation menu. Under **Oracle Database**, click **Operator Access Control**.
3. Click **Access Requests**.
4. Under **Filters**, select **Extension Requested** from the list.
5. From the list of Access Requests, click the name of the request for which you want to reject the extension.

   You can also click **Action** and select **Reject Extension**.
6. In the Request ID page, click **Reject Extension**.
7. In the Reject Extension Request page, in the comment field, enter your reason for rejecting the extension request.
8. Click **Reject Extension**.

4

Using the API to Manage Operator Access Control Resources

Operator Access Control application programming interfaces (APIs) assist with managing and auditng access control to your Oracle Cloud Infrastructure compartments.

For information about using the API and signing requests, see REST APIs and Security Credentials. For information about SDKs, see Software Development Kits and Command Line Interface.

- Using the API to Manage Operator Control
  Review the list of REST API endpoints to manage Operator Control.
- Using the API to Manage Operator Control Assignment
  Review the list of REST API endpoints to manage Operator Control Assignment.
- Using the API to Manage Access Request
  Review the list of REST API endpoints to manage Accees Request.
- Using the API to Manage Operator Action
  Review the list of REST API endpoints to manage operator actions.
- Using the API to Manage Operator Control Compartment
  Review the list of REST API endpoints to manage the Operator Control compartment.

Using the API to Manage Operator Control

Review the list of REST API endpoints to manage Operator Control.

- Create Operator Control: CreateOperatorControl
- Delete Operator Control: DeleteOperatorControl
- View the details of an Operator Control: GetOperatorControl
- View the list of Operator Controls: ListOperatorControls
- Modify an Operator Control: UpdateOperatorControl

Using the API to Manage Operator Control Assignment

Review the list of REST API endpoints to manage Operator Control Assignment.

- Assign Operator Control: CreateOperatorControlAssignment
- View the details of an Operator Control assignment: GetOperatorControlAssignment
- Modify Operator Control assignment: UpdateOperatorControlAssignment
- Remove Operator Control assignment: DeleteOperatorControlAssignment
- View the list of Operator Control assignments: ListOperatorControlAssignments

Using the API to Manage Access Request

Review the list of REST API endpoints to manage Accees Request.

- View the details of an access request: GetAccessRequest
- View the history of all statuses associated with a specific access request: ListAccessRequestHistories
- View the list of access requests: ListAccessRequests
- Approve access request: ApproveAccessRequest
- Reject access request: RejectAccessRequest
- Revoke access request: RevokeAccessRequest

Using the API to Manage Operator Action

Review the list of REST API endpoints to manage operator actions.

- View the details of an operator actions: GetOperatorAction
- View the list of operator actions: ListOperatorActions

Using the API to Manage Operator Control Compartment

Review the list of REST API endpoints to manage the Operator Control compartment.

- Change the compartment for the specified Operator Control ID: ChangeOperatorControlCompartment
- Change the compartment for the specified Operator Control assignment ID: ChangeOperatorControlAssignmentCompartment

5

Creating Policies to Control Operator Access with Operator Access Control

Learn to develop your own policies that use Actions to control access to Operator Access Control resources.

> **Note:**
>
> For an example policy, see Let database admins manage Exadata Cloud@Customer instances.

- About Resource-Types and Operator Access Control Policies
  Learn about resource-types that you can use in your policies.
- Resource-Types for Operator Access Control
  Review the list of resource-types specific to Operator Access Control.
- Supported Variables for Operator Access Control
  Use variables when adding conditions to a policy.
- Details for Verb + Resource-Type Combinations
  Review the list of permissions and API operations covered by each verb for Operator Access Control.
- Permissions Required for Each API Operation
  Review the list of API operations for Operator Control Access resources in a logical order, grouped by resource type.

Related Topics

- How Policies Work

About Resource-Types and Operator Access Control Policies

Learn about resource-types that you can use in your policies.

An aggregate resource-type covers the list of individual resource-types that directly follow. For example, writing one policy to allow a group to have access to the `operator-control-family` is equivalent to writing three separate policies for the group that would grant access to the `operator-control`, `operator-control-assignment`, `operator-control-accessrequest`, and the rest of the individual resource-types. For more information, see Resource-Types.

Resource-Types for Operator Access Control

Review the list of resource-types specific to Operator Access Control.

Aggregate Resource-Type

```
operator-control-family
```

Individual Resource-Types

```
operator-control
operator-control-assignment
operator-control-accessrequest
```

Supported Variables for Operator Access Control

Use variables when adding conditions to a policy.

Operator Access Control supports only the general variables. For more information, see General Variables for All Requests.

Details for Verb + Resource-Type Combinations

Review the list of permissions and API operations covered by each verb for Operator Access Control.

For more information, see Permissions, Verbs, and Resource-Types.

- Operator-Control-Family Resource Types
  Each Operator Access Control resource-type verb grants different levels of access.
- operator-control-family
  Review the list of permissions and API operations for `operator-control-family` resource-type.
- operator-control
  Review the list of permissions and API operations for `operator-control` resource-type.
- operator-control-assignment
  Review the list of permissions and API operations for `operator-control-assignment` resource-type.
- operator-control-accessrequest
  Review the list of permissions and API operations for `operator-control-accessrequest` resource-type.

Operator-Control-Family Resource Types

Each Operator Access Control resource-type verb grants different levels of access.

The level of access is cumulative as you go from **inspect** to **read**, to **use**, and to **manage**. A plus sign (+) in a table cell indicates incremental access compared to the cell directly above it, whereas "no extra" indicates no incremental access.

For example, the `read` verb for the `operator-control` resource-type covers no extra permissions or API operations compared to the `inspect` verb. However, the `use` verb

includes one more permission, fully covers one more operation, and partially covers another additional operation.

operator-control-family

Review the list of permissions and API operations for `operator-control-family` resource-type.

Table 5-1 operator-control-family

Verbs	Permissions	APIs Fully Covered	APIs Partially Covered
INSPECT	OPERATOR_CONTROL_INSPECT OPERATOR_CONTROL_ASSIGNMENT_INSPECT OPERATOR_CONTROL_ACCESSREQUEST_INSPECT	ListOperatorControls ListOperatorControlAssignments ListAccessRequests	*none*
READ	*INSPECT* + OPERATOR_CONTROL_READ OPERATOR_CONTROL_ASSIGNMENT_READ OPERATOR_CONTROL_ACCESSREQUEST_READ	GetOperatorControl GetOperatorControlAssignment GetAccessRequest	*none*
USE	*READ* + OPERATOR_CONTROL_UPDATE OPERATOR_CONTROL_ASSIGNMENT_UPDATE OPERATOR_CONTROL_ACCESSREQUEST_UPDATE	UpdateOperatorControl UpdateOperatorControlAssignment RevokeAccessRequest	*none*
MANAGE	*USE* + OPERATOR_CONTROL_CREATE OPERATOR_CONTROL_DELETE OPERATOR_CONTROL_MOVE OPERATOR_CONTROL_ASSIGNMENT_CREATE OPERATOR_CONTROL_ASSIGNMENT_DELETE OPERATOR_CONTROL_ASSIGNMENT_MOVE	CreateOperatorControl DeleteOperatorControl ChangeOperatorControlCompartment CreateOperatorControlAssignment DeleteOperatorControlAssignment ChangeOperatorControlAssignmentCompartment	*none*

operator-control

Review the list of permissions and API operations for `operator-control` resource-type.

Table 5-2 operator-control

Verbs	Permissions	APIs Fully Covered	APIs Partially Covered
INSPECT	`OPERATOR_CONTROL_INSPECT`	`ListOperatorControls`	*none*
READ	*INSPECT* + `OPERATOR_CONTROL_READ`	`GetOperatorControl`	*none*
USE	*READ* + `OPERATOR_CONTROL_UPDATE`	`UpdateOperatorControl`	*none*
MANAGE	*USE* + `OPERATOR_CONTROL_CREATE` `OPERATOR_CONTROL_DELETE` `OPERATOR_CONTROL_MOVE`	`CreateOperatorControl` `DeleteOperatorControl` `ChangeOperatorControlCompartment`	*none*

operator-control-assignment

Review the list of permissions and API operations for `operator-control-assignment` resource-type.

Table 5-3 operator-control-assignment

Verbs	Permissions	APIs Fully Covered	APIs Partially Covered
INSPECT	`OPERATOR_CONTROL_ASSIGNMENT_INSPECT`	`ListOperatorControlAssignments`	*none*
READ	*INSPECT* + `OPERATOR_CONTROL_ASSIGNMENT_READ`	`GetOperatorControlAssignment`	*none*
USE	*READ* + `OPERATOR_CONTROL_ASSIGNMENT_UPDATE`	`UpdateOperatorControlAssignment`	*none*

Table 5-3 (Cont.) operator-control-assignment

Verbs	Permissions	APIs Fully Covered	APIs Partially Covered
MANAGE	*USE* + `OPERATOR_CONTROL_ASSIGNMENT_CREATE` `OPERATOR_CONTROL_ASSIGNMENT_DELETE` `OPERATOR_CONTROL_ASSIGNMENT_MOVE`	`CreateOperatorControlAssignment` `DeleteOperatorControlAssignment` `ChangeOperatorControlAssignmentCompartment`	*none*

operator-control-accessrequest

Review the list of permissions and API operations for `operator-control-accessrequest` resource-type.

Table 5-4 operator-control-accessrequest

Verbs	Permissions	APIs Fully Covered	APIs Partially Covered
INSPECT	`OPERATOR_CONTROL_ACCESSREQUEST_INSPECT`	*none*	*none*
READ	*INSPECT* + `OPERATOR_CONTROL_ACCESSREQUEST_READ`	`GetAccessRequest`	*none*
USE	*READ* +	*none*	*none*
MANAGE	*USE* + `OPERATOR_CONTROL_ACCESSREQUEST_UPDATE`	`ApproveAccessRequest` `RejectAccessRequest` `RevokeAccessRequest`	*none*

Permissions Required for Each API Operation

Review the list of API operations for Operator Control Access resources in a logical order, grouped by resource type.

For information about permissions, see Permissions.

> **Note:**
>
> `operator-control-accessrequest` is special kind of resource. You cannot create it. Oracle operators create it and you will have ability to approve or reject the requests.

