ORACLE

Oracle Operator Access Control for Exadata Cloud@Customer

A Priviliged Access Management Service for Exadata Cloud@Customer

September 28, 2021, Version 3.05

Public

Purpose statement

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

Disclaimer

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

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

Table of contents

List of images

List of tables

Overview

Oracle Operator Access Control (OpCtl) is an Oracle Cloud Infrastructure (OCI) access control service that gives customers a technical mechanism to better control how Oracle staff can access their Exadata Cloud@Customer (ExaC@C) infrastructure to help customers meet common requirements in regulated industries. The description of controls in this paper is a summary of the Operator Access Control product documentation, and intended to help customer security staff evaluate the OpCtl service as a potential compensating control to permit ExaC@C adoption.

ExaC@C requires the customer to accept the following service delivery requirements:

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

OpCtl provides customers interfaces with the following controls:

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

Security staff evaluating OpCtl should also review the related documentation that describes additional controls in the ExaC@C service and the Oracle Cloud Infrastructure control plane, including:

- Exadata Cloud@Customer Security Controls
- Exadata Cloud@Customer Security Guide
- Oracle Cloud Infrastructure Security Architecture
- Oracle Cloud Infrastructure Security Guide
- Oracle Software Security Assurance Policy
- Oracle Incident Response Policy
- Oracle Data Processing Agreement

Introduction

Cloud computing is fundamentally different from traditional on-premises computing. In the traditional model, organizations are typically in full control of their technology infrastructure located on-premises (e.g., physical control of the hardware, full control over the technology stack in production). In the cloud, organizations must leverage resources and practices that are under the control of the cloud service provider. In effect, managing security and privacy in the cloud is a shared responsibility between the cloud customer and the cloud service provider.

In the Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) cloud models, the cloud service provider manages a subset of the system, such as the infrastructure (cloud provider tenancy), and the customer manages other parts of the system, such as virtual machines, applications, and databases (customer tenancy). Certain regulatory frameworks may require customers to be responsible and controlt the actions any person takes when accessing the system, including the actions by the cloud provider staff in the cloud provider tenancy. To help customers meet these requirements, Oracle customers can use Oracle Operator Access Control (OpCtl) with Exadata Cloud@Customer (ExaC@C) and Autonomous Database Dedicated (ADB-D) on ExaC@C.

OpCtl is an Oracle Cloud Infrastructure (OCI) privileged access management (PAM) service for Exadata Cloud@Customer (ExaC@C). OpCtl provides customers with software interfaces in the customer's tenancy to control and govern if, when, and how Oracle Cloud Operations (Cloud Ops) staff can access the Oracle managed infrastructure in the Oracle tenancy of the ExaC@C service. These controls are a standard part of the ExaC@C service and are available at no extra cost to Oracle customers.

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

The OpCtl service provides segregation of duties where the customer authorizes access and Oracle performs work.

OpCtl preventative security control features include:

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

OpCtl detective security control features include:

- Customer notification when Oracle staff need to access infrastructure
- Individually identifiable audit logging of every command and keystroke executed by Oracle staff
- Customer security monitoring of all commands and keystrokes entered by Oracle staff
- Oracle-supplied record of the Oracle staff identity to the customer when required for any command executed
- Oracle security staff monitoring of all Oracle Cloud Ops staff activities

OpCtl responsive security control features include

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

Service Scope

OpCtl permits the customer to control Oracle human staff access to resources that Oracle staff are chartered to maintain, such as ExaC@C infrastructure. OpCtl does not permit the customer to control software automation access to the ExaC@C infrastructure, or customer access to customer-controlled resources.

Service Architecture

Figure 1 describes the Gen 2 ExaC@C service delivery network architecture.

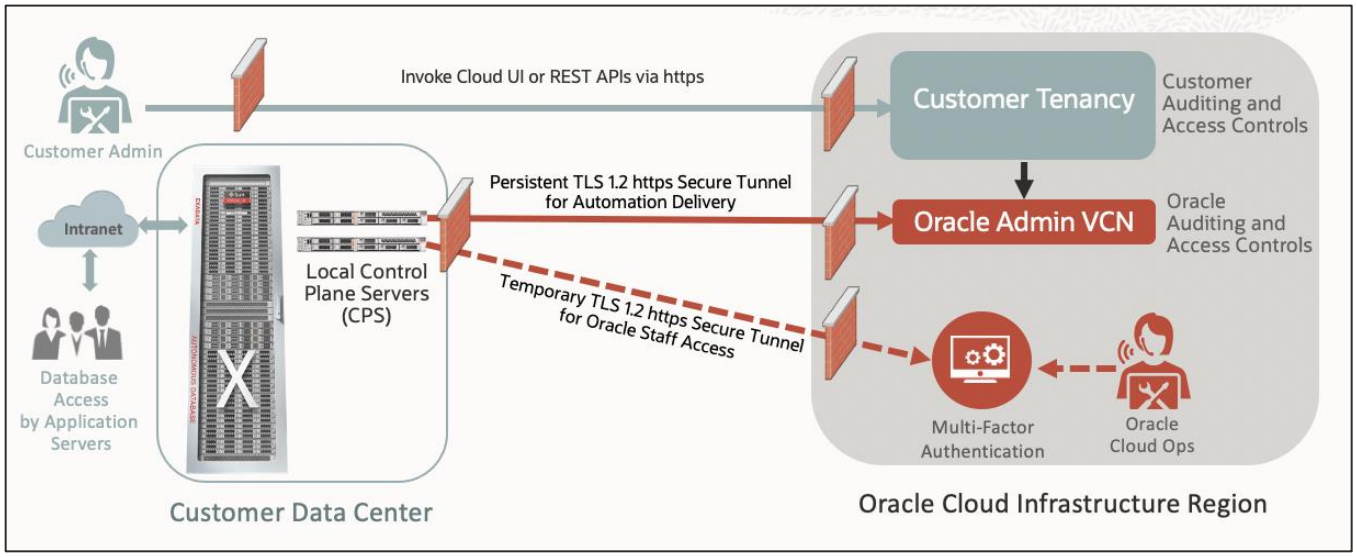

Figure 1: Gen 2 ExaC@C Network Architecture Overview

The following implementation details are relevant to the security model described in Figure 1:

- Customers authenticate to their tenancy with customer-controlled credentials via https protocol; OCI Identity and Access Management (IAM) Service governs customer authentication and access to their tenancy, and is documented at https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm
- The customer's tenancy is secured by the OCI security architecture, documented at https://www.oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf
- The ExaC@C service is secured by the OCI security architecture and the additional software of the ExaC@C service, described at https://www.oracle.com/a/ocom/docs/engineered-systems/exadata/exadata-cloud-at-customer-security-controls.pdf
- Customers apply OpCtl management policies to their ExaC@C infrastructure resources to govern Oracle Cloud Ops access to their ExaC@C infrastructure; this process is secured and controlled by the OCI IAM, described at https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm
- The local Control Plane Servers (CPS) installed in the ExaC@C rack maintain a persistent outbound secure tunnel (layer 7 websocket) secured by TLS 1.2 to an OCI Web Socket Service to support REST API command transmission from the customer's tenancy and from the Oracle Admin Virtual Cloud Network (VCN) to the local CPS
- When the customer authorizes Oracle Cloud Ops to access the ExaC@C infrastructure, a REST API command is sent over the persistent secure tunnel to agents in the ExaC@C infrastructure, and then a temporary secure operator tunnel (layer 7 stunnel) is established from the infrastructure component outbound to a Secure Tunnel Service in OCI

- Oracle Cloud Ops staff use the temporary secure operator tunnel to establish an `ssh` connection where they authenticate as a named user from their Oracle managed device via hardware multi-factor authentication to the customer-authorized infrastructure component

Figure 2 details the major components in the OpCtl `ssh` access flow that occur after the customer has approved access and the OpCtl software has deployed the temporary credentials in the chroot jails on the infrastructure components.

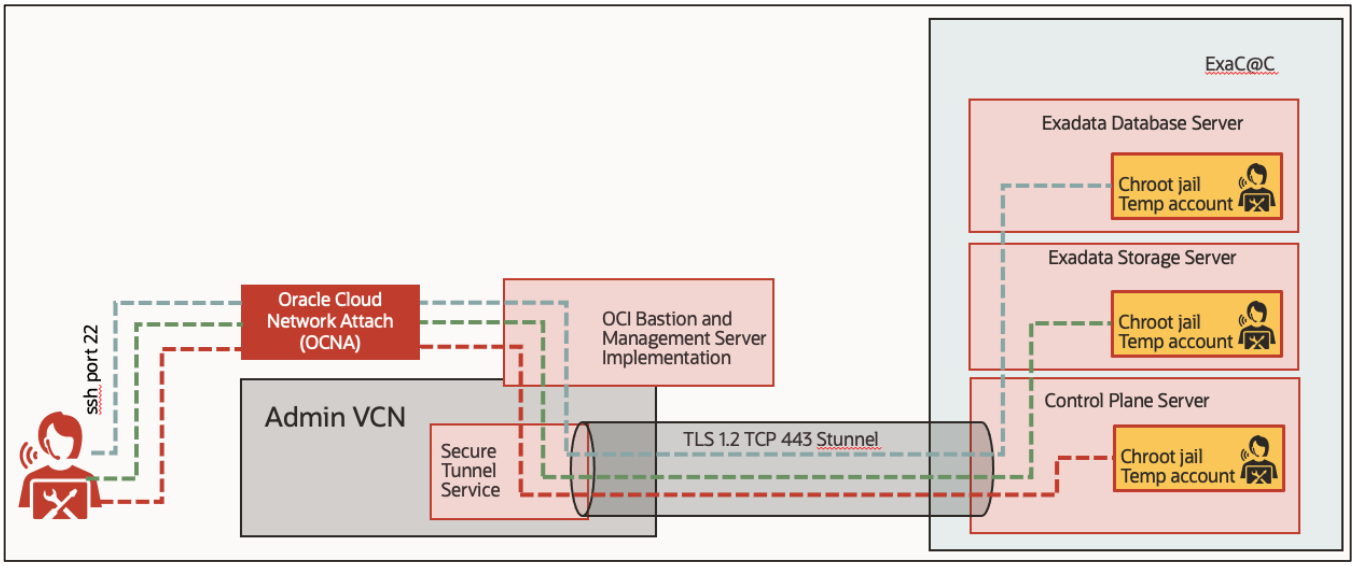

Figure 2: Oracle Operator via ssh over temporary secure tunnel to temporary account deployed in chroot jail

Oracle access to ExaC@C infrastructure includes the following controls implemented by Oracle:

- The Cloud Ops person must connect to the Oracle Cloud Network Attach (OCNA) using their hardware Yubikey (FIPS 140-2 level 3 hardware multi-factor authentication); the end user device is automatically scanned for the following after VPN authentication, and access is denied if the following scanning standards are not met:
  - Compliance with Oracle endpoint/device requirements such as virus scanning software standards (see https://www.oracle.com/corporate/security-practices/corporate/laptop-mobile-devices.html)
  - Compliance with Oracle geographic access control standards (see OCI Consensus Assessment Initiative Questionnaire (CAIQ) for Oracle Cloud Infrastructure (PDF)
  - Compliance with authorization requirements for role-based access (see https://www.oracle.com/corporate/security-practices/corporate/access-control.html)
- The Cloud Ops person must be authorized to access to OCI Bastion and Management servers for the purposes of establishing an `ssh` connection to ExaC@C infrastructure
  - This access is controlled internally at Oracle by Oracle's corporate identity management (OIM) and the internal OCI permissions service
  - Access is tied to job code and implemented in a least-privileged access model, published at https://www.oracle.com/corporate/security-practices/corporate/access-control.html
- The Cloud Ops person uses their Oracle-issued laptop and Oracle-issued Yubikey to authenticate the `ssh` connection from their laptop to the ExaC@C infrastructure
- The Cloud Ops person must have the hardware Yubikey and know the passcode to the hardware Yubikey used to create the access request to authenticate to the temporary account

