Oracle Private Cloud Appliance

Security Guide for Release 3.0.1

F49406-03
May 2022

ORACLE

Oracle Private Cloud Appliance Security Guide for Release 3.0.1,

F49406-03

Contents

3 Security Features for Oracle Private Cloud Appliance

4 Secure Deployments Checklist

Preface

This publication is part of the customer documentation set for Oracle Private Cloud Appliance Release 3.0.1. Note that the documentation follows the release numbering scheme of the appliance software, not the hardware on which it is installed. All Oracle Private Cloud Appliance product documentation is available at https://docs.oracle.com/en/engineered-systems/private-cloud-appliance/index.html.

Oracle Private Cloud Appliance Release 3.x is a flexible general purpose Infrastructure as a Service solution, engineered for optimal performance and compatibility with Oracle Cloud Infrastructure. It allows customers to consume the core cloud services from the safety of their own network, behind their own firewall.

Audience

This documentation is intended for owners, administrators and operators of Oracle Private Cloud Appliance. It provides architectural and technical background information about the engineered system components and services, as well as instructions for installation, administration, monitoring and usage.

Oracle Private Cloud Appliance has two strictly separated operating areas, known as enclaves. The Compute Enclave offers a practically identical experience to Oracle Cloud Infrastructure: It allows users to build, configure and manage cloud workloads using compute instances and their associated cloud resources. The Service Enclave is where privileged administrators configure and manage the appliance infrastructure that provides the foundation for the cloud environment. The target audiences of these enclaves are distinct groups of users and administrators. Each enclave also provides its own separate interfaces.

It is assumed that readers have experience with system administration, network and storage configuration, and are familiar with virtualization technologies. Depending on the types of workloads deployed on the system, it is advisable to have a general understanding of container orchestration, and UNIX and Microsoft Windows operating systems.

Feedback

Provide feedback about this documentation at https://www.oracle.com/goto/docfeedback.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, code in examples, text that appears on the screen, or text that you enter.
`$` prompt	The dollar sign (`$`) prompt indicates a command run as a non-root user.
`#` prompt	The pound sign (`#`) prompt indicates a command run as the `root` user.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at https://www.oracle.com/corporate/accessibility/.

For information about the accessibility of the Oracle Help Center, see the Oracle Accessibility Conformance Report at https://www.oracle.com/corporate/accessibility/templates/t2-11535.html.

Access to Oracle Support for Accessibility

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit https://www.oracle.com/corporate/accessibility/learning-support.html#support-tab.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

1

Introduction to Oracle Private Cloud Appliance Security

The Oracle Private Cloud Appliance is an engineered system that combines customer-premise-based hardware and preloaded software with a cloud component that runs entirely within the customer data center and on-premises network. Although there is no Oracle Cloud Infrastructure account involved, Oracle Private Cloud Appliance offers core Oracle Cloud Infrastructure services, and is fully compatible with Oracle Cloud Infrastructure services such as Compute, Network, Block Volume Storage, Object Storage, File System Storage, Identity and Access Management, and some other smaller or less visible elements. Because Oracle Private Cloud Appliance is disconnected, it also has its own control plane implementation, known as the Service Enclave.

This engineered system is installed by Oracle, which provides a level of security independent of local practices. However, this also requires the system administrators to understand exactly what is provided as a security baseline. Then the administrators can adjust security practices and configurations to achieve the desired level of security needed for their specific circumstances.

Product Security Overview

Product Security Overview

The core security components of the Oracle Private Cloud Appliance are layered. The three layers of the Oracle Private Cloud Appliance are:

- Infrastructure - This is the physical rack hardware installed on the customers premises. Some security-related tasks are performed at this basic level when the system is installed.
- Service Enclave - This is the part of the system where the appliance infrastructure is controlled. Access to this enclave is closely monitored and restricted to privileged administrators. The Service Enclave runs on a cluster of three management nodes, and many security-related tasks are performed at this level.
- Compute Enclave - The Compute Enclave, designed for compatibility with Oracle Cloud Infrastructure, is where workloads are created, configured and hosted by users or groups and where cloud resources such as compute instances, networks, and storage are controlled.

The Oracle Private Cloud Appliance follows the same basic security principles as other OracleOracle products. These principles are:

- Authentication: Authentication is how a user is identified, typically through confidential information such as user name and password, or shared keys. All components use authentication to ensure that users are who they say they are. By default, local user names and passwords are used for authentication. Shared key-based authentication is also available.
- Authorization: Administrators configure user or group privileges to resources along with the level of access allowed to the resources. Personnel can only access the resources

with the level of access that has been given to them. Users with administrative privileges can authorize users and groups with one or more types of access (inspect, read, use, manage) to resources (all-resources, instance-family, and so on).

- Auditing: Auditing maintains a record of user activity at the various layers of the Oracle Private Cloud Appliance. Audit records exist for the Service Enclave, Compute Enclave, and for the infrastructure. Using audit records, an administrator is able to associate a particular user with a change that occurred in one or more components in the system. Monitor audit records to ensure users in the layers are properly accessing and using components and monitoring for excessive or insufficient resource privileges for users. Audit records can also identify unexpected system usage patterns that could identify denial of service attempts, attempts to access services through probing attacks of the boundaries or misuse of resources that resulted in data loss or unexpected resource modifications.
- Accounting: Accounting lets administrators track inventories of hardware and cloud resources. Hardware assets are tracked through serial numbers whereas cloud resources are tracked through Oracle Cloud IDs (OCIDs). For hardware components, Oracle part numbers are electronically recorded on all cards, modules and mother boards. These can be used for inventory or for association with issues reported to Oracle. Cloud resources tracked by OCIDs can be monitored by administrators to track usage and resource consumption.

When applied properly, the above security principles allow:

- Survivability of Mission-Critical Workloads - Oracle Private Cloud Appliance prevents or minimizes the damage caused from accidental and malicious actions taken by internal users or external parties. This is accomplished by security testing of components, checking protocols for vulnerabilities, and verifying software continuity even during security breaches.
- Defense in Depth to Secure the Operating Environment - Oracle Private Cloud Appliance employs multiple, independent, and mutually-reinforcing security controls to help organizations create a secure operating environment for their workloads and data. All levels of the system are protected by an array of security capabilities.
- Least-Privilege Access for Services and Users - Oracle Private Cloud Appliance promotes the use of security policies that ensure that applications, services, and users have access to the capabilities that they need to perform their tasks. However, it is equally important to ensure that access to unnecessary capabilities, services, and interfaces are limited. Users and administrators are confined to their particular areas of concern.
- Accountability of Events and Actions - Oracle Private Cloud Appliance offers detailed audit trails at each layer as well as controls to help account for resources. This helps an administrator detect and report incidents as they are occurring (such as a denial of service attack) or after they occurred if it was not preventable (through traceability through audit logs to resulting changes to resources).
- Understanding of Operating System Security - The operating system requires stringent security during patches and updates to ensure the integrity of the operating system at all times. This is possible by enforcing security policies, limiting network access, and monitoring all operating-system-level activities.

Security Planning

Security cannot be added onto a product like a new software feature or parameter adjustment.

Some categories and examples of the kinds of things to consider during this initial product installation planning are:

- Networking: Virtual and physical interfaces, bridged and routed
- User Access: Users and groups, what their role is, and what resources they will access to inspect, read, use or manage
- Password rules: length and character requirements, other characteristics
- Cryptographic algorithms: allowed or mandated, usage guidelines
- Patch or update process security: limitations, roles allowed to execute procedures

This is not an exhaustive list. The more things that can be planned ahead of time, the better.

Basic Security Considerations

These principles are fundamental for securing the product:

- Keep software up-to-date. This includes the latest product release and any patches that apply to it. For more information, see Oracle Private Cloud Appliance Installation Guide and Oracle Private Cloud Appliance Patching Guide.
- Limit privileges wherever possible. Give users only the access necessary to perform their work. Review user privileges periodically to determine relevance to current work requirements. For more information, see Oracle Private Cloud Appliance Concepts Guide.
- Monitor system activity. Establish who has access to which system components, and how often, and monitor those components.
- Learn about and use Oracle security features.
- Use best practices for security.

Customer Security Responsibilities

The customer is always responsible for securing aspects of the system that are under the customer's direct control. These responsibilities include:

- **Information and Data:** The customer always retains control over information and data. The customer controls how and when this data is used. The Cloud provider (Oracle) has zero visibility into customer data, and all data access is under the customer's control by design.
- **Application Logic and Code:** Regardless of how Cloud resources are spun up, the customer secures and controls the customer's proprietary applications during the entire application life cycle. This includes securing code repositories from malicious misuse or intrusion, application build testing during the development and integration process, ensuring secure production access, and maintaining the security of any connected systems.

- **Identity and Access:** The customer is always responsible for all aspects of identity and access management (IAM). This includes authentication and authorization mechanisms, any single sign-on (SSO) access, multi-factor authentication (MFA), access keys, certificates, the user creation processes, and password management.
- **Platform and Resource Configuration:** When cloud environments spin up, the customer controls the operating environment. How control is maintained over those environments varies, based on whether instances are server-based or serverless (PaaS). A server-based instance requires more hands-on control over security, including OS and application hardening, maintaining OS and application patches, and so on. Server-based instances in the cloud behave like physical servers, and function as an extension of the customer's data center. For serverless resources, the provider’s control plane gives the customer access to the setup of the configuration. In all cases, the customer is responsible for knowing how to configure customer instances in a secure manner.

  Additionally, the customer maintains responsibility for securing everything in the customer organization that connects with the cloud. This includes:

  – The on-premises infrastructure stack and user devices.
  – Customer-owned networks and applications.
  – The communication layers that connect your users, both internal and external, to the cloud and to each other.

  The customer also needs to set up monitoring and alerting for security threats, incidents, and responses for domains that remain under customer control.

A Note on Auditing

Good auditing practices require a firm separation of duties. This separation makes it easier, if issues with changes are causing problems, to determine the following:

- Who made the change? (More than information that "root" made the alteration.)
- When was the change made? (An adequate log retention period is important.)
- What was the purpose of the change? (If not malicious, the change was made for a reason.)

The main point of the audit process is to allow personnel to move forward in a better way to implement the changes needed.

2

Secure Installation and Configuration for Oracle Private Cloud Appliance

The Oracle Private Cloud Appliance is an engineered systems and installation is generally performed for the customer. When the system is first powered on, there are various tasks that need to be performed in order to get the system initially set up. Tasks like defining the first "admin" user account (note that a default administrator account is no longer provided due to security requirements), configuring system parameters like realm and region, and configuring basic networking parameters. Oracle Private Cloud Appliance supports two ways for an operator to view and configure system information: a GUI and a session-based CLI. For the initial installation, it is envisioned that the GUI would be used to guide the operator through the various initial configurations that are needed. If desired, the operator may wish to use the CLI to perform these actions instead.

Installation Overview

As an engineered system, installation of Oracle Private Cloud Appliance is not usually performed by the customer. Nevertheless, security concerns are the responsibility of everyone who uses the system. Security issues must be addressed before the system is installed because security cannot be added on to a system later.

Pre-Installation Security Details

Before Oracle Private Cloud Appliance installation, create a document to outline the services provided. Have it reviewed and updated to address any shortcomings.

- For each application or service, have those responsible for security review the information.
- Provide all URLs and links needed so that reviewers can easily find the source material employed to create the pre-installation plan.
- Repeat the process until all reviewers are satisfied that all initial security goals have been satisfied.

Make a list of all the roles needed to deploy the Oracle Private Cloud Appliance in a secure environment. Identify the personnel needed to fill these roles.

> **Note:**
>
> Make sure that the roles and users identified do not overlap and that capabilities are appropriately isolated.

- Identify the various administrators for all layers of the Oracle Private Cloud Appliance: infrastructure, Service Enclave, andCompute Enclave.

- Identify the users of services at all relevant layers of the Oracle Private Cloud Appliance. List privileges needed and restrictions necessary.

Produce a draft implementation plan with the virtual machines and network connections needed for the Oracle Private Cloud Appliance. Have this reviewed and modified until it is as complete as feasible before installation.

- Describe the role of each virtual machine as clearly as possible.
- If there are departures from the typical front-end, back-end, and load balancer arrangement, describe it in full.
- Describe the circumstances for starting virtual machines, both for initial use and for handling increased loads.

Describe the network connections needed, if any, between the virtual machines at each layer of the Oracle Private Cloud Appliance architecture.

- List the secure network protocols to be used to operate and maintain the system.
- Provide initial policy rules for virtual machines communications, at least at a prose level.
- Determine which network connections can be switched: that is, can be handled by a simple VLAN and single IP address space.
- Determine which network connections must be routed: that is, must be handled by more than one VLAN and multiple of subnetted IP address spaces.

