

# **Oracle® Private Cloud Appliance**

## **Administrator's Guide for Release 2.4.3**

**ORACLE®**

F23081-02  
August 2020

---

## Oracle Legal Notices

Copyright © 2013, 2020, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

**U.S. GOVERNMENT END USERS:** Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

---

---

# Table of Contents

Preface .....	ix
1 Concept, Architecture and Life Cycle of Oracle Private Cloud Appliance .....	1
1.1 What is Oracle Private Cloud Appliance .....	1
1.2 Hardware Components .....	2
1.2.1 Management Nodes .....	4
1.2.2 Compute Nodes .....	5
1.2.3 Storage Appliance .....	5
1.2.4 Network Infrastructure .....	8
1.3 Software Components .....	12
1.3.1 Oracle Private Cloud Appliance Dashboard .....	12
1.3.2 Password Manager (Wallet) .....	13
1.3.3 Oracle VM Manager .....	13
1.3.4 Operating Systems .....	13
1.3.5 Databases .....	13
1.3.6 Oracle Private Cloud Appliance Management Software .....	17
1.3.7 Oracle Private Cloud Appliance Diagnostics Tool .....	18
1.4 Provisioning and Orchestration .....	19
1.4.1 Appliance Management Initialization .....	19
1.4.2 Compute Node Discovery and Provisioning .....	19
1.4.3 Server Pool Readiness .....	20
1.5 High Availability .....	21
1.6 Oracle Private Cloud Appliance Backup .....	22
1.7 Oracle Private Cloud Appliance Upgrader .....	23
2 Monitoring and Managing Oracle Private Cloud Appliance .....	25
2.1 Connecting and Logging in to the Oracle Private Cloud Appliance Dashboard .....	26
2.2 Oracle Private Cloud Appliance Accessibility Features .....	28
2.3 Hardware View .....	28
2.4 Network Settings .....	32
2.5 Functional Networking Limitations .....	35
2.5.1 Network Configuration of Ethernet-based Systems .....	36
2.5.2 Network Configuration of InfiniBand-based Systems .....	38
2.6 Network Customization .....	39
2.6.1 Configuring Custom Networks on Ethernet-based Systems .....	40
2.6.2 Configuring Custom Networks on InfiniBand-based Systems .....	44
2.6.3 Deleting Custom Networks .....	49
2.7 VM Storage Networks .....	50
2.7.1 Creating VM Storage Networks .....	50
2.7.2 Creating Storage Shares .....	51
2.7.3 Storage Profiles .....	53
2.8 Tenant Groups .....	54
2.8.1 Design Assumptions and Restrictions .....	54
2.8.2 Configuring Tenant Groups .....	54
2.9 Authentication .....	58
2.10 Health Monitoring .....	61
2.11 Fault Monitoring .....	63
2.11.1 Using Fault Monitoring Checks .....	64
2.11.2 Phone Home Service .....	67
2.12 Cloud Backup .....	68
2.12.1 Configuring the Cloud Backup Service .....	68
2.12.2 Configuring a Manual Cloud Backup .....	69
2.12.3 Deleting Cloud Backups .....	70

2.12.4 Deleting Oracle Cloud InfrastructureTargets .....	71
2.13 Kubernetes Engine .....	71
2.13.1 Kubernetes Guidelines and Limitations .....	71
2.13.2 Prepare the Cluster Environment .....	72
2.13.3 Create a Kubernetes Cluster on a DHCP Network .....	74
2.13.4 Create a Kubernetes Cluster on a Static Network .....	75
2.13.5 Use the Kubernetes Dashboard .....	77
2.13.6 Managing a Cluster .....	78
2.13.7 Stop a Cluster .....	79
2.13.8 Monitor Cluster Status .....	79
2.13.9 Resize Kubernetes Virtual Machine Disk Space .....	80
2.13.10 Maintain the Operating Systems on the Kubernetes Virtual Machines .....	81
3 Updating Oracle Private Cloud Appliance .....	83
3.1 Before You Start Updating .....	83
3.1.1 Warnings and Cautions .....	84
3.1.2 Backup Prevents Data Loss .....	86
3.1.3 Determine Firmware Versions .....	86
3.2 Using the Oracle Private Cloud Appliance Upgrader .....	86
3.2.1 Rebooting the Management Node Cluster .....	87
3.2.2 Installing the Oracle Private Cloud Appliance Upgrader .....	88
3.2.3 Verifying Upgrade Readiness .....	89
3.2.4 Executing a Controller Software Update .....	91
3.2.5 Upgrading the Storage Network .....	97
3.3 Upgrading the Virtualization Platform .....	99
3.4 Upgrading Component Firmware .....	102
3.4.1 Firmware Policy .....	102
3.4.2 Install the Current Firmware on All Compute Nodes .....	103
3.4.3 Upgrading the Operating Software on the Oracle ZFS Storage Appliance .....	103
3.4.4 Upgrading the Cisco Switch Firmware .....	108
3.4.5 Upgrading the NM2-36P Sun Datacenter InfiniBand Expansion Switch Firmware .....	116
3.4.6 Upgrading the Oracle Fabric Interconnect F1-15 Firmware .....	119
4 The Oracle Private Cloud Appliance Command Line Interface (CLI) .....	123
4.1 CLI Usage .....	124
4.1.1 Interactive Mode .....	125
4.1.2 Single-command Mode .....	126
4.1.3 Controlling CLI Output .....	127
4.1.4 Internal CLI Help .....	129
4.2 CLI Commands .....	130
4.2.1 add compute-node .....	130
4.2.2 add initiator .....	131
4.2.3 add network .....	132
4.2.4 add network-to-tenant-group .....	133
4.2.5 add nfs-exception .....	134
4.2.6 add node-pool .....	134
4.2.7 add node-pool-node .....	135
4.2.8 backup .....	137
4.2.9 configure vhbases .....	138
4.2.10 create iscsi-storage .....	139
4.2.11 create lock .....	140
4.2.12 create network .....	141
4.2.13 create nfs-storage .....	143
4.2.14 create kube-cluster .....	144
4.2.15 create oci-backup .....	145
4.2.16 create oci-target .....	145

4.2.17 create tenant-group .....	146
4.2.18 create uplink-port-group .....	147
4.2.19 delete config-error .....	148
4.2.20 delete iscsi-storage .....	149
4.2.21 delete kube-cluster .....	150
4.2.22 delete lock .....	151
4.2.23 delete network .....	152
4.2.24 delete nfs-storage .....	153
4.2.25 delete oci-backup .....	154
4.2.26 delete oci-target .....	155
4.2.27 delete task .....	156
4.2.28 delete tenant-group .....	157
4.2.29 delete uplink-port-group .....	158
4.2.30 deprovision compute-node .....	159
4.2.31 diagnose .....	160
4.2.32 get log .....	164
4.2.33 list .....	164
4.2.34 remove compute-node .....	171
4.2.35 remove initiator .....	172
4.2.36 remove network .....	173
4.2.37 remove network-from-tenant-group .....	174
4.2.38 remove nfs exceptions .....	175
4.2.39 remove node-pool .....	175
4.2.40 remove node-pool-node .....	176
4.2.41 reprovision .....	177
4.2.42 rerun .....	178
4.2.43 set system-property .....	179
4.2.44 set kube-dns .....	182
4.2.45 set kube-load-balancer .....	182
4.2.46 set kube-master-pool .....	183
4.2.47 set kube-network .....	183
4.2.48 set kube-vm-shape .....	184
4.2.49 set kube-worker-pool .....	185
4.2.50 show .....	186
4.2.51 start .....	191
4.2.52 start kube-cluster .....	192
4.2.53 stop .....	193
4.2.54 stop kube-cluster .....	195
4.2.55 update appliance .....	195
4.2.56 update password .....	196
4.2.57 update compute-node .....	198
5 Managing the Oracle VM Virtual Infrastructure .....	201
5.1 Guidelines and Limitations .....	202
5.2 Logging in to the Oracle VM Manager Web UI .....	205
5.3 Monitoring Health and Performance in Oracle VM .....	205
5.4 Creating and Managing Virtual Machines .....	206
5.5 Managing Virtual Machine Resources .....	209
5.6 Configuring Network Resources for Virtual Machines .....	211
5.6.1 Configuring VM Network Resources on Ethernet-based Systems .....	211
5.6.2 Configuring VM Network Resources on InfiniBand-based Systems .....	214
5.7 Viewing and Managing Storage Resources .....	217
5.7.1 Oracle ZFS Storage Appliance ZS7-2 .....	218
5.7.2 Oracle ZFS Storage Appliance ZS5-ES and Earlier Models .....	218
5.8 Tagging Resources in Oracle VM Manager .....	219

5.9	Managing Jobs and Events .....	219
5.10	Exporting VMs to Oracle Cloud Infrastructure .....	219
5.10.1	Prepare Your Oracle Cloud Infrastructure .....	220
5.10.2	Create the Oracle VM Exporter Appliance Virtual Machine .....	220
5.10.3	Configure the Oracle VM Exporter Appliance Virtual Machine .....	221
5.10.4	Create a Network for the Oracle VM Exporter Appliance VM .....	222
5.10.5	Attach the New Network to the Oracle VM Exporter Appliance VM .....	225
5.10.6	Prepare a Storage Repository .....	226
6	Servicing Oracle Private Cloud Appliance Components .....	229
6.1	Oracle Auto Service Request (ASR) .....	230
6.1.1	Understanding Oracle Auto Service Request (ASR) .....	230
6.1.2	ASR Prerequisites .....	231
6.1.3	Setting Up ASR and Activating ASR Assets .....	232
6.2	Replaceable Components .....	232
6.2.1	Rack Components .....	232
6.2.2	Oracle Server X8-2 Components .....	233
6.2.3	Oracle Server X7-2 Components .....	234
6.2.4	Oracle Server X6-2 Components .....	235
6.2.5	Oracle Server X5-2 Components .....	236
6.2.6	Sun Server X4-2 Components .....	237
6.2.7	Sun Server X3-2 Components .....	238
6.2.8	Oracle ZFS Storage Appliance ZS7-2 Components .....	238
6.2.9	Oracle ZFS Storage Appliance ZS5-ES Components .....	240
6.2.10	Oracle ZFS Storage Appliance ZS3-ES Components .....	241
6.2.11	Sun ZFS Storage Appliance 7320 Components .....	242
6.2.12	Oracle Switch ES1-24 Components .....	243
6.2.13	NM2-36P Sun Datacenter InfiniBand Expansion Switch Components .....	244
6.2.14	Oracle Fabric Interconnect F1-15 Components .....	244
6.3	Preparing Oracle Private Cloud Appliance for Service .....	245
6.4	Servicing the Oracle Private Cloud Appliance Rack System .....	246
6.4.1	Powering Down Oracle Private Cloud Appliance (When Required) .....	246
6.4.2	Service Procedures for Rack System Components .....	247
6.5	Servicing an Oracle Server X8-2 .....	248
6.5.1	Powering Down Oracle Server X8-2 for Service (When Required) .....	248
6.5.2	Service Procedures for Oracle Server X8-2 Components .....	250
6.6	Servicing an Oracle Server X7-2 .....	250
6.6.1	Powering Down Oracle Server X7-2 for Service (When Required) .....	250
6.6.2	Service Procedures for Oracle Server X7-2 Components .....	252
6.7	Servicing an Oracle Server X6-2 .....	252
6.7.1	Powering Down Oracle Server X6-2 for Service (When Required) .....	253
6.7.2	Service Procedures for Oracle Server X6-2 Components .....	254
6.8	Servicing an Oracle Server X5-2 .....	255
6.8.1	Powering Down Oracle Server X5-2 for Service (When Required) .....	255
6.8.2	Service Procedures for Oracle Server X5-2 Components .....	256
6.9	Servicing a Sun Server X4-2 .....	257
6.9.1	Powering Down Sun Server X4-2 for Service (When Required) .....	257
6.9.2	Service Procedures for Sun Server X4-2 Components .....	259
6.10	Servicing a Sun Server X3-2 .....	260
6.10.1	Powering Down Sun Server X3-2 for Service (When Required) .....	260
6.10.2	Service Procedures for Sun Server X3-2 Components .....	261
6.11	Servicing the Oracle ZFS Storage Appliance ZS7-2 .....	262
6.11.1	Powering Down the Oracle ZFS Storage Appliance ZS7-2 for Service (When Required) .....	262
6.11.2	Service Procedures for Oracle ZFS Storage Appliance ZS7-2 Components .....	264

6.12	Servicing the Oracle ZFS Storage Appliance ZS5-ES .....	265
6.12.1	Powering Down the Oracle ZFS Storage Appliance ZS5-ES for Service (When Required) .....	265
6.12.2	Service Procedures for Oracle ZFS Storage Appliance ZS5-ES Components .....	266
6.13	Servicing the Oracle ZFS Storage Appliance ZS3-ES .....	267
6.13.1	Powering Down the Oracle ZFS Storage Appliance ZS3-ES for Service (When Required) .....	268
6.13.2	Service Procedures for Oracle ZFS Storage Appliance ZS3-ES Components .....	270
6.14	Servicing the Sun ZFS Storage Appliance 7320 .....	271
6.14.1	Powering Down the Sun ZFS Storage Appliance 7320 for Service (When Required) ..	271
6.14.2	Service Procedures for Sun ZFS Storage Appliance 7320 Components .....	272
6.15	Servicing an Oracle Switch ES1-24 .....	273
6.15.1	Powering Down the Oracle Switch ES1-24 for Service (When Required) .....	273
6.15.2	Service Procedures for Oracle Switch ES1-24 Components .....	274
6.16	Servicing an NM2-36P Sun Datacenter InfiniBand Expansion Switch .....	274
6.16.1	Powering Down the NM2-36P Sun Datacenter InfiniBand Expansion Switch for Service (When Required) .....	274
6.16.2	Service Procedures for NM2-36P Sun Datacenter InfiniBand Expansion Switch Components .....	275
6.17	Servicing an Oracle Fabric Interconnect F1-15 .....	275
6.17.1	Powering Down the Oracle Fabric Interconnect F1-15 for Service (When Required) ..	275
6.17.2	Service Procedures for Oracle Fabric Interconnect F1-15 Components .....	276
6.18	Servicing a Cisco Nexus 9336C-FX2 Switch .....	277
6.18.1	Powering Down the Cisco Nexus 9336C-FX2 Switch for Service (When Required) ...	277
6.18.2	Service Procedures for Cisco Nexus 9336C-FX2 Switch Components .....	277
6.19	Servicing a Cisco Nexus 9348GC-FXP Switch .....	278
6.19.1	Powering Down the Cisco Nexus 9348GC-FXP Switch for Service (When Required) ..	278
6.19.2	Service Procedures for Cisco Nexus 9348GC-FXP Switch Components .....	278
7	Troubleshooting .....	281
7.1	Setting the Oracle Private Cloud Appliance Logging Parameters .....	281
7.2	Adding Proxy Settings for Oracle Private Cloud Appliance Updates .....	282
7.3	Configuring Data Center Switches for VLAN Traffic .....	283
7.4	Changing the Oracle VM Agent Password .....	284
7.5	Running Manual Pre- and Post-Upgrade Checks in Combination with Oracle Private Cloud Appliance Upgrader .....	284
7.6	Enabling Fibre Channel Connectivity on a Provisioned Appliance .....	286
7.7	Restoring a Backup After a Password Change .....	288
7.8	Enabling SNMP Server Monitoring .....	290
7.9	Using a Custom CA Certificate for SSL Encryption .....	291
7.9.1	Creating a Keystore .....	292
7.9.2	Importing a Keystore .....	293
7.10	Reprovisioning a Compute Node when Provisioning Fails .....	294
7.11	Deprovisioning and Replacing a Compute Node .....	295
7.12	Eliminating Time-Out Issues when Provisioning Compute Nodes .....	296
7.13	Returning Oracle VM Server Pool to Operation After Network Services Restart .....	297
7.14	Recovering from Tenant Group Configuration Mismatches .....	298
7.15	Configure Xen CPU Frequency Scaling for Best Performance .....	299
	Index .....	301





---

# 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. It conforms to Compliance Model No. ESY27.

## **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 UNIXes, 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/cd/E85660\\_01/index.html](https://docs.oracle.com/cd/E85660_01/index.html)
- Oracle Server X8-2  
[https://docs.oracle.com/cd/E93359\\_01/index.html](https://docs.oracle.com/cd/E93359_01/index.html)
- Oracle Server X7-2  
[https://docs.oracle.com/cd/E72435\\_01/index.html](https://docs.oracle.com/cd/E72435_01/index.html)
- Oracle Server X6-2  
[https://docs.oracle.com/cd/E62159\\_01/index.html](https://docs.oracle.com/cd/E62159_01/index.html)
- Oracle Server X5-2  
[https://docs.oracle.com/cd/E41059\\_01/index.html](https://docs.oracle.com/cd/E41059_01/index.html)
- Oracle ZFS Storage Appliance ZS7-2  
[https://docs.oracle.com/cd/F13758\\_01/index.html](https://docs.oracle.com/cd/F13758_01/index.html)
- Oracle ZFS Storage Appliance ZS5-ES  
[https://docs.oracle.com/cd/E59597\\_01/index.html](https://docs.oracle.com/cd/E59597_01/index.html)
- Oracle Integrated Lights Out Manager (ILOM)  
[https://docs.oracle.com/cd/E81115\\_01/index.html](https://docs.oracle.com/cd/E81115_01/index.html)
- Oracle Switch ES1-24  
[https://docs.oracle.com/cd/E39109\\_01/index.html](https://docs.oracle.com/cd/E39109_01/index.html)

- NM2-36P Sun Datacenter InfiniBand Expansion Switch  
[https://docs.oracle.com/cd/E76424\\_01/index.html](https://docs.oracle.com/cd/E76424_01/index.html)
- Oracle Fabric Interconnect F1-15  
[https://docs.oracle.com/cd/E38500\\_01/index.html](https://docs.oracle.com/cd/E38500_01/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/13.3.1/empca/index.html>

## Feedback

Provide feedback about this documentation at:

<http://www.oracle.com/goto/docfeedback>

## Conventions

The following text conventions are used in this document:

Convention	Meaning
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

## Document Revision

Document generated on: 2020-08-27 (revision: 2266)

## 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

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>.



---

# Chapter 1 Concept, Architecture and Life Cycle of Oracle Private Cloud Appliance

## Table of Contents

- 1.1 What is Oracle Private Cloud Appliance ..... 1
- 1.2 Hardware Components ..... 2
  - 1.2.1 Management Nodes ..... 4
  - 1.2.2 Compute Nodes ..... 5
  - 1.2.3 Storage Appliance ..... 5
  - 1.2.4 Network Infrastructure ..... 8
- 1.3 Software Components ..... 12
  - 1.3.1 Oracle Private Cloud Appliance Dashboard ..... 12
  - 1.3.2 Password Manager (Wallet) ..... 13
  - 1.3.3 Oracle VM Manager ..... 13
  - 1.3.4 Operating Systems ..... 13
  - 1.3.5 Databases ..... 13
  - 1.3.6 Oracle Private Cloud Appliance Management Software ..... 17
  - 1.3.7 Oracle Private Cloud Appliance Diagnostics Tool ..... 18
- 1.4 Provisioning and Orchestration ..... 19
  - 1.4.1 Appliance Management Initialization ..... 19
  - 1.4.2 Compute Node Discovery and Provisioning ..... 19
  - 1.4.3 Server Pool Readiness ..... 20
- 1.5 High Availability ..... 21
- 1.6 Oracle Private Cloud Appliance Backup ..... 22
- 1.7 Oracle Private Cloud Appliance Upgrader ..... 23

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.

## 1.1 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 master 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

Oracle 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

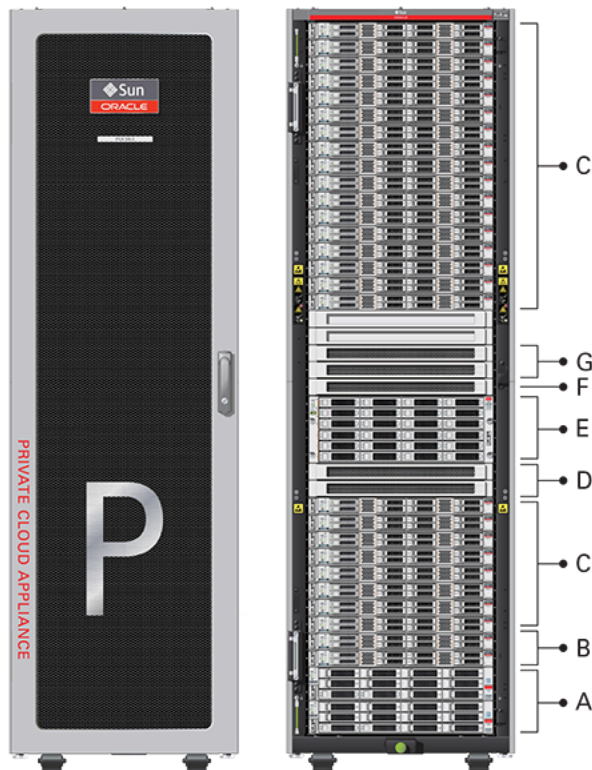
With Oracle Private Cloud Appliance, Oracle offers a unique full stack of hardware, software, virtualization technology and rapid application deployment through virtual appliances. All this is packaged in a single modular and extensible product. The minimum configuration consists of a base rack with 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 Oracle 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.

## 1.2 Hardware Components

The current Oracle 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 [Figure 1.1](#). Previous generations of hardware components continue to be supported by the latest Controller Software, as described below.

**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	2-25	Oracle Server X8-2, used as virtualization compute nodes  (Due to the power requirements of the Oracle Server X8-2, 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 continues to support all earlier configurations of the hardware platform. These may include the following components:

**Table 1.2 Supported Hardware**

Component Type	Component Name and Minimum Software Version
Management Nodes	<ul style="list-style-type: none"> <li>Oracle Server X5-2 (release 2.0.3 or newer)</li> </ul>

Component Type	Component Name and Minimum Software Version
Compute Nodes	<ul style="list-style-type: none"> <li>• Sun Server X4-2 (release 1.1.3 or newer)</li> <li>• Sun Server X3-2 (since initial release)</li> </ul>
	<ul style="list-style-type: none"> <li>• Oracle Server X7-2 (release 2.3.2 or newer)</li> <li>• Oracle Server X6-2 (release 2.2.1 or newer)</li> <li>• Oracle Server X5-2 (release 2.0.3 or newer)</li> <li>• Sun Server X4-2 (release 1.1.3 or newer)</li> <li>• Sun Server X3-2 (since initial release)</li> </ul>
Storage Appliance	<ul style="list-style-type: none"> <li>• Oracle ZFS Storage Appliance ZS5-ES (release 2.3.3 or newer)</li> <li>• Oracle ZFS Storage Appliance ZS3-ES (release 1.1.3 or newer)</li> <li>• Sun ZFS Storage Appliance 7320 (since initial release)</li> </ul>
InfiniBand Network Hardware	<ul style="list-style-type: none"> <li>• Oracle Fabric Interconnect F1-15 (since initial release)</li> <li>• NM2-36P Sun Datacenter InfiniBand Expansion Switch (since initial release)</li> </ul>
Internal Management Switch	<ul style="list-style-type: none"> <li>• Oracle Switch ES1-24 (since initial release)</li> </ul>

## 1.2.1 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 master while the other is ready to take over the master functions in case a failure occurs. The master 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 master role. The master 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 master 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 Oracle Private Cloud Appliance, refer to [Section 1.5, “High Availability”](#).

When you power on the Oracle 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 *master* role at any given time. During system initialization, after the management cluster is set up successfully, the master 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 [Section 1.4, “Provisioning and Orchestration”](#).



## 1.2.2 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, refer to [Server Components](#) 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 Oracle 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 25 compute nodes. 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 master 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 Oracle Server X8-2 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 Oracle 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*.



### Caution

When using expansion nodes containing fibre channel cards in a system with InfiniBand-based network architecture, the vHBAs **must** be disabled on those compute nodes.

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*.

## 1.2.3 Storage Appliance

The Oracle Private Cloud Appliance Controller Software continues to provide support for previous generations of the ZFS Storage Appliance installed in the base rack. However, there are functional differences between the Oracle ZFS Storage Appliance ZS7-2, which is part of systems with an Ethernet-based network architecture, and the previous models of the ZFS Storage Appliance, which are part of systems with an InfiniBand-based network architecture. For clarity, this section describes the different storage appliances separately.

### 1.2.3.1 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 Oracle 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 Oracle Private Cloud Appliance
  - [Database](#) – placeholder file system for databases
  - [Incoming](#) (20GB) – to be used for FTP file transfers, primarily for Oracle 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 the Oracle Private Cloud Appliance Release Notes.

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

### 1.2.3.2 Oracle ZFS Storage Appliance ZS5-ES and Earlier Models

The Oracle ZFS Storage Appliance ZS5-ES installed at the bottom of the appliance rack should be considered a 'system disk' for the entire appliance. Its main purpose is to provide storage space for the Oracle Private Cloud Appliance software. A portion of the disk space is made available for customer use and is sufficient for an Oracle VM storage repository with a limited number of virtual machines, templates and assemblies.

The hardware configuration of the Oracle ZFS Storage Appliance ZS5-ES is as follows:

- Two clustered storage heads with two 3.2TB SSDs each, used exclusively for cache
- One fully populated disk chassis with twenty 1.2TB 10000 RPM SAS hard disks
- RAID-Z2 configuration, for best balance between performance and data protection, with a total usable space of approximately 15TB



### Note

Oracle Private Cloud Appliance base racks shipped prior to software release 2.3.3 use a Sun ZFS Storage Appliance 7320 or Oracle ZFS Storage Appliance ZS3-ES. Those systems may be upgraded to a newer software stack, which continues to provide support for each Oracle Private Cloud Appliance storage configuration. The newer storage appliance offers the same functionality and configuration, with modernized hardware and thus better performance.

The storage appliance is connected to the management subnet ( [192.168.4.0/24](#) ) and the InfiniBand (IPoIB) 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-Z2 storage pool contains two projects, named [OVCA](#) and [OVM](#) .

The [OVCA](#) project contains all LUNs and file systems used by the Oracle 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 Oracle Private Cloud Appliance
  - [Database](#) – placeholder file system for databases

- `Incoming` (20GB) – to be used for FTP file transfers, primarily for Oracle 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` (300GB) – 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` (300GB) – to be used as Oracle VM storage repository in case NFS is preferred over iSCSI
  - `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 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 master management node in order to orchestrate the provisioning of all Oracle Private Cloud Appliance system components.

## 1.2.4 Network Infrastructure

For network connectivity, Oracle 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.

Depending on the exact hardware configuration of your appliance, the physical network layer is either high-speed Ethernet or InfiniBand. In this section, both network architectures are described separately in more detail.

### 1.2.4.1 Ethernet-Based 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 master 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. An Oracle 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 Oracle 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 Oracle 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 Oracle 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 Oracle 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 master 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.

### 1.2.4.2 InfiniBand-Based Network Architecture

Oracle Private Cloud Appliance with InfiniBand-based network architecture relies on a physical InfiniBand network fabric, with additional Ethernet connectivity for internal management communication.

## Ethernet

The Ethernet network relies on two interconnected Oracle Switch ES1-24 switches, to which all other rack components are connected with CAT6 Ethernet cables. This network serves as the appliance management network, in which every component has 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 InfiniBand fabric is not accessible, which means that the management network is the only way to connect to the system. Therefore, the administrator should connect a workstation to the available Ethernet port 19 in one of the Oracle Switch ES1-24 switches, 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 master management node at <http://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.

## InfiniBand

The Oracle Private Cloud Appliance rack contains two NM2-36P Sun Datacenter InfiniBand Expansion Switches. These redundant switches have redundant cable connections to both InfiniBand ports in each management node, compute node and storage head. Both InfiniBand switches, in turn, have redundant cable connections to both Fabric Interconnects in the rack. All these components combine to form a physical InfiniBand backplane with a 40Gbit (Quad Data Rate) bandwidth.

When the appliance initialization is complete, all necessary Oracle Private Cloud Appliance software packages, including host drivers and InfiniBand kernel modules, have been installed and configured on each component. At this point, the system is capable of using software defined networking (SDN) configured on top of the physical InfiniBand fabric. SDN is implemented through the Fabric Interconnects.

## Fabric Interconnect

All Oracle Private Cloud Appliance network connectivity is managed through the Fabric Interconnects. Data is transferred across the physical InfiniBand fabric, but connectivity is implemented in the form of Software Defined Networks (SDN), which are sometimes referred to as 'clouds'. The physical InfiniBand backplane is capable of hosting thousands of virtual networks. These Private Virtual Interconnects (PVI) dynamically connect virtual machines and bare metal servers to networks, storage and other virtual machines, while maintaining the traffic separation of hard-wired connections and surpassing their performance.

During the initialization process of the Oracle Private Cloud Appliance, five essential networks, four of which are SDNs, are configured: a storage network, an Oracle VM management network, a management Ethernet network, and two virtual machine networks. Tagged and untagged virtual machine traffic is supported. VLANs can be constructed using virtual interfaces on top of the existing bond interfaces of the compute nodes.

- The **storage network**, technically not software-defined, is a bonded IPoIB connection between the management nodes and the ZFS storage appliance, and uses the `192.168.40.0/24` subnet. This network also fulfills the heartbeat function for the clustered Oracle VM server pool. DHCP ensures that compute nodes are assigned an IP address in this subnet.
- The **Oracle VM management network** is a PVI that connects the management nodes and compute nodes in the `192.168.140.0/24` subnet. It is used for all network traffic inherent to Oracle VM Manager, Oracle VM Server and the Oracle VM Agents.
- The **management Ethernet network** is a bonded Ethernet connection between the management nodes. The primary function of this network is to provide access to the management nodes from the data center network, and enable the management nodes to run a number of system services. Since all compute

nodes are also connected to this network, Oracle VM can use it for virtual machine connectivity, with access to and from the data center network. 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.

- The **public virtual machine network** is a bonded Ethernet connection between the compute nodes. Oracle VM uses this network for virtual machine connectivity, where external access is required. Untagged traffic is supported by default over this network. Customers can add their own VLANs to the Oracle VM network configuration, and define the subnet(s) appropriate for IP address assignment at the virtual machine level. For external connectivity, the next-level data center switches must be configured to accept your tagged VLAN traffic.
- The **private virtual machine network** is a bonded Ethernet connection between the compute nodes. Oracle VM uses this network for virtual machine connectivity, where only internal access is required. 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.

Finally, the Fabric Interconnects also manage the physical public network connectivity of the Oracle Private Cloud Appliance. Two 10GbE ports on each Fabric Interconnect must be connected to redundant next-level data center switches. 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 Oracle 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 master 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** Fabric Interconnects have **two** 10GbE connections each to a pair of next-level data center switches. This configuration with four cable connections provides redundancy and load splitting at the level of the Fabric Interconnects, the 10GbE ports and the data center switches. This outbound cabling should not be crossed or meshed, because the internal connections to the pair of Fabric Interconnects are already configured that way. The cabling pattern plays a key role in the continuation of service during failover scenarios involving Fabric Interconnect outages and other components.