Service Roles and Responsibilities

The customer has the following responsibilities when controlling Oracle staff access with the OpCtl service:

- Create and apply policies that govern the rules by which a system can be accessed
- Configure notifications and logging per customer standards
- Monitor Oracle staff commands and keystrokes for security and audit purposes
- Revoke or deny access to infrastructure as business and security needs dictate
- Respond to OpCtl Access Requests in a timely manner[1]

When a customer controls Oracle staff access with the OpCtl service, then Oracle:

- Must issue Access Requests to the customer when Oracle staff need to access infrastructure controlled by OpCtl
- May only perform required work within the technical limits imposed by OpCtl controls
- Will associate an identifiable Oracle employee with any commands or keystrokes entered by an Oracle employee on any system managed by OpCtl.

Implications for Service Support and Availability

In the case of pre-approved access for an OpCtl Policy, Oracle staff are permitted access to maintain the service and there are no additional exclusions beyond the standard exclusions of the service. In the case of explicit access approval, Oracle staff cannot access the service until the customer approves the Cloud Ops Access Request. If a customer revokes an Access Request while the request is being processed, then the maintenance action will not be completed.

Oracle Cloud Ops staff work to support the ExaC@C service availability and quality for customers. When customers implement OpCtl to govern Oracle Cloud Ops work, customers must take care to update customer business processes and technology to ensure timely response and approval for OpCtl access requests. If a customer can commit to responding to approve or reject an OpCtl Access Request in 15 minutes or less, then Oracle support operations can execute to maintain service quality and availability.

If a customer cannot commit to responding (approving or rejecting) an OpCtl Access Request in 15 minutes or less, then Oracle Cloud Ops execution efficiency will be degraded and the customer will be exposed to service quality and availablilty reductions. If a customer cannot commit to responding to an OpCtl Access Request in 15 minutes or less, then they should implement preapproval of OpCtl Access Requests.

OpCtl Access Request preapproval can be modified any time to meet changing business and risk management needs. For example, a service implemented for test and development can be managed with pre-approved policies, and when that system is moved to production the policies can be updated to require explicit human approval by select customer staff. OpCtl Access Request preapproval can also be scheduled to permit preapproved access during planned maintenance windows, such as ExaC@C infrastructure software updates, or to have explicit access request approval during sensitive time windows.

OpCtl Access Request preapproval can be configured and modifited for each privilege level (diagnostics, service update/restart, hypervisor, full) so customers can gain the efficiency of preapproval for access with low risk in the context of the specific system.

[1] Timely response to a Cloud Ops access request is required to maintain service quality and availability, and can be achieved by implementing a pre-approved policy; a 15-minute response time is sufficient for practical use cases; longer response times may lead to service outages

Security and Access Controls

OpCtl provides a number of preventative, detective, and responsive security controls.

- **Preventative** controls limit the scope of actions an Oracle Cloud Ops staff can take, such as if and when they can log into the infrastructure, how long they can access the infrastructure, the commands they can run, and the files and devices they can access.
- **Detective** controls show what Oracle Cloud Ops staff are doing and included the commands they are executing and the keystrokes they are entering.
- **Responsive** controls stop Oracle Cloud Ops staff from performing further work and include termination of TCP connections and processes started by the Oracle Cloud Ops staff.

By applying these 3 types of controls, customers can govern access to the ExaC@C infrastructure, prove the scope of work any person performed when accessing the infrastructure, and detect and terminate unauthorized access.

Preventative Controls

This section details the preventative controls OpCtl provides for customers to govern access to ExaC@C infrastructures

Access Controls to Infrastructure

By default there is no account on the infrastructure that permits remote login when OpCtl is used to govern access to infrastructure,. Because of this, customers must take care to monitor and respond to OpCtl access requests so that Oracle Cloud Ops can perform the work necessary to maintain service quality and availability. If customers deny Oracle Cloud Ops access requests, or do not respond to requests in a timely manner, service outages may occur.

When a customer authorizes an OpCtl access, the OpCtl software orchestrates the deployment of a temporary credential to permit access to the target infrastructure by the Oracle Cloud Ops person who created the access request. The technical preventative control that prevents this credential from being used by another person is the Cloud Ops person's hardware Yubikey. This authentication control requires the person making the `ssh` connection to have the physical Yubikey used to make the access request and to know the passcode of the hardware Yubikey.

Access Controls within Infrastructure

After the Cloud Ops person is authorized and authenticated to access the ExaC@C infrastructure, an Oracle Linux chroot jail governs the infrastructure the Cloud Ops person can access.

A chroot jail changes the apparent root directory for a running process and its children. It allows you to run a program with a root directory other than /. The program cannot see or access files outside the designated directory tree. Such an artificial root directory is called a chroot jail, and its purpose is to limit the directory access of a potential attacker. The chroot jail locks down a given process and any user ID that it is using so that all they see is the directory in which the process is running. To the process, it appears that the directory in which it is running is the root directory. Oracle Linux 7 chroot jails are documented at https://docs.oracle.com/en/operating-systems/oracle-linux/7/security/ol7-implement-sec.html#ol7-s3-syssec.

The OpCtl implementation of chroot jails is called an OpCtl Actions, and are described in the Enforcement of Actions in Operator Access Control product documentation. OpCtl Actions define the operations an operator can perform on ExaC@C infrastructure such as the Exadata Database Server Infrastructure (Dom0), Exadata Storage Server (cell/cell server), and Control Plane Servers (CPS). OpCtl Actions are applicable to the ExaC@C infrastructure as whole (all of the Exadata Database Servers, Storage Servers, and CPS in a specified ExaC@C rack), meaning a customer does not specify access to an individual component in the infrastructure. OpCtl does not provide a method to deploy temporary accounts to access the customer VM (DomU).