Table 5-5 Resource-Type and Permissions

Resource Type	Permissions
operator-control-family	OPERATOR_CONTROL_INSPECT OPERATOR_CONTROL_READ OPERATOR_CONTROL_CREATE OPERATOR_CONTROL_UPDATE OPERATOR_CONTROL_DELETE OPERATOR_CONTROL_ASSIGNMENT_INSPECT OPERATOR_CONTROL_ASSIGNMENT_READ OPERATOR_CONTROL_ASSIGNMENT_CREATE OPERATOR_CONTROL_ASSIGNMENT_UPDATE OPERATOR_CONTROL_ASSIGNMENT_DELETE OPERATOR_CONTROL_ACCESSREQUEST_INSPECT OPERATOR_CONTROL_ACCESSREQUEST_READ OPERATOR_CONTROL_ACCESSREQUEST_UPDATE
operator-control	OPERATOR_CONTROL_INSPECT OPERATOR_CONTROL_READ OPERATOR_CONTROL_CREATE OPERATOR_CONTROL_UPDATE OPERATOR_CONTROL_DELETE OPERATOR_CONTROL_MOVE
operator-control-assignment	OPERATOR_CONTROL_ASSIGNMENT_INSPECT OPERATOR_CONTROL_ASSIGNMENT_READ OPERATOR_CONTROL_ASSIGNMENT_CREATE OPERATOR_CONTROL_ASSIGNMENT_UPDATE OPERATOR_CONTROL_ASSIGNMENT_DELETE OPERATOR_CONTROL_ASSIGNMENT_MOVE
operator-control-accessrequest	OPERATOR_CONTROL_ACCESSREQUEST_INSPECT OPERATOR_CONTROL_ACCESSREQUEST_READ OPERATOR_CONTROL_ACCESSREQUEST_UPDATE

Table 5-6 Operator Access Control API Operations

API Operation	Permissions Required to Use the Operation
CreateOperatorControl	OPERATOR_CONTROL_CREATE
DeleteOperatorControl	OPERATOR_CONTROL_DELETE
GetOperatorControl	OPERATOR_CONTROL_READ
ListOperatorControls	OPERATOR_CONTROL_INSPECT

Table 5-6 (Cont.) Operator Access Control API Operations

API Operation	Permissions Required to Use the Operation
UpdateOperatorControl	OPERATOR_CONTROL_UPDATE
CreateOperatorControlAssignment	OPERATOR_CONTROL_ASSIGNMENT_CREATE
GetOperatorControlAssignment	OPERATOR_CONTROL_ASSIGNMENT_READ
UpdateOperatorControlAssignment	OPERATOR_CONTROL_ASSIGNMENT_UPDATE
DeleteOperatorControlAssignment	OPERATOR_CONTROL_ASSIGNMENT_DELETE
ListOperatorControlAssignments	OPERATOR_CONTROL_ASSIGNMENT_INSPECT
GetAccessRequest	OPERATOR_CONTROL_ACCESSREQUEST_READ
ListAccessRequestHistories	OPERATOR_CONTROL_ACCESSREQUEST_LIST
ListAccessRequests	OPERATOR_CONTROL_ACCESSREQUEST_LIST
ApproveAccessRequest	OPERATOR_CONTROL_ACCESSREQUEST_UPDATE
RevokeAccessRequest	OPERATOR_CONTROL_ACCESSREQUEST_UPDATE
GetOperatorAction	OPERATOR_CONTROL_READ
ListOperatorActions	OPERATOR_CONTROL_INSPECT
ChangeOperatorControlCompartment	OPERATOR_CONTROL_MOVE
ChangeOperatorControlAssignmentCompartment	OPERATOR_CONTROL_ASSIGNMENT_MOVE

6

Managing and Searching Logs with Operator Access Control

Learn to enable logs to view the list of Operator Controls created and in use in a compartment. Also, to monitor operator activities in a cage.

- Enabling Logs and Creating Log Groups with Operator Access Control
  To track Oracle operator activities on your system., learn how to enable logs, and how to create log groups to manage logs.
- Log Format for Operator Access Control
  Learn about the fields that an audit log published in the logging service contains.
- Searching Logs
  To perform a search on logs, use this procedure to specify the fields, time range, and text strings for logs that you want to search.

Enabling Logs and Creating Log Groups with Operator Access Control

To track Oracle operator activities on your system., learn how to enable logs, and how to create log groups to manage logs.

To audit the actions that an Oracle operator performs on your system, you can create an audit log for a compartment and a particular service where you want to monitor Oracle operator actions.

1. On the left navigation menu, select **Logging**, and then select **Logs**.
2. Click **Enable Service Log**. The Enable Resource Log window opens.
3. In the **Select Resource** section, provide information for each of the fields:
   - **Resource Compartment**: Select the compartment where you want to create the log.
   - **Service**: Select **Operator Access Control Service** for which you want to enable log.
   - **Resource**: Select an Operator Control for which you want to enable log.
4. In the **Configure Log** section, provide information for the following fields:
   - **Log Category**: Select **Access Logs**.
   - **Log Name**: Provide a name for the log that you want to create.
5. (Optional) Click **Show Advanced Options**.
6. (Optional) In the **Log Location** section, provide information for the following fields:
   - **Compartment**: Select a compartment, if you want log files to be placed in a different compartment from the one for which you are creating an audit log.
   - **Log Group**: Select a log group to which you wan to add the log. A log group is a logical container for logs. Use log groups to streamline log management, including

applying policy or analyzing groups of logs. If you want to create a new log group, the click **Create New Group**, and provide information for the following fields:

  - **Compartment** Select the compartment where you want to place the log group.
  - **Name**: Provide a name for the log group.
  - **Description**: Provide a description for the purpose of the log group.

- In the **Tag Namespace** field, consider adding a **tag namespace** (an identifying text string applied to a set of compartments), or tagging the control with an existing tag namespace.

7. In the **Log Retention** section, select a log retention period.
8. When you have completed and reviewed your selections, click **Enable Log**. The log pertaining to the operator control is enabled.

Related Topics

- Tagging Overview

Log Format for Operator Access Control

Learn about the fields that an audit log published in the logging service contains.

Table 6-1 Audit Log Fields

Field	Description
`data`	Contains all the data obtained from the Exadata audit logs.
`data.accessRequestId`	Contains the Oracle Cloud Identifier (OCID) of the access request. This identifier is obtained from the access request listing page in the Console.
`data.message`	Contains audit log in the raw format. The audit log format follows the audit logging format as output by the `ausearch` command. For more information, see the `ausearch(8)` manual pages.
`data.systemOcid`	The Oracle Cloud Identifier (OCID) of the Exadata system from which the log was collected.
`data.timestamp`	The time stamp, usually in the Universal Time Coordinated (UTC) time zone (TZ) at which point the action that the log represents was performed.
`source`	The service that is publishing the log. The source of the log is the `OperatorAccessControl` for this service.

> **Note:**
>
> There are a few additional fields, which are primarily for accounting purposes of the service.

Example 6-1 Operator Access Control Audit Log


```
{
  "logContent": {
    "data": {
      "accessRequestId": "ocid1.opctlaccessrequest.oc1.ap-
chuncheon-1.aaaaaaaaqk67mpzb74nsssg4ppwk7cyg46dwoxegtvhopdp7lxbktpymk4kq",
      "message": "type=PROCTITLE msg=audit(09/08/2021
09:01:24.335:34495595) : proctitle=ps -ef \ntype=PATH msg=audit(09/08/2021
09:01:24.335:34495595) : item=1 name=/lib64/ld-linux-x86-64.so.2
inode=2546207 dev=fc:00 mode=file,755 ouid=root ogid=root rdev=00:00
nametype=NORMAL cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 \ntype=PATH
msg=audit(09/08/2021 09:01:24.335:34495595) : item=0 name=/usr/bin/ps
inode=33619160 dev=fc:00 mode=file,755 ouid=root ogid=root rdev=00:00
nametype=NORMAL cap_fp=none cap_fi=none cap_fe=0 cap_fver=0 \ntype=CWD
msg=audit(09/08/2021 09:01:24.335:34495595) : cwd=/home/
b9dc42d68f6e4e26a1d843a4c5e70187 \ntype=EXECVE msg=audit(09/08/2021
09:01:24.335:34495595) : argc=2 a0=ps a1=-ef \ntype=SYSCALL
msg=audit(09/08/2021 09:01:24.335:34495595) : arch=x86_64 syscall=execve
success=yes exit=0 a0=0x1848d50 a1=0x184c360 a2=0x184c040 a3=0x7ffeec95b760
items=2 ppid=94699 pid=95635 auid=b9dc42d68f6e4e26a1d843a4c5e70187
uid=b9dc42d68f6e4e26a1d843a4c5e70187 gid=opctl_facc1
euid=b9dc42d68f6e4e26a1d843a4c5e70187 suid=b9dc42d68f6e4e26a1d843a4c5e70187
fsuid=b9dc42d68f6e4e26a1d843a4c5e70187 egid=opctl_facc1 sgid=opctl_facc1
fsgid=opctl_facc1 tty=pts0 ses=813000 comm=ps exe=/usr/bin/ps key=(null) \n",
      "status": "",
      "systemOcid": "ocid1.exadatainfrastructure.oc1.ap-
chuncheon-1.ab4w4ljr46tyytihmindrbshch3jjhrxxpctq4eiaksakp4kqamluuwkzdga",
      "target": "",
      "timestamp": "2021-09-08T09:01:24.000Z"
    },
    "id": "b3b102aa-daee-4861-8e2c-9014faac9de2",
    "oracle": {
      "compartmentid":
"ocid1.tenancy.oc1..aaaaaaaazxdmffivtoe32kvio5e2dcgz24re5rqbkis3452yi2e7tc3x2
erq",
      "ingestedtime": "2021-09-08T16:02:26.182Z",
      "loggroupid": "ocid1.loggroup.oc1.ap-
chuncheon-1.amaaaaaajobtc3ia3iypuri32bhvrgmosztobwi72wgdofkpfdbyfg4yxlrq",
      "logid": "ocid1.log.oc1.ap-
chuncheon-1.amaaaaaajobtc3iahnkkwizgpoakdafmrttikohparjl7icmcfjzkechekfq",
      "tenantid":
"ocid1.tenancy.oc1..aaaaaaaazxdmffivtoe32kvio5e2dcgz24re5rqbkis3452yi2e7tc3x2
erq"
    },
    "source": "OperatorAccessControl",
    "specversion": "1.0",
    "time": "2021-09-08T16:01:52.989Z",
    "type": "com.oraclecloud.opctl.audit"
  },
  "datetime": 1631116912989
}
```

Searching Logs

To perform a search on logs, use this procedure to specify the fields, time range, and text strings for logs that you want to search.