## 1.3 Software Components

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

### 1.3.1 Oracle Private Cloud Appliance Dashboard

The Oracle 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 Oracle Private Cloud Appliance configuration components



The Oracle Private Cloud Appliance Dashboard is described in detail in [Chapter 2, Monitoring and Managing Oracle Private Cloud Appliance](#).

### 1.3.2 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.

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 [Section 2.9, "Authentication"](#).

### 1.3.3 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 Oracle 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 12c:** including Application Development Framework (ADF) Release 12c, used to host and run the Oracle VM Manager application
- **MySQL 5.6 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 [Chapter 5, 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 an Oracle Private Cloud Appliance.

### 1.3.4 Operating Systems

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

- Management Nodes: Oracle Linux 6 with UEK R4
- Compute Nodes: Oracle VM Server 3.4.6
- 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 Oracle 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.

### 1.3.5 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 Oracle Private Cloud Appliance.

**Table 1.3 Oracle Private Cloud Appliance Databases**

Item	Description
Oracle Private Cloud Appliance Node Database	<p>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.</p> <p><b>Type:</b> BerkeleyDB</p> <p><b>Location:</b> <code>MGMT_ROOT/db/node</code> on the ZFS, accessible via <code>/nfs/shared_storage/db/node</code> on each management node</p>
Oracle Private Cloud Appliance Inventory Database	<p>Contains information on all hardware components appearing in the management network <code>192.168.4.0/24</code>. 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 Oracle Private Cloud Appliance services.</p> <p><b>Type:</b> BerkeleyDB</p> <p><b>Location:</b> <code>MGMT_ROOT/db/inventory</code> on the ZFS, accessible via <code>/nfs/shared_storage/db/inventory</code> on each management node</p>
Oracle Private Cloud Appliance Netbundle Database	<p>Predefines Ethernet and bond device names for all possible networks that can be configured throughout the system, and which are allocated dynamically.</p> <p><b>Type:</b> BerkeleyDB</p> <p><b>Location:</b> <code>MGMT_ROOT/db/netbundle</code> on the ZFS, accessible via <code>/nfs/shared_storage/db/netbundle</code> on each management node</p>
Oracle Private Cloud Appliance DHCP Database	<p>Contains information on the assignment of DHCP addresses to newly detected compute nodes.</p> <p><b>Type:</b> BerkeleyDB</p> <p><b>Location:</b> <code>MGMT_ROOT/db/dhcp</code> on the ZFS, accessible via <code>/nfs/shared_storage/db/dhcp</code> on each management node</p>
Cisco Data Network Database	<p>Contains information on the networks configured for traffic through the spine switches, and the interfaces participating in the networks.</p> <p>Used only on systems with Ethernet-based network architecture.</p>

Item	Description
Cisco Management Switch Ports Database	<p><b>Type:</b> BerkeleyDB</p> <p><b>Location:</b> <code>MGMT_ROOT/db/cisco_data_network_db</code> on the ZFS, accessible via <code>/nfs/shared_storage/db/cisco_data_network_db</code> on each management node</p> <p>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.</p> <p>Used only on systems with Ethernet-based network architecture.</p> <p><b>Type:</b> BerkeleyDB</p> <p><b>Location:</b> <code>MGMT_ROOT/db/cisco_ports</code> on the ZFS, accessible via <code>/nfs/shared_storage/db/cisco_ports</code> on each management node</p>
Oracle Fabric Interconnect Database	<p>Contains IP and host name data for the Oracle Fabric Interconnect F1-15s.</p> <p>Used only on systems with InfiniBand-based network architecture.</p> <p><b>Type:</b> BerkeleyDB</p> <p><b>Location:</b> <code>MGMT_ROOT/db/infrastructure</code> on the ZFS, accessible via <code>/nfs/shared_storage/db/infrastructure</code> on each management node</p>
Oracle Switch ES1-24 Ports Database	<p>Defines the factory-configured map of Oracle Switch ES1-24 ports to the rack unit or element to which that port is connected. It is used to map Oracle Switch ES1-24 ports to machine names.</p> <p>Used only on systems with InfiniBand-based network architecture.</p> <p><b>Type:</b> BerkeleyDB</p> <p><b>Location:</b> <code>MGMT_ROOT/db/opus_ports</code> on the ZFS, accessible via <code>/nfs/shared_storage/db/opus_ports</code> on each management node</p>
Oracle Private Cloud Appliance Mini Database	<p>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 an Oracle Private Cloud Appliance component. Entries contain a sync ID for more convenient usage within the Command Line Interface (CLI).</p> <p><b>Type:</b> BerkeleyDB</p> <p><b>Location:</b> <code>MGMT_ROOT/db/mini_db</code> on the ZFS, accessible via <code>/nfs/shared_storage/db/mini_db</code> on each management node</p>
Oracle Private Cloud Appliance Monitor Database	<p>Records fault counts detected through the ILOMs of all active components identified in the Inventory Database.</p> <p><b>Type:</b> BerkeleyDB</p> <p><b>Location:</b> <code>MGMT_ROOT/db/monitor</code> on the ZFS, accessible via <code>/nfs/shared_storage/db/monitor</code> on each management node</p>

Item	Description
Oracle Private Cloud Appliance Setup Database	<p>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.</p> <p><b>Type:</b> BerkeleyDB</p> <p><b>Location:</b> <code>MGMT_ROOT/db/setup</code> on the ZFS, accessible via <code>/nfs/shared_storage/db/setup</code> on each management node</p>
Oracle Private Cloud Appliance Task Database	<p>Contains state data for all of the asynchronous tasks that have been dispatched within the Oracle Private Cloud Appliance.</p> <p><b>Type:</b> BerkeleyDB</p> <p><b>Location:</b> <code>MGMT_ROOT/db/task</code> on the ZFS, accessible via <code>/nfs/shared_storage/db/task</code> on each management node</p>
Oracle Private Cloud Appliance Synchronization Databases	<p>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 <code>sync_errored_tasks</code> database, from where they can be retried or acknowledged.</p> <p>Synchronization databases are not present by default. They are created when the first synchronization task of a given type is received.</p> <p><b>Type:</b> BerkeleyDB</p> <p><b>Location:</b> <code>MGMT_ROOT/db/sync_*</code> on the ZFS, accessible via <code>/nfs/shared_storage/db/sync_*</code> on each management node</p>
Oracle Private Cloud Appliance Update Database	<p>Used to track the two-node coordinated management node update process.</p> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;">  </div> <div> <p><b>Note</b></p> <p>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.</p> </div> </div> <p><b>Type:</b> BerkeleyDB</p> <p><b>Location:</b> <code>MGMT_ROOT/db/update</code> on the ZFS, accessible via <code>/nfs/shared_storage/db/update</code> on each management node</p>
Oracle Private Cloud Appliance Tenant Database	<p>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.</p> <p><b>Type:</b> BerkeleyDB</p> <p><b>Location:</b> <code>MGMT_ROOT/db/tenant</code> on the ZFS, accessible via <code>/nfs/shared_storage/db/tenant</code> on each management node</p>

Item	Description
Oracle VM Manager Database	<p>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.</p> <p><b>Type:</b> MySQL Database</p> <p><b>Location:</b> <code>MGMT_ROOT/ovmm_mysql/data/</code> on the ZFS, accessible via <code>/nfs/shared_storage/ovmm_mysql/data/</code> on each management node</p>

## 1.3.6 Oracle Private Cloud Appliance Management Software

The Oracle 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 and some are listed as follows:

- `pca-backup`: the script responsible for performing backups of the appliance configuration as described in [Section 1.6, “Oracle Private Cloud Appliance Backup”](#)
- `pca-check-master`: a script that verifies which of the two management nodes currently has the master role
- `ovca-daemon`: the core provisioning and management daemon for the Oracle Private Cloud Appliance
- `pca-dhcpd`: a helper script to assist the DHCP daemon with the registration of compute nodes
- `pca-diag`: a tool to collect diagnostic information from your Oracle Private Cloud Appliance, as described in [Section 1.3.7, “Oracle Private Cloud Appliance Diagnostics Tool”](#)
- `pca-factory-init`: the appliance initialization script used to set the appliance to its factory configuration. This script does not function as a reset; it is only used for initial rack setup.
- `pca-redirect`: a daemon that redirects HTTP or HTTPS requests to the Oracle Private Cloud Appliance Dashboard described in [Section 1.3.1, “Oracle Private Cloud Appliance Dashboard”](#)
- `ovca-remote-rpc`: a script for 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`: a script that allows the Oracle 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 Oracle Private Cloud Appliance library that is installed in `/usr/lib/python2.6/site-packages/ovca/` on each management node.

### 1.3.7 Oracle Private Cloud Appliance Diagnostics Tool

The Oracle Private Cloud Appliance includes a tool that can be run to collect diagnostic data: logs and other types of files that can help to troubleshoot hardware and software problems. This tool is located in `/usr/sbin/` on each management and compute node, and is named `pca-diag`. The data it retrieves, depends on the selected command line arguments:

- `pca-diag`

When you enter this command, without any additional arguments, the tool retrieves a basic set of files that provide insights into the current health status of the Oracle Private Cloud Appliance. You can run this command on all management and compute nodes. All collected data is stored in `/tmp`, compressed into a single tarball (`ovcadiag_<node-hostname>_<ID>_<date>_<time>.tar.bz2`).

- `pca-diag version`

When you enter this command, version information for the current Oracle Private Cloud Appliance software stack is displayed. The `version` argument cannot be combined with any other argument.

- `pca-diag ilom`

When you enter this command, diagnostic data is retrieved, by means of `ipmitool`, through the host's ILOM. The data set includes details about the host's operating system, processes, health status, hardware and software configuration, as well as a number of files specific to the Oracle Private Cloud Appliance configuration. You can run this command on all management and compute nodes. All collected data is stored in `/tmp`, compressed into a single tarball (`ovcadiag_<node-hostname>_<ID>_<date>_<time>.tar.bz2`).

- `pca-diag vmpinfo`



#### Caution

When using the `vmpinfo` argument, the command must be run from the master management node.

When you enter this command, the Oracle VM diagnostic data collection mechanism is activated. The `vmpinfo3` script collects logs and configuration details from the Oracle VM Manager, and logs and `sosreport` information from each Oracle VM Server or compute node. All collected data is stored in `/tmp`, compressed into **two tarballs**: `ovcadiag_<node-hostname>_<ID>_<date>_<time>.tar.bz2` and `vmpinfo3-<version>-<date>-<time>.tar.gz`.

To collect diagnostic information for a subset of the Oracle VM Servers in the environment, you run the command with an additional `servers` parameter: `pca-diag vmpinfo servers='ovcacn07r1,ovcacn08r1,ovcacn09r1'`

Diagnostic collection with `pca-diag` is possible from the command line of any node in the system. Only the master management node allows you to use all of the command line arguments. Although `vmpinfo` is not available on the compute nodes, running `pca-diag` directly on the compute can help 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 may use it as part of their standard operating procedures, or Oracle Support teams may 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, also refer to the section [“Data Collection for Service and Support”](#) in the Oracle Private Cloud Appliance Release Notes.

## 1.4 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 master management node. This section explains what happens as the Oracle Private Cloud Appliance is initialized and all nodes are provisioned.

### 1.4.1 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 6 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 up 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 master management node continues to load the remaining Oracle Private Cloud Appliance services, including `dhcpd`, Oracle VM Manager and the Oracle 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.

### 1.4.2 Compute Node Discovery and Provisioning

#### Node Manager

To discover compute nodes, the Node Manager on the master 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 Oracle 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.

### 1.4.3 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 an Oracle 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 individual component level. Some are visible to the administrator, and some are entirely internal to the system. Throughout the life cycle 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 an Oracle 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.

## 1.5 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 an Oracle 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 master or active node in the cluster.

When the Oracle 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 master or active management node, runs the full complement of Oracle 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 Oracle 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 Oracle 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.

The [Oracle VM Concepts Guide](#) provides good background information about the principles of high availability. Refer to the section [How does High Availability \(HA\) Work?](#).

## 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, 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 Oracle 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 [Section 1.2.4, “Network Infrastructure”](#).

## 1.6 Oracle Private Cloud Appliance Backup

The configuration of all components within Oracle 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 [Command Line Interface](#). For details, refer to [Section 4.2.8, “backup”](#).

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
- **nm2**: used only on systems with InfiniBand-based network architecture; contains the NM2-36P Sun Datacenter InfiniBand Expansion Switch configuration data
- **opus**: used only on systems with InfiniBand-based network architecture; contains the Oracle Switch ES1-24 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 Oracle 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 the section entitled [Backing up and Restoring Oracle VM Manager](#), in the [Oracle VM Manager Administration 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.
- **xsigo**: used only on systems with InfiniBand-based network architecture; contains the configuration data for the Fabric Interconnects.
- **zfsa**: 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<sup>1</sup>.

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](#).

## 1.7 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

<sup>1</sup> Restoration from backup must only be performed by Oracle Service Personnel.

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.

For software update instructions, see [Chapter 3, \*Updating Oracle Private Cloud Appliance\*](#).

For specific Oracle Private Cloud Appliance Upgrader details, see [Section 3.2, “Using the Oracle Private Cloud Appliance Upgrader”](#).

---

# Chapter 2 Monitoring and Managing Oracle Private Cloud Appliance

## Table of Contents

2.1	Connecting and Logging in to the Oracle Private Cloud Appliance Dashboard .....	26
2.2	Oracle Private Cloud Appliance Accessibility Features .....	28
2.3	Hardware View .....	28
2.4	Network Settings .....	32
2.5	Functional Networking Limitations .....	35
2.5.1	Network Configuration of Ethernet-based Systems .....	36
2.5.2	Network Configuration of InfiniBand-based Systems .....	38
2.6	Network Customization .....	39
2.6.1	Configuring Custom Networks on Ethernet-based Systems .....	40
2.6.2	Configuring Custom Networks on InfiniBand-based Systems .....	44
2.6.3	Deleting Custom Networks .....	49
2.7	VM Storage Networks .....	50
2.7.1	Creating VM Storage Networks .....	50
2.7.2	Creating Storage Shares .....	51
2.7.3	Storage Profiles .....	53
2.8	Tenant Groups .....	54
2.8.1	Design Assumptions and Restrictions .....	54
2.8.2	Configuring Tenant Groups .....	54
2.9	Authentication .....	58
2.10	Health Monitoring .....	61
2.11	Fault Monitoring .....	63
2.11.1	Using Fault Monitoring Checks .....	64
2.11.2	Phone Home Service .....	67
2.12	Cloud Backup .....	68
2.12.1	Configuring the Cloud Backup Service .....	68
2.12.2	Configuring a Manual Cloud Backup .....	69
2.12.3	Deleting Cloud Backups .....	70
2.12.4	Deleting Oracle Cloud InfrastructureTargets .....	71
2.13	Kubernetes Engine .....	71
2.13.1	Kubernetes Guidelines and Limitations .....	71
2.13.2	Prepare the Cluster Environment .....	72
2.13.3	Create a Kubernetes Cluster on a DHCP Network .....	74
2.13.4	Create a Kubernetes Cluster on a Static Network .....	75
2.13.5	Use the Kubernetes Dashboard .....	77
2.13.6	Managing a Cluster .....	78
2.13.7	Stop a Cluster .....	79
2.13.8	Monitor Cluster Status .....	79
2.13.9	Resize Kubernetes Virtual Machine Disk Space .....	80
2.13.10	Maintain the Operating Systems on the Kubernetes Virtual Machines .....	81

Monitoring and management of the Oracle 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.

**Warning**

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 [Section 2.4, “Network Settings”](#).
- Hardware provisioning monitoring and identification of each hardware component used in the appliance, accessed via the Hardware View window described in [Section 2.3, “Hardware View”](#).
- Resetting the passwords used for different components within the appliance, via the Password Management window, as described in [Section 2.9, “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 Oracle 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 [Section 1.6, “Oracle Private Cloud Appliance Backup”](#).

- **Update**

The update process is controlled from the command line of the master management node, using the Oracle Private Cloud Appliance Upgrader. For details, see [Section 1.7, “Oracle Private Cloud Appliance Upgrader”](#). For step-by-step instructions, see [Chapter 3, \*Updating 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 [Section 2.6, “Network Customization”](#).

- **Tenant Groups**

The command line interface provides commands to optionally subdivide an Oracle 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 [Section 2.8, “Tenant Groups”](#).

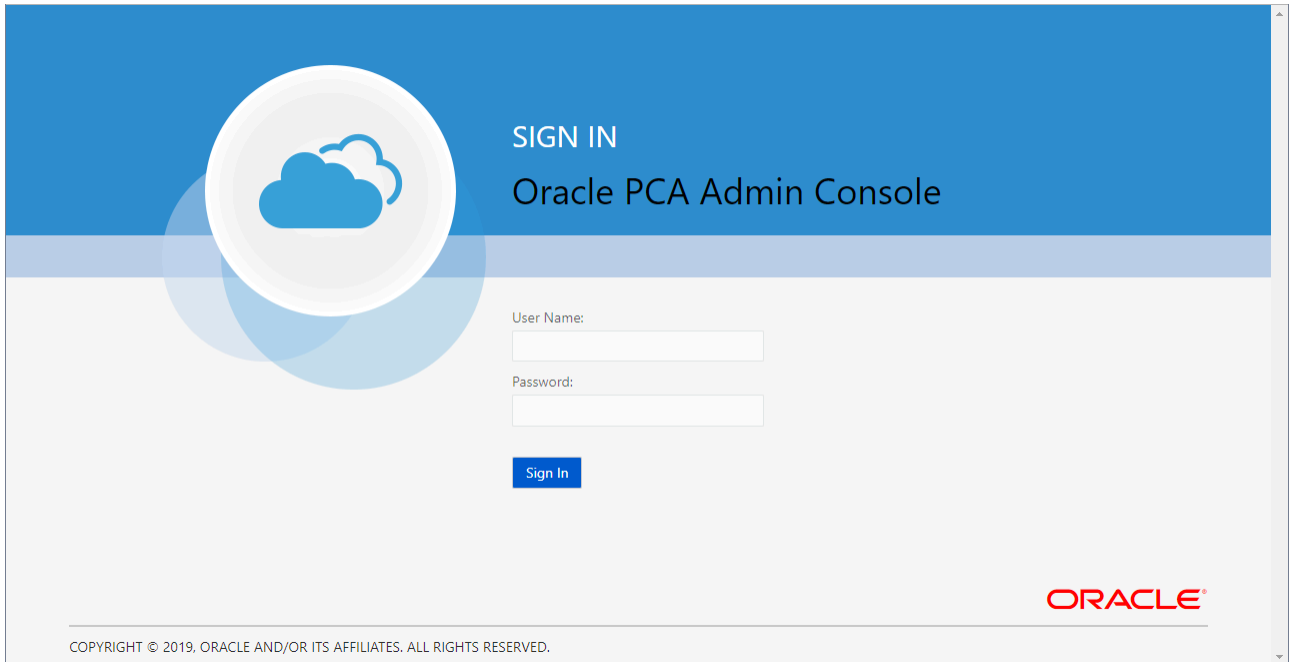
## 2.1 Connecting and Logging in to the Oracle Private Cloud Appliance Dashboard

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 have 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 master 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.

Systems with an InfiniBand-based network architecture contain a pair Oracle Switch ES1-24 switches instead. If your appliance contains such switches, connected the workstation to Ethernet port 19 in one of them, not both.

The default user name is **admin** and the default password is **Welcome1**. For security reasons, you must set a new password at your earliest convenience.



**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.

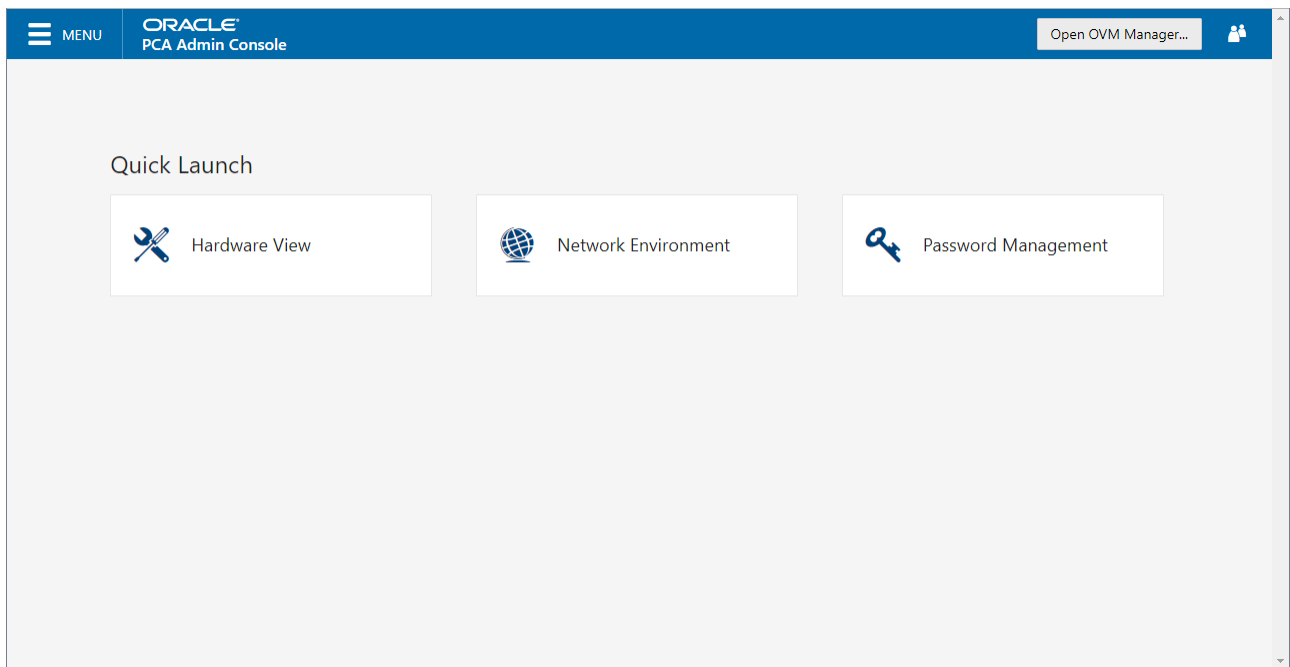


### Important

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.

## 2.2 Oracle Private Cloud Appliance Accessibility Features

For detailed accessibility information, refer to the chapter [Documentation Accessibility](#) in the *Oracle Private Cloud Appliance Release Notes*.

### 2.3 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 [Section 7.10, “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 Oracle 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 Oracle 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.

# Base Rack Front View

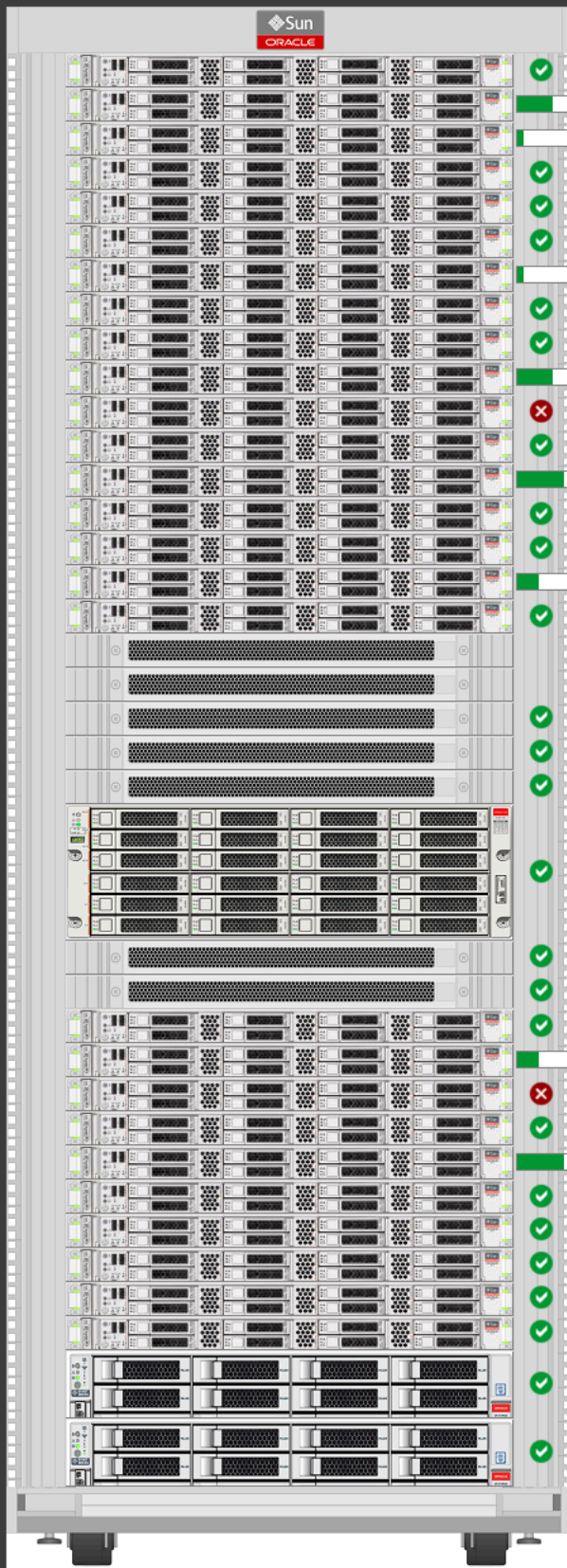
Refresh

Disable CN Provisioning

Auto refresh interval

30 seconds

✔ 7    ⌚ 0    ✖ 0



## 2.4 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
- 192.168.140.0/24 – internal Oracle VM management network: connects Oracle VM Manager, Oracle VM Server and Oracle VM Agents (applies only to the InfiniBand-based architecture)
- 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 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**

The screenshot shows the Oracle PCA Admin Console interface for the Network Environment configuration. The page title is "Network Environment" and it includes a sub-header "Changes to the Network Environment configuration data requires entering the PCA Admin Password before selecting the 'Apply Changes' button." The "Management Nodes" tab is selected, showing three configuration sections: "Management Node 1", "Management Node 2", and "Management Virtual IP Address". Each section has an "IP Address" and "Host Name" field. The "Management Virtual IP Address" section has an "IP Address" field. At the bottom, there is a "PCA Admin Password" field and "Reset" and "Apply Changes" buttons.

Field	Value
Management Node 1 IP Address	10.19.1.101
Management Node 1 Host Name	manager1
Management Node 2 IP Address	10.19.1.102
Management Node 2 Host Name	manager2
Management Virtual IP Address IP Address	10.19.1.100

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**

For systems with Ethernet-based network architecture, a management VLAN requires additional configuration steps.

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, refer to the [Oracle VM documentation](#).

- **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**

The screenshot shows the Oracle PCA Admin Console interface for the 'Network Environment' section. The 'Data Center Network' tab is selected. The configuration includes a 'Management Network VLAN' toggle (turned on) and a dropdown menu showing '20'. Below this are four required fields: 'Domain Name' (example.com), 'Netmask' (255.255.0.0), 'Default Gateway' (10.19.1.1), and 'NTP' (10.19.1.1). At the bottom, there is a password field labeled '\* PCA Admin Password(Required for changes)', a 'Reset' button, and an 'Apply Changes' button. The top navigation bar includes a 'MENU' icon, 'ORACLE PCA Admin Console' text, and an 'Open OVM Manager...' button.

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

The screenshot displays the 'Network Environment' configuration page in the Oracle PCA Admin Console, specifically the 'DNS' tab. The page header includes the Oracle logo and 'PCA Admin Console'. A navigation bar at the top shows 'Management Nodes', 'Data Center Network', and 'DNS'. Below the navigation bar, there is a warning message: 'Changes to the Network Environment configuration data requires entering the PCA Admin Password before selecting the 'Apply Changes' button.' The main content area contains three rows for DNS server configuration:

Label	Value
* DNS Server 1	217.6.34.47
DNS Server 2	144.20.190.70
DNS Server 3	

At the bottom of the page, there is a password field labeled '\* PCA Admin Password(Required for changes)', a 'Reset' button, and an 'Apply Changes' button.

You must enter the current Oracle 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 afterwards.

## 2.5 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 Architecture Differences

Oracle Private Cloud Appliance exists in two different types of network architecture. One is built around a physical InfiniBand fabric; the other relies on physical high speed Ethernet connectivity. While the two implementations offer practically the same functionality, there are visible hardware and configuration differences.

This section is split up by network architecture to avoid confusion. Refer to the subsection that applies to your appliance.

### 2.5.1 Network Configuration of Ethernet-based Systems

This section describes the Oracle Private Cloud Appliance and Oracle VM network configuration for systems with an Ethernet-based network architecture.

- **Virtual Machine Network**

By default, a fully provisioned Oracle 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 [Section 5.6, “Configuring Network Resources for Virtual Machines”](#).



#### Note

Do not create virtual machine networks using the `ethx` ports. These are detected in Oracle VM Manager as physical compute node network interfaces, but they are not cabled. Also, the `bondx` 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 Oracle 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 Oracle 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 [Section 2.6, “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 [Section 2.8, “Tenant Groups”](#).

Once custom networks have been fully configured through the Oracle 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 Oracle 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 is 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.

## 2.5.2 Network Configuration of InfiniBand-based Systems

This section describes the Oracle Private Cloud Appliance and Oracle VM network configuration for systems with an InfiniBand-based network architecture.

### • Virtual Machine Network

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

- `vm_public_vlan`, created on the `bond4` interfaces of all compute nodes during provisioning
- `vm_private`, created on the `bond3` 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' `bond4` ports. For internal-only VM traffic, use the `bond3` ports. For details, see [Section 5.6, “Configuring Network Resources for Virtual Machines”](#).



#### Note

Do not create virtual machine networks using the `ethx` ports. These are detected in Oracle VM Manager as physical compute node network interfaces, but they are not cabled. Also, most network interfaces are combined in pairs to form bond ports, and are not intended to be connected individually.

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 Oracle Private Cloud Appliance CLI. This generates additional bond ports equivalent to the default `bond3` and `bond4`. The custom networks and associated bond ports 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 bond ports and terminating on different Fabric Interconnect I/O ports. Whenever public connectivity is required, additional cabling between the I/O ports 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 Oracle 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 [Section 2.6, “Network Customization”](#).

If your environment has 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 [Section 2.8, “Tenant Groups”](#).

Once custom networks have been fully configured through the Oracle 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 bond ports, 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: `mgmt_public_eth`, `192.168.140.0`, `192.168.40.0`, `vm_public_vlan` and `vm_private`. For networks connecting compute nodes, including custom networks, you must use the Oracle 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 Fabric Interconnect configuration, which cannot be controlled from within Oracle VM Manager.

## • VLAN Management

With the exception of the appliance management VLAN, which is configured 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 is 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.

## 2.6 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.



### Warning

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.



### Warning

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 Oracle 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 Oracle 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.

## Network Architecture Differences

Oracle Private Cloud Appliance exists in two different types of network architecture. One is built around a physical InfiniBand fabric; the other relies on physical high speed Ethernet connectivity. While the two implementations offer practically the same functionality, the configuration of custom networks is different due to the type of network hardware.

This section is split up by network architecture to avoid confusion. Refer to the subsection that applies to your appliance.