OpCtl Actions translate Oracle Linux permissions on the target ExaC@C system. The permissions are categorized into file system privileges, command execution privileges, and `su` or `sudo` privileges. The OpCtl Actions are categorized by the nature of the change that can be implemented by the operator on the ExaC@C system. OpCtl provides 4 types of Actions:

- System Diagnostics, which is identified as INFRA_DIAG is intended to be used for diagnosing any issue in the ExaC@C infrastructure layer
- 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
- System Maintenance with Hypervisor 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 Exadata Database Server is required
- Full System Access, which is identified as INFRA_FULL is to be used to offer the Oracle operator maximum flexibility to address complex or unusual situations, including diagnostics of kernel code, firmware, and hardware issues

OpCtl Action: System Diagnostics

System Diagnostics, which is identified as INFRA_DIAG is intended to be used for diagnosing any issue in the ExaC@C infrastructure layer. In cases where Oracle Cloud Ops only has a need to perform diagnostics access, Oracle Cloud Ops will ask for INFRA_DIAG privileges. In cases where Oracle Cloud Ops knows there is a need for an action that cannot be performed with INFRA_DIAG, then Oracle Cloud Ops will ask for the necessary privileges, including INFRA_FULL. Cases that need INFRA_FULL for the purposes of diagnostics include diagnostics of Oracle Linux kernel functionality, such as device drivers, and hardware/firmware fault diagnosis.

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

Table 1 details the chroot jail configuration that governs access and privileges of the temporary account.

Note:

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

Table 1: Diagnostics Action Privileges

ACTION NAME	ACTION IDENTIFIER	OPERATOR PRIVILEGES
System Diagnostics	`INFRA_DIAG`	Oracle Linux user privilege: Non-root. Can `su` to `root`: No `chroot` caged: Yes Directories Readable: Exadata Storage Server:

		`/opt, /proc, /sys, /tmp, /var, /var/log, /usr/lib64, /usr/bin, /usr/etc, /usr/include, /usr/lib, /usr/libexec, /usr/local, /usr/share, /usr/java, /opt/cellconf, /home/cellmonitor/`
		Exadata Database Server Infrastructure:
		`/bin, /lib64, /lib, /opt, /proc, /sys, /tmp, /var, /usr/lib64, /usr/bin, /usr/etc, /usr/include, /usr/lib, /usr/libexec, /usr/local, /usr/share`
		Control Plane Server:
		`/opt, /proc, /sys, /tmp, /var, /usr/lib64, /usr/bin, /usr/etc, /usr/include, /usr/lib, /usr/libexec, /usr/local, /usr/share`
		Files Readable:
		`/var/log/*`
		Directories Writeable:
		Exadata Storage Server: `/var/db, /opt/oracle`
		Exadata Database Server Infrastructure: `/var/db`
		Control Plane Server: `/var/db`
		List of commands executable:
		All commands in
		`/bin, /usr/bin, /usr/local/bin, /sbin/ifconfig, /sbin/ip, /sbin/lspci`
		`cellcli` on Exadata Storage Server
		Can `su` into:
		Cell: `cellmonitor`
		Exadata Database Server Infrastructure: `dbmmonitor`
		Control Plane Server: `ecra, exawatcher, dbmsvc`
		Execute as `root`:
		`cat`
		`head`
		`tail`
		`cp` for files inside `/var/log/*`
		[CPS]: `systemctl`
		Exadata Storage Server Privileges: Act as `cell monitor`.
		Network Privileges: Can `SSH` into all Exadata Database Server Infrastructure, Exadata Storage Servers and Control Plane Servers. The user name is same across all of these.

OpCtl 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 (Exadata Database Server, Exadata Storage Server), to restart specific sub-systems, such as the network, and to restart cell disks.

Table 2 details the chroot jail configuration that governs access and privileges of the temporary account.

Note:

- Be aware that System Maintenance with Restart Privileges action can create significant service availability risk to the system. However, it does not expose any data to risk.
- System Maintenance with Restart Privileges action:
  - Permits the Oracle operator to perform system maintenance activities with `root` privileges. The operator cannot become `root` but can run maintenance commands as `root`.
  - Does not allow the operator to change the audit parameters or access the audit logs; however, the action allows the operator to take the whole ExaC@C system offline.
  - Allows the operators to change configuration of the operating system through permanent changes. For example, the Oracle operator is permitted to change `/etc/` parameters.
  - Permits the Oracle operator to start daemon processes, and to manage the cell disks using the `cell admin` privilege of `cellcli` on Exadata Storage Servers.
  - Permits the Oracle operator to access the manage the cloud orchestration infrastructure on the Control Plane Server, with capability to restart all daemons on the Control Plane Server.

Inheritance: All privileges of System Diagnostics

Table 2: System Maintenance with Restart Privileges

ACTION NAME	ACTION IDENTIFIER	OPERATOR PRIVILEGES
System Maintenance with Restart Privileges	`INFRA_UPDATE_RESTART`	Same as System Diagnostics privilege + the following: Can `su` to `root`: No `chroot` caged: Yes Can `su` into: `exawatcher, dbmsvc, dbmadmin, dbmmonitor` on Exadata Database Server Infrastructure Execute as `root`: `restart, ip, ifconfig, lspci` Exadata Storage Server privileges: `celladmin` in Exadata Storage Server Network Privileges: Can `SSH` into all Exadata Database Server Infrastructure, Exadata Storage Servers and Control Plane Servers. The user name is the same across all of these layers

OpCtl Action: System Maintenance with Hypervisor Access

System Maintenance with Hypervisor Access, which is identified as `INFRA_HYPERVISOR` is intended to be used for diagnostics and maintenance scenarios where VM management on the Exadata Database Server is required.