The log is enabled based on specific Operator Controls. Hence these form the top level filter for the log searches. Additionally, you can also search logs for the Access Request IDs, Exadata systems where the operator action occurred, or the time when the action occurred.

The following examples help you understand how to search for specific field.

1. On the left navigation menu, select **Logging**, and then select **Logs**.
2. Choose the compartment where the logs are stored.
   This will provide a list of logs which were enabled.
3. Click the log that you are interested in. log detail page is displayed.
   These logs are always related to a single operator control.
4. Click the **Explore with Log Search** link to search for specific logs.
5. **Case 1:** Searching for actions performed using the approval for a specific access request, **ocid.opctlaccessrequest.x** during a period T-start to T-end pertaining to an Operator Control, **ocid.opctl.x**.
   a. Choose **Custom** from the **Filter By Time** field.
   b. Select **Start Date** and **End Date**.
   c. Click **Search**.
      After choosing you would be able to see a set of logs.
   d. Now, for example, add the following search criteria ino the **Filter By Field or Text Search** field.

      ```
      data.accessRequestId='ocid.opctlaccessrequest.x'
      ```

      This will list the logs matching the search criteria.
6. **Case 2:** Searching for actions on an Exadata systems, **ocid.exadata.x** during a period T-start to T-end pertaining to an Operator Control, **ocid.opctl.x**.
   a. Choose **Custom** from the **Filter By Time** field.
   b. Click **Search**.
      After choosing you would be able to see a set of logs.
   c. Now, for example, add the following search criteria ino the **Filter By Field or Text Search** field.

      ```
      data.systemOcid ='ocid.exadata.x'
      ```

      This will list the logs matching the search criteria.
7. You can also search the logs by the content. Use the **log-content** field. For more information, see Searching Logs.
8. To search for specific linux commands executed, use the **Advanced Mode**.

a. Create a basic search using the examples given above (case 1 or case 2), and then switch to Advanced Mode.
For example, to search for all the logs with the action `vi` add the following criteria:

```
and text_contains(data.message, 'proctitle=vi ', true)
```

9. When performing a search on the Logging Search page, you can click **Show Advanced Mode** to enter your own custom log search queries.
For example:

```
search "ocid1.compartment.oc1..x/ocid1.loggroup.oc1.iad.loggroup_x/
ocid1.log.oc1.iad.log_x"
 | data.systemOcid='ocid1.exadata.x' and text_contains(data.message,
'proctitle=vi ', true)
 | sort by datetime desc
```

7

Auditing Operator Access Control Lifecycle Events

Learn how to audit Operator Access Control lifecycle events and critical activities of operators (log in and log out) on Exadata Cloud@Customer machine events.

For more information about auditing generally, see *Overview of Audit*.

- Operator Access Control Event Types
  The Operator Access Control resources emit events, which are structured messages that indicate changes in resources.
- Viewing Audit Log Events
  Audit provides records of API operations performed against supported services as a list of log events.

Related Topics

- Overview of Audit

Operator Access Control Event Types

The Operator Access Control resources emit events, which are structured messages that indicate changes in resources.

Table 7-1 Operator Access Control Event Types

Friendly Name	Event Type
Operator Control - Create	`com.oraclecloud.operatorcontrol.CreateOperatorControl`
Operator Control - Update	`com.oraclecloud.operatorcontrol.UpdateOperatorControl`
Operator Control - Delete	`com.oraclecloud.operatorcontrol.DeleteOperatorControl`
Assign Operator Control - Create	`com.oraclecloud.operatorcontrol.CreateOperatorControlAssignment`
Assign Operator Control - Update	`com.oraclecloud.operatorcontrol.UpdateOperatorControlAssignment`
Assign Operator Control - Delete	`com.oraclecloud.operatorcontrol.DeleteOperatorControlAssignment`
Access Request - Approve	`com.oraclecloud.operatorcontrol.ApproveAccessRequest`
Access Request - AutoApprove	`com.oraclecloud.operatorcontrol.AutoApproveAccessRequest`
Access Request - Create	`com.oraclecloud.operatorcontrol.CreateAccessRequest`

Table 7-1 (Cont.) Operator Access Control Event Types

Friendly Name	Event Type
AddSharedOperator	com.oraclecloud.operatoraccesscontrol.AddSharedOperator
Access Request - Reject	com.oraclecloud.operatorcontrol.RejectAccessRequest
Access Request - Revoke	com.oraclecloud.operatorcontrol.RevokeAccessRequest
Access Request - Expired	com.oraclecloud.operatorcontrol.ExpiredAccessRequest
Access Request - Closed	com.oraclecloud.operatorcontrol.ClosedAccessRequest
Access Request - Extend	com.oraclecloud.operatorcontrol.ExtendAccessRequest
Operator - Login	com.oraclecloud.operatorcontrol.OperatorLogin
Operator - Logout	com.oraclecloud.operatorcontrol.OperatorLogout

Example 7-1 Reference Event for Operator Control - Create


```
{
  "eventType": "com.oraclecloud.operatorcontrol.createoperatorcontrol",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "OperatorAccessControl",
  "eventId": "356eeecc-4cd9-4bcd-90c2-478937c52681",
  "eventTime": "2020-09-11T10:07:11.464Z",
  "contentType": "application/json",
  "data": {
    "eventGroupingId": null,
    "eventName": "CreateOperatorControl",
    "compartmentId":
"ocid1.compartment.oc1..aaaaaaaa4fboeyqkh2h4nft34qgdavsxmd7wgb2erbtvaks
5f477qtn2qc5a",
    "compartmentName": "ccavcn",
    "resourceName": "OperatorControl",
    "resourceId":
"ocid1.opctloperatorcontrol.oc1..aaaaaaaa5eyhyfocwewepjiacgoihjrjxnpb4s
qt3hdzqow5knof7yrdjhpq",
    "availabilityDomain": "AD1",
    "freeformTags": null,
    "definedTags": null,
    "identity": {
      "principalName": "test.user@oracle.com",
      "principalId":
"ocid1.user.oc1..aaaaaaaaaazh2gydmfjnl3sstigrjac4z5tvvn4zkt2khofzfumawo
haynba",
      "authType": "natv",
      "callerName": null,
      "callerId": null,
      "tenantId":
"ocid1.tenancy.oc1..aaaaaaaavrjqbg24tohoixm7bju6otfn5au73atpa7d6atxf36z
```

```
w2espdu3q",
      "ipAddress": "172.23.128.3",
      "credentials":
"ocid1.tenancy.oc1..aaaaaaaavrjqbg24tohoixm7bju6otfn5au73atpa7d6atxf36zw2espd
u3q/
ocid1.user.oc1..aaaaaaaaaazh2gydmfjnl3sstigrjac4z5tvvn4zkt2khofzfumawohaynba/
b3:39:8d:75:85:1a:01:b0:f8:cd:68:0a:23:05:7b:76",
      "userAgent": "Oracle-JavaSDK/1.15.0 (Linux/
4.1.12-124.28.6.el7uek.x86_64; Java/1.8.0_212; OpenJDK 64-Bit Server VM/
25.212-b04)",
      "consoleSessionId": null
    },
    "request": {
      "id": "request-policy-12345/5902EC63E925318838B62A66E57528FD/
4E0EBF1295A02B7FFFB1B8DD8E41A759",
      "path": "/20200630/operatorControls",
      "action": "POST",
      "parameters": {},
      "headers": {
        "Accept": [
          "application/json"
        ],
        "Authorization": [
          "Signature headers=\"date (request-target) host content-length
content-type x-content-
sha256\",keyId=\"ocid1.tenancy.oc1..aaaaaaaavrjqbg24tohoixm7bju6otfn5au73atpa
7d6atxf36zw2espdu3q/
ocid1.user.oc1..aaaaaaaaaazh2gydmfjnl3sstigrjac4z5tvvn4zkt2khofzfumawohaynba/
b3:39:8d:75:85:1a:01:b0:f8:cd:68:0a:23:05:7b:76\",algorithm=\"rsa-
sha256\",signature=\"*****\",version=\"1\""
        ],
        "Connection": [
          "keep-alive"
        ],
        "Content-Length": [
          "827"
        ],
        "Content-Type": [
          "application/json"
        ],
        "Date": [
          "Fri, 11 Sep 2020 10:07:11 GMT"
        ],
        "User-Agent": [
          "Oracle-JavaSDK/1.15.0 (Linux/4.1.12-124.28.6.el7uek.x86_64; Java/
1.8.0_212; OpenJDK 64-Bit Server VM/25.212-b04)"
        ],
        "X-Forwarded-For": [
          "209.17.43.241,0.0.0.0"
        ],
        "X-Real-IP": [
          "209.17.43.241"
        ],
        "X-Real-Port": [
          "26413"
```

```
        ],
        "oci-original-url": [
          "https://operator-access-control-dev.us-ashburn-1.oci.oc-
test.com/20200630/operatorControls"
        ],
        "opc-client-info": [
          "Oracle-JavaSDK/1.15.0"
        ],
        "opc-request-id": [
          "request-policy-12345"
        ],
        "opc-retry-token": [
          "5378a205-f978-41b1-bbc4-8a9032a02d3a"
        ],
        "x-content-sha256": [
          "HxwrSen2PgmZEWl0mwoeOBszNTiR2nxyk1ZVGQgKGVc="
        ]
      }
    },
    "response": {
      "status": "200",
      "responseTime": "2020-09-11T10:07:13.216Z",
      "headers": {
        "Content-Length": [
          "1222"
        ],
        "Content-Type": [
          "application/json"
        ],
        "Date": [
          "Fri, 11 Sep 2020 10:07:11 GMT"
        ],
        "opc-request-id": [
          "request-policy-12345/5902EC63E925318838B62A66E57528FD/
4E0EBF1295A02B7FFFB1B8DD8E41A759"
        ]
      },
      "payload": null,
      "message": "OperatorControl for
ocid1.opctloperatorcontrol.oc1..aaaaaaaa5eyhyfocwewepjiacgoihjrjxnpb4sq
t3hdzqow5knof7yrdjhpq has been executed "
    },
    "stateChange": {
      "previous": null,
      "current": {
        "OperatorControl": {
          "approverGroupsList": [

"ocid1.group.oc1..aaaaaaaaszj62swosn4xbz3xgkungjnvi2hbrrxx3d7ojtzulukvy
ewyqdva",

"ocid1.group.oc1..aaaaaaaajwlf3b5slsljcmeix3ki53ivk56ew7mikkxm6hdzyu7ey
ijgmbsq"
          ],
          "approversList": [
```

```
"ocid1.user.oc1..aaaaaaaanfy5pvezsopjdzs26sorubsmlidvf7m32raoie6dtwhyyxwlzgda
",

"ocid1.user.oc1..aaaaaaaaaazh2gydmfjnl3sstigrjac4z5tvvn4zkt2khofzfumawohaynba
"
          ],
          "compartmentId":
"ocid1.compartment.oc1..aaaaaaaa4fboeyqkh2h4nft34qgdavsxmd7wgb2erbtvaks5f477q
tn2qc5a",
          "description": "Creating an demo OpControl where all
accessrequests are preapproved",
          "id":
"ocid1.opctloperatorcontrol.oc1..aaaaaaaa5eyhyfocwewepjiacgoihjrjxnpb4sqt3hdz
qow5knof7yrdjhpq",
          "isFullyPreApproved": true,
          "lifecycleState": "CREATED",
          ],
          "operatorControlName": "All Preapproved OpControl Policy",
          "systemMessage": "Preapproved OpControl Policy disclaimer",
          "timeOfCreation": "2020-09-11T10:07:12.750Z",
          "timeOfModification": "2020-09-11T10:07:12.750Z"
        }
      }
    },
    "additionalDetails": {
      "operatorcontrol_name": "All Preapproved OpControl Policy",
      "operatorcontrol_ocid":
"ocid1.opctloperatorcontrol.oc1..aaaaaaaa5eyhyfocwewepjiacgoihjrjxnpb4sqt3hdz
qow5knof7yrdjhpq"
    }
  }
}
```