### 2.6.1 Configuring Custom Networks on Ethernet-based Systems

This section describes how to configure custom networks on a system with an Ethernet-based network architecture.

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 the *Oracle Private Cloud Appliance Installation Guide*.

#### Creating a Custom Network on an Ethernet-based System

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



### Note

The default `root` password is *Welcome1*. For security reasons, you must set a new password at your earliest convenience.

```
# 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: 2.4.3
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 [Section 4.2.18, “create uplink-port-group”](#) for command details.

Network ports can not be part of more than one network configuration.

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

- `rack_internal_network`
- `external_network`
- `host_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 [Section 4.2.12, "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 ovcaen07r1
Status: Success
PCA> add network MyPublicNetwork ovcaen08r1
Status: Success
PCA> add network MyPublicNetwork ovcaen09r1
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     ovcaen07r1, ovcaen08r1, ovcaen09r1
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.



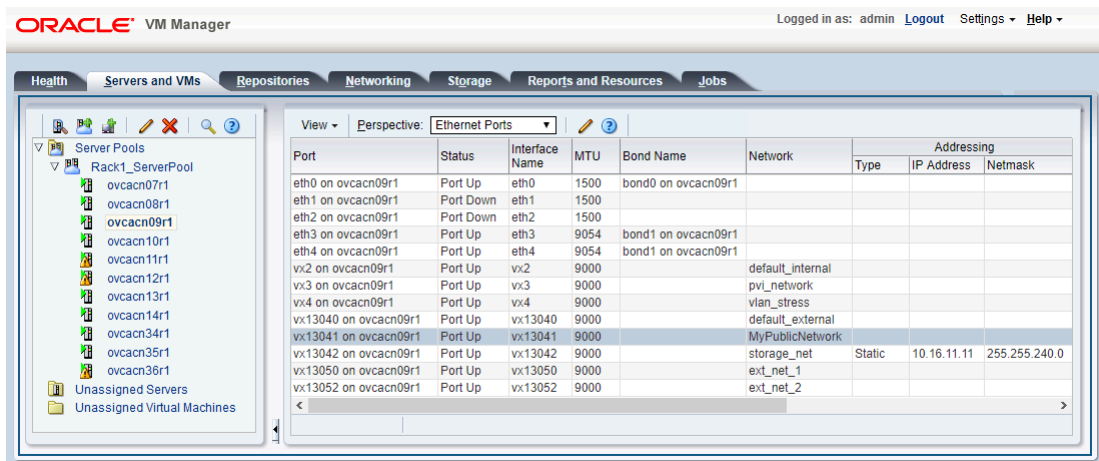
**Note**

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 (Ethernet-based Architecture)**



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



**Warning**

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
```

## 2.6.2 Configuring Custom Networks on InfiniBand-based Systems



This section describes how to configure custom networks on a system with an InfiniBand-based network architecture.

For all networks with external connectivity the Fabric Interconnect I/O 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.

### Creating a Custom Network on an InfiniBand-based System

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



#### Note

The default `root` password is *Welcome1*. For security reasons, you must set a new password at your earliest convenience.

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

- Launch the Oracle Private Cloud Appliance command line interface.

```
# pca-admin
Welcome to PCA! Release: 2.4.3
PCA>
```

- If your custom network requires public connectivity, you need to use one or more Fabric Interconnect ports. Verify the number of I/O modules and ports available and carefully plan your network customizations accordingly. The following example shows how to retrieve that information from your system:

```
PCA> list network-card --sorted-by Director
```

Slot	Director	Type	State	Number_Of_Ports
3	ovcasw15r1	sanFc2Port8GbLrCardEthIb	up	2
18	ovcasw15r1	sanFc2Port8GbLrCardEthIb	up	2
16	ovcasw15r1	nwEthernet4Port10GbCardEthIb	up	4
5	ovcasw15r1	nwEthernet4Port10GbCardEthIb	up	4
17	ovcasw15r1	nwEthernet4Port10GbCardEthIb	up	4
4	ovcasw15r1	nwEthernet4Port10GbCardEthIb	up	4
16	ovcasw22r1	nwEthernet4Port10GbCardEthIb	up	4
5	ovcasw22r1	nwEthernet4Port10GbCardEthIb	up	4
18	ovcasw22r1	sanFc2Port8GbLrCardEthIb	up	2
17	ovcasw22r1	nwEthernet4Port10GbCardEthIb	up	4
4	ovcasw22r1	nwEthernet4Port10GbCardEthIb	up	4
3	ovcasw22r1	sanFc2Port8GbLrCardEthIb	up	2

```
-----
12 rows displayed

Status: Success
PCA> list network-port --filter-column Type --filter nwEthernet* --sorted-by State
```

Port	Director	Type	State	Networks
4:4	ovcasw15r1	nwEthernet10GbPort	down	None
4:3	ovcasw15r1	nwEthernet10GbPort	down	None
4:2	ovcasw15r1	nwEthernet10GbPort	down	None
5:4	ovcasw15r1	nwEthernet10GbPort	down	None
5:3	ovcasw15r1	nwEthernet10GbPort	down	None
5:2	ovcasw15r1	nwEthernet10GbPort	down	None
10:4	ovcasw15r1	nwEthernet10GbPort	down	None
10:3	ovcasw15r1	nwEthernet10GbPort	down	None
10:2	ovcasw15r1	nwEthernet10GbPort	down	None

```

10:1      ovcasw15r1      nwEthernet10GbPort      down      None
11:4      ovcasw15r1      nwEthernet10GbPort      down      None
11:3      ovcasw15r1      nwEthernet10GbPort      down      None
11:2      ovcasw15r1      nwEthernet10GbPort      down      None
11:1      ovcasw15r1      nwEthernet10GbPort      down      None
4:4       ovcasw22r1      nwEthernet10GbPort      down      None
4:3       ovcasw22r1      nwEthernet10GbPort      down      None
4:2       ovcasw22r1      nwEthernet10GbPort      down      None
5:4       ovcasw22r1      nwEthernet10GbPort      down      None
5:3       ovcasw22r1      nwEthernet10GbPort      down      None
5:2       ovcasw22r1      nwEthernet10GbPort      down      None
10:4      ovcasw22r1      nwEthernet10GbPort      down      None
10:3      ovcasw22r1      nwEthernet10GbPort      down      None
10:1      ovcasw22r1      nwEthernet10GbPort      down      None
11:3      ovcasw22r1      nwEthernet10GbPort      down      None
11:2      ovcasw22r1      nwEthernet10GbPort      down      None
11:1      ovcasw22r1      nwEthernet10GbPort      down      None
4:1       ovcasw15r1      nwEthernet10GbPort      up        mgmt_public_eth, vm_public_vlan
5:1       ovcasw15r1      nwEthernet10GbPort      up        mgmt_public_eth, vm_public_vlan
4:1       ovcasw22r1      nwEthernet10GbPort      up        mgmt_public_eth, vm_public_vlan
5:1       ovcasw22r1      nwEthernet10GbPort      up        mgmt_public_eth, vm_public_vlan
10:2      ovcasw22r1      nwEthernet10GbPort      up        None
11:4      ovcasw22r1      nwEthernet10GbPort      up        None
-----
32 rows displayed

Status: Success
    
```

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

- [rack\\_internal\\_network](#)
- [external\\_network](#)
- [host\\_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 Fabric Interconnect port(s) to be configured for external traffic.

```

PCA> create network MyPublicNetwork external_network '4:2 5:2'
Status: Success
    
```



#### Note

The port arguments are specified as '*x:y*' where *x* is the I/O module slot number and *y* is the number of the port on that module. The example above shows how to retrieve that information.

I/O ports can not be part of more than one network configuration.

If, instead of using the CLI interactive mode, you create a network in a single CLI command from the Oracle Linux prompt, you must escape the quotation

marks to prevent bash from interpreting them. Add a backslash character before each quotation mark:

```
# pca-admin create network MyPublicNetwork external_network \'4:2 5:2\'
```

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

```
PCA> create network MyHostNetwork host_network '10:1 11:1' \  
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 [Section 4.2.12, "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.

5. 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

6. Verify the configuration of the new custom network.

```
PCA> show network MyPublicNetwork

-----
Network_Name      MyPublicNetwork
Trunkmode         True
Description       User defined network
Ports             ['4:2', '5:2']
vNICs            ovcacn09r1-eth8, ovcacn07r1-eth8, ovcacn08r1-eth8
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 bond of two new vNICs 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.



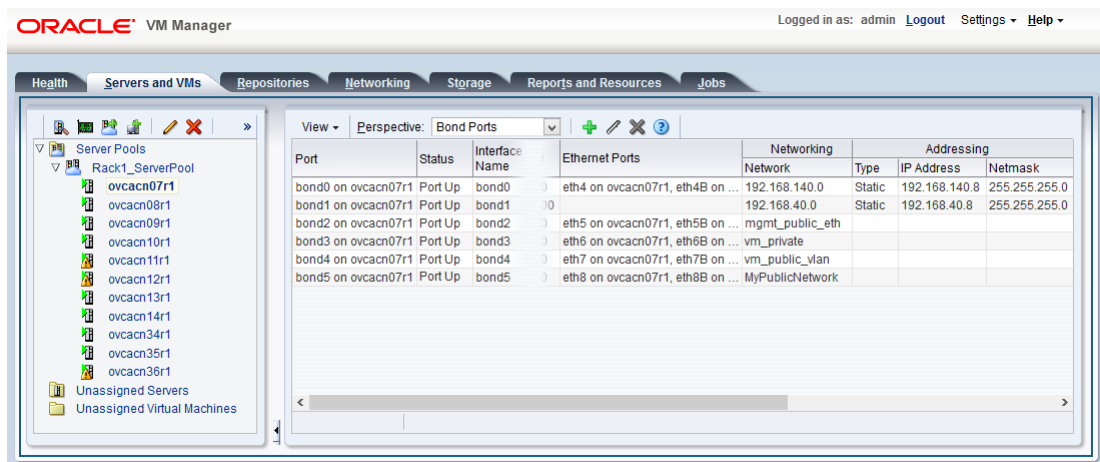
**Note**

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 2.8 shows a custom network named *MyPublicNetwork*, which is VLAN-enabled and uses the compute node's *bond5* interface consisting of Ethernet ports (vNICs) *eth8* and *eth8B*.

**Figure 2.8 Oracle VM Manager View of Custom Network Configuration (InfiniBand-based Architecture)**



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



**Warning**

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
```

## 2.6.3 Deleting Custom Networks

This section describes how to delete custom networks. The procedure is the same for systems with an Ethernet-based and InfiniBand-based network architecture.

### Deleting a Custom Network



**Caution**

Before deleting a custom network, make sure that all servers have been disconnected from it first.

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



**Note**

The default `root` password is `Welcome1`. For security reasons, you must set a new password at your earliest convenience.

```
# 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: 2.4.3
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.



**Note**

The command output sample below shows a public network configuration on an Ethernet-based system. The configuration of a public network on an InfiniBand-based system looks slightly different.

```
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.

## 2.7 VM Storage Networks

Starting with Oracle Private Cloud Appliance Controller Software release 2.4.3 running on Ethernet-based systems, you can configure private storage networks that grant users access to the internal ZFS storage appliance from their Oracle VM environment. Oracle 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. To ensure you can use this functionality, upgrade the storage network as described in [Section 3.2.5, “Upgrading the Storage Network”](#).

Administrators can create up to sixteen VM storage networks, which can be aligned with any particular tenant group, and users can be associated with one or more VM storage networks. Each VM storage network is assigned a single, private non-routed VXLAN to ensure the network is isolated. End users cannot gain root access to manage the internal ZFS storage appliance through the VM storage networks.

### 2.7.1 Creating VM Storage Networks

This section describes how to create a VM storage network on an Ethernet-based system.

#### Creating a VM Storage Network

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



**Note**

The default `root` password is `Welcome1`. For security reasons, you must set a new password at your earliest convenience.

```
# 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: 2.4.3
PCA>
```

3. Create the new VM storage network. Specify the network name, the network prefix, netmask, and ZFS IP address.

```
PCA> create network stg_nw1 storage_network 10.10.10 255.255.254.0 10.10.10.100
Status: Success
```

The new VM storage network appears in Oracle VM Manager network tab.

4. Connect the required compute nodes to the new storage network. You must provide the network name and the name of the server to connect. Run this command for each server you want to add to the network.

```
PCA> add network stg_nw1 ovcacn07r1
Status: Success
```

To add the network to all compute nodes in a tenant group at once, use this command:

```
PCA> add network-to-tenant-group stg_nw1 Rack01_ServerPool
```

The new storage network appears.



### Caution

Do not assign the IP address to the Ethernet interface that gets assigned to the compute with the addition of storage network

5. Verify the configuration of the new VM storage network.

```
PCA> show network l_stg_nw
-----
Network_Name      stg_nw1
Trunkmode         None
Description       None
Ports            None
vNICs            None
Status           ready
Network_Type     storage_network
Compute_Nodes    ovcacn07r1
Prefix           10.10.10
Netmask          255.255.254.0
Route_Destination None
Route_Gateway    None
Storage_IP       None
-----
Status: Success
```

Next, assign shares to the VM storage network.

## 2.7.2 Creating Storage Shares

Once you have created a VM storage network, you can add storage shares to that network. These procedures describe how to add NFS file system and iSCSI LUNs storage shares, and grant access to those shares.



**Caution**

Do not use NFS Shares and iSCSI LUNs created from the Oracle Private Cloud Appliance command line to create Repositories from the compute nodes. This can cause data corruption if the shares are already in use by the virtual machines.

**Create and Map an NFS File System Share**

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



**Note**

The default `root` password is *Welcome1*. For security reasons, you must set a new password at your earliest convenience.

```
# 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: 2.4.3
PCA>
```

3. Create an NFS file system share. Specify these arguments: share name, the LUN name, the network name, the LUN size, and the optional profile name.

```
PCA> create nfs-storage fs1 accounting 50G bkup_basic
```

For more information about the optional storage profile argument, see [Section 2.7.3, "Storage Profiles"](#).

The new storage share appears on the internal ZFS storage appliance.

4. Grant access to the NFS file system share by creating an exception. Specify the share name, and list the IP address or CIDR you want to have access to the share. See [Section 4.2.5, "add nfs-exception"](#).



**Note**

Only virtual machines within the same subnet/network can have access to the filesystem.

```
PCA> add nfs-exception fs1 10.10.0.151/32
Status: Success
```

5. Verify the configuration of the new storage share.

```
PCA> show nfs-storage fs1
-----
Share Name          fs1
Network Name        2_stg_nw
Quota                10G
Profile              general
Mount point          /export/vminternal/fs1
NFS Exceptions       ['10.10.0.151/32']
-----
Status: Success
```

6. To remove an exception from a storage share use the `remove nfs-exception` command.

```
PCA> remove nfs-exception fs1 10.10.0.151/32
```



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

### Create and Map an iSCSI LUN Share

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



**Note**

The default `root` password is `Welcome1`. For security reasons, you must set a new password at your earliest convenience.

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

- Launch the Oracle Private Cloud Appliance command line interface.

```
# pca-admin
Welcome to PCA! Release: 2.4.3
PCA>
```

- Create an iSCSI LUN share. Specify the share name, the network name, the quota/size, and the optional profile name.

```
PCA> create iscsi-storage myNFSstorage management 120G general
```

For more information about the optional storage profile argument, see [Section 2.7.3, "Storage Profiles"](#).

The new storage share appears on the internal ZFS storage appliance.

- Grant access to the iSCSI LUN share by adding an initiator. Specify the LUN name, and list the initiator IQN from the virtual machine you want to have access to the share. See [Section 4.2.2, "add initiator"](#).



**Note**

Only virtual machines within the same subnet/network can have access to the filesystem.

```
PCA> add initiator myNFSstorage iqn.1918-12.com.mycompany:181b866f5a
need example
Status: Success
```

The new storage shares are now accessible from Oracle VM servers on the compute nodes just added.

## 2.7.3 Storage Profiles

Oracle Private Cloud Appliance provides a default storage profile based on I/O performance for NFS and iSCSI shares. If you have the need, you can choose from two additional storage profiles when creating your storage shares. The following profiles are available for each share type:

**Table 2.2 Storage Profiles**

Storage Share Type	Profile 1: general (default)	Profile 2: dbms_oracle	Profile 3: bkup_basic
NFS	• compression=lz4	• compression=lz4	• compression=lz4

Storage Share Type	Profile 1: general (default)	Profile 2: dbms_oracle	Profile 3: bkup_basic
	<ul style="list-style-type: none"> <li>recordsize=128K</li> <li>logbias=latency</li> </ul>	<ul style="list-style-type: none"> <li>recordsize=32K</li> <li>logbias=latency</li> </ul>	<ul style="list-style-type: none"> <li>recordsize=1M</li> <li>logbias=latency</li> </ul>
iSCSI	<ul style="list-style-type: none"> <li>compression=lz4</li> <li>logbias=latency</li> <li>volblocksize =128K</li> </ul>	<ul style="list-style-type: none"> <li>compression=lz4</li> <li>logbias=latency</li> <li>volblocksize =32K</li> </ul>	<ul style="list-style-type: none"> <li>compression=lz4</li> <li>logbias=throughput</li> <li>volblocksize =1M</li> </ul>

After creation, you can change the storage profile from the storage appliance command line or browser interface. See the [Shares and Projects](#) section in *Oracle® ZFS Storage Appliance Administration Guide, Release OS8.8.x*.

## 2.8 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 Oracle Private Cloud Appliance environment. Tenant groups provide an optional mechanism for an Oracle 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.

### 2.8.1 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 Oracle 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.

### 2.8.2 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 VM operations to set up the server pool, and a synchronization service maintains settings across the members of the tenant group.



#### Warning

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 Oracle 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 [Section 7.14, “Recovering from Tenant Group Configuration Mismatches”](#).



**Note**

For detailed information about the Oracle Private Cloud Appliance CLI tenant group commands, see [Chapter 4, The Oracle Private Cloud Appliance Command Line Interface \(CLI\)](#).



**Note**

The command output samples in this section reflect the network configuration on an Ethernet-based system. The network-related properties of a tenant group look slightly different on an InfiniBand-based system.

**Creating and Populating a Tenant Group**

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



**Note**

The default `root` password is `Welcome1`. For security reasons, you must set a new password at your earliest convenience.

```
# 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: 2.4.3
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 un-present 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

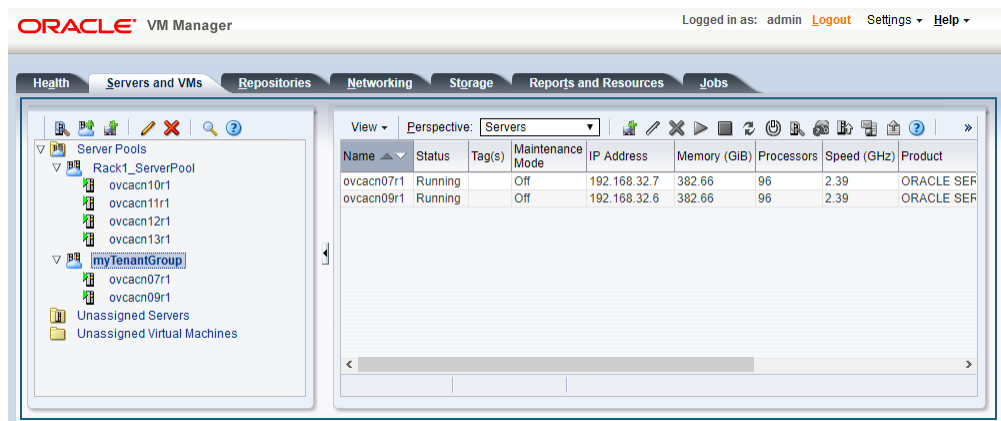
-----
Name                myTenantGroup
Default             False
Tenant_Group_ID    0004fb00000200008154bf592c8ac33b
Servers            ['ovcacn07r1', 'ovcacn09r1']
State              ready
Tenant_Group_VIP   None
Tenant_Networks    ['storage_internal', 'mgmt_internal', 'underlay_internal', 'underlay_external',
                    '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 2.9](#) 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 [Section 5.7, “Viewing and Managing Storage Resources”](#).

**Figure 2.9 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 server 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 more details, refer to the support note with [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.

## 2.9 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 Oracle Private Cloud Appliance `admin` user in the field labelled **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 Oracle 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 mis-typed 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. By clicking **Select All** you can apply a global password to all components that are used in the appliance. 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.



### Note

On InfiniBand-based systems, the list contains three separate password settings for the data network leaf switches, which are NM2-36P Sun Datacenter InfiniBand Expansion Switches:

- The **Leaf Switch root password** check box sets the password for the root user for the NM2-36P Sun Datacenter InfiniBand Expansion Switches.
  - The **Leaf Switch ILOM admin password** check box sets the password for the admin user for the ILOM of the NM2-36P Sun Datacenter InfiniBand Expansion Switches.
  - The **Leaf Switch ILOM operator password** check box sets the password for the operator user for the ILOM of the NM2-36P Sun Datacenter InfiniBand Expansion Switches.
- **Oracle Management Network Switch admin password:** Set the new password for the admin user for the Cisco Nexus 9348GC-FXP Switch.



### Note

On InfiniBand-based systems, this setting applies to the root user for the Oracle Switch ES1-24 switches.

- **Oracle Data Network Spine Switch admin password:** Set the new password for the admin user for the *spine* Cisco Nexus 9336C-FX2 Switches.

**Note**

On InfiniBand-based systems, the list contains three separate password settings for the data network spine switches, which are Oracle Fabric Interconnect F1-15 devices:

- The **Spine Switch admin password** check box sets the password for the admin user for the Oracle Fabric Interconnect F1-15s.
  - The **Spine Switch recovery password** sets the password for recovery operations on the Oracle Fabric Interconnect F1-15s. This password is used in the case of a corruption or when the admin password is lost. The Fabric Interconnects can be booted in 'recovery mode' and this password can be used to access the recovery mode menu.
  - The **Spine Switch root password** check box sets the password for the root user for the Oracle Fabric Interconnect F1-15s.
- **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 2.10 Password Management

The screenshot shows the Oracle PCA Admin Console interface for password management. The header includes the Oracle logo and 'PCA Admin Console'. The main content area is titled 'Password Management' and has a sub-tab 'Change Passwords'. On the left, there are three password input fields: '\* Current PCA Admin Password', '\* New Password', and '\* Verify New Password'. On the right, under 'Apply New Password To:', there is a 'Select All' checkbox and a list of components with checkboxes, all of which are checked. The components listed are: Oracle VM Manager/PCA Admin password, Oracle MySQL password, Oracle Weblogic Server password, Oracle Data Network Leaf Switch admin password, Oracle Management Network Switch admin password, Oracle Data Network Spine Switch admin password, Oracle ZFS Storage root password, PCA Management Node root password, PCA Compute Node root password, PCA Management Node SP/ILOM root password, and PCA Compute Node SP/ILOM root password. At the bottom right, there are 'Reset' and 'Apply Changes' buttons.

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 [Section 4.2.56, “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.

## 2.10 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 master management node, 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.



#### Note

The default `root` password is *Welcome1*. For security reasons, you must set a new password at your earliest convenience.

```
# 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.

## 2.11 Fault Monitoring

For Oracle Private Cloud Appliance 2.4.3, the existing health checker becomes a service, started by the `ovca-daemon` on the active management node. Checks can be run manually from the command line, or

using definitions in the scheduler. Depending on the check definition, the PCA health checker, the Oracle VM health check, and the PCA pre-upgrade checks can be invoked.

- `pca_healthcheck` monitors the health of system hardware components. For more details, refer to the [Health Monitoring](#).
- `ovm_monitor` monitors the Oracle VM manger objects and other environment factors.
- `pca_upgrader` monitors the system during an upgrade.

Health checking can be integrated with ZFS Phone Home service to send reports on a weekly basis to Oracle. The Phone Home function needs to be activated by the customer and requires that the appliance is registered with ASR. No separate installation is required; all functions come with controller software in Oracle Private Cloud Appliance 2.4.3. For configuration information see [Section 2.11.2, “Phone Home Service”](#).

## 2.11.1 Using Fault Monitoring Checks

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

### Running Fault Monitor Tests Manually

The Fault Monitoring utility provides flexibility in that you can choose to run an individual check, all the check for a particular monitoring service, or all of the checks 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 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
```

```
[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            check_hardware_faults
validate_image                  check_available_space           check_ovs_version
check_max_paths_iscsi           check_serverUpdateConfiguration check_uptime
check_onf_error                 verify_password                 verify_ntp_server
check_rpm_db                    verify_network_config           check_custom_multipath
check_yum_proxy                 check_motd                      verify_ovmm_cache
check_yum_repo                  connect_mysql                   check_os
check_osa_disabled              check_xsigo_configs            verify_ntp_xsigo
check_pca_services              check_mysql_desync_passwords    check_max_paths_fc
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 a list of specific checks. List one or more checks, preceded with `-m`.

```
[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 certain checks have resulted in failures, 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` check are scheduled to run weekly. You can change the frequency of these checks or add additional individual 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 scheduling format described below.

```

* * * * *  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
```

## 2.11.2 Phone Home Service

The fault management 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 existing Phone Home service of the ZFS storage appliance.

### Activating the Phone Home Service for Oracle Private Cloud Appliance

1. Install ASR on the Oracle Private Cloud Appliance. See [How to Install Auto Service Request \(ASR\) on Private Cloud Appliance \(PCA\) X8 \(Doc ID 2560988.1\)](#).
2. Once ASR is installed on your PCA, you must log in to your My Oracle Service account and approve the Oracle Private Cloud Appliance as a new asset. See [How To Manage and Approve Pending Oracle Auto Service Request \(ASR\) Assets In My Oracle Support \(Doc ID 1329200.1\)](#).
3. Using SSH and an account with superuser privileges, log in to the active management node.



#### Note

The default `root` password is `Welcome1`. For security reasons, you must set a new password at your earliest convenience.

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

4. Enable Phone Home in the fault monitoring service by setting the `enable_phonehome` property to `1` in the `ovca-system.conf` file on both management nodes.

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

```
[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
```

5. Log in to the ZFS storage appliance browser interface and enable Phone Home. **Go to Configuration > Services > Phone Home** and click the power icon to bring the service online.

Now your system is configured to send fault reports to Oracle for automated service response.

## 2.12 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 Oracle Private Cloud Appliance to a running state after a catastrophic event, it 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 [Doc ID 1959182.1 Oracle VM 3: Getting Started with Disaster Recovery using Oracle Site Guard](#).

The Cloud Backup service requires an Oracle Cloud Infrastructure cloud tenancy. The service is designed create a snapshot of backup data from the system, store that snapshot on the internal ZFSSA, 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 ZFSSA and on your Oracle Cloud Infrastructure tenancy. At this time, contact Oracle Service to restore your Oracle 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 Oracle 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 <https://docs.cloud.oracle.com/en-us/iaas/Content/Object/Concepts/objectstorageoverview.htm>.

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

For the best experience using the Cloud Backup service, 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, 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](#).

### 2.12.1 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 Oracle Private



Cloud Appliance, and finally pushes those backups from your Oracle 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 store bucket on your Oracle Cloud Infrastructure tenancy. See the [Creating a Bucket](#) section of [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 Oracle 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.



#### Note

The default `root` password is `Welcome1`. For security reasons, you must set a new password at your earliest convenience.

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

- b. Launch the Oracle Private Cloud Appliance command line interface.

```
# pca-admin
Welcome to PCA! Release: 2.4.3
PCA>
```

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

This step creates a target on your PCA ZFSSA that sends scheduled backups to an object storage bucket on Oracle Cloud Infrastructure. For more information see [Section 4.2.16, "create oci-target"](#).

```
PCA> create oci-target <target name> <target location> <target user> <target bucket> <target tenancy>
```

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.

## 2.12.2 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.



**Note**

The default `root` password is `Welcome1`. For security reasons, you must set a new password at your earliest convenience.

```
# 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: 2.4.3
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.

### 2.12.3 Deleting Cloud Backups

This section describes how to delete a Cloud Backup, which removes the backup from both the Oracle 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.



**Note**

The default `root` password is `Welcome1`. For security reasons, you must set a new password at your earliest convenience.

```
# 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: 2.4.3
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
```

## 2.12.4 Deleting Oracle Cloud InfrastructureTargets

This section describes how to remove an Oracle Cloud Infrastructure target from your Oracle Private Cloud Appliance. The related object store buckets in your Oracle Cloud Infrastructure tenancy are not removed, this operation simply removes the selected target on your PCA, 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.



#### Note

The default `root` password is *Welcome1*. For security reasons, you must set a new password at your earliest convenience.

```
# 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: 2.4.3
PCA>
```

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

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

## 2.13 Kubernetes Engine

The Kubernetes Engine for Oracle Private Cloud Appliance automates the provisioning of Oracle VM infrastructure and Kubernetes components to provide an integrated solution for Oracle Private Cloud Appliance. Oracle Private Cloud Appliance administrators define and build Kubernetes clusters and later scale them up or down depending on the Kubernetes administrator's needs.

Oracle Private Cloud Appliance easily automates deployment, scaling and management of Kubernetes application containers. To use Kubernetes Engine for Oracle Private Cloud Appliance, follow the steps below.

### 2.13.1 Kubernetes Guidelines and Limitations

This section describes the guidelines and limitations for Kubernetes on Oracle Private Cloud Appliance.

- Kubernetes clusters built with the Oracle Private Cloud Appliance service always contain three master nodes and a load balancer.

- A Kubernetes cluster requires a static, floating, IPv4 address for the load balancer (regardless of whether the virtual machines will use DHCP or static addresses for the cluster nodes).
- Only IPv4 clusters are supported.
- If a network with static addresses will be used for the VM external network, the host names used on the virtual machines must be able to be resolved.
- A maximum of 255 Kubernetes clusters can be created per Oracle Private Cloud Appliance.
- A maximum of 255 node pools can be created per Kubernetes cluster.
- An Oracle Private Cloud Appliance administrator should understand the Virtual Routing Redundancy Protocol (VRRP) and if it is already in use on the external network that will host their Kubernetes cluster(s) prior to provisioning Kubernetes clusters. For more information, see [Virtual Routing Redundancy Protocol](#).
- When deprovisioning an Oracle Private Cloud Appliance compute node running a Kubernetes cluster, follow this procedure: [Section 7.11, "Deprovisioning and Replacing a Compute Node"](#)
- A mirrored storage pool is the preferred ZFS configuration for Kubernetes on Oracle Private Cloud Appliance.
- Perform a manual backup of a Kubernetes cluster configuration after performing any changes (CRUD) on Kubernetes cluster configuration to ensure a consistent backup.
- The time it takes to start a Kubernetes cluster after defining it can vary widely depending on the size of the Kubernetes cluster and on the usage of Oracle VM management operations during the building of the cluster. If Oracle VM is not heavily used at the same time as the Kubernetes cluster start, a default Kubernetes cluster that builds 3 master nodes and 3 worker nodes takes approximately 45 minutes. For each additional (or for each worker node subtracted), adjust the build time by approximately 5 minutes, depending on Oracle VM management usage and overlapping cluster operations.

Additionally, the more compute nodes there are in an Oracle Private Cloud Appliance, the more time it will take to build a cluster due to the start and stop timing increases as Network/VLAN interfaces are created and added or removed to or from all of the nodes.

### 2.13.2 Prepare the Cluster Environment

This section describes how to prepare for a cluster environment on your Oracle Private Cloud Appliance. First, download the Kubernetes Oracle VM Virtual Appliance, then create the `k8s_private` network for Kubernetes, as shown below.

The virtual appliance templates behave much like other virtual appliances in the Oracle VM environment. The Kubernetes virtual appliances require 50 GB of space per virtual machine. Once you download the virtual appliance and add it to one or more Oracle VM repositories, it can be used to build Kubernetes clusters.

The `k8s_private` network is required to provide a way for the cluster to communicate internally. Once configured, the `k8s_private` network should require minimal management.

#### Download the Kubernetes Engine for Oracle Private Cloud Appliance

1. Download the Kubernetes Engine for Oracle Private Cloud Appliance from [Oracle Software Delivery Cloud](#) to a reachable http server. Search for "Kubernetes Engine" to locate the file.



**Tip**

To stage a simple http server, see <https://docs.python.org/2/library/simplehttpserver.html>. For example, change directory to where you downloaded the virtual appliance as issue this command:

```
python -m SimpleHTTPServer 8000

The URL in the next step will be

http://<your client IP address>:8000/<the downloaded filename>
-----
```

Enter this URL in the next step:

```
http://<your-client-IP-address>:8000/<the-downloaded-filename>
```

2. From the Oracle VM Manager **Repositories** tab, select the desired repository, then choose Virtual Appliances.
3. Click Import Virtual Appliances then:
  - Enter the URL for the virtual appliance you just downloaded.
 

The Kubernetes Oracle VM Virtual Appliance is here: (input URL)
  - Enter the hostname or IP address of the proxy server.
4. If Oracle VM changed the name of the virtual appliance (it may have appended characters), rename it back to `pca-k8s-1-0-0.ova`.
5. Repeat for each repository where you want to build Kubernetes cluster nodes.

**Create the `K8s_Private` Network**

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



**Note**

The default `root` password is `Welcome1`. For security reasons, you must set a new password at your earliest convenience.