System Site Preparation

For pre-installation site preparation, see the Oracle Private Cloud Appliance Installation Guide.

Product Installation

Regardless of who installs the Oracle Private Cloud Appliance, each component of the Oracle Private Cloud Appliance product automatically installs into a secure state. Security options, such as SSL, are already configured and enabled.

You can tailor the installed product for your specific deployment scenario, as long as security is not compromised.

You can uninstall or disable any component of the system which are not used in your specific deployment.

Post-Installation Configuration

This section describes the security configuration changes that must be made after installation. Generally, do not weaken the security posture of the Oracle Private Cloud Appliance when making changes to configurations.

Securing the Hardware

After installation of Oracle Private Cloud Appliance, secure the hardware by restricting access to the hardware and recording the serial numbers.

Oracle recommends the following practices to restrict access:

- Install Oracle Private Cloud Appliance and related equipment in a locked, restricted-access room.
- Lock the rack door unless service is required on components within the rack.
- Restrict access to hot-pluggable or hot-swappable devices because the components are designed to be easily removed.
- Store spare field-replaceable units (FRUs) or customer-replaceable units (CRUs) in a locked cabinet. Restrict access to the locked cabinet to authorized personnel.
- Limit SSH listener ports to the management and private networks. Use SSH protocol 2 (SSH-2) and FIPS 140-2 approved ciphers.
- Limit SSH allowed authentication mechanisms. Inherently insecure methods are disabled.
- Label all significant items of computer hardware, such as FRUs.
- Keep hardware activation keys and licenses in a secure location that is easily accessible to the system managers in the case of a system emergency.

Retrieving the Appliance Serial Number

An Oracle Private Cloud Appliance has a serial number that identifies the appliance as a whole entity. When working with Oracle Support Services, the appliance serial number may be required.

There is a label on the rack with the serial number. The serial number label is the white label about midway up the front right rail of the rack.

There are several other techniques to obtaining the overall appliance serial number:

- Use the Service Enclave console (Administrative Console) - To get the appliance serial number from the Service Enclave console:
  1. Use a supported web browser to log into the console with a username and password that has sufficient authorization (`https://adminconsole.<domain>`).
  2. If you just completed the initial setup, then use the admin username with the configured password (otherwise the administrator may provide you with a specific user for access).
  3. Access the Appliance Details section from the menu.
  4. Record the ID and the Realm from this page. The Realm is the physical appliance serial number: record both the ID and the physical appliance serial number.
- Use the appropriate monitoring dashboard (Grafana) - To obtain the appliance serial number from the monitoring dashboard:
  1. Use a supported web browser to log into the dashboard with a username and Password that has sufficient authorization (`https://grafana.<domain>`).
  2. Go to the Dashboards → Manage Dashboards section.
  3. Open the Service Monitoring → Hardware Stats dashboard. The appliance serial number is displayed on this dashboard.
  4. Record the ID and the Realm from this page. The Realm is the physical appliance serial number: record both the ID and the physical appliance serial number.
- Use the Admin Command Line Interface (CLI) - To obtain the appliance serial number using the CLI:

1. Log into the Admin CLI with a username and password that has sufficient authorizations (use the command `ssh -l` ***<username>*** `management host -p 30006`). The management host is one of the three management nodes (`pcamn01`, `pcamn02`, or `pcamn03`) and the username, by default, is `admin`. If the section on rotating the passwords is not completed yet, then use the password supplied during initial setup.
2. From the prompt, there are a variety of ways to get the rack serial number. A quick report can be obtained with the command: `list Rack fields name,rackNumber,rackSerialnumber,rackType`.

   For example,

```
PCA-ADMIN> list Rack fields rackSerialnumber
Command: list Rack fields rackSerialnumber
Status: Success
Time: 2022-02-17 20:15:41,773 UTC
Data:
  id                                   rackSerialnumber
  --                                   ----------------
  x6d9f31a-b1ds-4a43-bc09-7270609abd8k CL00888510
PCA-ADMIN>
```

3. Store the information from the Appliance Details in a secure location.

Retrieving the Serial Numbers for Hardware Components in the Rack

An Oracle Private Cloud Appliance is an engineered system that is made up of many hardware components. For simplicity we will call these the *rack* components, though the components can span multiple racks. The most efficient way to collect the serial numbers for the rack components is to use the Admin CLI, though they can also be obtained from the Service Enclave console (Administrative Console). These serial numbers may also be needed when working with Oracle Support Services.

To get a list of rack component serial numbers from the Admin CLI:

1. Log into the Admin CLI with a username and password that has sufficient authorizations (use the command `ssh -l` ***<username>*** `management host -p 30006`). More details are in the Retrieving the Appliance Serial Number section.
2. Once logged in, get a report using a command such as the following: `list RackUnit fields name,rackElevation,serialNumber,hostname`.
3. Store the information recorded above in a secure location.

To use the Service Enclave console, log into the console with a username and password that has sufficient authorization (https://adminconsole.<domain>). After logging in:

1. Using the menu, navigate to the Rack Units context.
2. For each unit in the list, choose to View Details:
   a. Once in the details, choose the System tab.
   b. Record the Serial Number along with other component information.
3. Return to the Rack Units list and record the next component.
4. Store the information recorded above in a secure location.

Securing the Software

After installation of Oracle Private Cloud Appliance, secure the software. In many cases, hardware security is implemented through software.

After initial installation of Oracle Private Cloud Appliance, Oracle recommends the following practices to restrict system access:

- Limit use of the super-user account, such as `root` on the management nodes and SuperAdmin accounts in the Service Enclave and Compute Enclave. Create and use individual user accounts because they ensure positive identification in audit trails, and require less maintenance when administrators leave the team or company.
- Do not create new users on the management nodes.
- Disable unnecessary protocols and modules for layers under customer control.
- Restrict physical access to USB ports, network ports, and system consoles because physical severs and network switches have ports and console connections providing direct access to the system.
- Restrict the capability to restart the system over the network.
- For more information on how to enable other security features, see Security Features for Oracle Private Cloud Appliance in this guide.

By using the privileged users and multi-factor access control, and other tools such as data encryption, auditing, monitoring, and data masking, customers can deploy reliable data security solutions that do not require any changes to existing applications.

Securing the Network

Oracle Private Cloud Appliance is a private cloud environment. During initialization, the appliance core network components are integrated with your existing data center network design. Uplink ports in the appliance switches connect to your next-level data center switches to provide a redundant high-speed and high-bandwidth physical connection that carries all traffic into and out of the appliance. In other words, from the private cloud environment perspective, the public network is your on-premises network, and internet access is always indirect through your data center edge router.

This private environment has several consequences when it comes to securing Oracle Private Cloud Appliance with regard to networking:

- The rack is located on your premises, set up inside your data center, and connected directly to your on-premises network. There is no need for a secure tunnel over the internet to allow your cloud resources and your on-premises network to communicate. Access is enabled through a gateway between your virtual cloud network (VCN) and your on-premises network
- When it comes to internet access, inbound or outbound, resources in your cloud environment have no direct internet access. In contrast with a public cloud environment, no gateway is capable of enabling direct internet connectivity for a VCN. The configuration of the networking components in the data center determines how cloud resources can connect to the internet and whether they can be reached from the internet.
- Generally, this private environment means that theOracle Private Cloud Appliance virtual network is well-isolated from public internet threats. However, It is possible to use public IP addresses inside this private network. A public IP makes a resource reachable from

outside the VCN it resides in. The IP addresses that are considered "public" are really part of the data center's private range.

Nevertheless, there are steps that can be taken to control cloud network security and access to compute instances:

- Use private subnets if instances do not require a public IP address.
- Configure firewall rules on the instance to control traffic into and out of an instance at the packet level. However, Oracle-provided images that run Oracle Linux automatically include default rules that allow ingress on TCP port 22 for SSH traffic. In addition, the Microsoft Windows images include default rules that allow ingress on TCP port 3389 for Remote Desktop access.
- Configure gateways and route tables to allow only required connectivity. This can control traffic flow to "outside" destinations such as your on-premises network or another VCN.
- Use IAM policies to control access to Oracle Private Cloud Appliance interfaces. You can control which cloud resources can be accessed and which type of access is allowed. For example, you can control who can set up your network and subnets, or who can update route tables, network security groups, or security lists.

For more information on Oracle Private Cloud Appliance network security, see the Oracle Private Cloud Appliance User Guide and Oracle Private Cloud Appliance Administrator Guide .

Networking and DNS

Oracle Private Cloud Appliance networks require DNS service in three areas:

- Kubernetes DNS in Service Enclave.
- Authoritative DNS service in Customer Data Center Network for ***<pca>.<domain>***.
- Authoritative DNS service inCompute Enclave (accessible from subnets in customer tenancy) for ***<pca>.<domain>*** and internalpca.local.
- Recursive DNS in Compute Enclave for foreign zones.

Kubernetes provides a DNS service using CoreDNS that gets dynamically configured with service endpoints when the corresponding Kubernetes service is deployed. One or both of the other two DNS services may be able to leverage this already required CoreDNS deployment. In the worst case each could use a separate DNS deployment using CoreDNS or another implementation.

Creating and Maintaining Accounts and Passwords

When the Oracle Private Cloud Appliance system is first powered on, various tasks need to be performed in order to initially set up the system. These tasks include defining the first super-admin user account, configuring system parameters such as system and domain name, and configuring basic networking parameters that make the appliance part of the data center network.

There are three layers of the Oracle Private Cloud Appliance, each of these three layers will be administered in a different way:

- Infrastructure - The rack hardware contains default users and passwords. Infrastructure does not usually need to be accessed in day-to-day operations. After installation, update any default passwords and store them in a secure location.

Individual accounts are not supported in the infrastructure context. On most infrastructure components there are only two accessible users, the administrative user and an account for Oracle Support Services that can only be accessed with support from the administrative user.

- Service Enclave - The administrative user created during installation applies to this layer. Additional users can be added to the Service Enclave to help manage the Oracle Private Cloud Appliance but, in practice, there are few of these users as their operations are across the entire appliance.
- Compute Enclave - Users of the Compute Enclave have day-to-day tasks within a tenancy. They may be creating compute instances or monitoring cloud resources. When an administrative user creates a tenancy, they define an administrator for the tenancy that can then expand access to the tenancy from the Compute Enclave console.

Each layer has different requirements and techniques for maintaining the user accounts.

Password Maintenance in the Infrastructure Layer

The infrastructure layer is not accessed in day-to-day operations and is not intended to be a multi-user experience. Infrastructure is largely managed either through the Service Enclave layer, or by the individual software components running within the Service Enclave. Change any default passwords immediately after successful rack installation and configuration.

Passwords to be updated include:

- Compute node passwords
- Compute node Oracle Integrated Lights Out Manager (ILOM) passwords
- Management node passwords
- Management node ILOM passwords
- Leaf switch password
- Management switch password
- Spine switch password
- Oracle ZFS Storage Appliance password
- Oracle ZFS Storage ApplianceILOM password

There is a tool available on the management nodes to check for default passwords in the infrastructure that must be changed. To run it:

1. Log into a management node using the default administrative user and password supplied to you by the installation team.
2. Run the following command: `/var/lib/pca-foundation/scripts/healthcheck.py`.

The output of the tool will show passwords to change from factory defaults.

All passwords except the MySQL database password must be updated using the `pca-admin` tool that resides on the management node. Using the various native infrastructure tools will result in Service Enclave failures. An example of why the tool must be used is with the management node passwords. Updating the management nodes using the `pca-admin` tool keeps all management node passwords synchronized. The `pca-admin` tool also stores the password for the management nodes in a service-accessible database, allowing the Service Enclave tools and services to manage the nodes.

The MySQL database password is updated using the following command from one of the management nodes: `/var/lib/pca-foundation/scripts/pca_change_mysql_root_password.py`

Passwords are stored in two locations:

- A vault instance where they are stored using 256-bit Advanced Encryption Standard (AES) cipher in the Galois Counter Mode (GCM) with 96-bit nonces.
- The native password tool for the infrastructure component

Refer to documentation for the infrastructure component information for password access information.

The password complexity policy for infrastructure components is:

- Length is 8 characters to 20 characters
- The password must contain a character from each of the groups
  - Lower case letters (a-z)
  - Upper case letters (A-Z)
  - Digits (0-9)
  - Symbols (@$!#%*?&)

The password complexity policy for the infrastructure cannot be changed.

To update an infrastructure password

- Start the `pca-admin` tool on any of the management nodes (after logging in)
- Use the `change password <component> <password>` command. For example: `change password zfs <updated_password>`.

The password update can take a short amount of time to complete even after a successful password update response is returned.

The Power Distribution Units (PDUs) in the PCA racks vary depending on the locale. Refer to the PDU hardware documentation for information regarding password updates. Refer to the Oracle Private Cloud Appliance Release Notes for potential updates on the infrastructure processes.