System Maintenance with VM Control Privileges action is intended to be used for diagnostics and maintenance scenarios where VM management on the Exadata Database Server is required. Any data on the customer VM is treated as customer data. As VM management involves the ability to access the VM data, this action potentially exposes data risk. However, all customer data created in the ExaC@C database is encrypted with TDE and this action does not give any access to the TDE keys of the data stored in Exadata Storage Servers. VM management is required in cases where there are problems with the VM software infrastructure or where a VM configuration needs to be modified. Configuration involves the external aspect of the VMs such as the networks attached, disks attached, or resources (CPU, Memory) allocated. Table 3 details the chroot jail configuration that governs access and privileges of the temporary account.

Note:

- System Maintenance with VM Control Privileges action poses significant data risks and availability risks to the customer. The data risks are exposed due to the fact that the customer VM file systems are accessible through access of VM disks. The availability risks are exposed due to the fact that the VMs can be controlled by the operator.
- System Maintenance with VM Control Privileges action:
  - Allows the operator to perform Xen/KVM management commands with `root` privileges. The operator cannot become `root`. This action is applicable only to the Exadata Database Server.
  - Inherits the privileges from the "System Maintenance with Restart Privileges" action.
  - Does not allow the operator to change operating system parameters of Exadata Database Servers or Exadata Storage Servers. However, this allows the operator to shut down the customer VM and significantly change the configuration of the customer VM.
  - Does not allow the operator to change the configuration of the Oracle Linux Audit service

Inheritance: All privileges of System Maintenance with Restart.

Table 3: System Maintenance with Hypervisor Access Privileges

ACTION NAME	ACTION IDENTIFIER	OPERATOR PRIVILEGES
System Maintenance with Data Access / VM Control Privileges	`INFRA_HYPERVISOR`	Same as "System Maintenance with Restart" privileges + the following: Oracle Linux user privilege: Non-root. Can `su` to `root`: No `chroot` caged: Yes Directories Readable: `/EXAVMIMAGES` on Exadata Database Server Infrastructure `/home/celladmin/` on Exadata Storage Server List of commands executable: `/usr/sbin/xm /usr/sbin/xentop` on Exadata Database Server Infrastructure `cellcli` on Exadata Storage Server Can `su` into: `celladmin` in Exadata Storage Server

		Execute as root:
		`/usr/sbin/xm`
		`/usr/sbin/xentop`
		`/usr/sbin/virsh`
		Exadata Storage Server Privileges: `celladmin`
		Network Privileges: Can `SSH` into all Exadata Database Server Infrastructure, Exadata Storage Servers and Control Plane Servers. The user name is same across all of these.

OpCtl Action: Full System Access

Full System Access, which is identified as INFRA_FULL is necessary to diagnose and resolve issues within the core Oracle Linux operating system, Oracle Linux kernel code, and hardware/firmware issues. Full System Access action is also used when full access of the ExaC@C infrastructure is required, such as access to power distribution units (PDU) and Integrated Lights Out Management (ILOM) console. Access is always limited to non-customer VM layers. Full access means the root privileges on every operating system instance in the ExaC@C system, other than the customer VM. Customers should expect INFRA_FULL access requests for diagnostics related to driver software and hardware devices, as well as for resolution of issues related to driver software and hardware devices. INFRA_FULL access is also required to restart or perform diagnostics and maintenance on infrastructure components that fail to boot.

Table 4 details the chroot jail configuration that governs access and privileges of the temporary account.

Note:

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

Table 4: Full System Access Privileges

ACTION NAME	ACTION IDENTIFIER	OPERATOR PRIVILEGES
Full System Access	INFRA_FULL	Linux User Privilege: Non-root Can `su` to `root`: yes `chroot` 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 Exadata Storage Server privileges: `root` and `celladmin`

		Network Privileges: Can `SSH` into all Exadata Database Server Infrastructure, Exadata Storage Servers and Control Plane Servers. The user name is same across all of these. Also, connect to `root` directly on Exadata Database Server Infrastructure, Exadata Storage Server to using `exassh`

Detective Controls

OpCtl provides operator command and keystroke logging via the Oracle Linux (OL) audit service running on the infrastructure components. The information from the OL audit service is available to the customer via 2 interfaces:

- OCI Logging Service
- Direct send of audit logs in syslog format to customer-supplied IP address or hostname of a customer-controlled syslog server; this is useful for the transmission of the audit logs to a customer Security Information Event Management (SIEM) system

OL audit service content is typically available in the OCI Logging Service within 30 seconds of command execution.

Documentation for the OCI Logging Service is published at https://docs.oracle.com/en-us/iaas/Content/Logging/Concepts/loggingoverview.htm. The OCI Logging Service can be integrated with the OCI Streaming Service to send OpCtl Audit Log information to arbitrary endpoints supported by the OCI Streaming Service. The OCI Streaming Service is published at https://docs.oracle.com/en-us/iaas/Content/Streaming/Concepts/streamingoverview.htm.

Oracle publishes tutorials on how to stream OCI Logs to Splunk at https://docs.oracle.com/en/solutions/logs-stream-splunk/index.html#GUID-8D87CAA4-CD41-4E90-A333-5B04E23DBFAA and https://blogs.oracle.com/cloud-infrastructure/announcing-the-oracle-cloud-infrastructure-logging-plugin-for-splunk.

Responsive Controls

Customers may use OpCtl interfaces to revoke Cloud Ops access for a specific access request if the customer suspects unauthorized actions. Customers are encouraged to file a security Support Request (SR) whenever unauthorized actions are suspected. When access is revoked, OpCtl software performs the following:

- Identify and terminate all shells started by the operator
- Identity and terminate all processes started by the operator, and any child processes started by any process started by the operator
- Terminate the TCP connection used by the ssh session
- Remove the temporary account used by the operator from all infrastructure components

Following the customer action to revoke access there is no credential for the Cloud Ops staff to perform additional work, and the work the Cloud Ops staff was executing will be terminated. Consequently, if the work the cloud ops staff was performing was necessary to prevent an outage or to maintain service quality, then a service outage, service quality degradation, or an incomplete service maintenance operation (such as cleaning up a near full file system) could happen.