```
# 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: 2.4.3
PCA>
```

3. Create the private network. Specify the name of the internal network to be used by the `K8s_Private` network.

```
PCA> create network K8S_Private rack_internal_network
```

4. Add the private network to each tenant groups that will be used for Kubernetes clusters.

```
PCA> add network-to-tenant-group K8S_Private tenant_group1
```

**Note**

Depending upon the number of compute nodes available in Oracle Private Cloud Appliance, the `add network-to-tenant-group` command may take 10 or more minutes. You should perform cluster creation only after the `K8S_Private` network is assigned to all compute nodes.

5. Verify the network was created.

```
PCA> list network
```

## 2.13.3 Create a Kubernetes Cluster on a DHCP Network

This section describes how to create a Kubernetes cluster definition on a DHCP network with the default 3 master nodes and 3 worker nodes. For command reference information, see [Section 4.2.14, “create kube-cluster”](#).

### Creating a Kubernetes Cluster on a DHCP Network

1. From the Oracle Private Cloud Appliance command line interface, specify a name for the cluster, a server pool, an external network, the load balancer IP address (a static IPv4 address), the storage repository, and optionally a virtual appliance name.

```
PCA> create kube-cluster cluster-1 Rack1-ServerPool vm_public_lan load_balancer_ipaddress Rack1-Repository
Kubernetes cluster configuration (cluster-1) created
Status: Success
```

**Note**

`vm_public_lan` or any external network you use for your cluster must be up and reachable to successfully create a cluster. This network must be assigned to all compute nodes in the storage pool you use, otherwise clusters will not start.

2. Verify the cluster definition was created correctly.

```
PCA> show kube-cluster cluster-1

-----
Cluster           cluster-1
Tenant_Group      Rack1_ServerPool
Tenant_Group_ID   0004fb000020000001398d8312a2bc3b
State             CONFIGURED
Sub_State         VALID
Ops_Required      None
Load_Balancer     100.80.151.119
External_Network  vm_public_vlan
External_Network_ID 1096679b1e
Repository        Rack1-Repository
Repository_ID     0004fb0000300000005398d83dd67126791
Assembly          PCA_K8s_va.ova
Assembly_ID       11af134854_PCA_K8s_OVM_OL71
Masters           3
Workers           3
-----

Status: Success
```

3. To add worker nodes to the cluster definition, specify the cluster name, and the quantity of nodes in the worker pool, or the names of the nodes in the worker pool. See [Section 4.2.49, “set kube-worker-pool”](#).

4. Start the cluster. This step builds the cluster from the cluster configuration you just created. Depending on the size of the cluster definition this process can take from 30 minutes to hours. A master node pool is defined with 3 master nodes and cannot be changed. However worker nodes may be added to the DHCP cluster definition.

```
PCA> start kube-cluster cluster-1
```

5. Follow the progress of the build using the `show kube-cluster` command.

```
PCA> show kube-cluster cluster-1
-----
Cluster          cluster-1
Tenant_Group     Rack1_ServerPool
Tenant_Group_ID  0004fb000020000001398d8312a2bc3b
State            AVAILABLE
Sub_State        None
Ops_Required     None
Load_Balancer    172.16.0.157
Vrrp_ID          236
External_Network default_external
Cluster_Network_Type dhcp
Gateway          None
Netmask          None
Name_Servers     None
Search_Domains   None
Repository       Rack2-Repository
Assembly         PCA_K8s_va.ova
Masters          3
Workers          3
Cluster_Start_Time 2020-06-14 06:11:32.765239
Cluster_Stop_Time  None
Job_ID           None
Job_State        None
Error_Code       None
Error_Message    None
-----
Status: Success
```

For more information on cluster states, see [Section 4.2.52, “start kube-cluster”](#).

6. Once the cluster is started, collect the node pool information for the cluster.

Save this information, you will use it to hand the clusters off to Kubernetes later.

```
PCA> list node-pool --filter-column=Cluster --filter=cluster-1

Cluster      Node_Pool      Tenant_Group      CPUs      Memory      Nodes
-----
cluster-1    master         Rack1_ServerPool  4         16384       3
cluster-1    worker        Rack1_ServerPool  2         8192        2

-----
2 rows displayed

Status: Success
```

7. Once the cluster is in the AVAILABLE state, consider performing a manual backup to capture the new cluster state. See [Section 4.2.8, “backup”](#).

## 2.13.4 Create a Kubernetes Cluster on a Static Network

This section describes how to create a Kubernetes cluster with 3 master nodes and 1 worker node on a static network.

## Creating a Kubernetes Cluster on a Static Network

1. From the Oracle Private Cloud Appliance command line interface, specify a name for the cluster, a server pool, an external network, the load balancer IP address, the storage repository, and optionally a virtual appliance.

```
PCA> create kube-cluster cluster-2 Rack1-ServerPool vm_public_lan load-balancer_ipaddress Rack1-Repository
Kubernetes cluster configuration (cluster-2) created
Status: Success
```

2. Set the network type to static for the cluster. Specify the cluster name, network type, netmask, and gateway. See [Section 4.2.47, “set kube-network”](#).



### Note

The network you use for your cluster must be up and reachable to successfully create a cluster. This network must be assigned to all compute nodes in the storage pool you use, otherwise clusters will not start.

```
PCA> set kube-network cluster-2 static netmask_IP gateway_IP
```

3. Set the DNS server for the cluster. Specify the cluster name, DNS name server address(es), and search domains. See [Section 4.2.44, “set kube-dns”](#).

```
PCA> set kube-dns dns_IP_1,dns_IP_2 mycompany.com
```

4. Verify the cluster definition was created correctly.

```
PCA> show kube-cluster cluster-2
-----
Cluster                Static
Tenant_Group           Rack1_ServerPool
State                  AVAILABLE
Sub_State              None
Ops_Required           None
Load_Balancer          172.16.0.220
Vrrp_ID                152
External_Network       default_external
Cluster_Network_Type   static
Gateway                172.16.0.1
Netmask                255.254.0.0
Name_Servers           144.20.190.70
Search_Domains         ie.company.com,us.voip.companys.com
Repository             Rack1-Repository
Assembly              OVM_OL7U7_x86_64_PVHVM.ova
Masters                3
Workers                3
Cluster_Start_Time     2020-07-06 23:53:17.717562
Cluster_Stop_Time      None
Job_ID                 None
Job_State              None
Error_Code             None
Error_Message          None
-----
Status: Success
```

5. To add worker nodes to the cluster definition, specify the cluster name, then list the names of the nodes you want in the worker pool. See [Section 4.2.49, “set kube-worker-pool”](#).

```
PCA> set kube-worker-pool cluster-2 worker-node-vm7 worker-node-vm8 worker-node9
```



- To add the master pool to the cluster definition, specify the cluster name, list the primary master node with its name and IP address, then list the names of the other nodes you want in the master pool. See [Section 4.2.46, “set kube-master-pool”](#).

```
PCA> set kube-master-pool demo-cluster cluster-master-0,192.168.0.10 cluster-master-1 cluster-master-2
```

- Start the cluster. This step builds the cluster from the cluster configuration you just created. Depending on the size of the cluster definition this process can take from 30 minutes to several hours.

```
PCA> start kube-cluster cluster-2
```

```
Status: Success
```

- Follow the progress of the build using the `show kube-cluster` command.

```
PCA> show kube-cluster cluster-2
```

```
<need example>
```

For more information on cluster states, see [Section 4.2.52, “start kube-cluster”](#).

- Once the cluster is started, collect the node pool information for the cluster.

Save this information, you will use it to hand the clusters off to Kubernetes later.

```
PCA> list node-pool --filter-column=Cluster --filter=cluster-2
```

Cluster	Node_Pool	Tenant_Group	CPUs	Memory	Nodes
cluster-2	master	Rack1_ServerPool	4	16384	3
cluster-2	worker	Rack1_ServerPool	2	8192	2

```
-----  
2 rows displayed
```

```
Status: Success
```

- Consider performing a manual backup to capture the new cluster state. See [Section 4.2.8, “backup”](#).

## 2.13.5 Use the Kubernetes Dashboard

This section describes how to use the Kubernetes dashboard that is deployed with your Kubernetes cluster during the `start kube-cluster` operation.

### Using the Kubernetes Dashboard

- Install `kubectl` on your local machine.

Follow the directions to [Install and Set Up kubectl](#) from [kubernetes.io](#).

- Copy the cluster configuration from the master to your local machine.

```
# scp root@<load-balancer-ip>:~/.kube/config ~/.kube/config
```

- Create the `.kube` subdirectory on your local machine.

```
# mkdir -p $HOME/.kube
```

- Set your Kubernetes configuration file location.

```
# export KUBECONFIG=~/.kube/config
```

- Confirm the nodes in the cluster are up and running.

```
# kubectl get nodes
```

6. Create default user roles for the Kubernetes dashboard, using `dashboard-rbac.yaml`.

```
# kubectl apply -f dashboard-rbac.yaml
```

For more information on the Kubernetes dashboard, see <https://docs.oracle.com/en/operating-systems/olcne/orchestration/dashboard.html>.

For more information on `kubectl`, see <https://docs.oracle.com/en/operating-systems/olcne/orchestration/kubectl-setup-master.html>.

7. Create a login token for the Kubernetes dashboard.

Follow the *Getting a Bearer Token* directions at the [Kubernetes dashboard github site](#).

8. Start the proxy on your host.

```
# kubectl proxy
```

9. Open the Kubernetes dashboard.

```
http://localhost:8001/api/v1/namespaces/kubernetes-dashboard/services/https:kubernetes-dashboard:/proxy/#/1
```

You should see your cluster in the dashboard. Now a Kubernetes administrator can manage the cluster through the dashboard just as you would any other Kubernetes cluster. For more information see [Oracle Linux Cloud Native Container Orchestration documentation](#).

If needed, you can configure internet access for worker nodes. This can ease deployment of applications that have dependencies outside of your corporate network.

## 2.13.6 Managing a Cluster

This section describes some of the common changes you might make to an existing cluster. Once you have made changes to a cluster, perform a manual backup of your Oracle Private Cloud Appliance to save the new configuration. See [Section 4.2.8, “backup”](#).

Task	Description
Stop a cluster	<pre>PCA&gt; stop kube-cluster <i>cluster-name</i></pre> <p>See <a href="#">Section 4.2.54, “stop kube-cluster”</a>.</p>
Add a node pool	<pre>PCA&gt; add node-pool <i>cluster-name</i> &lt;nodepool name&gt; &lt;cpus&gt; &lt;memory&gt; &lt;repos&gt;</pre> <p>See <a href="#">Section 4.2.6, “add node-pool”</a>.</p>
Remove a node pool	<pre>PCA&gt; remove node-pool <i>cluster-name</i> <i>nodepool-name</i></pre> <p>See <a href="#">Section 4.2.39, “remove node-pool”</a>.</p>
Add a node pool node	<pre>PCA&gt; add node-pool-node <i>cluster-name</i> <i>nodepool-name</i> <i>hostname</i></pre> <p>See <a href="#">Section 4.2.7, “add node-pool-node”</a>.</p>
Remove a node pool node	<pre>PCA&gt; remove node-pool-node <i>cluster-name</i> <i>nodepool-name</i> <i>hostname</i></pre> <p>See <a href="#">Section 4.2.40, “remove node-pool-node”</a>.</p>

Task	Description
Change the profile of the VMs that are part of the default node pool for masters or workers	<pre>PCA&gt; set kube-vm-shape <i>cluster-name</i> &lt;master   worker&gt; &lt;cpus&gt; &lt;memory&gt;</pre> <p>See <a href="#">Section 4.2.48, "set kube-vm-shape"</a>.</p>

## 2.13.7 Stop a Cluster

To stop a cluster, you must empty all nodes from the cluster node pools other than the base master and worker node pools, then delete the extra node pools once they are emptied. This section describes the order to stopping a running cluster, then deleting the configuration information afterward.

Note that the cluster configuration does not have to be deleted after stopping a cluster. The stopped cluster retains information about the master and worker node pools from when the cluster was stopped. Assuming other clusters are not built that would conflict with the addresses in the stopped the cluster, the cluster configuration could be used to start the cluster again with the contents reset to the original state.

### Stopping a Cluster and Deleting the Configuration Data

1. From the Oracle Private Cloud Appliance command line interface, remove the worker nodes.

```
PCA> remove node-pool-node MyCluster node-pool-0 hostname
```

Repeat for each worker node in the node pool, until the node pool is empty.

2. Remove the node pool.

```
PCA> remove node-pool MyCluster node-pool-0
```

Repeat for each node pool in the cluster, until the cluster is empty.

3. Stop the cluster once the non-master and non-worker node pools are removed.

```
PCA> stop kube-cluster MyCluster
```



#### Note

the `--force` option can be used on the `stop kube-cluster` command. This option attempts to stop all workers regardless of their node pool, remove the node pools (other than master and worker), and leave the cluster in a stopped state.

4. Delete the cluster

```
PCA> delete kube-cluster MyCluster
```

5. Consider performing a manual backup to capture the new cluster state. See [Section 4.2.8, "backup"](#).

## 2.13.8 Monitor Cluster Status

There are two parts to a Kubernetes cluster status, the status of the virtual machines used in the Kubernetes cluster, and Kubernetes itself.

- To monitor the virtual machines that host the Kubernetes cluster, get the list of those virtual machines using the Oracle Private Cloud Appliance command line. Once you have the list, log in to Oracle VM to look more deeply at each VM, its run state, and other relevant information.
- An Oracle Private Cloud Appliance administrator has access to the Oracle VM health, but they do not have access to the Kubernetes runtime health. To view the status of Kubernetes, the Kubernetes

administrator should use the [Section 2.13.5, “Use the Kubernetes Dashboard”](#) and various `kubectl` commands. See [Overview of kubectl](#) .

## 2.13.9 Resize Kubernetes Virtual Machine Disk Space

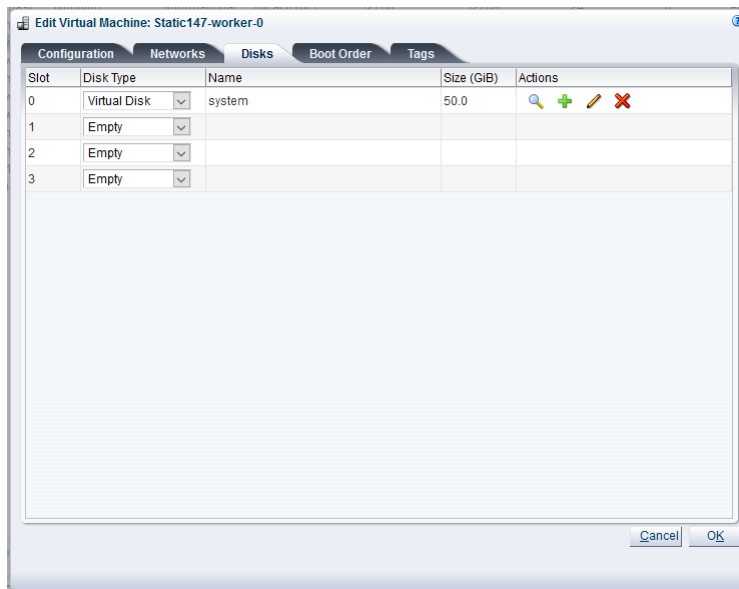
### Resizing Kubernetes Virtual Machine Disk Space

1. Log in to Oracle VM Manager.

For details, see [Section 5.2, “Logging in to the Oracle VM Manager Web UI”](#).

2. Select the Kubernetes virtual machine you wish to change, click Edit, select the Disks tab, and edit the desired disk size.

**Figure 2.11** Figure showing Oracle VM Manager resize VM disk screen.



For details, see [Edit the Virtual Machine](#)

3. Log in to the Kubernetes virtual machine you just edited and check the amount of disk space.

```
[root@dhcpl-m-1 ~]# df -kh
Filesystem Size Used Avail Use% Mounted on
devtmpfs 16G 0 16G 0% /dev
tmpfs 16G 0 16G 0% /dev/shm
tmpfs 16G 18M 16G 1% /run
tmpfs 16G 0 16G 0% /sys/fs/cgroup
/dev/xvda3 46G 5.8G 39G 14% /
/dev/xvda1 497M 90M 407M 19% /boot
```

This example shows increasing the size of `/dev/xvda3` from **46G** to **496G**.

4. Run `fdisk` to partition the disk space.

```
[root@dhcpl-m-1 ~]# fdisk /dev/xvda
Welcome to fdisk (util-linux 2.23.2).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.
Command (m for help): d
Partition number (1-3, default 3): 3
Partition 3 is deleted
```

```
Command (m for help): n
Partition type:
p primary (2 primary, 0 extended, 2 free)
e extended
Select (default p): p
Partition number (3,4, default 3):
First sector (9414656-1048575999, default 9414656):
Using default value 9414656
Last sector, +sectors or +size{K,M,G} (9414656-1048575999, default 1048575999):
Using default value 1048575999
Partition 3 of type Linux and of size 495.5 GiB is set
Command (m for help): w
The partition table has been altered!
Calling ioctl() to re-read partition table.
WARNING: Re-reading the partition table failed with error 16: Device or resource busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.
```

5. Use the `partprobe` command to make the kernel aware of the new partition.

```
[root@dhcpl-m-1 ~]# partprobe
```

6. Use the `btrfs` command to resize the partition to `max`.

```
[root@dhcpl-m-1 ~]# btrfs filesystem resize max /
Resize '/' of 'max'
```

7. Verify the size of the new partition.

```
[root@dhcpl-m-1 ~]# df -kh
Filesystem Size Used Avail Use% Mounted on
devtmpfs 16G 0 16G 0% /dev
tmpfs 16G 0 16G 0% /dev/shm
tmpfs 16G 18M 16G 1% /run
tmpfs 16G 0 16G 0% /sys/fs/cgroup
/dev/xvda3 496G 5.7G 489G 2% /
/dev/xvda1 497M 90M 407M 19% /boot
```

### 2.13.10 Maintain the Operating Systems on the Kubernetes Virtual Machines

When an Oracle Private Cloud Appliance administrator adds worker nodes or re-adds master nodes, the individual node becomes available with the Oracle Linux version, Kubernetes version, and the default settings that were a part of the Kubernetes virtual appliance.

Kubernetes administrators should update the new node(s) with:

- an updated `root` password or changes to use passwordless authorization
- update the proxies that are used by CRI-O to obtain new container images
- possibly update the Oracle Linux distribution components

Many of these operation can be achieved with efficiency using Ansible playbooks that are applied when a new node is added.

The Kubernetes virtual appliance is based on Oracle Linux 7 Update 8. Administrators can update these images once they are running, keeping in mind new nodes have the original Oracle Linux 7 Update 8 on it.

Because the Kubernetes virtual appliances use Oracle Linux, administrators can follow the instructions at <https://docs.oracle.com/en/operating-systems/oracle-linux/7/relnotes7.8/ol7-preface.html> to put selected updates on their runtime nodes (such as updating the kernel or individual packages for security updates).

Administrators should do as few updates on the runtime nodes as possible and look for Oracle guidance through [My Oracle Support](#) notes for specific suggestions for maintaining the Kubernetes virtual appliance.

---

# Chapter 3 Updating Oracle Private Cloud Appliance

## Table of Contents

3.1 Before You Start Updating .....	83
3.1.1 Warnings and Cautions .....	84
3.1.2 Backup Prevents Data Loss .....	86
3.1.3 Determine Firmware Versions .....	86
3.2 Using the Oracle Private Cloud Appliance Upgrader .....	86
3.2.1 Rebooting the Management Node Cluster .....	87
3.2.2 Installing the Oracle Private Cloud Appliance Upgrader .....	88
3.2.3 Verifying Upgrade Readiness .....	89
3.2.4 Executing a Controller Software Update .....	91
3.2.5 Upgrading the Storage Network .....	97
3.3 Upgrading the Virtualization Platform .....	99
3.4 Upgrading Component Firmware .....	102
3.4.1 Firmware Policy .....	102
3.4.2 Install the Current Firmware on All Compute Nodes .....	103
3.4.3 Upgrading the Operating Software on the Oracle ZFS Storage Appliance .....	103
3.4.4 Upgrading the Cisco Switch Firmware .....	108
3.4.5 Upgrading the NM2-36P Sun Datacenter InfiniBand Expansion Switch Firmware .....	116
3.4.6 Upgrading the Oracle Fabric Interconnect F1-15 Firmware .....	119

Due to the nature of the Oracle Private Cloud Appliance – where the term *appliance* is key – an update is a delicate and complicated procedure that deals with different hardware and software components at the same time. It is virtually impossible to automate the entire process, and more importantly it would be undesirable to take the appliance and the virtual environment it hosts out of service entirely for updating. Instead, updates can be executed in phases and scheduled for minimal downtime. The following table explains how an Oracle Private Cloud Appliance update handles different levels or areas of appliance functionality.

**Table 3.1 Functional Break-Down of an Appliance Update**

Functionality	Physical Location	Description
<b>controller software</b>	management nodes	all components required to set up the management cluster, manage and configure the appliance, and orchestrate compute node provisioning
<b>virtualization platform</b>	compute nodes	all components required to configure the compute nodes and allow virtual machines to be hosted on them
<b>component firmware</b>	infrastructure components	all low-level software components required by the various hardware components for their normal operation as part of the appliance

## 3.1 Before You Start Updating

Please read and observe the critical information in this section before you begin any procedure to update your Oracle Private Cloud Appliance.

All the software included in a given release of the Oracle Private Cloud Appliance software is tested to work together and should be treated as one package. Consequently, no appliance component should be updated individually, unless Oracle provides specific instructions to do so. All Oracle Private Cloud

Appliance software releases are downloaded as a single large `.iso` file, which includes the items listed above.

**Note**

The appliance update process must **always** be initiated from the **master management node**.

To view supported firmware versions for all releases of Oracle Private Cloud Appliance, see support note [Doc ID 1610373.1](#).

### 3.1.1 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.

**Minimum Release**

In this version of the Oracle Private Cloud Appliance Administrator's Guide, it is assumed that your system is currently **running Controller Software release 2.3.4 or 2.4.1 prior to this software update**.

If your system is currently running an earlier version, please refer to the [Update chapter](#) of the [Administrator's Guide for Release 2.3](#). Follow the appropriate procedures and make sure that your appliance configuration is valid for the Release 2.4.2 update.

**No Critical Operations**

When updating the Oracle 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.

**YUM Disabled**

On Oracle 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 only be applied through the update mechanism described in the documentation.

**Firmware Policy**

To ensure that your Oracle 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 [Section 3.4.1, "Firmware Policy"](#).

**No Backup**

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

**CA Certificate and Keystore**

If you have generated custom keys using `ovmkeytool.sh` in a previous version of the Oracle Private Cloud Appliance software, you must regenerate the keys prior to



updating the Controller Software. For instructions, refer to the support note with [Doc ID 2597439.1](#). See also [Section 7.9.1, “Creating a Keystore”](#).



### 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 Oracle 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 [Section 7.2, “Adding Proxy Settings for Oracle Private Cloud Appliance Updates”](#) for more information.



### 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 the Oracle Private Cloud Appliance Release Notes.



### 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.



### Compute Node Upgrade ONLY Through Oracle Private Cloud Appliance CLI

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 `update compute-node` command within the Oracle Private Cloud Appliance CLI.

To perform this CLI-based upgrade procedure, follow the specific instructions in [Section 3.3, “Upgrading the Virtualization Platform”](#).



### Do Not Override Oracle VM Global Update Settings

As stated in [Section 5.1, “Guidelines and Limitations”](#), at the start of [Chapter 5, \*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, and overriding this will cause the update to fail.



### 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.

### 3.1.2 Backup Prevents Data Loss

An update of the Oracle 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 Oracle Private Cloud Appliance environment, always back up the *oraInventory* Agent data to [/nfs/shared\\_storage](#) before updating the controller software. You can restore the data after the Oracle Private Cloud Appliance software update is complete.

For detailed instructions, refer to the [Agent Recovery](#) section in the [Oracle Enterprise Manager Plug-in documentation](#).

### 3.1.3 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 sp_bios
```

- ZFS Storage Appliances

```
ovcasn02r1:> maintenance system updates show
current contains current version
```

- Cisco switches

```
ovcasw21r1# show version
```

- Oracle Fabric Interconnect F1-15

```
admin@ovcasw22r1[xsigo] show system version
Build 4.0.13-XGOS - (sushao) Wed Dec 19 11:28:28 PST 2018
```

- NM2-36P Sun Datacenter InfiniBand Expansion Switch

```
[root@ilom-ovcasw19r1 ~]# version
SUN DCS 36p version: 2.2.13
```

- Oracle Switch ES1-24

```
-> cd /SYS/fs_cli
cd: Connecting to Fabric Switch CLI

ilom-ovcasw21ar1 SEFOS# show system information
...
Firmware Version           :ES1-24-1.3.1.23
```

## 3.2 Using the Oracle Private Cloud Appliance Upgrader



### 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**.



### 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 update process. A version of the Oracle Private Cloud Appliance Upgrader is included in the Controller Software `.iso` image. However, Oracle recommends that you download and install the latest stand-alone version of the Upgrader tool on the management nodes. 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 [Section 1.7, “Oracle Private Cloud Appliance Upgrader”](#).

## 3.2.1 Rebooting the Management Node Cluster

It is advised to reboot both management nodes before starting the appliance software update. 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.



#### Note

The default `root` password is `Welcome1`. For security reasons, you must set a new password at your earliest convenience.

2. Run the command `pca-check-master` on both management nodes to verify which node owns the master role.
3. Reboot the management node that is **NOT** currently the master. 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 master 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 master role.

6. Verify that both management nodes have come back online after reboot and that the master 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 update steps below.

## 3.2.2 Installing the Oracle Private Cloud Appliance Upgrader

The Oracle Private Cloud Appliance Upgrader is a separate application with its own release plan, independent of Oracle Private Cloud Appliance. 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. Log into [My Oracle Support](#) and download the latest version of the Oracle Private Cloud Appliance Upgrader.

The Upgrader can be found under patch ID 30459450, 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`.

2. Copy the downloaded `*.rpm` package to the master management node and install it.

```
[root@ovcamn05r1 ~]# pca-check-master
NODE: 192.168.4.3 MASTER: True
root@ovcamn05r1 tmp]# rpm -ivh pca_upgrader-1.2-111.el6.noarch.rpm
Preparing...##### [100%]
1:pca_upgrader##### [100%]
```



#### Caution

Always download and use the latest available version of the Oracle Private Cloud Appliance Upgrader.

3. If the version of the Oracle Private Cloud Appliance Upgrader you downloaded, is newer than the version shipped in the Controller Software ISO, then upgrade to the newer version. From the directory where the `*.rpm` package was saved, run the command `rpm -U pca_upgrader-1.2-111.el6.noarch.rpm`.

- Repeat the `*.rpm` upgrade on the second management node.

The Oracle Private Cloud Appliance Upgrader verifies the version of the Upgrader installed on the second management node. Only if the version in the ISO is newer, the package on the second management node is automatically upgraded in the process. If you downloaded a newer version, you must upgrade the package manually on both management nodes.

### 3.2.3 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 update.



#### 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 this command  
`pca_upgrader --kill`.

#### Verifying the Upgrade Readiness of the Oracle Private Cloud Appliance

- 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 instructions to correct the compute node status, refer to the support note with [Doc ID 2245197.1](#).
- Perform the required manual pre-upgrade checks. Refer to [Section 7.5, “Running Manual Pre- and Post-Upgrade Checks in Combination with Oracle Private Cloud Appliance Upgrader”](#) for instructions.
- Log in to [My Oracle Support](#) and download the required Oracle 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 update and Oracle VM upgrade.

- Make the update, a zipped ISO, available on an HTTP or FTP server that is reachable from your Oracle 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.

- Using SSH and an account with superuser privileges, log in to the **master** 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.

The default `root` password is *Welcome1*. For security reasons, you must set a new password at your earliest convenience.