Service Enclave User and Password Maintenance

At installation and configuration time, an initial user with the SuperAdmin Authorization Group and password is set up for the Service Enclave, refer to the configuration chapter of the Oracle Private Cloud Appliance Installation Guide

The Service Enclave is a multi-user environment where users do not share credentials. Because actions in the Service Enclave affect all tenancies on the appliance, very few users are necessary in this space. General security guidelines are:

- Do not share credentials.
- Create a user for each individual that requires access to the Service Enclave administration tools. This practice enables better audit tracking and easier administration of individual needs.
- Apply the rule of least privileges by choosing the authorization group most appropriate for the individual.

- When creating a new user, do not use a common password and do not use a default initial password for new users.
- Change passwords regularly. There are no proactive password change or timeout notifications in the Service Enclave.

There are 4 important authorization groups in the Service Enclave:

- Admin - Authorization for most operations except user management
- Monitor - A read-only role that can only manage their own profile or browse service enclave information without changing it
- SuperAdmin - Authorization for all capabilities, only a SuperAdmin can create new users for the Service Enclave and change roles for existing users
- DrAdmin - Authorization for setting up Disaster Recovery (this group is used only during Day-0 configuration)

In the Service Enclave, the list of authorization groups is static. Existing groups cannot be modified to change authorizations and new groups cannot be created with different authorizations.

The password policy for the Service Enclave is as follows:

- Password has a minimum length of 12 characters
- Password contains at least one uppercase letter
- Password contains at least one lowercase letter
- Password contains at least one symbol (@$!#%*?&)
- Password contains at least one number

The Service Enclave password policy cannot be changed.

Password storage is in the service database and uses Password Based Key Derivation Function 2 (PBKDF2) with a 32 character salt to hash the password.

User maintenance and password maintenance for the Service Enclave for a user in the SuperAdmin group is done using the Service Enclave Administration Console (`https://adminconsole.`***`<domain>`***) or the Admin CLI. A user in the MONITOR or ADMIN group must use the Admin CLI or request a password change from a user in the SuperAdmin authorization group.

From the Admin CLI, use the command to change the password:

`changePassword id=` ***`<id>`*** `password=` ***`<new_password>`*** `confirmPassword=` ***`<new_password>`***

To get the ID for the current user, use the command:

```
show UserPreference
```

A user in the SuperAdmin group can change the password of any user in the Admin CLI. A list of user IDs can be obtained using the command: `list user`.

Additional notes on password management in the 3.0.1 software version:

- A user in the MONITOR or ADMIN group cannot change their password in the Service Enclave Administration Console.

- There is no password recovery or password reset functionality, as a result, it is strongly advised that a second user with SuperAdmin capability is created.
- Accounts will not be locked out or disabled with any number of invalid login attempts.

For more information on use of Identity Providers with the Service Enclave layer, see Service Enclave Security Features.

Compute Enclave User and Password Maintenance

There are no default Compute Enclave users or tenancies immediately following an Oracle Private Cloud Appliance Installation Guide install and configuration.

When a Service Enclave administrator creates a tenancy, an initial user is created and a password is assigned.

Have the new tenancy administrator log into the account and change their password using the Compute Enclave console (`https://console.<domain>`).

Once logged in, use the Change Password drop down located in the top right of the console where the user name is displayed. The tenancy administrator is the only user account that cannot be reset by any user (including themselves). The only option available to the primary tenancy administrator created by the Service Enclave SuperAdmin is to store their password securely and use the Change Password action in the user interface after a successful login.

The password policy for the Compute Enclave is as follows:

- Password has a minimum length of 12 characters
- Password contains at least one uppercase letter
- Password contains at least one lowercase letter
- Password contains at least one symbol (@$!#%*?&)
- Password contains at least one number

The password policy cannot be changed.

Password storage is in the service database and uses Password Based Key Derivation Function 2 (PBKDF2) with a 32 character salt to hash the password.

The tenancy administrator also sets up the CLI with their account so they can start making use of Identity and Access Management (IAM) operations. For instructions on setting up the CLI to use with a tenancy and user on the Oracle Private Cloud Appliance refer to Working in the Service Enclave.

Every tenancy comes with a default administrators group. This group can perform any action on all resources in a tenancy (that is, they have root access to the tenancy). Oracle recommends that you keep the group of tenancy administrators as small as possible but have at least one backup administrator.

Some security recommendations on managing tenancy administrators:

- Have security policies granting membership of tenancy administrator group strictly on a as-needed basis.
- Tenancy administrators use high-complexity passwords, along with MFA, and periodically rotate their passwords.

- After account set up and configuration, Oracle recommends that you don't use the tenancy administrator account for day-to-day operations. Instead, create less privileged users and groups.
- Though administrator accounts are not used for daily operations, they are still needed to address emergency scenarios impacting customer tenancy and operations. Specify secure and auditable "break-glass" procedures for using administrator accounts in such emergencies.
- Disable tenancy administration access immediately when an employee leaves the organization.
- Because the tenancy administrator group membership is restricted, Oracle recommends that you create security policies which prevent administrator account lock-out (for example, if the tenancy administrator leaves the company and no current employees have administrator privileges).

Users in the Compute Enclave other than the default administrator for a tenancy can have their passwords reset by a user in the Administrator group through the Users context in the Compute Enclave console (`https://adminconsole.<domain>`).

A user can reset their own password if they have the CLI installed and configured via the command:

```
oci iam user ui-password create-or-reset --user-id <id>
```

An administrator can use the CLI command to reset any other user's password. After reset, the administrator securely communicates the reset password to the user. The user will be prompted on login to the console to change the password.

For more information on the user of Identity Providers with the Compute Enclave and IAM security features to help administer the Compute Enclave layer, refer to Identity Provider Security Features.

Maintaining the Monitoring and Logging Password

The monitoring and logging facilities for Oracle Private Cloud Appliance are accessed via consoles at:

- Grafana: https://grafana.***<domain>***
- Prometheus: https://prometheus.***<domain>***

In Oracle Private Cloud Appliance 3.0.1, the infrastructure layer has a single user for both Grafana and Prometheus (`admin`), and they have a default password. Change this password after installation and configuration.

For proper security, it is required that admins set the new password by running the Python CLI tool **sauron_credential_update.py** from the management node.

The password policy requires that the password:

- Must be 12-20 characters long
- Must contain at least 1 uppercase, 1 lowercase and one digit
- Can contain the symbols -_+=

The monitoring and logging tools in Oracle Private Cloud Appliance 3.0.1 have the following restrictions:

- More users cannot be added
- The credential update tool does not check the password or return information on success or failure of the request
- The Grafana and Prometheus screens do not lock out users after invalid attempts

Due to these characteristics:

- Choose a complex password
- Designate a user as the focal point for monitoring and logging
- Do not share the password for the admin account
- Change the password regularly
- Do not share the password with tenancy administrators (Grafana and Prometheus contains logs for all tenancies and should therefore not be shared with a tenancy administrator due to information leakage between tenancies)

Viewing Failed Password Log-in Attempts

Security monitoring for all layers (Infrastructure, Service Enclave and Compute Enclave) can be viewed in the Grafana instance (https://grafana.***<domain>***).

To view logs that include security notifications:

- Log into Grafana using the Grafana admin user and password you set in Maintaining the Monitoring and Logging Password
- Go to the Explore context
- Choose the Loki data source

From that data source, choose the infrastructure or software component to view information. The various components can be filtered using log labels for:

- Management and compute nodes, use the `host` filter, such as `{host="pcamn01"}`
- Oracle ZFS Storage Appliance, use `{log="audit"}`
- Compute Enclave, use `{log="api-server"}`
- Other labels are possible

Some components cannot be monitored at this tier:

- Switches (Spine, Leaf and Management)
- ILOM

If audit logs are required for those components, log directly into the component.

3

Security Features for Oracle Private Cloud Appliance

This section outlines the specific security mechanisms offered by the Oracle Private Cloud Appliance. Oracle Private Cloud Appliance offers a full suite of authentication, access control, and security audit features. This section provides guidance on how to enable and use these features.

Whenever possible and practical, choose and configure secure default settings. Use the following default settings in Oracle Private Cloud Appliance:

- A minimal software installation to reduce attack surface.
- Oracle secure settings developed and implemented using Oracle best practices.
- A password policy that enforces a standard complexity for password formulation.
- Failed log-in attempts cause a lockout after a set number of failed attempts.
- All default operating system accounts are locked and blocked from logging in.
- Limited ability to use the `su` command.
- Password-protected boot loader installation.
- All unnecessary system services are disabled, including the internet service daemon (`inetd`/`xinetd`).
- Software firewall configured wherever practical.
- Restrictive file permissions on key security-related configuration files and executable files.
- SSH listen ports restricted to management and private networks.
- SSH limited to v2 protocol.
- Disabled insecure SSH authentication mechanisms.
- Configured-specific cryptographic ciphers.
- Unnecessary protocols and modules are disabled from the operating system kernel.

Remote network access is always a security concern. Manage the management network switch configuration file offline, and limit access to the configuration file to authorized administrators. Place descriptive comments in the configuration file for each setting. Consider keeping a static copy of the configuration file in a source code control system. Periodic reviews of the client access network are required to ensure that secure host and other settings remain intact and in effect. In addition, periodic reviews of the settings ensure that they remain intact and in effect.

These network security guidelines help to ensure the security of local and remote access to the Oracle Private Cloud Appliance system:

- Create a login banner to state that unauthorized access is prohibited.
- Use access control lists to apply restrictions where appropriate.

- Set time-outs for extended sessions and set privilege levels.
- Use authentication, authorization, and accounting (AAA) features for local and remote access to a switch.
- Use the port mirroring capability of the switch for intrusion detection system (IDS) access.
- Implement port security to limit access based upon a MAC address. Disable auto-trunking on all ports for any switch connected to Oracle Private Cloud Appliance.
- Limit remote configuration to specific IP addresses using SSH.
- Require users to use strong passwords by setting a standard complexity for password formulation and establishing password expiration policies.
- Enable logging and send logs to a dedicated secure log host.
- Configure logging to include accurate time information, using NTP and timestamps.
- Review logs for possible incidents and archive them in accordance with the organization's security policy.

Security Feature Overview

Oracle Private Cloud Appliance is an engineered system that combines customer-premises-based hardware and preloaded software that allows you to build cloud services and applications inside your own data center. You can consume the core Oracle Cloud Infrastructure services from the safety of your own on-premises network, behind your own firewall.

As a rack-scale system, Oracle Private Cloud Appliance can be considered the smallest deployable unit of Oracle Cloud Infrastructure, aligned with the physical hierarchy of the public cloud design.

The self-contained aspect of the system makes some security features simpler to implement, while the cloud communication aspects require strict attention to other security features, such as virtual networking security.

From the security perspective, the Oracle Private Cloud Appliance system consists of three distinct layers, or enclaves. These layers are:

- Infrastructure-The infrastructure services provide a foundation for building PaaS and SaaS solutions; the deployed workloads can be migrated between the public and the private cloud infrastructure with minimal or no modification required. For this purpose, Oracle Private Cloud Appliance is fully compatible with Oracle Cloud Infrastructure.
- Service Enclave-The appliance infrastructure is controlled from the Service Enclave. It runs on a cluster of three management nodes and its functions includes hardware and capacity management, service delivery, monitoring, and tools for service and support. This is also where various tenancies are set up. A tenancy is a logical partition of a Compute Enclave controlled by the Service Enclave.
- Compute Enclave-The Compute Enclave offers compatibility with Oracle Cloud Infrastructure. This is where workloads are created, configured and hosted. The principal building blocks are compute instances (based on various operating system images) and associated virtual cloud network and storage resources.

Each enclave or layer provides its own set of interfaces: a web UI, a CLI and an API. With the exception of certain administration accounts, all permissions are isolated within a particular enclave or tenancy.

The layers also have their own security concerns.

Infrastructure Security Features

The Infrastructure administrative services, which have no equivalent in Oracle Cloud Infrastructure, are either internal or restricted to administrators of the appliance. These services enable the cloud services and provide support for the Service Enclave Administration operations, such as system initialization, compute node provisioning, capacity expansion, tenancy management, upgrading, and so on,

This section describes the security features of the Infrastructure Services layer.

Infrastructure Network Security

The network security consideration should be discussed before connecting the Oracle Private Cloud Appliance to the network.

- Considering intrusion prevention systems to monitoring the traffic into or out of the Oracle Private Cloud Appliance.
- Considering network layer firewall to protect the information into or out of the Oracle Private Cloud Appliance.
- Do not connect any unnecessary device to the Oracle Private Cloud Appliance.
- Do not use the Oracle Private Cloud Appliance infrastructure for any non-Oracle Private Cloud Appliance supported usage.

