Oracle Private Cloud Appliance

Administration Guide for Release 2.4.4

F37607-09
December 2022

Oracle Private Cloud Appliance Administration Guide for Release 2.4.4,

F37607-09

Contents

4 Oracle Private Cloud Appliance Command Line Interface (CLI)

5 Managing the Oracle VM Virtual Infrastructure

6 Servicing Oracle Private Cloud Appliance Components

7 Troubleshooting

Preface

This document is part of the documentation set for Oracle Private Cloud Appliance (PCA) Release 2.4. All Oracle Private Cloud Appliance product documentation is available at:

https://docs.oracle.com/en/engineered-systems/private-cloud-appliance/index.html.

The documentation set consists of the following items:

Oracle Private Cloud Appliance Release Notes
The release notes provide a summary of the new features, changes, fixed bugs and known issues in Oracle Private Cloud Appliance.

Oracle Private Cloud Appliance Licensing Information User Manual
The licensing information user manual provides information about the various product licenses applicable to the use of Oracle Private Cloud Appliance.

Oracle Private Cloud Appliance Installation Guide
The installation guide provides detailed instructions to prepare the installation site and install Oracle Private Cloud Appliance. It also includes the procedures to install additional compute nodes, and to connect and configure external storage components.

Oracle Private Cloud Appliance Safety and Compliance Guide
The safety and compliance guide is a supplemental guide to the safety aspects of Oracle Private Cloud Appliance.

Oracle Private Cloud Appliance Administrator's Guide
The administrator's guide provides instructions for using the management software. It is a comprehensive guide to how to configure, monitor and administer Oracle Private Cloud Appliance.

Oracle Private Cloud Appliance Quick Start Poster
The quick start poster provides a step-by-step description of the hardware installation and initial software configuration of Oracle Private Cloud Appliance. A printed quick start poster is shipped with each Oracle Private Cloud Appliance base rack, and is intended for data center operators and administrators who are new to the product.
The quick start poster is also available in the documentation set as an HTML guide, which contains alternate text for ADA 508 compliance.

Oracle Private Cloud Appliance Expansion Node Setup Poster
The expansion node setup poster provides a step-by-step description of the installation procedure for an Oracle Private Cloud Appliance expansion node. A printed expansion node setup poster is shipped with each Oracle Private Cloud Appliance expansion node.
The expansion node setup poster is also available in the documentation set as an HTML guide, which contains alternate text for ADA 508 compliance.

Audience

The Oracle Private Cloud Appliance documentation is written for technicians, authorized service providers, data center operators and system administrators who want to install, configure and maintain a private cloud environment in order to deploy virtual machines for users. It is assumed that readers have experience installing and troubleshooting hardware, are familiar with web and virtualization technologies and have a general understanding of operating systems such as UNIX (including Linux) and Windows.

The Oracle Private Cloud Appliance makes use of Oracle Linux and Oracle Solaris operating systems within its component configuration. It is advisable that administrators have experience of these operating systems at the very least. Oracle Private Cloud Appliance is capable of running virtual machines with a variety of operating systems including Oracle Solaris and other UNIX systems, Linux, and Microsoft Windows. The selection of operating systems deployed in guests on Oracle Private Cloud Appliance determines the requirements of your administrative knowledge.

Related Documentation

Additional Oracle components may be included with Oracle Private Cloud Appliance depending on configuration. The documentation for such additional components is available as follows:

> **Note:**
>
> If your appliance contains components that are not mentioned below, please consult the related documentation list for Oracle Private Cloud Appliance Release 2.3.

- Oracle Rack Cabinet 1242

  https://docs.oracle.com/en/servers/options/rack-cabinet-1242/index.html
- Oracle Server X86 Servers

  https://docs.oracle.com/en/servers/index.html
- Oracle ZFS Storage Appliance ZS7-2

  https://docs.oracle.com/en/storage/zfs-storage/zfs-appliance/os8-8-x/
- Oracle Integrated Lights Out Manager (ILOM) 4.0.x

  https://docs.oracle.com/cd/E81115_01/index.html
- Oracle Integrated Lights Out Manager (ILOM) 5.0

  https://docs.oracle.com/en/servers/management/ilom/index.html
- Oracle VM

  https://docs.oracle.com/en/virtualization/oracle-vm/index.html
- Oracle Enterprise Manager Plug-in

https://docs.oracle.com/en/enterprise-manager/cloud-control/enterprise-manager-cloud-control/13.5/index.html

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, URLs, code in examples, text that appears on the screen, or text that you enter.

Documentation Accessibility

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

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

Concept, Architecture and Life Cycle of Oracle Private Cloud Appliance

This chapter describes what Oracle Private Cloud Appliance is, which hardware and software it consists of, and how it is deployed as a virtualization platform.

What is Oracle Private Cloud Appliance

Responding to the Cloud Challenges

Cloud architectures and virtualization solutions have become highly sophisticated and complex to implement. They require a skill set that no single administrator has had to acquire in traditional data centers: system hardware, operating systems, network administration, storage management, applications. Without expertise in every single one of those domains, an administrator cannot take full advantage of the features and benefits of virtualization technology. This often leads to poor implementations with sub-optimal performance and reliability, which impairs the flexibility of a business.

Aside from the risks created by technical complexity and lack of expertise, companies also suffer from an inability to deploy new infrastructure quickly enough to suit their business needs. The administration involved in the deployment of new systems, and the time and effort to configure these systems, can amount to weeks. Provisioning new applications into flexible virtualized environments, in a fraction of the time required for physical deployments, generates substantial financial benefits.

Fast Deployment of Converged Infrastructure

Private Cloud Appliance is an offering that industry analysts refer to as a *Converged Infrastructure Appliance*: an infrastructure solution in the form of a hardware appliance that comes from the factory pre-configured. It enables the operation of the entire system as a single unit, not a series of individual servers, network hardware and storage providers. Installation, configuration, high availability, expansion and upgrading are automated and orchestrated to an optimal degree. Within a few hours after power-on, the appliance is ready to create virtual servers. Virtual servers are commonly deployed from virtual appliances, in the form of Oracle VM templates (individual pre-configured VMs) and assemblies (interconnected groups of pre-configured VMs).

Modular Implementation of a Complete Stack

With Private Cloud Appliance, Oracle offers a unique full stack of hardware, software, virtualization technology and rapid application deployment through virtual appliances. All this is packaged in a single modular and extensible product. The minimum configuration consists of a base rack with infrastructure components, a pair of management nodes, and two compute nodes. This configuration can be extended by one compute node at a time. All rack units, whether populated or not, are pre-cabled and pre-configured at the factory in order to facilitate the installation of expansion compute nodes on-site at a later time.

Ease of Use

The primary value proposition of Private Cloud Appliance is the integration of components and resources for the purpose of ease of use and rapid deployment. It should be considered a general purpose solution in the sense that it supports the widest variety of operating systems, including Windows, and any application they might host. Customers can attach their existing storage or connect new storage solutions from Oracle or third parties.

Hardware Components

The current Private Cloud Appliance hardware platform, with factory-installed Controller Software Release 2.4.x, consists of an Oracle Rack Cabinet 1242 base, populated with the hardware components identified in the following figure.

Figure 1-1 Components of an Oracle Private Cloud Appliance Rack

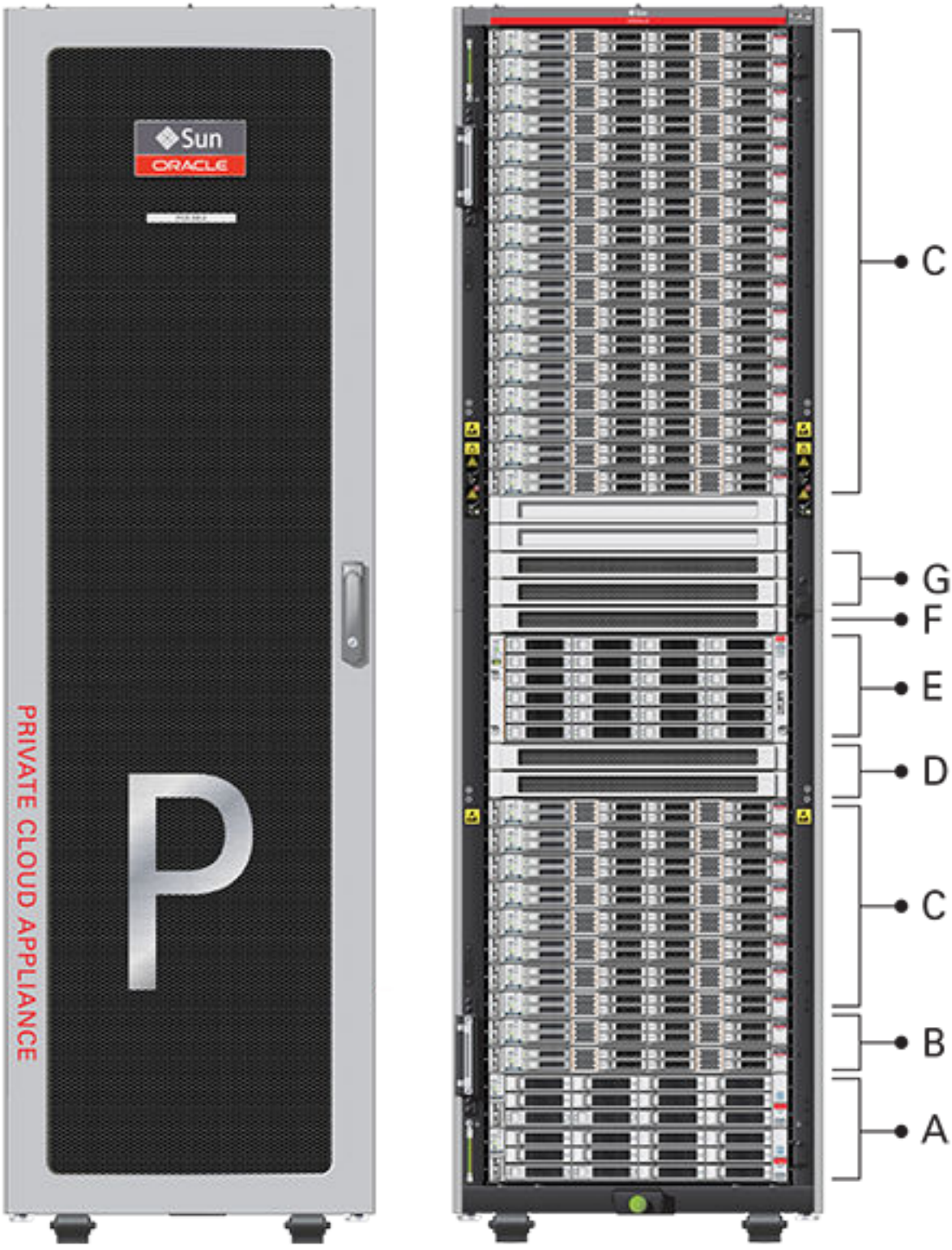


Table 1-1 Figure Legend

Item	Quantity	Description
A	2	Oracle ZFS Storage Appliance ZS7-2 controller server
B	2	Oracle Server X8-2, used as management nodes
C	2-22	Oracle Server X9-2, used as virtualization compute nodes Due to the power requirements of the Oracle Server X9-2, if the appliance is equipped with 22kVA PDUs, the maximum number of compute nodes is 22. With 15KVA PDUs the maximum is 13 compute nodes.
D	2	Cisco Nexus 9336C-FX2 Switch, used as leaf/data switches
E	1	Oracle ZFS Storage Appliance ZS7-2 disk shelf
F	1	Cisco Nexus 9348GC-FXP Switch
G	2	Cisco Nexus 9336C-FX2 Switch, used as spine switches

Support for Previous Generations of Hardware Components

The latest version of the Oracle Private Cloud Appliance Controller Software supports only the hardware configurations listed above.

Management Nodes

At the heart of each Oracle Private Cloud Appliance installation is a pair of management nodes. They are installed in rack units 5 and 6 and form a cluster in active/standby configuration for high availability: both servers are capable of running the same services and have equal access to the system configuration, but one operates as the active while the other is ready to take over the active functions in case a failure occurs. The active management node runs the full set of services required, while the standby management node runs a subset of services until it is promoted to the active role. The active role is determined at boot through OCFS2 Distributed Lock Management on an iSCSI LUN, which both management nodes share on the ZFS Storage Appliance installed inside the rack. Because rack units are numbered from the bottom up, and the bottom four are occupied by components of the ZFS Storage Appliance, the active management node is typically the server in rack unit 5. It is the only server that must be powered on by the administrator in the entire process to bring the appliance online.

For details about how high availability is achieved with Private Cloud Appliance, refer to High Availability.

When you power on the Private Cloud Appliance for the first time, you can change the factory default IP configuration of the management node cluster, so that it can be easily reached from your data center network. The management nodes share a virtual IP, where the management web interface can be accessed. This virtual IP is assigned to whichever server has the *active* role at any given time. During system initialization, after the management cluster is set up successfully, the active management node loads a number of Oracle Linux services, in addition to Oracle VM and its associated MySQL database – including network, sshd, ntpd, iscsi initiator, dhcpd – to orchestrate the provisioning of all system components. During provisioning, all networking and storage is configured, and all compute nodes are discovered, installed and added to

an Oracle VM server pool. All provisioning configurations are preloaded at the factory and should not be modified by the customer.

For details about the provisioning process, refer to Provisioning and Orchestration.

Compute Nodes

The compute nodes in the Oracle Private Cloud Appliance constitute the virtualization platform. The compute nodes provide the processing power and memory capacity for the virtual servers they host. The entire provisioning process is orchestrated by the management nodes: compute nodes are installed with Oracle VM Server 3.4.x and additional packages for Software Defined Networking. When provisioning is complete, the Oracle Private Cloud Appliance Controller Software expects all compute nodes in the same rack to be part of the same Oracle VM server pool. For hardware configuration details of the compute nodes, see "Server Components" in Introduction to Oracle Private Cloud Appliance Installation in the *Oracle Private Cloud Appliance Installation Guide*.

The Oracle Private Cloud Appliance Dashboard allows the administrator to monitor the health and status of the compute nodes, as well as all other rack components, and perform certain system operations. The virtual infrastructure is configured and managed with Oracle VM Manager.

The Private Cloud Appliance offers modular compute capacity that can be increased according to business needs. The minimum configuration of the base rack contains just two compute nodes, but it can be expanded by one node at a time up to 22 compute nodes. For information about compute node configuration maximums and supported rack locations, see Compute Node Rack Location Reference in the *Oracle Private Cloud Appliance Installation Guide*.

Apart from the hardware installation, adding compute nodes requires no intervention by the administrator. New nodes are discovered, powered on, installed and provisioned automatically by the active management node. The additional compute nodes are integrated into the existing configuration and, as a result, the Oracle VM server pool offers increased capacity for more or larger virtual machines.

As a further expansion option, the compute nodes can be ordered with pre-installed fibre channel cards, or equipped with fibre channel cards after installation. Once these compute nodes are integrated in the Private Cloud Appliance environment, the fibre channel HBAs can connect to standard FC switches and storage hardware in your data center. External FC storage configuration is managed through Oracle VM Manager. For more information, refer to the Fibre Channel Storage Attached Network section of the *Oracle VM Concepts Guide*.

Because of the diversity of possible virtualization scenarios, it is difficult to quantify the compute capacity as a number of virtual machines. For sizing guidelines, refer to the chapter entitled Configuration Maximums in the *Oracle Private Cloud Appliance Release Notes*.

Storage Appliance

The Oracle Private Cloud Appliance Controller Software provides support for the Oracle ZFS Storage Appliance ZS7-2.

Oracle ZFS Storage Appliance ZS7-2

The Oracle ZFS Storage Appliance ZS7-2, which consists of two controller servers installed at the bottom of the appliance rack and disk shelf about halfway up, fulfills the role of 'system

disk' for the entire appliance. It is crucial in providing storage space for the Oracle Private Cloud Appliance software.

A portion of the disk space, 3TB by default, is made available for customer use and is sufficient for an Oracle VM storage repository with several virtual machines, templates and assemblies. The remaining part of approximately 100TB in total disk space can also be configured as a storage repository for virtual machine resources. Further capacity extension with external storage is also possible.

The hardware configuration of the Oracle ZFS Storage Appliance ZS7-2 is as follows:

- Two clustered storage heads with two 14TB hard disks each
- One fully populated disk chassis with twenty 14TB hard disks
- Four cache disks installed in the disk shelf: 2x 200GB SSD and 2x 7.68TB SSD
- RAID-1 configuration, for optimum data protection, with a total usable space of approximately 100TB

The storage appliance is connected to the management subnet (`192.168.4.0/24`) and the storage subnet (`192.168.40.0/24`). Both heads form a cluster in active-passive configuration to guarantee continuation of service in the event that one storage head should fail. The storage heads share a single IP in the storage subnet, but both have an individual management IP address for convenient maintenance access. The RAID-1 storage pool contains two projects, named `OVCA` and `OVM`.

The `OVCA` project contains all LUNs and file systems used by the Private Cloud Appliance software:

- LUNs
  - `Locks` (12GB) – to be used exclusively for cluster locking on the two management nodes
  - `Manager` (200GB) – to be used exclusively as an additional file system on both management nodes
- File systems:
  - `MGMT_ROOT` – to be used for storage of all files specific to the Private Cloud Appliance
  - `Database` – placeholder file system for databases
  - `Incoming` (20GB) – to be used for FTP file transfers, primarily for Private Cloud Appliance component backups
  - `Templates` – placeholder file system for future use
  - `User` – placeholder file system for future use
  - `Yum` – to be used for system package updates

The `OVM` project contains all LUNs and file systems used by Oracle VM:

- LUNs
  - `iscsi_repository1` (3TB) – to be used as Oracle VM storage repository
  - `iscsi_serverpool1` (12GB) – to be used as server pool file system for the Oracle VM clustered server pool
- File systems:

- `nfs_repository1` (3TB) – used by `kdump`; not available for customer use
- `nfs_serverpool1` (12GB) – to be used as server pool file system for the Oracle VM clustered server pool in case NFS is preferred over iSCSI

> **Caution:**
>
> If the internal ZFS Storage Appliance contains customer-created LUNs, make sure they are not mapped to the default initiator group. See "Customer Created LUNs Are Mapped to the Wrong Initiator Group" in Known Limitations and Workarounds in the *Oracle Private Cloud Appliance Release Notes*.

In addition to offering storage, the ZFS storage appliance also runs the xinetd and tftpd services. These complement the Oracle Linux services on the active management node in order to orchestrate the provisioning of all Private Cloud Appliance system components.

Along with the Oracle Private Cloud Appliance Backup capabilities, you can also use the native ZFS features to backup the internal ZFS storage appliance. Oracle ZFS Storage Appliance supports snapshot-based replication of projects and shares from a source appliance to a replication target, to a different pool on the same appliance, or to an NFS server for offline replication. You can configure replication to be executed manually, on a schedule, or continuously. For more information see Remote Replication in the *Oracle ZFS Storage Appliance Administration Guide, Release OS8.8.x*.

> **Note:**
>
> Do not configure the internal ZFS appliance as a storage device for external hosts.

Network Infrastructure

For network connectivity, Private Cloud Appliance relies on a physical layer that provides the necessary high-availability, bandwidth and speed. On top of this, several different virtual networks are optimally configured for different types of data traffic. Only the internal administration network is truly physical; the appliance data connectivity uses Software Defined Networking (SDN). The appliance rack contains redundant network hardware components, which are pre-cabled at the factory to help ensure continuity of service in case a failure should occur.

Network Architecture

Oracle Private Cloud Appliance with Ethernet-based network architecture relies on redundant physical high-speed Ethernet connectivity.

Administration Network

The administration network provides internal access to the management interfaces of all appliance components. These have Ethernet connections to the Cisco Nexus 9348GC-FXP Switch, and all have a predefined IP address in the `192.168.4.0/24` range. In addition, all management and compute nodes have a second IP address in this range, which is used for Oracle Integrated Lights Out Manager (ILOM) connectivity.

While the appliance is initializing, the data network is not accessible, which means that the internal administration network is temporarily the only way to connect to the system. Therefore, the administrator should connect a workstation to the reserved Ethernet port 48 in the Cisco Nexus 9348GC-FXP Switch, and assign the fixed IP address `192.168.4.254` to the workstation. From this workstation, the administrator opens a browser connection to the web server on the active management node at `https://192.168.4.216` , in order to monitor the initialization process and perform the initial configuration steps when the appliance is powered on for the first time.

Data Network

The appliance data connectivity is built on redundant Cisco Nexus 9336C-FX2 Switches in a leaf-spine design. In this two-layer design, the leaf switches interconnect the rack hardware components, while the spine switches form the backbone of the network and perform routing tasks. Each leaf switch is connected to all the spine switches, which are also interconnected. The main benefits of this network architecture are extensibility and path optimization. A Private Cloud Appliance rack contains two leaf and two spine switches.

The Cisco Nexus 9336C-FX2 Switch offers a maximum throughput of 100Gbit per port. The spine switches use 5 interlinks (500Gbit); the leaf switches use 2 interlinks (200Gbit) and 2x2 crosslinks to the spines. Each compute node is connected to both leaf switches in the rack, through the `bond1` interface that consists of two 100Gbit Ethernet ports in link aggregation mode. The two storage controllers are connected to the spine switches using 4x40Gbit connections.

For external connectivity, 5 ports are reserved on each spine switch. Four ports are available for custom network configurations; one port is required for the default uplink. This **default external uplink** requires that port 5 on both spine switches is split using a QSFP+-to-SFP+ four way splitter or breakout cable. Two of those four 10GbE SFP+ breakout ports per spine switch, ports 5/1 and 5/2, must be connected to a pair of next-level data center switches, also called top-of-rack or ToR switches.

Software Defined Networking

While the physical data network described above allows the data packets to be transferred, the true connectivity is implemented through Software Defined Networking (SDN). Using VxLAN encapsulation and VLAN tagging, thousands of virtual networks can be deployed, providing segregated data exchange. Traffic can be internal between resources within the appliance environment, or external to network storage, applications, or other resources in the data center or on the internet. SDN maintains the traffic separation of hard-wired connections, and adds better performance and dynamic (re-)allocation. From the perspective of the customer network, the use of VxLANs in Private Cloud Appliance is transparent: encapsulation and de-encapsulation take place internally, without modifying inbound or outbound data packets. In other words, this design extends customer networking, tagged or untagged, into the virtualized environment hosted by the appliance.

During the initialization process of the Private Cloud Appliance, several essential default networks are configured:

- The **Internal Storage Network** is a redundant 40Gbit Ethernet connection from the spine switches to the ZFS storage appliance. All four storage controller interfaces are bonded using LACP into one datalink. Management and compute nodes can reach the internal storage over the `192.168.40.0/21` subnet on VLAN 3093. This network also fulfills the heartbeat function for the clustered Oracle VM server pool.

- The **Internal Management Network** provides connectivity between the management nodes and compute nodes in the subnet `192.168.32.0/21` on VLAN 3092. It is used for all network traffic inherent to Oracle VM Manager, Oracle VM Server and the Oracle VM Agents.
- The **Internal Underlay Network** provides the infrastructure layer for data traffic between compute nodes. It uses the subnet `192.168.64.0/21` on VLAN 3091. On top of the internal underlay network, internal VxLAN overlay networks are built to enable virtual machine connectivity where only internal access is required.

  One such internal VxLAN is configured in advance: the *default internal VM network*, to which all compute nodes are connected with their `vx2` interface. Untagged traffic is supported by default over this network. Customers can add VLANs of their choice to the Oracle VM network configuration, and define the subnet(s) appropriate for IP address assignment at the virtual machine level.
- The **External Underlay Network** provides the infrastructure layer for data traffic between Private Cloud Appliance and the data center network. It uses the subnet `192.168.72.0/21` on VLAN 3090. On top of the external underlay network, VxLAN overlay networks with external access are built to enable public connectivity for the physical nodes and all the virtual machines they host.

  One such public VxLAN is configured in advance: the *default external network*, to which all compute nodes and management nodes are connected with their `vx13040` interface. Both tagged and untagged traffic are supported by default over this network. Customers can add VLANs of their choice to the Oracle VM network configuration, and define the subnet(s) appropriate for IP address assignment at the virtual machine level.

  The default external network also provides access to the management nodes from the data center network and allows the management nodes to run a number of system services. The management node external network settings are configurable through the Network Settings tab in the Oracle Private Cloud Appliance Dashboard. If this network is a VLAN, its ID or tag must be configured in the Network Setup tab of the Dashboard.

For the appliance default networking to be configured successfully, the default external uplink must be in place before the initialization of the appliance begins. At the end of the initialization process, the administrator assigns three reserved IP addresses from the data center (public) network range to the management node cluster of the Private Cloud Appliance: one for each management node, and an additional Virtual IP shared by the clustered nodes. From this point forward, the Virtual IP is used to connect to the active management node's web server, which hosts both the Oracle Private Cloud Appliance Dashboard and the Oracle VM Manager web interface.

Caution:

It is critical that **both** spine Cisco Nexus 9336C-FX2 Switches have **two** 10GbE connections each to a pair of next-level data center switches. For this purpose, a 4-way breakout cable must be attached to port 5 of each spine switch, and 10GbE breakout ports 5/1 and 5/2 must be used as uplinks. Note that ports 5/3 and 5/4 remain unused.

This outbound cabling between the spine switches and the data center network should be crossed or meshed, to ensure optimal continuity of service.

Software Components

This section describes the main software components the Oracle Private Cloud Appliance uses for operation and configuration.

Oracle Private Cloud Appliance Dashboard

The Private Cloud Appliance provides its own web-based graphical user interface that can be used to perform a variety of administrative tasks specific to the appliance. The Oracle Private Cloud Appliance Dashboard is an Oracle JET application that is available through the active management node.

Use the Dashboard to perform the following tasks:

- Appliance system monitoring and component identification
- Initial configuration of management node networking data
- Resetting of the global password for Private Cloud Appliance configuration components

The Oracle Private Cloud Appliance Dashboard is described in detail in Monitoring and Managing Oracle Private Cloud Appliance.

Password Manager (Wallet)

All components of the Oracle Private Cloud Appliance have administrator accounts with a default password. After applying your data center network settings through the Oracle Private Cloud Appliance Dashboard, it is recommended that you modify the default appliance password. The Authentication tab allows you to set a new password, which is applied to the main system configuration components. You can set a new password for all listed components at once or for a selection only. Best practices suggest that if you want to change all passwords, do so in two phases. First change all hardware component passwords, wait at least 10 minutes for those changes to take effect, then change the `ovm-admin`, `mysql`, and `wls-weblogic` passwords.

Passwords for all accounts on all components are stored in a global Wallet, secured with 512-bit encryption. To update the password entries, you use either the Oracle Private Cloud Appliance Dashboard or the Command Line Interface. For details, see Authentication.

Oracle VM Manager

All virtual machine management tasks are performed within Oracle VM Manager, a WebLogic application that is installed on each of the management nodes and which provides a web-based management user interface and a command line interface that allows you to manage your Oracle VM infrastructure within the Private Cloud Appliance.

Oracle VM Manager is comprised of the following software components:

- **Oracle VM Manager application**: provided as an Oracle WebLogic Server domain and container.
- **Oracle WebLogic Server 12*c***: including Application Development Framework (ADF) Release 12*c*, used to host and run the Oracle VM Manager application.

- **MySQL 8.0 Enterprise Edition Server**: for the exclusive use of the Oracle VM Manager application as a management repository and installed on the Database file system hosted on the ZFS Storage Appliance.

Administration of virtual machines is performed using the Oracle VM Manager web user interface, as described in Managing the Oracle VM Virtual Infrastructure. While it is possible to use the command line interface provided with Oracle VM Manager, this is considered an advanced activity that should only be performed with a thorough understanding of the limitations of Oracle VM Manager running in the context of a Private Cloud Appliance.

Operating Systems

Hardware components of the Oracle Private Cloud Appliance run their own operating systems:

- Management Nodes: Oracle Linux 7 with UEK R5
- Compute Nodes: Oracle VM Server 3.4.7
- Oracle ZFS Storage Appliance: Oracle Solaris 11

All other components run a particular revision of their respective firmware. All operating software has been selected and developed to work together as part of the Private Cloud Appliance. When an update is released, the appropriate versions of all software components are bundled. When a new software release is activated, all component operating software is updated accordingly. You should not attempt to update individual components unless Oracle explicitly instructs you to.

Databases

The Oracle Private Cloud Appliance uses a number of databases to track system states, handle configuration and provisioning, and for Oracle VM Manager. All databases are stored on the ZFS Storage Appliance, and are exported via an NFS file system. The databases are accessible to each management node to ensure high availability.

> **Caution:**
>
> Databases must never be edited manually. The appliance configuration depends on them, so manipulations are likely to break functionality.

The following table lists the different databases used by the Private Cloud Appliance.

Table 1-2 Oracle Private Cloud Appliance Databases

Item	Description
Oracle Private Cloud Appliance Node Database	Contains information on every compute node and management node in the rack, including the state used to drive the provisioning of compute nodes and data required to handle software updates. **Type:** BerkeleyDB **Location:**`MGMT_ROOT/db/node` on the ZFS, accessible via `/nfs/shared_storage/db/node` on each management node

Table 1-2 (Cont.) Oracle Private Cloud Appliance Databases

Item	Description
Oracle Private Cloud Appliance Inventory Database	Contains information on all hardware components appearing in the management network `192.168.4.0/24`. Components include the management and compute nodes but also switches, fabric interconnects, ZFS Storage Appliance and PDUs. The stored information includes IP addresses and host names, pingable status, when a component was last seen online, etc. This database is queried regularly by a number of Private Cloud Appliance services. **Type:** BerkeleyDB **Location:**`MGMT_ROOT/db/inventory` on the ZFS, accessible via `/nfs/shared_storage/db/inventory` on each management node
Oracle Private Cloud Appliance Netbundle Database	Predefines Ethernet and bond device names for all possible networks that can be configured throughout the system, and which are allocated dynamically. **Type:** BerkeleyDB **Location:**`MGMT_ROOT/db/netbundle` on the ZFS, accessible via `/nfs/shared_storage/db/netbundle` on each management node
Oracle Private Cloud Appliance DHCP Database	Contains information on the assignment of DHCP addresses to newly detected compute nodes. **Type:** BerkeleyDB **Location:**`MGMT_ROOT/db/dhcp` on the ZFS, accessible via `/nfs/shared_storage/db/dhcp` on each management node
Cisco Data Network Database	Contains information on the networks configured for traffic through the spine switches, and the interfaces participating in the networks. Used only on systems with Ethernet-based network architecture. **Type:** BerkeleyDB **Location:**`MGMT_ROOT/db/cisco_data_network_db` on the ZFS, accessible via `/nfs/shared_storage/db/cisco_data_network_db` on each management node
Cisco Management Switch Ports Database	Defines the factory-configured map of Cisco Nexus 9348GC-FXP Switch ports to the rack unit or element to which that port is connected. It is used to map switch ports to machine names. Used only on systems with Ethernet-based network architecture. **Type:** BerkeleyDB **Location:**`MGMT_ROOT/db/cisco_ports` on the ZFS, accessible via `/nfs/shared_storage/db/cisco_ports` on each management node
Oracle Private Cloud Appliance Mini Database	A multi-purpose database used to map compute node hardware profiles to on-board disk size information. It also contains valid hardware configurations that servers must comply with in order to be accepted as a Private Cloud Appliance component. Entries contain a sync ID for more convenient usage within the Command Line Interface (CLI). **Type:** BerkeleyDB **Location:**`MGMT_ROOT/db/mini_db` on the ZFS, accessible via `/nfs/shared_storage/db/mini_db` on each management node

Table 1-2 (Cont.) Oracle Private Cloud Appliance Databases

Item	Description
Oracle Private Cloud Appliance Monitor Database	Records fault counts detected through the ILOMs of all active components identified in the Inventory Database. **Type:** BerkeleyDB **Location:**`MGMT_ROOT/db/monitor` on the ZFS, accessible via `/nfs/shared_storage/db/monitor` on each management node
Oracle Private Cloud Appliance Setup Database	Contains the data set by the Oracle Private Cloud Appliance Dashboard setup facility. The data in this database is automatically applied by both the active and standby management nodes when a change is detected. **Type:** BerkeleyDB **Location:**`MGMT_ROOT/db/setup` on the ZFS, accessible via `/nfs/shared_storage/db/setup` on each management node
Oracle Private Cloud Appliance Task Database	Contains state data for all of the asynchronous tasks that have been dispatched within the Private Cloud Appliance. **Type:** BerkeleyDB **Location:**`MGMT_ROOT/db/task` on the ZFS, accessible via `/nfs/shared_storage/db/task` on each management node
Oracle Private Cloud Appliance Synchronization Databases	Contain data and configuration settings for the synchronization service to apply and maintain across rack components. Errors from failed attempts to synchronize configuration parameters across appliance components can be reviewed in the `sync_errored_tasks` database, from where they can be retried or acknowledged. Synchronization databases are not present by default. They are created when the first synchronization task of a given type is received. **Type:** BerkeleyDB **Location:**`MGMT_ROOT/db/sync_*` on the ZFS, accessible via `/nfs/shared_storage/db/sync_*` on each management node
Oracle Private Cloud Appliance Update Database	Used to track the two-node coordinated management node update process. **Note:** Database schema changes and wallet changes between different releases of the controller software are written to a file. It ensures that these critical changes are applied early in the software update process, before any other appliance components are brought back up. **Type:** BerkeleyDB **Location:**`MGMT_ROOT/db/update` on the ZFS, accessible via `/nfs/shared_storage/db/update` on each management node

Table 1-2 (Cont.) Oracle Private Cloud Appliance Databases

Item	Description
Oracle Private Cloud Appliance Tenant Database	Contains details about all tenant groups: default and custom. These details include the unique tenant group ID, file system ID, member compute nodes, status information, etc. **Type:** BerkeleyDB **Location:**`MGMT_ROOT/db/tenant` on the ZFS, accessible via `/nfs/shared_storage/db/tenant` on each management node
Oracle VM Manager Database	Used on each management node as the management database for Oracle VM Manager. It contains all configuration details of the Oracle VM environment (including servers, pools, storage and networking), as well as the virtualized systems hosted by the environment. **Type:** MySQL Database **Location:**`MGMT_ROOT/ovmm_mysql/data/` on the ZFS, accessible via `/nfs/shared_storage/ovmm_mysql/data/` on each management node

Oracle Private Cloud Appliance Management Software

The Private Cloud Appliance includes software that is designed for the provisioning, management and maintenance of all of the components within the appliance. The controller software, which handles orchestration and automation of tasks across various hardware components, is not intended for human interaction. Its appliance administration functions are exposed through the browser interface and command line interface, which are described in detail in this guide.

> **Important:**
>
> All configuration and management tasks must be performed using the Oracle Private Cloud Appliance Dashboard and the Command Line Interface. Do not attempt to run any processes directly without explicit instruction from an Oracle Support representative. Attempting to do so may render your appliance unusable.

Besides the Dashboard and CLI, this software also includes a number of Python applications that run on the active management node. These applications are found in `/usr/sbin` on each management node. Some of these applications are described in the following list:

- `pca-backup`: performs backups of the appliance configuration as described in Oracle Private Cloud Appliance Backup
- `pca-check-master`: reports which of the two management nodes currently has the active role
- `ovca-daemon`: core provisioning and management daemon for the Private Cloud Appliance
- `pca-dhcpd`: helps the DHCP daemon register compute nodes

- `pca-diag`: collects diagnostic information from your appliance, as described in Oracle Private Cloud Appliance Diagnostics Tool.
- `pca-factory-init`: appliance initialization script that sets the appliance to its factory configuration. This script does not function as a reset. This script is only used for initial rack setup.
- `pca-redirect`: redirects HTTP or HTTPS requests to the Oracle Private Cloud Appliance Dashboard described in Oracle Private Cloud Appliance Dashboard
- `ovca-remote-rpc`: makes remote procedure calls directly to the Oracle VM Server Agent. Currently it is only used by the management node to monitor the heartbeat of the Oracle VM Server Agent.
- `ovca-rpc`: allows the Private Cloud Appliance software components to communicate directly with the underlying management scripts running on the management node.

Many of these applications use a specific Private Cloud Appliance library that is installed in `/usr/lib/python2.7/site-packages/ovca/` on each management node.

Oracle Private Cloud Appliance Diagnostics Tool

Private Cloud Appliance includes a tool to collect diagnostic data: logs and other types of files that can help to troubleshoot hardware and software problems. This tool is available at `/usr/sbin/pca-diag` on each management node and compute node.

While you can run `pca-diag` from the command line of any node in the system, only the active management node allows you to use all of the command line arguments. The `vmpinfo` argument is not available on the compute nodes, but running `pca-diag` directly on a compute node can still retrieve important diagnostic information regarding Oracle VM Server that cannot be captured with `vmpinfo`.

The `pca-diag` tool is typically run by multiple users with different roles. System administrators or field service engineers might use it as part of their standard operating procedures, or Oracle Support teams might request that the tool be run in a specific manner as part of an effort to diagnose and resolve reported hardware or software issues. For additional information and instructions, see Data Collection for Service and Support.

The data that `pca-diag` retrieves depends on the specified command line arguments.

`pca-diag`
When you invoke the `pca-diag` command with no arguments, the tool retrieves a basic set of files that provide information about the current health status of the Private Cloud Appliance. You can run this command on all management and compute nodes.
The collected data is stored in the following compressed tarball:

`/tmp/ovcadiag_`***`node-hostname_ID_date_time`***`.tar.bz2`

`pca-diag version`
The `version` argument displays version information for the current Private Cloud Appliance software stack. The `version` argument cannot be combined with any other argument.

`pca-diag ilom`
The `ilom` argument uses `ipmitool` to retrieve diagnostic data through the host's ILOM. The data set includes details about the host's operating system, processes, health status, and hardware and software configuration, as well as a number of files specific to the Private Cloud Appliance configuration.

You can run this command on all management and compute nodes. If `ipmitool` is not installed on a particular system, ILOM data collection is skipped for that system.
If `ipmitool` is not able to collect the data, for example if the ILOM is down, `pca-diag` will retry for 600 seconds. After 600 seconds with no success, any further ILOM data collection is skipped for that system.
The collected data is stored in the following compressed tarball:

`/tmp/ovcadiag_`***`node-hostname_ID_date_time`***`.tar.bz2`

`pca-diag vmpinfo`

> **Important:**
>
> When using the `vmpinfo` argument, the command must be run from the active management node.

The `vmpinfo` argument collects data from two sources:

- The `vmpinfo` argument activates the Oracle VM diagnostic data collection mechanism.

  Oracle VM diagnostic data is stored in the following `ovcadiag` tarball:

  `/tmp/ovcadiag_`***`node-hostname_ID_date_time`***`.tar.bz2`

- The `vmpinfo` argument uses the `vmpinfo3` script to collect logs and configuration details from the Oracle VM Manager, and collect logs and `sosreport` information from each Oracle VM Server or compute node.

  When you run `pca-diag vmpinfo` on the active management node, the SOS report for the active management node is collected in `vmpinfo3-`***`timestamp`***`/mgrsosreport/`, and the SOS report for the passive management node is in `standby-mgrsosreport/`.

  When you run `pca-diag vmpinfo` on the passive management node, the SOS report for the passive management node is collected in `vmpinfo3-`***`timestamp`***`/mgrsosreport/`, and the SOS report for the active management node is in `master-mgrsosreport/`.

  Other Oracle VM Manager and Oracle VM Server and compute node data is stored in the following `vmpinfo3` tarball:

  `/tmp/vmpinfo3-`***`version-date-time`***`.tar.gz`

  To collect diagnostic information for a subset of the Oracle VM Servers in the environment, run the command with an additional `servers` parameter:

  ```
  pca-diag vmpinfo servers='ovcacn07r1,ovcacn08r1,ovcacn09r1'
  ```

Provisioning and Orchestration

As a converged infrastructure solution, the Oracle Private Cloud Appliance is built to eliminate many of the intricacies of optimizing the system configuration. Hardware components are installed and cabled at the factory. Configuration settings and installation software are preloaded onto the system. Once the appliance is connected to the data center power source and public network, the provisioning process between the administrator pressing the power button of the first management node and the

appliance reaching its *Deployment Readiness* state is entirely orchestrated by the active management node. This section explains what happens as the Private Cloud Appliance is initialized and all nodes are provisioned.

Appliance Management Initialization

Boot Sequence and Health Checks

When power is applied to the first management node, it takes approximately five minutes for the server to boot. While the Oracle Linux operating system is loading, an Apache web server is started, which serves a static welcome page the administrator can browse to from the workstation connected to the appliance management network.

The necessary Oracle Linux services are started as the server comes up to runlevel 3 (multi-user mode with networking). At this point, the management node executes a series of system health checks. It verifies that all expected infrastructure components are present on the appliance administration network and in the correct predefined location, identified by the rack unit number and fixed IP address. Next, the management node probes the ZFS Storage Appliance for a management NFS export and a management iSCSI LUN with OCFS2 file system. The storage and its access groups have been configured at the factory. If the health checks reveal no problems, the `ocfs2` and `o2cb` services are started automatically.

Management Cluster Setup

When the OCFS2 file system on the shared iSCSI LUN is ready, and the `o2cb` services have started successfully, the management nodes can join the cluster. In the meantime, the first management node has also started the second management node, which will come up with an identical configuration. Both management nodes eventually join the cluster, but the first management node will take an exclusive lock on the shared OCFS2 file system using Distributed Lock Management (DLM). The second management node remains in permanent standby and takes over the lock only in case the first management node goes down or otherwise releases its lock.

With mutual exclusion established between both members of the management cluster, the active management node continues to load the remaining Private Cloud Appliance services, including `dhcpd`, Oracle VM Manager and the Private Cloud Appliance databases. The virtual IP address of the management cluster is also brought online, and the Oracle Private Cloud Appliance Dashboard is activated. The static Apache web server now redirects to the Dashboard at the virtual IP, where the administrator can access a live view of the appliance rack component status.

Once the `dhcpd` service is started, the system state changes to *Provision Readiness*, which means it is ready to discover non-infrastructure components.

Compute Node Discovery and Provisioning

Node Manager

To discover compute nodes, the Node Manager on the active management node uses a DHCP server and the node database. The node database is a BerkeleyDB type database, located on the management NFS share, containing the state and configuration details of each node in the system, including MAC addresses, IP addresses and host names. The discovery process of a node begins with a DHCP request from the ILOM. Most discovery and provisioning actions are synchronous and occur sequentially, while time consuming installation and configuration processes are launched in parallel and asynchronously. The DHCP server hands out pre-assigned IP addresses on the appliance administration network

(`192.168.4.0/24`). When the Node Manager has verified that a node has a valid service tag for use with Oracle Private Cloud Appliance, it launches a series of provisioning tasks. All required software resources have been loaded onto the ZFS Storage Appliance at the factory.

Provisioning Tasks

The provisioning process is tracked in the node database by means of status changes. The next provisioning task can only be started if the node status indicates that the previous task has completed successfully. For each valid node, the Node Manager begins by building a PXE configuration and forces the node to boot using Private Cloud Appliance runtime services. After the hardware RAID-1 configuration is applied, the node is restarted to perform a kickstart installation of Oracle VM Server. Crucial kernel modules and host drivers are added to the installation. At the end of the installation process, the network configuration files are updated to allow all necessary network interfaces to be brought up.

Once the internal management network exists, the compute node is rebooted one last time to reconfigure the Oracle VM Agent to communicate over this network. At this point, the node is ready for Oracle VM Manager discovery.

As the Oracle VM environment grows and contains more and more virtual machines and many different VLANs connecting them, the number of management operations and registered events increases rapidly. In a system with this much activity, the provisioning of a compute node takes significantly longer, because the provisioning tasks run through the same management node where Oracle VM Manager is active. There is no impact on functionality, but the provisioning tasks can take several hours to complete. It is recommended to perform compute node provisioning at a time when system activity is at its lowest.

Server Pool Readiness

Oracle VM Server Pool

When the Node Manager detects a fully installed compute node that is ready to join the Oracle VM environment, it issues the necessary Oracle VM CLI commands to add the new node to the Oracle VM server pool. With the discovery of the first node, the system also configures the clustered Oracle VM server pool with the appropriate networking and access to the shared storage. For every compute node added to Oracle VM Manager, the IPMI configuration is stored in order to enable convenient remote power-on/off.

Oracle Private Cloud Appliance expects that all compute nodes in one rack initially belong to a single clustered server pool with High Availability (HA) and Distributed Resource Scheduling (DRS) enabled. When all compute nodes have joined the Oracle VM server pool, the appliance is in *Ready* state, meaning virtual machines (VMs) can be deployed.

Expansion Compute Nodes

When an expansion compute node is installed, its presence is detected based on the DHCP request from its ILOM. If the new server is identified as a Private Cloud Appliance node, an entry is added in the node database with *New* state. This triggers the initialization and provisioning process. New compute nodes are integrated seamlessly to expand the capacity of the running system, without the need for manual reconfiguration by an administrator.

Synchronization Service

As part of the provisioning process, a number of configuration settings are applied, either globally or at the individual component level. Some are visible to the administrator, and some are entirely internal to the system. Throughout the lifecycle of the appliance, software updates, capacity extensions and configuration changes will occur at different points in time. For example, an expansion compute node may have different hardware, firmware, software, configuration and passwords compared to the servers already in use in the environment, and it comes with factory default settings that do not match those of the running system. A synchronization service, implemented on the management nodes, can set and maintain configurable parameters across heterogeneous sets of components within a Private Cloud Appliance environment. It facilitates the integration of new system components in case of capacity expansion or servicing, and allows the administrator to streamline the process when manual intervention is required. The CLI provides an interface to the exposed functionality of the synchronization service.

High Availability

The Oracle Private Cloud Appliance is designed for high availability at every level of its component make-up.

Management Node Failover

During the factory installation of a Private Cloud Appliance, the management nodes are configured as a cluster. The cluster relies on an OCFS2 file system exported as an iSCSI LUN from the ZFS storage to perform the heartbeat function and to store a lock file that each management node attempts to take control of. The management node that has control over the lock file automatically becomes the active node in the cluster.

When the Private Cloud Appliance is first initialized, the `o2cb` service is started on each management node. This service is the default cluster stack for the OCFS2 file system. It includes a node manager that keeps track of the nodes in the cluster, a heartbeat agent to detect live nodes, a network agent for intra-cluster node communication and a distributed lock manager to keep track of lock resources. All these components are in-kernel.

Additionally, the `ovca` service is started on each management node. The management node that obtains control over the cluster lock and is thereby promoted to the active management node, runs the full complement of Private Cloud Appliance services. This process also configures the Virtual IP that is used to access the active management node, so that it is 'up' on the active management node and 'down' on the standby management node. This ensures that, when attempting to connect to the Virtual IP address that you configured for the management nodes, you are always accessing the active management node.

In the case where the active management node fails, the cluster detects the failure and the lock is released. Since the standby management node is constantly polling for control over the lock file, it detects when it has control of this file and the `ovca` service brings up all of the required Private Cloud Appliance services. On the standby management node the Virtual IP is configured on the appropriate interface as it is promoted to the active role.

When the management node that failed comes back online, it no longer has control of the cluster lock file. It is automatically put into standby mode, and the Virtual IP is removed from the management interface. This means that one of the two management nodes in the rack is always available through the same IP address and is always correctly configured. The management node failover process takes up to 5 minutes to complete.

Oracle VM Management Database Failover

The Oracle VM Manager database files are located on a shared file system exposed by the ZFS Storage Appliance. The active management node runs the MySQL database server, which accesses the database files on the shared storage. In the event that the management node fails, the standby management node is promoted and the MySQL database server on the promoted node is started so that the service can resume as normal. The database contents are available to the newly running MySQL database server.

Compute Node Failover

High availability (HA) of compute nodes within the Private Cloud Appliance is enabled through the clustered server pool that is created automatically in Oracle VM Manager during the compute node provisioning process. Since the server pool is configured as a cluster using an underlying OCFS2 file system, HA-enabled virtual machines running on any compute node can be migrated and restarted automatically on an alternate compute node in the event of failure.

For background information about the principles of high availability, see How Does High Availability (HA) Work? in the *Oracle VM Concepts Guide*.

Storage Redundancy

Further redundancy is provided through the use of the ZFS Storage Appliance to host storage. This component is configured with RAID-1 providing integrated redundancy and excellent data loss protection. Furthermore, the storage appliance includes two storage heads or controllers that are interconnected in a clustered configuration. The pair of controllers operate in an active-passive configuration (all data pools and data interfaces owned by only one head in the cluster), meaning continuation of service is guaranteed in the event that one storage head should fail. The storage heads share a single IP in the storage subnet, but both have an individual management IP address for convenient maintenance access.

Network Redundancy

All of the customer-usable networking within the Private Cloud Appliance is configured for redundancy. Only the internal administrative Ethernet network, which is used for initialization and ILOM connectivity, is not redundant. There are two of each switch type to ensure that there is no single point of failure. Networking cabling and interfaces are equally duplicated and switches are interconnected as described in Network Infrastructure.

Oracle Private Cloud Appliance Backup

The configuration of all components within Private Cloud Appliance is automatically backed up and stored on the ZFS Storage Appliance as a set of archives. Backups are named with a time stamp for when the backup is run.

During initialization, a crontab entry is created on each management node to perform a global backup twice in every 24 hours. The first backup runs at 09h00 and the second at 21h00. Only the active management node actually runs the backup process when it is triggered.

> **Note:**
>
> To trigger a backup outside of the default schedule, use the backup command in the Oracle Private Cloud Appliance Command Line Interface (CLI).

Backups are stored on the `MGMT_ROOT` file system on the ZFS Storage Appliance and are accessible on each management node at `/nfs/shared_storage/backups`. When the backup process is triggered, it creates a temporary directory named with the time stamp for the current backup process. The entire directory is archived in a `*.tar.bz2` file when the process is complete. Within this directory several subdirectories are also created:

- **data_net_switch**: used only on systems with Ethernet-based network architecture; contains the configuration data of the spine and leaf switches
- **mgmt_net_switch**: used only on systems with Ethernet-based network architecture; contains the management switch configuration data
- **ovca**: contains all of the configuration information relevant to the deployment of the management nodes such as the password wallet, the network configuration of the management nodes, configuration databases for the Private Cloud Appliance services, and DHCP configuration.
- **ovmm**: contains the most recent backup of the Oracle VM Manager database, the actual source data files for the current database, and the UUID information for the Oracle VM Manager installation. Note that the actual backup process for the Oracle VM Manager database is handled automatically from within Oracle VM Manager. Manual backup and restore are described in detail in Backing Up and Restoring Oracle VM Manager in the *Oracle VM Administrator's Guide*.
- **ovmm_upgrade**: contains essential information for each upgrade attempt. When an upgrade is initiated, a time-stamped subdirectory is created to store the `preinstall.log` file with the output from the pre-upgrade checks. Backups of any other files modified during the pre-upgrade process, are also saved in this directory.
- **zfssa**: contains all of the configuration information for the ZFS Storage Appliance

The backup process collects data for each component in the appliance and ensures that it is stored in a way that makes it easy to restore that component to operation in the case of failure.

> **Note:**
>
> Restoration from backup must only be performed by Oracle Service Personnel.

Taking regular backups is standard operating procedure for any production system. The internal backup mechanism cannot protect against full system failure, site outage or disaster. Therefore, you should consider implementing a backup strategy to copy key system data to external storage. This requires what is often referred to as a *bastion host*: a dedicated system configured with specific internal and external connections.

For a detailed description of the backup contents, and for guidelines to export internal backups outside the appliance, refer to the Oracle technical paper entitled Oracle Private Cloud Appliance Backup Guide.

Oracle Private Cloud Appliance Upgrader

Together with Oracle Private Cloud Appliance Controller Software Release 2.3.4, a new independent upgrade tool was introduced: the Oracle Private Cloud Appliance Upgrader. It is provided as a separate application, with its own release and update schedule. It maintains the phased approach, where management nodes, compute nodes and other rack components are updated in separate procedures, while at the same time it groups and automates sets of tasks that were previously executed as scripted or manual steps. The new design has better error handling and protection against terminal crashes, ssh timeouts or inadvertent user termination. It is intended to reduce complexity and improve the overall upgrade experience.

The Oracle Private Cloud Appliance Upgrader was built as a modular framework. Each module consists of pre-checks, an execution phase such as upgrade or install, and post-checks. Besides the standard interactive mode, modules also provide silent mode for programmatic use, and verify-only mode to run pre-checks without starting the execution phase.

The first module developed within the Oracle Private Cloud Appliance Upgrader framework, is the management node upgrade. With a single command, it guides the administrator through the pre-upgrade validation steps (now included in the pre-checks of the Upgrader), software image deployment, Oracle Private Cloud Appliance Controller Software update, Oracle Linux operating system Yum update, and Oracle VM Manager upgrade.

As of Controller Software Release 2.4.4, the Oracle Private Cloud Appliance Upgrader includes functionality to perform compute node upgrades.

For software update instructions, see Upgrading Oracle Private Cloud Appliance.

For specific Oracle Private Cloud Appliance Upgrader details, see Upgrading the Management Node Controller Software.

2

Monitoring and Managing Oracle Private Cloud Appliance

Monitoring and management of the Private Cloud Appliance is achieved using the Oracle Private Cloud Appliance Dashboard. This web-based graphical user interface is also used to perform the initial configuration of the appliance beyond the instructions provided in the Quick Start poster included in the packaging of the appliance.

> **NOT_SUPPORTED:**
>
> Before starting the system and applying the initial configuration, read and understand the Oracle Private Cloud Appliance Release Notes. The section Known Limitations and Workarounds provides information that is critical for correctly executing the procedures in this document. Ignoring the release notes may cause you to configure the system incorrectly. Bringing the system back to normal operation may require a complete factory reset.

The Oracle Private Cloud Appliance Dashboard allows you to perform the following tasks:

- Initial software configuration (and reconfiguration) for the appliance using the Network Environment window, as described in Network Settings.
- Hardware provisioning monitoring and identification of each hardware component used in the appliance, accessed via the Hardware View window described in Hardware View.
- Resetting the passwords used for different components within the appliance, via the Password Management window, as described in Authentication.

The Oracle Private Cloud Appliance Controller Software includes functionality that is currently not available through the Dashboard user interface:

- **Backup**

  The configuration of all components within Private Cloud Appliance is automatically backed up based on a crontab entry. This functionality is not configurable. Restoring a backup requires the intervention of an Oracle-qualified service person. For details, see Oracle Private Cloud Appliance Backup.