- From the master 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 2.4.3 \
-l http://<path-to-iso>/ovca-2.4.3-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
-----
```

- 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 do 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 with [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 update.

### 3.2.4 Executing a Controller Software Update

During a Controller Software update, the virtualized environment does not accept any management operations. After successful upgrade of the management node cluster, upgrade the firmware on rack components, then perform the network storage upgrade, 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 update 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 [Section 3.2.3, “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 a 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 **master** 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.

The default `root` password is *Welcome1*. For security reasons, you must set a new password at your earliest convenience.



**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 master 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 2.4.3 \
-l http://<path-to-iso>/ovca-2.4.3-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...
[...]
```

```
*****
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 update on the other management node. If any 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:

- 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
Disable PCA Backups 1/16
Download ISO 2/16
Setup Yum Repo 3/16
Take OVM Backup 4/16
```



```

...

PCA Management Node upgrade of ovcamn06r1 completed after 43 minutes

Beginning PCA Post-Upgrade Checks...
OVM Manager Cache Size Check                                     1/1
PCA Post-Upgrade Checks completed after 2 minutes

-----
PCA Management Node Pre-Upgrade Checks                          Passed
-----
Validate the Image Provided                                     Passed
Internal ZFSSA Available Space Check                           Passed
[...]

-----
PCA Management Node Upgrade                                    Passed
-----
Disable PCA Backups                                           Passed
[...]
Restore PCA Backups                                           Passed
Upgrade is complete                                           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 just over 1 hour each. 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.

If you choose to copy the ISO locally, replace the location URL in the `pca_upgrader` command with `-l file:///<path-to-iso>/ovca-2.4.3-b000.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`. The example below shows several key sections in a typical log file.



### 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

[2019-09-26 12:10:13 44526] INFO (pca_upgrader:59) Starting PCA Upgrader...
[2019-09-26 12:10:13 44526] INFO (validate_rack:29) Rack Type: hardware_blue
[2019-09-26 12:10:13 44526] INFO (pca_upgrader:62) PCA Rack Type: PCA X8_BASE.
[2019-09-26 12:10:13 44526] DEBUG (util:511) the dlm_locks command output is debugfs.ocfs2 1.8.6
[?1034hdebugfs: dlm_locks -f /sys/kernel/debug/o2dlm/ovca/locking_state
Lockres: master                               Owner: 0      State: 0x0

```

## Executing a Controller Software Update

```
Last Used: 0      ASTs Reserved: 0    Inflight: 0    Migration Pending: No
Refs: 3    Locks: 1    On Lists: None
Reference Map: 1
Lock-Queue Node Level Conv Cookie          Refs AST BAST Pending-Action
Granted      0    EX    -1    0:1          2    No  No   None

debugfs: quit
[2019-09-26 12:10:13 44526] INFO (util:520) This node (192.168.4.3) is the master
[2019-09-26 12:10:14 44526] DEBUG (run_util:17) Writing 44633 to /var/run/ovca/upgrader.pid
[2019-09-26 12:10:14 44633] DEBUG (process_flow:37) Execute precheck steps for component: management
[2019-09-26 12:10:25 44633] INFO (precheck:159) [Validate the Image Provided
(Verify that the image exists and is correctly named)] Passed
[2019-09-26 12:10:25 44633] INFO (precheck_utils:471) Checking the existence of default OVMM networks.
[2019-09-26 12:10:25 44633] INFO (precheck_utils:2248) Checking for PCA services.
[2019-09-26 12:10:25 44633] INFO (precheck_utils:1970) Checking if there are multiple tenant groups.
[...]

[2019-09-26 12:10:32 44633] INFO (precheck_utils:1334) Checking hardware faults on host ovcasw16r1.
[2019-09-26 12:10:32 44633] INFO (precheck_utils:1334) Checking hardware faults on host ilom-ovcasn02r1.
[2019-09-26 12:10:32 44633] INFO (precheck_utils:1334) Checking hardware faults on host ilom-ovcamn06r1.
[2019-09-26 12:10:32 44633] INFO (precheck_utils:1334) Checking hardware faults on host ovcacn09r1.
[2019-09-26 12:10:32 44633] INFO (precheck_utils:1334) Checking hardware faults on host ovcacn08r1.
[2019-09-26 12:10:32 44633] INFO (precheck_utils:1334) Checking hardware faults on host ilom-ovcacn08r1.
[2019-09-26 12:10:32 44633] INFO (precheck:159) [Hardware Faults Check (Verifying that there are no
hardware faults on any rack component)] Passed
The check succeeded. There are no hardware faults on any rack component.
[...]

[2019-09-26 12:10:34 44633] INFO (precheck_utils:450) Checking storage...
Checking server pool...
Checking pool filesystem...
Checking rack repository Rack1-Repository...
[...]

[2019-09-26 12:10:53 44633] INFO (precheck:159) [OS Check (Checking the management nodes
and compute nodes are running the correct Oracle Linux version)] Passed
The check succeeded on the management nodes. The check succeeded on all the compute nodes.
[...]

***** PCA Management Node Pre-Upgrade Checks Summary *****
[2019-09-26 12:11:00 44633] INFO (precheck:112) [Validate the Image Provided
(Verify that the image exists and is correctly named)] Passed
[...]
[2019-09-26 12:11:00 44633] INFO (precheck:112) [OSA Disabled Check
(Checking OSA is disabled on all management nodes and compute nodes)] Passed
The check succeeded on the management nodes. The check succeeded on all the compute nodes.
[2019-09-26 12:11:00 44633] INFO (precheck:113)
***** End of Summary *****

[2019-09-26 12:11:02 44633] DEBUG (process_flow:98) Successfully completed precheck. Proceeding to upgrade.
[2019-09-26 12:11:02 44633] DEBUG (process_flow:37) Execute upgrade steps for component: management
[...]
[2019-09-26 12:25:04 44633] DEBUG (mn_upgrade_steps:237) Verifying ISO image version
[2019-09-26 12:25:04 44633] INFO (mn_upgrade_steps:243) Successfully downloaded ISO
[2019-09-26 12:25:17 44633] INFO (mn_upgrade_utils:136) /nfs/shared_storage/pca_upgrader/scripts/
1.2-89.el6/remote_yum_setup -t 2019_09_26-12.10.13 -f /nfs/shared_storage/pca_upgrader/pca_upgrade.repo
Successfully setup the yum config
[...]

[2019-09-26 12:26:44 44633] DEBUG (mn_upgrade_steps:339) Successfully completed break_ha_model
[2019-09-26 12:26:44 44633] INFO (util:184) Created lock: all_provisioning
[2019-09-26 12:26:44 44633] INFO (util:184) Created lock: database
[2019-09-26 12:26:44 44633] INFO (util:184) Created lock: cn_upgrade
[2019-09-26 12:26:44 44633] INFO (util:184) Created lock: mn_upgrade
[2019-09-26 12:26:44 44633] DEBUG (mn_upgrade_steps:148) Successfully completed place_pca_locks
[2019-09-26 12:26:45 44633] INFO (mn_upgrade_utils:461) Beginning Yum Upgrade
[...]
```

```
Setting up Upgrade Process
Resolving Dependencies
[...]
Transaction Summary
=====
Install      2 Package(s)
Upgrade     4 Package(s)

Total download size: 47 M
Downloading Packages:
[...]

[2019-09-26 12:35:40 44633] INFO (util:520) This node (192.168.4.3) is the master
[2019-09-26 12:35:40 44633] INFO (mn_upgrade_utils:706) Beginning Oracle VM upgrade on ovcamn06r1
[...]
Oracle VM upgrade script finished with success
STDOUT:
Oracle VM Manager Release 3.4.6 Installer
Oracle VM Manager Installer log file:
/var/log/ovmm/ovm-manager-3-install-2019-09-26-123633.log
Verifying upgrading prerequisites ...
[...]

Running full database backup ...
Successfully backed up database to /u01/app/oracle/mysql/dbbackup/3.4.6_preUpgradeBackup-20190926_12364
Running ovm_preUpgrade script, please be patient this may take a long time ...
Exporting weblogic embedded LDAP users
Stopping service on Linux: ovmcli ...
Stopping service on Linux: ovmm ...
Exporting core database, please be patient this may take a long time ...
[...]

Installation Summary
-----
Database configuration:
  Database type           : MySQL
  Database host name      : localhost
  Database name           : ovs
  Database listener port  : 1521
  Database user           : ovs

Weblogic Server configuration:
  Administration username : weblogic

Oracle VM Manager configuration:
  Username                : admin
  Core management port    : 54321
  UUID                    : 0004fb0000010000f1b07bf678cf43d6

Passwords:
There are no default passwords for any users. The passwords to use for Oracle VM Manager,
Database, and Oracle WebLogic Server have been set by you during this installation.
In the case of a default install, all passwords are the same.
[...]
Oracle VM Manager upgrade complete.
[...]

Successfully started Oracle VM services
Preparing to install the PCA UI
[...]
Successfully installed PCA UI
[...]

[09/26/2019 12:56:56 34239] DEBUG (complete_postupgrade_tasks:228) Copying switch config files
[09/26/2019 12:56:56 34239] INFO (complete_postupgrade_tasks:231)
[09/26/2019 12:56:56 34239] INFO (update:896) Scheduling post upgrade sync tasks...
```

```
[...]
STDOUT: Looking for [tenant group] [Rack1_ServerPool]
Looking for [storage array] [OVCA_ZFSSA_Rack1]
ID: 0004fb0000020000c500310305e98353
Server: ovcacn09r1
Server: ovcacn07r1
Server: ovcacn08r1
Finding the LUN that is used as the heartbeat device in tenant group by page83id.
page83_ID: 3600144f09c52bc4200005d8c891f0003
[...]

Successfully completed PCA management node post upgrade tasks
```

When the upgrade tasks have been completed successfully, the master management node is rebooted, and the upgraded management node assumes the master role. The new master 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/2) (Mon Sep 26 14:48:52 2019):
Management Node upgrade succeeded. The master manager will be rebooted to initiate failover in one minute.
```

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

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

[root@ovcamn06r1 ~]# head /etc/ovca-info
==== Begin build info ====
date: 2019-09-30
release: 2.4.2
build: 404
=== Begin compute node info ===
compute_ovm_server_version: 3.4.6
compute_ovm_server_build: 2.4.2-631
compute_rpms_added:
  osc-oracle-s7k-2.1.2-4.el6.noarch.rpm
  ovca-support-2.4.2-137.el6.noarch.rpm
```



### 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 master 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 master management node from where you executed the command for the first run.

```
root@ovcamn06r1 ~]# pca_upgrader -U -t management -c ovcamn05r1 -g 2.4.3 \
-l http://<path-to-iso>/ovca-2.4.3-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...
[...]

*****
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/2) (Mon Sep 26 23:18:27 2019):
Management Node upgrade succeeded. The master manager will be rebooted to initiate failover in one minu

```



### Note

After the first management node is successfully upgraded, a `fw_upgrade.LOCK` file is created to prevent the use of CLI commands during upgrade, and remains in place until the successful completion of the storage network upgrade.

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 [Inadvertant Reboot of Stand-by Management Node During Upgrade Suspends Upgrade](#).

6. Perform the required manual post-upgrade checks on management nodes and compute nodes. Refer to [Section 7.5, “Running Manual Pre- and Post-Upgrade Checks in Combination with Oracle Private Cloud Appliance Upgrader”](#) for instructions.

When the management node cluster upgrade is complete, proceed with the following tasks:

1. Firmware upgrades, as described in [Section 3.4, “Upgrading Component Firmware”](#).
2. Storage network upgrade, as described in [Section 3.2.5, “Upgrading the Storage Network”](#).
3. Compute node upgrades, as described in [Section 3.3, “Upgrading the Virtualization Platform”](#).

## 3.2.5 Upgrading the Storage Network

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

Make sure you perform the upgrades in this order before you proceed with the Storage Network upgrade:

1. Upgrade the management nodes with the controller software upgrade
2. Upgrade firmware on all components including the Cisco switches
3. Upgrade the storage network
4. Upgrade the compute nodes

Functionality is built in 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.

### 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

```

## 3.3 Upgrading the Virtualization Platform

Some releases of the Oracle Private Cloud Appliance Controller Software include a new version of Oracle VM, the virtualization platform used in Oracle Private Cloud Appliance. As part of the controller software update, the new Oracle VM Manager Release is automatically installed on both management nodes.

After the controller software update on the management nodes, Oracle VM Manager displays events indicating that the compute nodes are running outdated version of Oracle VM Server. These events are informational and do not prevent any operations, but it is recommended that you upgrade all compute nodes to the new Oracle VM Server Release at your earliest convenience.

The Oracle VM Server upgrade was intentionally decoupled from the automated controller software update process. This allows you to plan the compute node upgrades and the migration or downtime of your virtual machines in steps and outside peak hours. As a result, service interruptions for users of the Oracle VM environment can be minimized or even eliminated. By following the instructions in this section, you also make sure that previously deployed virtual machines remain fully functional when the appliance update to the new software release is complete.

During an upgrade of Oracle VM Server, no virtual machine can be running on a given compute node. VMs using resources on a shared storage repository can be migrated to other running compute nodes. If a VM uses resources local to the compute node you want to upgrade, it must be shut down, and returned to service after the Oracle VM Server upgrade.

When you install Oracle Private Cloud Appliance Controller Software Release 2.4.x, the management nodes are set up to run Oracle VM Manager 3.4.x. Compute nodes cannot be upgraded to the corresponding Oracle VM Server Release with the Oracle VM Manager web UI. You must upgrade them using the `update compute-node` command within the Oracle Private Cloud Appliance CLI.

### Upgrading a Compute Node to a Newer Oracle VM Server Release



#### Caution

Execute this procedure on each compute node *after* the software update on the management nodes has completed successfully.



#### Caution

If compute nodes are running other packages that are not part of Oracle Private Cloud Appliance, these must be uninstalled before the Oracle VM Server upgrade.

1. Make sure that the appliance software has been updated successfully to the new release.

You can verify this by logging into the master management node and entering the following command in the Oracle Private Cloud Appliance CLI:

```
# pca-admin
Welcome to PCA! Release: 2.4.3
PCA> show version

-----
Version           2.4.3
Build             000
Date              2020-08-06
-----

Status: Success
```

Leave the console and CLI connection open. You need to run the update command later in this procedure.

2. Log in to Oracle VM Manager.



For details, see [Section 5.2, “Logging in to the Oracle VM Manager Web UI”](#).

3. Migrate all running virtual machines away from the compute node you want to upgrade.

Information on migrating virtual machines is provided in the Oracle VM Manager User's Guide section entitled [Migrate or Move Virtual Machines](#).

4. Place the compute node in maintenance mode.

Information on using maintenance mode is provided in the Oracle VM Manager User's Guide section entitled [Edit Server](#).

- a. 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.

- b. Select the **Server in 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.

5. Run the Oracle VM Server update for the compute node in question.

- a. Return to the open management node console window with active CLI connection.
- b. Run the `update compute-node` command for the compute nodes you wish to update at this time. Run this command for one compute node at a time.



### Warning

Running the `update compute-node` command with multiple servers as arguments is not supported. Neither is running the command concurrently in separate terminal windows.

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

This CLI command invokes a validation mechanism, which verifies critical requirements that a compute node must meet to qualify for the Oracle VM Server 3.4.x upgrade. It also ensures that all the necessary packages are installed from the correct source location, and configured properly.

- c. Wait for the command to complete successfully. The update takes approximately 30 minutes for each compute node.

As part of the update procedure, the Oracle VM Server is restarted but remains in maintenance mode.



### Warning

If the compute node does not reboot during the update, you must restart it from within Oracle VM Manager.

6. Return to Oracle VM Manager to take the compute node out of maintenance mode.
  - a. 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.
  - b. Clear the **Server in Maintenance Mode** check box. Click OK.  
The Oracle VM Server rejoins the server pool as a fully functioning member.

7. Repeat this procedure for each compute node in your Oracle Private Cloud Appliance.

The appliance software update is now complete. Next, perform the required post-upgrade verification steps. The procedure for those additional manual verification tasks is documented in the *Post Upgrade* section of the support note with [Doc ID 2242177.1](#).

After successful completion of the post-upgrade verification steps, the Oracle Private Cloud Appliance is ready to resume all normal operations.

## 3.4 Upgrading Component Firmware

All the software components in a given Oracle 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 Oracle Private Cloud Appliance `.iso` file you downloaded from [My Oracle Support](#). When the image file is unpacked on the internal shared storage, the firmwares are located in this directory: `/nfs/shared_storage/mgmt_image/firmware/`.



### Warning

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 update. For additional information, refer to [Some Services Require an Upgrade of Hardware Management Pack](#) in the *Oracle Private Cloud Appliance Release Notes*.

If a specific or additional procedure to upgrade the firmware of an Oracle 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 the index page of the Oracle Private Cloud Appliance Documentation Library.

### 3.4.1 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 Oracle 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 *Oracle Private Cloud Appliance Release Notes* for that release. Please refer to the Release Notes for the Oracle Private Cloud Appliance Controller Software release running on your system, and open the chapter *Firmware Qualification*.

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



#### Interim Firmware Patches

Oracle periodically releases firmware patches for many products, for example to eliminate security vulnerabilities. It may occur that an important firmware patch is released for a component of Oracle 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 Oracle Private Cloud Appliance users through [My Oracle Support](#).

### 3.4.2 Install the Current Firmware on All Compute 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/`.

For firmware upgrade instructions, refer to the Administration Guide of the server series installed in your appliance rack.

### 3.4.3 Upgrading the Operating Software on the Oracle ZFS Storage Appliance

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



#### Caution

During this procedure, the Oracle 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, Oracle Private Cloud Appliance configuration changes, or Oracle VM Manager operations are taking place at the same time.



#### Warning

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 Oracle 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 the *Oracle Private Cloud Appliance Release Notes*.



**Note**

Detailed information about software upgrades can be found in the *Oracle ZFS Storage Appliance Customer Service Manual* (document ID: F13771). Refer to the section “Upgrading the Software”.

The Oracle Private Cloud Appliance internal ZFS Storage Appliance contains two clustered controllers in an active/passive configuration. You may 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 preparation instructions in the *Oracle ZFS Storage Appliance Customer Service Manual*. Refer to the section entitled “Preparing for a Software Upgrade”.
2. Log on to the master 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 Appliance running a firmware version older than 8.7.14, unzip the firmware package [p27357887\\_20131\\_Generic.zip](#) included in the Oracle 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 8.8.20. For an upgrade to version 8.7.14, substitute the file name in the commands as shown here.

- Version 8.8.20 - [ak-nas-2013.06.05.8.20-1.1.3x-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 download
ovcasn01r1:maintenance system updates download (uncommitted)> \
```

```

set url=http://192.168.4.100/shares/export/Yum/ak/ak-nas-2013.06.05.8.20-1.1.3x-nondebug.pkg
url = http://192.168.4.100/shares/export/Yum/ak/ak-nas-2013.06.05.8.20-1.1.3x-nondeb
ovcasn01r1:maintenance system updates download (uncommitted)> set user=root
user = root
ovcasn01r1:maintenance system updates download (uncommitted)> set password
Enter password:
password = *****
ovcasn01r1:maintenance system updates download (uncommitted)> commit
Transferred 157M of 484M (32.3%) ...

```

- c. Wait for the package to fully download and unpack before proceeding.
  - d. Repeat these steps for the second storage controller.
5. Check the storage cluster configuration and make sure you are logged on to the standby controller.

```

ovcasn02r1:> configuration cluster show
Properties:
state = AKCS_STRIPPED
description = Ready (waiting for failback)
peer_asn = 8a535bd2-160f-c93b-9575-d29d4c86cac5
peer_hostname = ovcasn01r1
peer_state = AKCS_OWNER
peer_description = Active (takeover completed)

```

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> 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@2013.06.05.8.20,1-1.3          2020-8-16 09:57:19         OS8.8.20                   waiting
ovcasn02r1:maintenance system updates> select ak-nas@2013.06.05.8.20,1-1.3

```

- b. Launch the upgrade process with the selected software version.

```

ovcasn02r1: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

```

- c. 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)".

```

ovcasn02r1:> configuration cluster show
Properties:
state = AKCS_STRIPPED
description = Ready (waiting for failback)
peer_asn = 8a535bd2-160f-c93b-9575-d29d4c86cac5
peer_hostname = ovcasn01r1
peer_state = AKCS_OWNER
peer_description = Active (takeover completed)

```

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



**Caution**

Do not skip this step. Executing the storage controller operating software upgrade while the Oracle 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@2013.06.05.8.20,1-1.3          2020-8-16 09:57:19   OS8.8.20            waiting

ovcasn01r1:maintenance system updates> select ak-nas@2013.06.05.8.20,1-1.3
```

- 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
chassis-000	1906NMQ803	ok	Oracle	Oracle Storage DE3-24C	1906NMQ803	7200
disk-000	HDD 0	ok	WDC	W7214A520ORA014T	001851N3VKLT 9JG3VKLT	7200
disk-001	HDD 1	ok	WDC	W7214A520ORA014T	001851N5K85T 9JG5K85T	7200
disk-002	HDD 2	ok	WDC	W7214A520ORA014T	001851N5MPXT 9JG5MPXT	7200
disk-003	HDD 3	ok	WDC	W7214A520ORA014T	001851N5L08T 9JG5L08T	7200
disk-004	HDD 4	ok	WDC	W7214A520ORA014T	001851N42KNT 9JG42KNT	7200

```
[...]
```

10. Initiate an Oracle 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.

- Log on to the master management node using SSH and an account with superuser privileges.
- Reboot the master management node.

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

- 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 master 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-2013.06.05.8.20-1.1.3x-nondebug.pkg OS8.8.20_Readme.html
# rm ak-nas-2013.06.05.8.20-1.2.20.4392.1x-nondebug.pkg OS8.8.20_Readme.html
rm: remove regular file `ak-nas-2013.06.05.8.20-1.1.3x-nondebug.pkg'? yes
rm: remove regular file `OS8.8.20_Readme.html'? yes
# cd ..
# rmdir ak
```

### 3.4.4 Upgrading the Cisco Switch Firmware

The instructions in this section are specific for a component firmware upgrade as part 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.



#### Note

Cisco switches are part of systems with an Ethernet-based network architecture.



#### Caution

When upgrading to Controller Software version 2.4.3, 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 **all** the upgrade operations have been completed, otherwise you could lose access to the storage network. See [Loading Incompatible Spine Switch Configuration Causes Storage Network Outage](#) 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 master 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 update, the Oracle Private Cloud Appliance Upgrader copies the file to this location:

```
/nfs/shared_storage/mgmt_image/firmware/ethernet/Cisco/nxos.7.0.3.I7.8.bin
```

3. Log on as admin to the switch you wish to upgrade.

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

Please upgrade the switches, one at a time, in this order:

- a. Leaf Cisco Nexus 9336C-FX2 Switches: ovcasw15r1, ovcasw16r1
  - b. Spine Cisco Nexus 9336C-FX2 Switches: ovcasw22r1, ovcasw23r1
  - c. Management Cisco Nexus 9348GC-FXP Switch: ovcasw21r1
4. Copy the Cisco NX-OS software file to the bootflash location on the switch.

The copy command for the management switch ovcasw21r1 is slightly different. Select the appropriate option.

- Leaf and Spine switches:

```
ovcasw15r1# copy scp://root@192.168.4.216//nfs/shared_storage/mgmt_image/firmware/ethernet \
/Cisco/nxos.7.0.3.I7.8.bin bootflash:nxos.7.0.3.I7.8.bin vrf management
root@192.168.4.216's password:
nxos.7.0.3.I7.8.bin 100% 937MB 16.2MB/s 00:58
```



```
Copy complete, now saving to disk (please wait)...
Copy complete.
```

- Management switch:

```
ovcasw21r1# copy scp://root@192.168.4.216//nfs/shared_storage/mgmt_image/firmware/ethernet \
/Cisco/nxos.7.0.3.I7.8.bin bootflash:nxos.7.0.3.I7.8.bin vrf default
root@192.168.4.216's password:
nxos.7.0.3.I7.8.bin                               100%  937MB  16.2MB/s   00:58
Copy complete, now saving to disk (please wait)...
Copy complete.
```

### 5. Verify the impact of the software upgrade.

```
ovcasw15r1# show install all impact nxos bootflash:nxos.7.0.3.I7.8.bin
Installer will perform impact only check. Please wait.

Verifying image bootflash:/nxos.7.0.3.I7.8.bin for boot variable "nxos".
[#####] 100% -- SUCCESS

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

Preparing "nxos" version info using image bootflash:/nxos.7.0.3.I7.8.bin.
[#####] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.7.0.3.I7.8.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 following table:
Module  Image  Running-Version(pri:alt)  New-Version  Upg-Required
-----  -----  -
      1    nxos          7.0(3)I7(7)             7.0(3)I7(8)             yes
      1    bios  v05.38(06/12/2019):v05.33(09/08/2018)  v05.38(06/12/2019)             no
```

### 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.
```

### 7. 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.I7.8.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.7.0.3.I7.8.bin for boot variable "nxos".
[#####] 100% -- SUCCESS

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

Preparing "nxos" version info using image bootflash:/nxos.7.0.3.I7.8.bin.
```

```
[#####] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.7.0.3.I7.8.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 following table:
Module  Image                Running-Version(pri:alt)  New-Version  Upg-Required
-----  -
      1      nxos                7.0(3)I7(7)              7.0(3)I7(8)  yes
      1      bios      v05.38(06/12/2019):v05.33(09/08/2018)  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.
```

### 8. 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.I7.8.bin for boot variable "nxos".
-- SUCCESS

Verifying image type.
-- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.7.0.3.I7.8.bin.
-- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.7.0.3.I7.8.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 following table:
Module      Image              Running-Version(pri:alt)          New-Version  Upg-Required
-----
1          nxos              7.0(3)I7(7)                      7.0(3)I7(8)          yes
1          bios          v05.38(06/12/2019):v05.33(09/08/2018)  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.

```

9. 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(8)
  BIOS compile time: 06/12/2019
  NXOS image file is: bootflash:///nxos.7.0.3.I7.8.bin
  NXOS compile time: 3/3/2020 20:00:00 [03/04/200 04:49:49]
[...]

ovcasw15r1#

```

10. 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
    
```

11. Log out of the switch. The firmware has been upgraded successfully.
12. Proceed to the next Cisco switch in the appliance. Upgrade the switches, one at a time, in this order:
  - a. Leaf Cisco Nexus 9336C-FX2 Switches: ovcasw15r1, ovcasw16r1
  - b. Spine Cisco Nexus 9336C-FX2 Switches: ovcasw22r1, ovcasw23r1
  - c. Management Cisco Nexus 9348GC-FXP Switch: ovcasw21r1



### Note

During the upgrade of switch software on the management switch, there will be network disruption between compute nodes, management nodes, the storage node, and Leaf and Spine switch management connections. This occurs due to the reboot of the switch as part of the upgrade process.



### Caution

Once an upgrade to Controller Software release 2.4.3 is complete on the spine switches, do not attempt to reload a spine switch backup **from a prior software release**. This could cause the management nodes to lose access to the storage network.

## 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.

1. Log on to the master 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 update, the Oracle Private Cloud Appliance Upgrader copies the file to this location:

```
/nfs/shared_storage/mgmt_image/firmware/ethernet/Cisco/n9000-epld.7.0.3.I7.8.img
```

3. Log on as admin to the switch you wish to upgrade.

```

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

Please upgrade the switches, one at a time, in this order:

- a. Leaf Cisco Nexus 9336C-FX2 Switches: ovcasw15r1, ovcasw16r1
- b. Spine Cisco Nexus 9336C-FX2 Switches: ovcasw22r1, ovcasw23r1

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

4. Copy the firmware file to the bootflash location on the switch.

The copy command for the management switch ovcasw21r1 is slightly different. Select the appropriate option.

- Leaf and Spine switches:

```
ovcasw15r1# copy scp://root@192.168.4.216//nfs/shared_storage/mgmt_image/firmware/ethernet \
/Cisco/n9000-epld.7.0.3.I7.8.img bootflash:n9000-epld.7.0.3.I7.8.img vrf management
root@192.168.4.216's password:
n9000-epld.7.0.3.I7.8.img                               100% 142MB 15.8MB/s 00:09
Copy complete, now saving to disk (please wait)...
Copy complete.
```

- Management switch:

```
ovcasw21r1# copy scp://root@192.168.4.216//nfs/shared_storage/mgmt_image/firmware/ethernet \
/Cisco/n9000-epld.7.0.3.I7.8.img bootflash:n9000-epld.7.0.3.I7.8.img vrf default
root@192.168.4.216's password:
n9000-epld.7.0.3.I7.8.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.I7.8.img

Retrieving EPLD versions... Please wait.
Images will be upgraded according to 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 the primary and golden regions of the FPGA, however only one upgrade is allowed per reload to avoid programming errors. The next steps describe upgrading 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.

```
ovcasw15r1# install epld bootflash:n9000-epld.7.0.3.I7.8.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 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...

```



### Caution

Do not interrupt, power cycle, or reload the switch during the upgrade.

- 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.

- 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.

```

ovcasw15r1# install epld bootflash:n9000-epld.7.0.3.I7.8.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...
    
```



### Caution

Do not interrupt, power cycle, or reload the switch during the upgrade.

- 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
    
```

- 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
    
```

- Log out of the switch. The firmware has been upgraded successfully.

13. Proceed to the next Cisco switch in the appliance. Upgrade the switches, one at a time, in this order:
  - a. Leaf Cisco Nexus 9336C-FX2 Switches: ovcasw15r1, ovcasw16r1
  - b. Spine Cisco Nexus 9336C-FX2 Switches: ovcasw22r1, ovcasw23r1
  - c. Management Cisco Nexus 9348GC-FXP Switch: ovcasw21r1



**Note**

During the upgrade of switch software on the management switch, there will be network disruption between compute nodes, management nodes, the storage node, and Leaf and Spine switch management connections. This occurs due to the reboot of the switch as part of the upgrade process.

### 3.4.5 Upgrading the NM2-36P Sun Datacenter InfiniBand Expansion Switch Firmware

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



**Note**

InfiniBand switches are part of systems with an InfiniBand-based network architecture.



**Warning**

For firmware upgrades to version 2.2.8 or newer, an intermediate upgrade to unsigned version 2.2.7-2 is required. Version 2.2.7-2 can then be upgraded to the intended newer version. For additional information, refer to [NM2-36P Sun Datacenter InfiniBand Expansion Switch Firmware Upgrade 2.2.9-3 Requires A Two-Phased Procedure](#) in the *Oracle Private Cloud Appliance Release Notes*.



**Note**

Detailed information about firmware upgrades can be found in the *Sun Datacenter InfiniBand Switch 36 Product Notes for Firmware Version 2.2* (document ID: E76431). Refer to the section “Upgrading the Switch Firmware”.



**Caution**

It is recommended that you back up the current configuration of the NM2-36P Sun Datacenter InfiniBand Expansion Switches prior to performing a firmware upgrade.