Example 7-2 Reference Event for Assign Operator Control - Create


```
{
  "eventType":
"com.oraclecloud.operatorcontrol.createoperatorcontrolassignment",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "OperatorAccessControl",
  "eventId": "f0041577-76fd-4d51-9275-38812e4d62c6",
  "eventTime": "2020-09-11T10:20:15.759Z",
  "contentType": "application/json",
  "data": {
    "eventGroupingId": null,
    "eventName": "CreateOperatorControlAssignment",
    "compartmentId":
"ocid1.compartment.oc1..aaaaaaaa4fboeyqkh2h4nft34qgdavsxmd7wgb2erbtvaks5f477q
tn2qc5a",
    "compartmentName": "ccavcn",
    "resourceName": "OperatorControlAssignment",
    "resourceId":
```

```
"ocid1.exadatainfrastructure.oc1.sea.abzwkljs5syf3f2pbypg5hn3zibypiqedc
cnomexcpd6judr5ecqijavkjyq",
    "availabilityDomain": "AD1",
    "freeformTags": null,
    "definedTags": null,
    "identity": {
      "principalName": "test.user@oracle.com",
      "principalId":
"ocid1.user.oc1..aaaaaaaaaazh2gydmfjnl3sstigrjac4z5tvvn4zkt2khofzfumawo
haynba",
      "authType": "natv",
      "callerName": null,
      "callerId": null,
      "tenantId":
"ocid1.tenancy.oc1..aaaaaaaavrjqbg24tohoixm7bju6otfn5au73atpa7d6atxf36z
w2espdu3q",
      "ipAddress": "172.23.128.3",
      "credentials":
"ocid1.tenancy.oc1..aaaaaaaavrjqbg24tohoixm7bju6otfn5au73atpa7d6atxf36z
w2espdu3q/
ocid1.user.oc1..aaaaaaaaaazh2gydmfjnl3sstigrjac4z5tvvn4zkt2khofzfumawoh
aynba/b3:39:8d:75:85:1a:01:b0:f8:cd:68:0a:23:05:7b:76",
      "userAgent": "Oracle-JavaSDK/1.15.0 (Linux/
4.1.12-124.28.6.el7uek.x86_64; Java/1.8.0_212; OpenJDK 64-Bit Server
VM/25.212-b04)",
      "consoleSessionId": null
    },
    "request": {
      "id": "request-policy-12345/4E4D1E067FC21B2D07384FD54F35728C/
515F40CD01EED0C6135D399009A88A2C",
      "path": "/20200630/operatorControlAssignments",
      "action": "POST",
      "parameters": {},
      "headers": {
        "Accept": [
          "application/json"
        ],
        "Authorization": [
          "Signature headers=\"date (request-target) host content-
length content-type x-content-
sha256\",keyId=\"ocid1.tenancy.oc1..aaaaaaaavrjqbg24tohoixm7bju6otfn5au
73atpa7d6atxf36zw2espdu3q/
ocid1.user.oc1..aaaaaaaaaazh2gydmfjnl3sstigrjac4z5tvvn4zkt2khofzfumawoh
aynba/
b3:39:8d:75:85:1a:01:b0:f8:cd:68:0a:23:05:7b:76\",algorithm=\"rsa-
sha256\",signature=\"*****\",version=\"1\""
        ],
        "Connection": [
          "keep-alive"
        ],
        "Content-Length": [
          "619"
        ],
        "Content-Type": [
          "application/json"
```

```
        ],
        "Date": [
          "Fri, 11 Sep 2020 10:20:15 GMT"
        ],
        "User-Agent": [
          "Oracle-JavaSDK/1.15.0 (Linux/4.1.12-124.28.6.el7uek.x86_64; Java/
1.8.0_212; OpenJDK 64-Bit Server VM/25.212-b04)"
        ],
        "X-Forwarded-For": [
          "209.17.43.241,0.0.0.0"
        ],
        "X-Real-IP": [
          "209.17.43.241"
        ],
        "X-Real-Port": [
          "26635"
        ],
        "oci-original-url": [
          "https://operator-access-control-dev.us-ashburn-1.oci.oc-test.com/
20200630/operatorControlAssignments"
        ],
        "opc-client-info": [
          "Oracle-JavaSDK/1.15.0"
        ],
        "opc-request-id": [
          "request-policy-12345"
        ],
        "opc-retry-token": [
          "22131e35-9494-4102-a3b9-9f86de408e46"
        ],
        "x-content-sha256": [
          "GgU7gwghhf5Bu/3HwqQGD7lyyGKYPbF9Y51zS+j8mZw="
        ]
      }
    },
    "response": {
      "status": "200",
      "responseTime": "2020-09-11T10:20:17.358Z",
      "headers": {
        "Content-Length": [
          "1093"
        ],
        "Content-Type": [
          "application/json"
        ],
        "Date": [
          "Fri, 11 Sep 2020 10:20:15 GMT"
        ],
        "opc-request-id": [
          "request-policy-12345/4E4D1E067FC21B2D07384FD54F35728C/
515F40CD01EED0C6135D399009A88A2C"
        ]
      },
      "payload": null,
      "message": "OperatorControlAssignment for
```

```
ocid1.exadatainfrastructure.oc1.sea.abzwkljs5syf3f2pbypg5hn3zibypiqedcc
nomexcpd6judr5ecqijavkjyq has been executed "
    },
    "stateChange": {
      "previous": null,
      "current": {
        "OperatorControlAssignment": {
          "assignerId":
"ocid1.user.oc1..aaaaaaaaaazh2gydmfjnl3sstigrjac4z5tvvn4zkt2khofzfumawo
haynba",
          "comment": "deploying on scaqak01adm0304_jyq",
          "compartmentId":
"ocid1.compartment.oc1..aaaaaaaa4fboeyqkh2h4nft34qgdavsxmd7wgb2erbtvaks
5f477qtn2qc5a",
          "detachmentDescription": "",
          "id":
"ocid1.opctloperatorcontrolassignment.oc1..aaaaaaaabtxbcqkpicasbmm7kmbf
umjdeaqwqv3xp5sn7g7v2babncnlga2a",
          "isEnforcedAlways": true,
          "lifecycleState": "CREATED",
          "operatorControlId":
"ocid1.opctloperatorcontrol.oc1..aaaaaaaa52eqysdkogsv2qd6apw3iafsrq5rxr
hqu4ninanpd3dwmc5ns4ca",
          "resourceCompartmentId":
"ocid1.compartment.oc1..aaaaaaaa4fboeyqkh2h4nft34qgdavsxmd7wgb2erbtvaks
5f477qtn2qc5a",
          "resourceId":
"ocid1.exadatainfrastructure.oc1.sea.abzwkljs5syf3f2pbypg5hn3zibypiqedc
cnomexcpd6judr5ecqijavkjyq",
          "resourceName": "scaqak01adm0304_jyq",
          "timeOfAssignment": "2020-09-11T10:20:15.931Z",
          "unassignerId": ""
        }
      }
    },
    "additionalDetails": {
      "exadatainfrastructure_ocid":
"ocid1.exadatainfrastructure.oc1.sea.abzwkljs5syf3f2pbypg5hn3zibypiqedc
cnomexcpd6judr5ecqijavkjyq",
      "operatorcontrol_name": "All Preapproved OpControl Policy",
      "operatorcontrol_ocid":
"ocid1.opctloperatorcontrol.oc1..aaaaaaaa52eqysdkogsv2qd6apw3iafsrq5rxr
hqu4ninanpd3dwmc5ns4ca"
    }
  }
}
```