- **Update**

  The update process is controlled from the command line of the active management node, using the Oracle Private Cloud Appliance Upgrader. For details, see Oracle Private Cloud Appliance Upgrader. For step-by-step instructions, see Upgrading Oracle Private Cloud Appliance.

- **Custom Networks**

  In situations where the default network configuration is not sufficient, the command line interface allows you to create additional networks at the appliance level. For details and step-by-step instructions, see Network Customization.

- **Tenant Groups**

  The command line interface provides commands to optionally subdivide a Private Cloud Appliance environment into a number of isolated groups of compute nodes. These groups of servers are called tenant groups, which are reflected in Oracle VM as different server pools. For details and step-by-step instructions, see Tenant Groups.

Guidelines and Limitations

The Oracle Private Cloud Appliance is provided as an appliance with carefully preconfigured hardware and software stacks. Making any changes to the hardware or software of the appliance, unless explicitly told to do so by the Oracle Private Cloud Appliance product documentation or Oracle support, will result in an unsupported configuration. This section lists some of the operations that are not permitted, presented as guidelines and limitations that should be followed when working within the Oracle Private Cloud Appliance Dashboard, CLI, or Oracle VM Manager interfaces. If you have a question about changing anything not explicitly permitted or described in the documentation, contact Oracle to open an SR.

The following actions must not be performed, except when Oracle gives specific instructions to do so.

Do Not:

- attempt to discover, remove, rename or otherwise modify servers or their configuration;
- add, remove, or update RPMs on Private Cloud Appliance server components other than those distributed with Private Cloud Appliance software except when specifically approved by Oracle;
- attempt to modify the NTP configuration of a server;
- attempt to add, remove, rename or otherwise modify server pools or their configuration;
- attempt to change the configuration of server pools corresponding with tenant groups configured through the appliance controller software (except for DRS policy setting);
- attempt to move servers out of the existing server pools, except when using the `pca-admin` commands for administering tenant groups;
- attempt to add or modify or remove server processor compatibility groups;
- attempt to modify or remove the existing local disk repositories or the repository named **Rack1-repository**;
- attempt to delete or modify any of the preconfigured default networks, or custom networks configured through the appliance controller software;
- attempt to connect virtual machines to the appliance management network;
- attempt to modify or delete any existing Storage elements that are already configured within Oracle VM, or use the reserved names of the default storage elements – for example `OVCA_ZFSSA_Rack1` – for any other configuration;
- attempt to configure global settings, such as YUM Update, in the **Reports and Resources** tab (except for tags, which are safe to edit);

- attempt to select a non-English character set or language for the operating system, because this is not supported by Oracle VM Manager – see support document [PCA 2.3.4] OVMM upgrade fails with Invalid FQN (Doc ID 2519818.1);
- attempt to connect any Private Cloud Appliance component to a customer's LDAP or Active Directory for authentication, including management nodes, compute nodes, ZFS Storage Appliances, NIS, NIS+, and other naming services;
- attempt to add users – for example – adding users to management nodes or to WebLogic;
- attempt to change DNS settings on compute nodes or ZFS Storage Appliances. The Oracle Private Cloud Appliance Dashboard contains the only permitted DNS settings.
- change settings on Ethernet switches integrated into the Oracle Private Cloud Appliance or Oracle Private Cloud at Customer.
- attempt to add a server running Oracle VM 3.4.6.x to a tenant group that already contains a compute node running Oracle VM 3.4.7.
- migrate a virtual machine from a compute node running Oracle VM 3.4.7 to a compute node running Oracle VM 3.4.6.x.

If you ignore this advice, the Private Cloud Appliance automation, which uses specific naming conventions to label and manage assets, may fail. Out-of-band configuration changes would not be known to the orchestration software of the Private Cloud Appliance. If a conflict between the Private Cloud Appliance configuration and Oracle VM configuration occurs, it may not be possible to recover without data loss or system downtime.

> **Note:**
>
> An exception to these guidelines applies to the creation of a *Service VM*. This is a VM created specifically to perform administrative operations, for which it needs to be connected to both the public network and internal appliance networks. For detailed information and instructions, see support document How to Create Service Virtual Machines on the Private Cloud Appliance by using Internal Networks (Doc ID 2017593.1).
>
> There is a known issue with the Oracle Private Cloud Appliance Upgrader, which stops the upgrade process if Service VMs are present. For the appropriate workaround, see support document [PCA 2.3.4] pca_upgrader Check Fails with Exception - Network configuration error: 'inet' (Doc ID 2510822.1).

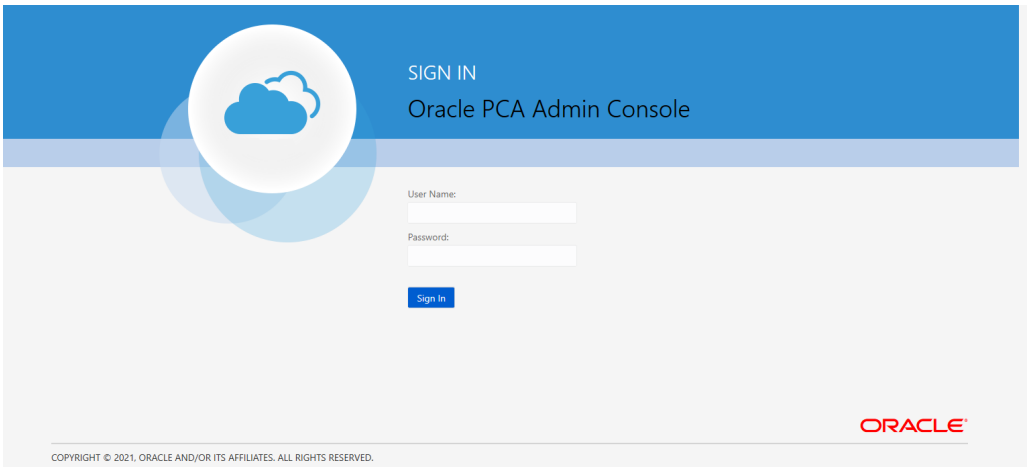
Connecting and Logging in to the Oracle Private Cloud Appliance Dashboard

To open the Login page of the Oracle Private Cloud Appliance Dashboard, enter the following address in a Web browser:

`https://`***`manager-vip`***`:7002/dashboard`

Where, ***`manager-vip`*** refers to the shared Virtual IP address that you configured for your management nodes during installation. By using the shared Virtual IP address, you ensure that you always access the Oracle Private Cloud Appliance Dashboard on the active management node.

Figure 2-1 Dashboard Login



Note:

If you are following the installation process and this is your first time accessing the Oracle Private Cloud Appliance Dashboard, the Virtual IP address in use by the active management node is set to the factory default `192.168.4.216`. This is an IP address in the internal appliance management network, which can only be reached if you use a workstation patched directly into the available Ethernet port 48 in the Cisco Nexus 9348GC-FXP Switch.

Important:

You must ensure that if you are accessing the Oracle Private Cloud Appliance Dashboard through a firewalled connection, the firewall is configured to allow TCP traffic on the port that the Oracle Private Cloud Appliance Dashboard is using to listen for connections.

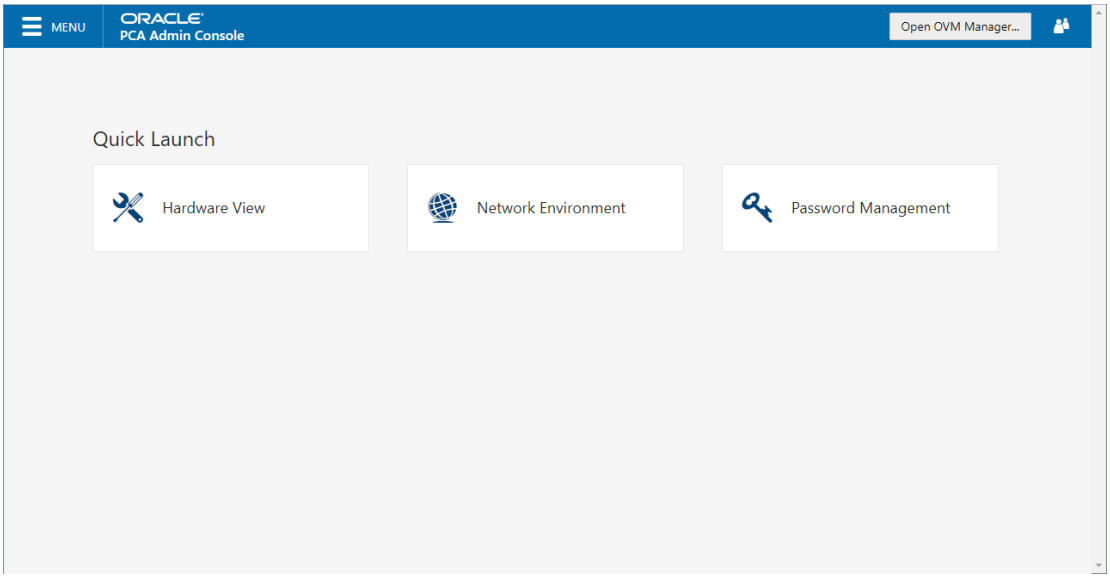
Enter your Oracle Private Cloud Appliance Dashboard administration user name in the **User Name** field. This is the administration user name you configured during installation. Enter the password for the Oracle Private Cloud Appliance Dashboard administration user name in the **Password** field.

Important:

The Oracle Private Cloud Appliance Dashboard makes use of cookies in order to store session data. Therefore, to successfully log in and use the Oracle Private Cloud Appliance Dashboard, your web browser must accept cookies from the Oracle Private Cloud Appliance Dashboard host.

When you have logged in to the Dashboard successfully, the home page is displayed. The central part of the page contains Quick Launch buttons that provide direct access to the key functional areas.

Figure 2-2 Dashboard Home Page



From every Dashboard window you can always go to any other window by clicking the Menu in the top-left corner and selecting a different window from the list. A button in the header area allows you to open Oracle VM Manager.

Hardware View

The **Hardware View** window within the Oracle Private Cloud Appliance Dashboard provides a graphical representation of the hardware components as they are installed within the rack. The view of the status of these components is automatically refreshed every 30 seconds by default. You can set the refresh interval or disable it through the Auto Refresh Interval list. Alternatively, a **Refresh** button at the top of the page allows you to refresh the view at any time.

During particular maintenance tasks, such as upgrading management nodes, you may need to disable compute node provisioning temporarily. This **Disable CN Provisioning** button at the top of the page allows you to suspend provisioning activity. When compute node provisioning is suspended, the button text changes to **Enable CN Provisioning** and its purpose changes to allow you to resume compute node provisioning as required.

Rolling over each item in the graphic with the mouse raises a pop-up window providing the name of the component, its type, and a summary of configuration and status information. For compute nodes, the pop-up window includes a **Reprovision** button, which allows you to restart the provisioning process if the node becomes stuck in an intermittent state or goes into error status before it is added to the Oracle VM server pool. Instructions to reprovision a compute node are provided in Reprovisioning a Compute Node when Provisioning Fails.

Caution:

The **Reprovision** button is to be used *only* for compute nodes that fail to complete provisioning. For compute nodes that have been provisioned properly and/or host running virtual machines, the **Reprovision** button is made unavailable to prevent incorrect use, thus protecting healthy compute nodes from loss of functionality, data corruption, or being locked out of the environment permanently.

Caution:

Reprovisioning restores a compute node to a clean state. If a compute node was previously added to the Oracle VM environment and has active connections to storage repositories other than those on the internal ZFS storage, the external storage connections need to be configured again after reprovisioning.

Alongside each installed component within the appliance rack, a status icon provides an indication of the *provisioning status* of the component. A status summary is displayed just above the rack image, indicating with icons and numbers how many nodes have been provisioned, are being provisioned, or are in error status. The Hardware View does not provide real-time health and status information about active components. Its monitoring functionality is restricted to the provisioning process. When a component has been provisioned completely and correctly, the Hardware View continues to indicate correct operation even if the component should fail or be powered off. See Table 2-1 for an overview of the different status icons and their meaning.

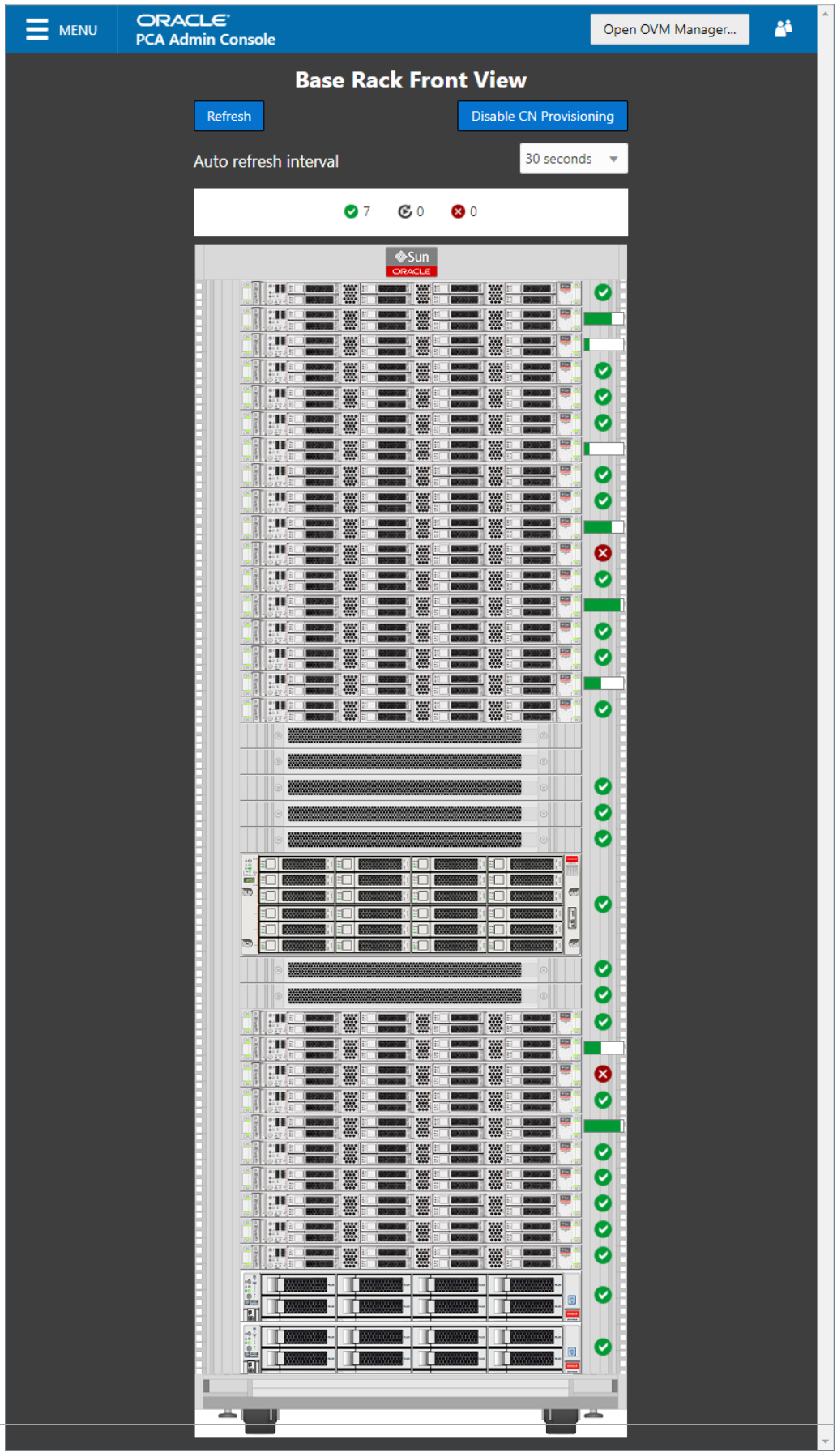
Table 2-1 Table of Hardware Provisioning Status Icons

Icon	Status	Description
	OK	The component is running correctly and has passed all health check operations. Provisioning is complete.
	Provisioning	The component is running, and provisioning is in progress. The progress bar fills up as the component goes through the various stages of provisioning. Key stages for compute nodes include: HMP initialization actions, Oracle VM Server installation, network configuration, storage setup, and server pool membership.
	Error	The component is not running and has failed health check operations. Component troubleshooting is required and the component may need to be replaced. Compute nodes also have this status when provisioning has failed.

> **Note:**
>
> For real-time health and status information of your active Private Cloud Appliance hardware, after provisioning, consult the Oracle VM Manager or Oracle Enterprise Manager UI.

The Hardware View provides an accessible tool for troubleshooting hardware components within the Private Cloud Appliance and identifying where these components are actually located within the rack. Where components might need replacing, the new component must take the position of the old component within the rack to maintain configuration.

Figure 2-3 The Hardware View



Network Settings

The **Network Environment** window is used to configure networking and service information for the management nodes. For this purpose, you should reserve three IP addresses in the public (data center) network: one for each management node, and one to be used as virtual IP address by both management nodes. The virtual IP address provides access to the Dashboard once the software initialization is complete.

To avoid network interference and conflicts, you must ensure that the data center network does not overlap with any of the infrastructure subnets of the Oracle Private Cloud Appliance default configuration. These are the subnets and VLANs you should keep clear:

Subnets:

- 192.168.4.0/24 – internal machine administration network: connects ILOMs and physical hosts
- 192.168.32.0/21 – internal management network: traffic between management and compute nodes
- 192.168.64.0/21 – underlay network for east/west traffic within the appliance environment
- 192.168.72.0/21 – underlay network for north/south traffic, enabling external connectivity
- 192.168.40.0/21 – storage network: traffic between the servers and the ZFS Storage Appliance

> **Note:**
>
> Each `/21` subnet comprises the IP ranges of eight `/24` subnets or over 2000 IP addresses. For example: `192.168.32.0/21` corresponds with all IP addresses from `192.168.32.1` to `192.168.39.255`.

VLANs:

- 1 – the Cisco default VLAN
- 3040 – the default service VLAN
- 3041-3072 – a range of 31 VLANs reserved for customer VM and host networks
- 3073-3099 – a range reserved for system-level connectivity

> **Note:**
>
> VLANs 3073-3088 are in use for VM access to the internal ZFS feature

  VLANs 3090-3093 are already in use for tagged traffic over the `/21` subnets listed above.

- 3968-4095 – a range reserved for Cisco internal device allocation

The **Network Environment** window is divided into three tabs: Management Nodes, Data Center Network, and DNS. Each tab is shown in this section, along with a description of the available configuration fields.

You can undo the changes you made in any of the tabs by clicking the Reset button. To confirm the configuration changes you made, enter the Dashboard Admin user password in the applicable field at the bottom of the window, and click Apply Changes.

> **Note:**
>
> When you click Apply Changes, the configuration settings in all three tabs are applied. Make sure that all required fields in all tabs contain valid information before you proceed.

Figure 2-4 shows the Management Nodes tab. The following fields are available for configuration:

- **Management Node 1:**
  - **IP Address:** Specify an IP address within your datacenter network that can be used to directly access this management node.
  - **Host Name:** Specify the host name for the first management node system.
- **Management Node 2:**
  - **IP Address:** Specify an IP address within your datacenter network that can be used to directly access this management node.
  - **Host Name:** Specify the host name for the second management node system.
- **Management Virtual IP Address:** Specify the shared Virtual IP address that is used to always access the active management node. This IP address must be in the same subnet as the IP addresses that you have specified for each management node.

Figure 2-4 Management Nodes Tab

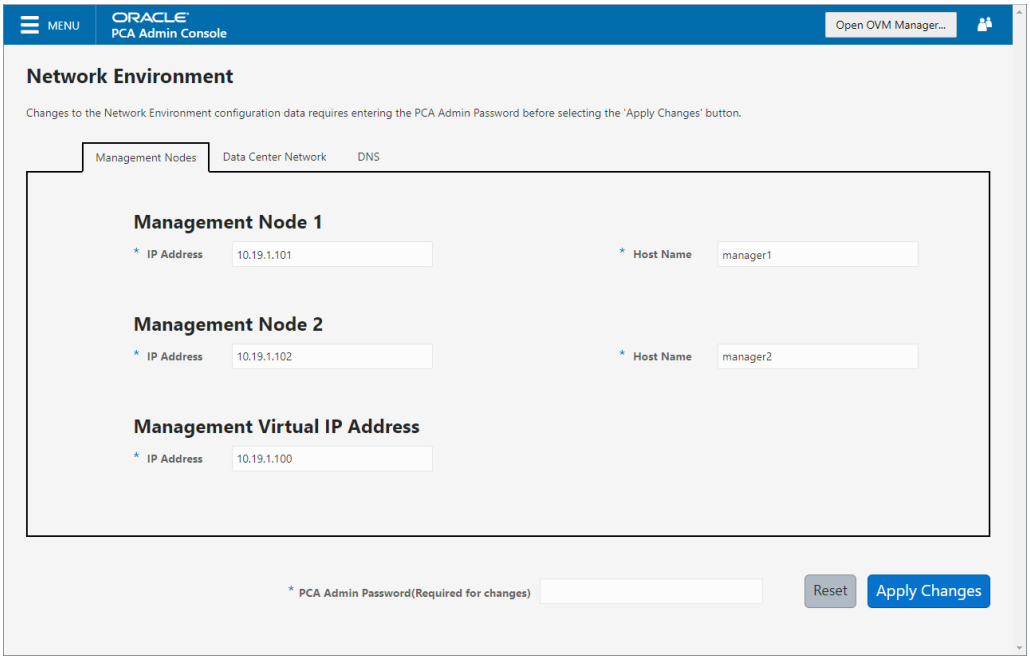


Figure 2-5 shows the Data Center Network tab. The following fields are available for configuration:

- **Management Network VLAN:** The default configuration does not assume that your management network exists on a VLAN. If you have configured a VLAN on your switch for the management network, you should toggle the slider to the *active* setting and then specify the VLAN ID in the provided field.

> **Caution:**
>
> When a VLAN is used for the management network, and VM traffic must be enabled over the same network, you must manually configure a VLAN interface on the vx13040 interfaces of the necessary compute nodes to connect them to the VLAN with the ID in question. For instructions to create a VLAN interface on a compute node, see Create VLAN Interfaces in the *Oracle VM Manager User's Guide*.

- **Domain Name:** Specify the data center domain that the management nodes belong to.
- **Netmask:** Specify the netmask for the network that the Virtual IP address and management node IP addresses belong to.
- **Default Gateway:** Specify the default gateway for the network that the Virtual IP address and management node IP addresses belong to.
- **NTP:** Specify the NTP server that the management nodes and other appliance components must use to synchronize their clocks to.

Figure 2-5 Data Center Network Tab

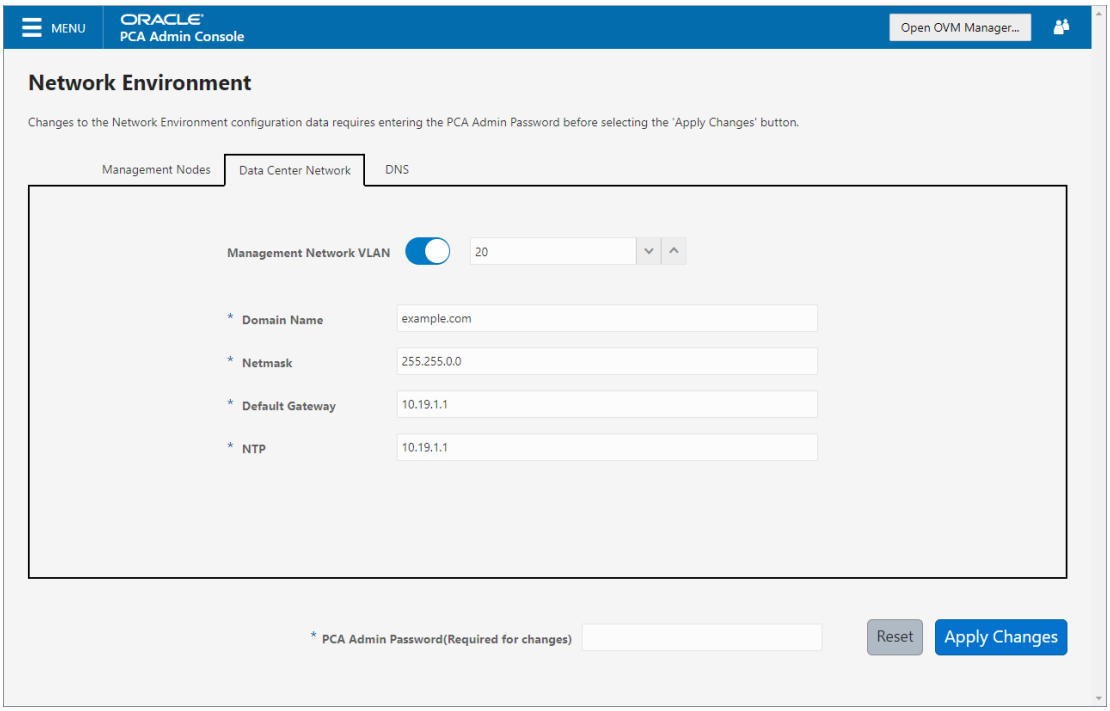
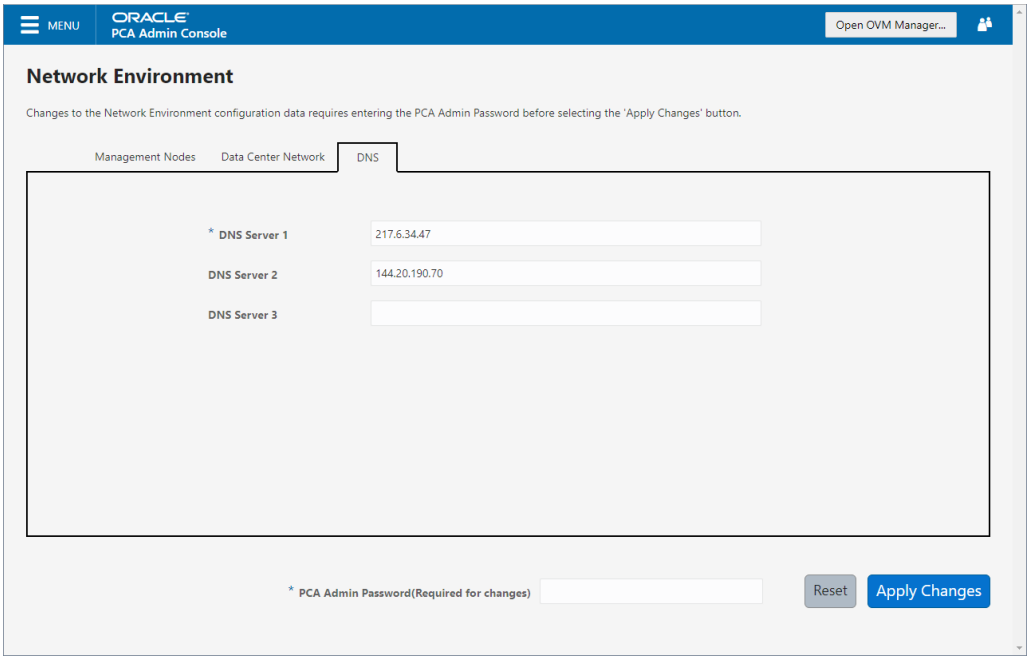


Figure 2-6 shows the Data Center Network tab. The following fields are available for configuration:

- **DNS Server 1:** Specify at least one DNS server that the management nodes can use for domain name resolution.
- **DNS Server 2:** Optionally, specify a second DNS server.
- **DNS Server 3:** Optionally, specify a third DNS server.

Figure 2-6 DNS Tab



You must enter the current Private Cloud Appliance *Admin* account password to make changes to any of these settings. Clicking the **Apply Changes** button at the bottom of the page saves the settings that are currently filled out in all three Network Environment tabs, and updates the configuration on each of the management nodes. The `ovca` services are restarted in the process, so you are required to log back in to the Dashboard afterward.

Functional Networking Limitations

There are different levels and areas of network configuration in an Oracle Private Cloud Appliance environment. For the correct operation of both the host infrastructure and the virtualized environment, it is critical that the administrator can make a functional distinction between the different categories of networking, and knows how and where to configure all of them. This section is intended as guidance to select the suitable interface to perform the main network administration operations.

In terms of functionality, practically all networks operate either at the appliance level or the virtualization level. Each has its own administrative interface: Oracle Private Cloud Appliance Dashboard and CLI on the one hand, and Oracle VM Manager on the other. However, the network configuration is not as clearly separated, because networking in Oracle VM depends heavily on existing configuration at the infrastructure level. For

example, configuring a new public virtual machine network in Oracle VM Manager requires that the hosts or compute nodes have network ports already connected to an underlying network with a gateway to the data center network or internet.

A significant amount of configuration – networking and other – is pushed from the appliance level to Oracle VM during compute node provisioning. This implies that a hierarchy exists; that appliance-level configuration operations must be explored before you consider making changes in Oracle VM Manager beyond the standard virtual machine management.

Network Configuration

This section describes the Oracle Private Cloud Appliance and Oracle VM network configuration.

- **Virtual Machine Network**

  By default, a fully provisioned Private Cloud Appliance is ready for virtual machine deployment. In Oracle VM Manager you can connect virtual machines to these networks directly:

  – `default_external`, created on the `vx13040` VxLAN interfaces of all compute nodes during provisioning

  – `default_internal`, created on the `vx2` VxLAN interfaces of all compute nodes during provisioning

  Also, you can create additional VLAN interfaces and VLANs with the *Virtual Machine* role. For virtual machines requiring public connectivity, use the compute nodes' `vx13040` VxLAN interfaces. For internal-only VM traffic, use the `vx2` VxLAN interfaces. For details, see Configuring Network Resources for Virtual Machines.

  > **Note:**
  >
  > Do not create virtual machine networks using the `eth`***x*** ports. These are detected in Oracle VM Manager as physical compute node network interfaces, but they are not cabled. Also, the `bond`***x*** ports and default VLAN interfaces (`tun-ext`, `tun-int`, `mgmt-int` and `storage-int`) that appear in Oracle VM Manager are part of the appliance infrastructure networking, and are not intended to be used in VM network configurations.

  Virtual machine networking can be further diversified and segregated by means of custom networks, which are described below. Custom networks must be created in the Private Cloud Appliance CLI. This generates additional VxLAN interfaces equivalent to the default `vx13040` and `vx2`. The custom networks and associated network interfaces are automatically set up in Oracle VM Manager, where you can expand the virtual machine network configuration with those newly discovered network resources.

- **Custom Network**

  Custom networks are infrastructure networks you create in addition to the default configuration. These are constructed in the same way as the default private and public networks, but using different compute node network interfaces and terminating on different spine switch ports. Whenever public connectivity is required, additional cabling between the spine switches and the next-level data center switches is required.

Because they are part of the infrastructure underlying Oracle VM, all custom networks must be configured through the Private Cloud Appliance CLI. The administrator chooses between three types: private, public or host network. For detailed information about the purpose and configuration of each type, see Network Customization.

If your environment has additional tenant groups, which are separate Oracle VM server pools, then a custom network can be associated with one or more tenant groups. This allows you to securely separate traffic belonging to different tenant groups and the virtual machines deployed as part of them. For details, see Tenant Groups.

Once custom networks have been fully configured through the Private Cloud Appliance CLI, the networks and associated ports automatically appear in Oracle VM Manager. There, additional VLAN interfaces can be configured on top of the new VxLAN interfaces, and then used to create more VLANs for virtual machine connectivity. The host network is a special type of custom public network, which can assume the *Storage* network role and can be used to connect external storage directly to compute nodes.

- **Network Properties**

  The network role is a property used within Oracle VM. Most of the networks you configure, have the *Virtual Machine* role, although you could decide to use a separate network for storage connectivity or virtual machine migration. Network roles – and other properties such as name and description, which interfaces are connected, properties of the interfaces and so on – can be configured in Oracle VM Manager, as long as they do not conflict with properties defined at the appliance level.

  Modifying network properties of the VM networks you configured in Oracle VM Manager involves little risk. However, you must **not** change the configuration – such as network roles, ports and so on – of the default networks: `eth_management`, `mgmt_internal`, `storage_internal`, `underlay_external`, `underlay_internal`, `default_external`, and `default_internal`. For networks connecting compute nodes, including custom networks, you must use the Private Cloud Appliance CLI. Furthermore, you cannot modify the functional properties of a custom network: you have to delete it and create a new one with the required properties.

  The maximum transfer unit (MTU) of a network interface, standard port or bond, cannot be modified. It is determined by the hardware properties or the SDN configuration, which cannot be controlled from within Oracle VM Manager.

- **VLAN Management**

  With the exception of the underlay VLAN networks configured through SDN, and the appliance management VLAN you configure in the Network Settings tab of the Oracle Private Cloud Appliance Dashboard, all VLAN configuration and management operations are performed in Oracle VM Manager. These VLANs are part of the VM networking.

  > **Tip:**
  >
  > When a large number of VLANs are required, it is good practice not to generate them all at once, because the process is time-consuming. Instead, add (or remove) VLANs in groups of 10.

Network Customization

The Oracle Private Cloud Appliance controller software allows you to add custom networks at the appliance level. This means that certain hardware components require configuration changes to enable the additional connectivity. The new networks are then configured automatically in your Oracle VM environment, where they can be used for isolating and optimizing network traffic beyond the capabilities of the default network configuration. All custom networks, both internal and public, are VLAN-capable.

The virtual machines hosted on the Private Cloud Appliance have access to external compute resources and storage, through the default external facing networks, as soon as the Oracle VM Manager is accessible.

If you need additional network functionality, custom networks can be configured for virtual machines and compute nodes. For example, a custom network can provide virtual machines with additional bandwidth or additional access to external compute resources or storage. Or you can use a custom network if compute nodes need to access storage repositories and data disks contained on external storage. The sections below describe how to configure and cable your Private Cloud Appliance for these custom networks.

NOT_SUPPORTED:

Do not modify the network configuration while upgrade operations are running. No management operations are supported during upgrade, as these may lead to configuration inconsistencies and significant repair downtime.

NOT_SUPPORTED:

Custom networks must never be deleted in Oracle VM Manager. Doing so would leave the environment in an error state that is extremely difficult to repair. To avoid downtime and data loss, always perform custom network operations in the Private Cloud Appliance CLI.

Caution:

The following network limitations apply:

- The maximum number of custom external networks is 7 per tenant group or per compute node.
- The maximum number of custom internal networks is 3 per tenant group or per compute node.
- The maximum number of VLANs is 256 per tenant group or per compute node.
- Only one host network can be assigned per tenant group or per compute node.

> **Caution:**
>
> When configuring custom networks, make sure that no provisioning operations or virtual machine environment modifications take place. This might lock Oracle VM resources and cause your Private Cloud Appliance CLI commands to fail.

Creating custom networks requires use of the CLI. The administrator chooses between three types: a network internal to the appliance, a network with external connectivity, or a host network. Custom networks appear automatically in Oracle VM Manager. The internal and external networks take the *virtual machine* network role, while a host network may have the *virtual machine* and *storage* network roles.

The host network is a particular type of external network: its configuration contains additional parameters for subnet and routing. The servers connected to it also receive an IP address in that subnet, and consequently can connect to an external network device. The host network is particularly useful for direct access to storage devices.

Configuring Custom Networks

For all networks with external connectivity, the spine Cisco Nexus 9336C-FX2 Switch ports must be specified so that these are reconfigured to route the external traffic. These ports must be cabled to create the physical uplink to the next-level switches in the data center. For detailed information, refer to "Appliance Uplink Configuration" in Network Requirements in the *Oracle Private Cloud Appliance Installation Guide*.

Creating a Custom Network

1. Using SSH and an account with superuser privileges, log into the active management node.

```
# ssh root@10.100.1.101
root@10.100.1.101's password:
root@ovcamn05r1 ~]#
```

2. Launch the Private Cloud Appliance command line interface.

```
# pca-admin
Welcome to PCA! Release: 2.4.4
PCA>
```

3. If your custom network requires public connectivity, you need to use one or more spine switch ports. Verify the number of ports available and carefully plan your network customizations accordingly. The following example shows how to retrieve that information from your system:

```
PCA> list network-port

Port      Switch          Type                State          Networks
----      ------          ----                -----          --------
1:1       ovcasw22r1      10G                 down           None
1:2       ovcasw22r1      10G                 down           None
1:3       ovcasw22r1      10G                 down           None
1:4       ovcasw22r1      10G                 down           None
2         ovcasw22r1      40G                 up             None
3         ovcasw22r1      auto-speed          down           None
```

```
4          ovcasw22r1      auto-speed              down            None
5:1        ovcasw22r1      10G                     up              default_external
5:2        ovcasw22r1      10G                     down            default_external
5:3        ovcasw22r1      10G                     down            None
5:4        ovcasw22r1      10G                     down            None
1:1        ovcasw23r1      10G                     down            None
1:2        ovcasw23r1      10G                     down            None
1:3        ovcasw23r1      10G                     down            None
1:4        ovcasw23r1      10G                     down            None
2          ovcasw23r1      40G                     up              None
3          ovcasw23r1      auto-speed              down            None
4          ovcasw23r1      auto-speed              down            None
5:1        ovcasw23r1      10G                     up              default_external
5:2        ovcasw23r1      10G                     down            default_external
5:3        ovcasw23r1      10G                     down            None
5:4        ovcasw23r1      10G                     down            None
-----------------
22 rows displayed

Status: Success
```

4. For a custom network with external connectivity, configure an uplink port group with the uplink ports you wish to use for this traffic. Select the appropriate breakout mode.

```
PCA> create uplink-port-group MyUplinkPortGroup '1:1 1:2' 10g-4x
Status: Success
```

> **Note:**
>
> The port arguments are specified as `'x:y'` where `x` is the switch port number and `y` is the number of the breakout port, in case a splitter cable is attached to the switch port. The example above shows how to retrieve that information.
>
> You must set the breakout mode of the uplink port group. When a 4-way breakout cable is used, all four ports must be set to either 10Gbit or 25Gbit. When no breakout cable is used, the port speed for the uplink port group should be either 100Gbit or 40Gbit, depending on connectivity requirements. See create uplink-port-group for command details.
>
> Network ports cannot be part of more than one network configuration.

5. Create a new network and select one of these types:

   - `rack_internal_network`: an Oracle VM virtual machine network with no access to external networking; no IP addresses are assigned to compute nodes. Use this option to allow virtual machines additional bandwidth beyond the default internal network.
   - `external_network`: an Oracle VM virtual machine network with access to external networking; no IP addresses are assigned to compute nodes. Use this option to allow virtual machines additional bandwidth when accessing external storage on a physical network separate from the default external facing network.
   - `host_network`: an Oracle VM compute node network with access to external networking; IP addresses are added to compute nodes. Use this option to allow compute nodes to access storage and compute resources external to the Private Cloud Appliance. This can also be used by virtual machines to access external compute resources just like `external_network`.

Use the following syntax:

- For an internal-only network, specify a network name.

```
PCA> create network MyInternalNetwork rack_internal_network
Status: Success
```

- For an external network, specify a network name and the spine switch port group to be configured for external traffic.

```
PCA> create network MyPublicNetwork external_network MyUplinkPortGroup
Status: Success
```

- For a host network, specify a network name, the spine switch ports to be configured for external traffic, the subnet, and optionally the routing configuration.

```
PCA> create network MyHostNetwork host_network MyUplinkPortGroup \
10.10.10 255.255.255.0 10.1.20.0/24 10.10.10.250
Status: Success
```

> **Note:**
>
> In this example the additional network and routing arguments for the host network are specified as follows, separated by spaces:
>
> – `10.10.10` = subnet prefix
>
> – `255.255.255.0` = netmask
>
> – `10.1.20.0/24` = route destination (as subnet or IPv4 address)
>
> – `10.10.10.250` = route gateway
>
> The subnet prefix and netmask are used to assign IP addresses to servers joining the network. The optional route gateway and destination parameters are used to configure a static route in the server's routing table. The route destination is a single IP address by default, so you must specify a netmask if traffic could be intended for different IP addresses in a subnet.
>
> When you define a host network, it is possible to enter invalid or contradictory values for the Prefix, Netmask and Route_Destination parameters. For example, when you enter a prefix with "0" as the first octet, the system attempts to configure IP addresses on compute node Ethernet interfaces starting with 0. Also, when the netmask part of the route destination you enter is invalid, the network is still created, even though an exception occurs. When such a poorly configured network is in an invalid state, it cannot be reconfigured or deleted with standard commands. If an invalid network configuration is applied, use the `--force` option to delete the network.
>
> Details of the create network command arguments are provided in create network in the CLI reference chapter.

> **Caution:**
>
> Network and routing parameters of a host network cannot be modified. To change these settings, delete the custom network and re-create it with updated settings.

6. Connect the required servers to the new custom network. You must provide the network name and the names of the servers to connect.

```
PCA> add network MyPublicNetwork ovcacn07r1
Status: Success
PCA> add network MyPublicNetwork ovcacn08r1
Status: Success
PCA> add network MyPublicNetwork ovcacn09r1
Status: Success
```

7. Verify the configuration of the new custom network.

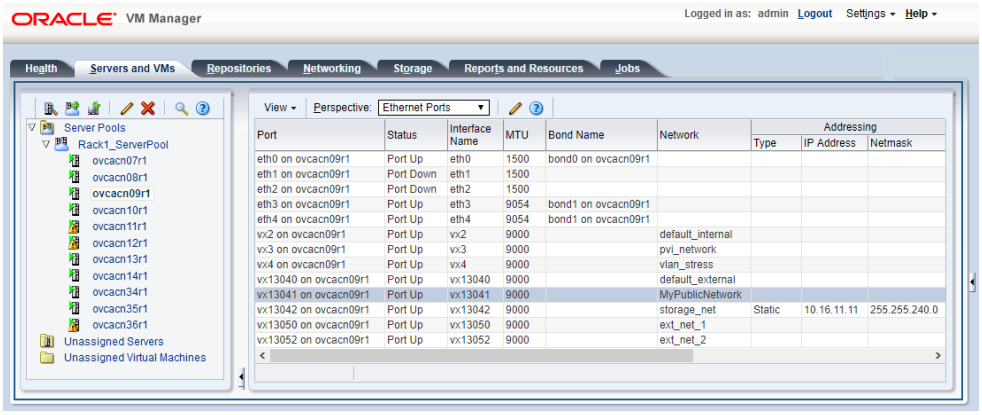
```
PCA> show network MyPublicNetwork

----------------------------------------
Network_Name         MyPublicNetwork
Trunkmode            None
Description          None
Ports                ['1:1', '1:2']
vNICs                None
Status               ready
Network_Type         external_network
Compute_Nodes        ovcacn07r1, ovcacn08r1, ovcacn09r1
Prefix               None
Netmask              None
Route Destination    None
Route Gateway        None
----------------------------------------

Status: Success
```

As a result of these commands, a VxLAN interface is configured on each of the servers to connect them to the new custom network. These configuration changes are reflected in the **Networking** tab and the **Servers and VMs** tab in Oracle VM Manager.

> **Note:**
>
> If the custom network is a host network, the server is assigned an IP address based on the prefix and netmask parameters of the network configuration, and the final octet of the server's internal management IP address.
>
> For example, if the compute node with internal IP address 192.168.4.9 were connected to the host network used for illustration purposes in this procedure, it would receive the address 10.10.10.9 in the host network.

Figure 2-7 shows a custom network named *MyPublicNetwork*, which is VLAN-capable and uses the compute node's `vx13041` interface.

Figure 2-7 Oracle VM Manager View of Custom Network Configuration



8. To disconnect servers from the custom network use the *remove network* command.

> **NOT_SUPPORTED:**
>
> Before removing the network connection of a server, make sure that no virtual machines are relying on this network.
>
> When a server is no longer connected to a custom network, make sure that its port configuration is cleaned up in Oracle VM.

```
PCA> remove network MyPublicNetwork
                          ovcacn09r1
************************************************************
 WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
************************************************************
Are you sure [y/N]:y

Status: Success
```

Deleting Custom Networks

This section describes how to delete custom networks.

Deleting a Custom Network

> **Caution:**
>
> Before deleting a custom network, make sure that all servers have been disconnected from it.

1. Using SSH and an account with superuser privileges, log into the active management node.

```
# ssh root@10.100.1.101
root@10.100.1.101's password:
root@ovcamn05r1 ~]#
```

2. Launch the Oracle Private Cloud Appliance command line interface.

```
# pca-admin
Welcome to PCA! Release: 2.4.4
PCA>
```

3. Verify that all servers have been disconnected from the custom network. No vNICs or nodes should appear in the network configuration.

> **Caution:**
>
> Related configuration changes in Oracle VM must be cleaned up as well.

```
PCA> show network MyPublicNetwork

----------------------------------------
Network_Name         MyPublicNetwork
Trunkmode            None
Description          None
Ports                ['1:1', '1:2']
vNICs                None
Status               ready
Network_Type         external_network
Compute_Nodes        None
Prefix               None
Netmask              None
Route_Destination    None
Route_Gateway        None
----------------------------------------
```

4. Delete the custom network.

```
PCA> delete network MyPublicNetwork
************************************************************
 WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
************************************************************
Are you sure [y/N]:y

Status: Success
```

> **Caution:**
>
> If a custom network is left in an invalid or error state, and the delete command fails, you may use the `--force` option and retry.

VM Storage Networks

Starting with Oracle Private Cloud Appliance Controller Software release 2.4.3, you can configure private storage networks that grant users access to the internal ZFS Storage Appliance from their Oracle VM environment. Private Cloud Appliance administrators with root access to the management nodes can create and manage the required networks and

ZFS shares (iSCSI/NFS) using the `pca-admin` command line interface. To ensure you can use this functionality, upgrade the storage network as described in Upgrading the Storage Network.

Private Cloud Appliance administrators can create up to sixteen VM storage networks which can be accessed by any virtual machine in any tenant group. End users of virtual machines configure their guest operating system to access one or more of these internal storage networks through NFS or iSCSI once the Private Cloud Appliance administrator has completed the setup.

The VM storage networks are designed to isolate different business systems or groups of end users from each other. For example, the HR department can use two VM storage networks for their virtual machines, while the payroll department can have three or four VM storage networks of their own. Each VM storage network is assigned a single, private non-routed VxLAN to ensure the network is isolated from other virtual machines owned by different end users. End users cannot gain root access to mange the internal ZFS Storage Appliance through the VM storage networks.

The ability to define internal storage networks directly for VMs was introduced in Oracle Private Cloud Appliance Controller Software release 2.4.3. Refer to Oracle Support Document 2722899.1 for important details before using this feature. Should you have any questions, contact Oracle support.

Tenant Groups

A standard Oracle Private Cloud Appliance environment built on a full rack configuration contains 25 compute nodes. A *tenant group* is a logical subset of a single Private Cloud Appliance environment. Tenant groups provide an optional mechanism for a Private Cloud Appliance administrator to subdivide the environment in arbitrary ways for manageability and isolation. The tenant group offers a means to isolate compute, network and storage resources per end customer. It also offers isolation from cluster faults.

Design Assumptions and Restrictions

Oracle Private Cloud Appliance supports a maximum of 8 tenant groups. This number includes the default tenant group, which cannot be deleted from the environment, and must always contain at least one compute node. Therefore, a single custom tenant group can contain up to 24 compute nodes, while the default *Rack1_ServerPool* can contain all 25.

Regardless of tenant group membership, all compute nodes are connected to all of the default Private Cloud Appliance networks. Custom networks can be assigned to multiple tenant groups. When a compute node joins a tenant group, it is also connected to the custom networks associated with the tenant group. When you remove a compute node from a tenant group, it is disconnected from those custom networks. A synchronization mechanism, built into the tenant group functionality, keeps compute node network connections up to date when tenant group configurations change.

When you reprovision compute nodes, they are automatically removed from their tenant groups, and treated as new servers. Consequently, when a compute node is reprovisioned, or when a new compute node is added to the environment, it is added automatically to *Rack1_ServerPool*. After successful provisioning, you can add the compute node to the appropriate tenant group.

When you create a new tenant group, the system does not create a storage repository for the new tenant group. An administrator must configure the necessary storage resources for virtual machines in Oracle VM Manager. See Viewing and Managing Storage Resources.

Configuring Tenant Groups

The tenant group functionality can be accessed through the Oracle Private Cloud Appliance CLI. With a specific set of commands, you manage the tenant groups, their member compute nodes, and the associated custom networks. The CLI initiates a number of Oracle VMoperations to set up the server pool, and a synchronization service maintains settings across the members of the tenant group.

NOT_SUPPORTED:

Do not modify the tenant group configuration while upgrade operations are running. No management operations are supported during upgrade, as these may lead to configuration inconsistencies and significant repair downtime.

Caution:

You must not modify the server pool in Oracle VM Manager because this causes inconsistencies in the tenant group configuration and disrupts the operation of the synchronization service and the Private Cloud Appliance CLI. Only server pool policies may be edited in Oracle VM Manager.

If you inadvertently used Oracle VM Manager to modify a tenant group, see Recovering from Tenant Group Configuration Mismatches.

Note:

For detailed information about the Private Cloud Appliance CLI tenant group commands, see Oracle Private Cloud Appliance Command Line Interface (CLI).

Creating and Populating a Tenant Group

1. Using SSH and an account with superuser privileges, log into the active management node.

```
# ssh root@10.100.1.101
root@10.100.1.101's password:
root@ovcamn05r1 ~]#
```

2. Launch the Private Cloud Appliance command line interface.

```
# pca-admin
Welcome to PCA! Release: 2.4.4
PCA>
```

3. Create the new tenant group.

```
PCA> create tenant-group myTenantGroup
Status: Success

PCA> show tenant-group myTenantGroup

----------------------------------------
Name                 myTenantGroup
Default              False
Tenant_Group_ID      0004fb00000200008154bf592c8ac33b
Servers              None
State                ready
Tenant_Group_VIP     None
Tenant_Networks      ['storage_internal', 'mgmt_internal',
'underlay_internal', 'underlay_external',
                     'default_external', 'default_internal']
Pool_Filesystem_ID   3600144f0d04414f400005cf529410003
----------------------------------------

Status: Success
```

The new tenant group appears in Oracle VM Manager as a new server pool. It has a 12GB server pool file system located on the internal ZFS Storage Appliance.

4. Add compute nodes to the tenant group.

   If a compute node is currently part of another tenant group, it is first removed from that tenant group.

   > **Caution:**
   >
   > If the compute node is hosting virtual machines, or if storage repositories are presented to the compute node or its current tenant group, removing a compute node from an existing tenant group will fail. If so, you have to migrate the virtual machines and unpresent the repositories before adding the compute node to a new tenant group.

   ```
   PCA> add compute-node ovcacn07r1 myTenantGroup
   Status: Success

   PCA> add compute-node ovcacn09r1 myTenantGroup
   Status: Success
   ```

5. Add a custom network to the tenant group.

   ```
   PCA> add network-to-tenant-group myPublicNetwork myTenantGroup
   Status: Success
   ```

   Custom networks can be added to the tenant group as a whole. This command creates synchronization tasks to configure custom networks on each server in the tenant group.

> **Caution:**
>
> While synchronization tasks are running, make sure that no reboot or provisioning operations are started on any of the compute nodes involved in the configuration changes.

6. Verify the configuration of the new tenant group.

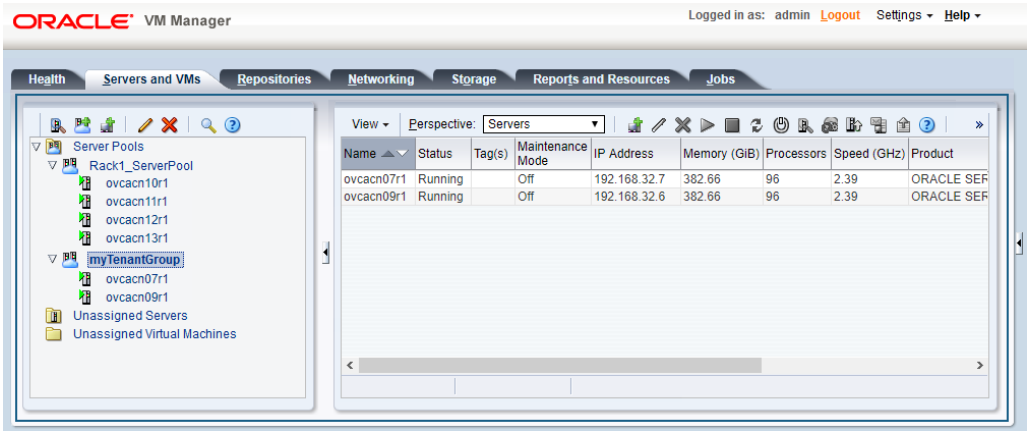
```
PCA> show tenant-group myTenantGroup

----------------------------------------
Name                 myTenantGroup
Default              False
Tenant_Group_ID      0004fb00000200008154bf592c8ac33b
Servers              ['ovcacn07r1', 'ovcacn09r1']
State                ready
Tenant_Group_VIP     None
Tenant_Networks      ['storage_internal', 'mgmt_internal', 'underlay_internal',
'underlay_external',
                     'default_external', 'default_internal', 'myPublicNetwork']
Pool_Filesystem_ID   3600144f0d04414f400005cf529410003
----------------------------------------

Status: Success
```

   The new tenant group corresponds with an Oracle VM server pool with the same name and has a pool file system. The command output also shows that the servers and custom network were added successfully.

These configuration changes are reflected in the **Servers and VMs** tab in Oracle VM Manager. Figure 2-8 shows a second server pool named `MyTenantGroup`, which contains the two compute nodes that were added as examples in the course of this procedure.

> **Note:**
>
> The system does not create a storage repository for a new tenant group. An administrator must configure the necessary storage resources for virtual machines in Oracle VM Manager. See Viewing and Managing Storage Resources.