Management Switch Outbound Connectivity

Make sure that you:

- Keep the unused port disabled.
- Connect the device to port 1 (or port 2) for running the day 0 configuration only.
- Disconnect the device from port 1 (or port 2) after day 0 configuration.
- Keep the management switch separated from the data center network. Don’t connect any external device to the management switch.
- Enable DHCP snooping trust on Port 1 and Port 2.
- Don’t modify the management switch configuration.
- Change the switch password from the default to a strong password.
- Use Grafana dashboard to monitor the switch traffic.

Data Switch Outbound Connectivity

Make sure that you:

- Keep the unused port disabled.

- Don’t modify the spine switch configuration. The spine switch is controlled by the Oracle Private Cloud Appliance switch manager service.
- Understand the uplink port usage. Ports 7, 8, 9, and 10 are for Oracle Exadata connectivity only.
- Change the switch password from the default to a strong password.
- Use Grafana dashboard to monitor the switch traffic.

Data Security

It is important to protect data stored outside of the Oracle Private Cloud Appliance, on backups or removed hard drives.

Data located outside of the Oracle Private Cloud Appliance can be secured by backing up important data. The data should then be stored in an off-site, secure location. Retain the backups according to organizational policies and requirements.

When disposing of an old hard drive, physically destroy the drive or completely erase all the data on the drive. Deleting the files or reformatting the drive removes only the address tables on the drive. The information can still be recovered from a drive after deleting files or reformatting the drive. The Oracle Private Cloud Appliance disk retention support option allows the retention of all replaced hard drives and flash drives, instead of returning them to Oracle.

Security Patches and Firmware Upgrades

Effective and proactive software management is a critical part of system security.

Security enhancements are introduced through new releases and software updates. Oracle recommends installing the latest release of the software, and all necessary security updates on the equipment. The application of Oracle-recommended security updates is a best practice for the establishment of baseline security.

Operating system and kernel updates for the Oracle Private Cloud Appliance database servers and storage servers are delivered with the Oracle Private Cloud Appliance software updates. Power distribution unit (PDU) firmware updates are handled separately from the software and other firmware updates. Ensure that the PDU is running the latest approved firmware for the Oracle Private Cloud Appliance. As PDU firmware updates are not issued frequently, it is usually sufficient to check the PDU firmware release when upgrading the Oracle Private Cloud Appliance software..

Service Enclave Security Features

The appliance administrator's working environment is the Service Enclave. It is the part of the system where the appliance infrastructure is controlled. It provides tools for hardware and capacity management, tenancy control, and centralized monitoring of components at all system layers. Changes to setting in the Service Enclave can affect appliance availability.

Because the scope of the Service Enclave encompasses the entire appliance, access to the Service Enclave should be tightly controlled. Some best practices for the Service Enclave include:

- Do not share user information

- Create a limited number of users for the Service Enclave
- Use the Service Enclave Groups to control access for the users: ADMIN, MONITOR, SUPERADMIN, DRADMIN (Refer to the section on Administrator Access in the Oracle Private Cloud Appliance Concepts Guide for a description of the roles available in the Service Enclave)
- Creation of a user with the DRADMIN role may only be able to be done via the Service Enclave CLI at this time

Locally defined users (as opposed to federated users) have access to the Private Cloud Appliance via the Compute Web UI and the OCI CLI. Refer to the chapter on working in the Service Enclave in the Oracle Private Cloud Appliance Administrator Guide for accessing the Service Enclave.

Creating a Secure Compute Enclave Tenancy with Identity Provider

An Identity Provider (IdP) can be used for access to the Service Enclave User Interface. Once one or more IdPs are created and groups are mapped, the users in the directory can access the Service Enclave User Interface via the browser. Identity users do not gain access to the Administrative CLI.

For more information about managing IdPs, users and groups, see the "Federating with Microsoft Active Directory" section in the Oracle Private Cloud Appliance Administrator Guide.

Creating a Secure Compute Enclave Tenancy

A tenancy is an Oracle Private Cloud Appliance environment where users of the tenancy create and manage cloud resources in order to build and configure virtualized workloads. All the tenancies in the environment are collectively referred to as the Compute Enclave. A Service Enclave administrator that is a part of the SUPERADMIN group can create and delete a tenancy. As part of the creation process, the Service Enclave administrator defines the administrator for the tenancy. Once the tenancy and tenancy administrator are created, the Service Enclave Administrator can only change tenancy description or delete the tenancy and all contents. All modifications of the resources within a tenancy are handled by the tenancy users.

Some general best practices for a secure Compute Enclave tenancy:

- Do not use the same initial password for the initial administrator in each tenancy
- Consider using different administrator user names for each tenancy
- Advise the new tenancy administrator to immediately change the password upon receiving the tenancy administrator information
- Do not convey the user and password for Grafana access to the new tenancy administrator (monitoring and logging through Grafana is for the entire appliance)

Once created, the resources built by tenancy users in the new tenancy are owned by the tenancy, not by the Service Enclave, though resources for all tenancies come from a single pool of resources.

For more information about managing IdPs, users and groups, see the "Tenancy Management" section in the Oracle Private Cloud Appliance Administrator Guide.

Certification Expiration

A variety of certificates are used throughout the Oracle Private Cloud Appliance. The certificate key algorithm and expiration for various certificates is shown in the following table.

Certificate	Public Key Algorithm	Expiration
PCA 3.0 Root Certificate Authority (CA)	RSA 4096 bit	20 years
PCA 3.0 Intermediate CA used for internal services	RSA 4096 bit	10 years
PCA 3.0 Intermediate CA used for external-facing services	RSA 4096 bit	10 years
PCA 3.0 Server certificate	RSA 2048 bit	1 year
PCA 3.0 Client certificate	RSA 2048 bit	1 year
Vault generated server certificate (automated rotation)	RSA 2048 bit	31 days
Vault generated ephemeral certificate (automated rotation)	RSA 2048 bit	1 hour
Compute Certificate Signing Request (CSR) - Vault client certificate	RSA 2048 bit	1 year

Some short-lived certificates have automated rotation. If a customer replaces certificates, then those certificates are outside the scope of the above table.

Audit Logs

Audit logs for the Service Enclave are available from the Grafana dashboard and are intermixed with the logs from the Service Enclave UI web server and the admin service itself.

For using various filters to isolate audit information, see the "Accessing System Logs" and "Audit Logs" sections of the Oracle Private Cloud Appliance Administrator Guide.

Monitoring and Logging

The monitoring and logging information (including audit logs) for Oracle Private Cloud Appliance is accessed via the centralized Grafana console, a link is provided from the dashboard of the Service Enclave UI. At this time there is only one user profile available from Grafana. Data in Grafana applies to all tenancies, the Service Enclave and infrastructure components. To protect the information available in Grafana:

- Do not distribute the login information for Grafana (or Prometheus)
- Centralize requests for information from tenancy administrators through the Grafana administrator (including VM statistics, audit information for a particular tenancy, etc...)

For more information on status and health monitoring, see the "Status and Health Monitoring" section of the Oracle Private Cloud Appliance Administrator Guide.

Security Patches to Maintain a Secure Environment

Security patches are a subset of the patches provided via the patch process. For more information, refer to the process described in the Oracle Private Cloud Appliance Patching Guide

Compute Enclave Security Features

This section describes the security features of the Compute Enclave layer of Oracle Private Cloud Appliance.

Identity Provider Security Features

Companies commonly use an identity provider (IdP) to manage user login/passwords and to authenticate users for access to secure websites, services and resources. A tenancy administrator can federate with a supported IdP so that employees can use their existing login and password with the Oracle Private Cloud Appliance Compute Web UI.

Oracle Private Cloud Appliance supports the following Security Assertion Markup Language (SAML) 2.0 compliant identity providers:

- Microsoft Active Directory via Active Directory Federation Services

The following conditions apply to the use of Identity Providers with Oracle Private Cloud Appliance:

- Users can only access the Compute Web UI - A federated user is not managed within the Oracle Private Cloud Appliance Identity and Access Management (IAM) framework. As a result, they cannot have API keys added for use of the OCI CLI or manage preferences.
- Group mappings between given Active Directory groups to Oracle Private Cloud Appliance must be made for federated users to have authorization to do operations within the Compute Web UI.
- Multifactor authentication to the Oracle Private Cloud Appliance Compute Web UI is only available via an Identity Provider.

For cases where the Identity Provider uses self-signed certificates, additional steps must be taken to add the Certificate Authority (CA) trust information to the Oracle Private Cloud Appliance prior to adding the IdP. To add the CA information, an appliance administrator will need to:

- Access a management node on the Oracle Private Cloud Appliance using the management node `root` account.
- Distribute the CA X.509 certificate to the management nodes using the tools included on the management node.

For more information, see the "Verifying Identity Provider Self-Signed Certificates" section of the Oracle Private Cloud Appliance Administrator Guide

Oracle makes the following recommendations with respect to Identity Providers in the tenancies:

- Use federation to manage authentication to the Compute Web UI if a supported Identity Provider is available.
- Create an administrators group within the compute tenancy that maps to the federated IdP administrator group and ensure a federated user is assigned to the IdP administrator group.
- Only use the local (non-federated) tenancy administrator for emergency purposes, such as:
  - Change the local (non-federated) administer password to an extremely complex password.
  - Escrow the local (non-federated) password to a safe location.
  - Restrict the federated IdP administrator group from modifying the local Administrators and the local Administrator group.
  - Periodically monitor the audit logs for illicit use of the local administrator account(s) and check for attempts at unauthorized actions.
  - Consider rotating the locally defined administrator's password and re-escrowing periodically and/or immediately after use.

For an overview of support for Identity Providers see the Identity and Access Management Overview chapter of the Oracle Private Cloud Appliance Concepts Guide.

For an overview of federating a tenancy with Microsoft Active Directory see the "Federating with Microsoft Active Directory" section of the Oracle Private Cloud Appliance User Guide.

IAM Security Features

Oracle Private Cloud Appliance Identity and Access Management (IAM) provides authentication of local users and authorization to resources. IAM facilitates organizational principles that aid with security management such as:

- Compartments - Collections of related resources (such as cloud networks, compute instances, or block volumes) that can be accessed by groups that have been given permission by a tenancy administrator.
- Groups - Collections of users that have similar requirements for authorizations (users can be in multiple groups).
- Resources - Objects (such as compute instances, block volumes, users, and so on) created using the various Oracle Cloud Infrastructure services.
- Tags - Metadata in the form of keys and values that are added to resources
- Tenancy - The root compartment that holds all resources, including additional compartments.

A security policy specifies the types of access a group defined in IAM has to resources at the specified aggregation level (Tenancy, Compartment, or Service) that can be further refined with information about tags.

For more information about policies in general, see the "Managing Policies" section in the Identity and Access Management chapter of the Oracle Private Cloud Appliance User Guide.

An end goal of a tenancy administrator is to achieve the principle of least privilege:

- Enable users to achieve what their role requires with resources and privileges required for their role.
- Disallow users from accessing resources or accessing resources with privileges that are not necessary for their role.
- Enable ease of administration to add and remove resources and privileges to a user or user group.

To achieve the principle of least privilege, use a combination of tenancy-use organizational concepts and security policy management techniques.

When designing and maintaining the tenancy:

- The root compartment, tenancy, offers central control and visibility for tenancy-wide administrators, while also allowing the tenancy to be subdivided to meet the needs of the teams.
- Compartments provide an effective mechanism to group tenancy resources based on their access privileges and authorize groups of users to access the compartments on as needed basis. For example, a compartment can be created to include all resources belonging to a business unit, and authorize only members of the business unit to access the compartment. Similarly, a group's access to a compartment can be revoked quickly when they do not need it anymore.
- Keep the following in mind with compartments and resource assignments:
  - Every resource belongs to a compartment.
  - A resource can be reassigned to a different compartment after creation.
  - A compartment can be deleted after creation.
- Resource tags provide a way to logically aggregate resources distributed across multiple compartments. For example, tenancy resources can be tagged as `test` or `production` depending on their use.

For more information about resource tags (free-form and defined tags), see the "Creating and Managing Compartments" section in the Identity and Access Management chapter, and the Resource Tag Management chapter of the Oracle Private Cloud Appliance User Guide.

When managing users in a tenancy:

- Create an IAM user for everyone in the customer organization who needs access to resources. Do not share user accounts, especially those with administrative accounts. Using distinct users enables easier enforcement of least privilege access for each user, and captures helps track actions in audit logs.
- The recommended unit of administration is IAM groups, making it easier to manage and keep track of security permissions (as opposed to individual users). Create groups with permissions to do commonly needed tasks (for example, network administration, volume administration), and assign users to these groups on an as-needed basis. IAM permissions can be used to give a group access to resources across multiple compartments in a tenancy.
- Periodically review membership of IAM users in IAM groups, and remove users from groups they do not need access to anymore. Using group membership to manage user access scales well with increasing number of users.
- Deactivate IAM users who do not need access to tenancy resources. Deleting an IAM user removes the user permanently. You can temporarily deactivate an IAM user by doing the following:

  - Rotate the user password and throw it away.
  - Remove all tenancy permissions of the user by removing membership from all groups.