Concept of Operations

OpCtl is a shared responsibility model that requires customers and Oracle to work together to request, approve, and monitor access. The intent of this section is to provide customer staff chartered with planning process and technology updates necessary to integrate customer approval processes with OpCtl technology. Oracle publishes important operational flow details in Process Flow for Operator Access Control (OpCtl) (Doc ID 2788316.1).

Operational Flow Block Diagram

Figure 3 depicts the OpCtl Operational flow. Oracle staff actions and Oracle internal interfaces are indicated in red. Customer administrative staff actions and customer OCI interfaces are indicated in gray. Customer security staff actions and interfaces are indicated in green. Customers may delegate customer staff responsibilities beyond what is shown within the diagram via the OCI Identity and Access Management (IAM) framework and interfaces.

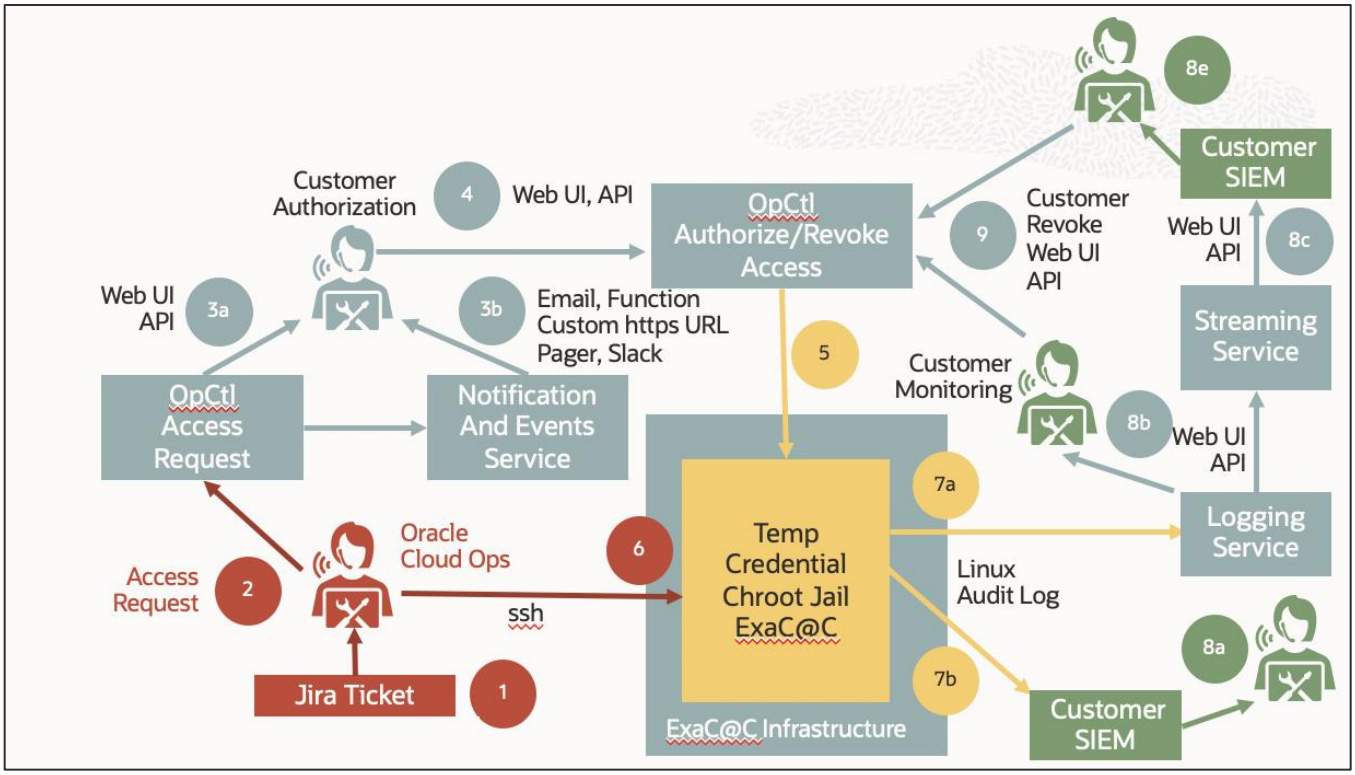

Figure 3: OpCtl Operational Flow

The process for requesting access, granting access, monitoring access, and revoking access is as follows

1) Oracle internal process, such as event processing on the ExaC@C infrastructure or proactive system maintenance, create a Jira ticket for a Cloud Ops staff to perform a task on a specific ExaC@C infrastructure, identified by OCID

2) The Oracle Cloud Ops staff assigned to the Jira ticket creates an OpCtl Access request for a specific profile (chroot jail configuration) using FIPS 140-2 hardware MFA device (Yubikey); the access request is attributed to an identifiable Oracle person and the public key associated with the private key of the Cloud Ops staff making the access request is recorded by the OpCtl service software

3) The customer receives the access request

3a) the customer can see the access request from the OpCtl interfaces (web UI, OCI CLI, REST API) in OCI

3b) the customer can be notified of the access request via OCI notification service; access request notification can be integrated into customer systems that are compatible with the OCI API

4) Customer grants access via OpCtl interfaces, including the web UI, OCI CLI, and REST API; access grant can be integrated into customer systems compatible with OCI API interfaces

5) OpCtl software orchestrates the deployment of a temporary named user account in the specified chroot jail on the ExaC@C infrastructure identified by the requested OCID; access to the temporary named user account is controlled by seeding the `~/.ssh/authorized_keys` file of the temporary account with the public key associated with the private keys used to create the access request; the `choot` jail prevents tampering with the `~/.ssh/authorized_keys` file

6) Oracle cloud ops staff accesses the temporary ExaC@C infrastructure via ssh; authentication is performed via FIPS 140-2 compliant hardware MFA and authorization to connect is granted to the private key associated with the initial access request

7) The Linux auditing services record and publish commands and keystrokes entered by Oracle Cloud Ops

7a) the audit log is available via the OCI Logging service

7b) direct send in syslog format from the Control Plane Server (CPS) to customer SIEM in syslog format

8) Customers monitor cloud ops actions from

8a) their local SIEM receiving audit information from the CPS

8b) OCI Logging Services

8c) OCI streaming service

8e) any other customer SIEM integrated with the OCI streaming service

Customers can revoke access any time via OpCtl interfaces, such as web UI and REST API, as described in the Responsive Controls section if this document.