Example 7-3 Reference Event for Access Request - AutoApprove


```
{
  "eventType":
"com.oraclecloud.operatorcontrol.autoapproveaccessrequest",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
```

```
  "source": "OperatorAccessControl",
  "eventId": "00d1a1f7-ab1b-4810-8f94-41b4328cf75d",
  "eventTime": "2021-08-04T16:40:19.428Z",
  "contentType": "application/json",
  "data": {
     "eventGroupingId": null,
     "eventName": "AutoApproveAccessRequest",
     "compartmentId":
"ocid1.compartment.oc1..aaaaaaaa4fboeyqkh2h4nft34qgdavsxmd7wgb2erbtvaks5f477q
tn2qc5a",
     "compartmentName": "ccavcn",
     "resourceName": "OpCtl Dev AVM",
     "resourceId":
"ocid1.autonomousvmcluster.oc1.sea.abzwkljspg36g7vt2iuze7xpbt7zzivxeeyesngdto
rk3nscaqar05adm0102clu11-avm5",
     "availabilityDomain": "ad2",
     "freeformTags": null,
     "definedTags": null,
     "identity": null,
     "request": null,
     "response": null,
     "stateChange": null,
     "additionalDetails": {
         "accessRequestId":
"ocid1.opctlaccessrequest.oc1.iad.aaaaaaaaeut2ul7yzz437g3axvxszjqeevabgej6twv
rqmb5ocryte24hbpa"
     }
  }
}
```


Example 7-4 Reference Event for Access Request - Create


```
{
  "eventType": "com.oraclecloud.operatorcontrol.createaccessrequest",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "OperatorAccessControl",
  "eventId": "cfa7a0f0-579c-4bc4-b1d7-e403d9597eb8",
  "eventTime": "2021-08-04T16:40:19.455Z",
  "contentType": "application/json",
  "data": {
     "eventGroupingId": null,
     "eventName": "CreateAccessRequest",
     "compartmentId":
"ocid1.compartment.oc1..aaaaaaaa4fboeyqkh2h4nft34qgdavsxmd7wgb2erbtvaks5f477q
tn2qc5a",
     "compartmentName": "ccavcn",
     "resourceName": "AccessRequest",
     "resourceId":
"ocid1.autonomousvmcluster.oc1.sea.abzwkljspg36g7vt2iuze7xpbt7zzivxeeyesngdto
rk3nscaqar05adm0102clu11-avm5",
     "availabilityDomain": "ad2",
     "freeformTags": null,
     "definedTags": null,
```

```
      "identity": null,
      "request": null,
      "response": {
         "status": "200",
         "responseTime": "2021-08-04T16:40:19.455Z",
         "headers": null,
         "payload": {
             "responsePayload":
"{\"id\":\"ocid1.opctlaccessrequest.oc1.iad.aaaaaaaaeut2ul7yzz437g3axvx
szjqeevabgej6twvrqmb5ocryte24hbpa\",\"requestId\":\"REQ2021080416401866
2\",\"accessReasonSummary\":\"testing avm notification
1\",\"resourceId\":\"ocid1.autonomousvmcluster.oc1.sea.abzwkljspg36g7vt
2iuze7xpbt7zzivxeeyesngdtork3nscaqar05adm0102clu11-
avm5\",\"resourceName\":\"OpCtl Dev
AVM\",\"compartmentId\":\"ocid1.compartment.oc1..aaaaaaaa4fboeyqkh2h4nf
t34qgdavsxmd7wgb2erbtvaks5f477qtn2qc5a\",\"resourceType\":\"AUTONOMOUSV
MCLUSTER\",\"actionRequestsList\":[\"Autonomous Exadata VM Cluster
Full
Access\"],\"severity\":\"S4\",\"duration\":24,\"extendDuration\":0,\"is
AutoApproved\":true,\"lifecycleState\":\"PREAPPROVED\",\"timeOfCreation
\":1628095219006,\"timeOfModification\":1628095219222,\"userId\":\"Syst
em\",\"approverComment\":\"Auto
Approving\",\"opctlId\":\"ocid1.opctloperatorcontrol.oc1.iad.aaaaaaaa73
dyogjdvh4qkyocwpoii2s7tormmokvl3lbdi76kr4fpxvebsaq\",\"opctlName\":\"hp
_autonomous_all_approve_1\",\"systemMessage\":\"Test
msg\",\"auditType\":[\"command-audit\"]}"
          },
         "message":
"com.oraclecloud.operatorcontrol.createaccessrequest"
    },
    "stateChange": null,
     "additionalDetails": {
        "accessRequestId":
"ocid1.opctlaccessrequest.oc1.iad.aaaaaaaaeut2ul7yzz437g3axvxszjqeevabg
ej6twvrqmb5ocryte24hbpa",
        "exadatainfrastructure_name": "OpCtl Dev AVM",
        "exadatainfrastructure_ocid":
"ocid1.autonomousvmcluster.oc1.sea.abzwkljspg36g7vt2iuze7xpbt7zzivxeeye
sngdtork3nscaqar05adm0102clu11-avm5",
        "opCtlId":
"ocid1.opctloperatorcontrol.oc1.iad.aaaaaaaa73dyogjdvh4qkyocwpoii2s7tor
mmokvl3lbdi76kr4fpxvebsaq",
        "opCtlName": "hp_autonomous_all_approve_1",
        "operatorId":
"ocid1.user.oc1..aaaaaaaaythelnxpc775wp6tjwwc3kkipzilregyl4iy4pic5yvpsk
3ol5oa",
       "reason": "testing avm notification 1"
    }
 }
}
```

Example 7-5 Reference Event for add Shared Operator


```
{
  "eventType": "com.oraclecloud.OperatorAccessControl.AddSharedOperator",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "OperatorAccessControl",
  "eventId": "f68ba0f3-e58c-44da-8820-76dcfd2ba5dd",
  "eventTime": "2020-09-11T11:36:14.870Z",
  "contentType": "application/json",
  "data": {
    "eventGroupingId": null,
    "eventName": "AddSharedOperator",
    "compartmentId":
"ocid1.compartment.oc1..aaaaaaaa4fboeyqkh2h4nft34qgdavsxmd7wgb2erbtvaks5f477q
tn2qc5a",
    "compartmentName": "ccavcn",
    "resourceName": "AccessRequest",
    "resourceId":
"ocid1.exadatainfrastructure.oc1.sea.abzwkljs5syf3f2pbypg5hn3zibypiqedccnomex
cpd6judr5ecqijavkjyq",
    "availabilityDomain": "ad1",
    "freeformTags": null,
    "definedTags": null,
    "identity": null,
    "request": {
      "id": "request-policy-12345",
      "path": "",
      "action": "POST",
      "parameters": {
        "requestData": [
          "{\"publicKey\":\"ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCWqpc33qla70w4M0bXxur2EB53HBFypX3ZscYw8rLDD9BPT
FknVdUBsDdjtqsDL0rKVtyJPjcV/
0Tx5lqqAnoJ3A5YD2HrYpiec25MC1kAg1uprXvfz5KOQJazFqSWZcgD4eCSv5FwSOcqrmntZxc+03
QbPFGedkr3O5TRRaheMd9L7eOZGZpDKQolawnZDPf1fejfb7uUjISf/
6yLnn6Wd8qUBTOd1gxllOLixC7Dsr3m7umje3auxqCvzr6KkggrkoTfCaFbd2uonEPL+DZgGlp9q/
a30Qhcw4Ia5C95Bu3lUzV/
hcBvKQAsqZBjUUr5mbJ73DR5FfqFCsjwwqvf\",\"emailId\":\"hprabhakara@gmail.com\",
\"reason\":\"adding new user for analyzing some issue in
scaqak01adm0304\",\"nationality\":\"USA\",\"soilLocation\":\"USA\"}"
        ]
      },
      "headers": null
    },
    "response": {
      "status": "202",
      "responseTime": "2020-09-11T11:36:14.870Z",
      "headers": null,
      "payload": null,
      "message": "com.oraclecloud.operatorcontrol.addsharedoperator"
    },
    "stateChange": null,
    "additionalDetails": {
      "accessRequestId":
```

```
"ocid1.opctlaccessrequest.oc1..aaaaaaaalovaxbsvmbzlf4twcds5ymghqwe4aoq4
kco2skdc3elqn5tspkpa",
      "exadatainfrastructure_name": "scaqak01adm0304_jyq",
      "exadatainfrastructure_ocid":
"ocid1.exadatainfrastructure.oc1.sea.abzwkljs5syf3f2pbypg5hn3zibypiqedc
cnomexcpd6judr5ecqijavkjyq",
      "operatorcontrol_name": "all preapproved opcontrol policy",
      "operatorcontrol_ocid":
"ocid1.opctloperatorcontrol.oc1..aaaaaaaa52eqysdkogsv2qd6apw3iafsrq5rxr
hqu4ninanpd3dwmc5ns4ca"
    }
  }
}
```