The above guidance on managing tenancy users changes slightly with IdP integration. Please note that:

- Cooperation with the IdP administrator to add and remove groups directly from a user is required.
- Group management rules still apply.

For more information on OCI CLI usage for IAM management, see the Identity and Access Management chapter in the Oracle Private Cloud Appliance User Guide.

Creating Service-level Administrators for Least Privilege

To implement the security principle of least privilege, groups can be created to administer individual services, with users being added to one or more of the service administrator roles. For example, network administrators need administrative (`manage`) access only to VCN resources, and not to other resources. A compute administrator may need compute privileges, but their work often also involves storage and volumes, requiring additional administration privileges. The following example shows policies that break administration into the more granular scope, allowing administrators to allocate and deallocate service-level authorizations.

First, a set of groups are created using the CLI commands (the same actions can be done with the GUI):

```
oci iam group create --name TenancyAdmin --description "Tenancy administrators"
oci iam group create --name VolumeAdmin --description "Volume admins includes
block volumes)"
oci iam group create --name NetworkAdmin --description "Network admins (VCNs,
subnets, etc...)"
oci iam group create --name StorageAdmin --description "Storage administrators
(Object storage)"
oci iam group create --name InstanceAdmin --description "Instance admins
(compute instances, etc.)"
```

These groups have no users at creation. There are also no security policies associated with the groups at this time.

Next, a set of policies are created that enable the various groups to administer the services:

```
oci iam policy create --name ServiceAdministratorPolicies --description
"Policies for svc admin"
  --statements '["Allow group TenancyAdmin to manage all-resources in tenancy",
  "Allow group VolumeAdmin to manage volume-family in tenancy",
  "Allow group NetworkAdmin to manage virtual-network-family in tenancy",
  "Allow group StorageAdmin to manage object-family in tenancy",
  "Allow group InstanceAdmin to manage instance-family in tenancy"]'
```

Once these groups and policies are in place, a local user can be added and removed from service-level administration duties across the entire tenancy quickly and efficiently:

```
oci iam group add-user --group-id ocid1.group.<id> --user-id ocid1.user.<id>
oci iam group remove-user --group-id ocid1.group.<id> --user-id ocid1.user.<id>
```

Break tenancies up into compartments to support multiple project, environments, or other organizational structures. The guidance to create service level administration groups can be quickly adapted to creating service level administration groups *for a compartment*.

For example, if there is a compartment named "HR" to support the Human Resources cloud, choose a group name such as `HRNetworkAdmin`.

Then adapt the policy statements appropriately to use the HR compartment rather than the tenancy:

```
"Allow group HRNetworkAdmin to manage virtual-network-family in compartment HR"
```

Creating Security Auditors

Not all tasks require active management of resources. Compliance auditors are tasked with examining cloud resources and assessing access to the resources. The following policy allows users in the group `InternalAuditors` to inspect (`list`) all resources in a tenancy:

```
"Allow group InternalAuditors to inspect all-resources in tenancy"
```

Alternatively, auditors may have specific roles to play. The following policy statement allows users in group `UserAuditors` to inspect just users and groups.

```
"Allow group UserAuditors to inspect users in tenancy"
"Allow group UserAuditors to inspect groups in tenancy"
```

If you want to create an auditor group that can only inspect VCN firewalls in the tenancy, then use the following policy:

```
"Allow group FirewallAuditors to inspect security-lists in tenancy"
```

You can constrain the policies in all these policy examples to a compartment by specifying `compartment` ***<name>*** (where ***<name>*** is the compartment name) in the policy.

Restricting the Ability to Change Tenancy Administrator Group Membership

Members in the group `Administrators` can manage all resources in a tenancy. Membership of the `Administrators` group is controlled by users in the group. Usually, it's convenient to have a group to create and add users in the tenancy, but restrict them from making changes to the `Administrators` group membership. The following example creates a group `UserAdmins` to do this.

```
"Allow group UserAdmins to inspect users in tenancy"
"Allow group UserAdmins to inspect groups in tenancy"

"Allow group UserAdmins to use users in tenancy where target.group.name!
='Administrators'"
"Allow group UserAdmins to use groups in tenancy where target.group.name!
='Administrators'"
```

The third and fourth policy statements allow `UserAdmins` to add users and groups using APIs (`UpdateUser`, `UpdateGroup`) to all groups in the tenancy except the `Administrators` group. However, because `target.group.name!='Administrators'` is not related to the `list` and `get` APIs (`ListUsers`, `GetUser`, `ListGroups`, and `GetGroup`), these APIs will fail without other

commands. So you must explicitly add `inspect` in the first and second policy statements to allow `UserAdmins` to get user and group membership information.

Preventing Deletion or Updating of Security Policies

The following example creates a group `PolicyAdmins` to be able to create and list security policies created by tenancy administrators, but not delete or update them:

```
"Allow group PolicyAdmins to use policies in tenancy"
"Allow group PolicyAdmins to manage policies in tenancy where
request.permission='POLICY_CREATE'"
```

The second security policy statement explicitly allows `POLICY_CREATE` permission, but not `POLICY_DELETE` and `POLICY_UPDATE`.

Preventing Administrators from Accessing or Altering User Credentials

Some compliance requirements need separation of duties, especially where user credential management functionality is separated from tenancy management. In this case, you can create two administration groups, `TenancyAdmins` and `CredentialAdmins`.

`TenancyAdmins` can perform all tenancy management functions except user credential management, and `CredentialAdmins` can manage user credentials.

`TenancyAdmins` can access all APIs except those that list, update, or delete user credentials. `CredentialAdmins` can only manage the user credentials.

To establish these administration groups, use the following:

```
"Allow group TenancyAdmins to manage all resources in tenancy
 where all {request.operation!='ListApiKeys',
            request.operation!='ListAuthTokens',
            request.operation!='ListCustomerSecretKeys',
            request.operation!='UploadApiKey',
            request.operation!='DeleteApiKey',
            request.operation!='UpdateAuthToken',
            request.operation!='CreateAuthToken',
            request.operation!='DeleteAuthToken',
            request.operation!='CreateSecretKey',
            request.operation!='UpdateCustomerSecretKey',
            request.operation!='DeleteCustomerSecretKey'}"
"Allow group CredentialAdmins to manage users in tenancy
 where any {request.operation='ListApiKeys',
            request.operation='ListAuthTokens',
            request.operation='ListCustomerSecretKeys',
            request.operation='UploadApiKey',
            request.operation='DeleteApiKey',
            request.operation='UpdateAuthToken',
            request.operation='CreateAuthToken',
            request.operation='DeleteAuthToken',
            request.operation='CreateSecretKey',
            request.operation='UpdateCustomerSecretKey',
            request.operation='DeleteCustomerSecretKey'}"
```

File Storage Service Security Features

The Oracle Private Cloud Appliance File Storage Service provides a durable, scalable, secure, enterprise-grade network file system. With the service, a user with proper authorization can create and manage file systems that can be accessed from compute instances in a Virtual Cloud Network (VCN).

The File Storage Service:

- Supports NFSv3, v4, v4.1, and SMB
- Encrypts data on disk using Advanced Encryption Standard (AES) 128-bit algorithm.
- Allows periodic snapshots of the file system to be taken (see the "Managing Snapshots" section of the Oracle Private Cloud Appliance User Guide).
- Supports a variety of NFS export options to manage client access and use.
- Uses VCN and Network Security Groups to manage client access to shares.

Administrators can use the File Storage Service as long as they have authorization through a security policy such as:

- Resource Type Family: file-family
- Resource Types: file-systems, mount-targets, export-sets

If a group `FileAdmin` exists, a policy that would grant them authorization to manage all aspects of the File Storage Service would be:

```
"Allow group FileAdmin to manage file-family in tenancy"
```

Because data storage is a critical function of any system, it may be useful to create a second group for users that allows them to create file systems, but does not allow accidental deletion of file systems. For example, if there is a group `FileUsers`, then the following policy statements could be added to limit their access:

```
"Allow group FileUsers to manage file-systems in tenancy
       where request.permission!='FILE_SYSTEM_DELETE'"
"Allow group FileUsers to manage mount-targets in tenancy
       where request.permission!='MOUNT_TARGET_DELETE'"
"Allow group FileUsers to manage export-sets in tenancy
       where request.permission!='EXPORT_SET_DELETE'"
```

For more ways to manage access to the File Storage Service, see the "Managing Policies" section in the Identity and Access Management chapter of the Oracle Private Cloud Appliance User Guide.

For a description of how to manage access to file system, including how to restrict access or allow access, from clients, see the section "Controlling Access to File Storage" in the File System Storage chapter of the Oracle Private Cloud Appliance User Guide.

Object Store Security Features

The Oracle Private Cloud Appliance Object Storage service stores and provides access to large amounts of unstructured data of any content type. Content stored in object storage can be accessed from within the Compute Enclave by compute instances as well as from the data center through the domain of the Oracle Private Cloud Appliance.

The Object Storage service:

- Encrypts data on disk (at rest) using Advanced Encryption Standard (AES) 128-bit algorithm. Encryption is on by default and cannot be turned off. The encryption keys are themselves encrypted with a master encryption key.
- In addition, customers can use client-side encryption to encrypt objects prior to upload to their Object Storage buckets. The Oracle Private Cloud Appliance supports the Amazon S3 Compatibility API, along with the client-side object encryption support available in AWS SDK for Java. For more details about this SDK, see Amazon S3 Compatibility API.
- Data in transit between customer clients (for example, SDKs and CLIs) and Object Storage public endpoints is encrypted with TLS 1.2 by default.
- Data integrity is facilitated by a checksum generated for each uploaded object and, for multi-part uploads, a checksum generated for each part.
- Objects can have revokable pre-authenticated requests built with varying authorization levels.
- Object versioning is available to retain changes to objects.
- Write-once Read-many (WORM) retention rules can be set to ensure an object retains its original contents.
- Users that are authenticated to the Oracle Private Cloud Appliance have the ability to manage the Object Storage service and resources that are managed within the security policy framework.

For more details on using the above features, see the "Object Storage" section in the Oracle Private Cloud Appliance User Guide

Security Recommendations

Assign least privileged access for IAM users and groups to resource types in *object-family* (such as objectstorage-namespaces, buckets, and objects). For example, the `inspect` verb gives the least privilege. The `inspect` verb lets you check to see if a bucket exists (`HeadBucket`) and list the buckets in a compartment (`ListBucket`). The `manage` verb gives all permissions on the resource. You can create IAM security policies to give appropriate bucket and object access to various IAM groups.

For more information about IAM verbs and permissions for Object Storage buckets and objects, see Details for Object Storage, Archive Storage, and Data Transfer.

For users without IAM credentials, we recommend that you use pre-authenticated requests (PARs) to give time-bound access to objects or buckets.

Pre-Authenticated Requests

Pre-authenticated requests provide a mechanism to give access to objects and buckets without requiring the client or user to log into the Oracle Private Cloud Appliance. As a result, objects and buckets can be used without an IAM user defined on the Oracle Private Cloud Appliance.

An IAM user with appropriate privileges for accessing objects creates a URL that grants time-bound access to objects. For more information on these grants, see the Oracle Cloud Infrastructure information on Using Pre-Authenticated Requests. Please note that:

- The creator of a pre-authenticated request must have `PAR_MANAGE` permission and the appropriate IAM permissions for the access type that you are granting. You can create a pre-authenticated request that grants read, write, or read/write access to one of the following:
  - All objects in the bucket.
  - A specific object in the bucket.
  - All objects in the bucket that have a specified prefix.

  For requests that apply to multiple objects, you can also decide whether you want to let users list those objects.
- Pre-authenticated request accesses to a bucket are logged in Audit logs. Pre-authenticated request accesses to an object are logged in Service logs.

> **Important:**
>
> The unique URL provided by the system when you create a pre-authenticated request is the only way a user can access the request target. Copy the URL to durable storage. The URL is displayed only at the time of creation, is not stored in Object Storage, and cannot be retrieved later.

Data Durability and Integrity

The Object Storage service provides a variety of ways to ensure data remains consistent and intact once stored. Please note that:

- Data loss can be minimized by preventing inadvertent deletes by an authorized user or malicious deletes:
  - Use object versioning to automatically create an object version each time a new object is uploaded, an existing object is overwritten, or when an object is deleted.
  - Give `BUCKET_DELETE` and `OBJECT_DELETE` permissions to a minimum set of IAM users and groups. Grant delete permissions only to tenancy and compartment administrators.
- Write once read many (WORM) compliance requires that objects cannot be deleted or modified. Use retention rules to achieve WORM compliance. Retention rules are configured at the bucket level and are applied to all individual objects in the bucket. You cannot update, overwrite, or delete objects or object metadata until the retention rule is deleted (indefinite rule) or for the duration specified (time-bound rules).