Figure 2-8 Oracle VM Manager View of New Tenant Group



Reconfiguring and Deleting a Tenant Group

1. Identify the tenant group you intend to modify.

```
PCA> list tenant-group

Name                 Default      State
----                 -------      -----
Rack1_ServerPool     True         ready
myTenantGroup        False        ready
----------------
2 rows displayed

Status: Success

PCA> show tenant-group myTenantGroup

----------------------------------------
Name                 myTenantGroup
Default              False
Tenant_Group_ID      0004fb00000200008154bf592c8ac33b
Servers              ['ovcacn07r1', 'ovcacn09r1']
State                ready
Tenant_Group_VIP     None
Tenant_Networks      ['storage_internal', 'mgmt_internal',
'underlay_internal', 'underlay_external',
                     'default_external', 'default_internal',
'myPublicNetwork']
Pool_Filesystem_ID   3600144f0d04414f400005cf529410003
----------------------------------------

Status: Success
```

2. Remove a network from the tenant group.

   A custom network that has been associated with a tenant group can be removed again. The command results in serial operations, not using the synchronization service, to unconfigure the custom network on each compute node in the tenant group.

```
PCA> remove network-from-tenant-group myPublicNetwork myTenantGroup
**********************************************************
```

```
 WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
************************************************************
Are you sure [y/N]:y

Status: Success
```

3. Remove a compute node from the tenant group.

   Use Oracle VM Manager to prepare the compute node for removal from the tenant group. Make sure that virtual machines have been migrated away from the compute node, and that no storage repositories are presented.

```
PCA> remove compute-node ovcacn09r1 myTenantGroup
************************************************************
 WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
************************************************************
Are you sure [y/N]:y

Status: Success
```

   When you remove a compute node from a tenant group, any custom network associated with the tenant group is automatically removed from the compute node network configuration. Custom networks that are not associated with the tenant group are not removed.

4. Delete the tenant group.

   Before attempting to delete a tenant group, make sure that all compute nodes have been removed.

   Before removing the last remaining compute node from the tenant group, use Oracle VM Manager to unpresent any shared repository from the compute node, and then release ownership of it. For details, see support document Remove Last Compute Node from Tenant Group Fails with "There are still OCFS2 file systems" (Doc ID 2653515.1).

```
PCA> delete tenant-group myTenantGroup
************************************************************
 WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
************************************************************
Are you sure [y/N]:y

Status: Success
```

   When the tenant group is deleted, operations are launched to remove the server pool file system LUN from the internal ZFS storage appliance. The tenant group's associated custom networks are not destroyed.

Authentication

The **Password Management** window is used to reset the global Oracle Private Cloud Appliance password and to set unique passwords for individual components within the appliance. All actions performed via this tab require that you enter the current password for the Private Cloud Appliance `admin` user in the field labeled **Current PCA Admin Password**. Fields are available to specify the new password value and to confirm the value:

- **Current PCA Admin Password:** You must provide the current password for the Private Cloud Appliance `admin` user before any password changes can be applied.
- **New Password:** Provide the value for the new password that you are setting.

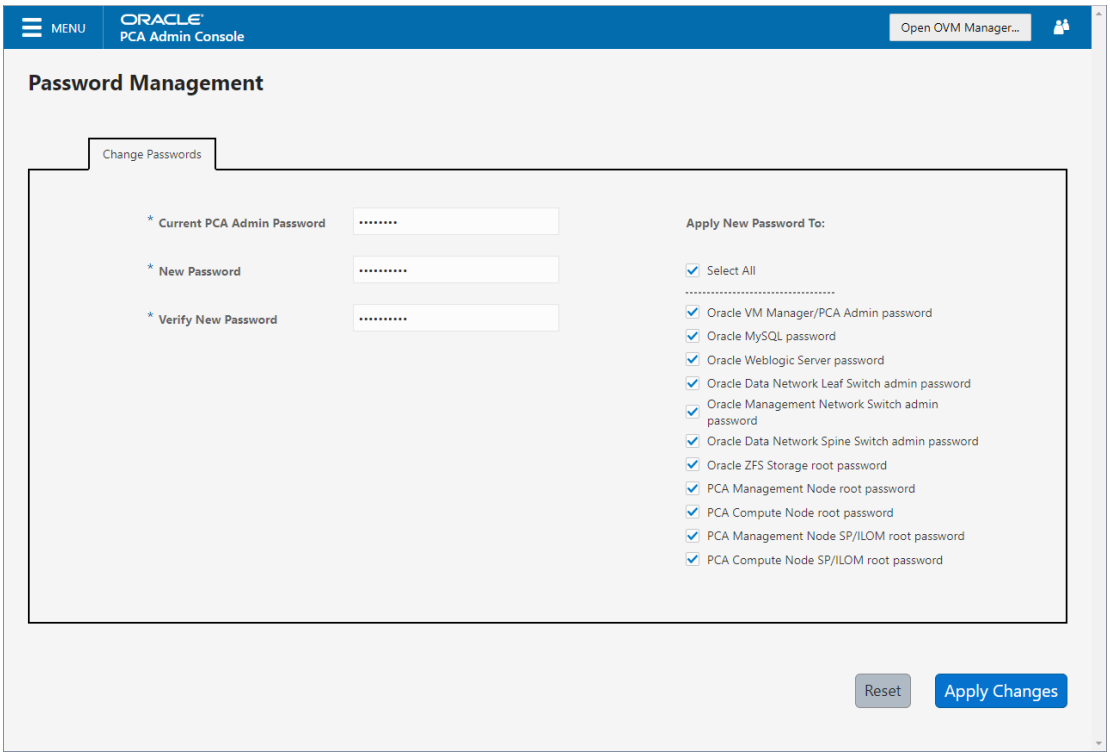
- **Verify Password:** Confirm the new password and check that you have not mistyped what you intended.

The window provides a series of check boxes that make it easy to select the level of granularity that you wish to apply to a password change. At this time, do not use the **Select All** button to apply a global password to all components that are used in the appliance. For more information see Changing Multiple Component Passwords Causes Authentication Failure in Oracle VM Manager. This action resets any individual passwords that you may have set for particular components. For stricter controls, you may set the password for individual components by simply selecting the check box associated with each component that you wish to apply a password to.

> **Caution:**
>
> Password changes are not instantaneous across the appliance, but are propagated through a task queue. When applying a password change, allow at least 30 minutes for the change to take effect. Do not attempt any further password changes during this delay. Verify that the password change has been applied correctly.

- **Select All**: Apply the new password to all components. All components in the list are selected.
- **Oracle VM Manager/PCA admin password**: Set the new password for the Oracle VM Manager and Oracle Private Cloud Appliance Dashboard `admin` user.
- **Oracle MySQL password**: Set the new password for the `ovs` user in MySQL used by Oracle VM Manager.
- **Oracle WebLogic Server password**: Set the new password for the `weblogic` user in WebLogic Server.
- **Oracle Data Network Leaf Switch admin password**: Set the new password for the `admin` user for the *leaf* Cisco Nexus 9336C-FX2 Switches.
- **Oracle Management Network Switch admin password**: Set the new password for the `admin` user for the Cisco Nexus 9348GC-FXP Switch.
- **Oracle Data Network Spine Switch admin password**: Set the new password for the `admin` user for the *spine* Cisco Nexus 9336C-FX2 Switches.
- **Oracle ZFS Storage root password**: Set the new password for the `root` user for the ZFS Storage Appliance.
- **PCA Management Node root password**: Set the new password for the `root` user for both management nodes.
- **PCA Compute Node root password**: Set the new password for the `root` user for all compute nodes.
- **PCA Management Node SP/ILOM root password**: Set the new password for the `root` user for the ILOM on both management nodes.
- **PCA Compute Node SP/ILOM root password**: Set the new password for the `root` user for the ILOM on all compute nodes.

Figure 2-9 Password Management



The functionality that is available in the Oracle Private Cloud Appliance Dashboard is equally available via the Oracle Private Cloud Appliance CLI as described in update password.

> **Caution:**
>
> Passwords of components must not be changed manually as this will cause mismatches with the authentication details stored in the Oracle Private Cloud Appliance Wallet.

Health Monitoring

The Oracle Private Cloud Appliance Controller Software contains a monitoring service, which is started and stopped with the `ovca` service on the active management node. When the system runs for the first time, it creates an *inventory database* and *monitor database*. Once these are set up and the monitoring service is active, health information about the hardware components is updated continuously.

The inventory database is populated with information about the various components installed in the rack, including the IP addresses to be used for monitoring. With this information, the *ping manager* pings all known components every 3 minutes and updates the inventory database to indicate whether a component is pingable and when it was last seen online. When errors occur, they are logged in the monitor database. Error information is retrieved from the component ILOMs.

For troubleshooting purposes, historic health status details can be retrieved through the CLI support mode by an authorized Oracle Field Engineer. When the CLI is used in support mode, a number of additional commands are available, two of which are used to display the contents of the health monitoring databases.

- Use `show db inventory` to display component health status information from the inventory database.
- Use `show db monitor` to display errors logged in the monitoring database.

The appliance administrator can retrieve current component health status information from the Oracle Linux command line on the active management node by using the Oracle Private Cloud Appliance Health Check utility. The Health Check utility is built on the framework of the Oracle Private Cloud Appliance Upgrader, and is included in the Upgrader package. It detects the appliance network architecture and runs the sets of health checks defined for the system in question.

Checking the Current Health Status of an Oracle Private Cloud Appliance Installation

1. Using SSH and an account with superuser privileges, log in to the active management node.

```
# ssh root@10.100.1.101
root@10.100.1.101's password:
root@ovcamn05r1 ~]#
```

2. Launch the Health Check utility.

```
# pca_healthcheck
PCA Rack Type: PCA X8_BASE.
Please refer to log file
/nfs/shared_storage/pca_upgrader/log/pca_healthcheck_2019_10_04-12.09.45.log
for more details.
```

After detecting the rack type, the utility executes the applicable health checks.

```
Beginning PCA Health Checks...

Check Management Nodes Are Running                                1/24
Check Support Packages                                            2/24
Check PCA DBs Exist                                               3/24
PCA Config File                                                   4/24
Check Shares Mounted on Management Nodes                          5/24
Check PCA Version                                                 6/24
Check Installed Packages                                          7/24
Check for OpenSSL CVE-2014-0160 - Security Update                 8/24
Management Nodes Have IPv6 Disabled                               9/24
Check Oracle VM Manager Version                                  10/24
Oracle VM Manager Default Networks                               11/24
Repositories Defined in Oracle VM Manager                        12/24
PCA Services                                                     13/24
Oracle VM Server Model                                           14/24
Network Interfaces on Compute Nodes                              15/24
Oracle VM Manager Settings                                       16/24
Check Network Leaf Switch                                        17/24
Check Network Spine Switch                                       18/24
All Compute Nodes Running                                        19/24
Test for ovs-agent Service on Compute Nodes                      20/24
Test for Shares Mounted on Compute Nodes                         21/24
Check for bash ELSA-2014-1306 - Security Update                  22/24
Check Compute Node's Active Network Interfaces                   23/24
```

```
Checking for xen OVMSA-2014-0026 - Security Update                    24/24

PCA Health Checks completed after 2 minutes
```

3. When the health checks have been completed, check the report for failures.

```
Check Management Nodes Are Running                                    Passed
Check Support Packages                                                Passed
Check PCA DBs Exist                                                   Passed
PCA Config File                                                       Passed
Check Shares Mounted on Management Nodes                              Passed
Check PCA Version                                                     Passed
Check Installed Packages                                              Passed
Check for OpenSSL CVE-2014-0160 - Security Update                     Passed
Management Nodes Have IPv6 Disabled                                   Passed
Check Oracle VM Manager Version                                       Passed
Oracle VM Manager Default Networks                                    Passed
Repositories Defined in Oracle VM Manager                             Passed
PCA Services                                                          Passed
Oracle VM Server Model                                                Passed
Network Interfaces on Compute Nodes                                   Passed
Oracle VM Manager Settings                                            Passed
Check Network Leaf Switch                                             Passed
Check Network Spine Switch                                            Failed
All Compute Nodes Running                                             Passed
Test for ovs-agent Service on Compute Nodes                           Passed
Test for Shares Mounted on Compute Nodes                              Passed
Check for bash ELSA-2014-1306 - Security Update                       Passed
Check Compute Node's Active Network Interfaces                        Passed
Checking for xen OVMSA-2014-0026 - Security Update                    Passed

--------------------------------------------------------------------------------
Overall Status                                                        Failed
--------------------------------------------------------------------------------

Please refer to log file
/nfs/shared_storage/pca_upgrader/log/pca_healthcheck_2019_10_04-12.09.45.log
for more details.
```

4. If certain checks have resulted in failures, review the log file for additional diagnostic information. Search for text strings such as "error" and "failed".

```
# grep -inr "failed" /nfs/shared_storage/pca_upgrader/log/
pca_healthcheck_2019_10_04-12.09.45.log

726:[2019-10-04 12:10:51 264234] INFO (healthcheck:254) Check Network Spine Switch
Failed -
731:  Spine Switch ovcasw22r1 North-South Management Network Port-channel
check                [FAILED]
733:  Spine Switch ovcasw22r1 Multicast Route
Check                                              [FAILED]
742:  Spine Switch ovcasw23r1 North-South Management Network Port-channel
check                [FAILED]
750:[2019-10-04 12:10:51 264234] ERROR (precheck:148) [Check Network Spine Switch
()] Failed
955:[2019-10-04 12:12:26 264234] INFO (precheck:116) [Check Network Spine Switch
()] Failed

# less /nfs/shared_storage/pca_upgrader/log/pca_healthcheck_2019_10_04-12.09.45.log

[...]
  Spine Switch ovcasw22r1 North-South Management Network Port-channel
```

```
check                 [FAILED]
  Spine Switch ovcasw22r1 OSPF Neighbor
Check                                                 [OK]
  Spine Switch ovcasw22r1 Multicast Route
Check                                               [FAILED]
  Spine Switch ovcasw22r1 PIM RP
Check                                                       [OK]
  Spine Switch ovcasw22r1 NVE Peer
Check                                                     [OK]
  Spine Switch ovcasw22r1 Spine Filesystem
Check                                             [OK]
  Spine Switch ovcasw22r1 Hardware Diagnostic
Check                                         [OK]
[...]
```

5. Investigate and fix any detected problems. Repeat the health check until the system passes all checks.

Fault Monitoring

Beginning with Oracle Private Cloud Appliance Controller software release 2.4.3, the health checker is a service started by the `ovca-daemon` on the active management node. Checks can be run manually from the command line, or by using definitions in the scheduler. Depending on the check definition, the Private Cloud Appliance health checker, the Oracle VM health check, and the Private Cloud Appliance pre-upgrade checks can be invoked.

- `pca_healthcheck` monitors the health of system hardware components. For details, see Health Monitoring.
- `ovm_monitor` monitors the Oracle VM Manager objects and other environment factors.
- `pca_upgrader` monitors the system during an upgrade.

Health checking can be integrated with the ZFS Phone Home service to send reports to Oracle on a weekly basis. The Phone Home function must be activated by the customer and requires that the appliance is registered with Oracle Auto Service Request (ASR). No separate installation is required: All functions come with the controller software in Oracle Private Cloud Appliance Controller software release 2.4.3 and later. For configuration information, see Phone Home Service. For more information about ASR, see Oracle Auto Service Request (ASR).

Using Fault Monitoring Checks

The appliance administrator can access current component health status information from the Oracle Linux command line on the active management node by using the Oracle Private Cloud Appliance Fault Monitoring utility. The Fault Monitoring utility is included in the `ovca` services. In addition, you can schedule checks to run automatically. The Fault Monitoring utility detects the appliance network architecture and runs the sets of health checks that are defined for that system.

Running Fault Monitor Tests Manually

The Fault Monitoring utility enables you to run an individual check, all the checks for a particular monitoring service, or all of the checks that are available.

1. Using SSH and an account with superuser privileges, log in to the active management node.

```
# ssh root@10.100.1.101
root@10.100.1.101's password:
root@ovcamn05r1 ~]#
```

2. List the available checks.

```
[root@ovcamn05r1 ~]# pca-faultmonitor --help
usage: pca-faultmonitor [-h] [--list_all_monitors][--list_ovm_monitors]
                        [--list_pca_healthcheck_monitors]
                        [--list_pca_upgrader_monitors]
                        [--run_all_monitors]
                        [--run_ovm_monitors]
                        [--run_pca_healthcheck_monitors]
                        [--run_pca_upgrader_monitors][-m MONITOR_LIST]
                        [--print_report]

optional arguments:
  -h, --help show this help message and exit
  --list_all_monitors List all Fault Monitors(Oracle VM, pca_healthcheck and
pca_upgrader)
  --list_ovm_monitors List Oracle VM Fault Monitors
  --list_pca_healthcheck_monitors List pca_healthcheck Fault Monitors
  --list_pca_upgrader_monitors List pca_upgrader Fault Monitors
  --run_all_monitors Run all Fault Monitors
  --run_ovm_monitors Run Oracle VM Fault Monitors
  --run_pca_healthcheck_monitors Run pca_healthcheck Fault Monitors
  --run_pca_upgrader_monitors Run pca_upgrader Fault Monitors
  -m MONITOR_LIST Runs a list of Fault Monitors. Each Fault Monitor must
     be specified with -m option
  --print_report Prints the report on console
None
PCA Rack type:      hardware_orange
Please refer the log file in /var/log/ovca-faultmonitor.log
Please look at fault report in /nfs/shared_storage/faultmonitor/20200512/
Note: Reports will not be created for success status
```

List all monitors of a specified check.

```
[root@ovcamn05r1 faultmonitor]# pca-faultmonitor --list_pca_upgrader_monitors
PCA Rack type:      hardware_orange
Please refer the log file in /var/log/faultmonitor/ovca-faultmonitor.log
Please look at fault report in /nfs/shared_storage/faultmonitor/20200221/
Note: Reports will not be created for success status

Listing all PCA upgrader faultmonitors

check_ib_symbol_errors                  verify_inventory_cns
validate_image                          check_available_space
check_max_paths_iscsi                   check_serverUpdateConfiguration
check_onf_error                         verify_password
check_rpm_db                            verify_network_config
check_yum_proxy                         check_motd
check_yum_repo                          connect_mysql
check_osa_disabled                      check_xsigo_configs
check_pca_services                      check_mysql_desync_passwords
check_storage_space                     verify_xms_cards
...
```

3. Run the desired checks.

- Run all checks.

```
[root@ovcamn05r1 ~]# pca-faultmonitor --run_all_monitors
```

- To run a specific check or list of checks, list one or more checks, each as an argument of a separate `-m` option.

```
[root@ovcamn05r1 ~]# pca-faultmonitor -m event_monitor -m
check_storage_space
```

- Run checks for a specific monitor.

```
[root@ovcamn05r1 ~]# pca-faultmonitor --run_pca_upgrader_monitors
[root@ovcamn05r1 faultmonitor]# pca-faultmonitor --run_ovm_monitors
PCA Rack type:      hardware_orange
Please refer the log file in /var/log/faultmonitor/ovca-faultmonitor.log
Please look at fault report in /nfs/shared_storage/faultmonitor/20200220/
Note: Reports will not be created for success status

Beginning OVM Fault monitor checks ...

event_monitor                          1/13
repository_utilization_monitor         2/13
storage_utilization_monitor            3/13
db_size_monitor                        4/13
onf_monitor                            5/13
db_backup_monitor                      6/13
firewall_monitor                       7/13
server_connectivity_monitor            8/13
network_monitor                        9/13
port_flapping_monitor                  10/13
storage_path_flapping_monitor          11/13
repository_mount_monitor               12/13
server_pool_monitor                    13/13
------------------------------------------------
Fault Monitor Report Summary
------------------------------------------------
OVM_Event_Monitor                       Success
OVM_Repository_Utilization_Monitor      Success
OVM_Storage_Utilization_Monitor         Success
DB_Size_Monitor                         Success
ONF_Monitor                             Success
DB_Backup_Monitor                       Success
Firewall_Monitor                        Success
Server_Connectivity_Monitor             Success
Network_Monitor                         Warning
Port_Flapping_Monitor                   Success
Storage_Path_Flapping_Monitor           Success
Repository_Mount_Monitor                Warning
Server_Pool_Monitor                     Success
------------------------------------------------
Overall                                    Failure
------------------------------------------------

PCA Rack type:      hardware_orange
Please refer the log file in /var/log/faultmonitor/ovca-faultmonitor.log
Please look at fault report in /nfs/shared_storage/faultmonitor/20200220/
Note: Reports will not be created for success status
Monitor execution completed after 5 minutes
```

4. If a check result is failed, review the console or log file for additional diagnostic information.

5. Investigate and fix any detected problems. Repeat the check until the system passes all checks.

Scheduling Fault Monitor Tests

By default, the `run_ovm_monitors`, `run_pca_healthcheck_monitors`, and `run_pca_upgrader_monitors` checks are scheduled to run weekly. You can change the frequency of these checks or add other checks to the scheduler. You must restart the `ovca` service to implement any schedule changes.

1. Using SSH and an account with superuser privileges, log in to the active management node.

```
# ssh root@10.100.1.101
root@10.100.1.101's password:
root@ovcamn05r1 ~]#
```

2. Change the schedule properties in the `ovca-system.conf` file.

   Use the following scheduling format:

```
* * * * *  command
- - - - -
| | | | |
| | | | ----  day of week (0-7, Sunday= 0 or 7)
| | | ------  month (1-12)
| | --------  day of month (1-31)
| ----------  hour (0-23)
------------  minute (0-59)

[root@ovcamn05r1 ~]# cat /var/lib/ovca/ovca-system.conf

[faultmonitor]
report_path: /nfs/shared_storage/faultmonitor/
report_format: json
report_dir_cleanup_days: 10
disabled_check_list: validate_image
enable_phonehome: 0
collect_report: 1

[faultmonitor_scheduler]
run_ovm_monitors: 0 2 * * *
run_pca_healthcheck_monitors: 0 1 * * *
run_pca_upgrader_monitors: 0 0 * * *
repository_utilization_monitor: 0 */2 * * *
check_ovmm_version: */30 * * * *
```

Changing Fault Monitoring Options

1. Using SSH and an account with superuser privileges, log in to the active management node.

```
# ssh root@10.100.1.101
root@10.100.1.101's password:
root@ovcamn05r1 ~]#
```

2. Change the appropriate property in the `ovca-system.conf` file.

   The `report_format` options are `json`, `text`, or `html`.

```
[root@ovcamn05r1 ~]# cat /var/lib/ovca/ovca-system.conf

[faultmonitor]
```

```
report_path: /nfs/shared_storage/faultmonitor/
report_format: json
report_dir_cleanup_days: 10
disabled_check_list: validate_image
enable_phonehome: 1
collect_report: 1
```

Phone Home Service

The Fault Monitoring utility is designed so that the management nodes collect fault data reports and copy those reports to the ZFS Storage Appliance.

If you want Oracle Service to monitor these fault reports, you can configure the Phone Home service to push these reports to Oracle on a weekly basis. Oracle Private Cloud Appliance uses the ZFS Storage Appliance Phone Home service.

Activating the Phone Home Service for Oracle Private Cloud Appliance

Use the following procedure to configure your system to send fault reports to Oracle for automated service response.

1. Make sure Oracle Auto Service Request (ASR) is installed on the Private Cloud Appliance, the appliance is registered with ASR, and ASR is enabled on the appliance. SeeOracle Auto Service Request (ASR).
2. Using SSH and an account with superuser privileges, log in to the active management node.

   ```
   # ssh root@10.100.1.101
   root@10.100.1.101's password:
   root@ovcamn05r1 ~]#
   ```

3. Enable Phone Home in the Fault Monitoring service.

   By default, Phone Home is disabled in Private Cloud Appliance.

   Use one of the following methods to enable the service:

   - Set the `enable_phonehome` property to `1` in the `ovca-system.conf` file on both management nodes.

     ```
     [root@ovcamn05r1 ~]# edit /var/lib/ovca/ovca-system.conf

     [faultmonitor]
     report_path: /nfs/shared_storage/faultmonitor/
     report_format: json
     report_dir_cleanup_days: 10
     disabled_check_list: validate_image
     enable_phonehome: 1
     collect_report: 1
     ```

   - Starting with release 2.4.4.1, you can also set the Phone Home property using the Private Cloud Appliance CLI `set system-property` command. Log in to each management node and type:

     ```
     [root@ovcamn05r1 ~]# pca-admin
     Welcome to PCA! Release: 2.4.4.1
     PCA> set system-property phonehome enable
     Status: Success
     ```

For more information, see set system-property.

4. Enable Phone Home in the ZFS Storage Appliance browser interface.
   a. Log in to the ZFS Storage Appliance browser interface.
   b. Go to **Configuration > Services > Phone Home**.
   c. Click the power icon to bring the service online.

Data Collection for Service and Support

If Oracle Auto Service Request (ASR) is enabled on the Private Cloud Appliance, a service request will be created and sent to Oracle Support automatically for some failures. See Oracle Auto Service Request (ASR).

If an issue is not automatically reported by ASR, open a service request at My Oracle Support to request assistance from Oracle Support. You need an Oracle Premier Support Agreement and your Oracle Customer Support Identifier (CSI). If you do not know your CSI, find the correct Service Center for your country (https://www.oracle.com/support/contact.html), then contact Oracle Services to open a non-technical service request (SR) to get your CSI.

When you open a service request, provide the following information where applicable:

- Description of the problem, including the situation where the problem occurs, and its impact on your operation.
- Machine type, operating system release, browser type and version, locale and product release, patches that you have applied, and other software that might be affecting the problem.
- Details of steps that you have taken to reproduce the problem.
- Applicable logs and other support data.

This section describes how to collect an archive file with relevant log files and other health information, and how to upload the information to Oracle Support. Oracle Support uses this information to analyze and diagnose the issues. Oracle Support might request that you collect particular data and attach it to an existing service request.

Collecting Support Data

Collecting support data files involves logging in to the command line on components in your Private Cloud Appliance and copying files to a storage location external to the appliance environment, in the data center network. This can only be achieved from a system with access to both the internal appliance management network and the data center network. You can set up a physical or virtual system with those connections, or use the active management node.

The most convenient way to collect the necessary files, is to mount the target storage location on the system using `nfs`, and copy the files using `scp` with the appropriate login credentials and file path. The command syntax should be similar to the following example:

```
# mkdir /mnt/mynfsshare
# mount -t nfs storage-host-ip:/path-to-share /mnt/mynfsshare
# scp root@component-ip:/path-to-file /mnt/mynfsshare/pca-support-data/
```

Using `kdump`

Oracle Support Services often require a system memory dump. For this purpose, `kdump` must be installed and configured on the component under investigation. By default, `kdump` is installed on all Private Cloud Appliance compute nodes and configured to write the system memory dump to the ZFS Storage Appliance at this location: `192.168.4.100:/export/nfs_repository1/`.

For more information, see How to Configure 'kdump' for Oracle VM 3.4.x (Doc ID 2142488.1).

Using OSWatcher

Oracle Support Services often recommend that the OSWatcher tool be run for an extended period of time to diagnose issues. OSWatcher is installed by default on all Private Cloud Appliance compute nodes.

For more information, see Oracle Linux: How To Start OSWatcher Black Box (OSWBB) Every System Boot Using RPM oswbb-service (Doc ID 580513.1).

Using `pca-diag`

Oracle Support Services use the `pca-diag` tool. This tool is part of the Private Cloud Appliance controller software installed on both management nodes and on all compute nodes.

The `pca-diag` tool collects troubleshooting information from the Private Cloud Appliance environment. For more information, see Oracle Private Cloud Appliance Diagnostics Tool.

Oracle Support might request specific output from `pca-diag` to help diagnose and resolve hardware or software issues.

Use the following procedure to use `pca-diag` to collect support data from your system.

1. Log in to the active management node as root.
2. Run `pca-diag` with the appropriate command-line arguments.

   For the most complete set of diagnostic data, run the command with both the `ilom` and `vmpinfo` arguments.

   - `pca-diag ilom`

     Use the `pca-diag ilom` command to detect and diagnose potential component hardware and software problems.

     ```
     [root@ovcamn05r1 ~]# pca-diag ilom

     Oracle Private Cloud Appliance diagnostics tool

     Gathering Linux information...
     Gathering system messages...
     Gathering PCA related files...
     Gathering OS version information...
     Gathering host specific information...
     Gathering PCI information...
     Gathering SCSI and partition data...
     Gathering OS process data...
     Gathering network setup information...
     ```

```
Gathering installed packages data...
Gathering disk information...
Gathering ILOM Service Processor data... this may take a while
Generating diagnostics tarball and removing temp directory

================================================================================
Diagnostics completed. The collected data is available in:
/tmp/pcadiag_ovcamn05r1_<ID>_<date>_<time>.tar.bz2
================================================================================
```

- `pca-diag vmpinfo`

  Use the `pca-diag vmpinfo` command to detect and diagnose potential problems in the Oracle VM environment.

  > **Note:**
  >
  > To collect diagnostic information for a subset of Oracle VM servers in the environment, run the command with an additional `servers` parameter, as shown in the following example:

```
[root@ovcamn05r1 ~]# pca-diag vmpinfo servers='ovcacn07r1,ovcacn08r1'

Oracle Private Cloud Appliance diagnostics tool
Gathering Linux information...
Gathering system messages...
Gathering PCA related files...
Gathering OS version information...
Gathering host specific information...
Gathering PCI information...
Gathering SCSI and partition data...
Gathering OS process data...
Gathering network setup information...
Gathering installed packages data...
Gathering disk information...
Gathering FRU data and console history. Use ilom option for complete ILOM data.
```

  When the `vmpinfo3` script is called as a sub-process from `pca-diag`, the console output continues as follows:

```
Running vmpinfo tool...
Starting data collection
Gathering files from servers: ovcacn07r1,ovcacn08r1  This process may take
some time.
Gathering OVM Model Dump files
Gathering sosreports from servers
The following server(s) will get info collected: [ovcacn07r1,ovcacn08r1]
Gathering sosreport from ovcacn07r1
Gathering sosreport from ovcacn08r1
Data collection complete
Gathering OVM Manager Logs
Clean up metrics
Copying model files
Copying DB backup log files
Invoking manager sosreport
```

When all files have been collected, the data is compressed into two tarballs. One is from the `pca-diag` tool, while `vmpinfo3` writes a separate tarball with its own specific data.

```
Compressing VMPinfo3 date-time.
================================================================================
==============
Please send /tmp/vmpinfo3-version-date-time.tar.gz to Oracle OVM support
================================================================================
==============

Generating diagnostics tarball and removing temp directory
================================================================================
=====
Diagnostics completed. The collected data is available in:
/tmp/pcadiag_ovcamn05r1_ID_date_time.tar.bz2
================================================================================
=====
```

3. If necessary, run `pca-diag`, with or without the `ilom` argument, on some or all compute nodes as well.
4. To allow better analysis of physical server issues (for example hanging, crashing, or rebooting), also include the system memory dump file: `vmcore`. See the beginning of this section for a convenient way to collect the files.

   The location of the file is: ***kdump-partition-mount-point***`/kdump/`***compute-node-ip-date-time***`/vmcore`. The partition and mount point are defined during `kdump` configuration. By default, `kdump` writes to `192.168.4.100:/export/nfs_repository1/`.

   For more information, see How to Configure 'kdump' for Oracle VM 3.4.x (Doc ID 2142488.1).
5. When required, collect the OSWatcher logs from the compute nodes. The default location is `/var/log/oswatcher/archive/`.
6. Copy all diagnostic files to a location external to the appliance environment, as described at the beginning of this section.

Uploading Support Data Files

For support data files up to 2 GB, upload the file as part of the Service Request (SR) process in My Oracle Support.

- If you are still in the process of creating the SR, upload the support data in the Upload Files/Attachments step.
- To upload files after you have created the SR, use the following procedure:
  1. Log into My Oracle Support and open the Dashboard or the Service Request tab.
  2. In the Service Request region, click the SR you want to update.
  3. In the Update section, select Add Attachment.
  4. In the pop-up window, select the file for upload, include any notes, and click Attach File.

If uploading the support data with the SR is not an option, or for support data files larger than 2 GB, use the FTPS file upload service from Oracle Support at

`transport.oracle.com`, as described in the following procedure. Oracle Support might request that you upload using a different mechanism.

1. Using an FTPS client, for example FileZilla or WinSCP, access the My Oracle Support File Upload Service `transport.oracle.com` in *passive* mode.
2. Log in with your Oracle Single Sign-On user name and password.
3. Select the support data file to upload.
4. Select a destination for the file.

   Use the directory path provided by Oracle Support.

   Typically, the directory path is constructed as follows: `/upload/issue/`***`sr_number`***`/`.

   The use of an SR number ensures that the file is correctly associated with the service request. Record the full path to the file and the SR number for future reference in communications with Oracle Support.
5. Upload the file.

   When the upload is complete, a confirmation message is displayed.

If you prefer to use a command-line client such as cURL, you typically enter a single command to connect, authenticate, and complete the upload. A cURL command will look similar to the following example:

```
curl -T path_to_file -u "user" ftps://transport.oracle.com/upload/issue/sr_number
```

For security reasons, you should omit the password from the command and instead enter the password at the prompt.

For detailed information about uploading files to Oracle Support, see How to Upload Files to Oracle Support (Doc ID 1547088.2).

Cloud Backup

The Oracle Private Cloud Appliance Cloud Backup service automates the backup of critical components and configuration data to your customer tenancy in Oracle Cloud Infrastructure (OCI). This feature is designed to recover a Private Cloud Appliance to a running state after a catastrophic event. This feature is not designed to backup virtual machines, guest operating systems, or applications and data hosted on virtual machines. Backups of customer virtual machines and applications can be managed using Oracle Site Guard. See Oracle VM 3: Getting Started with Disaster Recovery using Oracle Site Guard (Doc ID 1959182.1).

The Cloud Backup service requires an Oracle Cloud Infrastructure cloud tenancy. The service is designed to create a snapshot of backup data from the system, store that snapshot on the internal ZFS Storage Appliance, then push that snapshot to your Oracle Cloud Infrastructure cloud tenancy for remote storage. Once configured, the service automatically runs a backup weekly. For resource management reasons, the 10 latest backups are stored locally on the Oracle Cloud Infrastructure and on your Oracle Cloud Infrastructure tenancy. At this time, contact Oracle Service to restore your Private Cloud Appliance from an Oracle Cloud Infrastructure cloud backup.

The Cloud Backup service uses the object storage feature of Oracle Cloud Infrastructure to store your Private Cloud Appliance configuration backup data. With Object Storage, you can safely and securely store or retrieve data directly from the internet or from within the cloud platform. Object Storage is a regional service and is not tied to any specific compute instance. You can access data from anywhere inside or outside the context of the Oracle

Cloud Infrastructure, as long you have internet connectivity and can access one of the Object Storage endpoints. For more information about Object Storage, see the Object Storage Overview.

To use the Cloud Backup service with Private Cloud Appliance releases earlier than 2.4.3, or systems that have been upgraded to release 2.4.3, contact Oracle Service.

For the best experience using the Cloud Backup service, consider these items.

- Use an Oracle Private Cloud Appliance region that is in the same region as your Private Cloud Appliance.
- Very slow network speeds in the customer premise network (less than 100 Mbps) may result in timeouts, especially when crossing regions.
- If you experience timeouts, contact Oracle Service.
- If the connection to the ZFS Storage Appliance is severed, for example when a management node is rebooted, this could corrupt the Cloud Backup service. See "Cloud Backup Task Hangs When a ZFSSA Takeover is Performed During Backup" in Known Limitations and Workarounds in the *Oracle Private Cloud Appliance Release Notes*.

Configuring the Cloud Backup Service

This section describes how to initially configure the Cloud Backup service, including how to prepare your Oracle Cloud Infrastructure tenancy to receive backups from the Oracle Private Cloud Appliance.

Configuring the Cloud Backup service does three things: creates a location to store your backups on your Oracle Cloud Infrastructure tenancy, activates the script which gathers backup data from the Private Cloud Appliance, and finally pushes those backups from your Private Cloud Appliance to your Oracle Cloud Infrastructure tenancy on a weekly basis.

Configuring the Cloud Backup Service for Oracle Private Cloud Appliance

1. Create an object storage bucket on your Oracle Cloud Infrastructure tenancy. See "Creating a Bucket" in Putting Data into Object Storage.

   > **Note:**
   >
   > To locate the OCID for a bucket, see Managing Buckets.

   Each target must be associated with its own bucket. Perform this operation to set up each target location for your Private Cloud Appliance backups.

2. Set up the Oracle Private Cloud Appliance Cloud Backup configuration.

   a. Using SSH and an account with superuser privileges, log into the active management node.

   ```
   # ssh root@10.100.1.101
   root@10.100.1.101's password:
   root@ovcamn05r1 ~]#
   ```

   b. Launch the Private Cloud Appliance command line interface.

```
# pca-admin
Welcome to PCA! Release: 2.4.4
PCA>
```

c. Create an Oracle Cloud Infrastructure target on your Private Cloud Appliance that corresponds with the Oracle Cloud Infrastructure object store bucket created in step 1.

This step creates a target on your Private Cloud Appliance ZFS Storage Appliance that sends scheduled backups to an object storage bucket on Oracle Cloud Infrastructure. For more information see create oci-target.

```
PCA> create oci-target target_name target_location target_user
     target_bucket target_tenancy keyfile
```

For example:

```
PCA> create oci-target cloud_target_1 https://objectstorage.us-oci.com
ocid1.user.oc1..oos-test
     mybucket ocid1.tenancy.oc1..nobody /root/oci_api_key.pem

Status: Success
```

The cloud backup is now configured to run weekly.

Configuring a Manual Cloud Backup

This section describes how to trigger a manual cloud backup, which can be useful in preparation for a system upgrade.

Creating a Manual Cloud Backup

1. Using SSH and an account with superuser privileges, log into the active management node.

```
# ssh root@10.100.1.101
root@10.100.1.101's password:
root@ovcamn05r1 ~]#
```

2. Launch the Private Cloud Appliancecommand line interface.

```
# pca-admin
Welcome to PCA! Release: 2.4.4
PCA>
```

3. Create the Cloud Backup.

```
PCA> create oci-backup oci-target-name1 oci-target-name2

The create oci-backup job has been submitted. Use "show task < task id>" to
monitor the progress.

Task_ID         Status  Progress Start_Time           Task_Name

-------         ------  -------- ----------           ---------

386c911399b38e  RUNNING None     05-29-2020 21:48:24  oci_backup

---------------

1 row displayed
```

```
Status: Success
```

Only one backup can run at a time. If there is a conflict, you see this error:

```
Status: Failure

Error Message: Error (SYSTEM_002): Cannot invoke API function oci_backup
while lock oci_backup is in place.
```

To resolve this issue, run your manual backup again, once the other backup task is complete.

Deleting Cloud Backups

This section describes how to delete a Cloud Backup, which removes the backup from both the Private Cloud Appliance and your Oracle Cloud Infrastructure tenancy.

Deleting a Cloud Backup

1. Using SSH and an account with superuser privileges, log into the active management node.

   ```
   # ssh root@10.100.1.101
   root@10.100.1.101's password:
   root@ovcamn05r1 ~]#
   ```

2. Launch the Private Cloud Appliance command line interface.

   ```
   # pca-admin
   Welcome to PCA! Release: 2.4.4
   PCA>
   ```

3. Delete the backup.

   ```
   PCA> delete oci-backup <OVCA/
   OCI_backups@AK00000000_OCI_snap_2020_06_29-04.56.28
   >

   WARNING !!! THIS IS A DESTRUCTIVE OPERATION.

   Are you sure [y/N]:y
   ```

Deleting Oracle Cloud Infrastructure Targets

This section describes how to remove an Oracle Cloud Infrastructure target from your Private Cloud Appliance. The related object storage buckets in your Oracle Cloud Infrastructure tenancy are not removed. This operation removes only the selected target on your Private Cloud Appliance, thus breaking the link to that target in your Oracle Cloud Infrastructure tenancy.

Deleting a Target

1. Using SSH and an account with superuser privileges, log into the active management node.

   ```
   # ssh root@10.100.1.101
   root@10.100.1.101's password:
   root@ovcamn05r1 ~]#
   ```

2. Launch the Private Cloud Appliance command line interface.

```
# pca-admin
Welcome to PCA! Release: 2.4.4
PCA>
```

3. Delete the Oracle Cloud Infrastructure target on your Private Cloud Appliance.

```
PCA> delete oci-target <target>
```

3
Upgrading Oracle Private Cloud Appliance

Due to the nature of the Private Cloud Appliance – where the term *appliance* is key – an upgrade is a delicate and complicated procedure that deals with different hardware and software components at the same time. It would be undesirable to take the appliance and the virtual environment it hosts out of service entirely for upgrading. Instead, upgrades can be executed in phases and scheduled for minimal downtime. The following table describes the sequence to perform Private Cloud Appliance upgrades.

For additional information about using the Upgrader Tool with software release 2.4.4, see support note Upgrader Tool - Prechecks and Postchecks (Doc ID 2785963.1).

Table 3-1 Sequential Break-Down of an Appliance Upgrade

Order	Component	Description
1.	storage network upgrade	You must perform this upgrade before you move to controller software version 2.4.4. You can skip this step if you have already performed this upgrade on your 2.4.3 system, or if your system was shipped from the factory with 2.4.3 software pre-installed. See Upgrading the Storage Network.
2.	management nodes software	Install upgraded management software on both management nodes (`mn05` and `mn06`). See Upgrading the Management Node Controller Software.
3.	all firmware, in this order 1. management node firmware 2. compute node firmware 3. internal ZFS storage firmware 4. switch firmware • Firmware for Cisco leaf, spine, and management switches • EPLD image for Cisco leaf, spine, and management switches	See Upgrading Component Firmware.
4.	compute node software upgrades	See Upgrading the Compute Node Software.

Before You Start Upgrading

Read and observe the critical information in this section before you begin any procedure to upgrade your Private Cloud Appliance.

All the software included in a given release of the Private Cloud Appliance software is tested to work together and should be treated as one package. Consequently, no appliance

component should be upgraded individually, unless Oracle provides specific instructions to do so. All Private Cloud Appliance software releases are downloaded as a single large `.iso` file, which includes the items listed above.

Do not install any additional packages on your system besides those included in the Private Cloud Appliance `.iso` file, or packages recommended by your Oracle representative.

> **Note:**
>
> The appliance upgrade process must **always** be initiated from the **active management node**.

To view supported firmware versions for all releases of Private Cloud Appliance, see support note Firmware Policy for Private Cloud Appliance (PCA) (Doc ID 1610373.1).

Warnings and Cautions

Read and understand these warnings and cautions before you start the appliance update procedure. They help you avoid operational issues including data loss and significant downtime.

NOT_SUPPORTED:

Minimum Release

In this version of the *Oracle Private Cloud Appliance Administration Guide*, it is assumed that your system is currently **running Controller Software release 2.4.3 prior to this software update**.

If your system is currently running an earlier version, refer to the Updating Oracle Private Cloud Appliance chapter of the *Oracle Private Cloud Appliance Administrator's Guide for Release 2.4.3*. Follow the appropriate procedures and make sure that your appliance configuration is valid for the release 2.4.3 update before you continue.

NOT_SUPPORTED:

No Critical Operations

When updating the Private Cloud Appliance software, make sure that no provisioning operations occur and that any externally scheduled backups are suspended. Such operations could cause a software update or component firmware upgrade to fail and lead to system downtime.

NOT_SUPPORTED:

YUM Disabled

On Private Cloud Appliance management nodes, the YUM repositories have been intentionally disabled and should not be enabled by the customer. Updates and upgrades of the management node operating system and software components must be applied only through the update mechanism described in the documentation.

Caution:

Firmware Policy

To ensure that your Private Cloud Appliance configuration remains in a qualified state, take the required firmware upgrades into account when planning the controller software update. For more information, refer to Firmware Policy.

Caution:

No Backup

During controller software updates, backup operations must be prevented. The Oracle Private Cloud Appliance Upgrader disables `crond` and blocks backups.

Caution:

CA Certificate and Keystore

If you have generated custom keys using `ovmkeytool.sh` in a previous version of the Private Cloud Appliance software, you must regenerate the keys prior to updating the Controller Software. For instructions, refer to the support note PCA 2.3.x/2.4.x Upgrade not allowed if Certificates have been regenerated using ovmkeytool.sh. (Doc ID 2597439.1). See also Creating a Keystore.

Caution:

Proxy Settings

If direct public access is not available within your data center and you make use of proxy servers to facilitate HTTP, HTTPS and FTP traffic, it may be necessary to edit the Private Cloud Appliance system properties, using the CLI on each management node, to ensure that the correct proxy settings are specified for a download to succeed from the Internet. This depends on the network location from where the download is served. See Adding Proxy Settings for Oracle Private Cloud Appliance Updates for more information.

Caution:

Custom LUNs on Internal Storage

If the internal ZFS Storage Appliance contains customer-created LUNs, make sure they are not mapped to the default initiator group.

See "Customer Created LUNs Are Mapped to the Wrong Initiator Group" in Known Limitations and Workarounds in the *Oracle Private Cloud Appliance Release Notes*.

Caution:

Oracle VM Availability During Update to Release 2.4.x

When updating the Oracle Private Cloud Appliance Controller Software to Release 2.4.x, Oracle VM Manager is unavailable for the entire duration of the update. The virtualized environment remains functional, but configuration changes and other management operations are not possible.

NOT_SUPPORTED:

Compute Node Upgrade ONLY Through Oracle Private Cloud Appliance

Compute nodes cannot be upgraded to the appropriate Oracle VM Server Release 3.4.x with the Oracle VM Manager web UI. You must upgrade them using the `pca_upgrader` tool within the Private Cloud Appliance.

To perform this upgrade procedure, follow the specific instructions in Upgrading the Compute Node Software.

NOT_SUPPORTED:

Do Not Override Oracle VM Global Update Settings

As stated in Guidelines, at the start of Managing the Oracle VM Virtual Infrastructure, the settings of the default server pool and custom tenant groups must not be modified through Oracle VM Manager. For compute node upgrade specifically, it is critical that the server pool option "Override Global Server Update Group" remains deselected. The compute node update process must use the repository defined globally. Overriding this will cause the update to fail.

Caution:

Post-Update Synchronization

Once you have confirmed that the update process has completed, it is advised that you wait a further 30 minutes before starting another compute node or management node software update. This allows the necessary synchronization tasks to complete.

If you ignore the recommended delay between these update procedures, there could be issues with further updating as a result of interference between existing and new tasks.

Backup Local Customizations

An update of the Private Cloud Appliance software stack may involve a complete re-imaging of the management nodes. Any customer-installed **agents** or **customizations** are overwritten in the process. Before applying new appliance software, back up all local customizations and prepare to re-apply them after the update has completed successfully.

Oracle Enterprise Manager Plug-in Users

If you use Oracle Enterprise Manager and the Oracle Enterprise Manager Plug-in to monitor your Private Cloud Appliance environment, always back up the *oraInventory* Agent data to `/nfs/shared_storage` before updating the controller software.

For detailed instructions, refer to Enterprise Manager Agent Recovery After Oracle PCA Upgrade in Oracle Enterprise Manager: Monitoring an Oracle Private Cloud Appliance.

Oracle Auto Service Request (ASR) Users

If you use Oracle Auto Service Request (ASR) in the Private Cloud Appliance environment, backup your ASR configuration according to ASR Backup and Restore in Oracle Auto Service Request: ASR Manager User's Guide for Linux and Solaris.

You can restore the data after the Private Cloud Appliance software update is complete.

Determine Firmware Versions

Use the following commands to determine the current version of firmware installed on a component.

1. Using an account with superuser privileges, log in to the component.

   For Cisco switches you must log in as `admin`.

2. Use the appropriate command to find the current firmware version of each component.

   - compute/management nodes

     ```
     > fwupdate list all
     ```

     To find the CX5 card firmware version, query the PCI bus:

     ```
     [root@ovcamn05r1 ~]# lspci | grep Mell
     3b:00.0 Ethernet controller: Mellanox Technologies MT28800 Family
     [ConnectX-5 Ex]
     3b:00.1 Ethernet controller: Mellanox Technologies MT28800 Family
     [ConnectX-5 Ex]
     ```

     Use the `mstflint` command on the appropriate PCI bus to determine the card firmware version:

     ```
     [root@ovcamn05r1 ~]# mstflint -d /proc/bus/pci/3b/00.0 q
     Image type: FS4
     FW Version: 16.28.1002
     FW Release Date: 23.7.2020
     Product Version: 16.28.1002
     ```

   - ZFS Storage Appliances

     ```
     ovcasn02r1:> configuration version show
     ```

   - Cisco switches

     ```
     ovcasw21r1# show version
     ```

Upgrading the Storage Network

The Oracle Private Cloud Appliance Storage Network is available since Controller Software release 2.4.3. This feature enables access for virtual machines to the internal ZFS Storage Appliance, and requires 60TB of space on the ZFS Storage Appliance.

Functionality is built in to the storage network upgrade to ensure the upgrade process works properly. This includes three lock files that are set during the storage network upgrade and are designed to prevent specific behaviors that can interrupt the upgrade. The `all_provisioning.LOCK` prevents provisioning actions on compute nodes during upgrade. The `fw_upgrade.LOCK` is placed immediately following the successful completion of the first management node upgrade, and prevents the use of CLI commands before the storage network upgrade is complete. The `storage_network_upgrade.LOCK` prevents any customer-initiated changes to the spine or leaf switches while the upgrade is taking place. The locks are removed at the completion of the storage network upgrade, regardless of success or failure.

> **Caution:**
>
> This is a disruptive upgrade during which the Cisco spine switches are reconfigured and the network interfaces on the ZFS Storage Appliance will be reconfigured.

Performing Pre-checks and Upgrading the Oracle Private Cloud Appliance Storage Network

1. Log in to the management node and run the `verify` command.

   ```
   pca_upgrader -V -t storage-network
   ```

2. If you use the optional ASRM and OEM agents, stop them.

   ```
   service asrm stop
   service gcstartup stop
   ```

3. Upgrade the storage network.

   ```
   pca_upgrader -U -t storage-network
   PCA Rack Type: PCA X8_BASE.
     Please refer to log file /var/log/pca_upgrader_<date>-<time>.log for more
   details.

   Beginning PCA Storage Network Pre-Upgrade Checks...

   Rack Type Check                                                    1/14
   PCA Version Check                                                  2/14
   Upgrade Locks Check                                                3/14
   Backup Tasks Check                                                 4/14
   Storage Port Channel Status Check                                  5/14
   Spine Switch Firmware Check                                        6/14
   Check ZFSSA MGMT Network                                           7/14
   Check Cluster Status                                               8/14
   AK Firmware Version Check                                          9/14
   ZFSSA Resilvering Jobs Check                                      10/14
   iSCSI Target Check                                                11/14
   ZFSSA Hardware Error Check                                        12/14
   Check ZFSSA Default Shares                                        13/14
   ZFSSA Network Configuration Check                                 14/14

   PCA Storage Network Pre-Upgrade Checks completed after 0 minutes

   Beginning PCA Storage Network Upgrade
   Disable PCA Backups                                                1/6
   Take Spine Switch Backup                                           2/6
   Take ZFSSA Configuration Backup                                    3/6
   Place Storage Network Upgrade Locks                                4/6
   Perform Storage Network Upgrade                                    5/6
   Remove Firmware Upgrade Lock                                       6/6
   Remove PCA Upgrade Locks                                             1
   Re-enable PCA Backups                                                2
   PCA Storage Network Upgrade completed after 6 minutes

   Beginning PCA Storage Network Post-Upgrade Checks...

   PCA Storage Network Post-Upgrade Checks completed after 0 minutes

   --------------------------------------------------------------------------------
   ```

```
PCA Storage Network Pre-Upgrade Checks                                  Passed
--------------------------------------------------------------------------------
Rack Type Check                                                         Passed
PCA Version Check                                                       Passed
Upgrade Locks Check                                                     Passed
Backup Tasks Check                                                      Passed
Storage Port Channel Status Check                                       Passed
Spine Switch Firmware Check                                             Passed
Check ZFSSA MGMT Network                                                Passed
Check Cluster Status                                                    Passed
AK Firmware Version Check                                               Passed
ZFSSA Resilvering Jobs Check                                            Passed
iSCSI Target Check                                                      Passed
ZFSSA Hardware Error Check                                              Passed
Check ZFSSA Default Shares                                              Passed
ZFSSA Network Configuration Check                                       Passed
--------------------------------------------------------------------------------
PCA Storage Network Upgrade                                             Passed
--------------------------------------------------------------------------------
Disable PCA Backups                                                     Passed
Take Spine Switch Backup                                                Passed
Take ZFSSA Configuration Backup                                         Passed
Place Storage Network Upgrade Locks                                     Passed
Perform Storage Network Upgrade                                         Passed
Remove Firmware Upgrade Lock                                            Passed
--------------------------------------------------------------------------------
PCA Storage Network Post-Upgrade Checks                                 Passed
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Overall Status                                                          Passed
--------------------------------------------------------------------------------
PCA Storage Network Pre-Upgrade Checks                                  Passed
PCA Storage Network Upgrade                                             Passed
PCA Storage Network Post-Upgrade Checks                                 Passed
  Please refer to log file /var/log/pca_upgrader_<date>-<time>.log for more
details.
```

> **Note:**
>
> After the successful upgrade of management nodes, an upgrade lock *is left in place*. This lock is intentional to ensure that the storage network upgrade is performed before attempting to upgrade the compute nodes.

4. If you use the optional the ASRM and OEM agents, restart them.

```
service asrm start
service gcstartup start
```

Upgrading the Management Node Controller Software

NOT_SUPPORTED:

UPGRADE BOTH MANAGEMENT NODES CONSECUTIVELY

With the Oracle Private Cloud Appliance Upgrader, the two management node upgrade processes are theoretically separated. Each management node upgrade is initiated by a single command and managed through the Upgrader, which invokes the native Oracle VM Manager upgrade mechanisms. However, you must **treat the upgrade of the two management nodes as a single operation**.

During the management node upgrade, the high-availability (HA) configuration of the management node cluster is temporarily broken. To restore HA management functionality and mitigate the risk of data corruption, it is critical that you **start the upgrade of the second management node immediately after a successful upgrade of the first management node**.

NOT_SUPPORTED:

NO MANAGEMENT OPERATIONS DURING UPGRADE

The Oracle Private Cloud Appliance Upgrader manages the entire process to upgrade both management nodes in the appliance. Under no circumstances should you perform any management operations – through the Oracle Private Cloud Appliance Dashboard or CLI, or Oracle VM Manager – while the Upgrader process is running, and until **both management nodes** have been successfully upgraded through the Upgrader. Although certain management functions cannot be programmatically locked during the upgrade, they are not supported, and are likely to cause configuration inconsistencies and considerable repair downtime.

Once the upgrade has been successfully completed on **both management nodes**, you can safely execute appliance management tasks and configuration of the virtualized environment.

As of Release 2.3.4, a separate command line tool is provided to manage the Controller Software upgrade process. The Oracle Private Cloud Appliance Upgrader requires only a couple of commands to execute several sets of tasks, which were scripted or manual steps in previous releases. The Upgrader is more robust and easily extensible, and provides a much better overall upgrade experience.