Backup and restore instructions are provided in the maintenance and configuration management sections of the *Oracle ILOM Administration Guide* that corresponds with the current ILOM version used in the switch. For example:

- Oracle ILOM 3.0: [https://docs.oracle.com/cd/E36265\\_01/html/E36266/ceiidgfj.html#scrolltoc](https://docs.oracle.com/cd/E36265_01/html/E36266/ceiidgfj.html#scrolltoc)
- Oracle ILOM 3.2: [https://docs.oracle.com/cd/E37444\\_01/html/E37446/z400371a1482122.html#scrolltoc](https://docs.oracle.com/cd/E37444_01/html/E37446/z400371a1482122.html#scrolltoc)



## Upgrading the InfiniBand Switch Firmware

1. Log on to the master management node using SSH and an account with superuser privileges.
2. Unzip the firmware package included in the Oracle Private Cloud Appliance software image.

```
[root@ovcamn05r1 ~]# mkdir /nfs/shared_storage/yum/nm2
[root@ovcamn05r1 ~]# cd /nfs/shared_storage/yum/nm2
[root@ovcamn05r1 nm2]# unzip /nfs/shared_storage/mgmt_image/firmware/IB_gateway/NM2-36P/p22173626_227_G
Archive:  /nfs/shared_storage/mgmt_image/firmware/IB_gateway/NM2-36P/p22173626_227_Generic.zip
  inflating: license.txt
  inflating: readme_SUN_DCS_36p_2.1.8-1.txt
    creating: SUN_DCS_36p_2.1.8-1/
  inflating: SUN_DCS_36p_2.1.8-1/pkey_filter.pl
    creating: SUN_DCS_36p_2.1.8-1/SUN_DCS_36p/
  inflating: SUN_DCS_36p_2.1.8-1/SUN_DCS_36p/SUN-ILOM-CONTROL-MIB.mib
  inflating: SUN_DCS_36p_2.1.8-1/SUN_DCS_36p/SUN-FABRIC-MIB.mib
  inflating: SUN_DCS_36p_2.1.8-1/SUN_DCS_36p/sundcs_36p_repository_2.1.8_1.pkg
  inflating: SUN_DCS_36p_2.1.8-1/SUN_DCS_36p/SUN-HW-TRAP-MIB.mib
  inflating: SUN_DCS_36p_2.1.8-1/SUN_DCS_36p/SUN-DCS-IB-MIB.txt
  inflating: SUN_DCS_36p_2.1.8-1/SUN_DCS_36p/SUN-PLATFORM-MIB.mib
  inflating: SUN_DCS_36p_2.1.8-1/SUN_DCS_36p/ENTITY-MIB.mib
  inflating: SUN_DCS_36p_2.1.8-1/SUN_DCS_36p_2.1.8-1_metadata.xml
  inflating: SUN_DCS_36p_2.1.8-1/README_pkey_filter
  inflating: SUN_DCS_36p_2.1.8-1_THIRDPARTYLICENSE.pdf
```

3. Log on to one of the InfiniBand switches as root.

```
root@ovcamn05r1 ~]# ssh root@192.168.4.202
root@192.168.4.202's password:
You are now logged in to the root shell.
It is recommended to use ILOM shell instead of root shell.
All usage should be restricted to documented commands and documented config files.
To view the list of documented commands, use "help" at linux prompt.
[root@ilom-ovcasw19r1 ~]#
```

4. Check the master configuration and the state of the SubnetManager.

```
[root@ilom-ovcasw19r1 ~]# getmaster
Local SM not enabled
Last change in Master SubnetManager status detected at: Thu Mar 22 14:29:18 UTC 2018
Master SubnetManager on sm lid 6 sm guid 0x13970201001ba4 : MT25408 ConnectX Mellanox Technologies
Master SubnetManager Activity Count: 348521 Priority: 0
```



### Warning

The command output must read Local SM not enabled. If this is not the case, abort this procedure and contact Oracle Support.

5. List the details of the current firmware version.

```
[root@ilom-ovcasw19r1 ~]# version
SUN DCS 36p version: 1.3.3-2
Build time: Feb 19 2013 13:29:01
SP board info:
Manufacturing Date: 2012.06.23
Serial Number: "NCDBJ1073"
Hardware Revision: 0x0007
Firmware Revision: 0x0000
BIOS version: SUN0R100
BIOS date: 06/22/2010
```

6. Connect to the ILOM and start the firmware upgrade procedure. Press "Y" when prompted to load the file.

```
[root@ilom-ovcasw19r1 ~]# spsh
Oracle(R) Integrated Lights Out Manager
Version ILOM 3.0 r47111
Copyright (c) 2012, Oracle and/or its affiliates. All rights reserved.

-> load -source http://192.168.4.100/shares/export/Yum/nm2/ \
SUN_DCS_36p_2.1.8-1/SUN_DCS_36p/sundcs_36p_repository_2.1.8_1.pkg

Downloading firmware image. This will take a few minutes.
Are you sure you want to load the specified file (y/n)

Setting up environment for firmware upgrade. This will take few minutes.
Starting SUN DCS 36p FW update
=====
Performing operation: I4 A
=====
I4 fw upgrade from 7.3.0(INI:4) to 7.4.1010(INI:4):
Upgrade started...
Upgrade completed.
INFO: I4 fw upgrade from 7.3.0(INI:4) to 7.4.1010(INI:4) succeeded
=====
Summary of Firmware update
=====
I4 status                : FW UPDATE - SUCCESS
I4 update succeeded on   : A
I4 already up-to-date on : none
I4 update failed on     : none
=====
Performing operation: SUN DCS 36p firmware update
=====
SUN DCS 36p upgrade from 1.3.3-2 to 2.1.8-1:
Upgrade started...
Upgrade completed.
INFO: SUN DCS 36p upgrade from 1.3.3-2 to 2.1.8-1 succeeded
Firmware update is complete.
ILOM will be restarted and will take 2 minutes to come up.
You will need to reconnect to Integrated Lights Out Manager.
```

7. Reconnect to the InfiniBand switch to verify that the new firmware is running and to confirm that the SubnetManager remains disabled.

```
root@ovcamn05r1 ~]# ssh root@192.168.4.202
root@192.168.4.202's password:
[root@ilom-ovcasw19r1 ~]# version
SUN DCS 36p version: 2.1.8-1
Build time: Sep 18 2015 10:26:47
SP board info:
Manufacturing Date: 2013.06.15
Serial Number: "NCDBJ1073"
Hardware Revision: 0x0007
Firmware Revision: 0x0000
BIOS version: SUN0R100
BIOS date: 06/22/2010

[root@ilom-ovcasw19r1 ~]# getmaster
Local SM not enabled
```



### Warning

The command output must read Local SM not enabled. If this is not the case, abort this procedure and contact Oracle Support.

8. When the first InfiniBand switch has completed the upgrade successfully and has come back online, connect to the other InfiniBand switch, with IP address 192.168.4.203, and execute the same procedure.
9. When both InfiniBand switches have been upgraded, remove the shared storage directory you created to make the unzipped package available.

```
root@ovcamn05r1 ~]# cd /nfs/shared_storage/yum/
root@ovcamn05r1 yum]# ls -al
total 323
drwxr-xr-x  8 root root   8 Mar 26 07:57 .
drwxrwxrwx 31 root root  31 Mar 13 13:38 ..
drwxr-xr-x  2 root root   5 Mar 13 12:04 backup_COMPUTE
drwxr-xr-x  2 root root   5 Mar 13 13:19 current_COMPUTE
drwxr-xr-x  3 root root   6 Mar 26 07:58 nm2
drwxr-xr-x  3 root root 587 Mar 13 12:04 OVM_3.4.4_1735_server
drwxr-xr-x  3 root root  18 Mar 13 12:03 OVM_3.4.4_1735_transition
drwxr-xr-x  4 root root   9 Mar 13 12:03 OVM_3.4.4_1735_update
root@ovcamn05r1 yum]# rm -rf nm2/
```

### 3.4.6 Upgrading the Oracle Fabric Interconnect F1-15 Firmware

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



#### Note

Fabric Interconnects are part of systems with an InfiniBand-based network architecture.



#### Note

Detailed information about firmware upgrades can be found in the *XgOS User's Guide* (document ID: E53170). Refer to the section "System Image Upgrades".



#### Caution

It is recommended that you back up the current configuration of the Fabric Interconnects prior to performing a firmware upgrade. Store the backup configuration on another server and add a time stamp to the file name for future reference.

For detailed information, refer to the section "Saving and Restoring Your Configuration" in the *XgOS User's Guide* (document ID: E53170).

#### Upgrading the Fabric Interconnect Firmware

1. Log on to the master management node using SSH and an account with superuser privileges.
2. Copy the firmware package from the Oracle Private Cloud Appliance software image to the Yum repository share.

```
root@ovcamn05r1 ~]# cp /nfs/shared_storage/mgmt_image/firmware/IB_gateway/ \
OFI/xsigo-4.0.12-XGOS.xpf /nfs/shared_storage/yum/
```

3. Log on to one of the Fabric Interconnects as admin.

```
root@ovcamn05r1 ~]# ssh admin@192.168.4.205
Password:
Last login: Thu Oct 15 10:57:23 2015 from 192.168.4.4
```

```

Welcome to XgOS
Copyright (c) 2007-2012 Xsigo Systems, Inc. All rights reserved.
Enter "help" for information on available commands.
Enter the command "show system copyright" for licensing information
admin@ovcasw22r1[xsigo]

```

4. List the details of the current firmware version.

```

admin@ovcasw22r1[xsigo] show system version
Build 3.9.4-XGOS - (buildsys) Thu Mar 19 03:25:26 UTC 2015
admin@ovcasw22r1[xsigo]

```

5. Check the master configuration and the state of the SubnetManager. Optionally run the additional diagnostics command for more detailed information.

```

admin@ovcasw22r1[xsigo] show diagnostics sm-info
- SM is running on          ovcasw22r1
- SM Lid                    39
- SM Guid                   0x139702010017b4
- SM key                     0x0
- SM priority                0
- SM State                   MASTER

```

```

admin@ovcasw22r1[xsigo] show diagnostics opensm-param

```

```

OpenSM $ Current log level is 0x83
OpenSM $ Current sm-priority is 0
OpenSM $
OpenSM Version       : OpenSM 3.3.5
SM State             : Master
SM Priority           : 0
SA State              : Ready
Routing Engine       : minhop
Loaded event plugins : <none>

PerfMgr state/sweep state : Disabled/Sleeping

```

MAD stats

```

-----
QP0 MADs outstanding      : 0
QP0 MADs outstanding (on wire) : 0
QP0 MADs rcvd             : 6323844
QP0 MADs sent             : 6323676
QP0 unicasts sent        : 2809116
QP0 unknown MADs rcvd    : 0
SA MADs outstanding      : 0
SA MADs rcvd             : 120021107
SA MADs sent             : 120024422
SA unknown MADs rcvd    : 0
SA MADs ignored          : 0

```

Subnet flags

```

-----
Sweeping enabled          : 1
Sweep interval (seconds) : 10
Ignore existing lfts     : 0
Subnet Init errors       : 0
In sweep hop 0           : 0
First time master sweep  : 0
Coming out of standby    : 0

```

Known SMs

```

-----
Port GUID          SM State  Priority
-----
0x139702010017b4  Master   0          SELF
0x139702010017c0  Standby  0

```

```
OpenSM $
admin@ovcasw22r1[xsigo]
```

6. Start the system upgrade procedure.

```
admin@ovcasw22r1[xsigo] system upgrade
http://192.168.4.100/shares/export/Yum/xsigo-4.0.12-XGOS.xpf forcebaseos
Copying...
#####
[100%]
You have begun to upgrade the system software.
Please be aware that this will cause an I/O service interruption
and the system may be rebooted.
The following software will be installed:
1. XgOS Operating System software including SCP Base OS
2. XgOS Front-panel software
3. XgOS Common Chassis Management software on IOC
4. XgOS VNIC Manager and Agent software
5. XgOS VN10G and VN10x1G Manager and Agent software
6. XgOS VHBA and VHBA-2 Manager and Agent software
7. XgOS VN10G and VN10x1G Manager and Agent software with Eth/IB Interfaces
8. XgOS VN4x10G and VN2x10G Manager and Agent software with Eth/IB Interfaces
9. XgOS VHBA-3 Manager and Agent software
10. XgOS VHBA 2x 8G FC Manager and Agent software
Are you sure you want to update the software (y/n)? y
Running verify scripts...
Running preunpack scripts...
Installing...
#####
[100%]
Verifying...
#####
[100%]
Running preinstall scripts...
Installing Base OS - please wait...
LABEL=/dev/uba /mnt/usb vfat rw 0 0
Rootfs installation successful
The installer has determined that a reboot of the Base OS is required (HCA driver changed)
The installer has determined that a cold restart of the Director is necessary
Installing package...
Running postinstall scripts...
Installation successful. Please stand by for CLI restart.
admin@iowa[xsigo] Rebooting OS. Please log in again in a couple of minutes...

*****
Xsigo system is being shut down now
*****
Connection to 192.168.4.204 closed.
```

After reboot, it takes approximately 10 minutes before you can log back in. The upgrade resets the admin user's password to the default "admin". It may take several attempts, but login with the default password eventually succeeds.

7. Reconnect to the Fabric Interconnect to change the admin and root passwords back to the setting from before the firmware upgrade.



**Note**

When you log back in after the firmware upgrade, you may encounter messages similar to this example:

```
Message from syslogd@ovcasw22r1 at Fri Jun 22 09:49:33 2018 ...
ovcasw22r1 systemcontroller[2713]: [EMERG] ims::IMSService [ims::failedloginattempt]
user admin has tried to log on for 5 times in a row without success !!
```

These messages indicate failed login attempts from other Oracle Private Cloud Appliance components. They disappear after you set the passwords back to their original values.

Modify the passwords for users root and admin as follows:

```
admin@ovcasw22r1[xsigo] set system root-password
Administrator's password: admin
New password: myOriginalRootPassword
New password again: myOriginalRootPassword

admin@ovcasw22r1[xsigo] set user admin -password
New password: myOriginalAdminPassword
New password again: myOriginalAdminPassword
```

8. Reconnect to the Fabric Interconnect to verify that the new firmware is running and to confirm that all vNICs and vHBAs are in up/up state.

```
root@ovcamn05r1 ~]# ssh admin@192.168.4.205
admin@ovcasw22r1[xsigo] show system version
Build 4.0.12-XGOS - (buildsys) Fri Jun 22 04:42:35 UTC 2018

admin@ovcasw22r1[xsigo] show diagnostics sm-info
- SM is running on          ovcasw22r1
- SM Lid                    39
- SM Guid                   0x139702010017b4
- SM key                    0x0
- SM priority               0
- SM State                  MASTER

admin@ovcasw22r1[xsigo] show vnic

name                state      mac-addr          ipaddr           if              if-state
-----
eth4.ovcacn08r1    up/up     00:13:97:59:90:11  0.0.0.0/32      mgmt_pvi(64539)  up
eth4.ovcacn09r1    up/up     00:13:97:59:90:0D  0.0.0.0/32      mgmt_pvi(64539)  up
eth4.ovcacn10r1    up/up     00:13:97:59:90:09  0.0.0.0/32      mgmt_pvi(64539)  up
eth4.ovcacn11r1    up/up     00:13:97:59:90:1D  0.0.0.0/32      mgmt_pvi(64539)  up
eth4.ovcacn12r1    up/up     00:13:97:59:90:19  0.0.0.0/32      mgmt_pvi(64539)  up
[...]
eth7.ovcacn29r1    up/up     00:13:97:59:90:28  0.0.0.0/32      5/1             up
eth7.ovcamn05r1    up/up     00:13:97:59:90:04  0.0.0.0/32      4/1             up
eth7.ovcamn06r1    up/up     00:13:97:59:90:08  0.0.0.0/32      5/1             up
40 records displayed

admin@ovcasw22r1[xsigo] show vhba

name                state      fabric-state      if      if-state      wwnn
-----
vhba03.ovcacn07r1    up/up     down(Down)        12/1    down          50:01:39:71:00:58:B1:0A
vhba03.ovcacn08r1    up/up     down(Down)        3/1     down          50:01:39:71:00:58:B1:08
vhba03.ovcacn09r1    up/up     down(Down)        12/1    down          50:01:39:71:00:58:B1:06
vhba03.ovcacn10r1    up/up     down(Down)        3/1     down          50:01:39:71:00:58:B1:04
[...]
vhba04.ovcacn29r1    up/up     down(Down)        12/2    down          50:01:39:71:00:58:B1:13
vhba04.ovcamn05r1    up/up     down(Down)        3/2     down          50:01:39:71:00:58:B1:01
vhba04.ovcamn06r1    up/up     down(Down)        12/2    down          50:01:39:71:00:58:B1:03
20 records displayed
```

9. When the first Fabric Interconnect has completed the upgrade successfully and has come back online, connect to the other Fabric Interconnect, with IP address 192.168.4.204, and execute the same procedure.

---

# Chapter 4 The Oracle Private Cloud Appliance Command Line Interface (CLI)

## Table of Contents

4.1 CLI Usage .....	124
4.1.1 Interactive Mode .....	125
4.1.2 Single-command Mode .....	126
4.1.3 Controlling CLI Output .....	127
4.1.4 Internal CLI Help .....	129
4.2 CLI Commands .....	130
4.2.1 add compute-node .....	130
4.2.2 add initiator .....	131
4.2.3 add network .....	132
4.2.4 add network-to-tenant-group .....	133
4.2.5 add nfs-exception .....	134
4.2.6 add node-pool .....	134
4.2.7 add node-pool-node .....	135
4.2.8 backup .....	137
4.2.9 configure vhbases .....	138
4.2.10 create iscsi-storage .....	139
4.2.11 create lock .....	140
4.2.12 create network .....	141
4.2.13 create nfs-storage .....	143
4.2.14 create kube-cluster .....	144
4.2.15 create oci-backup .....	145
4.2.16 create oci-target .....	145
4.2.17 create tenant-group .....	146
4.2.18 create uplink-port-group .....	147
4.2.19 delete config-error .....	148
4.2.20 delete iscsi-storage .....	149
4.2.21 delete kube-cluster .....	150
4.2.22 delete lock .....	151
4.2.23 delete network .....	152
4.2.24 delete nfs-storage .....	153
4.2.25 delete oci-backup .....	154
4.2.26 delete oci-target .....	155
4.2.27 delete task .....	156
4.2.28 delete tenant-group .....	157
4.2.29 delete uplink-port-group .....	158
4.2.30 deprovision compute-node .....	159
4.2.31 diagnose .....	160
4.2.32 get log .....	164
4.2.33 list .....	164
4.2.34 remove compute-node .....	171
4.2.35 remove initiator .....	172
4.2.36 remove network .....	173
4.2.37 remove network-from-tenant-group .....	174
4.2.38 remove nfs exceptions .....	175
4.2.39 remove node-pool .....	175
4.2.40 remove node-pool-node .....	176

4.2.41 reprovision .....	177
4.2.42 rerun .....	178
4.2.43 set system-property .....	179
4.2.44 set kube-dns .....	182
4.2.45 set kube-load-balancer .....	182
4.2.46 set kube-master-pool .....	183
4.2.47 set kube-network .....	183
4.2.48 set kube-vm-shape .....	184
4.2.49 set kube-worker-pool .....	185
4.2.50 show .....	186
4.2.51 start .....	191
4.2.52 start kube-cluster .....	192
4.2.53 stop .....	193
4.2.54 stop kube-cluster .....	195
4.2.55 update appliance .....	195
4.2.56 update password .....	196
4.2.57 update compute-node .....	198

All Oracle 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 documentation available at <https://docs.oracle.com/en/virtualization/oracle-vm/3.4/cli/index.html>.

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.

## 4.1 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 [Section 4.1.1, “Interactive Mode”](#)) or in single-command mode (see [Section 4.1.2, “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 [Section 4.1.3, “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 [Section 4.1.4, “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 [Section 4.1.1.1, “Tab Completion”](#) for more information on this.

## 4.1.1 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.

### 4.1.1.1 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.

#### 4.1.1.2 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
```

#### 4.1.2 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 [Section 4.1.3.1, "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
```

#

## 4.1.3 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.

### 4.1.3.1 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.

### 4.1.3.2 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 [Section 4.1.1.1, "Tab Completion"](#) for more information.

### 4.1.3.3 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 [Section 4.1.1.1, "Tab Completion"](#) for more information.

## 4.1.4 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'].
```

## 4.2 CLI Commands

This section describes all of the documented commands available via the CLI.

Note that there are slight differences in the CLI commands available on Ethernet-based systems and InfiniBand-based systems. If you issue a command that is not available on your specific architecture, the command fails.

### 4.2.1 add compute-node

Adds a compute node to an existing tenant group. To create a new tenant group, see [Section 4.2.17, “create tenant-group”](#).

#### Syntax

```
add compute-node node tenant-group-name [ --json ] [ --less ] [ --more ] [ --
tee=OUTPUTFILENAME ]
```

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
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux

Option	Description
	command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	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 ovcaen09r1 myTenantGroup
Status: Success
```

## 4.2.2 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 [ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```

where `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 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
<code>initiator IQN</code>	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.
<code>LUN name</code>	Specify the LUN you want to make available using an initiator.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.

Option	Description
<code>--tee=OUTPUTFILENAME</code>	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.company.com myLUN
Status: Success
```

## 4.2.3 add network

Connects a server node to an existing network. To create a new custom network, see [Section 4.2.12, “create network”](#).

### Syntax

```
add network network-name node [ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```

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
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	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
```



## 4.2.4 add network-to-tenant-group

Associates a custom network with an existing tenant group. To create a new tenant group, see [Section 4.2.17, “create tenant-group”](#). To create a new custom network, see [Section 4.2.12, “create network”](#).

### Syntax

```
add network-to-tenant-group network-name tenant-group-name [ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```

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
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	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
```

## 4.2.5 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 expectations to particular groups of users.

### Syntax

```
add nfs-exception nfs-share-name network or IP address [ --json ][ --less ][ --more ][
--tee=OUTPUTFILENAME ]
```

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
<code>network or IP address</code>	List the IP address or CIDR you want to have access to the share.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	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
```

## 4.2.6 add node-pool

Adds a node pool to a Kubernetes cluster. When a cluster is first built, there are two node pools: `master` and `worker`. Additional worker node pools can be created. This is useful when a cluster needs worker nodes with more (or less) CPU and Memory or you possibly need to create the boot disks in an alternate repository.

### Syntax

```
add node-pool cluster-name node-pool-name cpus memory repository virtual-appliance
[ --json ][ --less ][ --more ][ --tee=OUTPUTFILENAME ]
```

where `cluster-name` is the name of the Kubernetes cluster where you wish to add a node pool.

## Description

Use the `add node-pool` command to add a node pool to the Kubernetes cluster. A new node pool can be a different repository than the original cluster and can use a different virtual appliance if there is more than one available. The number of CPUs and memory must be within valid ranges.

## Options

The following table shows the available options for this command.

Option	Description
<code>node pool name</code>	Choose a name for the node pool you want to add. Once created the new node pool is empty. See <a href="#">Section 4.2.7, “add node-pool-node”</a> .
<code>cpus</code>	Specify the number of CPUs. Node pools can have between 1 and 24 CPUs.
<code>memory</code>	Specify the amount of memory. Node pools can have between 8 and 393 GB of memory.
<code>repository</code>	Enter the repository that contains the virtual appliance to be used and that will be used for the virtual machine boot disks. A cluster can have node pools in multiple repositories as long as they are all attached to all of the nodes in the tenant group. If not specified, the repository specified on the <code>create kube-cluster</code> command is used.  Note that tab completion on this field returns the default repository, not a full list of storage repositories available in Oracle VM.
<code>virtual appliance</code>	Enter one of the pre-configured virtual appliances names. If not specified, the virtual appliance name used by the cluster is assumed.  A new node pool can use a different virtual appliance from the original cluster, if there is more than one virtual appliance available.  You must add the virtual appliances ( <code>none default OVA-name</code> ) you use to the <code>/etc/kubernetes.conf</code> file before you execute this command.

## Examples

### Example 4.8 Adding a Node Pool

```
PCA> add node-pool MyCluster np0 1 8192
Status: Success
```

## 4.2.7 add node-pool-node

Adds a node to a Kubernetes cluster node pool. A host name is only required for a static network configuration. This command is used to scale up an existing worker node pool, or to replace a master node that was previously removed.

## Syntax

```
add node-pool-node cluster-name node-pool-name hostname [ --json ] [ --less ] [ --more ]
[ --tee=OUTPUTFILENAME ]
```

where `cluster-name` is the name of the Kubernetes cluster where you wish to add a node.

## Description

Use the `add node-pool-node` command to add a node to a node pool in the Kubernetes cluster. This command starts the node through an asynchronous job. Progress can be viewed through the `show node-pool-node` or `list node-pool-node` commands.

## Options

The following table shows the available options for this command.

Option	Description
<code>node pool name</code>	Choose the node pool where you want to add a node.
<code>host name</code>	For a static network, a host name is required, and that host name must be able to be resolved on the static network. For DHCP, this command does not require a host name unless you are replacing a master node.  In the case of a master node replacement, you must use the name of an existing host. You can determine the existing host names from the <code>list node-pool-node</code> command.

## States

The following table shows the available states for this command. All states apply to worker nodes, some states also apply to master nodes.

State	Substate	Description
CONFIGURED		This state is seen only in nodes in the master and worker node pools and typically only while the cluster is in CONFIGURED or BUILDING state. A node in the master node pool can return to the CONFIGURED state when a cluster is AVAILABLE if the master node is temporarily removed from the cluster in order to be re-built.
SUBMITTED	QUEUED	Awaiting resources to start building.
BUILDING		Building the node.
	VM	Building the virtual machine and applying settings.
	JOIN	Joining the Kubernetes control plane.
RECOVERING	VM	Stopping and removing the VM.
STOPPING		Stopping the node. The node will first be removed from the Kubernetes cluster, then the virtual machine will be stopped and removed from Oracle VM.
AVAILABLE		The node finished the build process.

State	Substate	Description
	BUSY	A master node in this state is being used to interact with the Kubernetes cluster.
ERROR		An error occurred with the node while it was being built. The node should be removed after the error is understood..
	BUILD_VM	An error occurred while the virtual machine was being built. Checking the error message with <code>show node-pool-node</code> can help understand the issue, Oracle VM may have to be consulted directly for detailed information on the failure.
	JOIN	An error occurred while the virtual machine was joining the Kubernetes control plane. Consult with the Kubernetes administrator on potential Kubernetes issues.

## Examples

### Example 4.9 Adding a Node Pool Node

```
PCA> add node-pool-node MyCluster np0 myHost_1
Status: Success
```

## 4.2.8 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 [ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```

## 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 [Section 1.6, “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 4.74, “Show Task”](#) for more information.

## Options

There are no further options for this command.

## Examples

### Example 4.10 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
```

## 4.2.9 configure vhbases

Configures vHBAs on compute nodes. This command is used only on systems with InfiniBand-based network architecture.

### Syntax

```
configure vhbases { ALL | node } [ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```

where `node` is the compute node name for the compute node for which the vHBAs should be configured, and `ALL` refers to all compute nodes provisioned in your environment.

### Description

This command creates the default virtual host bus adapters (vHBAs) for fibre channel connectivity, if they do not exist. Each of the four default vHBAs corresponds with a bond on the physical server. Each vHBA connection between a server node and Fabric Interconnect has a unique mapping. Use the `configure vhbases` command to configure the virtual host bus adapters (vHBA) on all compute nodes or a specific subset of them.

### Options

The following table shows the available options for this command.

Option	Description
<code>ALL   node</code>	Configure vHBAs for all compute nodes or for one or more specific compute nodes.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

### Examples

#### Example 4.11 Configuring the vHBAs for Specific Compute Nodes

```
PCA> configure vhbases ovcaen11r1 ovcaen14r1
```

```

Compute_Node      Status
-----
ovcacn14r1       Succeeded
ovcacn11r1       Succeeded
-----
2 rows displayed
Status: Success

```

## 4.2.10 create iscsi-storage

Creates a new iSCSI LUN share for a VM storage network. See [Section 2.7.2, “Creating Storage Shares”](#) for detailed information.

### Syntax

```
create iscsi-storage iscsi-LUN-name storage_network_name LUN_size storage-profile
[ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```

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
<code>storage_network_name</code>	The name of the storage network where you wish to create the share.
<code>share_size</code>	The size of the share in Gigabytes, for example 100G.
<code>storage-profile</code>	Optionally, you can choose a pre-configured storage profile to maximize I/O performance for your environment. For more information, see <a href="#">Section 2.7.3, “Storage Profiles”</a> .
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

### Examples

#### Example 4.12 Creating an iSCSI LUN Share

```
PCA> create iscsi-storage my_iscsi_LUN myStorageNnetwork 100G general
```

Status: Success

## 4.2.11 create lock

Imposes a lock on certain appliance functionality.



### Caution

Never use locks without consultation or specific instructions from Oracle Support.

## Syntax

```
create lock { all_provisioning | cn_upgrade | database | install | manufacturing
| mn_upgrade | provisioning | service } [ --json ] [ --less ] [ --more ] [ --
tee=OUTPUTFILENAME ]
```

## 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
<code>all_provisioning</code>	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.
<code>cn_upgrade</code>	Prevent all compute node upgrade operations.
<code>database</code>	Impose a lock on the databases during the management node update process. The lock is released after the update.
<code>install</code>	Placeholder lock type. Currently not used.
<code>manufacturing</code>	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 <code>ovca</code> service does not start.
<code>mn_upgrade</code>	Prevent all management node upgrade operations.
<code>provisioning</code>	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.
<code>service</code>	Placeholder lock type. Behavior is identical to manufacturing lock.



Option	Description
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.13 Imposing a Provisioning Lock

```
PCA> create lock provisioning
Status: Success
```

## 4.2.12 create network

Creates a new custom network, private or public, at the appliance level. See [Section 2.6, “Network Customization”](#) for detailed information.

### Syntax

```
create network network-name { rack_internal_network | external_network port-
group | storage_network prefix netmask [zfs-ipaddress] | host_network port-group
prefix netmask [route-destination gateway] } [ --json ] [ --less ] [ --more ] [ --
tee=OUTPUTFILENAME ]
```

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 [Section 4.2.18, “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
<code>{ rack_internal_network   external_network   storage_network   host_network }</code>	The type of custom network to create. The options are: <ul style="list-style-type: none"> <li>• a network internal to the rack</li> <li>• a network with external connectivity</li> <li>• a network with external connectivity, accessible for physical hosts</li> <li>• a network with internal connectivity to the ZFS storage appliance</li> </ul>
<code>external_network port-group</code>	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.
<code>storage_network prefix netmask [zfs-ipaddress]</code>	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.
<code>host_network port-group prefix netmask [route-destination gateway]</code>	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.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.14 Creating an Internal Custom Network

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

**Example 4.15 Creating a Custom Network with External Connectivity**

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

**Example 4.16 Creating a Storage Network**

```
PCA> create network MyStorageNetwork storage_network 10.10.10 255.255.255.0 10.10.10.1
Status: Success
```

## 4.2.13 create nfs-storage

Creates a new NFS storage share for a VM storage network. See [Section 2.7.2, “Creating Storage Shares”](#) for detailed information.

### Syntax

```
create nfs-storage nfs-share-name storage_network_name share_size storage-profile
[ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```

where `nfs-share-name` is the name of the NFS share you wish to create.

### Description

Use this command to create an NFS share associated 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
<code>storage_network_name</code>	The name of the storage network where you wish to create the share.
<code>share_size</code>	The size of the share in Gigabytes, for example 100G.
<code>storage-profile</code>	Optionally, you can choose a pre-configured storage profile to maximize I/O performance for your environment. For more information, see <a href="#">Section 2.7.3, “Storage Profiles”</a> .
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

### Examples

**Example 4.17 Creating an NFS Share**

```
PCA> create nfs-storage myShare myStorageNnetwork 100G general
```

```
Status: Success
```

## 4.2.14 create kube-cluster

Creates a new Kubernetes cluster definition. Once you create a cluster definition, you start that cluster to make it active. See [Section 2.13.3, “Create a Kubernetes Cluster on a DHCP Network”](#) and [Section 2.13.4, “Create a Kubernetes Cluster on a Static Network”](#) for detailed information.

### Syntax

```
create kube-cluster cluster-name tenant-group external_network
load_balancer_IP_address repository virtual-appliance
```

where `cluster-name` is the name of the Kubernetes cluster you wish to create.