Access Approval Policies

An OpCtl Policy has 2 approval settings for each action:

- Pre-approved
- Explicit approval

When a policy is configured to pre-approve access to perform an OpCtl Action, the OpCtl software will automatically generate the temporary credential and deploy the chroot jail when Oracle Cloud Ops submits and access request to the customer. For pre-approved access, there is no change to the preventive (chroot jail), detective (logging), or responsive controls (revoking/terminating access) compared to explicit approval. Pre-approval is ideal to reduce management effort and improve service quality and availability when the business and security risks of pre-approving access to the specific chroot jail are small compared to the value of reduced management effort and service quality.

When a policy is not configured to pre-approve access to perform an OpCtl Action, then a customer must access an OCI interface to explicitly approve the access request to generate the temporary credential and deploy the chroot jail. There is no change to the preventative (chroot jail), detective, or responsive controls compared to pre-approved access. Explicit approval is ideal to reduce the risk of system access at a time when business or security reasons cannot permit system access. Explicit approval requires customers to grant access to systems in a timely manner[2], and failure to grant access to systems in a timely manner can lead to service outages and reduced service quality.

OpCtl permits customers to selectively pre-approve specific actions to balance the risk of the action with the benefit of the action, and to select specific time windows during which different actions are pre-approved or explicitly approved so that customers can balance service quality and availability with access control requirements. Preapproval policies for OpCtl can be changed by the customer at any time.

Customer Interfaces

OpCtl may be configured and managed via the OCI Console (web UI) or OCI APIs. The OCI Console is a simple, intuitive interface to permit a person to easily interact with the OpCtl service to configure policies, apply policies to infrastructure, and grant, monitor and revoke access. OCI Console documentation is published at https://docs.oracle.com/en-us/iaas/Content/GSG/Concepts/console.htm. The OCI API interfaces provide programmatic access to the same functionality as the OCI Console, and may be used by customers to integrate OpCtl management into any customer systems and processes that interoperate with OCI API interfaces, such as ticketing and change management systems. The OCI Developer Tools

[2] A 15-minute response time is sufficient for practical use cases; longer response times may lead to service outages or reduceitons in service quality

documentation, published at https://docs.oracle.com/en-us/iaas/Content/API/Concepts/devtoolslanding.htm, describes how to integrate with the OCI API framework.

Customer Notification

OpCtl access requests are published to customers in OpCtl interfaces. Customers may access these interfaces via the OCI Console and OCI API interfaces at any time to learn if they have a pending access request to grant. Customers planning to poll the OpCtl interfaces for access requests should ensure to execute frequent polling (<5 minutes) when policies are configured with explicit approval to avoid delayed processing of access requests and the risk of service outage or service quality reduction.

Customers may opt for push notifications via the OCI Events Service and OCI Notification Service. Customers can configure the OCI Events Service to publish the following OpCtl events:

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

Customers may push any combination of these events to the notifications service for processing purposes. Documentation for the OCI Events Service is published at https://docs.oracle.com/en-us/iaas/Content/Events/Concepts/eventsoverview.htm.

The OCI Notifications Service permits customers to subscribe to event notifications in the following formats:

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

Product documentation for the OCI Notifications Service is published at https://docs.oracle.com/en-us/iaas/Content/Notification/Concepts/notificationoverview.htm.

Customer Test and Validation of OpCtl Service Integration

Timely customer response to approve Oracle Access Requests is necessary to maintain the SLA of the governed service. Customers may integrate OpCtl Access Request processing into their existing processes and systems via OCI interfaces, and such integration may require testing to ensure successful operation. To accomplish testing requires 4 steps:

- Customer notifies Oracle Cloud Ops to create an Access Request
- Oracle Cloud Ops raises an Access Request
- Customer approves the Access Request
- Oracle Cloud Ops processes the Access Request

To initiate a Cloud Ops OpCtl test, a customer can open a Service Request (SR) to notify Oracle Cloud Ops to perform a standard Access Request test as described in the SR. Oracle Cloud Ops will make a best-effort response to perform the Access Request test so that customers can validate Access Request processing integration into their systems.

The standard Access Request tests will perform a predefined set of commands so that customers can validate OpCtl logging functionality and further integration of OpCtl audit logs into other services.

Prior to requesting an Access Request test, customers need the following:

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

The process to perform an Access Request test is as follows:

1. Log into My Oracle Support (MOS) and select “Create Technical SR”
2. Enter useful metadata in “Problem Summary”, “Problem Description”
3. Under “Where is the Problem?” select the “Cloud” Tab
4. In the “Service Type” field enter “Gen 2 Exadata Cloud at Customer”
5. For “Problem Type” select “Infrastructure (Dom0)” then select “Operator Access Control Test (Limited Availability)”
6. Select severity level 2[3]
7. Click “Next"
8. Provide your target OCID in the OCID field (can be easily copied and pasted from web)
9. Click the radio button for the desired test (Diagnostics Access is sufficient for most integration test work)
10. Submit the request
11. Approve OpCtl Access Request
12. Monitor Access Request logs (optional)
13. Verify completion of Access Request test
14. Close SR

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

Oracle Cloud Ops Staffing Updates

There are 3 use cases that may lead to a change in the identity of the Oracle Cloud Ops staff permitted to use the temporary account associated with a Cloud Ops access request