A more detailed description of the Oracle Private Cloud Appliance Upgrader is included in the introductory chapter of this book. Refer to Oracle Private Cloud Appliance Upgrader.

Rebooting the Management Node Cluster

It is advised to reboot both management nodes before starting the appliance software upgrade. This leaves the management node cluster in the cleanest possible state, ensures

that no system resources are occupied unnecessarily, and eliminates potential interference from processes that have not completed properly.

Rebooting the Management Node Cluster

1. Using SSH and an account with superuser privileges, log into both management nodes using the IP addresses you configured in the Network Setup tab of the Oracle Private Cloud Appliance Dashboard. If you use two separate consoles you can view both side by side.
2. Run the command `pca-check-master` on both management nodes to verify which node owns the active role.
3. Reboot the management node that is **NOT** currently the active node. Enter `init 6` at the prompt.
4. Ping the machine you rebooted. When it comes back online, reconnect using SSH and monitor system activity to determine when the secondary management node takes over the active role. Enter this command at the prompt: `tail -f /var/log/messages`. New system activity notifications will be output to the screen as they are logged.
5. In the other SSH console, which is connected to the current active management node, enter `init 6` to reboot the machine and initiate management node failover.

   The log messages in the other SSH console should now indicate when the secondary management node takes over the active role.
6. Verify that both management nodes have come back online after reboot and that the active role has been transferred to the other manager. Run the command `pca-check-master` on both management nodes.

   If this is the case, proceed with the software upgrade steps below.

Installing the Oracle Private Cloud Appliance Upgrader

Always download and install the latest version of the Oracle Private Cloud Appliance Upgrader before you execute any verification or upgrade procedures.

Downloading and Installing the Latest Version of the Oracle Private Cloud Appliance Upgrader

1. Confirm which version of the Oracle Private Cloud Appliance Upgrader is already on your system.

   ```
   [root@ovcamn05r1 ~]# yum search pca_upgrader
   pca_upgrader-version.el6.noarch
   ```
2. Log into My Oracle Support and download the latest version of the Oracle Private Cloud Appliance Upgrader to a secure location, if it is newer than the version on your system.

   The Upgrader can be found under patch ID 32982108, and is included in part 1 of a series of downloadable zip files. Any updated versions of the Upgrader will be made available in the same location.

   To obtain the Upgrader package, download this zip file and extract the file `pca_upgrader-version.el6.noarch.rpm`.

   Once you have downloaded and extracted the series of Upgrader zip files, execute the `RUN_ME_FIRST.sh` script to assemble the ISO image from the zip files.

3. If you downloaded a newer version of the Oracle Private Cloud Appliance Upgrader, you must upgrade to the newer version. From the directory where the `*.rpm` package was saved, run the command `yum update pca_upgrader-`***`version`***`.el6.noarch.rpm`.

   Verify the new version was installed using the `yum search pca_upgrader` command.

4. Copy the downloaded `*.rpm` package to the active management node and install it.

   > **Note:**
   >
   > Install the `pca_upgrader` version that matches the Oracle release that is currently running on the management node. For example, if you are upgrading the first management node to version 2.4.4, the current management node is running `pca_upgrader-`***`version`***`.el6.noarch.rpm`, so you must use the `.el6` version for upgrade. If you are upgrading the second management node, the first management node *has been upgraded* to version `pca_upgrader-`***`version`***`.el7.noarch.rpm`, so you must use the `.el7` version for this upgrade.

```
[root@ovcamn05r1 ~]# pca-check-master
NODE: 192.168.4.3  MASTER: True
root@ovcamn05r1 tmp]# yum install pca_upgrader-2.0.el7.noarch.rpm
Preparing..########################################### [100]
1:pca_upgrader############################################ [100%]
```

   > **Caution:**
   >
   > Always download and use the latest available version of the Oracle Private Cloud Appliance Upgrader.

5. Install the `*.rpm` upgrade on the second management node.

Verifying Upgrade Readiness

The Oracle Private Cloud Appliance Upgrader has a verify-only mode. It allows you to run all the pre-checks defined for a management node upgrade without proceeding to the actual upgrade steps. The terminal output and log file report any issues you need to fix before the system is eligible for the next Controller Software upgrade.

> **Note:**
>
> The Oracle Private Cloud Appliance Upgrader cannot be stopped by means of a keyboard interrupt or by closing the terminal session. After a keyboard interrupt (`Ctrl+C`) the Upgrader continues to execute all pre-checks. If the terminal session is closed, the Upgrader continues as a background process.
>
> If the Upgrader process needs to be terminated, enter the command `pca_upgrader --kill`.

Verifying the Upgrade Readiness of the Oracle Private Cloud Appliance

1. Go to Oracle VM Manager and make sure that all compute nodes are in *Running* status. If any server is not in Running status, resolve the issue before proceeding.

   For help resolving issues to correct the compute node status, refer to the support note OVM 3.4.1: OVM Manager showing the Oracle VM Server status as "Starting" although it is running (Doc ID 2245197.1) or contact Oracle Support.

2. Perform the required manual pre-upgrade checks. Refer to Running Manual Pre- and Post-Upgrade Checks in Combination with Oracle Private Cloud Appliance Upgrader for instructions.

3. Log in to My Oracle Support and download the required Private Cloud Appliance software update.

   You can find the update by searching for the product name "Oracle Private Cloud Appliance", or for the Patch or Bug Number associated with the update you need.

   > **Caution:**
   >
   > Read the information and follow the instructions in the `readme` file very carefully. It is crucial for a successful Oracle Private Cloud Appliance Controller Software upgrade and Oracle VM upgrade.

4. Make the update, a zipped ISO, available on an HTTP or FTP server that is reachable from your Private Cloud Appliance. Alternatively, if upgrade time is a major concern, you can download the ISO file to the local file system on both management nodes. This reduces the upgrade time for the management nodes, but has no effect on the time required to upgrade the compute nodes or the Oracle VM database.

   The Oracle Private Cloud Appliance Upgrader downloads the ISO from the specified location and unpacks it on the management node automatically at runtime.

5. Using SSH and an account with superuser privileges, log in to the **active** management node through its individually assigned IP address, **not** the shared virtual IP.

   > **Note:**
   >
   > During the upgrade process, the interface with the shared virtual IP address is shut down. Therefore, you must log in using the individually assigned IP address of the management node.

6. From the active management node, run the Oracle Private Cloud Appliance Upgrader in verify-only mode. The target of the command must be the *stand-by* management node.

> **Note:**
>
> The console output below is an example. You may see a different output, depending on the specific architecture and configuration of your appliance.

```
[root@ovcamn05r1 ~]# pca-check-master
NODE: 192.168.4.3  MASTER: True

root@ovcamn05r1 ~]# pca_upgrader -V -t management -c ovcamn06r1 -g 2.4.4 \
-l http://path-to-iso/ovca-2.4.4-b000.iso.zip

PCA Rack Type: PCA X8_BASE.

Please refer to log file
/nfs/shared_storage/pca_upgrader/log/pca_upgrader_date-time.log
for more details.

Beginning PCA Management Node Pre-Upgrade Checks...

Validate the Image Provided                                          1/44
Internal ZFSSA Available Space Check                                 2/44
MN Disk and Shared Storage Space Check                               3/44
[...]
Oracle VM Minimum Version Check                                     41/44
OS Check                                                            42/44
OSA Disabled Check                                                  43/44
ZFSSA Network Configuration Check                                   44/44

PCA Management Node Pre-Upgrade Checks completed after 0 minutes

--------------------------------------------------------------------------------
PCA Management Node Pre-Upgrade Checks                              Passed
--------------------------------------------------------------------------------
Validate the Image Provided                                         Passed
Internal ZFSSA Available Space Check                                Passed
[...]
OS Check                                                            Passed
Password Check                                                      Passed
OSA Disabled Check                                                  Passed
--------------------------------------------------------------------------------
Overall Status                                                      Passed
--------------------------------------------------------------------------------
```

7. As the verification process runs, check the console output for test progress. When all pre-checks have been completed, a summary is displayed. A complete overview of the verification process is saved in the file `/nfs/shared_storage/pca_upgrader/log/pca_upgrader_date-time.log`.

   Some pre-checks may result in a warning. These warnings are unlikely to cause issues, and therefore do not prevent you from executing the upgrade, but they do indicate a situation that should be investigated. When an upgrade command is issued, warnings cause the administrator to be prompted whether to proceed with the upgrade, or quit and investigate the warnings first.

8. If pre-checks have failed, consult the log file for details. Fix the reported problems, then execute the verify command again.

> **Note:**
>
> If errors related to SSL certificates are reported, check whether these have been re-generated using `ovmkeytool.sh`. This can cause inconsistencies between the information stored in the Wallet and the actual location of your certificate. For detailed information and instructions to resolve the issue, refer to the support note Upgrade not allowed if Certificates have been regenerated using ovmkeytool.sh. (Doc ID 2597439.1).

9. Repeat this process until no more pre-check failures are reported. When the system passes all pre-checks, it is ready for the Controller Software upgrade.

Executing a Controller Software Upgrade

During a Controller Software upgrade, the virtualized environment does not accept any management operations. Ensure the storage network upgrade has been completed, then upgrade the management node cluster, followed by the firmware upgrade on rack components, and finally, upgrade the compute nodes in phases. When you have planned all these upgrade tasks, and when you have successfully completed the upgrade readiness verification, your environment is ready for a Controller Software upgrade and any additional upgrades.

No upgrade procedure can be executed without completing the pre-checks. Therefore, the upgrade command first executes the same steps as in Verifying Upgrade Readiness. After successful verification, the upgrade steps are started.

> **Note:**
>
> The console output shown throughout this section is an example. You may see different output, depending on the specific architecture and configuration of your appliance.

> **Note:**
>
> The Oracle Private Cloud Appliance Upgrader cannot be stopped by means of a keyboard interrupt or by closing the terminal session.
>
> After a keyboard interrupt (`Ctrl+C`) the Upgrader continues the current phase of the process. If pre-checks are in progress, they are all completed, but the upgrade phase does not start automatically after successful completion of all pre-checks. If the upgrade phase is in progress at the time of the keyboard interrupt, it continues until upgrade either completes successfully or fails.
>
> If the terminal session is closed, the Upgrader continues as a background process.
>
> If the Upgrader process needs to be terminated, enter this command: `pca_upgrader --kill`.

Upgrading the Oracle Private Cloud Appliance Controller Software

1. Using SSH and an account with superuser privileges, log in to the **active** management node through its individually assigned IP address, **not** the shared virtual IP.

   > **Note:**
   >
   > During the upgrade process, the interface with the shared virtual IP address is shut down. Therefore, you must log in using the individually assigned IP address of the management node.

   > **NOT_SUPPORTED:**
   >
   > NO MANAGEMENT OPERATIONS DURING UPGRADE
   >
   > Under no circumstances should you perform any management operations – through the Oracle Private Cloud Appliance Dashboard or CLI, or Oracle VM Manager – while the Upgrader process is running, and until **both management nodes** have been successfully upgraded through the Upgrader.

2. From the active management node, run the Oracle Private Cloud Appliance Upgrader with the required upgrade parameters. The target of the command must be the *stand-by* management node.

```
[root@ovcamn05r1 ~]# pca-check-master
NODE: 192.168.4.3  MASTER: True

root@ovcamn05r1 ~]# pca_upgrader -U -t management -c ovcamn06r1 -g 2.4.4 \
-l http://path-to-iso/ovca-2.4.4-b301.iso.zip

PCA Rack Type: PCA X8_BASE.

Please refer to log file
/nfs/shared_storage/pca_upgrader/log/pca_upgrader_date-time.log
for more details.

Beginning PCA Management Node Pre-Upgrade Checks...
[...]

**********************************************************************
Warning: The management precheck completed with warnings.
It is safe to continue with the management upgrade from this point
or the upgrade can be halted to investigate the warnings.
**********************************************************************
Do you want to continue? [y/n]: y
```

   After successfully completing the pre-checks, the Upgrader initiates the Controller Software upgrade on the other management node. If errors occur during the upgrade phase, tasks are rolled back and the system is returned to its original state from before the upgrade command.

   Rollback works for errors that occur during these steps:

Table 3-2 Steps That Support Upgrader Rollback

Upgrading From Release 2.4.3	Upgrading From Release 2.4.4
• setting up the PXE directories • disabling the Oracle Private Cloud Appliance backups • downloading the ISO • generating PXE and Kickstart files • taking an Oracle VM backup • breaking the Oracle Private Cloud Appliance HA model	• downloading the ISO • setting up the YUM repository • taking an Oracle VM backup • breaking the Oracle Private Cloud Appliance HA model

```
Beginning PCA Management Node upgrade for ovcamn06r1
Setup PXE Directories                                                    1/19
Disable PCA Backups                                                      2/19
Download ISO                                                             3/19
Generate PXE and Kickstart Files                                         4/19
Take OVM Backup                                                          5/19
...

PCA Management Node upgrade of ovcamn06r1 completed after 83 minutes

Beginning PCA Post-Upgrade Checks...
OVM Manager Cache Size Check                                              1/1
PCA Post-Upgrade Checks completed after 1 minutes

--------------------------------------------------------------------------------
PCA Management Node Pre-Upgrade Checks                                   Passed
--------------------------------------------------------------------------------
Validate the Image Provided                                              Passed
Rack Type Check                                                          Passed
Internal ZFS 2T Space Check                                              Passed
[...]

--------------------------------------------------------------------------------
PCA Management Node Upgrade                                              Passed
--------------------------------------------------------------------------------
Setup PXE Directories                                                    Passed
[...]
Restore PCA Backups                                                      Passed
Upgrade is complete                                                      Passed
[...]
--------------------------------------------------------------------------------
PCA Post-Upgrade Checks                                                  Passed
--------------------------------------------------------------------------------
OVM Manager Cache Size Check                                             Passed
--------------------------------------------------------------------------------
Overall Status                                                           Passed
--------------------------------------------------------------------------------
PCA Management Node Pre-Upgrade Checks                                   Passed
PCA Management Node Upgrade                                              Passed
PCA Post-Upgrade Checks                                                  Passed
```

> **Tip:**
>
> When the ISO is copied to the local file system of both management nodes, the management node upgrade time is shortened. The duration of the entire upgrade process depends heavily on the size of the environment: the number of compute nodes and their configuration, the size of the Oracle VM database, etc, and can take from 1.5 to several hours.
>
> If you choose to copy the ISO locally, replace the location URL in the `pca_upgrader` command with `-l file:///`***`path-to-iso`***`/ovca-2.4.4-b301.iso.zip`.

3. Monitor the progress of the upgrade tasks. The console output provides a summary of each executed task. If you need more details on a task, or if an error occurs, consult the log file. You can track the logging activity in a separate console window by entering the command `tail -f /nfs/shared_storage/pca_upgrader/log/pca_upgrader_`***`date-time`***`.log`.

> **Note:**
>
> Once the upgrade tasks have started, it is no longer possible to perform a rollback to the previous state.

```
# tail -f /nfs/shared_storage/pca_upgrader/log/pca_upgrader_date-time.log
```

When the upgrade tasks have been completed successfully, the active management node is rebooted, and the upgraded management node assumes the active role. The new active management node's operating system is now up-to-date, and it runs the new Controller Software version and upgraded Oracle VM Manager installation.

> **Tip:**
>
> Rebooting the management node is expected to take up to 10 minutes.
>
> To monitor the reboot process and make sure the node comes back online as expected, log in to the rebooting management node ILOM.

```
Broadcast message from root@ovcamn05r1 (pts/0) (Fri May  7 00:23:25 2021):
Management Node upgrade succeeded. The master manager will be rebooted to initiate
failover in one minute.
```

> **Caution:**
>
> Do not remove any files created during the upgrade process until completion of the second management node upgrade.

4. Log into the upgraded management node, which has now become the **active** management node. Use its individually assigned IP address, **not** the shared virtual IP.

```
[root@ovcamn06r1 ~]# pca-check-master
NODE: 192.168.4.3  MASTER: True

[root@ovcamn06r1 ~]# head /etc/ovca-info
==== Begin build info ====
date: 2019-09-30
release: 2.4.4
build: 301
=== Begin compute node info ===
compute_ovm_server_version: 3.4.7
compute_ovm_server_build: 2.4.4-150
compute_rpms_added:
  osc-oracle-s7k-2.1.2-4.el7.noarch.rpm
  ovca-support-2.4.4-97.el7.noarch.rpm
```

> **NOT_SUPPORTED:**
>
> NO MANAGEMENT OPERATIONS DURING UPGRADE
>
> Under no circumstances should you perform any management operations – through the Oracle Private Cloud Appliance Dashboard or CLI, or Oracle VM Manager – while the Upgrader process is running, and until **both management nodes** have been successfully upgraded through the Upgrader.

5. From the new active management node, run the Oracle Private Cloud Appliance Upgrader command again. The target of the command must be the *stand-by* management node, which is the original active management node from where you executed the command for the first run.

```
root@ovcamn06r1 ~]# pca_upgrader -U -t management -c ovcamn05r1 -g 2.4.4 \
-l http://path-to-iso/ovca-2.4.4-b301.iso.zip

PCA Rack Type: PCA X8_BASE.

Please refer to log file
/nfs/shared_storage/pca_upgrader/log/pca_upgrader_date-time.log
for more details.

Beginning PCA Management Node Pre-Upgrade Checks...
[...]

**********************************************************************
Warning: The management precheck completed with warnings.
It is safe to continue with the management upgrade from this point
or the upgrade can be halted to investigate the warnings.
**********************************************************************
Do you want to continue? [y/n]: y

Beginning PCA Management Node upgrade for ovcamn05r1
[...]

--------------------------------------------------------------------------
Overall Status                                                      Passed
--------------------------------------------------------------------------
PCA Management Node Pre-Upgrade Checks                              Passed
PCA Management Node Upgrade                                         Passed
PCA Post-Upgrade Checks                                             Passed
```

```
Broadcast message from root@ovcamn05r1 (pts/3) (Mon Apr 19 18:07:54 2021):
Management Node upgrade succeeded. The master manager will be rebooted to initiate
failover in one minute.
```

The upgrade steps are executed the same way as during the first run. When the second management node is rebooted, the process is complete. At this point, both management nodes run the updated Oracle Linux operating system, Oracle Private Cloud Appliance Controller Software, and Oracle VM Manager. The high-availability cluster configuration of the management nodes is restored, and all Oracle Private Cloud Appliance and Oracle VM Manager management functionality is operational again. However, do not perform any management operations until you have completed the required manual post-upgrade checks.

> **Tip:**
>
> If the first management node is inadvertently rebooted at this point, the upgrade fails on the second management node. For more information, see "Inadvertent Reboot of Stand-by Management Node During Upgrade Suspends Upgrade" in Known Limitations and Workarounds in the *Oracle Private Cloud Appliance Release Notes*.

6. Perform the required manual post-upgrade checks on management nodes and compute nodes. Refer to Running Manual Pre- and Post-Upgrade Checks in Combination with Oracle Private Cloud Appliance Upgrader for instructions.

Upgrading Component Firmware

All the software components in a given Private Cloud Appliance release are designed to work together. As a general rule, no individual appliance component should be upgraded. If a firmware upgrade is required for one or more components, the correct version is distributed inside the Private Cloud Appliance `.iso` file you downloaded from My Oracle Support. When the image file is unpacked on the appliance internal shared storage, the firmware is located on the management nodes at `/nfs/shared_storage/mgmt_image/firmware/`.

> **NOT_SUPPORTED:**
>
> Do not perform any compute node provisioning operations during firmware upgrades.

> **Caution:**
>
> For certain services it is necessary to upgrade the Hardware Management Pack after a Controller Software upgrade. For additional information, refer to "Some Services Require an Upgrade of Hardware Management Pack" in Known Limitations and Workarounds in the *Oracle Private Cloud Appliance Release Notes*.

If a specific or additional procedure to upgrade the firmware of a Private Cloud Appliance hardware component is available, it appears in this section. For components not listed here, you may follow the instructions provided in the product documentation of the subcomponent. An overview of the documentation for appliance components can be found in the Preface of this book and on Oracle Private Cloud Appliance Documentation for Release 2.4.x.

Firmware Policy

To improve Oracle Private Cloud Appliance supportability, reliability and security, Oracle has introduced a standardized approach to component firmware. The general rule remains unchanged: Components and their respective firmware are designed to work together, and therefore should not be upgraded separately. However, the firmware upgrades, which are provided as part of the `.iso` file of a given controller software release, are no longer optional.

As part of the test process prior to a software release, combinations of component firmware are tested on all applicable hardware platforms. This allows Oracle to deliver a fully qualified set of firmware for the appliance as a whole, corresponding to a software release. In order to maintain their Private Cloud Appliance in a qualified state, customers who upgrade to a particular software release are expected to also install all the qualified firmware upgrades delivered as part of the controller software.

The firmware versions that have been qualified by Oracle for a given release are listed in the release notes for that release. Refer to the Firmware Qualification chapter.

Note that the file names shown in the procedures below may not exactly match the file names in the `.iso` image on your system.

> **Caution:**
>
> **Interim Firmware Patches**
>
> Oracle periodically releases firmware patches for many products, for example to limit security vulnerabilities. It may occur that an important firmware patch is released for a component of Private Cloud Appliance outside of the normal Controller Software release schedule. When this occurs, the patches go through the same testing as all other appliance firmware, but they are not added to the qualified firmware list or the installation `.iso` for the affected Controller Software release.
>
> After thorough testing, important firmware patches that cannot be included in the Controller Software `.iso` image are made available to Private Cloud Appliance users through My Oracle Support.

Install the Current Firmware on the Management Nodes

To avoid compatibility issues with newer Oracle Private Cloud Appliance Controller Software and Oracle VM upgrades, you should always install the server ILOM firmware included in the ISO image of the current Oracle Private Cloud Appliance software release. When the ISO image is unpacked on the appliance internal storage,

the firmware directory can be reached from the management nodes at this location: `/nfs/shared_storage/mgmt_image/firmware/`.

Installing the Current Firmware on the Management Nodes

1. To prepare the firmware, log in to the stand-by management node as `root` and extract the management node firmware from the `/nfs/shared_storage/mgmt_image/firmware/` directory.

   a. Confirm that the management node that you are logged in to is the stand-by management node.

   ```
   [root@ovcamn06r1 ~]# pca-check-master
   NODE: 192.168.4.4  MASTER: False
   ```

   b. Extract the management node firmware.

   ```
   [root@ovcamn06r1 ~]# cd /nfs/shared_storage/mgmt_image/firmware/compute/
   X8-2_FIRMWARE/
   [root@ovcamn06r1 X8-2_FIRMWARE]# unzip p***version***_Generic.zip
   ```

2. Log in as `root` to the stand-by management node's ILOM.

   ```
   [root@ovcamn06r1 ~]# ssh ilom-ovcamn06r1
   Password:
   Oracle(R) Integrated Lights Out Manager
   Version 5.1.0.20 r145377
   Copyright (c) 2022, Oracle and/or its affiliates. All rights reserved.
   Warning: HTTPS certificate is set to factory default.
   Hostname: ilom-ovcamn06r1
   ->
   ```

3. Upgrade the firmware using the `load -source` command. For example:

   ```
   -> load -source sftp://root@192.168.4.4/nfs/shared_storage/mgmt_image/firmware/
   compute/X8-2_FIRMWARE/
   Oracle_Server_X8-2-***version***-FIRMWARE_PACK/Firmware/service-processor/ILOM-***version***-
   ORACLE_SERVER_X8-2-rom.pkg
   ```

4. Respond yes to load the file, and to preserve the existing SP and BIOS configurations, then respond no to delay the BIOS upgrade, which will trigger the management node reboot.

   The reboot should take about 10 minutes.

5. If the prechecks indicate you need to update the firmware on your RAID card, do so now.

   Navigate to the location of the extracted firmware and install the card firmware. For example:

   ```
   # cd /nfs/shared_storage/mgmt_image/firmware/compute/X8-2_FIRMWARE/ \
   Oracle_Server_X8-2-***version***-FIRMWARE_PACK/Firmware/SAS9361-16i

   # fwupdate update controller -x metadata.xml
   ```

6. Once the stand-by management node comes back online, reboot the active management node and initiate failover to the newly-upgraded management node.

7. Log in to the newly-upgraded management node and run the `pca-check-master` command to confirm it is now the active node.

8. Now that one management node is upgraded and has assumed the active role, repeat this procedure to upgrade the firmware on the other management node.

Upgrading the Operating Software on the Oracle ZFS Storage Appliance

The instructions in this section are specific for a component firmware upgrade of the Oracle Private Cloud Appliance.

Caution:

During this procedure, the Private Cloud Appliance services on the management nodes must be halted for a period of time. Plan this upgrade carefully, so that no compute node provisioning, Private Cloud Appliance configuration changes, or Oracle VM Manager operations are taking place at the same time.

NOT_SUPPORTED:

The statement below regarding the two-phased procedure does not apply to X8-2 or newer systems. The Oracle ZFS Storage Appliance ZS7-2 comes with a more recent firmware version that is not affected by the issue described.

If the ZFS Storage Appliance is running a firmware version older than 8.7.14, an intermediate upgrade to version 8.7.14 is required. Version 8.7.14 can then be upgraded to the intended newer version. For additional information, refer to "Oracle ZFS Storage Appliance Firmware Upgrade 8.7.20 Requires A Two-Phased Procedure" in Known Limitations and Workarounds in the *Oracle Private Cloud Appliance Release Notes*.

Note:

For detailed information about software upgrades, see Upgrading the Software in the Oracle ZFS Storage Appliance Customer Service Manual, Release OS8.8.x.

The Private Cloud Appliance internal ZFS Storage Appliance contains two clustered controllers in an active/passive configuration. You can disregard the upgrade information for standalone controllers.

Upgrading the ZFS Storage Appliance Operating Software

1. Before initiating the upgrade on the storage controllers, follow the instructions in "Preparing for a Software Upgrade" in Upgrading the Software in the Oracle ZFS Storage Appliance Customer Service Manual, Release OS8.8.x.
2. Log on to the active management node using SSH and an account with superuser privileges.

3. If you are upgrading a ZFS Storage Appliance running firmware version 8.7.14 or newer, skip this step and proceed to the next step.

   If you are upgrading a ZFS Storage Appliancee running a firmware version older than 8.7.14, unzip the firmware package `p27357887_20131_Generic.zip` included in the Private Cloud Appliance software image.

   ```
   [root@ovcamn05r1 ~]# mkdir /nfs/shared_storage/yum/ak
   [root@ovcamn05r1 ~]# cd /nfs/shared_storage/yum/ak
   [root@ovcamn05r1 ak]# unzip /nfs/shared_storage/mgmt_image/firmware/storage/AK_NAS/
   p27357887_20131_Generic.zip
   Archive: /nfs/shared_storage/mgmt_image/firmware/storage/AK_NAS/
   p27357887_20131_Generic.zip
    extracting: ak-nas-2013-06-05-7-14-1-1-1-nd.pkg.gz
     inflating: OS8714_Readme.html
   ```

4. Select the appropriate software update package:

   > **Caution:**
   >
   > The procedure shows the upgrade to version 8.8.28 IDR. For an upgrade to version 8.7.14, substitute the file name in the commands as shown here.

   - Version 8.8.28 IDR - `ak-nas-2013.06.05.8.28-1.2.20.4392.1x-nondebug.pkg`
   - Version 8.7.14 - `ak-nas-2013-06-05-7-14-1-1-1-nd.pkg.gz`

   Download the software update package to both storage controllers. Their management IP addresses are 192.168.4.1 and 192.168.4.2.

   a. Log on to one of the storage controllers using SSH and an account with superuser privileges.

      ```
      [root@ovcamn05r1 ~]# ssh root@192.168.4.1
      Password:
      ovcasn01r1:>
      ```

   b. Enter the following series of commands to download the software update package from the shared storage directory to the controller.

      ```
      ovcasn01r1:> maintenance system updates
      ovcasn01r1:maintenance system updates> download
      ovcasn01r1:maintenance system updates download (uncommitted)> \
      set url=http://192.168.4.199/storage//FW_Updates/release_folders/
      2.4.4/zfs/8.8.28/ak-nas-2013.06.05.8.28-1.1.3x-nondebug.pkg
                 url = http://192.168.4.199/storage//FW_Updates/release_folders/
      2.4.4/zfs/8.8.28/ak-nas-2013.06.05.8.28-1.1.3x-nondebug.pkg
      ovcasn01r1:maintenance system updates download (uncommitted)> commit
      Transferred 1.86G of 1.86G (100%) ... done
      Unpacking ... done
      ```

   c. Wait for the package to fully download and unpack before proceeding.

   d. Repeat these steps for the second storage controller.

5. Ensure that you are logged in to the standby controller.

   Check the storage cluster configuration. If the storage cluster state is stripped, as shown in the following example, then you are logged in to the standby controller. Go to the next

step in this procedure to begin upgrading the standby controller. In the following example, controller `ovcasn02r1` is the standby controller. Upgrade `ovcasn02r1` first.

```
ovcasn02r1:> configuration cluster show
Properties:
                        state = AKCS_STRIPPED
                  description = Ready (waiting for failback)
                     peer_asn = 80e4823f-1573-caaa-8c44-fb3c8af3b921
                peer_hostname = ovcasn01r1
                   peer_state = AKCS_OWNER
            peer_description = Active (takeover completed)
Children:
                      resources => Configure resources
```

If the storage cluster state is clustered, as shown in the following example while logged in to `ovcasn01r1`, continue with this step to confirm which node is the standby node.

```
ovcasn01r1:> configuration cluster show
Properties:
                        state = AKCS_CLUSTERED
                  description = Active
                     peer_asn = b4213dea-8829-4a97-8039-86cbe919f373
                peer_hostname = ovcasn02r1
                   peer_state = AKCS_CLUSTERED
            peer_description = Active

Children:
                      resources => Configure resources
```

To confirm which node in a clustered configuration is the standby node, show cluster resources on each node.

In an active/passive configuration, all singleton resources have a single owner. The standby node is the node with no cluster/singleton resources when in clustered state.

The active controller owns all cluster/singleton resources and reports the size of the storage resource as shown in `zfs/OVCA_POOL` and `zfs/`***`pool_name`*** in the following example on `ovcasn01r1`:

```
ovcasn01r1:> configuration cluster resources show
Resources:

RESOURCE        OWNER           TYPE       LABEL         CHANGES  DETAILS
net/i40e4       ovcasn01r1      private    i40e4         no       192.168.4.1
net/ipmp1       ovcasn01r1      singleton  Management... no
192.168.4.100
net/vnic3       ovcasn01r1      singleton  Storage_In... no
192.168.40.1
net/vnic4       ovcasn01r1      singleton  Storage_In... no
192.168.235.200
net/vnic5       ovcasn01r1      singleton  Storage_In... no
192.168.236.200
zfs/OVCA_POOL   ovcasn01r1      singleton                no       110T
zfs/PCC_internal_pool_HC_01 ovcasn01r1      singleton
no       110T
```

The standby controller does not own any cluster/singleton resource. The standby controller reports only the name of the storage resource, not the size of the

storage resource, as shown in the following example on `ovcasn02r1`. In the following example, controller `ovcasn02r1` is the standby controller. Upgrade `ovcasn02r1` first.

```
ovcasn02r1:> configuration cluster resources show
aksh: warning: terminal type "xterm-256color" unknown; using "vt100"
Resources:

RESOURCE        OWNER           TYPE       LABEL         CHANGES  DETAILS
net/i40e5       ovcasn02r1      private    i40e5         no       192.168.4.2
net/ipmp1       ovcasn01r1      singleton  Management... no       192.168.4.100
net/vnic3       ovcasn01r1      singleton  Storage_In... no       192.168.40.1
net/vnic4       ovcasn01r1      singleton  Storage_In... no       192.168.235.200
net/vnic5       ovcasn01r1      singleton  Storage_In... no       192.168.236.200
zfs/OVCA_POOL   ovcasn01r1      singleton                no
zfs/PCC_internal_pool_HC_01 ovcasn01r1      singleton               no
```

6. Always upgrade the operating software **first** on the standby controller.

   a. Display the available operating software versions and select the version you downloaded.

   ```
   ovcasn02r1:> maintenance system updates
   ovcasn02r1:maintenance system updates> ls
   Updates:

   UPDATE                                   RELEASE DATE             STATUS
   ak-nas@2013.06.05.4.2,1-1.1              2015-6-16 17:03:41       previous
   ak-nas@2013.06.05.7.14,1-1.1             2018-1-6 17:16:42        previous
   ak-nas@2013.06.05.7.20,1-1.4             2018-7-17 02:27:51       current
   ak-nas@2013.06.05.8.20,1-1.3             2020-3-23 16:13:25       waiting
   * ak-nas@2013.06.05.8.28,1-1.3           2021-4-22 00:35:42       waiting
   [*] : Interim Diagnostics and Relief (IDR)

   Deferred updates:

   The appliance is currently configured as part of a cluster. The cluster peer
   may have shared resources for which deferred updates are available. After all
   updates are completed, check both cluster peers for any deferred updates.

   ovcasn01r1:maintenance system updates> select ak-
   nas@2013.06.05.8.28,1-1.3
   ```

   b. Run health checks on the system before you upgrade.

   ```
   ovcasn01r1:maintenance system updates ak-nas@2013.06.05.8.28,1-1.3> check
   You have requested to run checks associated with waiting upgrade media. This
   will execute the same
   set of checks as will be performed as part of any upgrade attempt to this
   media, and will
   highlight conditions that would prevent successful upgrade. No actual upgrade
   will be attempted,
   and the checks performed are of static system state and non-invasive. Do you
   wish to continue?

   Are you sure? (Y/N) y
   Healthcheck running ... -

   Healthcheck completed.  There are no issues at this time which would cause an
   upgrade to this media to be aborted.
   ```

   c. Launch the upgrade process with the selected software version.

```
ovcasn01r1:maintenance system updates ak-nas@2013.06.05.8.28,1-1.3>
upgrade
The system is currently running an IDR. You might negate the fix
provided with the current IDR.
You may still continue. This procedure will consume several minutes and
requires a system reboot
upon successful update, but can be aborted at any time prior to reboot.
A health check will
validate system readiness before an update is attempted, and may also be
executed independently by
clicking the Check button.

Are you sure? (Y/N) y
Updating from ... ak/nas@2013.06.05.8.20,1-2.20.4392.1
Loading media metadata ... done.
Selecting alternate product ... SUNW,maguroZ7
Installing Oracle ZFS Storage ZS7-2 2013.06.05.8.28,1-1.3
pkg://sun.com/ak/SUNW,maguroZ7@2013.06.05.8.28,1-1.3:20201215T215649Z
Creating system/ak-nas-2013.06.05.8.28_1-1.3 ... done.
Creating system/ak-nas-2013.06.05.8.28_1-1.3/install ... done.
Creating system/ak-nas-2013.06.05.8.28_1-1.3/boot ... done.
Creating system/ak-nas-2013.06.05.8.28_1-1.3/root ... done.
Creating system/ak-nas-2013.06.05.8.28_1-1.3/install/svc ... done.
Creating system/ak-nas-2013.06.05.8.28_1-1.3/install/var ... done.
Creating system/ak-nas-2013.06.05.8.28_1-1.3/install/home ... done.
Creating system/ak-nas-2013.06.05.8.28_1-1.3/install/stash ... done.
Creating system/ak-nas-2013.06.05.8.28_1-1.3/wiki ... done.
Extracting os image ... done.
Customizing Solaris ... done.
Creating driver_aliases.addendum... done.
Updating vfstab ... done.
Generating usr/man windex ... done.
Generating usr/gnu/share/man windex ... done.
Generating usr/perl5/man windex ... done.
Preserving ssh keys ... done.
Configuring smf(5) ... done.
Extracting appliance kit ... Creating private passwd and shadow
files ... done.
Creating private smbshadow file ... done.
Creating product symlink ... done.
Registering update job eb3a1611-8d7c-4347-b899-b8b8d3e8a863 ... done.
Creating install profile ... done.
Assigning appliance serial number ... 8ac3f3e4-4b92-4848-9d2b-
ee33fc76c0f4
Determining chassis serial number ... 1909XD2001
Setting appliance product string ... SUNW,maguroZ7
Setting appliance product class ... nas
Setting install timestamp ... done.
Setting virtualization status ... done.
Saving SSL keys ... done.
Updating phone-home key ... done.
Saving currently running profile ... done.
Installing firmware ... done.
Installing device links ... done.
Installing device files ... done.
Updating device links ... done.
Updating /etc ... done.
Creating /.domainroot ... done.
Installing boot amd64/unix ... done.
Assembling etc/system.d ... done.
Creating factory reset boot archive ... done.
```

```
Generating GRUB2 configuration ...  done.
Installing GRUB2 configuration ... done.
Snapshotting zfs filesystems ...  done.
Installation complete - unmounting datasets ...
Creating boot archive ...
done.
 done
Update completed; rebooting.
Connection to 192.168.4.1 closed.
```

d. Update the Oracle ILOM version on the controller.

```
ovcasn01r1:> maintenance system reboot
Upgrading both the Service Processor and host firmware and rebooting.
This process will take several minutes. During this process the service
processor will reboot and
access to the console via the Net MGMT port will be interrupted. After the
service processor
upgrade is complete the host will power down for five to ten minutes in order
to apply the new
host firmware. When the host firmware upgrade is complete the host will power
on and boot
automatically.

DO NOT INTERRUPT THIS PROCESS.

Are you sure? (Y/N) y
Connection to 192.168.4.1 closed.
```

e. At the end of the upgrade, when the controller has fully rebooted and rejoined the cluster, log back in and check the cluster configuration. The upgraded controller must still be in the state "Ready (waiting for failback)".

```
ovcasn01r1:> configuration version show
Appliance Name: ovcasn01r1
Appliance Product: Oracle ZFS Storage ZS7-2
Appliance Type: Sun ZFS Storage 7370
Appliance Version: 2013.06.05.8.28,1-1.3
First Installed: Sun Mar 03 2019 03:35:34 GMT+0000 (UTC)
Last Updated: Fri Apr 23 2021 09:25:34 GMT+0000 (UTC)
Last Booted: Fri Apr 23 2021 09:27:35 GMT+0000 (UTC)
Appliance Serial Number: a3xxxxx-1x60-7x0x-bxx0-84defg34714
Chassis Serial Number: 1XXXXXXX
Software Part Number: Oracle 000-0000-00
Vendor Product ID: ORACLE-ZFS-ZS7-2
Browser Name: aksh 1.0
Browser Details: aksh
HTTP Server: Apache/2.4.46 (Unix)
SSL Version: OpenSSL 1.0.2u-fips  20 Dec 2019
Appliance Kit: ak/SUNW,maguroZ7@2013.06.05.8.28,1-1.3
Release Name: OS8.8.28
Operating System: SunOS 5.11 11.4.28.82.3 64-bit
BIOS: American Megatrends Inc. (BIOS)42040200 (BIOS)08.17.2018
Service Processor: 4.0.4.52 r133103
ovcasn01r1:>
```

7. From the Private Cloud Appliance active management node, stop the Private Cloud Appliance services.

> **Caution:**
>
> You must perform this step if you are upgrading to Controller Software versions 2.3.1, 2.3.2, or 2.3.3. Is not required when upgrading to Controller Software version 2.3.4 or later. Executing the storage controller operating software upgrade while the Private Cloud Appliance services are running, will result in errors and possible downtime.

```
[root@ovcamn05r1 ~]# service ovca stop
```

8. Upgrade the operating software on the second storage controller.

   a. Check the storage cluster configuration. Make sure you are logged on to the active controller.

   ```
   ovcasn01r1:> configuration cluster show
   Properties:
                           state = AKCS_OWNER
                     description = Active (takeover completed)
                        peer_asn = 34e4292a-71ae-6ce1-e26c-cc38c2af9719
                    peer_hostname = ovcasn02r1
                       peer_state = AKCS_STRIPPED
                  peer_description = Ready (waiting for failback)
   ```

   b. Display the available operating software versions and select the version you downloaded.

   ```
   ovcasn01r1:> maintenance system updates
   ovcasn01r1:maintenance system updates> show
   Updates:

   UPDATE                                RELEASE DATE          RELEASE NAME
   STATUS
   ak-nas@2013.06.05.8.5,1-1.3           2019-3-30 07:27:20    OS8.8.5
   previous
   ak-nas@2013.06.05.8.6,1-1.4           2019-6-21 20:56:45    OS8.8.6
   current
   ak-nas@2013.06.05.8.28,1-1.3          2021-4-16 09:57:19    OS8.8.28
   waiting

   ovcasn01r1:maintenance system updates> select ak-
   nas@2013.06.05.8.28,1-1.3
   ```

   c. Launch the upgrade process with the selected software version.

   ```
   ovcasn01r1:maintenance system updates> upgrade
   This procedure will consume several minutes and requires a system reboot
   upon
   successful update, but can be aborted with [Control-C] at any time prior
   to
   reboot. A health check will validate system readiness before an update is
   attempted, and may also be executed independently using the check
   command.

   Are you sure? (Y/N) Y
   ```

   d. At the end of the upgrade, when the controller has fully rebooted and rejoined the cluster, log back in and check the cluster configuration.

```
ovcasn01r1:> configuration cluster show
Properties:
                        state = AKCS_STRIPPED
                  description = Ready (waiting for failback)
                     peer_asn = 34e4292a-71ae-6ce1-e26c-cc38c2af9719
                peer_hostname = ovcasn02r1
                   peer_state = AKCS_OWNER
             peer_description = Active (takeover completed)
```

The last upgraded controller must now be in the state "Ready (waiting for failback)". The controller that was upgraded first, took over the active role during the upgrade and reboot of the second controller, which held the active role originally.

9. Now that both controllers have been upgraded, verify that all disks are online.

```
ovcasn01r1:> maintenance hardware show
[...]
             NAME         STATE   MANUFACTURER   MODEL
SERIAL                   RPM    TYPE
chassis-000  1906NMQ803   ok      Oracle         Oracle Storage DE3-24C
1906NMQ803               7200   hdd
disk-000     HDD 0        ok      WDC            W7214A520ORA014T
001851N3VKLT 9JG3VKLT    7200   data
disk-001     HDD 1        ok      WDC            W7214A520ORA014T
001851N5K85T 9JG5K85T    7200   data
disk-002     HDD 2        ok      WDC            W7214A520ORA014T
001851N5MPXT 9JG5MPXT    7200   data
disk-003     HDD 3        ok      WDC            W7214A520ORA014T
001851N5L08T 9JG5L08T    7200   data
disk-004     HDD 4        ok      WDC            W7214A520ORA014T
001851N42KNT 9JG42KNT    7200   data
[...]
```

10. Initiate a Private Cloud Appliance management node failover and wait until all services are restored on the other management node. This helps prevent connection issues between Oracle VM and the ZFS storage.

    a. Log on to the active management node using SSH and an account with superuser privileges.

    b. Reboot the active management node.

```
[root@ovcamn05r1 ~]# pca-check-master
NODE: 192.168.4.3  MASTER: True
[root@ovcamn05r1 ~]# shutdown -r now
```

    c. Log on to the other management node and wait until the necessary services are running.

> **Note:**
>
> Enter this command at the prompt: `tail -f /var/log/messages`. The log messages should indicate when the management node takes over the active role.

Verify the status of the services:

```
[root@ovcamn06r1 ~]# service ovca status
Checking Oracle Fabric Manager: Running
```

```
MySQL running (70254)                                      [  OK  ]
Oracle VM Manager is running...
Oracle VM Manager CLI is running...
tinyproxy (pid 71315 71314 71313 71312 71310 71309 71308 71307 71306
71305 71301) is running...
dhcpd (pid  71333) is running...
snmptrapd (pid  71349) is running...
log server (pid 6359) is running...
remaster server (pid 6361) is running...
http server (pid 71352) is running...
taskmonitor server (pid 71356) is running...
xmlrpc server (pid 71354) is running...
nodestate server (pid 71358) is running...
sync server (pid 71360) is running...
monitor server (pid 71363) is running...
```

11. When the storage controller cluster has been upgraded, remove the shared storage directory you created to make the unzipped package available.

```
# cd /nfs/shared_storage/yum/ak
# ls ak-nas@2013.06.05.8.28,1-1.3x-nondebug.pkg OS8.8.28_Readme.html
# rm ak-nas@2013.06.05.8.28,1-1.3x-nondebug.pkg OS8.8.28_Readme.html
rm: remove regular file `ak-nas-2013.06.05.8.28-1.1.3x-nondebug.pkg'? yes
rm: remove regular file `OS8.8.28_Readme.html'? yes
# cd ..
# rmdir ak
```

Upgrading the Cisco Switch Firmware

The instructions in this section are specific for a component firmware upgrade of the Oracle Private Cloud Appliance. The Cisco switches require two upgrade procedures: upgrading the Cisco NX-OS software and upgrading the electronic programmable logic device (EPLD). Perform both procedures on each of the switches.

> **Caution:**
>
> When upgrading to Controller Software release 2.4.4, it is critical that you perform the upgrade operations in the correct order. This means the Cisco switch firmware must be upgraded after the management node upgrade, but before the storage network upgrade.
>
> Do not make any spine switch configuration changes until you have completed **all** the upgrade operations. If you make any spine switch configuration changes before all upgrade operations are complete, you could lose access to the storage network. See "Loading Incompatible Spine Switch Configuration Causes Storage Network Outage" in Known Limitations and Workarounds in the *Oracle Private Cloud Appliance Release Notes*.

Upgrading the Cisco NX-OS Software of All Cisco Leaf, Spine, and Management Switches

1. Log on to the active management node using SSH and an account with superuser privileges.

2. Verify that the new Cisco NX-OS software image is available on the appliance shared storage. During the Controller Software upgrade, the Oracle Private Cloud Appliance Upgrader copies the file to the following location:

   ```
   /nfs/shared_storage/mgmt_image/firmware/ethernet/Cisco/nxos.7.0.3.I7.9.bin
   ```

3. Upgrade the switches, one at a time, in the following order.

   a. Leaf Cisco Nexus 9336C-FX2 Switches: ovcasw15r1, ovcasw16r1

      First upgrade the switch that has the Primary or Operational Primary vPC role. Then upgrade the switch that has the Secondary or Operational Secondary vPC role. See Determining Which Switch is Primary or Operational Primary.

   b. Spine Cisco Nexus 9336C-FX2 Switches: ovcasw22r1, ovcasw23r1

      First upgrade the switch that has the Primary or Operational Primary vPC role. Then upgrade the switch that has the Secondary or Operational Secondary vPC role. See Determining Which Switch is Primary or Operational Primary.

   c. Management Cisco Nexus 9348GC-FXP Switch: ovcasw21r1

   After you determine the order in which the switches must be upgraded, follow the procedure Upgrading the Cisco NX-OS Software of Each Cisco Leaf, Spine, and Management Switch to upgrade each switch.

Determining Which Switch is Primary or Operational Primary

Use this procedure to determine which switch is Primary or Operational Primary and which switch is Secondary or Operational Secondary in your environment. Leaf switches are shown in this example. Use the same procedure for spine switches.

1. Log on as `admin` to the first switch in the pair.

   ```
   root@ovcamn05r1 ~]# ssh admin@ovcasw15r1
   User Access Verification
   Password:
   ovcasw15r1#
   ```

2. Determine the vPC role for this switch. In the following example, the vPC role shows that this switch is primary. Upgrade this switch first.

   ```
   ovcasw15r1(config)# show vpc role

   vPC Role status
   ----------------------------------------------------
   vPC role                        : primary
   Dual Active Detection Status    : 0
   vPC system-mac                  : 00:23:04:ee:be:01
   vPC system-priority             : 32667
   vPC local system-mac            : bc:5a:56:aa:a6:1b
   vPC local role-priority         : 1
   vPC local config role-priority  : 1
   vPC peer system-mac             : d4:e8:80:87:e0:ef
   vPC peer role-priority          : 2
   vPC peer config role-priority   : 2
   ovcasw15r1# exit
   Connection to ovcasw15r1 closed
   ```

3. Log on as `admin` to the second switch in the pair.

   ```
   root@ovcamn05r1 ~]# ssh admin@ovcasw16r1
   User Access Verification
   ```

```
Password:
ovcasw16r1#
```

4. Confirm the vPC role for the second switch. In the following example, the vPC role shows that this switch is secondary. Upgrade this switch second.

```
ovcasw16r1# show vpc role

vPC Role status
----------------------------------------------------
vPC role                        : secondary
Dual Active Detection Status    : 0
vPC system-mac                  : 00:23:04:ee:be:02
vPC system-priority             : 32667
vPC local system-mac            : d4:c9:3c:77:06:8f
vPC local role-priority         : 2
vPC local config role-priority  : 2
vPC peer system-mac             : d4:e8:80:87:eb:4b
vPC peer role-priority          : 1
vPC peer config role-priority   : 1
ovcasw16r1# exit
Connection to ovcasw16r1 closed.
```

In the preceding example, upgrade switch `ovcasw15r1` first, and then upgrade switch `ovcasw16r1`. This situation might be reversed in your environment. Your output might look like the following example. In the following example, the vPC role shows that the `ovcasw16r1` switch is operational primary. Upgrade this switch first.

```
ovcasw16r1# show vpc role

vPC Role status
----------------------------------------------------
vPC role                        : secondary, operational primary
Dual Active Detection Status    : 0
vPC system-mac                  : 00:23:04:ee:be:02
vPC system-priority             : 32667
vPC local system-mac            : d4:c9:3c:77:06:8f
vPC local role-priority         : 2
vPC local config role-priority  : 2
vPC peer system-mac             : d4:e8:80:87:eb:4b
vPC peer role-priority          : 1
vPC peer config role-priority   : 1
```

In this example, the vPC role shows that the `ovcasw15r1` switch is operational secondary. Upgrade this switch second.

```
ovcasw15r1# show vpc role

vPC Role status
----------------------------------------------------
vPC role                        : primary, operational secondary
Dual Active Detection Status    : 0
vPC system-mac                  : 00:23:04:ee:be:02
vPC system-priority             : 32667
vPC local system-mac            : d4:e8:80:87:eb:4b
vPC local role-priority         : 1
vPC local config role-priority  : 1
vPC peer system-mac             : d4:c9:3c:77:06:8f
vPC peer role-priority          : 2
vPC peer config role-priority   : 2
```

Use this same procedure for the spine switch pair: `ovcasw22r1` and `ovcasw23r1`.

Upgrading the Cisco NX-OS Software of Each Cisco Leaf, Spine, and Management Switch

> **Note:**
>
> Each pair of leaf and spine switches operates in a vPC topology. Note the vPC roles and upgrade order before you begin the upgrade: The roles will change temporarily during the upgrade process. See Determining Which Switch is Primary or Operational Primary. Leaf and spine switches must be upgraded in the prescribed order.

> **Caution:**
>
> Once an upgrade to Controller Software release 2.4.3 or later is complete on the spine switches, do not attempt to reload a spine switch backup **from a prior software release**. Loading a spine switch backup from a release older than Controller Software release 2.4.3 could cause the management nodes to lose access to the storage network.

> **Note:**
>
> Upgrading the management switch causes network disruption between compute nodes, management nodes, the storage node, and leaf and spine switch management connections. This network disruption is due to the reboot of the switch as part of the upgrade process.

1. Log on to the active management node using SSH and an account with superuser privileges.
2. Log on as `admin` to the first switch to be upgraded.

   Switches must be upgraded in the following order: Primary or Operating Primary leaf switch, Secondary or Operating Secondary leaf switch, Primary or Operating Primary spine switch, Secondary or Operating Secondary spine switch, management switch. See Determining Which Switch is Primary or Operational Primary. The switch shown in this example might not be the first switch to be upgraded in your environment.

   ```
   root@ovcamn05r1 ~]# ssh admin@ovcasw15r1
   User Access Verification
   Password:
   ovcasw15r1#
   ```

   Complete this entire procedure for one switch, then return to this step to upgrade the next switch.
3. Copy the Cisco NX-OS software file to the bootflash location on the switch.

Note that the copy command for the management switch `ovcasw21r1` is different from the copy command for the leaf and spine switches. Specify the appropriate parameter, `management` or `default`, as shown in the examples.

- Leaf and spine switches.

  Execute the following command for each leaf and spine switch, specifying the `management` parameter as shown:

```
ovcasw15r1# copy scp://root@192.168.4.216//nfs/shared_storage/mgmt_image/
firmware/ethernet/Cisco/nxos.7.0.3.I7.9.bin \
bootflash:nxos.7.0.3.I7.9.bin vrf management
root@192.168.4.216's password:
nxos.7.0.3.I7.9.bin                           100%  937MB  16.2MB/s   00:58
Copy complete, now saving to disk (please wait)...
Copy complete.
```

- Management switch.