  For an independent assessment of the Object Storage retention rules feature's ability to meet regulatory requirements for record management and retention, see Cohasset Associate's SEC 17a-4(f), FINRA 4511(c), CFTC 1.31(c)-(d) and MiFID II Compliance Assessment.
- Objects are stored in a ZFS file system with a SHA-256 checksum to avoid phantom reads and detect invalid data returned from devices.

In addition to facilities provided for durability, Object Storage provides mechanisms to ensure data integrity:

- A checksum is provided for all objects uploaded to Object Storage. The checksum can be used in two ways:

  - To verify that the object stored is the object that was uploaded
  - To verify that the object retrieved is the one that was originally stored
- Multipart uploads are used by the Object Storage service for efficiency and resiliency on large object uploads. In a multipart upload, a large object is broken up into smaller parts by specifying a part size in MiB. Each part is uploaded separately. Object Storage then combines all the parts to re-create the original object. If any of the parts fail to upload, only the failed parts need to be retried for upload, not the entire object. In a multipart upload, checksum values are computed for each part of the upload, and a single checksum is computed over all of the individual checksum values to get the checksum value reported by the object upload. To verify the value returned for a multipart upload, follow the same process for offline checksum calculation.

Using the checksum returned when the object is stored, the contents of the object can be verified when it is downloaded again or against the original object to verify uploaded object correctness.

Operating systems have a variety of tools for checksum verification. The checksum returned by an object upload (or viewing an object in the bucket) is a Base-64 encoded value. This value may have to be converted to hexadecimal depending on the tools used for checksum comparison.

Networking Security Features

VCN Feature	Security Description
Public and private subnets	A VCN can be partitioned into subnets. Subnets are specific to an availability domain. Instances inside private subnets cannot have public IP addresses. Instances inside public subnets can optionally have public IP addresses at your discretion.
Security rules	Security rules provide stateful and stateless firewall capability to control network access to your instances. To implement security rules in your VCN, you can use network security groups (NSGs) or security lists. For more information, see Comparison of Security Lists and Network Security Groups.

VCN Feature	Security Description
Gateways	Gateways let resources in a VCN communicate with destinations outside the VCN. The gateways include: • Internet gateway: For internet connectivity (for resources with public IP addresses in public subnets). • NAT gateway: For internet connectivity without exposing the resources to incoming internet connections (for resources in private subnets). • Dynamic routing gateway (DRG): For connectivity to your data center network. • Service gateway: For private connectivity to Oracle services such as Object Storage. • Local peering gateway (LPG): For connectivity to a peered VCN in the same region.
Route table rules	Route tables control how traffic is routed from your VCN's subnets to destinations outside the VCN. Routing targets can be VCN gateways or a private IP address in the VCN.
IAM polices for virtual-network-family	IAM policies specify access and actions permitted by IAM groups to resources in a VCN. For example, IAM polices can give administrative privileges to network administrators who manage the VCNs, and scoped-down permissions to normal users.

Oracle recommends that you periodically monitor Oracle Cloud Infrastructure Audit logs to review changes to VCN network security groups, security lists, route table rules, and VCN gateways.

Network Segmentation: VCN Subnets

Using multiple subnets within a VCN to deploy compute instances is a common strategy for controlling access to the data center network. To do this:

- Formulate a tiered subnet strategy for the VCN, to control network access. A common design pattern is to have the following subnet tiers:

  1. **Public subnet** for externally accessible hosts such as NAT instances, intrusion detection (IDS) instances, and web application servers
  2. **Private subnet** for internal hosts such as databases

  No special routing is required for the instances in the different subnets to communicate. However, you can control the types of traffic between the different tiers by using the VCN's network security groups or security lists.

- Instances in the private subnet only have private IP addresses and can be reached only by other instances in the VCN. Oracle recommends that you place security-sensitive hosts (DB systems, for example) in a private subnet, and use security rules to control the type of connectivity to hosts in a public subnet. In addition to VCN security rules,

configure host-based firewalls such as `iptables` or `firewalld` for network access control, as a defense-in-depth mechanism.

- You can add a service gateway to your VCN to enable DB systems in the private subnet to directly back up to Object Storage without the traffic traversing the data center network. You must set up the routing and security rules to enable that traffic. For more information for bare metal or virtual machine DB systems, see Network Setup for DB Systems. For more information for Oracle Exadata DB systems, see Network Setup for Exadata Cloud Service Instances.

VCN Security Rules and Security Lists

VCN security involves creating and using rules that are gathered into security lists or network security groups (NSGs). The rules can be stateful or stateless. Stateful rules presume various things about an instance interaction. For example, a stateful rule that applies to a request to an instance assumes that there will be a response and automatically allows this response. In contrast, stateless rules do not presume anything about any interactions. There are just messages from one instance to another, and the stateless rules apply to everything regardless of what has gone before. Stateful rules require overhead processing to track states that stateless rules do not. Instances with heavy and widely varied traffic, such as web sites, should use stateless rules where possible to minimize system loads.

> **Note:**
>
> Care is needed when creating stateless and stateful rules. When a message appears that fits both stateful and stateless rule criteria, the stateless rule is applied. This results in responses being blocked to requests that seemingly should be allowed.

Your VCN might have subnets that use the default security list. Do not delete any of the list's default security rules unless you've first confirmed that resources in your VCN do not require them. Otherwise, you might disrupt your VCN's connectivity.

Keep in mind that:

- A security rule is stateful by default, but can also be configured to be stateless. A common practice is to use stateless rules for high-performance applications. In a case where network traffic matches both stateful and stateless security lists, the stateless rule takes precedence. For more information about configuring VCN security rules, see Security Rules for the Oracle Cloud Infrastructure.
- To prevent unauthorized access or attacks on Compute instances, Oracle recommends that you use a VCN security rule to allow SSH or RDP access only from authorized CIDR blocks rather than leave them open to the internet (0.0.0.0/0). For additional security, you can temporarily enable SSH (port 22) or RDP (port 3389) access on an as-needed basis using the VCN API `UpdateNetworkSecurityGroupSecurityRules` (if you're using network security groups) or `UpdateSecurityList` (if you're using security lists). For more information about enabling RDP access, see To enable RDP access in Creating an Instance for the Oracle Cloud Infrastructure. For performing instance health checks, Oracle recommends that you configure VCN security rules to allow ICMP pings. For more information, see Rules to Enable Ping Oracle Cloud Infrastructure.

VCN network security groups (NSGs) and security lists enable security-critical network access control to Compute instances, and it is important to prevent any unintended or unauthorized changes to NSGs and security lists. To prevent unauthorized changes, Oracle recommends that you use IAM policies to allow only network administrators to make NSG and security list changes.

The default security list for a VCN comes without stateless rules: all the default security list rules are stateful. In most cases, the default rules should be changed to allow only inbound traffic from authorized subnets.

The default stateful security list rules are:

- Stateful ingress: Allow TCP traffic on destination port 22 (SSH) from authorized source IP addresses and any source port. This rule makes it easy for you to create a new cloud network and public subnet, launch a Linux instance, and then immediately use SSH to connect to that instance without needing to write any security list rules yourself.
- Stateful ingress: Allow ICMP traffic type 3 code 4 from authorized source IP addresses. This rule enables your instances to receive Path MTU Discovery fragmentation messages.
- Stateful ingress: Allow ICMP traffic type 3 (all codes) from your VCN's CIDR block. This rule makes it easy for your instances to receive connectivity error messages from other instances within the VCN.
- Stateful egress: Allow all traffic. This allows instances to initiate traffic of any kind to any destination. Notice that this means the instances with public IP addresses can talk to any internet IP address if the VCN has a configured internet gateway. And because stateful security rules use connection tracking, the response traffic is automatically allowed regardless of any ingress rules.

> **Note:**
>
> The default security list does not include a rule to allow Remote Desktop Protocol (RDP) access. If you're using Microsoft Windows images, make sure to add a stateful ingress rule for TCP traffic on destination port 3389 from authorized source IP addresses and any source port.

The default security list does not include a rule to allow ping requests. If you plan to ping an instance, ensure that the instance's applicable security list includes an additional stateful ingress rule to specifically allow ICMP traffic type 8 from the source network you plan to ping from. To allow ping access from the data center, use `0.0.0.0/0` for the source. Note that this rule for pinging is separate from the default ICMP-related rules in the default security list. Do not remove those rules.

If you decide to use stateless security rules to allow traffic to and from endpoints outside the VCN, it's important to add a security rule that allows ingress ICMP traffic type 3 code 4 from source `0.0.0.0/0` and any source port. This rule enables your instances to receive Path MTU Discovery fragmentation messages. This rule is critical for establishing a connection to your instances. Without it, you can experience connectivity issues.

Instances can send and receive UDP traffic. In some cases, UDP packets might be fragmented on links with smaller MTU sizes. If a UDP packet is too large for the connection size limit, it is fragmented. However, only the first fragment from the packet contains the protocol and port information. If the security rules that allow this ingress or egress traffic

specify a particular port number (source or destination), then the fragments after the first one are dropped. If you expect your instances to send or receive large UDP packets, set both the source and destination ports for the applicable security rules to ALL (instead of a particular port number).

On their own, security lists define a set of security rules that applies to all the VNICs in an entire subnet. To use a given security list with a particular subnet, you associate the security list with the subnet either during subnet creation or later. A subnet can be associated with a maximum of five security lists. Any VNICs that are created in that subnet are subject to the security lists associated with the subnet.

Controlling Traffic with Network Security Groups

Security list rules can be gathered into Network Security Groups (NSGs) to make application of sets of rules easier to a grouping of VNICs. NSGs let you define a set of security rules that apply to a group of VNICs of your choice (or the VNICs' parent resources such as load balances or DB systems). The VNICs that belong to a set of Compute Enclave instances that all have the same security posture can use an NSG to apply a set of rules.

To use a given NSG, you add the VNICs of interest to the group. Any VNICs added to that group are subject to that group's security rules. A VNIC can be added to a maximum of five NSGs.

> **Important:**
>
> Oracle recommends using NSGs instead of security lists because NSGs let you separate the VCN's subnet architecture from your application security requirements.

However, you can use both security lists and NSGs together if you want. In fact, there is no requirement to use NSGs. Also, NSGs are not supported by all types of Oracle Private Cloud Appliance services.

Currently, the following types of parent resources support the use of NSGs:

- Compute instances: When you create an instance, you can specify one or more NSGs for the instance's primary VNIC. If you add a secondary VNIC to an instance, you can specify one or more NSGs for that VNIC. You can also update existing VNICs on an instance so that they are in one or more NSGs.
- Mount targets: When you create a mount target for a file system, you can specify one or more NSGs. You can also update an existing mount target to use one or more NSGs.
- DNS resolver endpoint: When you create an endpoint for a private DNS resolver, you can specify one or more NSGs. You can also update an existing endpoint to use one or more NSGs.

For resource types that do not support NSGs, continue to use security lists to control traffic in and out of those parent resources.

Working with NSGs is a three-step process:

1. Create an NSG.

2. Add security rules to the NSG.
3. Add parent resources (or more specifically, VNICs) to the NSG. You can do this when you create the parent resource, or you can update the parent resource and add it to one or more NSGs. When you create a Compute instance and add it to an NSG, the instance's primary VNIC is added to the NSG. Separately, you can create secondary VNICs and optionally add them to NSGs.

You must remove all VNICs from an NSG before deleting an NSG.

Secure Connectivity for VCN Gateways

VCN gateways provide external connectivity (internet, on-premises, or peered VCN) to VCN hosts. See the table at the start of the Networking Security Features section of this guide for a list of the type of gateways. Oracle recommends that you use an IAM policy to allow only network administrators to create or modify VCN gateways.

Carefully consider allowing internet access to any instances. For example, you don't want to accidentally allow internet access to sensitive database instances. In order for an instance in a VCN to be *publicly accessible from the internet*, you must configure the following VCN options:

- The instance must be in a VCN public subnet.
- The VCN containing the instance must have an internet gateway enabled and configured to be the routing target for outbound traffic.
- The instance must have a public IP address assigned to it, either for an internet gateway to a public subnet (for instances with public IPs), or for a Network Address Translation (NAT) Gateway to a private subnet (for instances with private IPs).
- The VCN security list for the instance's subnet must be configured to allow inbound traffic from `0.0.0.0/0`, but for the specific destination port and IP protocol only. Or if you're using network security groups (NSG), the instance must be in an NSG that allows that traffic.