- Customer response time to approve the OpCtl Access Request exceeded the working shift hours of the Cloud Ops staff that issued the request
- The work indicated in the Access Request took longer than the remaining time in the Cloud Ops person's shift, and to complete the work the work request was assigned to a new Cloud Ops person
- An additional specialist was required to resolve the issue

The technical process to perform the staff change is the same in all 3 cases, and is described as follows:

- The new Cloud Ops person issues an "Add Shared Operator – Create" request that is authenticated with their hardware Yubikey
- The OpCtl software issues an "Add Shared Operator – Create" event in the customer's tenancy to alert the customer of the change
- The OpCtl software deploys an additional and unique temporary account that is bound by the same rules as the original access request (same chroot jail and same time bound access) with authentication via the new Cloud Ops person's hardware Yubikey
- The new OpCtl person authenticates to the new temporary credential and processes the work request

Each command and keystroke executed by any login to the temporary credential deployed by OpCtl is timestamped and can be correlated with which specific Yubikey that was used to authenticate to the temporary credential so that Oracle can always provide the unique person associated with the entry of any command on the ExaC@C infrastructure. If a customer revokes the access request, then all of the credentials related to the access request are revoked.

Exadata Infrastructure Software Updates

ExaC@C infrastructure updates are automated processes that are scheduled by the customer to run in specific maintenance windows. The customer control of the maintenance window is available via OCI interfaces and executed via customer controlled OCI IAM credentials. To ensure service quality during an ExaC@C infrastructure update, ExaC@C customers using OpCtl should pre-approve all system access profiles (diagnostics, maintenance update, hypervisor, and full) during customer approved maintenance windows to permit Oracle Cloud Ops staff immediate access to resolve any unexpected issue or failure that is discovered during the software update process. Following the maintenance window pre-approved access is revoked and the customer's previously applied access control is reinstated.

Exception Workflows

The OpCtl service provides process and technical controls to permit exception workflows execution in several important use cases. These use cases include:

- Cloud Ops staffing updates that require a new Oracle Cloud Ops staff to access the infrastructure to continue or complete work processing
- Cloud Ops staff access to the customer VM when work processing requires this access
- Recovery from OpCtl software failure or remote access failure

This section calls out the processing mechanics for these exception cases so that customers can prepare any required compensating controls.

Oracle Access to Customer VM

The ExaC@C service does not authorize Oracle staff to access the customer VM under normal operating conditions. There are exception cases where a failure in the customer VM requires Oracle staff access to resolve the issue. The process and technical

controls that govern how Oracle staff can access the customer VM depend on if the customer VM can be accessed by the customer, or if the customer VM is not accessible by the customer.

Case 1: Customer can log into the customer VM

If the customer VM is accessible by the customer, then OpCtl is not used to permit Oracle staff access to the customer VM. Instead, customer staff are required to access the customer VM using customer credentials, and then customer staff can share access to the customer VM using shared-screen technology (e.g., zoom, webex, skype, etc.). The process is as follows:

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

Case 2: Customer cannot log into the customer VM

If the customer cannot access the customer VM, then OpCtl is used to permit Oracle staff to access the customer VM from the infrastructure. This access is controlled by the SR process and the customer granting the use of a full-access OpCtl cage for the purposes of resolving the issue. The process is as follows:

- Customer opens a Service Request (SR) with the following language:
  - SR Title: "*SR granting Oracle explicit permission to access DomU of ExaCC with serial number AKXXXXXXXXX"*
  - SR Content: "*We are opening this SR to grant explicit permission to Oracle to access our DomU in order for support to help resolve issue described in SR# XXXXXXXX. We acknowledge that by providing this permission, we understand that Oracle will have access to ALL FILES in DomU and agree that there are no confidential files stored in any of the file systems in DomU. In addition, we also agree that customer security team has authorized Oracle to have access to customer DomU in order to resolve the issue described in the above SR."*
- Oracle opens an OpCtl a hypervisor or full Access Request request against target infrastructure
- Customer grants access request
- Oracle or customer will open a shared session and provide shared session information in the SR
- With Oracle and customer both accessing the shared session, Oracle will use OpCtl to access the components required to resolve the issue

Recovery from OpCtl Software Failure

The OpCtl service is implemented in a highly available (HA) delivery model that protects against any single hardware component failure. To ensure customers have complete control over all remote access, the OpCtl software does not provide Oracle an alternate human remote access method to mitigate against failure of the OpCtl software (e.g., access request processing, chroot jail deployment). If the OpCtl software fails and requires human shell access to resolve the issue, then the process for the customer to provide access to permit Oracle to recover from an OpCtl software failure is as follows:

- Oracle contacts the customer via the customer's specified contact method and indicates the issue to the customer
- Oracle staff travel to the location of the physical equipment
- Customer appointed staff escorts Oracle staff to the physical equipment

- Oracle staff accesses physical equipment and perform analysis and recovery

After OpCtl functionality is restored then subsequent access to perform any further remediation is executed through the OpCtl service.

Security Incident Reporting and Communication

In the event of a security incident, Oracle will comply with applicable laws and Oracle Global Security policies related to incident response and management. Details for Oracle Corporate Security Practices and Incident Response handling are published at https://www.oracle.com/corporate/security-practices/corporate/security-incident-response.html. Customers should report suspected unauthorized access or actions via the Oracle Service Request (SR) process by opening a Security Service Request (SR) and indicating the details of the suspected unauthorized access or actions.

Summary

The OpCtl service can help customers to meet policy and regulatory requirements regarding Oracle staff access to infrastructure components, and tightly couples Oracle Cloud Ops support with customer technology change management and security staff. The preventative, detective, and responsive controls provide customers with OCI interfaces to manage and govern Oracle staff access, and to help integrate control of Oracle staff access control into customer change management and SIEM systems. A consequence of customer control of Oracle staff access is that customers must grant access to Oracle access requests in a timely manner, so customers can either pre-approve access requests, or plan to integrate OpCtl Access Request processing with their existing 24x7 on-call support systems to ensure ExaC@C service availability and quality.