  Execute the following command for the management switch, specifying the `default` parameter as shown:

```
ovcasw21r1# copy scp://root@192.168.4.216//nfs/shared_storage/mgmt_image/
firmware/ethernet/Cisco/nxos.7.0.3.I7.9.bin \
bootflash:nxos.7.0.3.I7.9.bin vrf default
root@192.168.4.216's password:
nxos.7.0.3.I7.9.bin                           100%  937MB  16.2MB/s   00:58
Copy complete, now saving to disk (please wait)...
Copy complete.
```

4. Verify the impact of the software upgrade.

```
ovcasw15r1# show install all impact nxos bootflash:nxos.7.0.3.I7.9.bin
Installer will perform impact only check. Please wait.

Verifying image bootflash:/nxos.7.0.3.I7.9.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.7.0.3.I7.9.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.7.0.3.I7.9.bin.
[####################] 100% -- SUCCESS

Performing module support checks.

Notifying services about system upgrade.

Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes      disruptive         reset  default upgrade is not
hitless

Images will be upgraded according to the following table:
Module       Image                 Running-Version(pri:alt)           New-
Version  Upg-Required
------  ----------  ----------------------------------------
--------------------  ------------
     1        nxos                              7.0(3)I7(8)
```

```
7.0(3)I7(9)           yes
     1        bios     v05.44(04/02/2021):v05.39(08/30/2019)
v05.38(06/12/2019)            no
```

5. Save the current running configuration as the startup configuration.

```
ovcasw15r1# copy running-config startup-config
[########################################] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
```

6. Install the Cisco NX-OS software that was copied to the bootflash location. When prompted about the disruptive upgrade, enter `y` to continue with the installation.

```
ovcasw15r1# install all nxos bootflash:nxos.7.0.3.I7.9.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.7.0.3.I7.9.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.7.0.3.I7.9.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.7.0.3.I7.9.bin.
[####################] 100% -- SUCCESS

Performing module support checks.

Notifying services about system upgrade.

Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes      disruptive         reset  default upgrade is not hitless

Images will be upgraded according to the following table:
Module       Image                  Running-Version(pri:alt)           New-
Version  Upg-Required
------  ----------  ---------------------------------------
--------------------  ------------
     1        nxos                                7.0(3)I7(8)
7.0(3)I7(9)           yes
     1        bios     v05.44(04/02/2021):v05.39(08/30/2019)
v05.38(06/12/2019)            no

Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)?  [n] y

Install is in progress, please wait.

Performing runtime checks.
[####################] 100% -- SUCCESS

Setting boot variables.
[####################] 100% -- SUCCESS

Performing configuration copy.
[####################] 100% -- SUCCESS
```

```
Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Finishing the upgrade, switch will reboot in 10 seconds.
```

7. After switch reboot, confirm the install succeeded.

```
ovcasw15r1# show install all status
This is the log of last installation.

Verifying image bootflash:/nxos.7.0.3.I7.9.bin for boot variable "nxos".
 -- SUCCESS

Verifying image type.
 -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.7.0.3.I7.9.bin.
 -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.7.0.3.I7.9.bin.
 -- SUCCESS

Performing module support checks.
 -- SUCCESS

Notifying services about system upgrade.
 -- SUCCESS

Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes      disruptive         reset  default upgrade is not
hitless

Images will be upgraded according to the following table:
Module       Image                 Running-Version(pri:alt)           New-
Version  Upg-Required
------  ----------  ----------------------------------------
--------------------  ------------
     1        nxos                                7.0(3)I7(8)
7.0(3)I7(9)           yes
     1        bios     v05.44(04/02/2021):v05.39(08/30/2019)
v05.38(06/12/2019)            no

Switch will be reloaded for disruptive upgrade.

Install is in progress, please wait.

Performing runtime checks.
 -- SUCCESS

Setting boot variables.
 -- SUCCESS

Performing configuration copy.
 -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
 -- SUCCESS
```

```
Finishing the upgrade, switch will reboot in 10 seconds.
```

8. Verify that the correct software version is active on the switch.

```
ovcasw15r1# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
[...]

Software
  BIOS: version 05.38
  NXOS: version 7.0(3)I7(9)
  BIOS compile time:  06/12/2019
  NXOS image file is: bootflash:///nxos.7.0.3.I7.9.bin
  NXOS compile time:  3/3/2020 20:00:00 [03/04/200 04:49:49]
[...]

ovcasw15r1#
```

9. Verify the vPC status.

> **Note:**
>
> This step does not apply to the appliance internal management network switch (Cisco Nexus 9348GC-FXP Switch). Proceed to the next step.

Use the command shown below. The output values should match this example.

```
ovcasw15r1# show vpc brief
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 2
Peer status                       : peer adjacency formed ok <---- verify this
field
vPC keep-alive status             : peer is alive <----- verify this field
Configuration consistency status  : success <----- verify this field
Per-vlan consistency status       : success <----- verify this field
Type-2 consistency status         : success <----- verify this field
vPC role                          : primary, operational secondary
Number of vPCs configured         : 27
Peer Gateway                      : Enabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Disabled
Delay-restore status              : Timer is off.(timeout = 30s)
Delay-restore SVI status          : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router    : Enabled
```

10. Log out of the switch. The firmware has been upgraded successfully.

```
ovcasw15r1# exit
Connection to ovcasw15r1 closed
```

Repeat this procedure for the next switch to be upgraded.

Upgrading the Electronic Programmable Logic Device (EPLD) of all Cisco Leaf, Spine, and Management Switches

The instructions in this section are specific for a component firmware upgrade as part of the Oracle Private Cloud Appliance.

> **Note:**
>
> Upgrading the management switch causes network disruption between compute nodes, management nodes, the storage node, and leaf and spine switch management connections. This network disruption is due to the reboot of the switch as part of the upgrade process.

1. Log on to the active management node using SSH and an account with superuser privileges.
2. Verify that the new Cisco NX-OS EPLD firmware image is available on the appliance shared storage. During the Controller Software upgrade, the Oracle Private Cloud Appliance Upgrader copies the file to the following location:

   ```
   /nfs/shared_storage/mgmt_image/firmware/ethernet/Cisco/n9000-
   epld.7.0.3.I7.9.img
   ```

3. Log on as `admin` to the first switch to be upgraded.

   Switches must be upgraded in the following order: Primary or Operating Primary leaf switch, Secondary or Operating Secondary leaf switch, Primary or Operating Primary spine switch, Secondary or Operating Secondary spine switch, management switch. See Determining Which Switch is Primary or Operational Primary. The switch shown in this example might not be the first switch to be upgraded in your environment.

   ```
   root@ovcamn05r1 ~]# ssh admin@ovcasw15r1
   User Access Verification
   Password:
   ovcasw15r1#
   ```

   Complete this entire procedure for one switch, then return to this step to upgrade the next switch.

4. Copy the firmware file to the bootflash location on the switch.

   Note that the copy command for the management switch `ovcasw21r1` is different from the copy command for the leaf and spine switches. Specify the appropriate parameter, `management` or `default`, as shown in the examples.

   - Leaf and spine switches.

     Execute the following command for each leaf and spine switch, specifying the `management` parameter as shown:

     ```
     ovcasw15r1# copy scp://root@192.168.4.216//nfs/shared_storage/mgmt_image/
     firmware/ethernet/Cisco/n9000-epld.7.0.3.I7.9.img \
     bootflash:n9000-epld.7.0.3.I7.9.img vrf management
     root@192.168.4.216's password:
     n9000-epld.7.0.3.I7.9.img                   100%  142MB  15.8MB/s   00:09
     Copy complete, now saving to disk (please wait)...
     Copy complete.
     ```

- Management switch.

  Execute the following command for the management switch, specifying the `default` parameter as shown:

```
ovcasw21r1# copy scp://root@192.168.4.216//nfs/shared_storage/mgmt_image/
firmware/ethernet/Cisco/n9000-epld.7.0.3.I7.9.img \
bootflash:n9000-epld.7.0.3.I7.9.img vrf default
root@192.168.4.216's password:
n9000-epld.7.0.3.I7.9.img                     100%  142MB  15.8MB/s   00:09
Copy complete, now saving to disk (please wait)...
Copy complete.
```

5. Verify the impact of the EPLD upgrade.

```
ovcasw15r1# show install all impact epld bootflash:n9000-epld.7.0.3.I7.9.img

Retrieving EPLD versions.... Please wait.
Images will be upgraded according to the following table:
Module  Type   EPLD             Running-Version   New-Version  Upg-Required
------  ----  -------------      ---------------   -----------  ------------
     1   SUP  MI FPGA                   0x04        0x05            Yes
     1   SUP  IO FPGA                   0x09        0x11            Yes

Compatibility check:
Module        Type         Upgradable        Impact   Reason
-----------------------------------------------
     1            SUP           Yes       disruptive   Module Upgradable
```

6. Save the current running configuration as the startup configuration.

```
ovcasw15r1# copy running-config startup-config
[########################################] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
```

> **Note:**
>
> You must upgrade both the primary and golden regions of the FPGA. However, only one upgrade is allowed per reload to avoid programming errors. The next steps describe how to upgrade both regions of the FPGA.

7. Install the Cisco EPLD software that was copied to the bootflash location **to the primary region of the FPGA**. When prompted about the switch reload, enter `y` to continue with the installation.

> **Caution:**
>
> Do not interrupt, power cycle, or reload the switch during the upgrade.

```
ovcasw15r1# install epld bootflash:n9000-epld.7.0.3.I7.9.img module 1
Digital signature verification is successful
Compatibility check:
Module        Type         Upgradable       Impact   Reason
------  -----------------  ----------    ----------   ------
     1            SUP           Yes      disruptive   Module Upgradable
```

```
Retrieving EPLD versions.... Please wait.
Images will be upgraded according to the following table:
Module  Type   EPLD             Running-Version   New-Version  Upg-Required
------  ----  -------------      ---------------   -----------  ------------
     1   SUP  MI FPGA                   0x04         0x05            No
     1   SUP  IO FPGA                   0x09         0x11           Yes
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ?  [n] y

Proceeding to upgrade Modules.

 Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (     64 of      64 sectors)
Module 1 EPLD upgrade is successful.
Module        Type  Upgrade-Result
------  ------------------  --------------
     1         SUP         Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

Resetting Active SUP (Module 1) FPGAs. Please wait...
```

8. The switch reloads automatically and boots from the backup FPGA. Confirm the primary module upgrade succeeded.

```
ovcasw15r1# show version module 1 epld

EPLD Device                          Version
---------------------------------------
MI FPGA                               0x5
IO FPGA                               0x9
```

At this point, the `MI FPGA` version is upgraded, but the `IO FPGA` version is not upgraded.

9. Install the Cisco EPLD software that was copied to the bootflash location **to the golden region of the FPGA**. When prompted about the switch reload, enter `y` to continue with the installation.

> **Caution:**
>
> Do not interrupt, power cycle, or reload the switch during the upgrade.

```
ovcasw15r1# install epld bootflash:n9000-epld.7.0.3.I7.9.img module 1 golden
Digital signature verification is successful
Compatibility check:
Module        Type         Upgradable       Impact   Reason
------  -----------------  ----------    -----------   ------
     1            SUP           Yes      disruptive   Module Upgradable

Retrieving EPLD versions.... Please wait.
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
```

```
Do you want to continue (y/n) ?  [n] y

Proceeding to upgrade Modules.

 Starting Module 1 EPLD Upgrade

Module 1 : MI FPGA [Programming] : 100.00% (     64 of      64 sectors)
Module 1 : IO FPGA [Programming] : 100.00% (     64 of      64 sectors)
Module 1 EPLD upgrade is successful.
Module        Type  Upgrade-Result
------  ------------------  --------------
     1         SUP         Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

Resetting Active SUP (Module 1) FPGAs. Please wait...
```

10. The switch reloads automatically and boots from the backup FPGA. Confirm the both upgrades succeeded.

```
ovcasw15r1# show version module 1 epld

EPLD Device                          Version
---------------------------------------
MI FPGA                               0x5
IO FPGA                               0x11
```

11. Verify the vPC status.

> **Note:**
>
> This step does not apply to the appliance internal management network switch (Cisco Nexus 9348GC-FXP Switch). Proceed to the next step.

Use the command shown below. The output values should match this example.

```
ovcasw15r1# show vpc brief
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 2
Peer status                       : peer adjacency formed ok <---- verify this
field
vPC keep-alive status             : peer is alive <----- verify this field
Configuration consistency status  : success <----- verify this field
Per-vlan consistency status       : success <----- verify this field
Type-2 consistency status         : success <----- verify this field
vPC role                          : primary, operational secondary
Number of vPCs configured         : 27
Peer Gateway                      : Enabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Disabled
Delay-restore status              : Timer is off.(timeout = 30s)
Delay-restore SVI status          : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router    : Enabled
```

12. Log out of the switch. The firmware has been upgraded successfully.

```
ovcasw15r1# exit
Connection to ovcasw15r1 closed
```

Repeat this procedure for the next switch to be upgraded.

Install the Current Firmware on All Compute Nodes

Always install the server ILOM and component firmware included in the ISO image of the current Oracle Private Cloud Appliance software release. When the image file is unpacked on the appliance internal shared storage, the firmware is located on the management nodes at `/nfs/shared_storage/mgmt_image/firmware/`.

For firmware upgrade instructions, refer to the Administration Guide of the server series installed in your appliance rack at Servers Documentation. Supported firmware versions are listed in the Oracle Private Cloud Appliance Release Notes.

The following task map outlines the steps you should consider as you update compute node firmware.

Table 3-3 Compute Node Firmware Upgrade Task Map

Component	Resources
Migrate any VMs off of the compute nodes	See Migrate or Move Virtual Machines in the Oracle VM Manager User's Guide.
Update CX5 card firmware	For general card update instructions, see support document How to upgrade Private Cloud Appliance (PCA) compute or management node Sun InfiniBand Dual Port CX3 firmware (Doc ID 2399803.1). • For Oracle Server X9-2 CX5 upgrades, use the `Oracle_Server_X9-2-`***`version`***`-FIRMWARE_PACK/Firmware/Oracle_Dual_Port_CX5_100_Gb_OCP_Adapter` file. • For Oracle Server X8-2 CX5 upgrades, use the `firmware/compute/X8-2_FIRMWARE/Oracle_Dual_Port_100_Gb_RoCE_Adapter/fw-ConnectX5-rel-`***`version`*** `_MCX556A-EDAS_C14_OCI_Ax_Bx-UEFI-14.21.16.signed.bin` file. For more information refer to the Read Me file at `firmware/compute/X8-2_FIRMWARE/readme.txt`. NOTE: Do not upgrade to the Mellanox firmware provided in `p32629785_123_Generic.zip`. That file contains an outdated CX5 firmware version.
Update RAID Controller firmware	For general card update instructions, see support document 2399803.1. For Oracle Server X9-2, the RAID firmware is upgraded when the ILOM/BIOS is upgraded, so no further action is necessary.

Table 3-3 (Cont.) Compute Node Firmware Upgrade Task Map

Component	Resources
Update server ILOM/BIOS firmware	For general ILOM/BIOS firmware update instructions, see Updating System Firmware Using Oracle ILOM.
Proceed to Upgrading the Compute Node Software	See Upgrading the Compute Node Software.

Upgrading the Compute Node Software

Starting with Oracle Private Cloud Appliance Controller Software release 2.4.4, the compute node upgrade procedure has been revamped and includes reprovisioning the servers to upgrade both the operating system and the Oracle VM virtualization platform using the `pca_upgrader` tool.

> **Caution:**
>
> Do not make any management changes during the entire compute node upgrade procedure.

> **Note:**
>
> Prior to this release, compute nodes were updated using the `update compute-node` command. This update method is not supported for version 2.4.4.

To successfully upgrade a compute node the `pca_upgrader` tool performs several pre-checks to ensure the node is ready for upgrade. After successfully completing the pre-checks, the upgrader proceeds to these tasks:

1. Backs up the compute node configuration information: including network, repository, and storage information. Backups are stored here: `/nfs/shared_storage/pca_upgrader/cn_upgrade`
2. Reprovisions the compute node with the latest operating system and Oracle VM Server version.
3. Restores the compute node configuration information.

Essentially, the upgrade process involves a complete re-imaging of the compute node to reinstall the latest operating system and Oracle VM server versions, and this process can take around an hour. Any other applications installed on your compute nodes will be removed during the upgrade procedure. Make sure to back up any applications you want to restore to the compute nodes after upgrade.

Upgrading a Compute Node

> **Caution:**
>
> Execute this procedure on each compute node *after* the software upgrade on the management nodes has completed successfully. The management node upgrade creates the compute node image required for the following procedure.

> **Caution:**
>
> If compute nodes are running other packages that are not part of Oracle Private Cloud Appliance, these must be backed up before upgrade.

> **Caution:**
>
> Do not use the `add network-to-tenant-group`, `add compute-node`, and `reprovision` CLI commands during the compute node upgrade procedure.

1. Make sure that the management nodes are upgraded to the new release.

   You can verify this by logging into the active management node and entering the following command in the Oracle Private Cloud Appliance CLI:

   ```
   # pca-admin
   Welcome to PCA! Release: 2.4.4
   PCA> show version

   ----------------------------------------
   Version              2.4.4
   Build                000
   Date                 2021-03-22
   ----------------------------------------

   Status: Success
   ```

   Leave the console and CLI connection open. You need to run the upgrade command later in this procedure.

2. Migrate all virtual machines away from the compute node you want to upgrade.

   Information on migrating virtual machines is provided in Migrate or Move Virtual Machines in the Oracle VM Manager User's Guide.

3. Remove any Repository Exports on the compute node being upgraded.

   For more information, see Delete Repository Export in the Oracle VM Manager User's Guide.

4. Back up any other installed packages that are not part of Oracle Private Cloud Appliance.

If you have installed any other software on the compute node, back it up now; you will need to restore it once the upgrade is finished. See Backup Local Customizations.

5. From the active management node, run the Oracle Private Cloud Appliance Upgrader in verify-only mode on the compute node.

```
[root@ovcamn05r1 ~]# pca_upgrader -V -t compute -c ovcacn07r1
PCA Rack Type: PCA X8_BASE.
Please refer to log file /nfs/shared_storage/pca_upgrader/log/
pca_upgrader_2021_07_25-04.34.22.log for more details.
Beginning PCA Compute Node Pre-Upgrade Checks...
Check target Compute Node exists 1/10
Check the provisioning lock is not set 2/10
Check GRUB customizations 3/10
Check LUN and LUN path counts for FC HBA cards 4/10
Check OVCA release on Management Nodes 5/10
Check target Compute Node has no VMs 6/10
Check local repository of target Compute Node is empty 7/10
Check no physical disks on target Compute Node have repositories 8/10
Check Compute Node's Tenant matches Server Pool 9/10
Check target Compute Node has no local networks VNICs 10/10
PCA Compute Node Pre-Upgrade Checks completed after 0 minutes
--------------------------------------------------------------------------------
PCA Compute Node Pre-Upgrade Checks Passed
--------------------------------------------------------------------------------
Check target Compute Node exists Passed
Check the provisioning lock is not set Passed
Check GRUB customizations Passed
Check LUN and LUN path counts for FC HBA cards Passed
Check OVCA release on Management Nodes Passed
Check target Compute Node has no VMs Passed
Check local repository of target Compute Node is empty Passed
Check no physical disks ontarget Compute Node have repositories Passed
Check Compute Node's Tenant matches Server Pool Passed
Check target Compute Node has no local networks VNICs Passed
--------------------------------------------------------------------------------
Overall Status Passed
--------------------------------------------------------------------------------
PCA Compute Node Pre-Upgrade Checks Passed
  Please refer to log file /nfs/shared_storage/pca_upgrader/log/
pca_upgrader_date-04.34.22.log for more details.
```

The upgrader performs several pre-checks. If any pre-check fails, refer to the log file for details on any failures and fix those failures before running the upgrade. Find the compute node log files in this directory on the shared storage: `/nfs/shared_storage/pca_upgrader/log`.

If your pre-checks fail, ensure the compute node local repository is empty. For details, see "Pre-Upgrade Check of Local Repository to Ensure Target Compute Node is Empty" in Known Limitations and Workarounds in the *Oracle Private Cloud Appliance Release Notes*.

If you encounter FC HBA LUN errors, apply the `service multipathd restart` command to resolve the issue. If that does not resolve the issues, see the Oracle Private Cloud Appliance Release Notes for more information about LUN errors.

6. From the active management node, run the upgrade for the designated compute node.

```
[root@ovcamn05r1 ~]# pca_upgrader -U -t compute -c ovcacn07r1
PCA Rack Type: PCA X8_BASE.
Please refer to log file /nfs/shared_storage/pca_upgrader/log/
pca_upgrader_2021_07_25-04.36.30.log for more details.
```

```
Beginning PCA Compute Node Pre-Upgrade Checks...
Check target Compute Node exists 1/10
Check the provisioning lock is not set 2/10
Check LUN and LUN path counts for FC HBA cards 3/10
Check GRUB customizations 4/10
Check OVCA release on Management Nodes 5/10
Check Compute Node's Tenant matches Server Pool 6/10
Check target Compute Node has no local networks VNICs 7/10
Check no physical disks on target Compute Node have repositories 8/10
Check local repository of target Compute Node is empty 9/10
Check target Compute Node has no VMs 10/10
PCA Compute Node Pre-Upgrade Checks completed after 0 minutes
Beginning PCA Compute Node Upgrade
Place Compute Upgrade Locks 1/6
Backup Compute Node customizations 2/6
Unpresent repositories from Compute Node 3/6
Upgrade the Compute Node 4/6
Restore Compute Node customizations 5/6
Remove Compute Upgrade Locks 6/6
PCA Compute Node upgrade completed after 42 minutes
Beginning PCA Compute Node Post-Upgrade Checks...
PCA Compute Node Post-Upgrade Checks completed after 0 minutes
--------------------------------------------------------------------------------
PCA Compute Node Pre-Upgrade Checks Passed
--------------------------------------------------------------------------------
Check target Compute Node exists Passed
Check the provisioning lock is not set Passed
Check LUN and LUN path counts for FC HBA cards Passed
Check GRUB customizations Passed
Check OVCA release on Management Nodes Passed
Check Compute Node's Tenant matches Server Pool Passed
Check target Compute Node has no local networks VNICs Passed
Check no physical disks on target Compute Node have repositories Passed
Check local repository of target Compute Node is empty Passed
Check target Compute Node has no VMs Passed
--------------------------------------------------------------------------------
PCA Compute Node Upgrade Passed
--------------------------------------------------------------------------------
Place Compute Upgrade Locks Passed
Backup Compute Node customizations Passed
Unpresent repositories from Compute Node Passed
Upgrade the Compute Node Passed
Restore Compute Node customizations Passed
Remove Compute Upgrade Locks Passed
--------------------------------------------------------------------------------
PCA Compute Node Post-Upgrade Checks Passed
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Overall Status Passed
--------------------------------------------------------------------------------
PCA Compute Node Pre-Upgrade Checks Passed
PCA Compute Node Upgrade Passed
PCA Compute Node Post-Upgrade Checks Passed
  Please refer to log file /nfs/shared_storage/pca_upgrader/log/
pca_upgrader_date-04.36.30.log for more details.
```

7. Once the `pca_upgrader` tool completes the upgrade, log in to the Oracle VM Manager and confirm the compute node has been returned to the correct server pool.
8. Restore any other software that was on the compute node.

9. Repeat this procedure for each compute node in your Oracle Private Cloud Appliance.

After successful completion of the upgrade, the Oracle Private Cloud Appliance is ready to resume all normal operations.

4

Oracle Private Cloud Appliance Command Line Interface (CLI)

All Private Cloud Appliance command line utilities are consolidated into a single command line interface that is accessible via the management node shell by running the `pca-admin` command located at `/usr/sbin/pca-admin`. This command is in the system path for the root user, so you should be able to run the command from anywhere that you are located on a management node. The CLI provides access to all of the tools available in the Oracle Private Cloud Appliance Dashboard, as well as many that do not have a Dashboard equivalent. The design of the CLI makes it possible to script actions that may need to be performed more regularly, or to write integration scripts with existing monitoring and maintenance software not directly hosted on the appliance.

It is important to understand that the CLI, described here, is distinct from the Oracle VM Manager command line interface, which is described fully in the Oracle VM Manager Command Line Interface User's Guide.

In general, it is preferable that CLI usage is restricted to the active management node. While it is possible to run the CLI from either management node, some commands are restricted to the active management node and return an error if you attempt to run them on the passive management node.

CLI Usage

The Oracle Private Cloud Appliance command line interface is triggered by running the `pca-admin` command. It can run either in interactive mode (see Interactive Mode) or in single-command mode (see Single-command Mode) depending on whether you provide the syntax to run a particular CLI command when you invoke the command line interpreter.

The syntax when using the CLI is as follows:

```
PCA> Command
        Command_Target
        <Arguments>
        Options
```

where:

- ***Command*** is the command type that should be initiated. For example `list`;
- ***Command_Target*** is the Oracle Private Cloud Appliance component or process that should be affected by the command. For example management-node, compute-node, task etc;
- ***<Arguments>*** consist of positioning arguments related to the command target. For instance, when performing a reprovisioning action against a compute node, you should provide the specific compute node that should be affected as an argument for this command. For example: `reprovision compute-node ovcacn11r1 ;`

- ***Options*** consist of options that may be provided as additional parameters to the command to affect its behavior. For instance, the `list` command provides various sorting and filtering options that can be appended to the command syntax to control how output is returned. For example: `list compute-node --filter-column Provisioning_State --filter dead` . See Controlling CLI Output for more information on many of these options.

The CLI includes its own internal help that can assist you with understanding the commands, command targets, arguments and options available. See Internal CLI Help for more information on how to use this help system. When used in interactive mode, the CLI also provides tab completion to assist you with the correct construction of a command. See Tab Completion for more information on this.

Interactive Mode

The Oracle Private Cloud Appliance command line interface (CLI) provides an interactive shell that can be used for user-friendly command line interactions. This shell provides a closed environment where users can enter commands specific to the management of the Oracle Private Cloud Appliance. By using the CLI in interactive mode, the user can avail of features like tab completion to easily complete commands correctly. By default, running the `pca-admin` command without providing any additional parameters causes the CLI interpreter to run in interactive mode.

It is possible to identify that you are in a CLI shell running in interactive mode as the shell prompt is indicated by **PCA>**.

Example 4-1 An example of interactive mode usage of the CLI

```
# pca-admin
Welcome to PCA! Release: 2.4.1
PCA> list management-node

Management_Node IP_Address   Provisioning_Status  ILOM_MAC
Provisioning_State   Master
--------------- ----------   -------------------  --------
-----------------   ------
ovcamn05r1      192.168.4.3  RUNNING              00:10:e0:e9:1f:c9
running             Yes
ovcamn06r1      192.168.4.4  RUNNING              00:10:e0:e7:26:ad
running             None
----------------
2 rows displayed

Status: Success
PCA> exit
#
```

To exit from the CLI when it is in interactive mode, you can use either the `q`, `quit`, or `exit` command, or alternatively use the Ctrl+D key combination.

Tab Completion

The CLI supports tab-completion when in interactive mode. This means that pressing the tab key while entering a command can either complete the command on your behalf, or can indicate options and possible values that can be entered to complete a command. Usually you must press the tab key at least twice to effect tab-completion.

Tab-completion is configured to work at all levels within the CLI and is context sensitive. This means that you can press the tab key to complete or prompt for commands, command targets, options, and for certain option values. For instance, pressing the tab key twice at a blank prompt within the CLI automatically lists all possible commands, while pressing the tab key after typing the first letter or few letters of a command automatically completes the command for you. Once a command is specified, followed by a space, pressing the tab key indicates command targets. If you have specified a command target, pressing the tab key indicates other options available for the command sequence. If you press the tab key after specifying a command option that requires an option value, such as the --filter-column option, the CLI attempts to provide you with the values that can be used with that option.

Example 4-2 Examples showing tab-completion

```
PCA> <tab>
EOF          backup       create       deprovision  exit         help         q
remove       rerun        shell        start        update       add          configure
delete       diagnose     get          list         quit         reprovision  set
show         stop

              PCA> list <tab>
compute-node       lock               mgmt-switch-port   network-port       task
update-task        uplink-port-group  config-error       management-node    network
network-switch     tenant-group       uplink-port

                  PCA> list com<tab>pute-node
```

The ***<tab>*** indicates where the user pressed the tab key while in an interactive CLI session. In the final example, the command target is automatically completed by the CLI.

Running Shell Commands

It is possible to run standard shell commands while you are in the CLI interpreter shell. These can be run by either preceding them with the `shell` command or by using the `!` operator as a shortcut to indicate that the command that follows is a standard shell command. For example:

```
PCA> shell date
Wed Jun  5 08:15:56 UTC 2019
PCA> !uptime > /tmp/uptime-today
PCA> !rm /tmp/uptime-today
```

Single-command Mode

The CLI supports 'single-command mode', which allows you to execute a single command from the shell via the CLI and to obtain the output before the CLI exits back to the shell. This is particularly useful when writing scripts that may interact with the CLI, particularly if used in conjunction with the CLI's JSON output mode described in JSON Output.

To run the CLI in single-command mode, simply include the full command syntax that you wish to execute as parameters to the `pca-admin` command.

An example of single command mode is provided below:

```
# pca-admin list compute-node
Compute_Node  IP_Address    Provisioning_Status  ILOM_MAC           Provisioning_State
------------  ----------    -------------------  --------           ------------------
ovcacn12r1    192.168.4.8   RUNNING              00:10:e0:e5:e6:d3  running
ovcacn07r1    192.168.4.7   RUNNING              00:10:e0:e6:8d:0b  running
```

```
ovcacn13r1    192.168.4.11  RUNNING             00:10:e0:e6:f7:f7   running
ovcacn14r1    192.168.4.9   RUNNING             00:10:e0:e7:15:eb   running
ovcacn10r1    192.168.4.12  RUNNING             00:10:e0:e7:13:8d   running
ovcacn09r1    192.168.4.6   RUNNING             00:10:e0:e6:f8:6f   running
ovcacn11r1    192.168.4.10  RUNNING             00:10:e0:e6:f9:ef   running
----------------
7 rows displayed

#
```

Controlling CLI Output

The CLI provides options to control how output is returned in responses to the various CLI commands that are available. These are provided as additional options as the final portion of the syntax for a CLI command. Many of these options can make it easier to identify particular items of interest through sorting and filtering, or can be particularly useful when scripting solutions as they help to provide output that is more easily parsed.

JSON Output

JSON format is a commonly used format to represent data objects in a way that is easy to machine-parse but is equally easy for a user to read. Although JSON was originally developed as a way to represent JavaScript objects, parsers are available for a wide number of programming languages, making it an ideal output format for the CLI if you are scripting a custom solution that may need to interface directly with the CLI.

The CLI returns its output for any command in JSON format if the --json option is specified when a command is run. Typically this option may be used when running the CLI in single-command mode. An example follows:

```
# pca-admin list compute-node --json
{
    "00:10:e0:e5:e6:ce": {
        "name": "ovcacn12r1",
        "ilom_state": "running",
        "ip": "192.168.4.8",
        "tenant_group_name": "Rack1_ServerPool",
        "state": "RUNNING",
        "networks": "default_external, default_internal",
        "ilom_mac": "00:10:e0:e5:e6:d3"
    },
    "00:10:e0:e6:8d:06": {
        "name": "ovcacn07r1",
        "ilom_state": "running",
        "ip": "192.168.4.7",
        "tenant_group_name": "Rack1_ServerPool",
        "state": "RUNNING",
        "networks": "default_external, default_internal",
        "ilom_mac": "00:10:e0:e6:8d:0b"
    },
[...]
    "00:10:e0:e6:f9:ea": {
        "name": "ovcacn11r1",
        "ilom_state": "running",
        "ip": "192.168.4.10",
        "tenant_group_name": "",
        "state": "RUNNING",
        "networks": "default_external, default_internal",
```

```
        "ilom_mac": "00:10:e0:e6:f9:ef"
    }
}
```

In some cases the JSON output may contain more information than is displayed in the tabulated output that is usually shown in the CLI when the --json option is not used. Furthermore, the keys used in the JSON output may not map identically to the table column names that are presented in the tabulated output.

Sorting and filtering options are currently not supported in conjunction with JSON output, since these facilities can usually be implemented on the side of the parser.

Sorting

Typically, when using the `list` command, you may wish to sort information in a way that makes it easier to view items of particular interest. This is achieved using the --sorted-by and --sorted-order options in conjunction with the command. When using the --sorted-by option, you must specify the column name against which the sort should be applied. You can use the --sorted-order option to control the direction of the sort. This option should be followed either with ASC for an ascending sort, or DES for a descending sort. If this option is not specified, the default sort order is ascending.

For example, to sort a view of compute nodes based on the status of the provisioning for each compute node, you may do the following:

```
PCA> list compute-node --sorted-by Provisioning_State --sorted-order ASC

Compute_Node  IP_Address    Provisioning_Status  ILOM_MAC
Provisioning_State
------------  ----------    ----------           --------              ----------
ovcacn08r1    192.168.4.9   RUNNING              00:10:e0:65:2f:b7     dead
ovcacn28r1    192.168.4.10  RUNNING              00:10:e0:62:31:81
initializing_stage_wait_for_hmp
ovcacn10r1    192.168.4.7   RUNNING              00:10:e0:65:2f:cf
initializing_stage_wait_for_hmp
ovcacn30r1    192.168.4.8   RUNNING              00:10:e0:40:cb:59     running
ovcacn07r1    192.168.4.11  RUNNING              00:10:e0:62:ca:09     running
ovcacn26r1    192.168.4.12  RUNNING              00:10:e0:65:30:f5     running
ovcacn29r1    192.168.4.5   RUNNING              00:10:e0:31:49:1d     running
ovcacn09r1    192.168.4.6   RUNNING              00:10:e0:65:2f:3f     running
----------------
8 rows displayed

Status: Success
```

Note that you can use tab-completion with the --sorted-by option to easily obtain the options for different column names. See Tab Completion for more information.

Filtering

Some tables may contain a large number of rows that you are not interested in, to limit the output to items of particular interest you can use the filtering capabilities that are built into the CLI. Filtering is achieved using a combination of the --filter-column and --filter options. The --filter-column option must be followed by specifying the column name, while the --filter option is followed with the specific text that should be matched to form the filter. The text that should be specified for a --filter may contain wildcard characters. If that is not the case, it must be an exact match. Filtering does not currently support regular expressions or partial matches.

For example, to view only the compute nodes that have a Provisioning state equivalent to 'dead', you could use the following filter:

```
PCA> list compute-node --filter-column Provisioning_State --filter dead

Compute_Node  IP_Address    Provisioning_Status  ILOM_MAC
Provisioning_State
------------  ----------    ----------           --------              ----------
ovcacn09r1    192.168.4.10  DEAD                 00:10:e0:0f:55:cb
dead
ovcacn11r1    192.168.4.9   DEAD                 00:10:e0:0f:57:93
dead
ovcacn14r1    192.168.4.7   DEAD                 00:10:e0:46:9e:45
dead
ovcacn36r1    192.168.4.11  DEAD                 00:10:e0:0f:5a:9f
dead
----------------
4 rows displayed

Status: Success
```

Note that you can use tab-completion with the --filter-column option to easily obtain the options for different column names. See Tab Completion for more information.

Internal CLI Help

The CLI includes its own internal help system. This is triggered by issuing the `help` command:

```
PCA> help

Documented commands (type help <topic>):
========================================
add        create       diagnose  list         rerun  start
backup     delete       get       remove       set    stop
configure  deprovision  help      reprovision  show   update

Undocumented commands:
======================
EOF  exit  q  quit  shell
```

The help system displays all of the available commands that are supported by the CLI. These are organized into 'Documented commands' and 'Undocumented commands'. Undocumented commands are usually commands that are not specific to the management of the Oracle Private Cloud Appliance, but are mostly discussed within this documentation. Note that more detailed help can be obtained for any documented command by appending the name of the command to the `help` query. For example, to obtain the help documentation specific to the list command, you can do the following:

```
PCA> help list
Usage: pca-admin list <Command Target> [OPTS]

Command Targets:
  compute-node          List computer node.
  config-error          List configuration errors.
  lock                  List lock.
  management-node       List management node.
  mgmt-switch-port      List management switch port.
  network               List active networks.
  network-port          List network port.
```

```
  network-switch        List network switch.
  task                  List task.
  tenant-group          List tenant-group.
  update-task           List update task.
  uplink-port           List uplink port.
  uplink-port-group     List uplink port group.

Options:
  --json                Display the output in json format.
  --less                Display output in the less pagination mode.
  --more                Display output in the more pagination mode.
  --tee=OUTPUTFILENAME  Export output to a file.
  --sorted-by=SORTEDBY  Sorting the table by a column.
  --sorted-order=SORTEDORDER
                        Sorting order.
  --filter-column=FILTERCOLUMN
                        Table column that needs to be filtered.
  --filter=FILTER       filter criterion
```

You can drill down further into the help system for most commands by also appending the command target onto your `help` query:

```
PCA> help reprovision compute-node
  Usage:
  reprovision compute-node <compute node name> [options]

  Example:
  reprovision compute-node ovcacn11r1

  Description:
  Reprovision a compute node.
```

Finally, if you submit a help query for something that doesn't exist, the help system generates an error and automatically attempts to prompt you with alternative candidates:

```
PCA> list ta
Status: Failure
Error Message: Error (MISSING_TARGET_000): Missing command target for command: list.
Command targets can be: ['update-task', 'uplink-port-group', 'config-error',
'network',
'lock', 'network-port', 'tenant-group', 'network-switch', 'task', 'compute-node',
'uplink-port', 'mgmt-switch-port', 'management-node'].
```

CLI Commands

This section describes all of the documented commands available via the CLI.

add compute-node

Adds a compute node to an existing tenant group. To create a new tenant group, see create tenant-group.

Syntax

```
add compute-node node tenant-group-name [OPTIONS]
```

where *tenant-group-name* is the name of the tenant group you wish to add one or more compute nodes to, and *node* is the name of the compute node that should be added to the selected tenant group.

Description

Use the `add compute-node` command to add the required compute nodes to a tenant group you created. If a compute node is currently part of another tenant group, it is first removed from that tenant group. If custom networks are already associated with the tenant group, the newly added server is connected to those networks as well.

During `add compute-node` operations, Kubernetes cluster operations should not be underway or started. If existing Kubernetes clusters are in the tenant group, there will be a period after the compute node is added and the `K8S_Private` network is connected that the existing Kubernetes private cluster networks are extended. The Kubernetes private network extension is done asynchronously outside of the compute-node add.

Use the command `add network-to-tenant-group` to associate a custom network with a tenant group.

Options

The following table shows the available options for this command.

Option	Description
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-3 Adding a Compute Node to a Tenant Group

```
PCA> add compute-node ovcacn09r1 myTenantGroup

Status: Success
```

add initiator

Adds an initiator to an iSCSI LUN. This allows you to control access to the iSCSI LUN shares you created on the internal ZFS Storage Appliance.

Syntax

```
add initiator initiator-IQN LUN-name [OPTIONS]
```

LUN-name is the name of the iSCSI LUN share to which you are granting access using an initiator.

Description

Use the `add initiator` command to add an initiator to an iSCSI LUN. This command creates an initiator with the provided IQN in the ZFS Storage Appliance and adds it to initiator group associated with an iSCSI share.

Options

The following table shows the available options for this command.

Option	Description
initiator-IQN	List the initiator IQN from the virtual machine you want to have access to the LUN. Only virtual machines within the same subnet/network can have access to the filesystem.
LUN-name	Specify the LUN you want to make available using an initiator.
`--json`	Return the output of the command in JSON format.
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=`***OUTPUTFILENAME***	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-4 Adding an Initiator to a LUN

```
PCA> add initiator iqn.example.com myLUN
Status: Success
```

add network

Connects a server node to an existing network. To create a new custom network, see create network.

Syntax

```
add network network-name node [OPTIONS]
```

where *network-name* is the name of the network you wish to connect one or more servers to, and *node* is the name of the server node that should be connected to the selected network.

Description

Use the `add network` command to connect the required server nodes to a custom network you created. When you set up custom networks between your servers, you create the network first, and then add the required servers to the network. Use the `create network` command to configure additional custom networks.

Options

The following table shows the available options for this command.

Option	Description
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-5 Connecting a Compute Node to a Custom Network

```
PCA> add network MyNetwork ovcacn09r1
Status: Success
```

add network-to-tenant-group

Associates a custom network with an existing tenant group. To create a new tenant group, see create tenant-group. To create a new custom network, see create network.

Syntax

```
add network-to-tenant-group network-name tenant-group-name [OPTIONS]
```

where network-name is the name of an existing custom network, and tenant-group-name is the name of the tenant group you wish to associate the custom network with.

Description

Use the `add network-to-tenant-group` command to connect all member servers of a tenant group to a custom network. The custom network connection is configured when a server joins the tenant group, and unconfigured when a server is removed from the tenant group.

> **Note:**
>
> This command involves verification steps that are performed in the background. Consequently, even though output is returned and you regain control of the CLI, certain operations continue to run for some time.

Options

The following table shows the available options for this command.

Option	Description
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-6 Associating a Custom Network with a Tenant Group

```
PCA> add network-to-tenant-group myPublicNetwork myTenantGroup

Validating servers in the tenant group... This may take some time.

          The job for sync all nodes in tenant group  with the new network
myPublicNetwork has been submitted.
Please look into "/var/log/ovca.log" and "/var/log/ovca-sync.log" to monitor the
progress.

Status: Success
```

add nfs-exception

Adds an NFS exception to allowed clients list for an NFS share. This allows you to control access to the internal ZFS storage appliance by granting exceptions to particular groups of users.

Syntax

```
add nfs-exception network-or-IP-address [OPTIONS]
```

where *nfs-share-name* is the name of the NFS share to which you are granting access using exceptions.

Description

Use the `add nfs-exception` command to grant a client access to the NFS share.

Options

The following table shows the available options for this command.

Option	Description
`network or IP address`	List the IP address or CIDR you want to have access to the share.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-7 Adding an NFS Share Exception

```
PCA> add nfs-exception MyNFSshare 172.16.4.0/24
Status: Success
```

backup

Triggers a manual backup of the Oracle Private Cloud Appliance.

> **Note:**
>
> The backup command can only be executed from the active management node; not from the standby management node.

Syntax

```
backup [OPTIONS]
```

Description

Use the `backup` command to initiate a backup task outside of the usual cron schedule. The backup task performs a full backup of the Oracle Private Cloud Appliance as described in Oracle Private Cloud Appliance Backup. The CLI command does not monitor the progress of the backup task itself, and exits immediately after triggering the task, returning the task ID and name, its initial status, its progress and start time. This command must only ever be run on the active management node.

You can use the `show task` command to view the status of the task after you have initiated the backup. See Example 4-57 for more information.

Options

There are no further options for this command.

Option	Description
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-8 Running a backup task

```
PCA> backup

The backup job has been submitted. Use "show task <task id>" to monitor the progress.

Task_ID         Status  Progress Start_Time           Task_Name
-------         ------  -------- ----------           ---------
3769a13df448a2  RUNNING None     06-05-2019 09:21:36  backup
---------------
1 row displayed

Status: Success
```

create iscsi-storage

Creates a new iSCSI LUN share for a VM storage network.

Syntax

```
create iscsi-storage storage_network_name LUN_size storage-profile [OPTIONS]
```

where *iscsi-LUN-name* is the name of the iSCSI LUN share you wish to create.

Description

Use this command to create an iSCSI LUN share associated with a particular network. This iSCSI LUN share can then be used by Virtual Machines that have access to the specified network.

Options

The following table shows the available options for this command.

Option	Description
`storage_network_name`	The name of the storage network where you wish to create the share.
`share_size`	The size of the share in Gigabytes, for example 100G.
`storage-profile`	Optionally, you can choose a pre-configured storage profile to maximize I/O performance for your environment.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-9 Creating an iSCSI LUN Share

```
PCA> create iscsi-storage my_iscsi_LUN myStorageNnetwork 100G general

Status: Success
```

create lock

Imposes a lock on certain appliance functionality.

> **Caution:**
>
> Never use locks without consultation or specific instructions from Oracle Support.

Syntax

```
create lock lock-type [OPTIONS]
```

Description

Use the `create lock` command to temporarily disable certain appliance-level functions. The lock types are described in the Options.

Options

The following table shows the available options for this command.

Option	Description
`all_provisioning`	Suspend all management node updates and compute node provisioning. Running tasks are completed and stop before the next stage in the process. A daemon checks for locks every few seconds. Once the lock has been removed, the update or provisioning processes continue from where they were halted.
`cn_upgrade`	Prevent all compute node upgrade operations.
`database`	Impose a lock on the databases during the management node update process. The lock is released after the update.
`install`	Placeholder lock type. Currently not used.
`manufacturing`	For usage in manufacturing. This lock type prevents the first boot process from initiating between reboots in the factory. As long as this lock is active, the `ovca` service does not start.
`mn_upgrade`	Prevent all management node upgrade operations.
`provisioning`	Prevent compute node provisioning. If a compute node provisioning process is running, it stops at the next stage. A daemon checks for locks every few seconds. Once the lock has been removed, all nodes advance to the next stage in the provisioning process.
`service`	Placeholder lock type. Behavior is identical to manufacturing lock.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-10 Imposing a Provisioning Lock

```
PCA> create lock provisioning
Status: Success
```

create network

Creates a new custom network, private or public, at the appliance level. See Network Customization for detailed information.

Syntax

```
create network network-name network-type [OPTIONS]
```

where *network-name* is the name of the custom network you wish to create.

If the network type is `external_network`, then the spine switch ports used for public connectivity must also be specified as `port-group`. For this purpose, you must first create an uplink port group. See create uplink-port-group for more information.

If the network type is `storage_network`, then mandatory additional arguments are expected. Enter the prefix, netmask and the [zfs-ipaddress] that is assigned to the ZFS storage appliance network interface.

If the network type is `host_network`, then additional arguments are expected. The subnet arguments are mandatory; the routing arguments are optional.

- `prefix`: defines the fixed part of the host network subnet, depending on the netmask
- `netmask`: determines which part of the subnet is fixed and which part is variable
- `[route-destination]`: the external network location reachable from within the host network, which can be specified as a single valid IPv4 address or a subnet in CIDR notation.
- `[gateway]`: the IP address of the gateway for the static route, which must be inside the host network subnet

The IP addresses of the hosts or physical servers are based on the prefix and netmask of the host network. The final octet is the same as the corresponding internal management IP address. The routing information from the create network command is used to configure a static route on each compute node that joins the host network.

Options

The following table shows the available options for this command.

Option	Description
`{ rack_internal_network | external_network | storage_network | host_network }`	The type of custom network to create. The options are: • a network internal to the rack • a network with external connectivity • a network with external connectivity, accessible for physical hosts • a network with internal connectivity to the ZFS storage appliance
`external_network port-group`	To create a custom network with external connectivity, you must specify the ports on the spine switch as well. The ports must belong to an uplink port group, and you provide the port group name as an argument in this command.
`storage_network prefix netmask [zfs-ipaddress]`	To create a storage network, you must specify the prefix, netmask, and the ip address that is assigned to the ZFS storage appliance network interface.

Option	Description
`host_network port-group prefix netmask [route-destination gateway]`	To create a custom host network, you must specify the ports on the spine switch as with an external network. The ports must belong to an uplink port group, and you provide the port group name as an argument in this command. In addition, the host network requires arguments for its subnet. The routing arguments are optional. All four arguments are explained in the Syntax section above.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-11 Creating an Internal Custom Network

```
PCA> create network MyPrivateNetwork rack_internal_network
Status: Success
```

Example 4-12 Creating a Custom Network with External Connectivity

```
PCA> create network MyPublicNetwork external_network myUplinkPortGroup
Status: Success
```

Example 4-13 Creating a Storage Network

```
PCA> create network MyStorageNetwork storage_network 10.10.10 255.255.255.0 10.10.10.1

Status: Success
```

create nfs-storage

Creates a new NFS storage share for a VM storage network.

Syntax

```
create nfs-storage nfs-share-name storage_network_name share_size storage-
profile [OPTIONS]
```

where *nfs-share-name* is the name of the NFS share you wish to create.

Description

Use this command to create an NFS share accosciated with a particular network. This NFS share can then be used by Virtual Machines that have access to the specified network.

Options

The following table shows the available options for this command.

Option	Description
`storage_network_name`	The name of the storage network where you wish to create the share.
`share_size`	The size of the share in Gigabytes, for example 100G.
`storage-profile`	Optionally, you can choose a pre-configured storage profile to maximize I/O performance for your environment.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-14 Creating an NFS Share

```
PCA> create nfs-storage mySharemyStorageNnetwork 100G general

Status: Success
```

create oci-backup

Creates an on-demand Oracle Cloud Infrastructure dataset backup. For more information, see Configuring a Manual Cloud Backup.

Syntax

```
create oci-backup target-name target-name-2 [OPTIONS]
```

where *target-name* is the name of the Oracle Cloud Infrastructure target where you wish to locate the backup.

Description

Use this command to create an Oracle Cloud Infrastructure backup. You can push a backup to multiple configured targets by listing mutlitple targets with this command. To configure targets, see Configuring the Cloud Backup Service.

Options

The following table shows the available options for this command.

Option	Description
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-15 Creating an Oracle Cloud Infrastructure Backup

```
PCA> create oci-backup OCItarget_1 OCItarget_2

Status: Success
```

create oci-target

Creates an Oracle Cloud Infrastructure target, which is the location on your Oracle Cloud Infrastructure tenancy where you want to store backups.

Syntax

```
create oci-target target-name target-location target-user target-bucket
target-tenancy keyfile [OPTIONS]
```

where *target-name* is the name of the Oracle Cloud Infrastructure target where you wish to locate the backup.

Description

Use this command to create an Oracle Cloud Infrastructure target, and to send scheduled backups to that target. This command creates a cronjob which pushed this backup to the configured target weekly. For more information see Configuring the Cloud Backup Service.

Options

The following table shows the available options for this command.

Option	Description
`target-location`	The object storage endpoint. For a list of available endpoints, see https://docs.oracle.com/en-us/iaas/api/#/en/objectstorage/20160918/.
`target-user`	A user that has access to your Oracle Cloud Infrastructure tenancy.

Option	Description
`target-bucket`	A logical container for storing objects. Users or systems create buckets as needed within a region. See Managing Regions. To create a bucket for the Cloud Backup feature, see Configuring the Cloud Backup Service.
`target-tenancy`	Your Oracle Cloud Infrastructure tenancy where you wish to store backups.
`keyfile`	An API key required to access your Oracle Cloud Infrastructure tenancy. For more information see https://docs.oracle.com/en-us/iaas/Content/API/Concepts/apisigningkey.htm.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-16 Creating an Oracle Cloud Infrastructure Target

```
PCA> create oci-target MyTarget https://objectstorage.us-oci.com
ocid1.user.oc1..oos mybucketocid1.tenancy.oc1..no /root/oci_api_key.pem

Status: Success
```

create tenant-group

Creates a new tenant group. With the tenant group, which exists at the appliance level, a corresponding Oracle VM server pool is created. See Tenant Groups for detailed information.

Syntax

```
create tenant-group tenant-group-name [OPTIONS]
```

where *tenant-group-name* is the name of the tenant group – and server pool – you wish to add to the environment.

Description

Use the `create tenant-group` command to set up a new placeholder for a separate group of compute nodes. The purpose of the tenant group is to group a number of compute nodes in a separate server pool. When the tenant group exists, add the required compute nodes using the `add compute-node` command. If you want to connect all the members of a server pool to a custom network, use the command `add network-to-tenant-group`.

Options

The following table shows the available options for this command.

Option	Description
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-17 Creating a Tenant Group

```
PCA> create tenant-group myTenantGroup

Status: Success
```

create uplink-port-group

Creates a new uplink port group. Uplink port groups define which spine switch ports are used together and in which breakout mode they operate. For detailed information, refer to Network Requirements in the Oracle Private Cloud Appliance Installation Guide.

Syntax

```
create uplink-port-group port-group-name ports port-speed [OPTIONS]
```

where *port-group-name* is the name of the uplink port group, which must be unique. An uplink port group consists of a list of *ports* operating in one of the available breakout modes.

Description

Use the `create uplink-port-group` command to configure the ports reserved on the spine switches for external connectivity. Port 5 is configured and reserved for the default external network; ports 1-4 can be used for custom external networks. The ports can be used at their full 100Gbit bandwidth, at 40Gbit, or split with a breakout cable into four equal breakout ports: 4x 10Gbit or 4x 25Gbit. The port speed is reflected in the breakout mode of the uplink port group.

Options

The following table shows the available options for this command.

Option	Description
`ports`	To create an uplink port group, you must specify which ports on the spine switches belong to the port group. Ports must always be specified in adjacent pairs. They are identified by their port number and optionally, separated by a colon, also their breakout port ID. Put the port identifiers between quotes as a space-separated list, for example: `'1 2'` or `'3:1 3:2'`.
`{ 10g-4x | 25g-4x | 40g | 100g }`	Set the breakout mode of the uplink port group. When a 4-way breakout cable is used, all four ports must be set to either 10Gbit or 25Gbit. When no breakout cable is used, the port speed for the uplink port group should be either 100Gbit or 40Gbit, depending on connectivity requirements.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-18 Creating an Uplink Port Group

```
PCA> create uplink-port-group myUplinkPortGroup '3:1 3:2' 10g-4x
Status: Success

          PCA> create uplink-port-group myStoragePortGroup '1 2' 40g
Status: Success
```

delete config-error

The `delete config-error` command can be used to delete a failed configuration task from the configuration error database.

Syntax

```
delete config-error id [OPTIONS]
```

where *id* is the identifier for the configuration error that you wish to delete from the database.

Description

Use the `delete config-error` command to remove a configuration error from the configuration error database. This is a destructive operation and you are prompted to

confirm whether or not you wish to continue, unless you use the `--confirm` flag to override the prompt.

Once a configuration error has been deleted from the database, you may not be able to re-run the configuration task associated with it. To obtain a list of configuration errors, use the `list config-error` command. See Example 4-44 for more information.

Options

The following table shows the available options for this command.

Option	Description
`--confirm`	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
`--force`	Force the command to be executed even if the target is in an invalid state. This option is not risk-free and should only be used as a last resort.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-19 Removing a Configuration Error

```
PCA> delete config-error 87
************************************************************
 WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
************************************************************
Are you sure [y/N]:y
Status: Success
```

delete iscsi-storage

Deletes an iSCSI LUN share for a VM storage network.

Syntax

```
delete iscsi-storage iscsi-LUN-name
```

where *iscsi-LUN-name* is the name of the iSCSI LUN share you wish to delete.

Description

Use this command to permanently delete an iSCSI LUN share.

Options

The following table shows the available options for this command.

Option	Description
`--confirm`	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
`--force`	Force the command to be executed even if the target is in an invalid state. This option is not risk-free and should only be used as a last resort.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-20 Deleting an iSCSI LUN Share

```
PCA> delete iscsi-storage my_iscsi_LUN

Status: Success
```

delete lock

Removes a lock that was previously imposed on certain appliance functionality.

Syntax

```
delete lock lock-type [OPTIONS]
```

Description

Use the `delete lock` command to re-enable the appliance-level functions that were locked earlier.

Options

The following table shows the available options for this command.

Option	Description
`{ all_provisioning | cn_upgrade | database | install | manufacturing | mn_upgrade | provisioning | service }`	The type of lock to be removed. For a description of lock types, see create lock.

Option	Description
`--confirm`	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
`--force`	Force the command to be executed even if the target is in an invalid state. This option is not risk-free and should only be used as a last resort.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Example

Example 4-21 Unlocking Provisioning

```
PCA> delete lock provisioning
************************************************************
 WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
************************************************************
Are you sure [y/N]:y
Status: Success
```

delete network

Deletes a custom network. See Network Customization for detailed information.

Syntax

```
delete network network-name [OPTIONS]
```

where *network-name* is the name of the custom network you wish to delete.

Description

Use the `delete network` command to remove a previously created custom network from your environment. This is a destructive operation and you are prompted to confirm whether or not you wish to continue, unless you use the --confirm flag to override the prompt.

A custom network can only be deleted after all servers have been removed from it. See remove network.

Default Oracle Private Cloud Appliance networks are protected and any attempt to delete them will fail.

Options

The following table shows the available options for this command.