### Description

Use the `create kube-cluster` command to set up a new cluster configuration for a viable Kubernetes cluster.

### Options

The following table shows the available options for this command.

Option	Description
<code>tenant group</code>	Choose the Oracle Private Cloud Appliance tenant group where you want to build your cluster. See <a href="#">Section 2.8, “Tenant Groups”</a> .
<code>external network</code>	Choose an external network to connect to the cluster master node. This network should provide access to your nameserver and DHCP server, and enables the master node to act as a gateway for the worker nodes if needed.
<code>load balancer IP address</code>	The load balancer IP address is a floating IP address that uses Virtual Router Redundancy Protocol (VRRP) to fail over to other master nodes when the host of the address can no longer be contacted. The VRRP address is auto-selected by the <code>create kube-cluster</code> command as the next available on the Oracle Private Cloud Appliance.  If other resources on the network use VRRP, assign a specific VRRP ID to the cluster to avoid VRRP collisions. See <a href="#">Section 4.2.45, “set kube-load-balancer”</a> .
<code>repository</code>	Assign a storage repository to the cluster. Note that tab completion on this field returns the default repository, not a full list of storage repositories available in Oracle VM.
<code>virtual appliance</code>	Optionally, you can enter a virtual appliance, that you have downloaded, to use as a template for your Kubernetes cluster. See <a href="#">Section 2.13.2, “Prepare the Cluster Environment”</a> .

### Examples

#### Example 4.18 Creating a Cluster

```
PCA> create kube-cluster MyCluster Rack1_ServerPool vm_public_vlan 10.10.10.250 Rack1-Repository
```

```
Kubernetes cluster configuration (MyCluster) created
Status: Success
```

## 4.2.15 create oci-backup

Creates an on-demand Oracle Cloud Infrastructure dataset backup. For more information, see [Section 2.12.2, “Configuring a Manual Cloud Backup”](#).

### Syntax

```
create oci-backup target-name target-name-2
```

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 multiple targets with this command. To configure targets, see [Section 2.12.1, “Configuring the Cloud Backup Service”](#).

### Options

The following table shows the available options for this command.

Option	Description
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

### Examples

#### Example 4.19 Creating an Oracle Cloud Infrastructure Backup

```
PCA> create oci-backup OCITarget_1 OCITarget_2
Status: Success
```

## 4.2.16 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
```

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 [Section 2.12.1, “Configuring the Cloud Backup Service”](#).

## Options

The following table shows the available options for this command.

Option	Description
<code>target-location</code>	The object storage endpoint. For a list of available endpoints, see <a href="https://docs.cloud.oracle.com/en-us/iaas/api/#/en/objectstorage/20160918/">https://docs.cloud.oracle.com/en-us/iaas/api/#/en/objectstorage/20160918/</a> .
<code>target-user</code>	A user that has access to your Oracle Cloud Infrastructure tenancy.
<code>target-bucket</code>	A logical container for storing objects. Users or systems create buckets as needed <a href="#">within a region</a> . To create a bucket for Cloud Backup feature, see <a href="#">Section 2.12.1, “Configuring the Cloud Backup Service”</a> .
<code>target-tenancy</code>	Your Oracle Cloud Infrastructure tenancy where you wish to store backups.
<code>keyfile</code>	An API key required to access your Oracle Cloud Infrastructure tenancy. For more information see <a href="https://docs.cloud.oracle.com/en-us/iaas/Content/API/Concepts/apisigningkey.htm">https://docs.cloud.oracle.com/en-us/iaas/Content/API/Concepts/apisigningkey.htm</a> .
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.20 Creating an Oracle Cloud Infrastructure Target

```
PCA> create oci-target MyTarget https://objectstorage.us-oci.com ocid1.user.oc1..oos mybucketocid1.tenancy.oc1
Status: Success
```

## 4.2.17 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 [Section 2.8, “Tenant Groups”](#) for detailed information.

## Syntax

```
create tenant-group tenant-group-name [ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```

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
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.21 Creating a Tenant Group

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

## 4.2.18 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 [Appliance Uplink Configuration](#) in the *Oracle Private Cloud Appliance Installation Guide*. This command is used only on systems with Ethernet-based network architecture.

## Syntax

```
create uplink-port-group port-group-name ports { 10g-4x | 25g-4x | 40g | 100g } [ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```

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
<code>ports</code>	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: <code>'1 2'</code> or <code>'3:1 3:2'</code> .
<code>{ 10g-4x   25g-4x   40g   100g }</code>	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.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.22 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
```

## 4.2.19 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 [ --confirm ] [ --force ] [ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```



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 4.49, “List All Configuration Errors”](#) for more information.

## Options

The following table shows the available options for this command.

Option	Description
<code>--confirm</code>	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
<code>--force</code>	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.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.23 Removing a Configuration Error

```
PCA> delete config-error 87
*****
WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
*****
Are you sure [y/N]:y
Status: Success
```

## 4.2.20 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
<code>--confirm</code>	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
<code>--force</code>	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.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.24 Deleting an iSCSI LUN Share

```
PCA> delete iscsi-storage my_iscsi_LUN
Status: Success
```

## 4.2.21 delete kube-cluster

Deletes a Kubernetes cluster configuration. The cluster must be stopped and in a CONFIGURED state for this command to work. See [Section 2.13.7, “Stop a Cluster”](#).

## Syntax

```
delete kube-cluster cluster-name
```

where `cluster-name` refers to the name of the cluster configuration to be deleted.

## Description

Use the `delete kube-cluster` command to delete a cluster configuration file and remove the cluster from the master configuration.

## Options

The following table shows the available options for this command.

Option	Description
<code>--confirm</code>	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
<code>--force</code>	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.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.25 Deleting a Cluster

```
PCA> delete kube-cluster MyCluster
Status: Success
```

## 4.2.22 delete lock

Removes a lock that was previously imposed on certain appliance functionality.

### Syntax

```
delete lock { all_provisioning | cn_upgrade | database | install | manufacturing |
mn_upgrade | provisioning | service } [ --confirm ] [ --force ] [ --json ] [ --less ] [ --more ]
[ --tee=OUTPUTFILENAME ]
```

### 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
<code>{ all_provisioning   cn_upgrade   database   install   manufacturing   mn_upgrade   provisioning   service }</code>	The type of lock to be removed.  For a description of lock types, see <a href="#">Section 4.2.11, “create lock”</a> .
<code>--confirm</code>	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
<code>--force</code>	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
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Example

### Example 4.26 Unlocking Provisioning

```
PCA> delete lock provisioning
*****
WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
*****
Are you sure [y/N]:y
Status: Success
```

## 4.2.23 delete network

Deletes a custom network. See [Section 2.6, “Network Customization”](#) for detailed information.

### Syntax

```
delete network network-name [ --confirm ] [ --force ] [ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```

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 [Section 4.2.36, “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
<code>--confirm</code>	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.

Option	Description
<code>--force</code>	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.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.27 Deleting a Custom Network

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

### Example 4.28 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.']
```

## 4.2.24 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
<code>--confirm</code>	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.

Option	Description
<code>--force</code>	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.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.29 Deleting an NFS Storage Share

```
PCA> delete nfs-storage myStorageShare
Status: Success
```

## 4.2.25 delete oci-backup

Deletes an Oracle Cloud Infrastructure dataset backup. For more information, see [Section 2.12.3, “Deleting Cloud Backups”](#).

### Syntax

```
delete oci-backup oci-backup-name
```

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
<code>--confirm</code>	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
<code>--force</code>	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.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux

Option	Description
	command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.30 Deleting an Oracle Cloud Infrastructure Backup

```
PCA> delete oci-backup myOCIbackup
Status: Success
```

## 4.2.26 delete oci-target

Deletes an Oracle Cloud Infrastructure target from your ZFS storage appliance. For more information see [Section 2.12.4, “Deleting Oracle Cloud InfrastructureTargets”](#).

## Syntax

```
delete oci-target oci-target-name
```

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
<code>--confirm</code>	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
<code>--force</code>	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.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.31 Deleting an Oracle Cloud Infrastructure Target

```
PCA> delete nfs-storage myStorageShare
Status: Success
```

## 4.2.27 delete task

The `delete` command can be used to delete a task from the database.

### Syntax

```
delete task id [ --confirm ] [ --force ] [ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```

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
<code>--confirm</code>	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
<code>--force</code>	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.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.32 Removing a Task

```
PCA> delete task 341e7bc74f339c
*****
WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
*****
```



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

## 4.2.28 delete tenant-group

Deletes a tenant group. The default tenant group cannot be deleted. See [Section 2.8, “Tenant Groups”](#) for detailed information.

### Syntax

```
delete tenant-group tenant-group-name [ --confirm ][ --force ][ --json ][ --less ][ --more ][ --tee=OUTPUTFILENAME ]
```

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
<code>--confirm</code>	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
<code>--force</code>	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.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

### Examples

#### Example 4.33 Deleting a Tenant Group

```
PCA> delete tenant-group myTenantGroup
*****
WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
```

```
*****
Are you sure [y/N]:y
Status: Success
```

## 4.2.29 delete uplink-port-group

Deletes an uplink port group. See [Section 4.2.18, “create uplink-port-group”](#) for more information about the use of uplink port groups. This command is used only on systems with Ethernet-based network architecture.

### Syntax

```
delete uplink-port-group port-group-name [ --confirm ] [ --force ] [ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```

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
<code>--confirm</code>	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
<code>--force</code>	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.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

### Examples

#### Example 4.34 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
```

## 4.2.30 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 [ --confirm ] [ --force ] [ --json ] [ --less ]
[ --more ] [ --tee=OUTPUTFILENAME ]
```

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 *Welcome 1*. 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 [Section 4.2.11, “create lock”](#) and [Section 4.2.22, “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
<code>--confirm</code>	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
<code>--force</code>	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.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.

Option	Description
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.35 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
```

## 4.2.31 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 [Section 2.10, “Health Monitoring”](#) for more information.

The other `diagnose` commands remain functional.

## Syntax

```
diagnose { ilom | software | hardware | rack-monitor } [ --force ] [ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```

The following table describes each possible target of the `diagnose` command.

Command Target	Information Displayed
hardware	<p>The <code>hardware</code> diagnostic has two further options:</p> <ul style="list-style-type: none"> <li>The <code>rack</code> 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.</li> </ul> <p>If required, the results can be filtered by component type (cn, ilom, mn, etc.) Use tab completion to see all component types available.</p> <ul style="list-style-type: none"> <li>The <code>reset</code> option must be followed by a component host name. The command resets the</li> </ul>

Command Target	Information Displayed
	<p>event counters in the monitor database to zero for the component in question.</p> <p>If a component is or was in critical state, the reset command re-enables monitoring for that component.</p>
ilom	The <code>ilom</code> diagnostic checks that the ILOM for each component is accessible on the management network.
leaf-switch <b>(Ethernet-based systems only)</b>	The <code>leaf-switch</code> diagnostic performs health checks on the leaf switches.
leaf-switch-resources <b>(Ethernet-based systems only)</b>	The <code>leaf-switch-resource</code> diagnostic checks the CPU and memory status of each leaf switch.
link-status <b>(Ethernet-based systems only)</b>	The <code>link-status</code> diagnostic returns the status of the leaf switch link ports.
rack-monitor	<p>The <code>rack-monitor</code> diagnostic checks for errors that may have been registered by the monitor service. Optionally these can be filtered per component category.</p> <p>If required, the results can be filtered by component type (cn, ilom, mn, etc.) Use tab completion to see all component types available.</p>
software	The <code>software</code> diagnostic triggers the Oracle Private Cloud Appliance software acceptance tests.
spine-switch <b>(Ethernet-based systems only)</b>	The <code>spine-switch</code> diagnostic performs health checks on the spine switch.
spine-switch-resources <b>(Ethernet-based systems only)</b>	The <code>spine-switch-resource</code> diagnostic checks the CPU and memory status of the spine switch.
switch-logs <b>(Ethernet-based systems only)</b>	<p>The <code>switch-logs</code> diagnostic has two further options:</p> <ul style="list-style-type: none"> <li>• The <code>process</code> option displays information for the processes run on the switches.</li> <li>• The <code>core</code> option displays information about core dumps.</li> </ul> <p>Access the switch directly for log details.</p>
uplink-port-statistics <b>(Ethernet-based systems only)</b>	The <code>uplink-port-statistics</code> 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
<code>--force</code>	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.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.
<code>--tests=TESTS</code>	Returns the output of specific tests you designate, rather than running the full set of tests.
<code>--version=VERSION</code>	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 4.36 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 4.37 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 4.38 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

## 4.2.32 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 [ --confirm ] [ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```

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
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.39 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
```

## 4.2.33 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 { backup-task | compute-node | config-error | iscsi-storage | kube-cluster |
lock | management-node | mgmt-switch-port | network | network-card | network-port |
network-switch | nfs-storage | node-pool | node-pool-node | oci-backup | oci-target |
ofm-network | opus-port | server-profile | 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 ] ]
```

where *SORTEDBY* is one of the table column names returned for the selected command target, and *SORTEDORDER* can be either *ASC* for an ascending sort, or *DES* for a descending sort. See [Section 4.1.3.2, “Sorting”](#) for more information.

where *FILTERCOLUMN* is one of the table column names returned for the selected command target, and *FILTER* is the text that you wish to match to perform your filtering. See [Section 4.1.3.3, “Filtering”](#) for more information.

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 ( <b>Ethernet-based systems only</b> )	Displays all iSCSI LUNs for storage.
kube-cluster ( <b>Ethernet-based systems only</b> )	Displays all the Kubernetes clusters.
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-card ( <b>InfiniBand-based systems only</b> )	Displays information about the I/O modules installed in the Fabric Interconnects.
network-port	Displays the status of all ports on all I/O modules installed in the networking components.
network-switch ( <b>Ethernet-based systems only</b> )	Displays basic information about all switches installed in the Oracle Private Cloud Appliance environment.
nfs-storage ( <b>Ethernet-based systems only</b> )	Displays NFS shares for storage.
node-pool ( <b>Ethernet-based systems only</b> )	Displays all the Kubernetes node pools.

Command Target	Information Displayed
node-pool-node <b>(Ethernet-based systems only)</b>	Displays all the Kubernetes nodes.
oci-backup	Displays all the Oracle Cloud Infrastructure backups.
oci-target	Displays all the Oracle Cloud Infrastructure targets.
ofm-network <b>(InfiniBand-based systems only)</b>	Displays network configuration, read directly from the Oracle Fabric Manager software on the Fabric Interconnects.
opus-port <b>(InfiniBand-based systems only)</b>	Displays connection information about every port of every Oracle Switch ES1-24 in the Oracle Private Cloud Appliance environment.
server-profile <b>(InfiniBand-based systems only)</b>	Displays a list of connectivity profiles for servers, as stored by the Fabric Interconnects. The profile contains essential networking and storage information for the server in question.
storage-network	Displays a list of known storage clouds on InfiniBand-based systems. The configuration of each storage cloud contains information about participating Fabric Interconnect ports and server vHBAs.  Displays a list of known storage networks on Ethernet-based systems.
storage-profile <b>(Ethernet-based systems only)</b>	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 <b>(Ethernet-based systems only)</b>	Displays information about spine switch port configurations for external networking.
uplink-port-group <b>(Ethernet-based systems only)</b>	Displays information about all uplink port groups configured for external networking.
wwpn-info <b>(InfiniBand-based systems only)</b>	Displays a list of all World Wide Port Names (WWPNs) for all ports participating in the Oracle Private Cloud Appliance Fibre Channel fabric. In the standard configuration each compute node has a vHBA in each of the four default storage clouds.

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
<code>list { backup-task   compute-node   config-error   iscsi-storage   kube-cluster   lock   management-node   mgmt-switch-port   network   network-card   network-port   network-switch   nfs-storage   node-pool   node-pool-node   oci-backup   oci-target   ofm-network   opus-port   server-profile   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 ] ]</code>	The command target to list information for.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.
<code>[ --sorted-by SORTEDBY ]</code>	Sort the table by the values within a particular column in the table, specified by replacing <code>SORTEDBY</code> with the name of the column that should be used to perform the sort.
<code>[ --sorted-order SORTEDORDER ]</code>	Used to specify the sort order, which can either be <code>ASC</code> for an ascending sort, or <code>DES</code> for a descending sort. You must use the <code>--sorted-by</code> option in conjunction with this option.
<code>[ --filter-column FILTERCOLUMN ]</code>	Filter the table for a value within a particular column in the table, specified by replacing <code>FILTERCOLUMN</code> with the name of the column that should be used to perform the sort. You must use the <code>--filter</code> option in conjunction with this option.
<code>[ --filter FILTER ]</code>	The filter that should be applied to values within the column specified by the <code>--filter-column</code> option.

## Examples

### Example 4.40 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 4.41 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 4.42 List All Tenant Groups

```
PCA> list tenant-group
```

Name	Default	State
Rack1_ServerPool	True	ready
myTenantGroup	False	ready

-----  
2 rows displayed

Status: Success

### Example 4.43 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 4.44 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 4.45 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 4.46 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 4.47 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 4.48 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 4.49 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 4.50 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

```

## 4.2.34 remove compute-node

Removes a compute node from an existing tenant group.

### Syntax

```
remove compute-node node tenant-group-name [ --confirm ] [ --force ] [ --json ] [ --less ]
[ --more ] [ --tee=OUTPUTFILENAME ]
```

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
<code>--confirm</code>	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
<code>--force</code>	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.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.51 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
```

## 4.2.35 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 [ --confirm ] [ --force ] [ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```

where `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
<code>initiator IQN</code>	List the initiator IQN from the virtual machine that should no longer have access to the LUN.
<code>LUN name</code>	Specify the LUN you want remove the initiator from.
<code>--confirm</code>	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
<code>--force</code>	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.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.



## Examples

### Example 4.52 Removing an Initiator From a LUN

```
PCA> remove initiator iqn.company.com myLUN
Status: Success
```

## 4.2.36 remove network

Disconnects a server node from a network.

### Syntax

```
remove network network-name node [ --confirm ] [ --force ] [ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```

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
<code>--confirm</code>	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
<code>--force</code>	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.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.53 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
```

## 4.2.37 remove network-from-tenant-group

Removes a custom network from a tenant group.

### Syntax

```
remove network-from-tenant-group network-name tenant-group-name [ --confirm ] [ --force ] [ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```

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
<code>--confirm</code>	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
<code>--force</code>	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.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

### Examples

#### Example 4.54 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
```

## 4.2.38 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 network or IP address [ --confirm ] [ --force ] [
--json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```

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
<code>network or IP address</code>	List the IP address or CIDR that should no longer have access to the share.
<code>--confirm</code>	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
<code>--force</code>	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.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

### Examples

#### Example 4.55 Removing an NFS Exception From a Share

```
PCA> remove nfs-exception myNFSShare 172.16.4.0/24
Status: Success
```

## 4.2.39 remove node-pool

Removes a node pool definition from a Kubernetes cluster.

## Syntax

```
remove node-pool cluster-name node-pool-name
```

where `cluster-name` is the name of the Kubernetes cluster from which you wish to remove a node pool.

## Description

Use the `remove node-pool` command to remove a node pool from the Kubernetes cluster. The node pool must be empty before it can be removed. See [Section 4.2.40, “remove node-pool-node”](#).

## Options

The following table shows the available options for this command.

Option	Description
<code>node pool name</code>	Choose the node pool you want to remove. A nodepool must be empty to remove it. The <code>worker</code> and <code>master</code> node pools cannot be removed.
<code>--force</code>	Force the command to be executed even if the target is in an invalid state or contains nodes. This option is not risk-free and should only be used as a last resort. In the case that there are nodes in the node pool, the command will attempt to gracefully remove workers from Kubernetes. The Kubernetes administrator should be notified of all worker nodes that were run with this option.

## Examples

### Example 4.56 Removing a Node Pool

```
PCA> remove node-pool MyCluster np0
Status: Success
```

## 4.2.40 remove node-pool-node

Removes a node from the Kubernetes cluster and deletes the virtual machine.

## Syntax

```
remove node-pool-node cluster-name node-pool-name hostname
```

where `cluster-name` is the name of the Kubernetes cluster from which you wish to remove a node.

## Description

Use the `remove node-pool-node` command to remove a node from the Kubernetes cluster. Once a node is removed from the Kubernetes cluster, the virtual machine will be stopped and destroyed and the configuration information will be removed from the cluster unless the node is in the master node that the node was removed from the Kubernetes cluster.

## Options

The following table shows the available options for this command.

Option	Description
<code>node pool name</code>	Choose the node pool where you want to remove a node. Nodes can be removed from any node pool. Only two nodes can be removed from the master node pool.
<code>host name</code>	Enter the host name you want to remove from the node pool.
<code>--force</code>	<p>If your first try to remove a master or worker node fails, perform a retry without the <code>--force</code> option first for a clean cleanup. If all means fails, then use <code>--force</code> option to remove the Kubernetes node.</p> <p>Force the command to be executed even if the target is in an invalid state. When completed, the Kubernetes administrator should be informed of the node removed as it may be left in a Not Ready state in the Kubernetes cluster. If this is the case, the Kubernetes administrator must delete the node. This option is not risk-free and should only be used as a last resort.</p>

## Examples

### Example 4.57 Removing a Node Pool Node

```
PCA> remove node-pool-node MyCluster np0 myHost_1
*****
WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
*****
Are you sure [y/N]:y
Node (myHost_1) removed
Status: Success
```

### Example 4.58 Removing a Node Pool Master Node

```
PCA> remove node-pool-node MyCluster master cluster_master_1
*****
WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
*****
Are you sure [y/N]:y
Node (myHost_1) removed
Status: Success
```

## 4.2.41 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 [ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ] [ --force ] [ --save-local-repo ]
```

where `node` 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 [Section 1.4, “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 4.73, “Show System Properties”](#) for more information.

## Options

The following table shows the available options for this command.

Option	Description
<code>compute-node</code>	The command target to perform the reprovision operation against.
<code>--save-local-repo</code>	Skip the HMP step in the provisioning process in order to save the local storage repository.
<code>--json</code>	Return the output of the command in JSON format.
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--force</code>	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.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.59 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
```

## 4.2.42 rerun

Triggers a configuration task to re-run on the Oracle Private Cloud Appliance.

## Syntax

```
rerun { config-task } id [ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```

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 4.49, "List All Configuration Errors"](#) for more information.

## Options

The following table shows the available options for this command.

Option	Description
<code>config-task</code>	The command target to perform the rerun operation against.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.60 Re-run a configuration task

```
PCA> rerun config-task 84
Status: Success
```

## 4.2.43 set system-property

Sets the value for a system property on the Oracle Private Cloud Appliance.

### Syntax

```
set system-property { ftp_proxy | http_proxy | https_proxy | log_count |
log_file | log_level | log_size | timezone } value [ --json ] [ --less ] [ --more ] [ --
tee=OUTPUTFILENAME ]
```

where `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 4.73, “Show System Properties”](#) 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
<code>ftp_proxy</code>	Set the value for the IP address of an FTP Proxy
<code>http_proxy</code>	Set the value for the IP address of an HTTP Proxy
<code>https_proxy</code>	Set the value for the IP address of an HTTPS Proxy
<code>log_count</code>	Set the value for the number of log files that should be retained through log rotation
<code>log_file</code>	<p>Set the value for the location of a particular log file.</p> <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"></div> <div> <p><b>Caution</b></p> <p>Make sure that the new path to the log file exists. Otherwise, the log server stops working.</p> <p>The system always prepends <code>/var/log</code> to your entry. Absolute paths are converted to <code>/var/log/&lt;path&gt;</code>.</p> </div> </div> <p>This property can be defined separately for the following log files: backup, cli, diagnosis, monitor, ovca, snmp, and syncservice.</p>
<code>log_level</code>	<p>Set the value for the log level output. Accepted log levels are: CRITICAL, DEBUG, ERROR, INFO, WARNING.</p> <p>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.</p>
<code>log_size</code>	Set the value for the maximum log size before a log is rotated
<code>timezone</code>	Set the time zone for the location of the Oracle Private Cloud Appliance.



Option	Description
	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.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.61 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 [Section 7.1, “Setting the Oracle Private Cloud Appliance Logging Parameters”](#).

### Example 4.62 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 [Section 7.2, “Adding Proxy Settings for Oracle Private Cloud Appliance Updates”](#).

### Example 4.63 Configuring the Oracle Private Cloud Appliance Time Zone

```
PCA> set system-property timezone US/Eastern
```

```
Status: Success
```

## 4.2.44 set kube-dns

Configures the DNS information for a static network.

### Syntax

```
set kube-dns cluster-name name-servers search-domains
```

where `cluster-name` is the name of the cluster where you wish to configure external network settings.

### Description

Use the `set kube-dns` command to set the DNS name servers and search domains.

### Options

The following table shows the available options for this command.

Option	Description
<code>name servers</code>	Specify the domain name server address. If you use more than one domain name server, use a comma to separate the addresses.
<code>search domains</code>	Specify one or more search domains. DNS searches require a fully qualified domain name. Listing your often-used domains in the search domains field lets you search just a machine name, without using the fully-qualified domain name.

### Examples

#### Example 4.64 Set DNS Information for a Static Network

```
PCA> set kube-dns MyCluster 8.8.8.8,9.9.9.9 demo.org,demo.com
Status: Success
```

## 4.2.45 set kube-load-balancer

Sets the VRRP ID parameter for the Kubernetes load balancer. Use this setting to avoid VRRP conflicts on your network.

### Syntax

```
set kube-load-balancer cluster-name VRRP_ID
```

where `cluster-name` is the name of the Kubernetes cluster where you set the load balancer VRRP ID.

### Description

Use the `set kube-load-balancer` command to manually set the VRRP ID on your cluster when other systems in your network use VRRP.

### Options

The following table shows the available options for this command.

Option	Description
VRRP_ID	Generally, the VRRP address is auto-selected during the <code>create kube-cluster</code> command. If other resources on the same network as your Oracle Private Cloud Appliance use VRRP this randomize method could cause conflicts. In that case, find what VRRP IDs are available on your network for you to use, and assign one to the cluster using this command.

## Examples

### Example 4.65 Setting a VRRP ID on a Cluster

```
PCA> create kube-load-balancer MyCluster 232
Status: Success
```

## 4.2.46 set kube-master-pool

Configures the host names for the Kubernetes master nodes, these must be resolveable names on the external network.

### Syntax

```
set kube-master-pool cluster-name primary-hostname, ipv4address host-name host-name
```

where `cluster-name` is the name of the cluster where you wish to configure host names for the master nodes.

### Description

Use the `set kube-master-pool` create a list of valid host names for the master nodes in the cluster.

### Options

The following table shows the available options for this command.

Option	Description
<code>primary host name, IPv4 address</code>	The first host name must have an IP address associated with it. This command must be run if the external network is static, it is an invalid command if the external network is DHCP.
<code>host name</code>	Specify one or more additional host names for the master nodes, no IPv4 addresses required for additional hosts.

## Examples

### Example 4.66 Set DNS Information for a Static Network

```
PCA> set kube-master-pool MyCluster Master_host1,192.168.0.20 MasterHost2 MasterHost3
Status: Success
```

## 4.2.47 set kube-network

Configures the external network for either DHCP or static IP addressing.

## Syntax

```
set kube-network cluster-name DHCP | static netmask gateway
```

where `cluster-name` is the name of the cluster where you wish to configure external network settings.

## Description

Use the `set kube-network` command to set up either DHCP or static IP addressing for the selected cluster.

## Options

The following table shows the available options for this command.

Option	Description
<code>dhcp   static</code>	Choose the either DHCP or static IP addressing for the selected cluster. If you choose static, you must provide the netmask and gateway information. For static networks, you must also set this information: <ul style="list-style-type: none"> <li>• DNS information, see <a href="#">Section 4.2.44, “set kube-dns”</a></li> <li>• <code>set kube-master-pool</code></li> <li>• <code>set kube-worker-pool</code></li> </ul>
<code>netmask</code>	Netmask for the interface.
<code>gateway</code>	IP address for the gateway.

## Examples

### Example 4.67 Set a Cluster Network to DHCP

```
PCA> set kube-network MyCluster dhcp
Status: Success
```

### Example 4.68 Set a Cluster Network to Static

```
PCA> set kube-network MyCluster static 255.255.255.0 192.168.0.1
Status: Success
```

## 4.2.48 set kube-vm-shape

Changes the profile of the virtual machines that are part of the default node pool for masters or workers.

## Syntax

```
set kube-vm-shape cluster-name master | worker cpus memory
```

where `cluster-name` is the name of the cluster where you wish change the virtual machine profile.

## Description

Use the `set kube-vm-shape` to optionally set the virtual machine shapes for either the master or worker nodes in a cluster.

## Options

The following table shows the available options for this command.

Option	Description
<code>master</code>   <code>worker</code>	Choose which virtual machine shape to customize, the master or worker shape.
<code>cpus</code>	Master nodes can have between 4 and 24 CPUs. The default is 8 CPUs.  Worker nodes can have between 1 and 14 CPUs. The default is 4 CPUs.
<code>memory</code>	Master nodes can have between 16 and 393 GB of memory, if available. The default is 32 GB.  Worker nodes can have between 8 and 393 GB of memory, if available. The default is 16 GB.

## Examples

### Example 4.69 Set the kube-vm-shape for a Master Node

```
PCA> set kube-vm-shape MyCluster master 4 16384
Status: Success
```

### Example 4.70 Set the kube-vm-shape for a Worker Node

```
PCA> set kube-vm-shape MyCluster worker 16 64000
Status: Success
```

## 4.2.49 set kube-worker-pool

Resizes the Kubernetes cluster worker pool.

### Syntax

```
set kube-worker-pool cluster-name quantity [ ] host-name host-name
```

where `cluster-name` is the name of the cluster where you wish to resize the worker pool.

### Description

Use the `set kube-worker-pool` to change the size of a cluster worker pool.

### Options

The following table shows the available options for this command.

Option	Description
<code>quantity</code>	If the external network is DHCP, then the quantity of workers required in the worker pool may be specified, instead of specifying the list of host names. A quantity of 0 is valid for either DHCP and static networks. While quantity is not required for static cluster, if specified, it must be set to 0, to allow no workers to be created.

Option	Description
<code>host name</code>	For static networks, the list of host names is required and the cluster configuration is invalid without them. Specify the host names for the worker nodes in a static network.

## Examples

### Example 4.71 Set the Worker Pool Size for a Static Network

```
PCA> set kube-worker-pool MyCluster WorkerHost1 WorkerHost2 WorkerHost3
Status: Success
```

### Example 4.72 Set the Worker Pool Size for a DHCP Network

```
PCA> set kube-worker-pool MyCluster 2
Status: Success
```

## 4.2.50 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 { cloud-wwpn | compute-node | iscsi-storage | iscsi-storage-profile | kube-cluster
| network | node-pool | node-pool-node | nfs-storage | nfs-storage-profile | oci-backup
| oci-target | rack-layout | rack-type | server-profile | storage-network | system-
properties | task | tenant-group | version | vhba-info } object [ --json ] [ --less ] [ --more
] [ --tee=OUTPUTFILENAME ]
```

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
cloud-wwpn ( <b>Ethernet-based systems only</b> )	Storage Network/Cloud Name
compute-node	Compute Node Name
iscsi-storage ( <b>Ethernet-based systems only</b> )	iSCSI LUN Name
iscsi-storage-profile ( <b>Ethernet-based systems only</b> )	Storage Profile Name
kube-cluster ( <b>Ethernet-based systems only</b> )	Kubernetes Cluster Name
network	Network Name
nfs-storage ( <b>Ethernet-based systems only</b> )	NFS Share Name
nfs-storage-profile ( <b>Ethernet-based systems only</b> )	NFS Storage Profile Name
node-pool ( <b>Ethernet-based systems only</b> )	Node Pool Name
node-pool-node ( <b>Ethernet-based systems only</b> )	Node Pool Node Name
oci-backup ( <b>Ethernet-based systems only</b> )	Oracle Cloud Infrastructure Backup Name
oci-target ( <b>Ethernet-based systems only</b> )	Oracle Cloud Infrastructure Target Name

Command Target	Object Identifier
rack-layout	Rack Architecture or Type
rack-type	(none)
server-profile ( <b>InfiniBand-based systems only</b> )	Server Name
storage-network	Storage Network/Cloud Name
system-properties	(none)
task	Task ID
tenant-group	Tenant Group Name
version	(none)
vhba-info ( <b>InfiniBand-based systems only</b> )	Compute Node Name

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
<code>show { cloud-wwpn   compute-node   iscsi-storage   iscsi-storage-profile   kube-cluster   network   node-pool   node-pool-node   nfs-storage   nfs-storage-profile   oci-backup   oci-target   rack-layout   rack-type   server-profile   storage-network   system-properties   task   tenant-group   version   vhba-info } object [ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]</code>	The command target to show information for.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.