Example 7-6 Reference Event for Access Request - Reject


```
{
  "eventType": "com.oraclecloud.operatorcontrol.rejectaccessrequest",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "OperatorAccessControl",
  "eventId": "49ebde1a-9a95-4a55-bebf-4aa347f19c0e",
  "eventTime": "2020-09-11T13:34:50.980Z",
  "contentType": "application/json",
  "data": {
    "eventGroupingId": null,
    "eventName": "RejectAccessRequest",
    "compartmentId":
"ocid1.compartment.oc1..aaaaaaaa4fboeyqkh2h4nft34qgdavsxmd7wgb2erbtvaks
5f477qtn2qc5a",
    "compartmentName": "ccavcn",
    "resourceName": "AccessRequest",
    "resourceId":
"ocid1.exadatainfrastructure.oc1.sea.abzwkljs5syf3f2pbypg5hn3zibypiqedc
cnomexcpd6judr5ecqijavkjyq",
    "availabilityDomain": "AD1",
    "freeformTags": null,
    "definedTags": null,
    "identity": {
      "principalName": "kailash.vimal@oracle.com",
      "principalId":
"ocid1.user.oc1..aaaaaaaaaazh2gydmfjnl3sstigrjac4z5tvvn4zkt2khofzfumawo
haynba",
      "authType": "natv",
      "callerName": null,
      "callerId": null,
      "tenantId":
"ocid1.tenancy.oc1..aaaaaaaavrjqbg24tohoixm7bju6otfn5au73atpa7d6atxf36z
w2espdu3q",
      "ipAddress": "172.23.128.3",
      "credentials":
"ocid1.tenancy.oc1..aaaaaaaavrjqbg24tohoixm7bju6otfn5au73atpa7d6atxf36z
w2espdu3q/
ocid1.user.oc1..aaaaaaaaaazh2gydmfjnl3sstigrjac4z5tvvn4zkt2khofzfumawoh
```

```
aynba/b3:39:8d:75:85:1a:01:b0:f8:cd:68:0a:23:05:7b:76",
      "userAgent": "Oracle-JavaSDK/1.15.0 (Linux/
4.1.12-124.28.6.el7uek.x86_64; Java/1.8.0_212; OpenJDK 64-Bit Server VM/
25.212-b04)",
      "consoleSessionId": null
    },
    "request": {
      "id": "request-policy-12345/773E1E920A98D3E2FC2AF46C7E248007/
F5F1D88A5AB2B30E9FDEE3AA1FFCAB4A",
      "path": "/20200630/accessRequests/
ocid1.opctlaccessrequest.oc1..aaaaaaaaj3n6z3nvndxj2f5qi7qjdgnojojaxbs5olfekkj
2xxztddsbwm6a/action/reject",
      "action": "POST",
      "parameters": {},
      "headers": {
        "Accept": [
          "application/json"
        ],
        "Authorization": [
          "Signature headers=\"date (request-target) host content-length
content-type x-content-
sha256\",keyId=\"ocid1.tenancy.oc1..aaaaaaaavrjqbg24tohoixm7bju6otfn5au73atpa
7d6atxf36zw2espdu3q/
ocid1.user.oc1..aaaaaaaaaazh2gydmfjnl3sstigrjac4z5tvvn4zkt2khofzfumawohaynba/
b3:39:8d:75:85:1a:01:b0:f8:cd:68:0a:23:05:7b:76\",algorithm=\"rsa-
sha256\",signature=\"*****\",version=\"1\""
        ],
        "Connection": [
          "keep-alive"
        ],
        "Content-Length": [
          "55"
        ],
        "Content-Type": [
          "application/json"
        ],
        "Date": [
          "Fri, 11 Sep 2020 13:34:50 GMT"
        ],
        "User-Agent": [
          "Oracle-JavaSDK/1.15.0 (Linux/4.1.12-124.28.6.el7uek.x86_64; Java/
1.8.0_212; OpenJDK 64-Bit Server VM/25.212-b04)"
        ],
        "X-Forwarded-For": [
          "209.17.43.241,0.0.0.0"
        ],
        "X-Real-IP": [
          "209.17.43.241"
        ],
        "X-Real-Port": [
          "29932"
        ],
        "oci-original-url": [
          "https://operator-access-control-dev.us-ashburn-1.oci.oc-test.com/
20200630/accessRequests/
```

```
ocid1.opctlaccessrequest.oc1..aaaaaaaaj3n6z3nvndxj2f5qi7qjdgnojojaxbs5o
lfekkj2xxztddsbwm6a/action/reject"
        ],
        "opc-client-info": [
          "Oracle-JavaSDK/1.15.0"
        ],
        "opc-request-id": [
          "request-policy-12345"
        ],
        "opc-retry-token": [
          "aa8c3689-b129-4749-9e09-9692afe9c7b4"
        ],
        "x-content-sha256": [
          "RgyYB+BnP9UxhdhWZ6VRTcJtNaFctHYM9Y6lxQOcDPU="
        ]
      }
    },
    "response": {
      "status": "204",
      "responseTime": "2020-09-11T13:34:51.612Z",
      "headers": {
        "Date": [
          "Fri, 11 Sep 2020 13:34:50 GMT"
        ],
        "opc-request-id": [
          "request-policy-12345/773E1E920A98D3E2FC2AF46C7E248007/
F5F1D88A5AB2B30E9FDEE3AA1FFCAB4A"
        ]
      },
      "payload": null,
      "message": "AccessRequest for
ocid1.exadatainfrastructure.oc1.sea.abzwkljs5syf3f2pbypg5hn3zibypiqedcc
nomexcpd6judr5ecqijavkjyq has been executed "
    },
    "stateChange": {
      "previous": null,
      "current": {
        "AccessRequest": {
          "id":
"ocid1.opctlaccessrequest.oc1..aaaaaaaaj3n6z3nvndxj2f5qi7qjdgnojojaxbs5
olfekkj2xxztddsbwm6a",
          "principalId":
"ocid1.user.oc1..aaaaaaaaaazh2gydmfjnl3sstigrjac4z5tvvn4zkt2khofzfumawo
haynba",
          "requestMap": {
            "action": "POST",
            "path": "",
            "requesetParams": "{\"approverComment\":\"rejected as this
need not be done\"}",
            "requestId": "request-policy-12345"
          },
          "responseMap": {
            "status": "202"
          }
        }
```

```
      }
    },
    "additionalDetails": {
      "accessRequestId":
"ocid1.opctlaccessrequest.oc1..aaaaaaaaj3n6z3nvndxj2f5qi7qjdgnojojaxbs5olfekk
j2xxztddsbwm6a",
      "exadatainfrastructure_name": "scaqak01adm0304_jyq",
      "exadatainfrastructure_ocid":
"ocid1.exadatainfrastructure.oc1.sea.abzwkljs5syf3f2pbypg5hn3zibypiqedccnomex
cpd6judr5ecqijavkjyq",
      "operatorcontrol_name": "restricted preapproved opcontrol policy",
      "operatorcontrol_ocid":
"ocid1.opctloperatorcontrol.oc1..aaaaaaaa2rfpcb6s5ktvibiw3kzwhwjnqje5jvhkjiqs
icikevpyu77xdtca"
    }
  }
}
```

Example 7-7 Reference Event for Access Request - Revoke

```
{
  "eventType": "com.oraclecloud.operatorcontrol.revokeaccessrequest",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "OperatorAccessControl",
  "eventId": "c437d6f6-f378-4736-8ca9-4ebf9f5ca68c",
  "eventTime": "2020-09-11T13:34:51.689Z",
  "contentType": "application/json",
  "data": {
    "eventGroupingId": null,
    "eventName": "RevokeAccessRequest",
    "compartmentId":
"ocid1.compartment.oc1..aaaaaaaa4fboeyqkh2h4nft34qgdavsxmd7wgb2erbtvaks5f477q
tn2qc5a",
    "compartmentName": "ccavcn",
    "resourceName": "AccessRequest",
    "resourceId":
"ocid1.exadatainfrastructure.oc1.sea.abzwkljs5syf3f2pbypg5hn3zibypiqedccnomex
cpd6judr5ecqijavkjyq",
    "availabilityDomain": "AD1",
    "freeformTags": null,
    "definedTags": null,
    "identity": {
      "principalName": "kailash.vimal@oracle.com",
      "principalId":
"ocid1.user.oc1..aaaaaaaaaazh2gydmfjnl3sstigrjac4z5tvvn4zkt2khofzfumawohaynba
",
      "authType": "natv",
      "callerName": null,
      "callerId": null,
      "tenantId":
"ocid1.tenancy.oc1..aaaaaaaavrjqbg24tohoixm7bju6otfn5au73atpa7d6atxf36zw2espd
u3q",
      "ipAddress": "172.23.128.3",
```

```
      "credentials":
"ocid1.tenancy.oc1..aaaaaaaavrjqbg24tohoixm7bju6otfn5au73atpa7d6atxf36z
w2espdu3q/
ocid1.user.oc1..aaaaaaaaaazh2gydmfjnl3sstigrjac4z5tvvn4zkt2khofzfumawoh
aynba/b3:39:8d:75:85:1a:01:b0:f8:cd:68:0a:23:05:7b:76",
      "userAgent": "Oracle-JavaSDK/1.15.0 (Linux/
4.1.12-124.28.6.el7uek.x86_64; Java/1.8.0_212; OpenJDK 64-Bit Server
VM/25.212-b04)",
      "consoleSessionId": null
    },
    "request": {
      "id": "request-policy-12345/E453EAB9C08AAAB77993E80FBBD965E9/
FE3768C7135F41A65981F9B1950D1B21",
      "path": "/20200630/accessRequests/
ocid1.opctlaccessrequest.oc1..aaaaaaaau5r3vhpgdu4k5svowjqydkh6qugynwyoe
b3egep4qdi4fvuoidla/action/revoke",
      "action": "POST",
      "parameters": {},
      "headers": {
        "Accept": [
          "application/json"
        ],
        "Authorization": [
          "Signature headers=\"date (request-target) host content-
length content-type x-content-
sha256\",keyId=\"ocid1.tenancy.oc1..aaaaaaaavrjqbg24tohoixm7bju6otfn5au
73atpa7d6atxf36zw2espdu3q/
ocid1.user.oc1..aaaaaaaaaazh2gydmfjnl3sstigrjac4z5tvvn4zkt2khofzfumawoh
aynba/
b3:39:8d:75:85:1a:01:b0:f8:cd:68:0a:23:05:7b:76\",algorithm=\"rsa-
sha256\",signature=\"*****\",version=\"1\""
        ],
        "Connection": [
          "keep-alive"
        ],
        "Content-Length": [
          "41"
        ],
        "Content-Type": [
          "application/json"
        ],
        "Date": [
          "Fri, 11 Sep 2020 13:34:51 GMT"
        ],
        "User-Agent": [
          "Oracle-JavaSDK/1.15.0 (Linux/4.1.12-124.28.6.el7uek.x86_64;
Java/1.8.0_212; OpenJDK 64-Bit Server VM/25.212-b04)"
        ],
        "X-Forwarded-For": [
          "209.17.43.241,0.0.0.0"
        ],
        "X-Real-IP": [
          "209.17.43.241"
        ],
        "X-Real-Port": [
```

```
          "29932"
        ],
        "oci-original-url": [
          "https://operator-access-control-dev.us-ashburn-1.oci.oc-test.com/
20200630/accessRequests/
ocid1.opctlaccessrequest.oc1..aaaaaaaau5r3vhpgdu4k5svowjqydkh6qugynwyoeb3egep
4qdi4fvuoidla/action/revoke"
        ],
        "opc-client-info": [
          "Oracle-JavaSDK/1.15.0"
        ],
        "opc-request-id": [
          "request-policy-12345"
        ],
        "opc-retry-token": [
          "7c6dbdff-419b-4275-be3a-db16bba9c239"
        ],
        "x-content-sha256": [
          "DIRn1fPko/9JuYnwL5vzFO0I7kuOp+coAzeY8by4Txk="
        ]
      }
    },
    "response": {
      "status": "204",
      "responseTime": "2020-09-11T13:34:53.463Z",
      "headers": {
        "Date": [
          "Fri, 11 Sep 2020 13:34:51 GMT"
        ],
        "opc-request-id": [
          "request-policy-12345/E453EAB9C08AAAB77993E80FBBD965E9/
FE3768C7135F41A65981F9B1950D1B21"
        ]
      },
      "payload": null,
      "message": "AccessRequest for
ocid1.exadatainfrastructure.oc1.sea.abzwkljs5syf3f2pbypg5hn3zibypiqedccnomexc
pd6judr5ecqijavkjyq has been executed "
    },
    "stateChange": {
      "previous": null,
      "current": {
        "AccessRequest": {
          "id":
"ocid1.opctlaccessrequest.oc1..aaaaaaaau5r3vhpgdu4k5svowjqydkh6qugynwyoeb3ege
p4qdi4fvuoidla",
          "principalId":
"ocid1.user.oc1..aaaaaaaaaazh2gydmfjnl3sstigrjac4z5tvvn4zkt2khofzfumawohaynba
",
          "requestMap": {
            "action": "POST",
            "path": "",
            "requesetParams": "{\"approverComment\":\"revoked by
Customer\"}",
            "requestId": "request-policy-12345"
```

```
          },
          "responseMap": {
            "status": "202"
          }
        }
      }
    },
    "additionalDetails": {
      "accessRequestId":
"ocid1.opctlaccessrequest.oc1..aaaaaaaau5r3vhpgdu4k5svowjqydkh6qugynwyo
eb3egep4qdi4fvuoidla",
      "exadatainfrastructure_name": "scaqak01adm0304_jyq",
      "exadatainfrastructure_ocid":
"ocid1.exadatainfrastructure.oc1.sea.abzwkljs5syf3f2pbypg5hn3zibypiqedc
cnomexcpd6judr5ecqijavkjyq",
      "operatorcontrol_name": "restricted preapproved opcontrol
policy",
      "operatorcontrol_ocid":
"ocid1.opctloperatorcontrol.oc1..aaaaaaaa2rfpcb6s5ktvibiw3kzwhwjnqje5jv
hkjiqsicikevpyu77xdtca"
    }
  }
}
```