Option	Description
`--confirm`	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
`--force`	Force the command to be executed even if the target is in an invalid state. This option is not risk-free and should only be used as a last resort.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-22 Deleting a Custom Network

```
PCA> delete network MyNetwork
************************************************************
 WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
************************************************************
Are you sure [y/N]:y
Status: Success
```

Example 4-23 Attempting to Delete a Default Network

```
PCA> delete network default_internal
Status: Failure
Error Message: Error (NETWORK_003): Exception while deleting network:
default_internal.
['INVALID_NAME_002: Invalid Network name: default_internal. Name is reserved.']
```

delete nfs-storage

Deletes an NFS storage share for a VM storage network.

Syntax

```
delete nfs-storage nfs-share-name
```

where nfs-share-name is the name of the NFS storage share you wish to delete.

Description

Use this command to permanently delete an NFS storage share.

Options

The following table shows the available options for this command.

Option	Description
`--confirm`	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
`--force`	Force the command to be executed even if the target is in an invalid state. This option is not risk-free and should only be used as a last resort.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-24 Deleting an NFS Storage Share

```
PCA> delete nfs-storage myStorageShare

Status: Success
```

delete oci-backup

Deletes an Oracle Cloud Infrastructure dataset backup. For more information, see Deleting Cloud Backups.

Syntax

```
delete oci-backup oci-backup-name [OPTIONS]
```

where *oci-backup-name* is the name of the Oracle Cloud Infrastructure backup you wish to delete.

Description

Use this command to permanently delete an Oracle Cloud Infrastructure backup.

Options

The following table shows the available options for this command.

Option	Description
`--confirm`	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.

Option	Description
`--force`	Force the command to be executed even if the target is in an invalid state. This option is not risk-free and should only be used as a last resort.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-25 Deleting an Oracle Cloud Infrastructure Backup

```
PCA> delete oci-backup myOCIbackup

Status: Success
```

delete oci-target

Deletes an Oracle Cloud Infrastructure target from your ZFS storage appliance. For more information see Deleting Oracle Cloud Infrastructure Targets .

Syntax

```
delete oci-target oci-target-name [OPTIONS]
```

where *oci-target-name* is the name of the Oracle Cloud Infrastructure target you wish to delete.

Description

Use this command to permanently delete an Oracle Cloud Infrastructure target.

Options

The following table shows the available options for this command.

Option	Description
`--confirm`	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
`--force`	Force the command to be executed even if the target is in an invalid state. This option is not risk-free and should only be used as a last resort.
`--json`	Return the output of the command in JSON format

Option	Description
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-26 Deleting an Oracle Cloud Infrastructure Target

```
PCA> delete nfs-storage myStorageShare

Status: Success
```

delete task

The `delete` command can be used to delete a task from the database.

Syntax

```
delete task id
```

where *id* is the identifier for the task that you wish to delete from the database.

Description

Use the `delete task` command to remove a task from the task database. This is a destructive operation and you are prompted to confirm whether or not you wish to continue, unless you use the `--confirm` flag to override the prompt.

Options

The following table shows the available options for this command.

Option	Description
`--confirm`	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
`--force`	Force the command to be executed even if the target is in an invalid state. This option is not risk-free and should only be used as a last resort.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.

Option	Description
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-27 Removing a Task

```
PCA> delete task 341e7bc74f339c
************************************************************
 WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
************************************************************
Are you sure [y/N]:y
Status: Success
```

delete tenant-group

Deletes a tenant group. The default tenant group cannot be deleted. See Tenant Groups for detailed information.

Syntax

```
delete tenant-group tenant-group-name [OPTIONS]
```

where *tenant-group-name* is the name of the tenant group – and server pool – you wish to add to the environment.

Description

Use the `delete tenant-group` command to remove a previously created, non-default tenant group from your environment. All servers must be removed from the tenant group before it can be deleted. When the tenant group is deleted, the server pool file system is removed from the internal ZFS storage.

This is a destructive operation and you are prompted to confirm whether or not you wish to continue, unless you use the `--confirm` flag to override the prompt.

Options

The following table shows the available options for this command.

Option	Description
`--confirm`	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
`--force`	Force the command to be executed even if the target is in an invalid state. This option is not risk-free and should only be used as a last resort.
`--json`	Return the output of the command in JSON format

Option	Description
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-28 Deleting a Tenant Group

```
PCA> delete tenant-group myTenantGroup
************************************************************
 WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
************************************************************
Are you sure [y/N]:y
Status: Success
```

delete uplink-port-group

Deletes an uplink port group. See create uplink-port-group for more information about the use of uplink port groups.

Syntax

```
delete uplink-port-group port-group-name [OPTIONS]
```

where *port-group-name* is the name of the uplink port group you wish to remove from the environment.

Description

Use the `delete uplink-port-group` command to remove a previously created uplink port group from your environment. If the uplink port group is used in the configuration of a network, this network must be deleted before the uplink port group can be deleted. Otherwise the delete command will fail.

This is a destructive operation and you are prompted to confirm whether or not you wish to continue, unless you use the `--confirm` flag to override the prompt.

Options

The following table shows the available options for this command.

Option	Description
`--confirm`	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.

Option	Description
`--force`	Force the command to be executed even if the target is in an invalid state. This option is not risk-free and should only be used as a last resort.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-29 Deleting an Uplink Port Group

```
PCA> delete uplink-port-group myUplinkPortGroup
************************************************************
 WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
************************************************************
Are you sure [y/N]:y
Status: Success
```

deprovision compute-node

Cleanly removes a previously provisioned compute node's records in the various configuration databases. A provisioning lock must be applied in advance, otherwise the node is reprovisioned shortly after deprovisioning.

Syntax

```
deprovision compute-node compute-node-name [OPTIONS]
```

where *compute-node-name* is the name of the compute node you wish to remove from the appliance configuration.

Description

Use the `deprovision compute-node` command to take an existing compute node out of the appliance in such a way that it can be repaired or replaced, and subsequently rediscovered as a brand new component. The compute node configuration records are removed cleanly from the system.

> **Caution:**
>
> For deprovisioning to succeed, the compute node ILOM password must be the default password. If this is not the case, the operation may result in an error. This also applies to reprovisioning an existing compute node.

By default, the command does not continue if the compute node contains running VMs. The correct workflow is to impose a provisioning lock before deprovisioning a compute node, otherwise it is rediscovered and provisioned again shortly after deprovisioning has completed. When the appliance is ready to resume its normal operations, release the provisioning lock again. For details, see create lock and delete lock.

This is a destructive operation and you are prompted to confirm whether or not you wish to continue, unless you use the `--confirm` flag to override the prompt.

Options

The following table shows the available options for this command.

Option	Description
`--confirm`	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
`--force`	Force the command to be executed even if the target is in an invalid state. This option is not risk-free and should only be used as a last resort.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-30 Deprovisioning a Compute Node

```
deprovision compute-node ovcacn29r1
************************************************************
 WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
************************************************************
Are you sure [y/N]:y
Shutting down dhcpd:                                [ OK ]
Starting dhcpd:                                     [ OK ]
Shutting down dnsmasq:                              [ OK ]
Starting dnsmasq:                                   [ OK ]

Status: Success
```

diagnose

Performs various diagnostic checks against the Oracle Private Cloud Appliance for support purposes.

> **Caution:**
>
> The `diagnose software` command is deprecated. It will be removed in the next release of the Oracle Private Cloud Appliance Controller Software. Diagnostic functions are now available through a separate health check tool. See Health Monitoring for more information.
>
> The other `diagnose` commands remain functional.

Syntax

```
diagnose { ilom | software | hardware | rack-monitor } [OPTIONS]
```

The following table describes each possible target of the `diagnose` command.

Command Target	Information Displayed
`hardware`	The `hardware` diagnostic has two further options: • The `rack` option displays status information for rack components that were pingable at least once in the lifetime of the rack. The command output is real-time information. If required, the results can be filtered by component type (cn, ilom, mn, etc.) Use tab completion to see all component types available. • The `reset` option must be followed by a component host name. The command resets the event counters in the monitor database to zero for the component in question. If a component is or was in critical state, the reset command re-enables monitoring for that component.
`ilom`	The `ilom` diagnostic checks that the ILOM for each component is accessible on the management network.
`leaf-switch`	The `leaf-switch diagnostic` performs health checks on the leaf switches.
`leaf-switch-resources`	The `leaf-switch-resource` diagnostic checks the CPU and memory status of each leaf switch.

Command Target	Information Displayed
`link-status`	The `link-status` diagnostic returns the status of the leaf switch link ports.
`rack-monitor`	The `rack-monitor` diagnostic checks for errors that may have been registered by the monitor service. Optionally these can be filtered per component category. If required, the results can be filtered by component type (cn, ilom, mn, etc.) Use tab completion to see all component types available.
`software`	The `software` diagnostic triggers the Oracle Private Cloud Appliance software acceptance tests.
`spine-switch`	The `spine-switch` diagnostic performs health checks on the spine switch.
`spine-switch-resources`	The `spine-switch`-resource diagnostic checks the CPU and memory status of the spine switch.
`switch-logs`	The `switch-logs` diagnostic has two further options: • The `process` option displays information for the processes run on the switches. • The `core` option displays information about core dumps. Access the switch directly for log details.
`uplink-port-statistics`	The `uplink-port-statistics` diagnostic displays north-south data traffic statistics for the spine switches.

Description

Use the `diagnose` command to initiate a diagnostic check of various components that make up Oracle Private Cloud Appliance.

A large part of the diagnostic information is stored in the inventory database and the monitor database. The inventory database is populated from the initial rack installation and keeps a history log of all the rack components. The monitor database stores rack component events detected by the monitor service. Some of the diagnostic commands are used to display the contents of these databases.

Options

The following table shows the available options for this command.

Option	Description
`--force`	Force the command to be executed even if the target is in an invalid state. This option is not risk-free and should only be used as a last resort.

Option	Description
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.
`--tests=TESTS`	Returns the output of specific tests you designate, rather than running the full set of tests.
`--version=VERSION`	Defines what version of software the command will run on. The default version is 2.4.2, but you can run the command on other version you specify here.

Examples

Example 4-31 Running the ILOM Diagnostic

```
PCA> diagnose ilom
Checking ILOM health.....please wait..

IP_Address      Status          Health_Details
----------      ------          --------------
192.168.4.129   Not Connected   None
192.168.4.128   Not Connected   None
192.168.4.127   Not Connected   None
192.168.4.126   Not Connected   None
192.168.4.125   Not Connected   None
192.168.4.124   Not Connected   None
192.168.4.123   Not Connected   None
192.168.4.122   Not Connected   None
192.168.4.121   Not Connected   None
192.168.4.120   Not Connected   None
192.168.4.101   OK              None
192.168.4.102   OK              None
192.168.4.105   Faulty          Mon Nov 25 14:17:37 2013  Power    PS1 (Power
Supply 1)
                                A loss of AC input to a power supply has

occurred.
                                (Probability: 100, UUID: 2c1ec5fc-ffa3-c768-e602-

ca12b86e3ea1,
                                Part Number: 07047410, Serial Number:

476856F+1252CE027X,
                                Reference Document: http://www.sun.com/msg/

SPX86-8003-73)
192.168.4.107   OK              None
192.168.4.106   OK              None
192.168.4.109   OK              None
192.168.4.108   OK              None
192.168.4.112   OK              None
192.168.4.113   Not Connected   None
192.168.4.110   OK              None
```

```
192.168.4.111   OK              None
192.168.4.116   Not Connected   None
192.168.4.117   Not Connected   None
192.168.4.114   Not Connected   None
192.168.4.115   Not Connected   None
192.168.4.118   Not Connected   None
192.168.4.119   Not Connected   None
-----------------
27 rows displayed

Status: Success
```

Example 4-32 Running the Software Diagnostic

```
PCA> diagnose software
PCA Software Acceptance Test runner utility
Test -  01 - OpenSSL CVE-2014-0160 Heartbleed bug Acceptance [PASSED]
Test -  02 - PCA package Acceptance [PASSED]
Test -  03 - Shared Storage Acceptance [PASSED]
Test -  04 - PCA services Acceptance [PASSED]
Test -  05 - PCA config file Acceptance [PASSED]
Test -  06 - Check PCA DBs exist Acceptance [PASSED]
Test -  07 - Compute node network interface Acceptance [PASSED]
Test -  08 - OVM manager settings Acceptance [PASSED]
Test -  09 - Check management nodes running Acceptance [PASSED]
Test -  10 - Check OVM manager version Acceptance [PASSED]
Test -  11 - OVM server model Acceptance [PASSED]
Test -  12 - Repositories defined in OVM manager Acceptance [PASSED]
Test -  13 - Management Nodes have IPv6 disabled [PASSED]
Test -  14 - Bash Code Injection Vulnerability bug Acceptance [PASSED]
Test -  15 - Check Oracle VM 3.4 xen security update Acceptance [PASSED]
Test -  16 - Test for ovs-agent service on CNs Acceptance [PASSED]
Test -  17 - Test for shares mounted on CNs Acceptance [PASSED]
Test -  18 - All compute nodes running Acceptance [PASSED]
Test -  19 - PCA version Acceptance [PASSED]
Test -  20 - Check support packages in PCA image Acceptance [PASSED]

Status: Success
```

Example 4-33 Running the Leaf-Switch Diagnostic

```
PCA> diagnose leaf-switch

Switch      Health Check Name                   Status
------      -----------------                   ------
ovcasw15r1  CDP Neighbor Check                  Passed
ovcasw15r1  Virtual Port-channel check          Passed
ovcasw15r1  Management Node Port-channel check  Passed
ovcasw15r1  Leaf-Spine Port-channel check       Passed
ovcasw15r1  OSPF Neighbor Check                 Passed
ovcasw15r1  Multicast Route Check               Passed
ovcasw15r1  Leaf Filesystem Check               Passed
ovcasw15r1  Hardware Diagnostic Check           Passed
ovcasw16r1  CDP Neighbor Check                  Passed
ovcasw16r1  Virtual Port-channel check          Passed
ovcasw16r1  Management Node Port-channel check  Passed
ovcasw16r1  Leaf-Spine Port-channel check       Passed
ovcasw16r1  OSPF Neighbor Check                 Passed
ovcasw16r1  Multicast Route Check               Passed
ovcasw16r1  Leaf Filesystem Check               Passed
ovcasw16r1  Hardware Diagnostic Check           Passed
```

```
-----------------
16 rows displayed

Status: Success
```

get log

Retrieves the log files from the selected components and saves them to a directory on the rack's shared storage.

> **Note:**
>
> Currently the spine or data switch is the only target component supported with this command.

Syntax

```
get log component [OPTIONS]
```

where *component* is the identifier of the rack component from which you want to retrieve the log files.

Description

Use the `get log` command to collect the log files of a given rack component or set of rack components of a given type. The command output indicates where the log files are saved: this is a directory on the internal storage appliance in a location that both management nodes can access. From this location you can examine the logs or copy them to your local system so they can be included in your communication with Oracle.

Options

The following table shows the available options for this command.

Option	Description
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-34 Collecting the Log Files from the Spine Switch

Note that the CLI uses 'data_switch' as the internal alias for a spine Cisco Nexus 9336C-FX2 Switch.

```
PCA> get log data_switch
Log files copied to: /nfs/shared_storage/incoming
Status: Success
```

list

The `list` command can be used to list the different components and tasks within the Oracle Private Cloud Appliance. The output displays information relevant to each component or task. Output from the list command is usually tabulated so that different fields appear as columns for each row of information relating to the command target.

Syntax

```
list target [OPTIONS]
```

The following table describes each possible target of the `list` command.

Command Target	Information Displayed
`backup-task`	Displays basic information about all backup tasks.
`compute-node`	Displays basic information for all compute nodes installed.
`config-error`	Displays all configuration tasks that were not completed successfully and ended in an error.
`iscsi-storage`	Displays all iSCSI LUNs for storage.
`lock`	Displays all locks that have been imposed.
`management-node`	Displays basic information for both management nodes.
`mgmt-switch-port`	Displays connection information about every port in the Oracle Private Cloud Appliance environment belonging to the internal administration or management network. The ports listed can belong to a switch, a server node or any other connected rack component type.
`network`	Displays all networks configured in the environment.
`network-port`	Displays the status of all ports on all I/O modules installed in the networking components.
`network-switch`	Displays basic information about all switches installed in the Oracle Private Cloud Appliance environment.
`nfs-storage`	Displays NFS shares for storage.
`oci-backup`	Displays all the Oracle Cloud Infrastructure backups.

Command Target	Information Displayed
`storage-network`	Displays a list of known storage networks.
`storage-profile`	Displays all the storage profiles.
`task`	Displays a list of running, completed and failed tasks.
`tenant-group`	Displays all configured tenant groups. The list includes the default configuration as well as custom tenant groups.
`update-task`	Displays a list of all software update tasks that have been started on the appliance.
`uplink-port`	Displays information about spine switch port configurations for external networking.
`uplink-port-group`	Displays information about all uplink port groups configured for external networking.

Note that you can use tab completion to help you correctly specify the object for the different command targets. You do not need to specify an object if the command target is system-properties or version.

Description

Use the `list` command to obtain tabulated listings of information about different components or activities within the Oracle Private Cloud Appliance. The `list` command can frequently be used to obtain identifiers that can be used in conjunction with many other commands to perform various actions or to obtain more detailed information about a specific component or task. The `list` command also supports sorting and filtering capabilities to allow you to order information or to limit information so that you are able to identify specific items of interest quickly and easily.

Options

The following table shows the available options for this command.

Option	Description
`list { backup-task | compute-node | config-error | iscsi-storage | lock | management-node | mgmt-switch-port | network | network-card | network-port | network-switch | nfs-storage | oci-backup | oci-target | ofm-network | opus-port | storage-network | storage-profile | task | tenant-group | update-task | uplink-port | uplink-port-group | wwpn-info } [--json] [--less] [--more] [--tee=OUTPUTFILENAME] [[--sorted-by SORTEDBY | --sorted-order SORTEDORDER]] [[--filter-column FILTERCOLUMN | --filter FILTER]]`	The command target to list information for.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.
`[ --sorted-by SORTEDBY ]`	Sort the table by the values within a particular column in the table, specified by replacing `SORTEDBY` with the name of the column that should be used to perform the sort. See Sorting for more information.
`[ --sorted-order SORTEDORDER ]`	Used to specify the sort order, which can either be `ASC` for an ascending sort, or `DES` for a descending sort. You must use the `--sorted-by` option in conjunction with this option.
`[ --filter-column FILTERCOLUMN ]`	Filter the table for a value within a particular column in the table, specified by replacing `FILTERCOLUMN` with the name of the column that should be used to perform the sort. You must use the `--filter` option in conjunction with this option. See Filtering for more information.
`[ --filter FILTER ]`	The filter that should be applied to values within the column specified by the `--filter-column` option.

Examples

Example 4-35 List all management nodes

```
PCA> list management-node

Management_Node IP_Address   Provisioning_Status  ILOM_MAC
Provisioning_State   Master
--------------- ----------   -------------------  --------
------------------   ------
ovcamn05r1      192.168.4.3  RUNNING              00:10:e0:e9:1f:c9
running              None
ovcamn06r1      192.168.4.4  RUNNING              00:10:e0:e7:26:ad
running              Yes
----------------
2 rows displayed

Status: Success
```

Example 4-36 List all compute nodes

```
PCA> list compute-node
Compute_Node  IP_Address    Provisioning_Status  ILOM_MAC
Provisioning_State
------------  ----------    -------------------  --------
------------------
ovcacn10r1    192.168.4.7   RUNNING              00:10:e0:65:2f:4b   running
ovcacn08r1    192.168.4.5   RUNNING              00:10:e0:65:2f:f3
initializing_stage_wait_...
ovcacn09r1    192.168.4.10  RUNNING              00:10:e0:62:98:e3   running
ovcacn07r1    192.168.4.8   RUNNING              00:10:e0:65:2f:93   running
----------------
4 rows displayed

Status: Success
```

Example 4-37 List All Tenant Groups

```
PCA> list tenant-group

Name                Default      State
----                -------      -----
Rack1_ServerPool    True         ready
myTenantGroup       False        ready
----------------
2 rows displayed

Status: Success
```

Example 4-38 List Appliance Networks

```
PCA> list network

Network_Name          Default      Type                   Trunkmode
Description
------------          -------      ----                   ---------
-----------
custom_internal       False        rack_internal_network  None         None
default_internal      True         rack_internal_network  None         None
storage_net           False        host_network           None         None
default_external      True         external_network       None         None
----------------
4 rows displayed
```

```
Status: Success
```

Example 4-39 List the Network Ports Configured on the Spine Cisco Nexus 9336C-FX2 Switches

```
PCA> list network-port

Port      Switch          Type                 State          Networks
----      ------          ----                 -----          --------
1         ovcasw22r1      40G                  up             storage_net
2         ovcasw22r1      40G                  up             storage_net
3         ovcasw22r1      auto-speed           down           None
4         ovcasw22r1      auto-speed           down           None
5:1       ovcasw22r1      10G                  up             default_external
5:2       ovcasw22r1      10G                  down           default_external
5:3       ovcasw22r1      10G                  down           None
5:4       ovcasw22r1      10G                  down           None
1         ovcasw23r1      40G                  up             storage_net
2         ovcasw23r1      40G                  up             storage_net
3         ovcasw23r1      auto-speed           down           None
4         ovcasw23r1      auto-speed           down           None
5:1       ovcasw23r1      10G                  up             default_external
5:2       ovcasw23r1      10G                  down           default_external
5:3       ovcasw23r1      10G                  down           None
5:4       ovcasw23r1      10G                  down           None
-----------------
16 rows displayed

Status: Success
```

Example 4-40 List Ports on the Management Cisco Nexus 9348GC-FXP Switch Using a Filter

Note that the CLI uses the internal alias `mgmt-switch-port`. In this example the command displays all internal Ethernet connections from compute nodes to the Cisco Nexus 9348GC-FXP Switch. A wildcard is used in the --filter option.

```
PCA> list mgmt-switch-port --filter-column=Hostname --filter=*cn*r1

Dest      Dest_Port  Hostname       Key          MGMTSWITCH RACK  RU    Src_Port   Type
----      ---------  --------       ---          ---------- ----  --    --------   ----
07        Net-0      ovcacn07r1     CISCO-1-5    CISCO-1    1     7     5
compute
08        Net-0      ovcacn08r1     CISCO-1-6    CISCO-1    1     8     6
compute
09        Net-0      ovcacn09r1     CISCO-1-7    CISCO-1    1     9     7
compute
10        Net-0      ovcacn10r1     CISCO-1-8    CISCO-1    1     10    8
compute
11        Net-0      ovcacn11r1     CISCO-1-9    CISCO-1    1     11    9
compute
12        Net-0      ovcacn12r1     CISCO-1-10   CISCO-1    1     12    10
compute
13        Net-0      ovcacn13r1     CISCO-1-11   CISCO-1    1     13    11
compute
14        Net-0      ovcacn14r1     CISCO-1-12   CISCO-1    1     14    12
compute
34        Net-0      ovcacn34r1     CISCO-1-15   CISCO-1    1     34    15
compute
35        Net-0      ovcacn35r1     CISCO-1-16   CISCO-1    1     35    16
```

```
compute
36          Net-0       ovcacn36r1      CISCO-1-17 CISCO-1    1     36
17          compute
37          Net-0       ovcacn37r1      CISCO-1-18 CISCO-1    1     37
18          compute
38          Net-0       ovcacn38r1      CISCO-1-19 CISCO-1    1     38
19          compute
39          Net-0       ovcacn39r1      CISCO-1-20 CISCO-1    1     39
20          compute
40          Net-0       ovcacn40r1      CISCO-1-21 CISCO-1    1     40
21          compute
41          Net-0       ovcacn41r1      CISCO-1-22 CISCO-1    1     41
22          compute
42          Net-0       ovcacn42r1      CISCO-1-23 CISCO-1    1     42
23          compute
26          Net-0       ovcacn26r1      CISCO-1-35 CISCO-1    1     26
35          compute
27          Net-0       ovcacn27r1      CISCO-1-36 CISCO-1    1     27
36          compute
28          Net-0       ovcacn28r1      CISCO-1-37 CISCO-1    1     28
37          compute
29          Net-0       ovcacn29r1      CISCO-1-38 CISCO-1    1     29
38          compute
30          Net-0       ovcacn30r1      CISCO-1-39 CISCO-1    1     30
39          compute
31          Net-0       ovcacn31r1      CISCO-1-40 CISCO-1    1     31
40          compute
32          Net-0       ovcacn32r1      CISCO-1-41 CISCO-1    1     32
41          compute
33          Net-0       ovcacn33r1      CISCO-1-42 CISCO-1    1     33
42          compute
-----------------
25 rows displayed

Status: Success
```

Example 4-41 List All Tasks

```
PCA> list task

Task_ID         Status  Progress Start_Time           Task_Name
-------         ------  -------- ----------           ---------
376a676449206a  SUCCESS      100 06-06-2019 09:00:01  backup
376ce11fc6c39c  SUCCESS      100 06-06-2019 04:23:41  update_download_image
376a02cf798f68  SUCCESS      100 06-05-2019 21:00:02  backup
376c7c8afcc86a  SUCCESS      100 06-05-2019 09:00:01  backup
----------------
4 rows displayed

Status: Success
```

Example 4-42 List Uplink Ports to Configure External Networking

```
PCA> list uplink-port

Interface Name  Switch       Status    Admin_Status  PortChannel  Speed
--------------  ------       ------    ------------  -----------  -----
Ethernet1/1     ovcasw22r1   up        up            111          40G
Ethernet1/1     ovcasw23r1   up        up            111          40G
Ethernet1/2     ovcasw22r1   up        up            111          40G
Ethernet1/2     ovcasw23r1   up        up            111          40G
```

```
Ethernet1/3     ovcasw22r1   down      down          None         auto
Ethernet1/3     ovcasw23r1   down      down          None         auto
Ethernet1/4     ovcasw22r1   down      down          None         auto
Ethernet1/4     ovcasw23r1   down      down          None         auto
Ethernet1/5/1   ovcasw22r1   up        up            151          10G
Ethernet1/5/1   ovcasw23r1   up        up            151          10G
Ethernet1/5/2   ovcasw22r1   down      up            151          10G
Ethernet1/5/2   ovcasw23r1   down      up            151          10G
Ethernet1/5/3   ovcasw22r1   down      down          None         10G
Ethernet1/5/3   ovcasw23r1   down      down          None         10G
Ethernet1/5/4   ovcasw22r1   down      down          None         10G
Ethernet1/5/4   ovcasw23r1   down      down          None         10G
-----------------
16 rows displayed

Status: Success
```

Example 4-43 List Uplink Port Groups

```
PCA> list uplink-port-group

Port_Group_Name    Ports      Mode    Speed    Breakout_Mode    Enabled   State
---------------    -----      ----    -----    -------------    -------   -----
default_5_1        5:1 5:2    LAG     10g      10g-4x           True      (up)* Not
all ports are up
default_5_2        5:3 5:4    LAG     10g      10g-4x           False     down
----------------
2 rows displayed

Status: Success
```

Example 4-44 List All Configuration Errors

```
PCA> list config-error

ID        Module                      Host             Timestamp
--        ------                      ----             ---------
87        Management node password    192.168.4.4      Mon Jun 03 02:45:42 2019
54        MySQL management password   192.168.4.216    Mon Jun 03 02:44:54 2019
----------------
2 rows displayed

Status: Success
```

Example 4-45 List All Storage Profiles

```
PCA> list storage-profile

Name             Type             Default
----             ----             -------
dbms_demo        iscsi            N
general          iscsi            Y
bkup_basic       iscsi            N
general          nfs              Y
bkup_basic       nfs              N
dbms_demo        nfs              N
----------------
6 rows displayed

Status: Success
```

remove compute-node

Removes a compute node from an existing tenant group.

Syntax

```
remove compute-node node tenant-group-name [OPTIONS]
```

where *tenant-group-name* is the name of the tenant group you wish to remove one or more compute nodes from, and *node* is the name of the compute node that should be removed from the selected tenant group.

Description

Use the `remove compute-node` command to remove the required compute nodes from their tenant group. Use Oracle VM Manager to prepare the compute nodes first: make sure that virtual machines have been migrated away from the compute node, and that no storage repositories are presented. Custom networks associated with the tenant group are removed from the compute node, not from the tenant group.

This is a destructive operation and you are prompted to confirm whether or not you wish to continue, unless you use the `--confirm` flag to override the prompt.

Options

The following table shows the available options for this command.

Option	Description
`--confirm`	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
`--force`	Force the command to be executed even if the target is in an invalid state. This option is not risk-free and should only be used as a last resort.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-46 Removing a Compute Node from a Tenant Group

```
PCA> remove compute-node ovcacn09r1 myTenantGroup
************************************************************
 WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
```

```
************************************************************
Are you sure [y/N]:y

Status: Success
```

remove initiator

Removes an initiator from an iSCSI LUN, thereby removing access to the iSCSI LUN from that initiator.

Syntax

```
remove initiator initiator-IQN LUN-name [OPTIONS]
```

LUN-name is the name of the iSCSI LUN share to which you are revoking access for the listed initiator.

Description

Use the `remove initiator` command to remove an initiator from an iSCSI LUN.

Options

The following table shows the available options for this command.

Option	Description
initiator-IQN	List the initiator IQN from the virtual machine that should no longer have access to the LUN.
LUN-name	Specify the LUN you want remove the initiator from.
`--confirm`	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
`--force`	Force the command to be executed even if the target is in an invalid state. This option is not risk-free and should only be used as a last resort.
`--json`	Return the output of the command in JSON format.
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=`***OUTPUTFILENAME***	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-47 Removing an Initiator From a LUN

```
PCA> remove initiator iqn.example.com myLUN
Status: Success
```

remove network

Disconnects a server node from a network.

Syntax

```
remove network network-name node [OPTIONS]
```

where *network-name* is the name of the network from which you wish to disconnect one or more servers, and *node* is the name of the server node that should be disconnected from the selected network.

Description

Use the `remove network` command to disconnect server nodes from a custom network you created. In case you want to delete a custom network from your environment, you must first disconnect all the servers from that network. Then use the `delete network` command to delete the custom network configuration. This is a destructive operation and you are prompted to confirm whether or not you wish to continue, unless you use the `--confirm` flag to override the prompt.

Options

The following table shows the available options for this command.

Option	Description
`--confirm`	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
`--force`	Force the command to be executed even if the target is in an invalid state. This option is not risk-free and should only be used as a last resort.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-48 Disconnecting a Compute Node from a Custom Network

```
PCA> remove network MyNetwork
                    ovcacn09r1
************************************************************
 WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
************************************************************
```

```
Are you sure [y/N]:y
Status: Success
```

remove network-from-tenant-group

Removes a custom network from a tenant group.

Syntax

```
remove network-from-tenant-group network-name tenant-group-name [OPTIONS]
```

where *network-name* is the name of a custom network associated with a tenant group, and *tenant-group-name* is the name of the tenant group you wish to remove the custom network from.

Description

Use the `remove network-from-tenant-group` command to break the association between a custom network and a tenant group. The custom network is unconfigured from all tenant group member servers.

This is a destructive operation and you are prompted to confirm whether or not you wish to continue, unless you use the `--confirm` flag to override the prompt.

Options

The following table shows the available options for this command.

Option	Description
`--confirm`	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
`--force`	Force the command to be executed even if the target is in an invalid state. This option is not risk-free and should only be used as a last resort.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-49 Removing a Custom Network from a Tenant Group

```
PCA> remove network-from-tenant-group myPublicNetwork
                 myTenantGroup
************************************************************
 WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
```

```
************************************************************
Are you sure [y/N]:y

Status: Success
```

remove nfs exceptions

Removes an NFS exception, thereby removing access to the NFS share from the listed machine.

Syntax

```
remove nfs-exception nfs-share-name [OPTIONS]
```

where ***nfs-share-name*** is the name of the NFS share to which you are granting access using exceptions.

Description

Use the `remove nfs-exception` command to remove an `nfs-exception` from a share.

Options

The following table shows the available options for this command.

Option	Description
`network or IP address`	List the IP address or CIDR that should no longer have access to the share.
`--confirm`	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
`--force`	Force the command to be executed even if the target is in an invalid state. This option is not risk-free and should only be used as a last resort.
`--json`	Return the output of the command in JSON format.
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=`***OUTPUTFILENAME***	When returning the output of the command, also write the output to the specified output file.

Examples

Example 4-50 Removing an NFS Exception From a Share

```
PCA> remove nfs-exception myNFSshare 172.16.4.0/24
Status: Success
```

reprovision

The `reprovision` command can be used to trigger reprovisioning for a specified compute node within the Oracle Private Cloud Appliance.

> **Caution:**
>
> Reprovisioning restores a compute node to a clean state. If a compute node was previously added to the Oracle VM environment and has active connections to storage repositories other than those on the internal ZFS storage, the external storage connections need to be configured again after reprovisioning.

Syntax

```
reprovision compute-node node-name [OPTIONS]
```

where *node-name* is the compute node name for the compute node that should be reprovisioned.

Description

Use the `reprovision` command to reprovision a specified compute node. The provisioning process is described in more detail in Provisioning and Orchestration.

The `reprovision` command triggers a task that is responsible for handling the reprovisioning process and exits immediately with status 'Success' if the task has been successfully generated. This does not mean that the reprovisioning process itself has completed successfully. To monitor the status of the reprovisioning task, you can use the `list compute-node` command to check the provisioning state of the servers. You can also monitor the log file for information relating to provisioning tasks. The location of the log file can be obtained by checking the Log_File parameter when you run the `show system-properties` command. See Example 4-56 for more information.

Options

The following table shows the available options for this command.

Option	Description
`compute-node`	The command target to perform the reprovision operation against.
`--save-local-repo`	Skip the HMP step in the provisioning process in order to save the local storage repository.
`--json`	Return the output of the command in JSON format.
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.

Option	Description
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--force`	Force the command to be executed even if the target is in an invalid state. This option is not risk-free and should only be used as a last resort.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-51 Reprovisioning a Compute Node

> **Caution:**
>
> Do not force reprovisioning on a compute node with running virtual machines because they will be left in an indeterminate state.

```
PCA> reprovision compute-node ovcacn11r1
The reprovision job has been submitted.
Use "show compute-node <compute node name>" to monitor the progress.
Status: Success
```

rerun

Triggers a configuration task to re-run on the Oracle Private Cloud Appliance.

Syntax

```
rerun config-task id [OPTIONS]
```

where *id* is the identifier for the configuration task that must be re-run.

Description

Use the `rerun` command to re-initiate a configuration task that has failed. Use the `list config-error` command to view the configuration tasks that have failed and the associated identifier that you should use in conjunction with this command. See Example 4-44 for more information.

Options

The following table shows the available options for this command.

Option	Description
`config-task`	The command target to perform the rerun operation against.
`--json`	Return the output of the command in JSON format

Option	Description
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-52 Re-run a configuration task

```
PCA> rerun config-task 84
Status: Success
```

set system-property

Sets the value for a system property on the Oracle Private Cloud Appliance.

Syntax

```
set system-property property-name value [OPTIONS]
```

where *property-name* is the system property you want to change, and *value* is the value for the system property that you are setting.

Description

Use the `set system-property` command to set the value for a system property on the Oracle Private Cloud Appliance.

> **Important:**
>
> The `set system-property` command only affects the settings for the management node where it is run. If you change a setting on the active management node, using this command, you should connect to the passive management node and run the equivalent command there as well, to keep the two systems synchronized. This is the only exception where it is necessary to run a CLI command on the passive management node.

You can use the `show system-properties` command to view the values of various system properties at any point. See Example 4-56 for more information.

Important:

Changes to system-properties usually require that you restart the service for the change to take effect. To do this, you must run `service ovca restart` in the shell of the active management node after you have set the system property value.

Options

The following table shows the available options for this command.

Option	Description
`ftp_proxy`	Set the value for the IP address of an FTP Proxy
`http_proxy`	Set the value for the IP address of an HTTP Proxy
`https_proxy`	Set the value for the IP address of an HTTPS Proxy
`log_count`	Set the value for the number of log files that should be retained through log rotation
`log_file`	Set the value for the location of a particular log file. **Caution:** Make sure that the new path to the log file exists. Otherwise, the log server stops working. The system always prepends `/var/log` to your entry. Absolute paths are converted to `/var/log/`***`<path>`*** . This property can be defined separately for the following log files: backup, cli, diagnosis, monitor, ovca, snmp, and syncservice.
`log_level`	Set the value for the log level output. Accepted log levels are: CRITICAL, DEBUG, ERROR, INFO, WARNING. This property can be defined separately for the following log files: backup, cli, diagnosis, monitor, ovca, snmp, and syncservice. Use tab completion to insert the log file in the command before the log level value.
`log_size`	Set the value for the maximum log size before a log is rotated

Option	Description
phonehome	Set the state for the phone home service on the management nodes. The accepted values are: enable, disable. This command does not require a [service ovca restart] and should be executed on both the active and passive management nodes to take effect. Also, this command will ONLY enable the phone home flag on management nodes. The rest of the configuration required for phone home should be done explicitly, as described in Phone Home Service. This option is available starting with software release 2.4.4.1.
timezone	Set the time zone for the location of the Oracle Private Cloud Appliance. There are several hundred options, and the selection is case sensitive. It is suggested to use tab completion to find the most accurate setting for your location.
--json	Return the output of the command in JSON format
--less	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
--more	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
--tee=OUTPUTFILENAME	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-53 Changing the location of the sync service log file

```
PCA> set system-property log_file syncservice sync/ovca-sync.log
Status: Success

PCA> show system-properties
----------------------------------------
[...]
Backup.Log_File      /var/log/ovca-backup.log
Backup.Log_Level     DEBUG
Cli.Log_File         /var/log/ovca-cli.log
Cli.Log_Level        DEBUG
          Sync.Log_File        /var/log/sync/ovca-sync.log
Sync.Log_Level       DEBUG
Diagnosis.Log_File   /var/log/ovca-diagnosis.log
Diagnosis.Log_Level  DEBUG
[...]
----------------------------------------
Status: Success
```

> **Note:**
>
> Log configuration through the CLI is described in more detail in Setting the Oracle Private Cloud Appliance Logging Parameters.

Example 4-54 Configuring and unconfiguring an HTTP proxy

```
PCA> set system-property http_proxy http://10.1.1.11:8080
Status: Success

PCA> set system-property http_proxy ''
Status: Success
```

> **Note:**
>
> Proxy configuration through the CLI is described in more detail in Adding Proxy Settings for Oracle Private Cloud Appliance Updates.

Example 4-55 Configuring the Oracle Private Cloud Appliance Time Zone

```
PCA> set system-property timezone US/Eastern
Status: Success
```

show

The `show` command can be used to view information about particular objects such as tasks, rack layout or system properties. Unlike the `list` command, which applies to a whole target object type, the `show` command displays information specific to a particular target object. Therefore, it is usually run by specifying the command, the target object type and the object identifier.

Syntax

```
show object [OPTIONS]
```

Where *object* is the identifier for the target object that you wish to show information for. The following table provides a mapping of identifiers that should be substituted for *object*, depending on the command target.

Command Target	Object Identifier
`compute-node`	Compute Node Name
`iscsi-storage`	iSCSI LUN Name
`iscsi-storage-profile`	Storage Profile Name
`network`	Network Name
`nfs-storage`	NFS Share Name
`nfs-storage-profile`	NFS Storage Profile Name

Command Target	Object Identifier
oci-backup	Oracle Cloud Infrastructure Backup Name
oci-target	Oracle Cloud Infrastructure Target Name
rack-layout	Rack Architecture or Type
rack-type	(none)
storage-network	Storage Network/Cloud Name
system-properties	(none)
task	Task ID
tenant-group	Tenant Group Name
version	(none)

Note that you can use tab completion to help you correctly specify the *object* for the different command targets. You do not need to specify an *object* if the command target is `system-properties` or `version`.

Description

Use the `show` command to view information specific to a particular target object, identified by specifying the identifier for the object that you wish to view. The exception to this is the option to view `system-properties`, for which no identifier is required.

Frequently, the `show` command may display information that is not available using the `list` command in conjunction with its filtering capabilities.

Options

The following table shows the available options for this command.

Option	Description
`show { cloud-wwpn | compute-node | iscsi-storage | iscsi-storage-profile | network | nfs-storage | nfs-storage-profile | oci-backup | oci-target | rack-layout | rack-type | storage-network | system-properties | task | tenant-group | version } object [--json] [--less] [--more] [--tee=OUTPUTFILENAME]`	The command target to show information for.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.

Option	Description
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-56 Show System Properties

> **Note:**
>
> This command only displays the system properties for the management node where it is run. If the system properties have become unsynchronized across the two management nodes, the information reflected by this command may not apply to both systems. You can run this command on either the active or passive management node if you need to check that the configurations match.

```
PCA> show system-properties

----------------------------------------
HTTP_Proxy           None
HTTPS_Proxy          None
FTP_Proxy            None
Log_File             /var/log/ovca.log
Log_Level            DEBUG
Log_Size (MB)        250
Log_Count            5
Timezone             Etc/UTC
Backup.Log_File      /var/log/ovca-backup.log
Backup.Log_Level     DEBUG
Cli.Log_File         /var/log/ovca-cli.log
Cli.Log_Level        DEBUG
Sync.Log_File        /var/log/ovca-sync.log
Sync.Log_Level       DEBUG
Diagnosis.Log_File   /var/log/ovca-diagnosis.log
Diagnosis.Log_Level  DEBUG
Monitor.Log_File     /var/log/ovca-monitor.log
Monitor.Log_Level    INFO
Snmp.Log_File        /nfs/shared_storage/logs/ovca_snmptrapd.log
Snmp.Log_Level       DEBUG
----------------------------------------

Status: Success
```

Example 4-57 Show Task

```
PCA> show task 341e7bc74f339c

----------------------------------------
Task_Name            backup
```

```
Status               RUNNING
Progress             70
Start_Time           05-27-2019 09:59:36
End_Time             None
Pid                  1503341
Result               None
----------------------------------------

Status: Success
```

Example 4-58 Show Rack Layout

```
PCA> show rack-layout x8-2_base

RU  Name         Role             Type         Sub_Type     Units
--  ----         ----             ----         --------     -----
42  ovcacn42r1   compute          compute                   [42]
41  ovcacn41r1   compute          compute                   [41]
40  ovcacn40r1   compute          compute                   [40]
39  ovcacn39r1   compute          compute                   [39]
38  ovcacn38r1   compute          compute                   [38]
37  ovcacn37r1   compute          compute                   [37]
36  ovcacn36r1   compute          compute                   [36]
35  ovcacn35r1   compute          compute                   [35]
34  ovcacn34r1   compute          compute                   [34]
33  ovcacn33r1   compute          compute                   [33]
32  ovcacn32r1   compute          compute                   [32]
31  ovcacn31r1   compute          compute                   [31]
30  ovcacn30r1   compute          compute                   [30]
29  ovcacn29r1   compute          compute                   [29]
28  ovcacn28r1   compute          compute                   [28]
27  ovcacn27r1   compute          compute                   [27]
26  ovcacn26r1   compute          compute                   [26]
25  N / A        infrastructure   filler                    [25, 24]
24  N / A        infrastructure   filler                    [25, 24]
23  ovcasw23r1   infrastructure   cisco-data   cisco4       [23]
22  ovcasw22r1   infrastructure   cisco-data   cisco3       [22]
21  ovcasw21r1   infrastructure   cisco                     [21]
20  N / A        infrastructure   zfs-storage  disk-shelf   [20, 19, 18, 17]
19  N / A        infrastructure   zfs-storage  disk-shelf   [20, 19, 18, 17]
18  N / A        infrastructure   zfs-storage  disk-shelf   [20, 19, 18, 17]
17  N / A        infrastructure   zfs-storage  disk-shelf   [20, 19, 18, 17]
16  ovcasw16r1   infrastructure   cisco-data   cisco2       [16]
15  ovcasw15r1   infrastructure   cisco-data   cisco1       [15]
14  ovcacn14r1   compute          compute                   [14]
13  ovcacn13r1   compute          compute                   [13]
12  ovcacn12r1   compute          compute                   [12]
11  ovcacn11r1   compute          compute                   [11]
10  ovcacn10r1   compute          compute                   [10]
9   ovcacn09r1   compute          compute                   [9]
8   ovcacn08r1   compute          compute                   [8]
7   ovcacn07r1   compute          compute                   [7]
6   ovcamn06r1   infrastructure   management   management2  [6]
5   ovcamn05r1   infrastructure   management   management1  [5]
4   ovcasn02r1   infrastructure   zfs-storage  zfs-head2    [4, 3]
3   ovcasn02r1   infrastructure   zfs-storage  zfs-head2    [4, 3]
2   ovcasn01r1   infrastructure   zfs-storage  zfs-head1    [2, 1]
1   ovcasn01r1   infrastructure   zfs-storage  zfs-head1    [2, 1]
0   ovcapduBr1   infrastructure   pdu          pdu2         [0]
0   ovcapduAr1   infrastructure   pdu          pdu1         [0]
-----------------
```

```
44 rows displayed

Status: Success
```

Example 4-59 Show the Configuration Details of the default_external Network

```
PCA> show network default_external

----------------------------------------
Network_Name         default_external
Trunkmode            None
Description          None
Ports                ['5:1', '5:2']
vNICs                None
Status               ready
Network_Type         external_network
Compute_Nodes        ovcacn12r1, ovcacn07r1, ovcacn13r1, ovcacn14r1, ovcacn10r1,
ovcacn09r1, ovcacn11r1
Prefix               192.168.200.0/21
Netmask              None
Route_Destination    None
Route_Gateway        None
----------------------------------------

Status: Success
```

Example 4-60 Show Details of a Tenant Group

```
PCA> show tenant-group myTenantGroup

----------------------------------------
Name                 myTenantGroup
Default              False
Tenant_Group_ID      0004fb0000020000155c15e268857a78
Servers              ['ovcacn09r1', 'ovcacn10r1']
State                ready
Tenant_Group_VIP     None
Tenant_Networks      ['myPublicNetwork']
Pool_Filesystem_ID   3600144f0d29d4c86000057162ecc0001
----------------------------------------

Status: Success
```

Example 4-61 Show Details of a Custom Network

```
PCA> show network myHostNetwork

----------------------------------------
Network_Name         myHostNetwork
Trunkmode            None
Description          None
Ports                ['1', '2']
vNICs                None
Status               ready
Network_Type         host_network
Compute_Nodes        ovcacn42r1, ovcacn01r2, ovcacn02r2
Prefix               10.10.10
Netmask              255.255.240.0
Route_Destination    10.10.20.0/24
Route_Gateway        10.10.10.250
----------------------------------------
```

```
Status: Success
```

Example 4-62 Show the WWPNs for a Storage Network

```
PCA> show cloud-wwpn Cloud_A

----------------------------------------
Cloud_Name       Cloud_A
WWPN_List        50:01:39:70:00:58:91:1C, 50:01:39:70:00:58:91:1A,
                 50:01:39:70:00:58:91:18, 50:01:39:70:00:58:91:16,
                 50:01:39:70:00:58:91:14, 50:01:39:70:00:58:91:12,
                 50:01:39:70:00:58:91:10, 50:01:39:70:00:58:91:0E,
                 50:01:39:70:00:58:91:0C, 50:01:39:70:00:58:91:0A,
                 50:01:39:70:00:58:91:08, 50:01:39:70:00:58:91:06,
                 50:01:39:70:00:58:91:04, 50:01:39:70:00:58:91:02,
                 50:01:39:70:00:58:91:00
----------------------------------------

Status: Success
```

Example 4-63 Show Oracle Private Cloud Appliance Version Information

```
PCA> show version

----------------------------------------
Version              2.4.1
Build                819
Date                 2019-06-20
----------------------------------------

Status: Success
```

start

Starts up a rack component.

> **Caution:**
>
> The `start` command is deprecated. It will be removed in the next release of the Oracle Private Cloud Appliance Controller Software.

Syntax

```
start compute-node CN|management-node MN [OPTIONS]
```

where *CN* refers to the name of the compute node and *MN* refers to the name of the management node to be started.

Description

Use the `start` command to boot a compute node or management node. You must provide the host name of the server you wish to start.

Options

The following table shows the available options for this command.

Option	Description
`compute-node CN | management-node MN`	Start either a compute node or a management node. Replace *CN* or *MN* respectively with the host name of the server to be started.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-64 Starting a Compute Node

```
PCA> start compute-node ovcacn11r1
Status: Success
```

stop

Shuts down a rack component or aborts a running task.

> **Caution:**
>
> The `stop` commands to shut down rack components are deprecated. It will be removed in the next release of the Oracle Private Cloud Appliance Controller Software.
>
> The other `stop` commands, to abort tasks, remain functional.

Syntax

```
stop { compute-node CN | management-node MN | task id | update-task
id } [OPTIONS]
```

where *CN* or *MN* refers to the name of the server to be shut down, and *id* refers to the identifier of the task to be aborted.

Description

Use the `stop` command to shut down a compute node or management node or to abort a running task. Depending on the command target you must provide either the host name of the server you wish to shut down, or the unique identifier of the task you

wish to abort. This is a destructive operation and you are prompted to confirm whether or not you wish to continue, unless you use the `--confirm` flag to override the prompt.

Options

The following table shows the available options for this command.

Option	Description
`compute-node CN | management-node MN`	Shut down either a compute node or a management node. Replace *CN* or *MN* respectively with the host name of the server to be shut down. **Caution:** These options are deprecated.
`task id | update-task id`	Aborts a running task. Use the `update-task` target type specifically to abort a software update task. It does not take a task ID as an argument, but the management node IP address. **Caution:** Stopping an update task is a risky operation and should be used with extreme caution.
`--confirm`	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-65 Aborting a Task

```
PCA> stop task 341d45b5424c16
************************************************************
 WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
```

```
************************************************************
Are you sure [y/N]:y

Status: Success
```

update appliance

This command is deprecated. Its functionality is part of the Oracle Private Cloud Appliance Upgrader.

> **Caution:**
>
> Release 2.4.1 is for factory installation only. It cannot be used for field updates or upgrade operations on existing appliance environments.

update password

Modifies the password for one or more components within the Oracle Private Cloud Appliance.

Syntax

```
update password component PCA-password target-password [OPTIONS]
```

where *component* is the name of the component you are changing the password, and *PCA-password* is the current password of the Oracle Private Cloud Appliance admin user, and *target-password* is the new password to be applied to the target rack component.

Description

Use the `update password` command to modify the password for one or more components within the Oracle Private Cloud Appliance. This is a destructive operation and you are prompted to confirm whether or not you wish to continue, unless you use the `--confirm` flag to override the prompt.

Optionally you provide the current Oracle Private Cloud Appliance password and the new target component password with the command. If not, you are prompted for the current password of the Oracle Private Cloud Appliance admin user and for the new password that should be applied to the target.

> **Caution:**
>
> Password changes are not instantaneous across the appliance, but are propagated through a task queue. When applying a password change, allow at least 30 minutes for the change to take effect. Do not attempt any further password changes during this delay. Verify that the password change has been applied correctly.

Options

The following table shows the available options for this command.

Option	Description
`LeafSwitch-admin`	Sets a new password for the `admin` user on the leaf Cisco Nexus 9336C-FX2 Switches.
`MgmtNetSwitch-admin`	Sets a new password for the `admin` user on the Cisco Nexus 9348GC-FXP Switch.
`SpineSwitch-admin`	Sets a new password for the `admin` user on the spine Cisco Nexus 9336C-FX2 Switches.
`mgmt-root`	Sets a new password for the `root` user on the management nodes.
`mysql-appfw`	Sets a new password for the `appfw` user in the MySQL database. The `mysql-appfw`, `mysql-ovs`, `mysql-root` and `wls-weblogic` passwords are synchronized automatically, because these must always be identical.
`mysql-ovs`	Sets a new password for the `ovs` user in the MySQL database. The `mysql-appfw`, `mysql-ovs`, `mysql-root` and `wls-weblogic` passwords are synchronized automatically, because these must always be identical.
`mysql-root`	Sets a new password for the `root` user in the MySQL database. The `mysql-appfw`, `mysql-ovs`, `mysql-root` and `wls-weblogic` passwords are synchronized automatically, because these must always be identical.
`ovm-admin`	Sets a new password for the `admin` user in Oracle VM Manager.
`spCn-root`	Sets a new password for the `root` user in the compute node ILOMs.
`spMn-root`	Sets a new password for the `root` user in the management node ILOMs.
`spZfs-root`	Sets a new password for the `root` user on the ZFS storage appliance as well as its ILOM.
`system-root`	Sets a new password for the `root` user on all compute nodes.
`wls-weblogic`	Sets a new password for the `weblogic` user in WebLogic Server. The `mysql-appfw`, `mysql-ovs`, `mysql-root` and `wls-weblogic` passwords are synchronized automatically, because these must always be identical.
`zfs-root`	Sets a new password for the `root` user on the ZFS storage appliance as well as its ILOM.
`--confirm`	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.

Option	Description
`--force`	Force the command to be executed even if the target is in an invalid state. This option is not risk-free and should only be used as a last resort.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-66 Changing the Oracle VM Manager Administrator Password

```
PCA> update password ovm-admin
************************************************************
 WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
************************************************************
Are you sure [y/N]:y
Current PCA Password:
New ovm-admin Password:
Confirm New ovm-admin Password:
Status: Success
```

update compute-node

As of release 2.4.4, this command is no longer supported for compute node upgrade. Compute node upgrade functionality is now a part of the Oracle Private Cloud Appliance Upgrader.

Updates the Oracle Private Cloud Appliance compute nodes to the Oracle VM Server version included in the Oracle Private Cloud Appliance ISO image.

Syntax

```
update compute-node node [OPTIONS]
```

where *node* is the identifier of the compute node that must be updated with the Oracle VM Server version provided as part of the appliance software ISO image. Run this command for one compute node at a time.

NOT_SUPPORTED:

Running the `update compute-node` command with multiple `node` arguments is not supported. Neither is running the command concurrently in separate terminal windows.

Description

Use the `update compute-node` command to install the new Oracle VM Server version on the selected compute node or compute nodes. This is a destructive operation and you are prompted to confirm whether or not you wish to continue, unless you use the --confirm flag to override the prompt.

Options

The following table shows the available options for this command.

Option	Description
`--confirm`	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
`--force`	Force the command to be executed even if the target is in an invalid state. This option is not risk-free and should only be used as a last resort.
`--json`	Return the output of the command in JSON format
`--less`	Return the output of the command one screen at a time for easy viewing, as with the `less` command on the Linux command line. This option allows both forward and backward navigation through the command output.
`--more`	Return the output of the command one screen at a time for easy viewing, as with the `more` command on the Linux command line. This option allows forward navigation only.
`--tee=OUTPUTFILENAME`	When returning the output of the command, also write it to the specified output file.