  For more information about VCN gateway security, see the "Network Security" section in the Oracle Private Cloud Appliance Concepts Guide

DNS Security Features

DNS zones and records are critical for accessibility of web properties. Incorrect updates or unauthorized deletions could result in outage of services, accessed through the DNS names. Oracle recommends that you limit IAM users who can modify DNS zones and records.

Oracle Private Cloud Appliance DNS uses DNSSEC. DNSSEC has vulnerabilities that are discussed at the externalk site on DNSSEC Vulnerabilities.

VCN Security Policy Examples

Here are three examples of security policies for VCNs:

1. Allow Users to Only View Security Lists
   - Your network administrators are the personnel who should have the ability to create and manage network security groups and security lists.

- The first line in the following example policy allows the NetworkUsers group to view security lists and their contents. This policy does not let the group create, attach, delete, or modify security lists.
- The second line lets the NetworkUsers group view the security rules in NSGs, and also view what VNICs and parent resources are in NSGs. The second line does not let the NetworkUsers group change the security rules in NSGs.

```
"Allow group NetworkUsers to inspect security-lists in tenancy"
"Allow group NetworkUsers to use network-security-groups in
tenancy"
```

2. Prevent Users from Creating External Connection to the Internet
   - In some cases, you might need to prevent users from creating external internet connectivity to their VCN. In the following example policy, the NetworkUsers group is prevented from creating an internet gateway.

```
"Allow group NetworkUsers to manage internet-gateways in tenancy
where request.permission!='INTERNET_GATEWAY_CREATE'"
```

3. Prevent Users from Updating DNS Records and Zones
   - In the following example policy, the NetworkUsers group is prevented from deleting and updating DNS zones and records.

```
"Allow group NetworkUsers to manage dns-records in tenancy
 where all {request.permission!='DNS_RECORD_DELETE',
            request.permission!='DNS_RECORD_UPDATE'}"

"Allow group NetworkUsers to manage dns-zones in tenancy
 where all {request.permission!='DNS_ZONE_DELETE',
            request.permission!='DNS_ZONE_UPDATE'}"
```

Useful CLI Commands for VCN Security

In all the following examples, the environment variables $C and $VCN are set to compartment OCID and VCN OCID, respectively.

1. List open security lists in a VCN

```
# list open (0.0.0.0/0) security lists in VCN $VCN in compartment $C
oci network security-list list -c $C --vcn-id $VCN | grep "source" | grep
"\"0.0.0.0/0\""
```

2. List gateways in a VCN

```
# list all internet gateways in VCN $VCN in compartment $C
oci network internet-gateway list -c $C --vcn-id $VCN
# list all DRGs in compartment $C
oci network drg list -c $C
# list all local peering gateways in vcn $VCN in compartment $C
oci network local-peering-gateway list -c $C --vcn-id $VCN
```

3. List route table rules in a VCN

```
# list route table rules in VCN $VCN in compartment $C
oci network route-table list -c $C --vcn-id $VCN
```

Compute Service Security Features

The core feature of the compute service are compute instances and related resources such as instance configurations, instance pools, and custom images. The compute

service relies on several services: block volume for boot images and volume expansion, networking for connectivity and object storage for image import.

You should:

- Apply restrictive, least privilege access, IAM policies and techniques for block volumes, networks and object storage. This is critical to prevent malicious use of custom images and preventing compute instances from network access and being accessed.
- Apply restrictive, least privilege access to the compute service to prevent changes to configuration and deployed resources.

To prevent inadvertent or malicious termination of critical instances (for example, production instances), Oracle recommends that you give `INSTANCE_DELETE` permissions to a minimal set of groups. Give `DELETE` permissions only to tenancy and compartment administrators. For instance policy examples, see the Instance Security Policy Examplessection. of this guide

Instance Metadata Access Control

Instance metadata (located at `http://169.254.169.254`) provides predefined instance information, such as OCID and display name, and custom fields. Oracle recommends that you limit instance metadata access to privileged users on the instance. The following example shows how to use `iptables` to restrict instance metadata access to the root user.

```
iptables -A OUTPUT -m owner ! --uid-owner root -d 169.254.169.254 -j
DROP
```

Instances use link local addresses to access the instance metadata service (`169.254.169.254:80`), DNS (`169.254.239.254:53`), and NTP (`169.254.169.254:123`). You can use host-based firewalls, such as iptables, to ensure that only the root user is authorized to access these IPs. Make sure these operating system firewall rules are not altered.

Instance Network Access Control

There are a variety of best practices for Oracle Linux compute instances that should be followed. Similar restrictions are available on other operating system types.

Security Recommendation	Configuration sshd_config	Comments
Use public-key logins only	PubkeyAuthentication yes	Periodically review SSH public keys in the `~/.ssh/authorized_keys` file
Disable password logins	PasswordAuthentication no	Mitigates password brute-force attacks
Disable root logins	PermitRootLogin no	Prevents root privileges for remote logins
Change SSH port to a non-standard port number	Port <port-number>	(Optional) Verify the change does not break applications using port 22 for SSH.

In addition:

- Harden secure shell (SSH) on all instances. The following table shows some SSH security recommendations. SSH configuration options can be set in the sshd_config file (located at `/etc/ssh/sshd_config` in Linux).
- Use secure SSH private keys to access instances and to prevent inadvertent disclosures. For more information about creating an SSH key pair and configuring an instance with the keys, see Managing Key Pairs on Linux Instances.
- To limit instance access to authorized IP addresses, use VCN network security groups or security lists. Fail2ban is an application that blocklists IP addresses involved in brute-force sign-in attempts (that is, too many failed attempts to sign in to an instance). By default, `Fail2ban` inspects SSH accesses, and you can configure it to inspect other protocols. For more information about `Fail2ban`, see Fail2ban Main Page.
- In addition to VCN network security groups and security lists, use host-based firewalls, such as `iptables` and `firewalld`, to restrict network access to instances by controlling ports, protocols, and packet types. Use these firewalls to prevent potential network security attack reconnaissance, such as port scanning and intrusion attempts. Custom firewall rules can be configured, saved, and initialized on every instance boot.

  The following example shows commands for `iptables`:

  ```
  # save iptables rules after configuration
  sudo iptables-save > /etc/iptables/iptables.rules
  # restore iptables rules on next reboot
  sudo /sbin/iptables-restore < /etc/iptables.rules
  # restart iptables after restore
  sudo service iptables restart
  ```

Instance Entropy

Instances have random number generators whose output is fed into the entropy pools used by the operating system to generate random numbers. In Linux instances, `/dev/random` is non-blocking and should be used for security applications requiring random numbers. You can use the following commands to check the throughput and quality of the random numbers generated by `/dev/random` before using the output in applications.

```
# check sources of entropy
sudo rngd -v
# enable rngd, if not already
sudo systemctl start rngd
# verify rngd status
sudo systemctl status rngd
# verify /dev/random throughput and quality using rngtest
cat /dev/random | rngtest -c 1000
```

Host Security Hardening and Patching

Establish a baseline for security hardening of Linux and Microsoft Windows images running on instances. For more information about security hardening of Oracle Linux images, see Tips for Hardening an Oracle Linux Server. The Center for Internet Security Benchmarks provides a comprehensive set of operating system security hardening benchmarks for various distributions of Linux and Microsoft Windows Server.

Keep instance software up to date with security patches. Oracle recommends that you periodically apply the latest available software updates to your instances.

> **Caution:**
>
> Only install patches from the pca* channels. Manually updating the appliance using other channels and other methods is not supported. Security and other updates to OL7 will come through the pca* channels. For more information, see Configure Your Environment for Patching in the Oracle Private Cloud Appliance Patching Guide.

For Oracle Linux images, check the yum and dnf configuration and make sure that repositories and software streams can be reached from the VCN.

Update the compute instance. For more information on software updates for Oracle Linux 7 and Oracle Linux 8, see (Getting Started with Oracle Linux Yum Server).

If a new image needs to be created based on an updated instance, see the section "Creating an Image from an Instance" in the Compute Images chapter of the Oracle Private Cloud Appliance User Guide.

Instance Security Logging and Monitoring

Various security-related events are captured in log files on each compute instance. Oracle recommends that you periodically review these log files to detect any security issues. In Oracle Linux, the log files are located in `/var/log`. Some security-relevant log files and their locations are listed in the following table.

Log File or Directory	Description
`var/log/secure`	Authorization log showing failed and successful sign ins.
`var/log/audit`	Auditd logs capturing system calls issued, `sudo` attempts, user sign-ins, and so on. `ausearch` and `aureport` are two tools used to query auditd logs.
`var/log/yum.log`	Lists packages installed or updated on instances with yum.
`var/log/cloud-init.log`	During instance boot, cloud-init can run user-provided scripts as a privileged user. For example, `cloud-init` can introduce SSH keys. Oracle recommends that you review the `cloud-init` logs for any unrecognized commands.

Instance Security Policy Examples

In all the following examples, the policies are scoped to a tenancy. However, by specifying a compartment name, they can be scoped down to specific compartment in a tenancy.

Restrict Users Ability to Delete Instances

The following example allows the `InstanceUsers` group to launch instances, but not to delete them.

```
"Allow group InstanceUsers to manage instance-family in tenancy
 where request.permission!='INSTANCE_DELETE'"
"Allow group InstanceUsers to use volume-family in tenancy"
"Allow group InstanceUsers to use virtual-network-family in tenancy"
```

Restrict Ability to Use Instance Console

For security compliance reasons, some customers do not want to expose the instance console to users in their tenancy. The following policy example restricts ability to create or read from consoles.

```
"Allow group InstanceUsers to manage instance-console-connection in tenancy
 where all {request.permission!= INSTANCE_CONSOLE_CONNECTION_READ,
            request.permission!= INSTANCE_CONSOLE_CONNECTION_CREATE}"
```

Block Volume Security Features

There are two types of volumes: block volumes and boot volumes. Block volumes allow instance storage capacity to be expanded dynamically. A boot volume contains the image used to boot a compute instance.

The IAM service groups the family of related volume resource types into a combined resource type called `volume-family`.

In addition, block volumes:

- Are encrypted on disk (at rest) using Advanced Encryption Standard (AES) 128-bit algorithm. Encryption is on by default and cannot be turned off. The encryption keys are themselves encrypted with a master encryption key.
- Volumes can be further encrypted using tools like `dm-crypt`, `veracrypt`, and Bit-Locker.
- Users that are authenticated to the Oracle Private Cloud Appliance have the ability to manage volumes and to manage resources within the security policy framework.

Assign least privilege access for IAM users and groups to resource types in `volume-family`. The resource types in `volume-family` are `volumes`, `volume-attachments`, and `volume-backups`.

Block Volume Data Durability

Block volumes are stored in a ZFS file system with a SHA-256 checksum to avoid phantom reads and detect invalid data returned from devices.

To minimize loss of data due to inadvertent deletes by an authorized user or malicious deletes, Oracle recommends giving `VOLUME_DELETE`, `VOLUME_ATTACHMENT_DELETE` and `VOLUME_BACKUP_DELETE` permissions to a minimum possible set of IAM users and groups. `DELETE` permissions should be given only to tenancy and compartment administrators.

To minimize loss of data due to deletes or corruption, Oracle recommends that you make periodic backups of volumes. Oracle Cloud Infrastructure allows automated scheduled backups. For more information about scheduled backups, see Policy-Based Backups.

Block Volume Security Policy Examples

Prevent Delete of Volumes

The following example policy allows group `VolumeUsers` to perform all actions on volumes and backups, except deleting them:

```
"Allow group VolumeUsers to manage volumes in tenancy
 where request.permission!='VOLUME_DELETE'"
"Allow group VolumeUsers to manage volume-backups in tenancy
 where request.permission!='VOLUME_BACKUP_DELETE'"
```

If `VolumeUsers` can't detach volumes from instances, you can add the following policy to the previous example:

```
"Allow group VolumeUsers to manage volume-attachments in tenancy
 where request.permission!='VOLUME_ATTACHMENT_DELETE'"
```

Block Volume Security-Related Tasks

Encrypting Non-root Volumes with `dm-crypt`

`dm-crypt` is a kernel-level encryption mechanism (part of Linux device mapper framework) to provide encrypted volumes. It encrypts data passed from the filesystem (for example, ext4 and NTFS), and stores it on a storage device in Linux Unified Key Setup (LUKS) format. The encrypted volumes can be stored on a complete disk, disk partition, logical volume, or a file-backed storage created using loopback devices. `cryptsetup` is the user-level utility used to manage `dm-crypt`, and used to encrypt partitions and files. `dm-crypt` uses the Linux crypto APIs for encryption routines.

To encrypt the volume:

1. Attach block storage volume to an instance (for example, `/dev/sdb`).
2. Format `/dev/sdb` for LUKS encryption. Enter LUKS passphrase when prompted. The passphrase is used to encrypt the LUKS master key used for encrypting the volume.