Example 7-8 Reference Event for Access Request - Expired


```
{
  "eventType":
"com.oraclecloud.OperatorAccessControl.ExpireAccessRequest",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "OperatorAccessControl",
  "eventId": "0739bacf-7c3a-4ff5-a477-9c9fc7482ba1",
  "eventTime": "2020-09-11T12:11:37.964Z",
  "contentType": "application/json",
  "data": {
    "eventGroupingId": null,
    "eventName": "ExpireAccessRequest",
    "compartmentId":
"ocid1.compartment.oc1..aaaaaaaa4fboeyqkh2h4nft34qgdavsxmd7wgb2erbtvaks
5f477qtn2qc5a",
    "compartmentName": "ccavcn",
    "resourceName": "OpCtl SAR ExaCC (scaqae08adm0304clu5)",
    "resourceId":
"ocid1.exadatainfrastructure.oc1.sea.abzwkljrjlviym5wek52ccc67yoqzbf37k
yz7rsq43nyb6am2phny57qho7q",
    "availabilityDomain": "ad2",
    "freeformTags": null,
    "definedTags": null,
    "identity": null,
    "request": null,
    "response": null,
    "stateChange": null,
    "additionalDetails": {
```

```
      "accessRequestId":
"ocid1.opctlaccessrequest.oc1..aaaaaaaaiilwvp3pu4kiz62d5k4qjemxoerzrpsdqbk67k
xq64yusefsfcsa"
    }
  }
}
```

Example 7-9 Reference Event for Access Request - Closed

```
{
  "eventType": "com.oraclecloud.OperatorAccessControl.CloseAccessRequest",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "OperatorAccessControl",
  "eventId": "e2a56a89-bebc-47c0-b223-4c6dd8adbec6",
  "eventTime": "2020-09-11T13:34:59.248Z",
  "contentType": "application/json",
  "data": {
    "eventGroupingId": null,
    "eventName": "CloseAccessRequest",
    "compartmentId":
"ocid1.compartment.oc1..aaaaaaaa4fboeyqkh2h4nft34qgdavsxmd7wgb2erbtvaks5f477q
tn2qc5a",
    "compartmentName": "ccavcn",
    "resourceName": "AccessRequest",
    "resourceId":
"ocid1.exadatainfrastructure.oc1.sea.abzwkljs5syf3f2pbypg5hn3zibypiqedccnomex
cpd6judr5ecqijavkjyq",
    "availabilityDomain": "ad1",
    "freeformTags": null,
    "definedTags": null,
    "identity": null,
    "request": {
      "id": "request-policy-12345",
      "path": "",
      "action": "POST",
      "parameters": {
        "requestData": [
          "{\"description\":\"closing acessrequest by USER_OCID_ALL as the
work is finished\"}"
        ]
      },
      "headers": null
    },
    "response": {
      "status": "202",
      "responseTime": "2020-09-11T13:34:59.248Z",
      "headers": null,
      "payload": null,
      "message": "com.oraclecloud.operatorcontrol.closedaccessrequest"
    },
    "stateChange": null,
    "additionalDetails": {
      "accessRequestId":
```

```
"ocid1.opctlaccessrequest.oc1..aaaaaaaambvqfgtb76dva566k4rwi3yev73abd67
5wyvx34rw47tyod5s6va",
      "exadatainfrastructure_name": "scaqak01adm0304_jyq",
      "exadatainfrastructure_ocid":
"ocid1.exadatainfrastructure.oc1.sea.abzwkljs5syf3f2pbypg5hn3zibypiqedc
cnomexcpd6judr5ecqijavkjyq",
      "operatorcontrol_name": "restricted preapproved opcontrol
policy",
      "operatorcontrol_ocid":
"ocid1.opctloperatorcontrol.oc1..aaaaaaaa2rfpcb6s5ktvibiw3kzwhwjnqje5jv
hkjiqsicikevpyu77xdtca"
    }
  }
}
```


Example 7-10 Reference Event for Access Request - Extend


```
{
  "eventType":
"com.oraclecloud.OperatorAccessControl.ExtendAccessRequest",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "OperatorAccessControl",
  "eventId": "282f6c6b-a1c2-4e63-b0e4-b3ec211bb3a7",
  "eventTime": "2020-09-11T14:25:08.871Z",
  "contentType": "application/json",
  "data": {
    "eventGroupingId": null,
    "eventName": "ExtendAccessRequest",
    "compartmentId":
"ocid1.compartment.oc1..aaaaaaaa4fboeyqkh2h4nft34qgdavsxmd7wgb2erbtvaks
5f477qtn2qc5a",
    "compartmentName": "ccavcn",
    "resourceName": "AccessRequest",
    "resourceId":
"ocid1.exadatainfrastructure.oc1.sea.abzwkljs5syf3f2pbypg5hn3zibypiqedc
cnomexcpd6judr5ecqijavkjyq",
    "availabilityDomain": "ad1",
    "freeformTags": null,
    "definedTags": null,
    "identity": null,
    "request": {
      "id": "request-policy-12345",
      "path": "",
      "action": "POST",
      "parameters": {
        "requestData": [
          "{\"description\":\"request for extension\",\"duration\":2}"
        ]
      },
      "headers": null
    },
    "response": {
      "status": "202",
```

```
      "responseTime": "2020-09-11T14:25:08.871Z",
      "headers": null,
      "payload": null,
      "message": "com.oraclecloud.operatorcontrol.extendaccessrequest"
    },
    "stateChange": null,
    "additionalDetails": {
      "accessRequestId":
"ocid1.opctlaccessrequest.oc1..aaaaaaaakabn5u3nb4c5xwxvpa6ewn7pa4wtuzmqpnvugp
5pmnazr3zz75vq",
      "exadatainfrastructure_name": "scaqak01adm0304_jyq",
      "exadatainfrastructure_ocid":
"ocid1.exadatainfrastructure.oc1.sea.abzwkljs5syf3f2pbypg5hn3zibypiqedccnomex
cpd6judr5ecqijavkjyq",
      "operatorcontrol_name": "restricted preapproved opcontrol policy",
      "operatorcontrol_ocid":
"ocid1.opctloperatorcontrol.oc1..aaaaaaaa2rfpcb6s5ktvibiw3kzwhwjnqje5jvhkjiqs
icikevpyu77xdtca"
    }
  }
}
```


Example 7-11 Reference Event for Operator - Login


```
{
  "eventType": "com.oraclecloud.OperatorAccessControl.operatorlogin",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "OperatorAccessControl",
  "eventId": "1184e9a9-236d-41de-a7ab-6448ed4849bd",
  "eventTime": "2020-09-04T18:27:00.000Z",
  "contentType": "application/json",
  "data": {
    "eventGroupingId": null,
    "eventName": "operatorlogin",
    "compartmentId":
"ocid1.compartment.oc1..aaaaaaaa4fboeyqkh2h4nft34qgdavsxmd7wgb2erbtvaks5f477q
tn2qc5a",
    "compartmentName": "ccavcn",
    "resourceName": "scaqak01adm0304",
    "resourceId":
"ocid1.exadatainfrastructure.oc1.sea.abzwkljs5syf3f2pbypg5hn3zibypiqedccnomex
cpd6judr5ecqijavkjyq",
    "availabilityDomain": "ad1",
    "freeformTags": null,
    "definedTags": null,
    "identity": null,
    "request": null,
    "response": {
      "status": "200",
      "responseTime": "2020-09-04T18:27:00.000Z",
      "headers": null,
      "payload": null,
      "message": "com.oraclecloud.OperatorAccessControl.operatorlogin"
```

```
    },
    "stateChange": {
      "previous": null,
      "current": {
        "OperatorAccessControl":
"{\"EventName\":\"cca_audtilog_ocid1.opctlaccessrequest.oc1..aaaaaaaanb
jh226h7nhfewx34sfdkojsqapnu3dof6cnkzoypxy27jk2f55q\",\"DisplayName\":\"
operatorlogin\"}"
      }
    },
    "additionalDetails": {
      "desthost": "10.31.18.82",
      "loginId": "9c649b4afafa4e54bcd3d95698346ceb",
      "accessRequestId":
"ocid1.opctlaccessrequest.oc1..aaaaaaaanbjh226h7nhfewx34sfdkojsqapnu3do
f6cnkzoypxy27jk2f55q"
    }
  }
}
```