Examples

Example 4-67 Upgrade a Compute Node to Oracle VM Server Release 4.2.x

```
PCA> update compute-node ovcacn10r1
************************************************************
 WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
************************************************************
Are you sure [y/N]:y

Status: Success
```

5

Managing the Oracle VM Virtual Infrastructure

> **NOT_SUPPORTED:**
>
> Access to the Oracle VM Manager Web User Interface (Web UI), command line interface and Web Services API (WSAPI) is provided without restrictions. The configuration of Oracle Private Cloud Appliance components within Oracle VM Manager is automatic and handled by the Private Cloud Appliance provisioning process. Altering the configuration of these components directly within Oracle VM Manager is not supported and may result in the malfunction of the appliance.

Following is a non-exhaustive list of critical limitations. Violating these limitations results in severe system configuration problems and significant downtime:

- **DO NOT rename host names** of compute nodes or other Private Cloud Appliance components.
- **DO NOT rename server pools**.
- **DO NOT rename built-in repositories**.
- **DO NOT rename existing networks or modify their properties** (VLAN tag, MTU, and so on), except as documented explicitly in this *Oracle Private Cloud Appliance Administration Guide*.
- **DO NOT add the VM role to the internal management network or internal storage network**.

> **NOT_SUPPORTED:**
>
> The appliance controller software enables customization of networking, external storage connectivity and server pools – known as tenant groups in Private Cloud Appliance. The resulting Oracle VM configurations also must not be altered within Oracle VM Manager.
>
> Use of Oracle VM Manager in the context of Private Cloud Appliance should be limited to the management and creation of virtual machines.
>
> Configuring additional storage, creating repositories, and setting up additional networks specifically for the use of virtual machines is possible. However, this should be done carefully, to avoid disrupting the configuration specific to the Private Cloud Appliance.

Management of virtual machines and your Oracle VM environment is achieved using the Oracle VM Manager Web UI. While Oracle VM Manager does provide a command line interface and WSAPI, use of these on your Private Cloud Appliance should only be attempted

by advanced users with a thorough understanding of Oracle VM and the usage limitations within a Private Cloud Appliance context.

The information provided here is a description of the Oracle VM Manager Web UI within the context of the Private Cloud Appliance. Where particular actions within the Oracle VM Manager Web UI are referenced, a link to the appropriate section within the Oracle VM Manager User's Guide is provided.

> **Note:**
>
> When consulting the Oracle VM documentation directly, keep in mind the limitations imposed by using it within Private Cloud Appliance. More details about the use of the Oracle VM documentation library can be found in About the Oracle VM Documentation Library.

New users of Oracle VM who want to learn the fundamentals of creating and maintaining a virtualized environment should consult the Oracle VM Concepts Guide. It describes the concepts on which the Oracle VM components and functionality are based, and also links to operational procedures in the Oracle VM Manager User's Guide.

The Oracle VM Manager Web UI is available at the virtual IP address that you configured for your management nodes during installation. This virtual IP address is automatically assigned to whichever management node is currently the active node within the cluster. If that management node becomes unavailable, the standby management node is promoted to the active role and takes over the IP address automatically. See High Availability for more information on management node failover.

The Oracle VM Manager Web UI is configured to listen for HTTPS requests on port 7002.

Guidelines

The Oracle VM Manager Web UI is provided without any software limitation to its functionality. However, it is important that you only use the functionality documented for use with Oracle Private Cloud Appliance. Follow these warnings while managing the appliance:

- Managing the Oracle VM Virtual Infrastructure
- Guidelines and Limitations

As a general rule, perform actions on the appliance only if Oracle gives specific instructions to do so. If you have a question about changing anything not explicitly permitted or described in the documentation, contact Oracle to open an SR.

If you ignore this advice, the Private Cloud Appliance automation, which uses specific naming conventions to label and manage assets, may fail. Out-of-band configuration changes would not be known to the orchestration software of the Private Cloud Appliance. If a conflict between the Private Cloud Appliance configuration and Oracle VM configuration occurs, it may not be possible to recover without data loss or system downtime.

> **Note:**
>
> An exception to these guidelines applies to the creation of a *Service VM*. This is a VM created specifically to perform administrative operations, for which it needs to be connected to both the public network and internal appliance networks. For detailed information and instructions, refer to support note How to Create Service Virtual Machines on the Private Cloud Appliance by using Internal Networks (Doc ID 2017593.1).
>
> There is a known issue with the Oracle Private Cloud Appliance Upgrader, which stops the upgrade process if Service VMs are present. For the appropriate workaround, consult the support note [PCA 2.3.4] pca_upgrader Check Fails with Exception - Network configuration error: 'inet' (Doc ID 2510822.1).

Regardless of which interface you use to access the Oracle VM functionality directly, the same restrictions apply. In summary, you may use the Web UI, CLI or WSAPI for the operations listed below.

Use the Oracle VM Interfaces for:

- configuration and management of VM networks, VLAN interfaces and VLANs;
- configuration of VM vNICs and connecting VMs to networks;
- all VM configuration and life cycle management;
- attaching and managing external storage for VM usage;
- compute node IPMI control.

About the Oracle VM Documentation Library

You can find the complete Oracle VM documentation library at this URL: https://docs.oracle.com/en/virtualization/oracle-vm/index.html.

It is critical that you understand the scope of Oracle VM within the specific context of Oracle Private Cloud Appliance. A major objective of the appliance is to orchestrate or fully automate a number of Oracle VM operations. It also imposes restrictions that do not exist in other Oracle VM environments, on infrastructure aspects such as server hardware, networking and storage configuration. Consequently, some chapters or even entire books in the Oracle VM documentation library are irrelevant to Oracle Private Cloud Appliance customers, or should not be used because they describe procedures that conflict with the way the appliance controller software configures and manages the Oracle VM infrastructure.

This list, which is not meant to be exhaustive, explains which parts of the Oracle VM documentation should not be referenced because the functionality in question is either not supported or managed at the level of the appliance controller software:

- Installation and Upgrade Guide

  Oracle Private Cloud Appliance always contains a clustered pair of management nodes with Oracle VM Manager pre-installed. When you power on the appliance for the first time, the compute node provisioning process begins, and one of the provisioning steps is to install Oracle VM Server on the compute nodes installed in the appliance rack. The installation of additional compute nodes and upgrades of the appliance software are orchestrated in a similar way.

- Getting Started Guide

  Although the getting started guide is an excellent way to progress through the entire chain of operations from discovering the first Oracle VM Server to the point of accessing a fully operational virtual machine, it does not help the Oracle Private Cloud Appliance user, who only needs Oracle VM Manager in order to create and manage virtual machines.

- Administration Guide

  This guide describes a number of advanced system administration tasks, most of which are performed at the level of the virtualization platform. The information in this book may be useful for specific configurations or environments, but we recommend that you consult with Oracle subject matter experts to avoid making changes that adversely affect the Oracle Private Cloud Appliance environment.

- Command Line Interface and Web Services API

  The recommended interface to manage the Oracle VM environment within Oracle Private Cloud Appliance is the Oracle VM Manager Web UI. The CLI and WSAPI should be used with care, within the limitations described in the Oracle Private Cloud Appliance documentation. They can be safely used in a programmatic context, for example to automate operations related to the virtual machine life cycle (which includes create, clone, start, stop, migrate VMs, pinning CPUs, uploading templates and ISOs, and so on).

Since Oracle VM Manager is the preferred interface to manage the virtualized environment, this chapter provides links to various sections of the Oracle VM Manager User's Guide in order to help Oracle Private Cloud Appliance users perform the necessary tasks. The book is closely aligned with the structure of the Web UI it describes, and the sections and links in this chapter conveniently follow the same basic outline. Where the Oracle VM Manager functionality overlaps with the default Oracle Private Cloud Appliance configuration the document indicates which operations are safe and which should be avoided.

Logging in to the Oracle VM Manager Web UI

To open the Login page of the Oracle VM Manager Web UI, enter the following address in a Web browser:

https://***manager-vip***:7002/ovm/console

Where, ***manager-vip*** refers to the virtual IP address, or corresponding host name, that you have configured for your management nodes during installation. By using the virtual IP address, you ensure that you always access the Oracle VM Manager Web UI on the active management node.

> **Important:**
>
> You must ensure that if you are accessing Oracle VM Manager through a firewalled connection, the firewall is configured to allow TCP traffic on the port that Oracle VM Manager is using to listen for connections.

Enter your Oracle VM Manager administration user name in the **Username** field. This is the administration user name you configured during installation. Enter the password for the Oracle VM Manager administration user name in the **Password** field.

> **Important:**
>
> The Oracle VM Manager Web UI makes use of cookies in order to store session data. Therefore, to successfully log in and use the Oracle VM Manager Web UI your web browser must accept cookies from the Oracle VM Manager host.

Monitoring Health and Performance in Oracle VM

The **Health** tab provides a view of the health of the compute nodes and the server pool within your environment. This information complements the Hardware View provided in the Oracle Private Cloud Appliance Dashboard. See Hardware View for more information.

The **Statistics** subtabs available on the Health tab provides statistical information, including graphs that can be refreshed with short intervals or at the click of a button, for CPU and memory usage and for file system utilization. These statistics can be viewed at a global scale to determine overall usage, or at the detail level of a category of resources or even a single item.

The Server and VM Statistics subtab can display information per server to see the performance of each individual compute node, or per virtual machine to help track the usage and resource requirements for any of the virtual machines within your environment. The File System Statistics subtab displays storage space utilization information, organized by storage location, and allows you to track available space for individual file systems over time.

For detailed information on using the Health tab, please refer to the section entitled Health Tab in the Oracle VM Manager User's Guide.

In addition to the Health tab you can also monitor the status of many resource categories through the **Info perspective** or **Events perspective**. When you select these perspectives in the Management pane, the type of information displayed depends on the active item in the Navigation pane on the left hand side. Both the Info perspective and the Events perspective are common to many elements within the Oracle VM Manager Web UI.

The following sections in the Oracle VM Manager User's Guide provide detailed information about both perspectives, using the server pool item as an example:

- the Oracle VM Manager Info Perspective
- the Oracle VM Manager Events Perspective

Creating and Managing Virtual Machines

The **Servers and VMs** tab is used to create and manage your virtual machines. By default, compute nodes in the base rack of the appliance are listed as belonging to a single server pool called **Rack1_ServerPool**. The configuration of the default server pool must not be altered. There is no need to discover servers, as compute nodes are automatically provisioned and discovered within an Oracle Private Cloud Appliance. Editing the configuration of the server pool, servers and processor compatibility groups is not supported.

The primary purpose of this tab within the Oracle Private Cloud Appliance context is to create and manage your virtual machines.

Virtual machines can be created using:

- ISO files in a repository (hardware virtualized only)
- Mounted ISO files on an NFS, HTTP or FTP server (paravirtualized only)
- Virtual machine templates (by cloning a template)
- Existing virtual machines (by cloning a virtual machine)
- Virtual machine assemblies or virtual appliances

Virtual machines require most installation resources to be located in the storage repository, managed by Oracle VM Manager, with the exception of mounted ISO files for paravirtualized guests. See Managing Virtual Machine Resources for more information on importing these resources into the Oracle Private Cloud Appliance repository.

The following list provides an outline of actions that you can perform in this tab, with links to the relevant documentation within the Oracle VM Manager User's Guide:

- Create a virtual machine

  You can create a virtual machine following the instructions provided in the section entitled Create Virtual Machine.

  You do not need to create any additional server pools. You need only ensure that your installation media has been correctly imported into the Oracle Private Cloud Appliance repository.
- View virtual machine information and events

  You can view information about your virtual machine or access virtual machine events by following the information outlined in the section entitled View Virtual Machine Events.
- Edit a virtual machine

  You can edit virtual machine parameters as described in the section entitled Edit Virtual Machine.
- Start a virtual machine

  Further information is provided in the section entitled Start Virtual Machines.
- Connect to a virtual machine console

  There are two options for virtual machine console connections:

  – For more information about the use of the VM console, refer to the section entitled Launch Console.

  – For more information about the use of the VM serial console, refer to the section entitled Launch Serial Console.
- Stop a virtual machine

  Further information is provided in the section entitled Stop Virtual Machines.
- Kill a virtual machine

  Further information is provided in the section entitled Kill Virtual Machines.
- Restart a virtual machine

Further information is provided in the section entitled Restart Virtual Machines.

- Suspend a virtual machine

  Further information is provided in the section entitled Suspend Virtual Machines.

- Resume a virtual machine

  Further information is provided in the section entitled Resume Virtual Machine.

- Migrate or move a virtual machine between repositories, between servers, and to or from the Unassigned Virtual Machines folder

  Further information is provided in the section entitled Migrate or Move Virtual Machines.

  It is possible to create alternate repositories if you have extended the system with external storage. If you have an additional repository, this function can be used to move a virtual machine from one repository to another.

  Because there is only a single server pool available in a default Oracle Private Cloud Appliance base rack, migration of virtual machines can only be achieved between servers and between a server and the Unassigned Virtual Machines folder. Migration between server pools is possible if you have customized the default configuration by creating tenant groups. See Tenant Groups for more information.

  Modifying Server Processor Compatibility Groups is not permitted.

  > **Caution:**
  >
  > Compute nodes of different hardware generations operate within the same server pool but belong to different CPU compatibility groups. By default, live migration between CPU compatibility groups is not supported, meaning that virtual machines must be cold-migrated between compute nodes of different generations.
  >
  > If *live* migration between compute nodes of different generations is required, it must only be attempted from an older to a newer hardware generation, and never in the opposite direction. To achieve this, the administrator must first create new compatibility groups.
  >
  > For more information about CPU compatibility groups, please refer to the section entitled Server Processor Compatibility Perspective.

  For more information about the Unassigned Virtual Machines folder, refer to the section entitled Unassigned Virtual Machines Folder.

- Control virtual machine placement through anti-affinity groups.

  You can prevent virtual machines from running on the same physical host by adding them to an anti-affinity group. This is particularly useful for redundancy and load balancing purposes.

  Further information about anti-affinity groups is provided in the section entitled What are Anti-Affinity Groups? in the *Oracle VM Concepts Guide*.

  For instructions to create and manage anti-affinity groups, refer to the section entitled Anti-Affinity Groups Perspective in the *Oracle VM Manager User's Guide*.

- Clone a virtual machine

Further information is provided in the section entitled Clone a Virtual Machine or Template.

You can create a clone customizer to set up the clone parameters, such as networking, and the virtual disk, and ISO resources. For more information about clone customizers, please refer to the section entitled Manage Clone Customizers.

- Export virtual machines to a virtual appliance

  Exporting a virtual appliance lets you reuse virtual machines with other instances of Oracle VM, or with other virtualization environments that support the Open Virtualization Format (OVA). You can export one or more virtual machines to a virtual appliance. Further information is provided in the section entitled Export to Virtual Appliance.

- Export virtual machines to your Oracle Cloud Infrastructure tenancy

  Exporting an Oracle VM virtual machine using the Oracle VM Exporter Appliance transfers the virtual machine to Oracle Cloud Infrastructure. Exporting a virtual machine does not remove the virtual machine from Oracle VM. You can export a virtual machine to other places in Oracle Cloud Infrastructure. Further information is provided in the section entitled Export to Oracle Cloud Infrastructure Using Oracle VM Exporter Appliance.

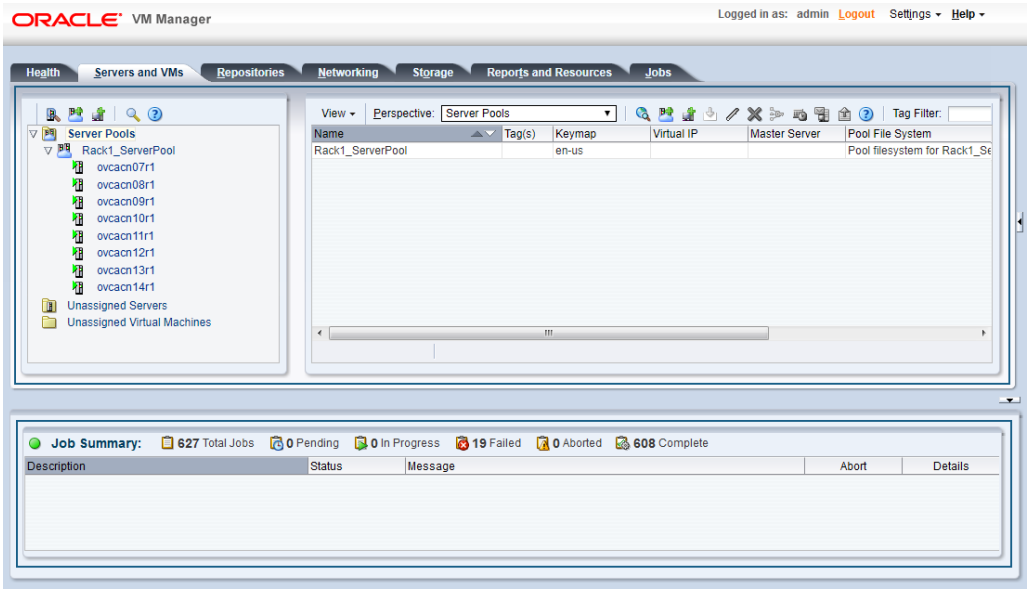
- Send a message to a virtual machine

  If you have installed Oracle VM Guest Additions within your virtual machine, you can use the Oracle VM Messaging framework to send messages to your virtual machines to trigger actions within a virtual machine. Refer to the section entitled Send VM Messages for more information.

- Delete a virtual machine

  Further information is provided in the section entitled Delete Virtual Machines.

Figure 5-1 A view of the Servers and VMs tab



Managing Virtual Machine Resources

The **Repositories** tab provides a view of the Oracle Private Cloud Appliance repository. By default, a shared repository is configured on the internal ZFS Storage Appliance and named **Rack1-repository**. Additional local repositories are configured using the free disk space of each compute node. None of the default repository configurations can be altered.

> **Caution:**
>
> Using local storage on the compute nodes has implications that you should consider when planning the deployment of your virtual environment. See the following list.

- Virtual machines with resources in a local storage repository can be migrated to another compute node's local storage if you select the option "Migrate a running VM, and migrate its local storage, to a different Server within the same Server Pool."
- Templates, assemblies and ISOs in local storage repositories cannot be used to create virtual machines on another compute node.
- If a compute node becomes unavailable, its locally stored virtual machines and resources cannot be restored or migrated to another compute node for continued service.
- The virtual machines and resources in local storage repositories are not protected by automatic failover and high-availability mechanisms normally offered by a clustered Oracle VM server pool with shared storage repository.

Additional repositories should be configured using external storage solutions. If the system contains an Oracle ZFS Storage Appliance ZS7-2, extra disk trays can be installed to provide the space for additional repositories. For information about extending the storage capacity of Private Cloud Appliance, see Viewing and Managing Storage Resources.

The Repositories tab is used to manage virtual machine resources, such as installation media and virtual disks. From this tab, it is possible to create, import or clone Oracle VM templates, virtual appliances, and ISO image files. It is also possible to create, modify, or clone virtual disks here. The following list provides an outline of actions that you can perform in the Repositories tab, with links to the relevant documentation within the Oracle VM Manager User's Guide:

- Manage Virtual Machine Templates
  - Import a template
  - Edit a template
  - Clone a VM or template
  - Move a template
  - Manage template clone customizers
  - Delete a template

  All documentation for these actions can be found in the section entitled VM Templates Perspective.
- Manage Virtual Appliances

  - Import a virtual appliance
  - Create a VM from a virtual appliance
  - Edit a virtual appliance
  - Refresh a virtual appliance
  - Delete a virtual appliance

  All documentation for these actions can be found in the section entitled Virtual Appliances Perspective.

  For specific information about virtual appliances offered through Oracle Technology Network, refer to Virtual Appliances from Oracle.

- Manage Virtual Machine ISO Image Files
  - Import an ISO
  - Edit an ISO
  - Clone an ISO
  - Delete an ISO

  All documentation for these actions can be found in the section entitled ISOs Perspective.

- Manage Virtual Disks
  - Create a virtual disk
  - Import a virtual disk
  - Edit a virtual disk
  - Clone a virtual disk
  - Delete a virtual disk

  All documentation for these actions can be found in the section entitled Virtual Disks Perspective.

- View Virtual Machine Configuration Entries

  For more information, refer to the section entitled VM Files Perspective.

Virtual Appliances from Oracle

On the Oracle Virtualization product page, you can find several pre-configured Oracle VM Virtual Appliances, which can be downloaded for convenient deployment on Oracle Private Cloud Appliance. These virtual appliances allow users of Oracle Private Cloud Appliance to rapidly set up a typical Oracle product stack within their Oracle VM environment, without having to perform the full installation and configuration process.

For detailed information, including documentation specific to the virtual appliances, refer to the Oracle VM Virtual Appliances overview page.

For Oracle VM instructions related to virtual appliances, follow the links provided above.

For more general information about the use of virtual appliances and templates, refer to Understanding Repositories in the *Oracle VM Concepts Guide*. The most relevant sections are:

- How is a Repository Organized?
- How are Virtual Appliances Managed?

Configuring Network Resources for Virtual Machines

The **Networking** tab is used to manage networks within the Oracle VM environment running on the Oracle Private Cloud Appliance.

> **Caution:**
>
> By default, a number of networks are defined during factory installation. These **must not be altered** as they are required for the correct operation of the Oracle Private Cloud Appliance software layer.

Configuring VM Network Resources

The default networks are set up as follows:

- `192.168.32.0` : the internal management network

  This is a private network providing connectivity between the management nodes and compute nodes, using VLAN 3092. It is used for all network traffic inherent to Oracle VM Manager, Oracle VM Server and the Oracle VM Agents.

- `192.168.40.0` : the internal storage network

  This is a private network used exclusively for traffic to and from the ZFS storage appliance. Both management nodes and compute nodes can reach the internal storage on VLAN 3093. The network also fulfills the heartbeat function for the clustered Oracle VM server pool.

Additionally, two networks are listed with the **VM Network** role:

- `default_external`

  This default network is the standard choice for virtual machines requiring external network connectivity. It supports both tagged and untagged traffic. For untagged traffic it uses the Oracle VM standard VLAN 1, meaning no additional configuration is required.

  If you prefer to use VLANs for your VM networking, configure the additional VLAN interfaces and networks of your choice as follows:

  > **Note:**
  >
  > When reprovisioning compute nodes or provisioning newly installed compute nodes, you always need to configure VLANs manually. The VLAN configuration is not applied automatically when the compute node joins an existing server pool.

  1. Go to the **Networking** tab and select the **VLAN Interfaces** subtab.

The process for creating VLAN Interfaces is described in detail in the Oracle VM Manager User's Guide in the section entitled Create VLAN Interfaces.

2. Click **Create VLAN Interface**. In the navigation tree of the Create VLAN Interfaces window, select the `vx13040` VxLAN interface of each compute node in the default **Rack1_ServerPool**.
3. In the next step of the wizard, add the VLAN IDs you require. When you complete the wizard, a new VLAN interface for each new VLAN ID is configured on top of each compute node interface you selected.
4. Create a new Oracle VM network with the *VM role*, on the VLAN interfaces for each VLAN tag you created. Each new network should contain the VLAN interfaces associated with a particular VLAN ID; for example all VLAN interfaces with ID 11 on top of a `vx13040` interface.

   > **Tip:**
   >
   > You can filter the VLAN interfaces by ID to simplify the selection of the VLAN interfaces participating in the new network.

   The process for creating networks with VLAN interfaces is described in the Oracle VM Manager User's Guide in the section entitled Create New Network.

   > **Note:**
   >
   > To start using the new network at the VM level, edit the necessary VMs and assign a VNIC to connect to the new network.

5. Configure your data center network accordingly.

- `default_internal`

  This default network is intended for virtual machines requiring network connectivity to other virtual machines hosted on the appliance, but *not* external to the appliance. For untagged traffic it uses the Oracle VM standard VLAN 1. To use the VLANs of your choice, configure the additional VLAN interfaces and networks as follows:

  > **Note:**
  >
  > When reprovisioning compute nodes or provisioning newly installed compute nodes, you always need to configure VLANs manually. The VLAN configuration is not applied automatically when the compute node joins an existing server pool.

  1. Go to the **Networking** tab and select the **VLAN Interfaces** subtab.

     The process for creating VLAN Interfaces is described in detail in the Oracle VM Manager User's Guide in the section entitled Create VLAN Interfaces.

2. Click **Create VLAN Interface**. In the navigation tree of the Create VLAN Interfaces window, select the `vx2` VxLAN interface of each compute node in the default **Rack1_ServerPool**.
3. In the next step of the wizard, add the VLAN IDs you require. When you complete the wizard, a new VLAN interface for each new VLAN ID is configured on top of each compute node network port you selected.
4. Create a new VLAN network with the *VM role* for each VLAN tag you added. Each new network should contain the VLAN interfaces associated with a particular VLAN ID; for example all VLAN interfaces with ID 1001 on top of a `vx2` interface.

   > **Tip:**
   >
   > You can filter the VLAN interfaces by ID to simplify the selection of the VLAN interfaces participating in the new network.

   The process for creating networks with VLAN interfaces is described in the Oracle VM Manager User's Guide in the section entitled Create New Network.

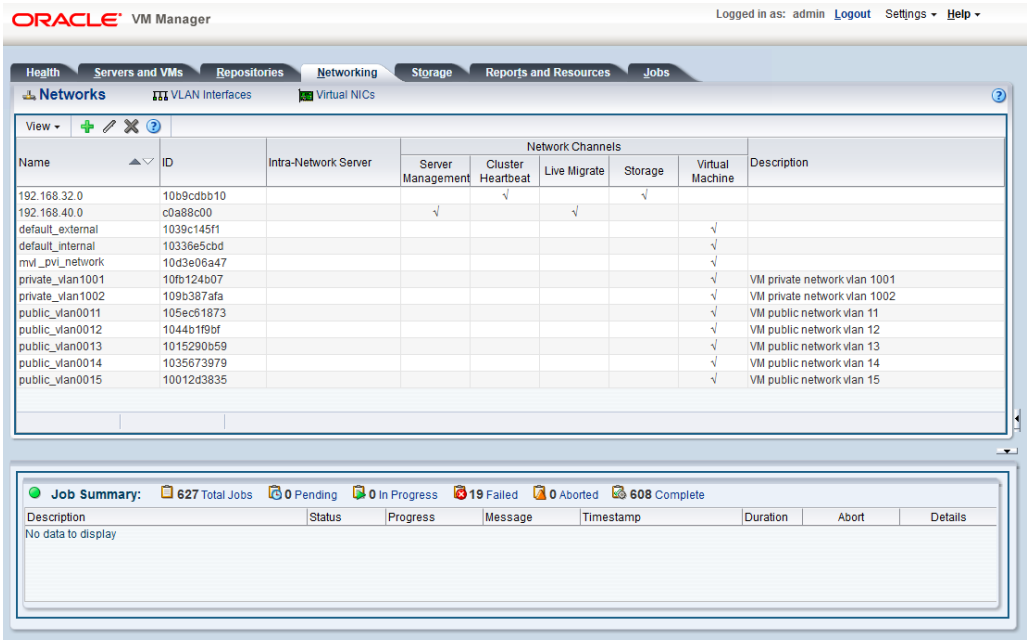
For more information about Oracle Private Cloud Appliance network configuration, see Network Infrastructure.

> **Caution:**
>
> Do not alter the internal appliance administration network (`192.168.4.0`) connections on the compute nodes or any other rack components. The environment infrastructure depends on the correct operation of this network.
>
> For example, if you configured networking for virtual machines in such a way that they can obtain an IP address in the `192.168.4.0` subnet, IP conflicts and security issues are likely to occur.

> **Note:**
>
> If VM-to-VM network performance is not optimal, depending on the type of network load, you could consider increasing the guests' MTU from the default 1500 bytes to 9000. Note that this is a change at the VM level; the compute node interfaces are set to accommodate 9000 bytes already, and must never be modified. Connectivity between VMs and external systems may also benefit from the higher MTU, provided this is supported across the entire network path.

Do not edit or delete any of the networks listed here. Doing so may cause your appliance to malfunction. In an Oracle Private Cloud Appliance context, use the Networking tab to configure and manage Virtual NICs and VLANs for use by your virtual machines.

Figure 5-2 A view of the Networking tab



Viewing and Managing Storage Resources

The storage resources underlying the built-in Oracle Private Cloud Appliance ZFS storage repository and the server pool clustering file system are listed under the **Storage** tab within Oracle VM Manager. The internal ZFS storage is listed under the SAN Servers folder. Do not modify or attempt to delete this storage.

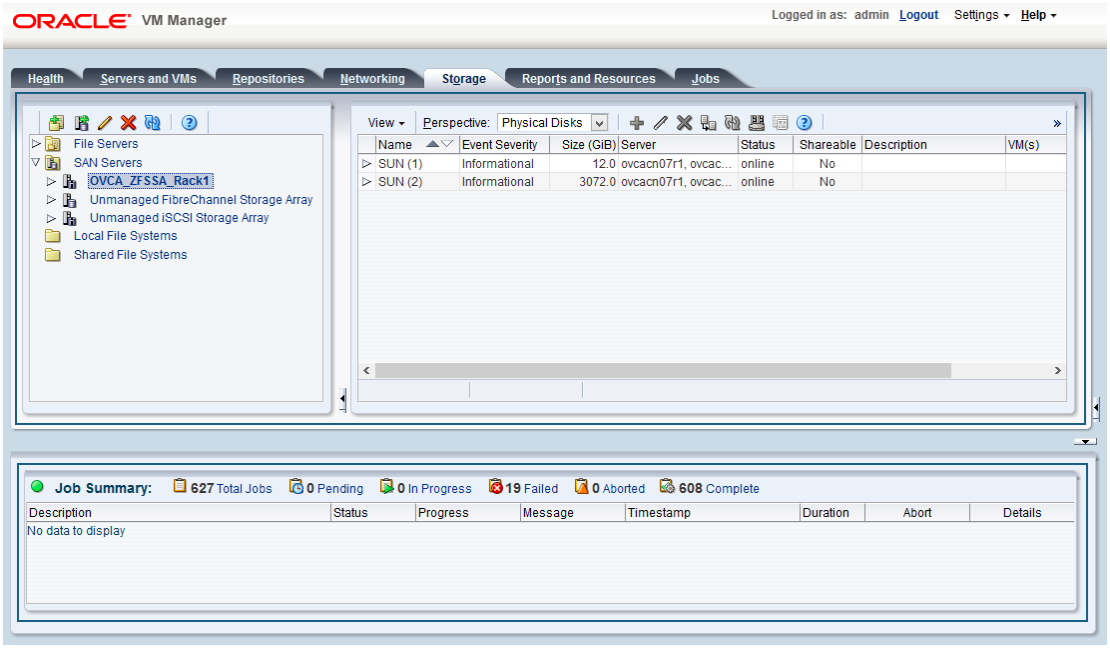
> **NOT_SUPPORTED:**
>
> Compute node provisioning relies on the internal ZFS file server and its exported storage. Changing the configuration will cause issues with provisioning and server pool clustering.

Oracle ZFS Storage Appliance ZS7-2

The internal ZFS Storage Appliance has sufficient disk space (100TB) for a basic virtualized environment, but the storage capacity for virtual disks and shared file systems can be extended with additional external storage for use within Oracle VM.

Information about expanding your Oracle VM environment with storage repositories located on the external storage is provided in Storage Tab in the *Oracle VM Manager User's Guide*. You are also fully capable of using other networked storage, available on the public network or a custom network, within your own Virtual Machines.

Figure 5-3 A view of the Storage tab (with Oracle ZFS Storage Appliance ZS7-2)



Tagging Resources in Oracle VM Manager

The **Reports and Resources** tab is used to configure global settings for Oracle VM and to manage tags, which can be used to identify and group resources. Since many of the global settings such as server update management and NTP configuration are managed automatically within Oracle Private Cloud Appliance, you do not need to edit any settings here. Those configuration changes could cause the appliance to malfunction.

You are able to create, edit and delete tags by following the instructions in Tags.

You can also use this tab to generate XML reports about Oracle VM objects and attributes, as described in Reports.

Managing Jobs and Events

The **Jobs** tab provides a view of the job history within Oracle VM Manager. It is used to track and audit jobs and to help troubleshoot issues within the Oracle VM environment. Jobs and events are described in detail within the Oracle VM Manager User's Guide in the section entitled Jobs Tab.

Since the Recurring Jobs, described in the Oracle VM Manager User's Guide, are all automated and handled directly by the Oracle Private Cloud Appliance, you must not edit any of the settings for recurring jobs.

Exporting VMs to Oracle Cloud Infrastructure

The Oracle VM Exporter Appliance is a special type of virtual machine used to export another virtual machine from the Oracle VM environment. This section describes how to install and

configure the Oracle VM Exporter Appliance on the Oracle Private Cloud Appliance. For more information, see Installing and Configuring the Oracle VM Exporter Appliance.

For the best experience exporting VMs to Oracle Cloud Infrastructure, consider these items.

- Use an Oracle Cloud Infrastructure region that is in the same region as your Oracle Private Cloud Appliance.
- Very slow network speeds in the customer premise network (<100Mbps) may result in timeouts, espectially when crossing regions.
- If you experience timeouts, contact Oracle Service.

Prerequisites

Before you begin, you need:

- A valid Oracle VM account
- An active tenancy and user account in Oracle Cloud Infrastructure
- Access to the internet in order to communicate with Oracle Cloud Infrastructure
- Access to the virtual disks of the VM being exported

> **Note:**
>
> The LUN's and shares directly mounted from the VM, and the data on it, will not be exported to Oracle Cloud Infrastructure as part of export process.

Prepare Your Oracle Cloud Infrastructure

You need to provide information that pairs the Oracle VM Exporter Appliance to your Oracle Cloud Infrastructure tenancy.

1. Collect this resource information about your Oracle Cloud Infrastructure environment, you need it to configure your Oracle VM Exporter Appliance:
   - Region
   - Compartment
   - Availability Domain
   - Instance Shapes (and their quotas)

   Find your Resource Identifiers.
2. The Oracle VM Exporter Appliance uses Oracle Cloud Infrastructure APIs to perform the export. Upload the Oracle VM Exporter Appliance public key to Oracle Cloud Infrastructure to export a virtual machine. See How to Upload the Public Key.

Create the Oracle VM Exporter Appliance Virtual Machine

1. Download the Oracle VM Exporter Appliance from Oracle Software Delivery Cloud (OSDC) at https://edelivery.oracle.com.

2. Create the Oracle VM Exporter Appliance virtual machine from the Oracle VM Exporter Appliance OVA. See Create Virtual Machine.
3. Once this virtual machine is created, you should edit the name to **Exporter Appliance**.

   Using this name enables the Oracle VM Exporter Appliance wizard to make several user interface steps easier.

Configure the Oracle VM Exporter Appliance Virtual Machine

For additional information see Configuring the Oracle VM Exporter Appliance Virtual Machine.

1. Log in to the Logging in to the Oracle VM Manager Web UI of your Oracle Private Cloud Appliance.
2. Ethernet-based systems can have NFS shares created on the internal ZFS storage appliance using VM Storage Networks for the Oracle VM Exporter Appliance *nfs share path*. The corresponding VM Storage network must be added to the Exporter Appliance for mounting the nfs share created on the internal ZFS storage appliance. For more information, see VM Storage Networks.

Create a Network for the Oracle VM Exporter Appliance VM

This section describes Oracle Private Cloud Appliance specific considerations to export a VM created on Rack1-Repository using the Oracle Private Cloud Appliance command line interface

1. Using SSH and an account with superuser privileges, log into the active management node.

```
# ssh root@10.100.1.101
root@10.100.1.101's password:
root@ovcamn05r1 ~]#
```

2. Launch the Oracle Private Cloud Appliance command line interface.

```
# pca-admin
Welcome to PCA! Release: 2.4.4
PCA>
```

3. Create an internal network.

```
PCA> create network internal_net rack_internal_network
Status: Success
```

4. Add the new internal network to the server pool.

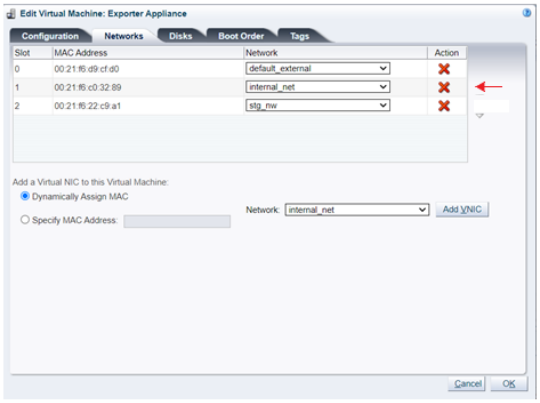
```
PCA> add network-to-tenant-group internal_net Rack1_ServerPool
Validating servers in the tenant group... This may take some time.

The job for sync all nodes in tenant group with the new network internal_net has
been submitted.
Please look into "/var/log/ovca.log" and "/var/log/ovca-sync.log" to monitor the
progress.

Status: Success
```

5. You can now configure the new internal network for Repository Exports, see Configure the New Network for Repository Exports.

Attach the New Network to the Oracle VM Exporter Appliance VM

1. From the Servers and VM tab, select the Exporter Appliance VM, then click the Edit icon.
2. Choose the network you just created from the Network drop down list.

Figure 5-4 Select Network Ports



Now that you have attached the internal network to the Exporter Appliance, you can use the example networks as described below.

- `default_external` network can be used to reach the Oracle Cloud Infrastructure.
- `internal_net` can be used for Repository Exports which can be mounted by Exporter appliance for VM disk conversions, see Configure the New Network for Repository Exports.
- `stg_nw` can be used for NFS share mount.

Prepare a Storage Repository

Depending on the location of the virtual disks of the VM you are exporting, choose the appropriate procedure.

> **Note:**
>
> Access to VM's created on the Rack1-Repository is provided to the exporter appliance using repository exports. The repository export is created on the newly created network on either vx2 or bond3 depending on the type of the rack.

- Prepare a LUN Repository

  When the virtual disks of the VM you are exporting are located in a LUN repository, follow these steps.

  1. Create a Repository Export of the LUN repository on any compute node where the repository is presented. The client IP should be the one assigned to the *ServiceVMOnly* interface, so it is accessible from Exporter Appliance VM.
  2. Run the below command on the Oracle VM Exporter Appliance VM to check if the repository exported above, is visible to it. It's should return the repository.

     ```
     showmount -e <IP-on-CN-from-Step-4>
     ```

  3. Edit the `/etc/hosts` file to translate the compute node hostname to the IP address from Step 4

- Prepare an NFS Repository

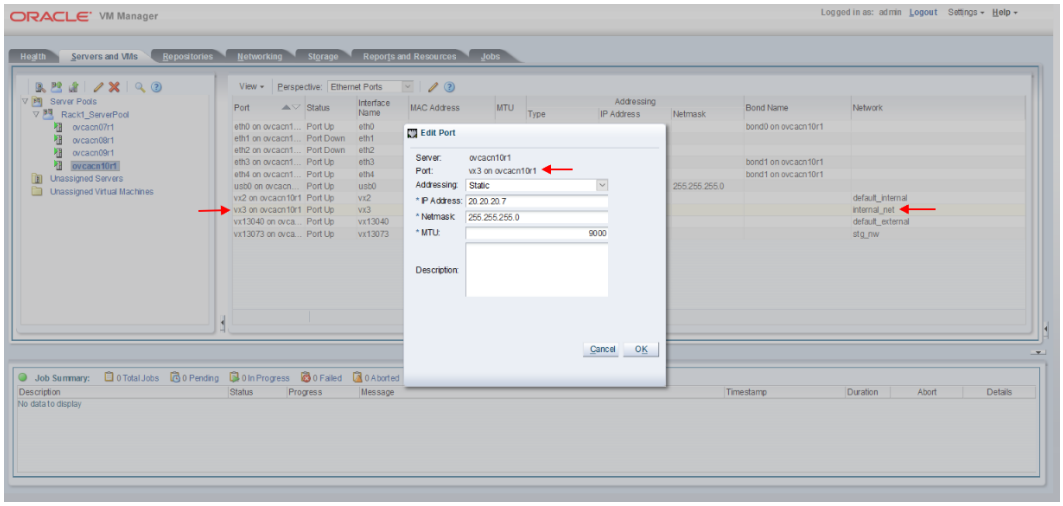
  When the virtual disks of the VM you are exporting are located in an NFS repository, the Oracle VM Exporter Appliance needs read-only access to NFS shares of repositories that contain virtual machine resources.

  1. Modify the NFS export on the NFS server to export these resources to the Oracle VM Exporter Appliance IP address on the appropriate Storage Network.

Configure the New Network for Repository Exports

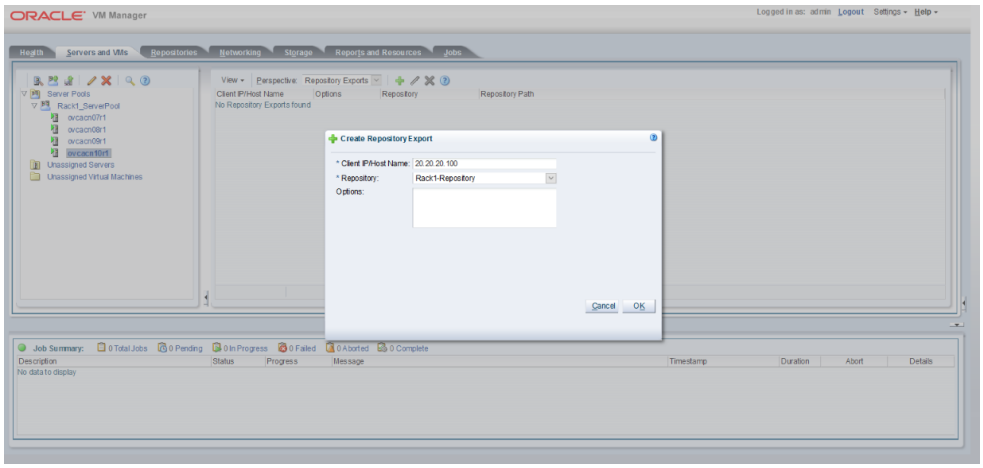
1. From the Servers and VM tab, select the compute node, then choose the Ethernet Port Perspective.
2. Choose the network you just created from the Network Ethernet Ports list.

Figure 5-5 Select Compute Node Ethernet Port Perspective



3. Assign a static IP address to the new internal network interface. This IP address should be in the same subnet as the VNIC of the Exporter Appliance.
4. From the Perspective drop down menu, choose Repository Exports.
5. Select Create Repository Export.

Figure 5-6 Select Create Repository Export



6. In the Client IP/Hostname field, enter the IP address assigned to the internal network VNIC used on the Exporter Appliance, and click OK.

   This internal network can now be used for Repository Exports used for ISCSI LUN-based or FC LUN-based repositories.

6

Servicing Oracle Private Cloud Appliance Components

This chapter explains the service procedures for Oracle Private Cloud Appliance in case a failure occurs. Optionally, you can configure the system with Oracle Auto Service Request (ASR), which generates a service request with Oracle automatically when it detects a hardware fault. Certain components of Private Cloud Appliance are customer-replaceable. These components are listed in this chapter, along with the replacement instructions.

Oracle Auto Service Request (ASR)

Oracle Private Cloud Appliance is qualified for Oracle Auto Service Request (ASR), a software feature for support purposes.

When ASR is enabled, a service request is automatically created and sent to Oracle Support Services when specific Private Cloud Appliance hardware faults occur. Both the My Oracle Support email account and the technical contact for Private Cloud Appliance are automatically notified that the service request was made. ASR expedites and simplifies the delivery of replacement hardware.

ASR detects faults in the most common hardware components, such as disks, fans, and power supplies. Oracle is continuously analyzing and improving the ASR fault rules. However, ASR does not detect all possible hardware faults, and it is not a replacement for other monitoring mechanisms. In addition, a service request might not be filed automatically in some cases, for example if a loss of connectivity to ASR occurs. Administrators should monitor their systems for faults and call Oracle Support Services if they do not receive notice that a service request has been filed automatically.

To use ASR, install and configure the software, register the Private Cloud Appliance as an ASR asset, and configure the Private Cloud Appliance to send hardware fault telemetry to Oracle Support.

For more information about ASR, see the following resources:

- Oracle Auto Service Request web page: https://www.oracle.com/servers/technologies/auto-service-request.html.
- Oracle Auto Service Request user documentation: https://docs.oracle.com/cd/E37710_01/index.htm.

Installing and Configuring ASR

ASR Prerequisites

Before you install ASR, ensure the following prerequisites are satisfied:

- You have a valid My Oracle Support account.

  If necessary, create an account at https://support.oracle.com/.
- The following are set up correctly in My Oracle Support:

  - Technical contact person at the customer site who is responsible for Private Cloud Appliance.
  - Valid shipping address at the customer site where the Private Cloud Appliance is located, so that parts are delivered to the site where they must be installed.
- The management nodes have an active outbound Internet connection using HTTPS or an HTTPS proxy.

ASR Manager (ASRM)

Download ASR Manager (ASRM) packages to a secure location that is accessible from both management nodes. ASRM must be installed on both management nodes. Both management nodes must have an active outbound Internet connection using HTTPS or an HTTPS proxy. Failover must be configured so that the ASR Manager role is always fulfilled by the management node that also has the active role.

You can register the ASRM as a stand-alone ASRM, or as a relay to another ASRM in your network, including the Oracle Advanced Support Gateway. Registering the Private Cloud Appliance as a stand-alone ASRM means it communicates directly with the Oracle backend systems through My Oracle Support, which is the standard registration method.

Installing ASR

To install and configure ASR, see the following support documents:

- How to Install Auto Service Request (ASR) on Private Cloud Appliance (PCA) 2.4.1 or Later (Doc ID 2560988.1).
- How to Install Auto Service Request (ASR) on Private Cloud Appliance (PCA) X8 (Doc ID 2560988.1).

Adding ASR Assets

When ASR is installed on your Private Cloud Appliance, log in to your My Oracle Support account and approve the Private Cloud Appliance as a new asset. See How To Manage and Approve Pending Oracle Auto Service Request (ASR) Assets In My Oracle Support (Doc ID 1329200.1).

Enabling ASR

To enable ASR, the Private Cloud Appliance components must be configured to send hardware fault telemetry to the ASR Manager (ASRM) software. See Phone Home Service.

Replaceable Components

According to Oracle's Component Replacement Policy, the replaceable components in your system are designated as either field-replaceable units (FRUs) or customer-replaceable units (CRUs).

- A part designated as a FRU must be replaced by an Oracle-qualified service technician.
- A part designated as a CRU can be replaced by a person who is not an Oracle-qualified service technician.

Servicing instructions included in this Oracle Private Cloud Appliance Administration Guide are focused primarily on CRUs. For FRU replacement, please contact Oracle.

Rack Components

The following table lists the replaceable components of the Oracle Private Cloud Appliance rack.

> **Note:**
>
> For the current list of replacement parts and their manufacturing part numbers, refer to the Oracle Private Cloud Appliance components list in the Oracle System Handbook.
>
> You access the Oracle System Handbook using this link: https://support.oracle.com/handbook_private/.
>
> Click *Current Systems*, then click your generation of *Oracle Private Cloud Appliance Hardware* to open the main product page in the System Handbook.

Table 6-1 Replaceable Oracle Private Cloud Appliance Rack Components

Component Description	Hot-Swap
Oracle Rack Cabinet 1242:	No
Jumper Cable C13-C14, 2m	Yes
Ethernet Cable, Category 5/5E, 10ft, Black	Yes
Ethernet Cable, Category 5/5E, 10ft, Blue	Yes
Ethernet Cable, Shielded, Category 5E, 1m, Grey	Yes
Ethernet Cable, Category 5, 8ft, Black	Yes
Ethernet Cable, Category 5, 8ft, Green	Yes
Ethernet Cable, Category 5, 8ft, Yellow	Yes
Active Optical Cable, Blue, 3m	Yes
10Gbps QSFP to QSFP Cable, Passive Copper, 3m	Yes
QSFP28 Cable, 30AWG, Passive Copper, 3m	Yes
QSFP28 Cable, 30AWG, Passive Copper, 1m	Yes
1U/2U Screw-Mount Slide Rail Kit	No
1U/2U Cable Management Arm (Snap-in)	No
Power Distribution Units (PDUs):	
15KVA Single-Phase PDU, North America	Yes
15KVA Three-Phase PDU, North America	Yes
15KVA Three-Phase PDU, International	Yes
22KVA Single-Phase PDU, North America	Yes
22KVA Single-Phase PDU, International	Yes

Table 6-1 (Cont.) Replaceable Oracle Private Cloud Appliance Rack Components

Component Description	Hot-Swap
24KVA Three-Phase PDU, North America	Yes
24KVA Three-Phase PDU, International	Yes

For rack-level component servicing instructions, see Servicing the Oracle Private Cloud Appliance Rack System.

Oracle Server X9-2 Components

The following table lists the replaceable components of the Oracle Server X9-2 compute nodes.

> **Note:**
>
> For the current list of replacement parts and their manufacturing part numbers, refer to the Oracle Private Cloud Appliance components list in the Oracle System Handbook.
>
> You access the Oracle System Handbook using this link: https://support.oracle.com/handbook_private/.
>
> Click *Current Systems*, then click your generation of *Oracle Private Cloud Appliance Hardware* to open the main product page in the System Handbook.

Table 6-2 Replaceable Oracle Server X9-2 Components

Component Description	Hot-Swap
Motherboard Assembly	No
Fan Modules	Yes
PCI Risers	No
PCI Cards	No
Type A269.2 1200 Watt AC Input Power Supply	Yes
(2) Thirty-two-core Intel Xeon P-8358 processors (2.6 GHz), 250W	No
CPU Heatsink	No
Front LED Indicator Module	No
Disk Backplane Assembly	No
Internal M2 flash SSDs	No
DDR4 DIMM, 32GB	No
DDR4 DIMM, 64GB	No
Temperature sensor	No
Dual port 100Gbps Ethernet OCP V3 Network Interface Card	No
(2) 240GB M.2 SATA boot devices configured as RAID 1 mirror	No

Table 6-2 (Cont.) Replaceable Oracle Server X9-2 Components

Component Description	Hot-Swap
System Battery	No
NVMe Cables	No

For Oracle Server X9-2 component servicing instructions, see Servicing a Compute Node.

Oracle Server X8-2 Components

The following table lists the replaceable components of the Oracle Server X8-2 compute nodes.

> **Note:**
>
> For the current list of replacement parts and their manufacturing part numbers, refer to the Oracle Private Cloud Appliance components list in the Oracle System Handbook.
>
> You access the Oracle System Handbook using this link: https://support.oracle.com/handbook_private/.
>
> Click *Current Systems*, then click your generation of *Oracle Private Cloud Appliance Hardware* to open the main product page in the System Handbook.

Table 6-3 Replaceable Oracle Server X8-2 Components

Component Description	Hot-Swap
Motherboard Assembly	No
Quad Counter Rotating Fan Module	Yes
1-Slot PCI Express Riser Assembly	No
2-Slot PCI Express Riser Assembly	No
Type A266 800/1200 Watt AC Input Power Supply	Yes
Sixteen-core Intel Xeon G-5218 processor (2.3 GHz), 125W	No
Twenty-four-core Intel Xeon P-8260 processor (2.4 GHz), 165W	No
CPU Heatsink	No
2.5" Disk Cage Front Indicator Module	No
8-Slot 2.5" Disk Backplane Assembly	No
1.2TB - 10000 RPM SAS-3 Disk Assembly with 1 bracket	Yes
DDR4 DIMM, 32GB	No
DDR4 DIMM, 64GB	No
Dual port 100Gbps Ethernet PCI Express 3.0 Host Channel Adapter (CX-5)	No
Dual port 32Gbps Fibre Channel PCI Express 3.0 Host Bus Adapter (optional component)	No

Table 6-3 (Cont.) Replaceable Oracle Server X8-2 Components

Component Description	Hot-Swap
8-Port 12Gbps SAS-3 RAID PCI Express HBA	No
System Battery	No
Cable kit	No

For Oracle Server X8-2 component servicing instructions, see Servicing a Compute Node.

Oracle ZFS Storage Appliance ZS7-2 Components

The following table lists the replaceable components of the Oracle ZFS Storage Appliance ZS7-2.

> **Note:**
>
> For the current list of replacement parts and their manufacturing part numbers, refer to the Oracle Private Cloud Appliance components list in the Oracle System Handbook.
>
> You access the Oracle System Handbook using this link: https://support.oracle.com/handbook_private/.
>
> Click *Current Systems*, then click your generation of *Oracle Private Cloud Appliance Hardware* to open the main product page in the System Handbook.

Table 6-4 Replaceable Oracle ZFS Storage Appliance ZS7-2 Components

Component Description	Hot-Swap
Oracle ZFS Storage Appliance ZS7-2 Storage Head:	NA
2.3GHz Intel 18-Core Xeon G-6140, 140W	No
Pre-greased CPU Heatsink	No
64GB DDR4 DIMM	No
7.68TB SAS-3 Disk Assembly	Yes
1.2TB - 10000 RPM SAS-3 Disk Assembly	Yes
Fortville dual PCIe 40Gb Ethernet Adapter	No
2.5" Disk Cage Front Indicator Module	No
12-Slot 2.5" Disk Backplane Assembly	No
Interlock Cable, 125mm	No
Cable Kit	No
Dual Counter Rotating Fan Module	Yes
System Board Assembly	No

Table 6-4 (Cont.) Replaceable Oracle ZFS Storage Appliance ZS7-2 Components

Component Description	Hot-Swap
3V lithium coin cell battery	No
Type A266 800/1200 Watt AC Input Power Supply	Yes
Cluster Heartbeat Assembly	No
8-Port 12Gbps SAS HBA	No
4x4 Port 12Gbps SAS-3 PCI Express HBA	No
Oracle Storage DE3-24C Disk Shelf:	NA
580 Watt AC Input Power Supply	Yes
12Gbps SAS-3 I/O Controller Module	Yes
4RU Chassis Assembly with Midplane	No
36-Pin Mini SAS3 HD Cable, SFF-8644 to SFF-8644, 3M	Yes
DE3-24C Mounting Rail Kit	No
14TB - 7200 RPM SAS-3 Disk Drive Assembly	Yes
200GB SAS-3 Solid State Drive Assembly	Yes

For Oracle ZFS Storage Appliance ZS7-2 component servicing instructions, see Servicing the Oracle ZFS Storage Appliance ZS7-2.