   ```
   cryptsetup -y luksFormat /dev/sdb
   ```
3. Verify that the LUKS formatting is successful.

   ```
   cryptsetup isLuks /dev/sdb && echo Success
   ```
4. Get encryption information about the device.

   ```
   cryptsetup luksDump /dev/sdb
   ```
5. Get LUKS UUID of the device. The UUID value is used to configure the `/etc/crypttab`.

   ```
   cryptsetup luksUUID /dev/sdb
   ```
6. Create a LUKS container with device name, `dev_name`. This also creates a device node, `/dev/mapper/<dev_name>`.

   ```
   cryptsetup luksOpen /dev/sdb <dev_name>
   ```
7. Get information about the mapped device.

```
dmsetup info <dev_name>
```

8. Format the device node as ext4 filesystem.

```
sudo mkfs -t ext4 /dev/sdb
```

9. Mount the device node.

```
mount /dev/mapper/<dev_name> /home/encrypt_fs
```

10. Add an entry to `/etc/crypttab`.

```
<dev_name> UUID=<LUKS UUID of /dev/sdb> none
```

All the files copied to `/home/encrypt_fs` are encrypted by LUKS.

11. Add a keyfile to an available keyslot of the encrypted volume. This keyfile can be used to access the encrypted volume.

```
dd if=/dev/urandom of=$HOME/keyfile bs=32 count=1
chmod 600 $HOME/keyfile
cryptsetup luksAddKey /dev/sdb ~/keyfile
```

12. Verify the encryption status of files.

```
cryptsetup status /home/encrypt_fs
```

13. Unmount after you're finished.

```
umount /home/encrypt_fs
cryptsetup luksClose <dev_name>
```

To access the encrypted volume:

```
cryptsetup luksOpen /dev/sdb <dev_name> --key-file=/home/opc/keyfile
mount /dev/mapper/<dev_name> /home/encrypt_fs
```

If you lose the keyfile, or if the keyfile or passphrase gets corrupted, you can't decrypt the encrypted volume.

> **Important:**
>
> If you lose or corrupt the keyfile, this results in a permanent loss of data.

Oracle recommends that you store durable copies of the keyfile on an on-premises host.

Remote Mounting of `dm-crypt` Encrypted Data Volumes

The following steps assume that the keyfile is on an on-premises host (`SRC_IP`) and that `<OCI_SSH_KEY>` is the SSH private key of the instance.

1. Copy keyfile from the on-premises host to an instance.

```
scp -i <OCI_SSH_KEY> keyfile opc@SRC_IP:/home/opc
```

2. Open the encrypted volume.

```
ssh i <OCI_SSH_KEY> opc@SRC_IP "cryptsetup luksOpen /dev/sdb <dev_name>
      --key-file=/home/opc/keyfile"
```

3. Mount the volume.

```
ssh -i <OCI_SSH_KEY> opc@SRC_IP "mount /dev/mapper/<dev_name> /home/encrypt_fs"
```

4. Perform operations on data in the mounted volume.
5. Unmount the encrypted volume.

```
ssh -i <OCI_SSH_KEY> opc@SRC_IP "umount /home/encrypt_fs"
ssh -i <OCI_SSH_KEY> opc@SRC_IP "cryptsetup luksClose <dev_name>"
```

6. Delete the keyfile from the instance.

```
ssh -i <OCI_SSH_KEY> opc@SRC_IP "\rm -f /home/opc/keyfile"
```

4

Secure Deployments Checklist

This section provides a checklist of steps used to install and configure the Oracle Private Cloud Appliance product in a secure manner for operational deployment. This checklist section contains items relating to all three layers of the Oracle Private Cloud Appliance.

The three layers of the Oracle Private Cloud Appliance are:

- Infrastructure - This is the physical rack hardware installed on the customers premises. Some security-related tasks are performed at this basic level when the system is installed.
- Service Enclave - This is the part of the system where the appliance infrastructure is controlled. Access to this enclave is closely monitored and restricted to privileged administrators. The Service Enclave runs on a cluster of three management nodes. Many security-related tasks are performed at this level.
- Compute Enclave - The Compute Enclave is designed for compatibility with Oracle Cloud Infrastructure. The Compute Enclave is where resources such as compute instances, networks, and storage are controlled.

Pre-installation General Considerations

Before product installation, it is important that each of the following items are considered:

- Networking: Virtual and physical interfaces, bridged and routed
- User roles: Operator and administrator and others, view or modify or delete
- Password rules: length and character requirements, other characteristics
- Cryptographic algorithms: allowed or mandated, usage guidelines
- Patch or update process security: limitations, roles allowed to execute procedures

This is not an exhaustive list. The more things that can be planned ahead of time, the better.

Post-installation General Considerations

After installation, make sure that you:

- Keep software up-to-date. This includes the latest product release and any patches that apply to it.
- Limit privileges wherever possible. Give users only the access necessary to perform their work. Review user privileges periodically to determine relevance to current work requirements.
- Monitor system activity. Establish who has access to which system components, and how often, and monitor those components.
- Learn about and use Oracle security features.
- Use best practices for security.

Auditing Goals

Auditing should make it easy to detemrine:

- Who made the change? (More than information that "root" made the alteration.)
- When was the change made? (An adequate log retention period is important.)
- What was the purpose of the change? (If not malicious, the change was made for a reason.)

Installation Security Checklist

Before product installation, create a document to outline the services provided by the product. Have it reviewed and updated to address any shortcomings.

For pre-installation site preparation, see the Oracle Private Cloud Appliance Installation Guide.

For more information on pre-installation security, see Pre-Installation Security Details

Post-Installation Configuration Security Checklists

After installation of Oracle Private Cloud Appliance, secure the hardware by restricting access to the hardware and recording the serial numbers.

Hardware Security Checklist

In order to restrict access to the system hardware, Oracle recommends the following practices:

- Install Oracle Private Cloud Appliance and related equipment in a locked, restricted-access room.
- Lock the rack door unless service is required on components within the rack.
- Restrict access to hot-pluggable or hot-swappable devices because the components are designed to be easily removed.
- Store spare field-replaceable units (FRUs) or customer-replaceable units (CRUs) in a locked cabinet. Restrict access to the locked cabinet to authorized personnel.
- Limit SSH listener ports to the management and private networks. Use SSH protocol 2 (SSH-2) and FIPS 140-2 approved ciphers.
- Limit SSH allowed authentication mechanisms. Inherently insecure methods are disabled.
- Label all significant items of computer hardware, such as FRUs.
- Keep hardware activation keys and licenses in a secure location that is easily accessible to the system managers in the case of a system emergency.

Hardware Serial Number Checklist

You should record all serial numbers and keep them in a secure location. There are several techniques to obtaining the overall appliance serial number:

- Use the Service Enclave console (Administrative Console)
- Use the appropriate monitoring dashboard (Grafana)
- Use the Admin Command Line Interface (CLI)

For information on how to get rack component serial numbers, see Retrieving the Serial Numbers for Hardware Components in the Rack

Software Security Checklist

In order to secure the software, after initial installation of Oracle Private Cloud Appliance, Oracle recommends the following practices to restrict system access:

- Limit use of the `root` super-user account. Create and use individual user accounts because they ensure positive identification in audit trails, and require less maintenance when administrators leave the team or company.
- Do not create new users on the management nodes.
- Disable unnecessary protocols and modules for layers under customer control.
- Restrict physical access to USB ports, network ports, and system consoles because physical severs and network switches have ports and console connections providing direct access to the system.
- Restrict the capability to restart the system over the network.
- For more information on how to enable other security features, see Security Features for Oracle Private Cloud Appliance in this guide.

Network Security Checklist

There are other steps that can be taken to control cloud network security and access to compute instances:

- Use private subnets if instances do not require a public IP address.
- Configure firewall rules on the instance to control traffic into and out of an instance at the packet level. However, Oracle-provided images that run Oracle Linux automatically include default rules that allow ingress on TCP port 22 for SSH traffic. In addition, the Microsoft Windows images include default rules that allow ingress on TCP port 3389 for Remote Desktop access.
- Configure gateways and route tables to allow only required connectivity. This can control traffic flow to "outside" destinations such as your on-premises network or another VCN.
- Use IAM policies to control access to Oracle Private Cloud Appliance interfaces. You can control which cloud resources can be accessed and which type of access is allowed. For example, you can control who can set up your network and subnets, or who can update route tables, network security groups, or security lists.

For more information on Oracle Private Cloud Appliance network security, see the Oracle Private Cloud Appliance User Guide and Oracle Private Cloud Appliance Administrator Guide .

Account and Password Security Checklists

When the Oracle Private Cloud Appliance system is first powered on, various tasks need to be performed in order to initially set up the system. The accounts and passwords established must be watched to make sure that no unexpected changes oocur.

Infrastructure Account and Password Security Checklist

Change any default passwords immediately after successful rack installation and configuration.

Passwords to be updated include:

- Compute node passwords
- Compute node Oracle Integrated Lights Out Manager (ILOM) passwords
- Management node passwords
- Management node ILOM passwords
- Leaf switch password
- Management switch password
- Spine switch password
- Oracle ZFS Storage Appliance password
- Oracle ZFS Storage ApplianceILOM password

There is a tool available on the management nodes to check for default passwords in the infrastructure that must be changed. To run it:

1. Log into a management node using the default administrative user and password supplied to you by the installation team.
2. Run the following command: `/var/lib/pca-foundation/scripts/healthcheck.py`.

The output of the tool will show passwords to change from factory defaults.

Service Enclave Account and Password Security Checklist

At installation and configuration time, an initial user with the SuperAdmin Authorization Group and password is set up for the Service Enclave, refer to the Oracle Private Cloud Appliance Installation Guide.

The Service Enclave is a multi-user environment where users do not share credentials. Because actions in the Service Enclave affect all tenancies on the appliance, very few users are necessary in this space. General security guidelines are:

- Do not share credentials.
- Create a user for each individual that requires access to the Service Enclave administration tools. This practice enables better audit tracking and easier administration of individual needs.

- Apply the rule of least privileges by choosing the authorization group most appropriate for the individual.
- When creating a new user, do not use a common password and do not use a default initial password for new users.
- Change passwords regularly. There are no proactive password change or timeout notifications in the Service Enclave.

There are 3 authorization groups in the Service Enclave:

- Admin - Authorization for most operations except user management.
- Monitor - A read-only role that can only manage their own profile or browse Service Enclave information without changing it.
- SuperAdmin - Authorization for all capabilities, only a SuperAdmin can create new users for the Service Enclave and change roles for existing users.

In the Service Enclave, the list of authorization groups is static. Existing groups cannot be modified to change authorizations and new groups cannot be created with different authorizations.

Service Customer Account and Password Security Checklist

There are no default Customer Enclave users or tenancies immediately following a Oracle Private Cloud Appliance Installation Guide install and configuration.

When a Service Enclave administrator creates a tenancy, an initial user is created and a password is assigned.

Have the new tenancy administrator log into the account and change their password using the Compute Enclave console (`https://adminconsole.<domain>`).

Once logged in, use the Change Password drop down located in the top right of the console where the user name is displayed. The tenancy administrator is the only user account that cannot be reset by any user (including themselves). The only option available to the primary tenancy administrator created by the Service Enclave SuperAdmin is to store their password securely and use the Change Password action in the user interface after a successful login.

The password policy for the Compute Enclave is as follows:

- Password has a minimum length of 12 characters
- Password contains at least one uppercase letter
- Password contains at least one lowercase letter
- Password contains at least one symbol (@$!#%*?&)
- Password contains at least one number

The password policy cannot be changed.

Monitoring and Logging Account and Password Security Checklist

The monitoring and logging facilities for Oracle Private Cloud Appliance are accessed via consoles at:

- Grafana: https://grafana.***<domain>***
- Prometheus: https://prometheus.***<domain>***

In Oracle Private Cloud Appliance, this tier has a single user for both platforms (`admin`) and is delivered with a default password. Change this password after installation and configuration. To change the password, log into one of the management nodes in the infrastructure layer using `root` and the password that was updated in Password Maintenance in the Infrastructure Layer.

Once logged in, update the password using the Python 3 runtime and this program:

```
python3 /lib/python3.6/site-packages/pca_foundation/
secret_service/scripts/sauron_credential_update.py -username
<username> -password <password>
```

The password policy requires that the password:

- Must be 12-20 characters long
- Must contain at least 1 uppercase, 1 lowercase and one digit
- Can contain the symbols -_+=

The monitoring and logging tools in Oracle Private Cloud Appliance have the following restrictions

- More users cannot be added
- The credential update tool does not check the password or return information on success or failure of the request
- The Grafana and Prometheus screens do not lock out users after invalid attempts