Example 7-12 Reference Event for Operator - Logout

```
{
  "eventType": "com.oraclecloud.OperatorAccessControl.operatorlogout",
  "cloudEventsVersion": "0.1",
  "eventTypeVersion": "2.0",
  "source": "OperatorAccessControl",
  "eventId": "9a0783fb-66cc-470e-a124-5a0bd0e80857",
  "eventTime": "2020-09-04T18:27:28.000Z",
  "contentType": "application/json",
  "data": {
    "eventGroupingId": null,
    "eventName": "operatorlogout",
    "compartmentId":
"ocid1.compartment.oc1..aaaaaaaa4fboeyqkh2h4nft34qgdavsxmd7wgb2erbtvaks
5f477qtn2qc5a",
    "compartmentName": "ccavcn",
    "resourceName": "scaqak01adm0304",
    "resourceId":
"ocid1.exadatainfrastructure.oc1.sea.abzwkljs5syf3f2pbypg5hn3zibypiqedc
cnomexcpd6judr5ecqijavkjyq",
    "availabilityDomain": "ad1",
    "freeformTags": null,
    "definedTags": null,
    "identity": null,
    "request": null,
    "response": {
      "status": "200",
      "responseTime": "2020-09-04T18:27:28.000Z",
      "headers": null,
      "payload": null,
      "message": "com.oraclecloud.OperatorAccessControl.operatorlogout"
    },
    "stateChange": {
```

```
      "previous": null,
      "current": {
        "OperatorAccessControl":
"{\"EventName\":\"cca_audtilog_ocid1.opctlaccessrequest.oc1..aaaaaaaanbjh226h
7nhfewx34sfdkojsqapnu3dof6cnkzoypxy27jk2f55q\",\"DisplayName\":\"operatorlogo
ut\"}"
      }
    },
    "additionalDetails": {
      "desthost": "?",
      "loginId": "9c649b4afafa4e54bcd3d95698346ceb",
      "accessRequestId":
"ocid1.opctlaccessrequest.oc1..aaaaaaaanbjh226h7nhfewx34sfdkojsqapnu3dof6cnkz
oypxy27jk2f55q"
    }
  }
}
```


Viewing Audit Log Events

Audit provides records of API operations performed against supported services as a list of log events.

For more information on searching logs, see Using the Console.

Related Topics

- Overview of Audit
- Viewing Audit Log Events
- Setting Audit Log Retention Period

A

Operator Access Control Reference

To find out more about Operator Access Control, refer to these topics.

- Example of Using Operator Access Control
  As an administrator, see how you can set up operator access controls that define the actions an Oracle operator can perform on a set of resources on your Exadata systems.

Example of Using Operator Access Control

As an administrator, see how you can set up operator access controls that define the actions an Oracle operator can perform on a set of resources on your Exadata systems.

Suppose an administrator has completed a review of administrative policy requirements and divided the Exadata systems into the following Operator Controls:

Example A-1 Creating Operator Policies for Containers on Exadata Cloud

Table A-1 Example of Operator Controls Configuration

Exadata Systems	Compartment	Compliance Regime	Administrator User Group	Operator Control User Group
Exadata Systems E1-E10	`prod-pci`	PCI	`pci_admin`, `pci_admin_2`	`top-security-users`
Exadata Systems E11-E15	`prod-hipaa`	HIPAA	`hipaa_admin`	`top-security-users`
Exadata Systems E16-E20	`prod-soc`	SOC-2	`soc_admin`	`top-security-users`
Exadata Systems E21-E25	`devops`	None	`devops_admin`	`devops_admin`
Exadata Systems E26-E30	`func-qa`	None	`qa_admin`	`qa_admin`
Exadata Systems E31-40	`perf-qa`	None	`perf_admin`	`psr-admin`

In this hypothetical case, there are six compartments, and five user groups that administer the compartments.

Since the Payment Card Industry (PCI), Service Organization Control 2 (SOC-2), and Health Insurance Portability and Accountability Act (HIPAA) compliance systems are governed by different compliance regimes, there are two ways to create Operator Controls governing them. One way is to create a distinct Operator Control for each compliance regime. The other way is to create the strictest Operator Control required, and have all three compliance categories of systems be governed by the same Operator Control. In this scenario, since the Functional-QA (`func-qa`) and Performance-QA (`perf-qa`) compartments are not under the

governance of any compliance regime, and the compartments are administered by the same user group, we can have a single Operator Control governing both of them.

Suppose you are the policy administrator for these systems. To create the Operator Policy controls for this configuration, you create one policy to govern all systems under compliance regimes, one policy for development operations (`devops`) deployment, and one option for quality assurance (QA) systems. The controls themselves are placed in a compartment named "policies", which is manageable only by the "top-security-users" group. The following CLI commands are indicative and adjusted for readability, for examples names are used in place of OCIDs. For more information, refer to the CLI guide.

```
/* Ensure only the top_security group has permission on the policies
compartment */
allow group top_security to manage operator-control in compartment
policies

/* create operator controls */
oci opctl operator-control create --operator-control-name "prod-opctl-
policy" --pre-approved-op-action-list '["INFRA_DIAG"]' --approver-
groups-list '["top_security_group"]' --is-fully-pre-approved false --
description "Production Operator Control" --compartment-id "policies"
oci opctl operator-control create --operator-control-name "devops-
opctl-policy" --pre-approved-op-action-list '["INFRA_DIAG",
"INFRA_UPDATE_RESTART"] --approver-groups-list '["devops-admin"]' --is-
fully-pre-approved false --description "Devops Operator Control" --
compartment-id "policies"
oci opctl operator-control create --operator-control-name "qa-opctl-
policy" --is-fully-pre-approved true --approver-groups-list '["qa-
admin, psr-admin"]' --description "QA/Test Operator Control" --
compartment-id "policies"

/* Ensure users have assignment permissions on the target Exadata.
They also need read privileges on the policies. An example for pci-
admin is given below*/
allow group pci-admin to manage operator-control-assignment in
compartment prod-pci;

/* Ensure the user groups have manage operator control request
privileges in there respective compartments */
allow group pci-sec-controller to manage operator-control-access-
request in compartment prod-pci
allow group hipaa-sec-controller to manage operator-control-access-
request in compartment prod-hipaa
allow group soc-sec-controller to manage operator-control-access-
request in compartment prod-soc
allow group devops-sec-controller to manage operator-control-access-
request in compartment devops
allow group qa-sec-controller to manage operator-control-access-
request in compartment func-qa
allow group perf-sec-controller to manage operator-control-access-
request in compartment perf-qa
allow group pci-admin to read operator-control in compartment policies;
```

Now that we have created the relevant user groups and given permissions. Users from these user groups can go ahead and bring the respective Exadata systems under control. The exadata systems should be assigned with the respective controls. The assignments themselves reside on the same compartments as the exadata systems. As mentioned earlier the following commands are indicative and adapted for readability. For more information, refer to the CLI guide.

Next, you create the relevant Operator Control policy user groups, and grant them read access to the compartments containing the operator controls that these group members administer:

```
oci opctl operator-control-assignment create --operator-control-id "prod-
opctl-policy" --compartment-id "prod-pci" --resource-compartment-id "prod-
pci" --resource-id "exadata-OCID..E1..E10" --resource-name "Exadata E1-E10"
--is-enforced-always true
oci opctl operator-control-assignment create --operator-control-id "prod-
opctl-policy" --compartment-id "prod-hipaa" --resource-compartment-id "prod-
hipaa" --resource-id "exadata-OCID..E11..E15" --resource-name "Exadata E11-
E15" --is-enforced-always true
oci opctl operator-control-assignment create --operator-control-id "prod-
opctl-policy" --compartment-id "prod-soc" --resource-compartment-id "prod-
soc" --resource-id "exadata-OCID..E16..E20" --resource-name "Exadata E16-
E20" --is-enforced-always true
oci opctl operator-control-assignment create --operator-control-id "devops-
opctl-policy" --compartment-id "devops" --resource-compartment-id "devops" --
resource-id "exadata-OCID..E21..E25" --resource-name "Exadata E21-E25" --is-
enforced-always true
oci opctl operator-control-assignment create --operator-control-id "qa-opctl-
policy" --compartment-id "func-qa" --resource-compartment-id "func-qa" --
resource-id "exadata-OCID..E26..E30" --resource-name "Exadata E26-E30" --is-
enforced-always true
oci opctl operator-control-assignment create --operator-control-id "qa-opctl-
policy" --compartment-id "perf-qa" --resource-compartment-id "perf-qa" --
resource-id "exadata-OCID..E31..E40" --resource-name "Exadata E31-E40" --is-
enforced-always true
```

You then approve, reject, or revoke the access request permissions for each Operator Control with the groups created above.

Example A-2 Granting an Operator DBA Privileges to Approve Access Requests

Suppose you have granted the group `top-security-users` the Operator Control User Group on several systems, but you decide you want to grant a subset of users in your tenancy to approve or revoke operator access control requests, without making that subset of users members of the `top-security-users` group, which would grant privileges to other tenancy, and other management privileges. To achieve that goal, complete the following steps

1. Create an IAM group, `opctl-prod-pci-operators`.
2. Grant members of that group privileges to grant or revoke access requests on the `prod-pci` compartment.
3. Add the users to whom you want to have these privileges to the `opctl-prod-pci-operators` group.

For example, the following is a list of IAM Policies required for the group to grant or revoke access requests:

```
Allow group opctl-prod-pci-operators to use operator-control-
accessrequest in compartment prod-pci
Allow group opctl-prod-pci-operators to inspect identity-providers in
tenancy
Allow group opctl-prod-pci-operators to inspect groups in tenancy
Allow group opctl-prod-pci-operators to inspect users in tenancy
```

Index