Preparing Oracle Private Cloud Appliance for Service

This section describes safety considerations and prerequisites for component replacement procedures.

Safety Precautions

For your protection, observe the following safety precautions when servicing your equipment:

- Follow all standard cautions, warnings, and instructions marked on the equipment and described in the following documents:
  - The printed document *Important Safety Information for Sun Hardware Systems (7063567)*
  - The Oracle Private Cloud Appliance Safety and Compliance Guide
- Follow the safety guidelines described in the Oracle Private Cloud Appliance Installation Guide:
- Follow the electrostatic discharge safety practices as described in this section.
- Disconnect all power supply cords before servicing components.

Electrostatic Discharge Safety

Devices that are sensitive to electrostatic discharge (ESD), such as motherboards, PCIe cards, drives, processors, and memory cards require special handling.

> **Caution:**
>
> **Equipment Damage**
>
> Take antistatic measures and do not touch components along their connector edges.

- **Use an antistatic wrist strap.**

  Wear an antistatic wrist strap and use an antistatic mat when handling components such as drive assemblies, boards, or cards. When servicing or removing rack node components, attach an antistatic strap to your wrist and then to a metal area on the chassis. Then disconnect the power cords from the component. Following this practice equalizes the electrical potentials between you and the component.

  An antistatic wrist strap is *not* included in the Oracle Private Cloud Appliance shipment.

- **Use an antistatic mat.**

  Place ESD-sensitive components such as the motherboard, memory, and other PCB cards on an antistatic mat.

  The following items can be used as an antistatic mat:

  – Antistatic bag used to wrap an Oracle replacement part
  – An ESD mat (orderable from Oracle)
  – A disposable ESD mat (shipped with some replacement parts or optional system components)

Servicing the Oracle Private Cloud Appliance Rack System

This section provides instructions to service replaceable components (CRUs/FRUs) in the appliance rack. Before starting any service procedure, read and follow the guidelines in Preparing Oracle Private Cloud Appliance for Service.

Powering Down Oracle Private Cloud Appliance (When Required)

Some service procedures may require you to power down the Oracle Private Cloud Appliance. Perform the following steps to manually power down the system.

> **Caution:**
>
> Whenever a hardware system must be powered down, make sure that the virtual machines hosted by that system are shut down first. If you power down the appliance with running virtual machines, these will be in an error state when the system is returned to operation.
>
> For details, consult the Oracle VM Manager User's Guide.
>
> - Stop Virtual Machines
> - Stop Server

Shutting Down the Oracle VM Environment

1. Log in to Oracle VM Manager and open the Servers and VMs tab.
2. Using the navigation tree, select each virtual machine and click Stop to shut it down gracefully.

   If the applications hosted by your VMs require the services and machines to be shut down in a particular order, respect those requirements just like you would with physical machines.

   Once the VMs have been shut down, you can proceed to power off the compute nodes.
3. Using the navigation tree, select each compute node and click Stop Server to shut it down gracefully.
4. Using SSH and an account with superuser privileges, log into the active management node at the management virtual IP address. Stop Oracle VM Manager by entering the command `service ovmm stop`.

Powering Down the System for Service

1. If, at this point, any compute nodes have not shut down properly, press the Power button on the running compute nodes in order to shut them down gracefully.
2. Press the Power button on the management nodes in order to shut them down gracefully.

   Once the servers are powered off, you can proceed to power off the storage appliance.
3. Press the Power button on the storage server heads attached to the chassis of the storage device.
4. Toggle the rack Power switches to the Off position.

> **Note:**
>
> The Ethernet switches do not have power switches. They power off when power is removed, by way of the power distribution unit (PDU) or at the breaker in the data center.

Returning the System to Operation After Service or Unplanned Outage

1. Toggle the power distribution unit (PDU) circuit breakers of both PDUs to the On position.
2. Wait at least two minutes to allow the PDUs to complete their power-on sequence.

The Ethernet switches are powered on with the PDUs.

3. Press the Power button on the storage server heads.

   Wait approximately two minutes until the power-on self-test completes, and the Power/OK LED on the front panel lights and remains lit.

4. Press the Power button on the management nodes.

   The management node that completes booting first assumes the active role.

> **Note:**
>
> Compute nodes do not power on automatically like the internal ZFS Storage Appliance, switches and other components. Make sure that the management nodes and internal storage are up and running, then manually power on the compute nodes.

5. When the management nodes are up, press the Power button on the compute nodes.

> **Caution:**
>
> The compute node ILOM policy for automatic power-on is disabled, and must remain disabled, to prevent a server from booting prematurely and disrupting the correct boot order of the appliance components.

When all compute nodes are up, verify the status of all system components in Oracle VM Manager.

If no components are in error state, the appliance is ready to resume normal operation.

Service Procedures for Rack System Components

For parts that are not hot-swappable, power down the Oracle Private Cloud Appliance before starting the service procedure. Generally speaking, hot-swappable components can be serviced without specific additional steps.

Table 6-5 Service Instructions for Rack System Components

Replaceable Part(s)	Oracle Server X8-2 Instructions	Oracle Server X9-2 Instructions
Power cables	NA	NA
Ethernet cables	NA	NA
Cable management arms (CMAs) (Oracle-qualified service technician only)	• Remove the Cable Management Arm • Install the Cable Management Arm	• Remove the Cable Management Arm • Install the Cable Management Arm

Table 6-5 (Cont.) Service Instructions for Rack System Components

Replaceable Part(s)	Oracle Server X8-2 Instructions	Oracle Server X9-2 Instructions
Slide rails (Oracle-qualified service technician only)	To service the slide rails, the server must be removed from the rack. For instructions, refer to: • Remove the Server From the Rack • Reinstall the Server Into the Rack For slide rail installation instructions, refer to the section Attach the Slide-Rails. To remove the slide rails, reverse the installation steps.	To service the slide rails, the server must be removed from the rack. For instructions, refer to: • Remove the Server From the Rack • Reinstall the Server Into the Rack For slide rail installation instructions, refer to the section Attach the Slide-Rails. To remove the slide rails, reverse the installation steps.

Servicing a Compute Node

This section provides instructions to service replaceable components in a supported Oracle Server X8-2 or Oracle Server X9-2 compute node. Before starting any service procedure, read and follow the guidelines in Preparing Oracle Private Cloud Appliance for Service.

Powering Down a Compute Node for Service (When Required)

If you need to execute a service procedure that requires the compute node to be powered down, follow these instructions:

Placing a Compute Node Into Maintenance Mode

Before a compute node compute node can be powered down, it must be placed into maintenance mode from within Oracle VM Manager. As a result, all virtual machines running on the compute node are automatically migrated to other servers in the Oracle VM server pool, if they are available. Information on maintenance mode is provided in the *Oracle VM Manager User's Guide* section entitled Edit Server.

1. Log in to the Oracle VM Manager Web UI.

   For details, refer to the section "Logging in to the Oracle VM Manager Web UI".

   a. Enter the following address in a Web browser: https://***manager-vip***:7002/ovm/console.

      Replace ***manager-vip*** with the virtual IP address, or corresponding host name, that you have configured for your management nodes during installation.

   b. Enter the Oracle VM Manager user name and password in the respective fields and click OK.

2. In the **Servers and VMs** tab, select the Oracle VM Server in the navigation pane. Click **Edit Server** in the management pane toolbar.

   The **Edit Server** dialog box is displayed.

3. Select the **Maintenance Mode** check box to place the Oracle VM Server into maintenance mode. Click OK.

The Oracle VM Server is in maintenance mode and ready for servicing.

4. When the compute node is ready to rejoin the Oracle VM server pool, perform the same procedure and clear the **Maintenance Mode** check box.

Powering Down the System

These steps briefly describe the procedure. For detailed instructions, refer to:

- For Oracle X8-2 Servers: Perparing the Server for Component Replacement
- For Oracle X9-2 Servers: Preparing the Server for Component Replacement

1. Power down the server gracefully whenever possible.

   The easiest way is to press and quickly release the Power button on the front panel.

2. Perform immediate shutdown only if the system does not respond to graceful power-down tasks.

> **Caution:**
>
> An immediate power down might corrupt system data, therefore, only use this procedure to power down the server after attempting the graceful power down procedure.

3. Disconnect the power cables from the server.
4. Extend the server to the service position.
5. All service operations can be performed while the server is in the service position.

Returning the System to Operation

These steps briefly describe the procedure. For detailed instructions, refer to:

- For Oracle X8-2 Servers: Returning the Server to Operation
- For Oracle X9-2 Servers: Returning the Server to Operation

1. If the top cover was removed to service a component, reinstall the top cover on the server.
2. If the server was removed, reinstall it into the rack.
3. Return the server to its normal operational position in the rack, making sure the CMA is correctly installed.
4. Reconnect data cables and power cords.
5. Power on the server.

Service Procedures for Compute Node Components

For parts that are not hot-swappable, power down the compute node before starting the service procedure. If the server is in use in the Oracle VM environment, place it in maintenance mode first. This protects your virtual infrastructure against data corruption, and allows it to remain in service as long as the configuration of your environment allows it.

Generally speaking, hot-swappable components can be serviced without specific additional steps for Oracle Private Cloud Appliance. Follow the applicable procedure in the Service Manual. The following tables provide links to each service procedure and indicates whether parts are hot-swappable or require the component to be taken offline and powered down.

Table 6-6 Service Procedures for Oracle Server X8-2 Components

Replaceable Part(s)	Hot-Swap	URL
Storage drives	Yes	https://docs.oracle.com/en/servers/x86/x8-2/service-manual/gquak.html
Fan Modules	Yes	https://docs.oracle.com/en/servers/x86/x8-2/service-manual/gquhg.html
Power supplies	Yes	https://docs.oracle.com/en/servers/x86/x8-2/service-manual/gqunc.html
DIMMs (Oracle-qualified service technician only)	No	https://docs.oracle.com/en/servers/x86/x8-2/service-manual/gqvkr.html
PCI Express risers (Oracle-qualified service technician only)	No	https://docs.oracle.com/en/servers/x86/x8-2/service-manual/gqvft.html
PCI Express cards (Oracle-qualified service technician only)	No	https://docs.oracle.com/en/servers/x86/x8-2/service-manual/gqvjk.html
Battery	No	https://docs.oracle.com/en/servers/x86/x8-2/service-manual/gqviw.html

Table 6-7 Service Procedures for Oracle Server X9-2 Components

Replaceable Part(s)	Hot-Swap	URL
Storage drives	Yes	https://docs.oracle.com/en/servers/x86/x9-2/service-manual/servicing-storage-drives-cru.html
Fan Modules	Yes	https://docs.oracle.com/en/servers/x86/x9-2/service-manual/servicing-fan-modules-cru.html
Power supplies	Yes	https://docs.oracle.com/en/servers/x86/x9-2/service-manual/servicing-power-supplies-cru.html
Internal M.2 SSDs	No	https://docs.oracle.com/en/servers/x86/x9-2/service-manual/servicing-internal-m-2-flash-ssds-cru.html
DIMMs (Oracle-qualified service technician only)	No	https://docs.oracle.com/en/servers/x86/x9-2/service-manual/servicing-dimms-cru.html
PCI Express risers (Oracle-qualified service technician only)	No	https://docs.oracle.com/en/servers/x86/x9-2/service-manual/servicing-pcie-risers-cru.html
PCI Express cards (Oracle-qualified service technician only)	No	https://docs.oracle.com/en/servers/x86/x9-2/service-manual/servicing-pcie-cards-cru.html
Battery	No	https://docs.oracle.com/en/servers/x86/x9-2/service-manual/servicing-battery-cru.html

Servicing the Oracle ZFS Storage Appliance ZS7-2

This section provides instructions to service replaceable components (CRUs/FRUs) in the Oracle ZFS Storage Appliance ZS7-2. Before starting any service procedure, read and follow the guidelines in Preparing Oracle Private Cloud Appliance for Service.

Powering Down the Oracle ZFS Storage Appliance ZS7-2 for Service (When Required)

If you need to execute a service procedure that requires the Oracle ZFS Storage Appliance ZS7-2 to be powered down, follow these instructions:

Powering Down the Storage Head/Controller

Because the storage controllers are clustered, there is no loss of access to storage when one controller is powered down for service. Performing a graceful shutdown ensures that data is saved and not corrupted, and that resources are assigned to the other controller in the storage head cluster. Power down a controller for component replacement using one of the following methods:

- Log in to the UI by using the server's IP address in the appliance management network:
  1. In your browser, enter `https://`***`ipaddress`***`:215`.
  2. Log in as root, using the system-wide Oracle Private Cloud Appliance password.
  3. Click the **Power** icon on the left side under *masthead*.
- Alternatively, SSH in to the storage appliance as root, and enter the command `maintenance system poweroff`.

If graceful shutdown as described above is not possible, use the power button:

- Use a pen or non-conducting pointed object to press and release the Power button on the front panel.
- SSH or use a serial connection to log in to the service processor (SP), and then issue the command `stop /SYS`.
- If the server did not respond, initiate an emergency shutdown. Press and hold the Power button for at least four seconds until the Power/OK status indicator on the front panel flashes, indicating that the storage controller is in standby power mode. To completely remove power, disconnect the AC power cords from the rear panel of the storage controller.

> **Caution:**
>
> An emergency shutdown causes all applications and files to be closed abruptly without saving. You might corrupt or lose system data, or lose the server configuration (the resources assigned to it) during an immediate power down.

> **Note:**
>
> **Powering down the disk shelf is not required**
>
> All replaceable components in the disk shelf are hot-swappable. The disk shelf itself does not need to be powered down for the replacement of defective components.
>
> However, do not remove a component if you do not have an immediate replacement. The disk shelf must not be operated without all components in place.

Powering on the Storage Appliance

> **Caution:**
>
> The disk shelf must not be operated without all components in place.

1. Connect any storage head power and data cables you removed to service a component.
2. Power on the server by pressing the Power button on the front panel.

   If you are not physically located at the system, use either of these ILOM methods instead:

   - Log in to the **Oracle ILOM web interface**.

     Click Host Management > Power Control, and in the Actions list click **Power On**.
   - Log in to the **Oracle ILOM command-line interface** (CLI).

     At the CLI prompt, type the following command: `start /System`.
3. When the controller is powered on and the power-on self-test (POST) code checkpoint tests have completed, the green Power/OK status indicator on the front panel lights and remains lit.
4. If you performed a graceful shutdown earlier, return resources to the server that was just serviced.
   a. Log into the web UI for the server that was not serviced.
   b. Go to Configuration > Cluster.
   c. Click **Failback**.

> **Note:**
>
> For information about configuring the clustered servers and attached disk shelves, see the "Oracle ZFS Storage System Administration Guide" for the appropriate software release.

Service Procedures for Oracle ZFS Storage Appliance ZS7-2 Components

For parts that are not hot-swappable, power down the Oracle ZFS Storage Appliance ZS7-2 before starting the service procedure.

NOT_SUPPORTED:

If you need to execute a service procedure that interrupts the connection between virtual machines and their virtual disks, shut down the virtual machines in Oracle VM Manager prior to servicing the storage hardware. Disconnecting a running virtual machine from its disks may cause data corruption.

Generally speaking, hot-swappable components can be serviced without specific additional steps for Oracle Private Cloud Appliance. Follow the applicable procedure in the Service Manual. The following table provides links to each service procedure and indicates whether parts are hot-swappable or require the component to be taken offline and powered down.

Table 6-8 Service Procedures for Oracle ZFS Storage Appliance ZS7-2 Components

Replaceable Part(s)	Hot-Swap	URL
Storage head hard drives	Yes	https://docs.oracle.com/cd/F13758_01/html/F13771/gtbno.html#scrolltoc
Disk shelf drives	Yes	https://docs.oracle.com/cd/F13758_01/html/F13771/goxds.html#scrolltoc
Fan modules	Yes	https://docs.oracle.com/cd/F13758_01/html/F13771/gtbxa.html#scrolltoc
Storage head power supplies	Yes	https://docs.oracle.com/cd/F13758_01/html/F13771/gtbon.html#scrolltoc
Disk shelf power supplies	Yes	https://docs.oracle.com/cd/F13758_01/html/F13771/goxbs.html#scrolltoc
Memory modules (Oracle-qualified service technician only)	No	https://docs.oracle.com/cd/F13758_01/html/F13771/gtbou.html#scrolltoc
PCI Express cards (Oracle-qualified service technician only)	No	https://docs.oracle.com/cd/F13758_01/html/F13771/gtbnz.html#scrolltoc
Battery	No	https://docs.oracle.com/cd/F13758_01/html/F13771/gtbwl.html#scrolltoc
Disk shelf I/O modules (Oracle-qualified service technician only)	Yes	https://docs.oracle.com/cd/F13758_01/html/F13771/goxeo.html#scrolltoc
Disk shelf SIM boards (Oracle-qualified service technician only)	Yes	https://docs.oracle.com/cd/F13758_01/html/F13771/goxef.html#scrolltoc

Servicing Cisco Nexus 9336C-FX2 Switch Components

This section provides instructions to service replaceable components (CRUs/FRUs) in an Cisco Nexus 9336C-FX2 Switch. Before starting any service procedure, read and follow the guidelines in Preparing Oracle Private Cloud Appliance for Service.

For parts that are not hot-swappable, power down the Cisco Nexus 9336C-FX2 Switch before starting the service procedure.

> **Caution:**
>
> Management, storage, VM and external network connectivity may be affected while the Cisco Nexus 9336C-FX2 Switch or an I/O module is out of service. Please take the necessary precautions.

> **Caution:**
>
> When replacing the entire switch assembly, begin by saving the configuration from the existing component, so that you can restore the configuration after replacement.

Generally speaking, hot-swappable components can be serviced without specific additional steps for Oracle Private Cloud Appliance. Follow the applicable procedure in the Service Manual. The following table provides links to each service procedure and indicates whether parts are hot-swappable or require the component to be taken offline and powered down.

Table 6-9 Service Procedures for Cisco Nexus 9336C-FX2 Switch Components

Replaceable Part(s)	Hot-Swap	URL
Power supplies (Oracle-qualified service technician only)	Yes	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/n9336cfx2_hig/guide/b_n9336cFX2_nxos_hardware_installation_guide/b_n9336cFX2_nxos_hardware_installation_guide_chapter_0101.html#concept_65E9CCDC546846709DF28AA295965D5C
Fan modules (Oracle-qualified service technician only)	Yes	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/n9336cfx2_hig/guide/b_n9336cFX2_nxos_hardware_installation_guide/b_n9336cFX2_nxos_hardware_installation_guide_chapter_0101.html#concept_62AF8E25C1F744AD9B2534999E521EE9

Servicing Cisco Nexus 9348GC-FXP Switch Components

This section provides instructions to service replaceable components (CRUs/FRUs) in an Cisco Nexus 9348GC-FXP Switch. Before starting any service procedure, read and follow the guidelines in Preparing Oracle Private Cloud Appliance for Service.

For parts that are not hot-swappable, power down the Cisco Nexus 9348GC-FXP Switch before starting the service procedure.

Note:

The switches are configured in high availability pairs, so if one switch fails, network traffic continues, although it may be degraded. If more than one switch is being serviced at one time, you should prepare your environment for disruption to the network connectivity.

NOT_SUPPORTED:

Internal Ethernet connectivity is affected while the component is out of service. Please take the necessary precautions.

Caution:

When replacing the entire switch assembly, begin by saving the configuration from the existing component, so that you can restore the configuration after replacement.

Generally speaking, hot-swappable components can be serviced without specific additional steps for Oracle Private Cloud Appliance. Follow the applicable procedure in the component documentation. The following table provides links to each service procedure and indicates whether parts are hot-swappable or require the component to be taken offline and powered down.

Table 6-10 Service Procedures for Cisco Nexus 9348GC-FXP Switch Components

Replaceable Part(s)	Hot-Swap	URL
Power supplies	Yes	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/n9348gcfxp_hig/guide/b_c9348gc-fxp_nxos_mode_hardware_install_guide/b_c9348gc-fxp_nxos_mode_hardware_install_guide_chapter_0101.html#concept_65E9CCDC546846709DF28AA295965D5C
Fan module	Yes	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/n9348gcfxp_hig/guide/b_c9348gc-fxp_nxos_mode_hardware_install_guide/b_c9348gc-fxp_nxos_mode_hardware_install_guide_chapter_0101.html#concept_62AF8E25C1F744AD9B2534999E521EE9

7
Troubleshooting

This chapter describes how to resolve a number of common problem scenarios.

Setting the Oracle Private Cloud Appliance Logging Parameters

When troubleshooting or if you have a support query open, you may be required to change the logging parameters for your Oracle Private Cloud Appliance. The settings for this are contained in `/etc/ovca.conf`, and can be changed using the CLI.

The following instructions must be followed for each of the two management nodes in your environment.

Changing the Oracle Private Cloud Appliance Logging Parameters for a Management Node

1. Gain command line access to the management node. Usually this is achieved using SSH and logging in as the root user with the global Oracle Private Cloud Appliance password.
2. Use the CLI, as described in Oracle Private Cloud Appliance Command Line Interface (CLI), to view or modify your appliance log settings. The CLI safely reads and edits the `/etc/ovca.conf` file, to prevent the possibility of configuration file corruption.
   - To view the current values for the configurable settings in the configuration file run the CLI as follows:

     ```
     # pca-admin show system-properties
     ```

   - To change the log level:

     ```
     # pca-admin set system-property log_level service
                   LEVEL
     ```

     The ***service*** argument is the log file category to which the new log level applies. The following services can be specified: backup, cli diagnosis, monitor, ovca, snmp, syncservice.

     The ***LEVEL*** value is one of the following: DEBUG, INFO, WARNING, ERROR, CRITICAL.

   - To change the log file size:

     ```
     # pca-admin set system-property log_size SIZE
     ```

     Where ***SIZE***, expressed in MB, is a number from 1 to 512.

   - To change the number of backup log files stored:

     ```
     # pca-admin set system-property log_count COUNT
     ```

     Where ***COUNT*** is a number of files ranging from 0 to 100.

- To change the location where log files are stored:

  ```
  # pca-admin set system-property log_file service
                PATH
  ```

  Where ***PATH*** is the new location where the log file for the selected ***service*** is to be stored. The following services can be specified: backup, cli, diagnosis, monitor, ovca, snmp, and syncservice.

  > **Caution:**
  >
  > Make sure that the new path to the log file exists. Otherwise, the log server stops working.
  >
  > The system always prepends `/var/log` to your entry. Absolute paths are converted to `/var/log/`***`PATH`*** .
  >
  > During management node upgrades, the log file paths are reset to the default values.

3. The new log level setting only takes effect after a management node has been rebooted or the service has been restarted by running the `service ovca restart` command on the active management node shell.

Adding Proxy Settings for Oracle Private Cloud Appliance Updates

If your data center does not provide unlimited internet access and has a proxy server in place to control HTTP, HTTPS or FTP traffic, you may need to configure your management nodes to be able to access external resources; for example for the purpose of performing software updates.

The following instructions must be followed for each of the two management nodes in your environment.

Adding Proxy Settings for a Management Node

1. Gain command line access to the management node. Usually this is achieved using SSH and logging in as the root user with the global Oracle Private Cloud Appliance password.
2. Use the CLI, as described in Oracle Private Cloud Appliance Command Line Interface (CLI), to view or modify your proxy settings. The CLI safely reads and edits the `/etc/ovca.conf` file, to prevent the possibility of configuration file corruption.

   - To view the current values for the configurable settings in the configuration file run the CLI as follows:

     ```
     # pca-admin show system-properties
     ```

   - To set an HTTP proxy:

     ```
     # pca-admin set system-property http_proxy http://IP:PORT
     ```

Where ***IP*** is the IP address of your proxy server, and ***PORT*** is the TCP port on which it is listening.

> **Caution:**
>
> If your proxy server expects a user name and password, these should be provided when the proxy service is accessed. Do not specify credentials as part of the proxy URL, because this implies that you send sensitive information over a connection that is not secure.

- To set an HTTPS proxy:

  ```
  # pca-admin set system-property https_proxy https://IP:PORT
  ```

- To set an FTP proxy:

  ```
  # pca-admin set system-property ftp_proxy ftp://IP:PORT
  ```

3. Setting any single parameter automatically rewrites the configuration file and the proxy settings become active immediately.

Changing the Oracle VM Agent Password

The password of the Oracle VM Agent cannot be modified in the Authentication tab of the Oracle Private Cloud Appliance Dashboard, nor with the `update password` command of the Oracle Private Cloud Appliance CLI. If you need to change the agent password, use Oracle VM Manager.

Instructions to change the Oracle VM Agent password can be found at the following location: Change Oracle VM Agent Passwords on Oracle VM Servers in the *Oracle VM Manager User's Guide for Release 3.4*.

Running Manual Pre- and Post-Upgrade Checks in Combination with Oracle Private Cloud Appliance Upgrader

Controller software updates must be installed using the Oracle Private Cloud Appliance Upgrader. While the Upgrader tool automates a large number of prerequisite checks, there are still some tasks that must be performed manually before and after the upgrade process. The manual tasks are listed in this section. For more detailed information, refer to one of the following support notes:

- [PCA 2.3.4] Upgrader tool - Usage and Known Issues (Doc ID 2442664.1)
- [PCA 2.4.2] Upgrader Tool - Prechecks and Postchecks (Doc ID 2605884.1)

Start by running the Oracle Private Cloud Appliance Upgrader in verify-only mode. The steps are described in Verifying Upgrade Readiness. Fix any issues reported by the Upgrader, and repeat the verification procedure until all checks complete without errors. Then proceed to the manual pre-upgrade checks.

Performing Manual Pre-Upgrade Checks

1. Verify the WebLogic password.

   On the active Management Node, run the following commands:

   ```
   # cd /u01/app/oracle/ovm-manager-3/bin
   # ./ovm_admin --listusers
   ```

   Enter the WebLogic password when prompted. If the password is incorrect, the `ovm_admin` command fails and exits with return code `1`. If the password is correct, the command lists the users and exits with return code of `0`. In the event of an incorrect password, login to the Private Cloud Appliance web interface and change the `wls-weblogic` password to the expected password.

2. Check that no external storage LUNs are connected to the management nodes.

   Verify that none of your external storage LUNs are visible from either management node. For more details, refer to the support note Management Node(MN) Panic When Sharing External LUNs With Compute Nodes(CN) (Doc ID 2148589.1).

3. Check for customized `inet` settings on the management nodes.

   Depending on the exact upgrade path you are following, `xinetd` may be upgraded. In this case, modified settings are automatically reset to default. Make a note of your custom `inet` settings and verify them after the upgrade process has completed. These setting changes are stored in the file `/etc/postfix/main.cf`.

4. Register the number of objects in the MySQL database.

   As the root user on the active management node, download and run the script `number_of_jobs_and_objects.sh`. To download the script, scroll to the Attachments section at the bottom of support note Doc ID 2442664.1 for Controller Software release 2.3.4, or support note Doc ID 2605884.1 for Controller Software release 2.4.2. The script returns the number of objects and the number of jobs in the database. Make a note of these numbers.

5. Verify management node failover.

   Reboot the active management node to ensure that the standby management node is capable of taking over the active role.

6. Check the NFS protocol used for the internal ZFS Storage Appliance.

   On both management nodes, run the command `nfsstat -m`. Each mounted share should use the NFSv4 protocol.

7. Check the file `/etc/yum.conf` on both management nodes.

   If a proxy is configured for YUM, comment out or remove that line from the file.

When you have submitted your system to all pre-upgrade checks and you have verified that it is ready for upgrade, execute the controller software update. The steps are described in Executing a Controller Software Upgrade. After successfully upgrading the controller software, proceed to the manual post-upgrade checks for management nodes and compute nodes.

Performing Manual Post-Upgrade Checks on the Management Nodes

1. Check the names of the Unmanaged Storage Arrays.

If the names of the Unmanaged Storage Arrays are no longer displayed correctly after the upgrade, follow the workaround documented in the support note After a 2.3.1 Upgrade, the Unmanaged Storage Arrays Lost Name Field in Oracle VM Manager GUI (Doc ID 2244130.1).

2. Check for errors and warnings in Oracle VM.

   In the Oracle VM Manager web UI, verify that none of these occur:

   - Padlock icons against compute nodes or storage servers
   - Red error icons against compute nodes, repositories or storage servers
   - Yellow warning icons against compute nodes, repositories or storage servers

3. Check the status of all components in the Oracle Private Cloud Appliance Dashboard.

   Verify that a green check mark appears to the right of each hardware component in the Hardware View, and that no red error icons are present.

4. Check networks.

   Verify that all networks – factory default and custom – are present and correctly configured.

Performing Manual Post-Upgrade Checks on the Compute Nodes

1. Change the `min_free_kbytes` setting on all compute nodes.

   Refer to the support note Compute Nodes Randomly Reboot after Upgraded to Release 2.3.x (Doc ID 2314504.1). Apply the corresponding steps and reboot the compute node after the change has been made permanent.

2. Check that the `fm` package is installed on all compute nodes.

   Run the command `rpm -q fm`. If the package is not installed, run the following command:

   ```
   # chkconfig ipmi on; service ipmi start; LFMA_UPDATE=1 /usr/bin/yum install fm -q -y -\-nogpgcheck
   ```

3. Perform a virtual machine test.

   Start a test virtual machine and verify that networks are functioning. Migrate the virtual machine to a compatible compute node to make sure that live migration works correctly.

Restoring a Backup After a Password Change

If you have changed the password for Oracle VM Manager or its related components Oracle WebLogic Server and Oracle MySQL database, and you need to restore the Oracle VM Manager from a backup that was made prior to the password change, the passwords will be out of sync. As a result of this password mismatch, Oracle VM Manager cannot connect to its database and cannot be started, so you must first make sure that the passwords are identical.

> **Note:**
>
> The steps below are not specific to the case where a password changed occurred after the backup. They apply to any restore operation.
>
> As of Release 2.3.1, which includes Oracle VM Manager 3.4.2, the database data directory cleanup is built into the restore process, so that step can be skipped.

Resolving Password Mismatches when Restoring Oracle VM Manager from a Backup

1. Create a manual backup of the Oracle VM Manager MySQL database to prevent inadvertent data loss. On the command line of the active management node, run the following command:

   - Release 2.2.x and older:

     ```
     # /u01/app/oracle/ovm-manager-3/bin/createBackup.sh -n ManualBackup1
     ```

   - Release 2.3.1 and newer:

     ```
     # /u01/app/oracle/ovm-manager-3/ovm_tools/bin/BackupDatabase -w
     INFO:  Backup started to:
             /u01/app/oracle/mysql/dbbackup/ManualBackup-20190524_102412
     ```

2. In the Oracle Private Cloud Appliance Dashboard, change the Oracle MySQL database password back to what it was at the time of the backup.

3. On the command line of the active management node, as `root` user, stop the Oracle VM Manager and MySQL services, and then delete the MySQL data.

   ```
   # service ovmm stop
   # service ovmm_mysql stop
   # cd /u01/app/oracle/mysql/data
   # rm -rf appfw ibdata ib_logfile* mysql mysqld.err ovs performance_schema
   ```

4. As `oracle` user, restore the database from the selected backup.

   - Release 2.2.x and older:

     ```
     # su oracle
                  $ bash /u01/app/oracle/ovm-manager-3/ovm_shell/tools/
     RestoreDatabase.sh BackupToBeRestored
     INFO: Expanding the backup image...
     INFO: Applying logs to the backup snapshot...
     INFO: Restoring the backup...
     INFO: Success - Done!
     INFO: Log of operations performed is available at:
                      /u01/app/oracle/mysql/dbbackup/BackupToBeRestored/
     Restore.log
     ```

   - Release 2.3.1 and newer:

     ```
     # su oracle
                  $ bash /u01/app/oracle/ovm-manager-3/ovm_tools/bin/
     RestoreDatabase.sh BackupToBeRestored
     INFO: Expanding the backup image...
     INFO: Applying logs to the backup snapshot...
     INFO: Restoring the backup...
     ```

```
INFO: Success - Done!
INFO: Log of operations performed is available at:
                      /u01/app/oracle/mysql/dbbackup/BackupToBeRestored/
Restore.log
```

5. As `root` user, start the MySQL and Oracle VM Manager services.

```
$ su root
# service ovmm_mysql start
# service ovmm start
```

After both services have restarted successfully, the restore operation is complete.

Enabling SNMP Server Monitoring

For troubleshooting or hardware monitoring, it may be useful to enable SNMP on the servers in your Oracle Private Cloud Appliance. While the tools for SNMP are available, the protocol is not enabled by default. This section explains how to enable SNMP with the standard Oracle Linux and additional Oracle Private Cloud Appliance Management Information Bases (MIBs).

Enabling SNMP on the Management Nodes

1. Using SSH and an account with superuser privileges, log into the management node.

> **Note:**
>
> The data center IP address used in this procedure is an example.

```
# ssh root@10.100.1.101
root@10.100.1.101's password:
[root@ovcamn05r1 ~]#
```

2. Locate the necessary `rpm` packages in the mounted directory `/nfs/shared_storage/mgmt_image/Packages`, which resides in the `MGMT_ROOT` file system on the ZFS storage appliance. The following packages are part of the Oracle Private Cloud Appliance ISO image:
   - net-snmp-5.7.2-49.el7_9.1.x86_64
   - net-snmp-agent-libs-5.7.2-49.el7_9.1.x86_64
   - net-snmp-libs-5.7.2-49.el7_9.1.x86_64
   - net-snmp-utils-5.7.2-49.el7_9.1.x86_64
   - ovca-snmp-0.9-3.el7.x86_64.rpm
   - lm_sensors-libs-3.4.0-8.20160601gitf9185e5.el7.x86_64.rpm
3. Install these packages by running the following command:

```
# rpm -ivh net-snmp-utils-5.7.2-49.el7_9.1.x86_64.rpm net-
snmp-5.7.2-49.el7_9.1.x86_64.rpm /
net-snmp-agent-libs-5.7.2-49.el7_9.1.x86_64.rpm /
net-snmp-libs-5.7.2-49.el7_9.1.x86_64.rpm
lm_sensors-3.4.0-8.20160601gitf9185e5.el7.x86_64.rpm
```

4. Create an SNMP configuration file: `/etc/snmp/snmpd.conf`.

This is a standard sample configuration:

```
rocommunity public
          syslocation MyDataCenter
dlmod ovca /usr/lib64/ovca-snmp/ovca.so
```

5. Enable the `snmpd` service.

```
# systemctl start snmpd
```

6. If desired, enable the `snmpd` service on boot.

```
# systemctl enable snmpd
```

7. Open the SNMP ports on the firewall.

```
# firewall-cmd --permanent --zone=public --add-port=161/udp
# firewall-cmd --permanent --zone=public --add-port=162/udp
# firewall-cmd --reload
```

SNMP is now ready for use on this management node. Besides the standard Oracle Linux MIBs, these are also available:

- ORACLE-OVCA-MIB::ovcaVersion
- ORACLE-OVCA-MIB::ovcaType
- ORACLE-OVCA-MIB::ovcaStatus
- ORACLE-OVCA-MIB::nodeTable

Usage examples:

```
# snmpwalk  -v 1 -c public -O e 130.35.70.186 ORACLE-OVCA-MIB::ovcaVersion
# snmpwalk  -v 1 -c public -O e 130.35.70.111 ORACLE-OVCA-MIB::ovcaStatus
# snmpwalk  -v 1 -c public -O e 130.35.70.111 ORACLE-OVCA-MIB::nodeTable
```

8. Repeat this procedure on the second management node.

Enabling SNMP on the Compute Nodes

> **Note:**
>
> On Oracle Private Cloud Appliance compute nodes, `net-snmp`, `net-snmp-utils` and `net-snmp-libs` are already installed at the factory, but the SNMP service is not enabled or configured.

1. Using SSH and an account with superuser privileges, log into the compute node. It can be accessed through the appliance internal management network.

```
ssh root@192.168.4.5
root@192.168.4.5's password:
[root@ovcacn27r1 ~]#
```

2. Create an SNMP configuration file: `/etc/snmp/snmpd.conf` and make sure this line is included:

```
rocommunity public
```

3. Enable the `snmpd` service.

```
# systemctl start snmpd
```

SNMP is now ready for use on this compute node.

4. If desired, enable the `snmpd` service on boot.

```
# systemctl enable snmpd
```

5. Repeat this procedure on all other compute nodes installed in your Oracle Private Cloud Appliance environment.

Using a Custom CA Certificate for SSL Encryption

By default, Oracle Private Cloud Appliance and Oracle VM Manager use a self-signed SSL certificate for authentication. While it serves to provide SSL encryption for all HTTP traffic, it is recommended that you obtain and install your own custom trusted certificate from a well-known and recognized Certificate Authority (CA).

Both the Oracle Private Cloud Appliance Dashboard and the Oracle VM Manager web interface run on Oracle WebLogic Server. The functionality to update the digital certificate and keystore is provided by the Oracle VM Key Tool in conjunction with the Java Keytool in the JDK. The tools are installed on the Oracle Private Cloud Appliance management nodes.

Creating a Keystore

If you do not already have a third-party CA certificate, you can create a new keystore. The keystore you create contains one entry for a private key. After you create the keystore, you generate a certificate signing request (CSR) for that private key and submit the CSR to a third-party CA. The CA then signs the CSR and returns a signed SSL certificate and a copy of the CA certificate, which you then import into your keystore.

Creating a Keystore with a Custom CA Certificate

1. Using SSH and an account with superuser privileges, log into the management node.

> **Note:**
>
> The data center IP address used in this procedure is an example.

```
# ssh root@10.100.1.101
root@10.100.1.101's password:
[root@ovcamn05r1 ~]#
```

2. Go to the security directory of the Oracle VM Manager WebLogic domain.

```
# cd /u01/app/oracle/ovm-manager-3/domains/ovm_domain/security
```

3. Create a new keystore. Transfer ownership to user *oracle* in the user group *dba*.

```
# /u01/app/oracle/java/bin/keytool -genkeypair -alias ca -keyalg RSA -keysize 2048
\
          -keypass W******1 -storetype jks -keystore mykeystore.jks -storepass
W******1
              # chown oracle.dba mykeystore.jks
```

4. Generate a certificate signing request (CSR). Transfer ownership to user *oracle* in the user group *dba*.

```
# /u01/app/oracle/java/bin/keytool -certreq -alias ca -file pcakey.csr \
        -keypass W******1 -storetype jks -keystore mykeystore.jks -storepass
W******1
            # chown oracle.dba pcakey.csr
```

5. Submit the CSR file to the relevant third-party CA for signing.
6. For the signed files returned by the CA, transfer ownership to user *oracle* in the user group *dba*.

```
# chown oracle.dba ca_cert_file
            # chown oracle.dba ssl_cert_file
```

7. Import the signed CA certificate into the keystore.

```
# /u01/app/oracle/java/bin/keytool -importcert -trustcacerts -noprompt -
alias ca \
          -file ca_cert_file -storetype jks -keystore mykeystore.jks -
storepass W******1
```

8. Import the signed SSL certificate into the keystore.

```
# /u01/app/oracle/java/bin/keytool -importcert -trustcacerts -noprompt -
alias ca \
          -file ssl_cert_file -keypass W******1 -storetype jks -keystore
mykeystore.jks \
              -storepass W******1
```

9. Use the **setsslkey** command to configure the system to use the new keystore.

```
# /u01/app/oracle/ovm-manager-3/ovm_upgrade/bin/ovmkeytool.sh setsslkey
          Path for SSL keystore: /u01/app/oracle/ovm-manager-3/domains/
ovm_domain/security/mykeystore.jks
Keystore password:
              Alias of key to use as SSL key: ca
Key password:
Updating keystore information in WebLogic
Oracle MiddleWare Home (MW_HOME): [/u01/app/oracle/Middleware]
WebLogic domain directory: [/u01/app/oracle/ovm-manager-3/domains/
ovm_domain]
Oracle WebLogic Server name: [AdminServer]
WebLogic username: [weblogic]
WebLogic password: [********]
WLST session logged at:
                              /tmp/wlst-session5820685079094897641.log
```

10. Configure the client certificate login.

```
# /u01/app/oracle/ovm-manager-3/bin/configure_client_cert_login.sh \
          /u01/app/oracle/ovm-manager-3/domains/ovm_domain/security/
pcakey.crt
```

11. Test the new SSL configuration by logging into the Oracle Private Cloud Appliance Dashboard. From there, proceed to Oracle VM Manager with the button "Login to OVM Manager". The browser now indicates that your connection is secure.

Importing a Keystore

If you already have a CA certificate and SSL certificate, use the SSL certificate to create a keystore. You can then import that keystore into Private Cloud Appliance and configure it as the SSL keystore.

> **Caution:**
>
> If you have generated custom keys using `ovmkeytool.sh` in a previous version of the Private Cloud Appliance software, you must regenerate the keys prior to updating the Controller Software. For instructions, refer to the support note PCA 2.3.x/2.4.x Upgrade not allowed if Certificates have been regenerated using ovmkeytool.sh. (Doc ID 2597439.1).

Importing a Keystore with an Existing CA and SSL Certificate

1. Using SSH and an account with superuser privileges, log into the management node.

   > **Note:**
   >
   > The data center IP address used in this procedure is an example.

   ```
   # ssh root@10.100.1.101
   root@10.100.1.101's password:
   [root@ovcamn05r1 ~]#
   ```

2. Import the keystore.

   ```
   # /u01/app/oracle/java/bin/keytool -importkeystore -noprompt \
   -srckeystore existing_keystore.jks -srcstoretype source_format -srcstorepass
   W******1
   -destkeystore mykeystore.jks -deststoretype jks -deststorepass W******1
   ```

3. Use the `setsslkey` command to configure the system to use the new keystore.

   ```
   # /u01/app/oracle/ovm-manager-3/ovm_upgrade/bin/ovmkeytool.sh setsslkey
   Path for SSL keystore: /u01/app/oracle/ovm-manager-3/domains/ovm_domain/security/
   mykeystore.jks
   Keystore password:
   Alias of key to use as SSL key: ca
   Key password:
   Updating keystore information in WebLogic
   Oracle MiddleWare Home (MW_HOME): [/u01/app/oracle/Middleware]
   WebLogic domain directory: [/u01/app/oracle/ovm-manager-3/domains/ovm_domain]
   Oracle WebLogic Server name: [AdminServer]
   WebLogic username: [weblogic]
   WebLogic password: [********]
   WLST session logged at: /tmp/wlst-session5820685079094897641.log
   ```

4. Configure the client certificate login.

   ```
   # /u01/app/oracle/ovm-manager-3/bin/configure_client_cert_login.sh /path/to/cacert
   ```

The value of */path/to/cacert* is the absolute path to the CA certificate.

5. Test the new SSL configuration by logging into the Oracle Private Cloud Appliance Dashboard. From there, proceed to Oracle VM Manager with the button "Login to OVM Manager". The browser now indicates that your connection is secure.

Reprovisioning a Compute Node when Provisioning Fails

Compute node provisioning is a complex orchestrated process involving various configuration and installation steps and several reboots. Due to connectivity fluctuations, timing issues or other unexpected events, a compute node may become stuck in an intermittent state or go into error status. The solution is to reprovision the compute node.

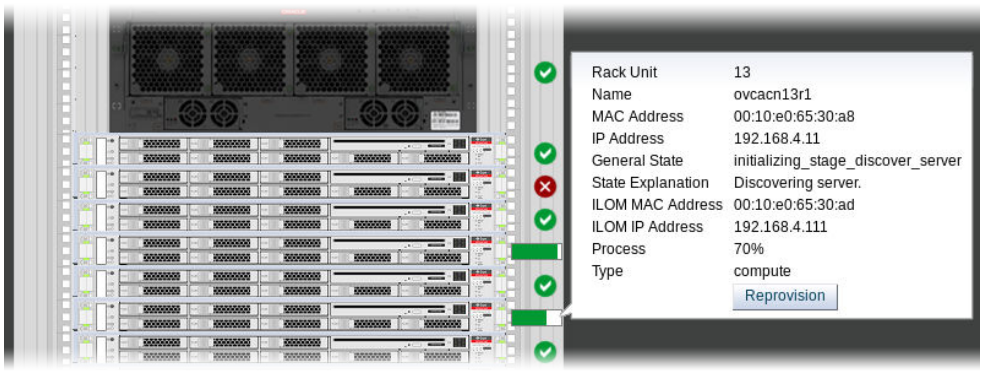
> **NOT_SUPPORTED:**
>
> Reprovisioning is to be applied *only* to compute nodes that fail to complete provisioning.
>
> For correctly provisioned and running compute nodes, reprovisioning functionality is blocked in order to prevent incorrect use that could lock compute nodes out of the environment permanently or otherwise cause loss of functionality or data corruption.

Reprovisioning a Compute Node when Provisioning Fails

1. Log in to the Oracle Private Cloud Appliance Dashboard.
2. Go to the **Hardware View** tab.
3. Roll over the compute nodes that are in Error status or have become stuck in the provisioning process.

   A pop-up window displays a summary of configuration and status information.

Figure 7-1 Compute Node Information and Reprovision Button in Hardware View



4. If the compute node provisioning is incomplete and the server is in error status or stuck in an intermittent state for several hours, click the **Reprovision** button in the pop-up window.

5. When the confirmation dialog box appears, click OK to start reprovisioning the compute node.

If compute node provisioning should fail after the server was added to the Oracle VM server pool, additional recovery steps could be required. The cleanup mechanism associated with reprovisioning may be unable to remove the compute node from the Oracle VM configuration. For example, when a server is in locked state or owns the server pool active role, it must be unconfigured manually. In this case you need to perform operations in Oracle VM Manager that are otherwise not permitted. You may also need to power on the compute node manually.

Removing a Compute Node from the Oracle VM Configuration

1. Log into the Oracle VM Manager user interface.

   For detailed instructions, see Logging in to the Oracle VM Manager Web UI.

2. Go to the **Servers and VMs** tab and verify that the server pool named `Rack1_ServerPool` does indeed contain the compute node that fails to provision correctly.

3. If the compute node is locked due to a running job, abort it in the **Jobs** tab of Oracle VM Manager.

   Detailed information about the use of jobs in Oracle VM can be found in the Oracle VM Manager User's Guide. Refer to the section entitled Jobs Tab.

4. Remove the compute node from the Oracle VM server pool.

   Refer to the section entitled Edit Server Pool in the Oracle VM Manager User's Guide. When editing the server pool, move the compute node out of the list of selected servers. The compute node is moved to the Unassigned Servers folder.

5. Delete the compute node from Oracle VM Manager.

   Refer to the Oracle VM Manager User's Guide and follow the instructions in the section entitled Delete Server.

When the failing compute node has been removed from the Oracle VM configuration, return to the Oracle Private Cloud Appliance Dashboard, to reprovision it. If the compute node is powered off and reprovisioning cannot be started, power on the server manually.

Deprovisioning and Replacing a Compute Node

When a defective compute node needs to be replaced or repaired, or when a compute node is retired in favor of a newer model with higher capacity and better performance, it is highly recommended that you deprovision the compute node before removing it from the appliance rack. Deprovisioning ensures that all configuration entries for a compute node are removed cleanly, so that no conflicts are introduced when a replacement compute node is installed.

Deprovisioning a Compute Node for Repair or Replacement

1. Log into the Oracle VM Manager user interface.

   For detailed instructions, see Logging in to the Oracle VM Manager Web UI.

2. Migrate all virtual machines away from the compute node you wish to deprovision. If any VMs are running on the compute node, the deprovision command fails.

3. Using SSH and an account with superuser privileges, log into the active management node, then launch the Oracle Private Cloud Appliance command line interface.

```
# ssh root@10.100.1.101
root@10.100.1.101's password:
root@ovcamn05r1 ~]# pca-admin
Welcome to PCA! Release: 2.4.2
PCA>
```

4. Lock provisioning to make sure that the compute node cannot be reprovisioned immediately after deprovisioning.

```
PCA> create lock provisioning
Status: Success
```

5. Deprovision the compute node you wish to remove. Repeat for additional compute nodes, if necessary.

```
PCA> deprovision compute-node ovcacn29r1
************************************************************
 WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
************************************************************
Are you sure [y/N]:y
Shutting down dhcpd:                                  [ OK ]
Starting dhcpd:                                       [ OK ]
Shutting down dnsmasq:                                [ OK ]
Starting dnsmasq:                                     [ OK ]

Status: Success
```

6. When the necessary compute nodes have been deprovisioned successfully, release the provisioning lock. The appliance resumes its normal operation.

```
PCA> delete lock provisioning
************************************************************
 WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
************************************************************
Are you sure [y/N]:y
Status: Success
```

When the necessary repairs have been completed, or when the replacement compute nodes are ready, install the compute nodes into the rack and connect the necessary cables. The controller software detects the new compute nodes and automatically launches the provisioning process.

Eliminating Time-Out Issues when Provisioning Compute Nodes

The provisioning process is an appliance level orchestration of many configuration operations that run at the level of Oracle VM Manager and the individual Oracle VM Servers or compute nodes. As the virtualized environment grows – meaning there are more virtual machines, storage paths and networks –, the time required to complete various discovery tasks increases exponentially.

The maximum task durations have been configured to reliably accommodate a standard base rack setup. At a given point, however, the complexity of the existing configuration, when replicated to a large number of compute nodes, increases the duration of tasks beyond their standard time-out. As a result, provisioning failures occur.

Because many provisioning tasks have been designed to use a common time-out mechanism, this problem cannot be resolved by simply increasing the global time-out.

Doing so would decrease the overall performance of the system. To overcome this issue, additional code has been implemented to allow a finer-grained definition of time-outs through a number of settings in a system configuration file: `/var/lib/ovca/ovca-system.conf`.

If you run into time-out issues when provisioning additional compute nodes, it may be possible to resolve them by tweaking specific time-out settings in the configuration. Depending on which job failures occur, changing the `storage_refresh_timeout`, `discover_server_timeout` or other parameters could allow the provisioning operations to complete successfully. These changes would need to be applied on both management nodes.

Please contact your Oracle representative if your compute nodes fail to provision due to time-out issues. Oracle product specialists can analyse these failures for you and recommend new time-out parameters accordingly.

Recovering from Tenant Group Configuration Mismatches

Tenant groups are essentially Oracle VM server pools, created and managed at the appliance level, with support for automatic custom network configuration across all pool members. The tenant groups appear in Oracle VM Manager, where the administrator could modify the server pool, but such operations are not supported in Oracle Private Cloud Appliance and cause configuration mismatches.

If you have inadvertently modified the configuration of a tenant group in Oracle VM Manager, follow the instructions in this section to correct the inconsistent state of your environment.

> **Caution:**
>
> If the operations described below do not resolve the issue, it could be necessary to reprovision the affected compute nodes. This can result in downtime and data loss.

Adding a Server to a Tenant Group

If you try to add a server to a pool or tenant group using Oracle VM Manager, the operation succeeds. However, the newly added server is not connected to the custom networks associated with the tenant group because the Oracle Private Cloud Appliance controller software is not aware that a server has been added.

To correct this situation, first remove the server from the tenant group again in Oracle VM Manager. Then add the server to the tenant group again using the correct method, which is through the Oracle Private Cloud Appliance CLI. See Configuring Tenant Groups.

As a result, Oracle VM Manager and Oracle Private Cloud Appliance are in sync again.

Removing a Server from a Tenant Group

If you try to remove a server from a pool or tenant group using Oracle VM Manager, the operation succeeds. However, the Oracle Private Cloud Appliance controller software is not aware that a server has been removed, and the custom network configuration associated with the tenant group is not removed from the server.

At this point, Oracle Private Cloud Appliance assumes that the server is still a member of the tenant group, and any attempt to remove the server from the tenant group through the Oracle Private Cloud Appliance CLI results in an error:

```
PCA> remove compute-node ovcacn09r1 myTenantGroup
************************************************************
 WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
************************************************************
Are you sure [y/N]:y

Status: Failure
Error Message: Error (SERVER_001): Exception while trying to
            remove the server ovcacn09r1 from tenant group myTenantGroup.
                    ovcacn09r1 is not a member of the Tenant Group myTenantGroup.
```

To correct this situation, use Oracle VM Manager to add the previously removed server to the tenant group again. Then use the Oracle Private Cloud Appliance CLI to remove the server from the tenant group. See Configuring Tenant Groups. After the `remove server` command is applied successfully, the server is taken out of the tenant group, custom network configurations are removed, and the server is placed in the Unassigned Servers group in Oracle VM Manager. As a result, Oracle VM Manager and Oracle Private Cloud Appliance are in sync again.

Configure Xen CPU Frequency Scaling for Best Performance

The Xen hypervisor offers a mechanism to balance performance and power consumption through CPU frequency scaling. Known as the Current Governor, this mechanism can lower power consumption by throttling the clock speed when a CPU is idle.

Certain versions of Oracle VM Server have the Current Governor set to `ondemand` by default, which dynamically scales the CPU clock based on the load. Oracle recommends that on Oracle Private Cloud Appliance compute nodes you run the Current Governor with the `performance` setting. Particularly if you find that systems are not performing as expected after an upgrade of Oracle VM Server, make sure that the Current Governor is configured correctly.

To verify the Current Governor setting of a compute node, log in using SSH and enter the following command at the Oracle Linux prompt:

```
]# xenpm get-cpufreq-para
cpu id               : 0
affected_cpus        : 0
cpuinfo frequency    : max [2301000] min [1200000] cur [2301000]
scaling_driver       : acpi-cpufreq
scaling_avail_gov    : userspace performance powersave ondemand
current_governor      : performance
scaling_avail_freq   : *2301000 2300000 2200000 2100000 2000000 1900000 1800000
1700000 1600000 1500000 1400000 1300000 1200000
scaling frequency    : max [2301000] min [1200000] cur [2301000]
turbo mode           : enabled
[...]
```

The command lists all CPUs in the compute node. If the `current_governor` parameter is set to anything other than `performance`, you should change the Current Governor configuration.

To set performance mode manually, enter this command: `xenpm set-scaling-governor performance`.

To make this setting persistent, add it to the `grub.cfg` file.

1. Add the xen cpu frequency setting to the `/etc/default/grub` template file, as shown in this example:

   ```
   GRUB_CMDLINE_XEN="dom0_mem=max:6144M allowsuperpage dom0_vcpus_pin
   dom0_max_vcpus=20 cpufreq=xen:performance max_cstate=1"
   ```

2. Rebuild `grub.cfg` by means of the following command:

   ```
   # grub2-mkconfig -o /boot/grub2/grub.cfg
   ```