Option	Description
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.73 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 4.74 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 4.75 Show Rack Layout

```
PCA> show rack-layout x8-2_base
```



show

```
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 4.76 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 4.77 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_Fileystem_ID   3600144f0d29d4c86000057162ecc0001
-----
```

```
Status: Success
```

### Example 4.78 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 4.79 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 4.80 Show the vHBA configuration for a Compute Node

```
PCA> show vhma-info ovcacn10r1
```

```
-----
vHBA_Name           Cloud           WWNN           WWPN
-----
```

## start

```
vhba03      Cloud_C      50:01:39:71:00:58:B1:04  50:01:39:70:00:58:B1:04
vhba02      Cloud_B      50:01:39:71:00:58:91:05  50:01:39:70:00:58:91:05
vhba01      Cloud_A      50:01:39:71:00:58:91:04  50:01:39:70:00:58:91:04
vhba04      Cloud_D      50:01:39:71:00:58:B1:05  50:01:39:70:00:58:B1:05
-----
4 rows displayed

Status: Success
```

### Example 4.81 Show Oracle Private Cloud Appliance Version Information

```
PCA> show version
```

```
-----
Version          2.4.1
Build            819
Date             2019-06-20
-----
```

```
Status: Success
```

### Example 4.82 Show Cluster Information

```
PCA> show kube-cluster MyCluster
```

```
-----
Cluster          MyCluster
Tenant_Group     Rack1_ServerPool
State            CONFIGURED
Sub_State        VALID
Ops_Required     None
Load_Balancer    100.80.111.129
Vrrp_ID          15
External_Network vm_public_vlan
Cluster_Network_Type dhcp
Gateway          None
Netmask          None
Name_Servers     None
Search_Domains   None
Repository       Rack1-Repository
Assembly         PCA_K8s_va.ova
Masters          3
Workers          3
Cluster_Start_Time None
Cluster_Stop_Time None
Job_ID           None
Error_Code       None
Error_Message    None
-----
```

```
Status: Success
```

## 4.2.51 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 } [ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```

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
<code>compute-node CN   management-node MN</code>	Start either a compute node or a management node. Replace <i>CN</i> or <i>MN</i> respectively with the host name of the server to be started.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.83 Starting a Compute Node

```
PCA> start compute-node ovcacn11r1
Status: Success
```

## 4.2.52 start kube-cluster

Builds a Kubernetes cluster from a cluster definition created using [Section 4.2.14, “create kube-cluster”](#). Depending on the size of the cluster definition, this process can take from 30 minutes to hours.

## Syntax

```
start kube-cluster cluster-name
```

where `cluster-name` refers to the name of the cluster to be started.

## Description

Use the `start kube-cluster` command to submit the Kubernetes cluster definition to be started through an asynchronous job. Progress can be viewed through the `show kube-cluster` or `list kube-cluster` commands.

## States

The following table shows the available states for this command. Note these are the *Kubernetes cluster states*, not the Oracle VM Kubernetes virtual machine states (stopped, suspended, etc.). View the states

using the `show kube-cluster` command while the cluster is starting, or with the `list kube-cluster` command.

State	Substate	Description
CONFIGURED	VALID	The cluster is valid.
	INVALID	The cluster is invalid and cannot be started.
SUBMITTED	QUEUED	Awaiting resources to start building.
BUILDING	NETWORK	Building the network.
	MASTER_VMS	Building the virtual machines for the control plane.
	LOADBALANCER	Applying the loadbalancer changes.
	CONTROL_PLANE	Joining the control plane.
	WORKERS	Building the workers.
RECOVERING	MASTER_VMS	Stopping and removing the master VMs.
	NETWORK	Stopping and removing the network.
STOPPING	VMs	Stopping VMs in a node pool: <i>nodepoolname</i>
	NETWORK	Stopping the network.
AVAILABLE		The cluster has finished the build process.
	WORKERS	Error occurred during build of the worker nodes.
	TBD	Cluster build is clear.
ERROR	TBD	The cluster was fully torn down.
	TBD	The cluster needs to be stopped and likely have manual intervention.

## Examples

### Example 4.84 Starting a Cluster

```
PCA> start kube-cluster MyCluster
Status: Success
```

## 4.2.53 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 } [ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```



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
<code>compute-node CN   management-node MN</code>	<p>Shut down either a compute node or a management node. Replace <code>CN</code> or <code>MN</code> respectively with the host name of the server to be shut down.</p> <div style="display: flex; align-items: center;">  <div> <p><b>Caution</b></p> <p>These options are deprecated.</p> </div> </div>
<code>task id   update-task id</code>	<p>Aborts a running task.</p> <p>Use the <code>update-task</code> 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.</p> <div style="display: flex; align-items: center;">  <div> <p><b>Caution</b></p> <p>Stopping an update task is a risky operation and should be used with extreme caution.</p> </div> </div>
<code>--confirm</code>	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.85 Aborting a Task

```
PCA> stop task 341d45b5424c16
*****
WARNING !!! THIS IS A DESTRUCTIVE OPERATION.
*****
```

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

## 4.2.54 stop kube-cluster

Stops a Kubernetes cluster.

### Syntax

```
stop kube-cluster cluster-name
```

where `cluster-name` refers to the name of the cluster to be stopped.

### Description

Use the `stop kube-cluster` command to stop an available Kubernetes cluster through an asynchronous job. Progress can be viewed through the `show kube-cluster` or `list kube-cluster` commands.

### States

The following table shows the available states for this command. View the states using the `show kube-cluster` command while the cluster is starting.

Cluster Substate	Description
AVAILABLE or ERROR	
SUBMITTED	Status of network configuration.  Possible states are: <code>build_network</code> , <code>build_control_plane</code> , <code>remove_network</code>
QUEUED	
STOPPING	
CONFIGURED	
VALID	

### Examples

#### Example 4.86 Stopping a Cluster

```
PCA> stop kube-cluster MyCluster
Status: Success
```

## 4.2.55 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.

## 4.2.56 update password

Modifies the password for one or more components within the Oracle Private Cloud Appliance.

### Syntax

```
update password { LeafSwitch-admin | MgmtNetSwitch-admin | SpineSwitch-admin | mgmt-root | mysql-appfw | mysql-ovs | mysql-root | ovm-admin | spCn-root | spMn-root | spZfs-root | system-root | wls-weblogic | zfs-root } [ PCA-password target-password ] [ --confirm ] [ --force ] [ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```

where `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
<code>LeafSwitch-admin</code>	Sets a new password for the <code>admin</code> user on the leaf Cisco Nexus 9336C-FX2 Switches.
<code>MgmtNetSwitch-admin</code>	Sets a new password for the <code>admin</code> user on the Cisco Nexus 9348GC-FXP Switch.
<code>SpineSwitch-admin</code>	Sets a new password for the <code>admin</code> user on the spine Cisco Nexus 9336C-FX2 Switches.
<code>mgmt-root</code>	Sets a new password for the <code>root</code> user on the management nodes.
<code>mysql-appfw</code>	Sets a new password for the <code>appfw</code> user in the MySQL database.  The <code>mysql-appfw</code> , <code>mysql-ovs</code> , <code>mysql-root</code> and <code>wls-weblogic</code> passwords are synchronized automatically, because these must always be identical.
<code>mysql-ovs</code>	Sets a new password for the <code>ovs</code> user in the MySQL database.



Option	Description
	The <code>mysql-appfw</code> , <code>mysql-ovs</code> , <code>mysql-root</code> and <code>wls-weblogic</code> passwords are synchronized automatically, because these must always be identical.
<code>mysql-root</code>	Sets a new password for the <code>root</code> user in the MySQL database.  The <code>mysql-appfw</code> , <code>mysql-ovs</code> , <code>mysql-root</code> and <code>wls-weblogic</code> passwords are synchronized automatically, because these must always be identical.
<code>ovm-admin</code>	Sets a new password for the <code>admin</code> user in Oracle VM Manager.
<code>spCn-root</code>	Sets a new password for the <code>root</code> user in the compute node ILOMs.
<code>spMn-root</code>	Sets a new password for the <code>root</code> user in the management node ILOMs.
<code>spZfs-root</code>	Sets a new password for the <code>root</code> user on the ZFS storage appliance as well as its ILOM.
<code>system-root</code>	Sets a new password for the <code>root</code> user on all compute nodes.
<code>wls-weblogic</code>	Sets a new password for the <code>weblogic</code> user in WebLogic Server.  The <code>mysql-appfw</code> , <code>mysql-ovs</code> , <code>mysql-root</code> and <code>wls-weblogic</code> passwords are synchronized automatically, because these must always be identical.
<code>zfs-root</code>	Sets a new password for the <code>root</code> user on the ZFS storage appliance as well as its ILOM.
<code>--confirm</code>	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
<code>--force</code>	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.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.87 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

```

## 4.2.57 update compute-node

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 } [ --confirm ] [ --force ] [ --json ] [ --less ] [ --more ] [ --tee=OUTPUTFILENAME ]
```

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.



#### Warning

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
<code>--confirm</code>	Confirm flag for destructive command. Use this flag to disable the confirmation prompt when you run this command.
<code>--force</code>	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.
<code>--json</code>	Return the output of the command in JSON format
<code>--less</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>less</code> command on the Linux command line. This option allows both forward and backward navigation through the command output.
<code>--more</code>	Return the output of the command one screen at a time for easy viewing, as with the <code>more</code> command on the Linux command line. This option allows forward navigation only.
<code>--tee=OUTPUTFILENAME</code>	When returning the output of the command, also write it to the specified output file.

## Examples

### Example 4.88 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
```



---

# Chapter 5 Managing the Oracle VM Virtual Infrastructure

## Table of Contents

5.1 Guidelines and Limitations .....	202
5.2 Logging in to the Oracle VM Manager Web UI .....	205
5.3 Monitoring Health and Performance in Oracle VM .....	205
5.4 Creating and Managing Virtual Machines .....	206
5.5 Managing Virtual Machine Resources .....	209
5.6 Configuring Network Resources for Virtual Machines .....	211
5.6.1 Configuring VM Network Resources on Ethernet-based Systems .....	211
5.6.2 Configuring VM Network Resources on InfiniBand-based Systems .....	214
5.7 Viewing and Managing Storage Resources .....	217
5.7.1 Oracle ZFS Storage Appliance ZS7-2 .....	218
5.7.2 Oracle ZFS Storage Appliance ZS5-ES and Earlier Models .....	218
5.8 Tagging Resources in Oracle VM Manager .....	219
5.9 Managing Jobs and Events .....	219
5.10 Exporting VMs to Oracle Cloud Infrastructure .....	219
5.10.1 Prepare Your Oracle Cloud Infrastructure .....	220
5.10.2 Create the Oracle VM Exporter Appliance Virtual Machine .....	220
5.10.3 Configure the Oracle VM Exporter Appliance Virtual Machine .....	221
5.10.4 Create a Network for the Oracle VM Exporter Appliance VM .....	222
5.10.5 Attach the New Network to the Oracle VM Exporter Appliance VM .....	225
5.10.6 Prepare a Storage Repository .....	226



### Warning

Access to the Oracle VM Manager web user interface, command line interface and web services API is provided without restrictions. The configuration of Oracle Private Cloud Appliance components within Oracle VM Manager is automatic and handled by the Oracle 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.

Here is a non-exhaustive list of critical limitations that are known to be violated regularly, which results in severe system configuration problems and significant downtime:

- **DO NOT rename host names** of compute names or other Oracle 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 the Oracle Private Cloud Appliance Administrator's Guide.
- **DO NOT add the VM role to the internal management network or internal storage network.**

**Warning**

The appliance controller software enables customization of networking, external storage connectivity and server pools – known as tenant groups in Oracle 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 Oracle 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 Oracle Private Cloud Appliance.

Management of virtual machines and your Oracle VM environment is achieved using the Oracle VM Manager Web UI (User Interface). While Oracle VM Manager does provide a command line interface and web services API, use of these on your Oracle Private Cloud Appliance should only be attempted by advanced users with a thorough understanding of Oracle VM and the usage limitations within an Oracle Private Cloud Appliance context.

The information provided in here, is a description of the Oracle VM Manager Web UI within the context of the Oracle 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. The complete Oracle VM Manager User's Guide is available at this URL: <https://docs.oracle.com/en/virtualization/oracle-vm/3.4/user/index.html>.

**Note**

When consulting the Oracle VM documentation directly, keep in mind the limitations imposed by using it within Oracle 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 master or 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 [Section 1.5, "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.

## 5.1 Guidelines and Limitations

The Oracle VM Manager Web User Interface is provided without any software limitation to its functionality. Once your appliance has been provisioned, the Oracle VM environment is fully configured and ready to use for the deployment and management of your virtual machines. In this section, the operations that are explicitly not permitted, are presented as guidelines and limitations that should be followed when working within Oracle VM Manager, or executing operations programmatically through the command line interface (CLI) or web services API (WSAPI).

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

**Do Not:**

- attempt to discover, remove, rename or otherwise modify servers or their configuration;
- 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;
- 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 note with [Doc ID 2519818.1](#);
- attempt to connect any Oracle Private Cloud Appliance component to a customer's LDAP or Active Directory for authentication, including management nodes, compute nodes, or ZFS storage appliances;
- 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.

If you ignore this advice, the Oracle 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 Oracle Private Cloud Appliance. If a conflict between the Oracle 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 the support note with [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 with [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.

## 5.2 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.

## 5.3 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 [Section 2.3, “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](#)

## 5.4 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 [Section 5.5, "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 [Section 2.8, “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

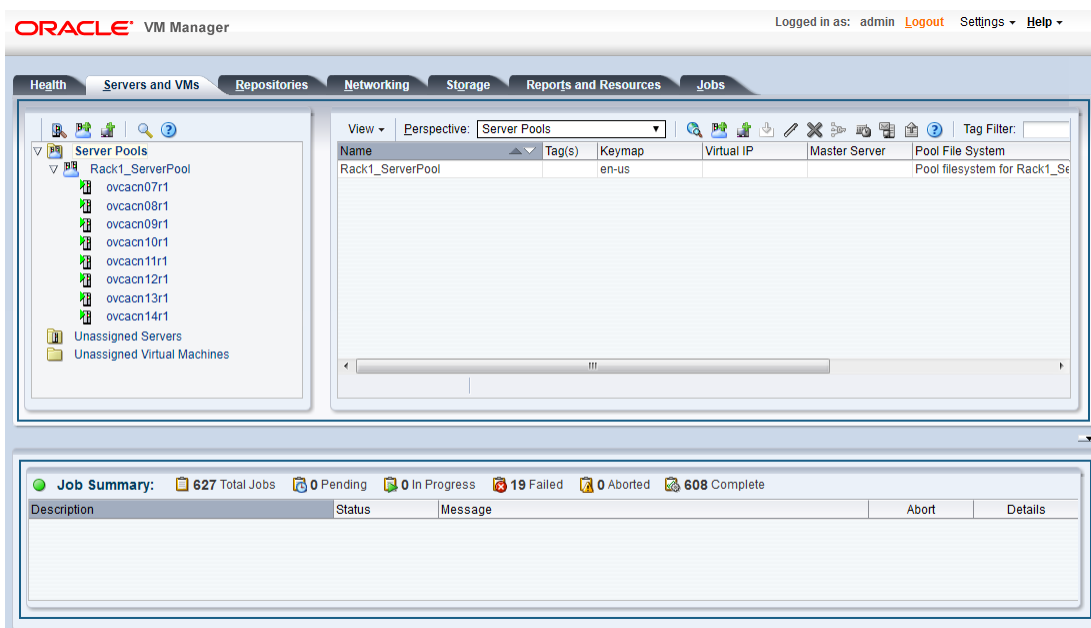
Exporting an Oracle VM virtual machine using the Oracle VM Exporter Appliance transfers the virtual machine to Oracle Cloud Infrastructure. Exporting a virtual machine does not remove the virtual machine from Oracle VM. You can export a virtual machine to other places in Oracle Cloud Infrastructure. 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**


## 5.5 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 may be altered.



### Caution

Using local storage on the compute nodes has implications that you should take into account when planning the deployment of your virtual environment. For example:

- Virtual machines with resources in a local storage repository cannot be migrated to another compute node.
- 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 Oracle Private Cloud Appliance, see [Section 5.7, “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 this 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](#).

For specific information about virtual appliances offered through Oracle Technology Network, refer to [Virtual Appliances from Oracle](#).

- 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

Through the [Oracle VM product pages](#), 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 the chapter [Understanding Repositories](#) in the *Oracle VM Concepts Guide*. The most relevant sections are:

- How is a Repository Organized?
- How are Virtual Appliances Managed?

## 5.6 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.

Oracle Private Cloud Appliance exists in two different types of network architecture. One is built around a physical InfiniBand fabric; the other relies on physical high speed Ethernet connectivity. While the two implementations offer practically the same functionality, the configuration of default networks is different due to the type of network hardware. As a result, the procedures to create VLAN networks for virtual machine traffic are different as well.

This section is split up by network architecture to avoid confusion. Refer to the subsection that applies to your appliance.

### 5.6.1 Configuring VM Network Resources on Ethernet-based Systems

On a system with an Ethernet-based network architecture, 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 [Section 1.2.4, "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 (Ethernet-based Architecture)**

The screenshot shows the Oracle VM Manager interface. The top navigation bar includes tabs for Health, Servers and VMs, Repositories, Networking (selected), Storage, Reports and Resources, and Jobs. The main content area is titled 'Networks' and contains a table of network channels. Below the table is a 'Job Summary' section with a table of job status.

Name	ID	Intra-Network Server	Network Channels					Description
			Server Management	Cluster Heartbeat	Live Migrate	Storage	Virtual Machine	
192.168.32.0	10b9cddb10			✓				
192.168.40.0	c0a88c00		✓		✓			
default_external	1039c145f1						✓	
default_internal	10336e5cbd						✓	
nmv_pvl_network	10d3e06a47						✓	
private_vlan1001	10fb124b07						✓	VM private network vlan 1001
private_vlan1002	109b387afa						✓	VM private network vlan 1002
public_vlan0011	105ec61873						✓	VM public network vlan 11
public_vlan0012	1044b1f9bf						✓	VM public network vlan 12
public_vlan0013	1015290b59						✓	VM public network vlan 13
public_vlan0014	1035673979						✓	VM public network vlan 14
public_vlan0015	10012d3835						✓	VM public network vlan 15

Job Summary: 627 Total Jobs 0 Pending 0 In Progress 19 Failed 0 Aborted 608 Complete							
Description	Status	Progress	Message	Timestamp	Duration	Abort	Details
No data to display							

## 5.6.2 Configuring VM Network Resources on InfiniBand-based Systems

On a system with an InfiniBand-based network architecture, default networks are set up as follows:

- `192.168.140.0` : the management network

This is a private network used exclusively for Oracle VM management traffic. Both management nodes and all compute nodes are connected to this network through their `bond0` interface.

- `192.168.40.0` : the storage network

This is a private IPoIB network used exclusively for traffic to and from the ZFS storage appliance. Both management nodes and both storage controllers are connected to this network through their `bond1` interface.

Additionally, three networks are listed with the **VM Network** role:

- `vm_public_vlan`

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 `bond4` port 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 11 on top of a `bond4` port.



**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](#).

5. Configure your data center network accordingly.

For details, see [Section 7.3, "Configuring Data Center Switches for VLAN Traffic"](#).

- `vm_private`

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 `bond3` port 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 `bond3` port.



**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](#).

- `mgmt_public_eth`

This network is automatically created during the initial configuration of the appliance. It uses the public network that you configured in the Oracle Private Cloud Appliance Dashboard. The primary function of this network is to provide access to the management nodes from the data center network, and enable the management nodes to run a number of system services. As long as you have not configured this network with a VLAN tag, it may also be used to provide external untagged network access to virtual machines. The subnet associated with this network is the same as your data center network.



**Caution**

Always use the `vm_public_vlan` network as your first VM network option. The `mgmt_public_eth` is unavailable for VM networking when configured with a management VLAN. When no management VLAN is configured, it is restricted to untagged VM traffic, and should only be considered if the circumstances require it.

For more information about Oracle Private Cloud Appliance network configuration, see [Section 1.2.4, "Network Infrastructure"](#).

**Caution**

Do not alter the internal appliance management 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 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 5.3 A view of the Networking tab (InfiniBand-based Architecture)**

The screenshot shows the Oracle VM Manager interface with the Networking tab selected. The main area displays a table of network configurations. Below the table is a Job Summary section showing the status of various jobs.

Name	ID	Intra-Network Server	Network Channels					Description
			Server Management	Cluster Heartbeat	Live Migrate	Storage	Virtual Machine	
192.168.40.0	10b9cdbb10			✓		✓		
192.168.140.0	c0a88c00		✓		✓	✓		
mgmt_public_eth	10d3e06a47						✓	
private_vlan1001	10fb124b07						✓	VM private network vlan 1001
private_vlan1002	109b387afa						✓	VM private network vlan 1002
public_vlan0011	105ec61873						✓	VM public network vlan 11
public_vlan0012	1044b1f9bf						✓	VM public network vlan 12
public_vlan0013	1015290b59						✓	VM public network vlan 13
public_vlan0014	1035673979						✓	VM public network vlan 14
public_vlan0015	10012d3835						✓	VM public network vlan 15
vm_private	10ec9a04e9						✓	
vm_public_vlan	10f62ad232						✓	

Job Summary: 627 Total Jobs 0 Pending 0 In Progress 19 Failed 0 Aborted 608 Complete							
Description	Status	Progress	Message	Timestamp	Duration	Abort	Details
No data to display							

## 5.7 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.



### Warning

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.

There are functional differences between the Oracle ZFS Storage Appliance ZS7-2, which is part of systems with an Ethernet-based network architecture, and the previous models of the ZFS Storage Appliance, which are part of systems with an InfiniBand-based network architecture. For clarity, this section describes the Oracle VM storage resources separately for the different storage appliances.

## 5.7.1 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 on expanding your Oracle VM environment with storage repositories located on the external storage is provided in the *Oracle VM Manager User's Guide*. Refer to the section entitled [Storage Tab](#). 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 5.4 A view of the Storage tab (with Oracle ZFS Storage Appliance ZS7-2)**

Name	Event Severity	Size (GiB)	Server	Status	Shareable	Description	VM(s)
SUN (1)	Informational	12.0	ovcacn07r1, ovcac...	online	No		
SUN (2)	Informational	3072.0	ovcacn07r1, ovcac...	online	No		

**Job Summary:** 627 Total Jobs, 0 Pending, 0 In Progress, 19 Failed, 0 Aborted, 608 Complete

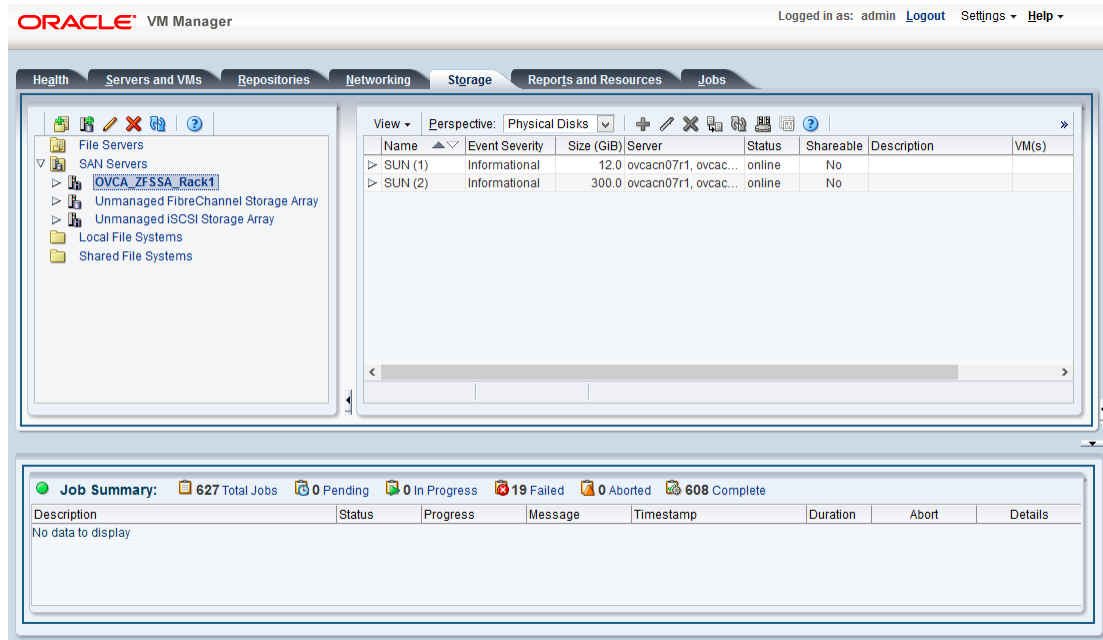
Description	Status	Progress	Message	Timestamp	Duration	Abort	Details
No data to display							

## 5.7.2 Oracle ZFS Storage Appliance ZS5-ES and Earlier Models

While the storage repository on the internal Oracle ZFS Storage Appliance ZS5-ES and earlier models can be used for a basic virtualized environment and for test purposes, the preferred approach for production environments is to attach additional external storage for use within Oracle VM. The options to extend the storage capacity of an Oracle Private Cloud Appliance are explained in detail in the *Oracle Private Cloud Appliance Installation Guide*: refer to the chapter entitled [Extending Oracle Private Cloud Appliance - Additional Storage](#).

Information on expanding your Oracle VM environment with storage repositories located on the external Fibre Channel or InfiniBand storage is provided in the *Oracle VM Manager User's Guide*. Refer to the section entitled [Storage Tab](#). 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 5.5 A view of the Storage tab (with Oracle ZFS Storage Appliance ZS5-ES)**



## 5.8 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 the section entitled [Tags](#).

You can also use this tab to generate XML reports about Oracle VM objects and attributes. For details, refer to the section entitled [Reports](#).

## 5.9 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.

## 5.10 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, especially 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.

### 5.10.1 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](#).

### 5.10.2 Create the Oracle VM Exporter Appliance Virtual Machine

1. Download the Oracle VM Exporter Appliance from the following location:  
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.

### 5.10.3 Configure the Oracle VM Exporter Appliance Virtual Machine

For additional information see [Configuring the Oracle VM Exporter Appliance Virtual Machine](#).

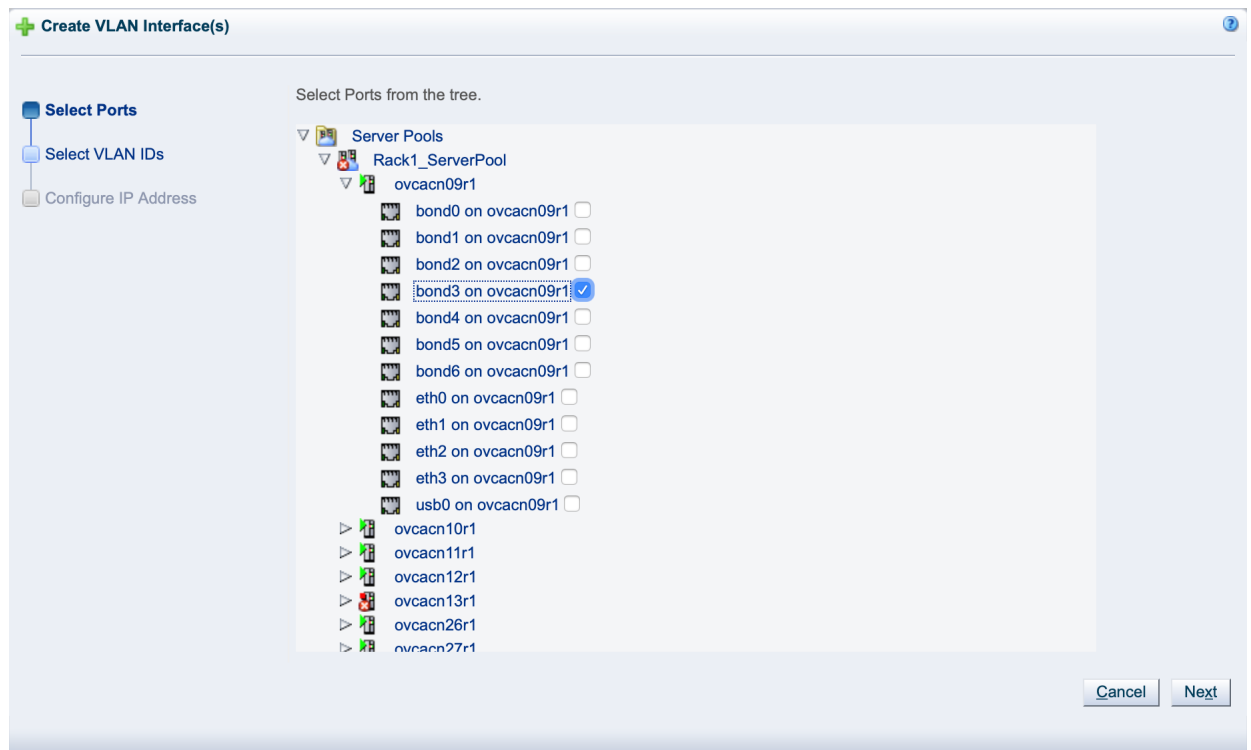
1. Log in to the [Oracle VM Manager web interface](#) of your Oracle Private Cloud Appliance.
2. Create a VLAN. From the Networking tab, select VLAN interfaces, then click the Create VLAN interface icon.
  - For Infiniband-based systems, use `bond3` on either compute node.
  - For Ethernet-based systems, use `vx2` interface on either compute node.
  - Click Next once you select a port.



#### Note

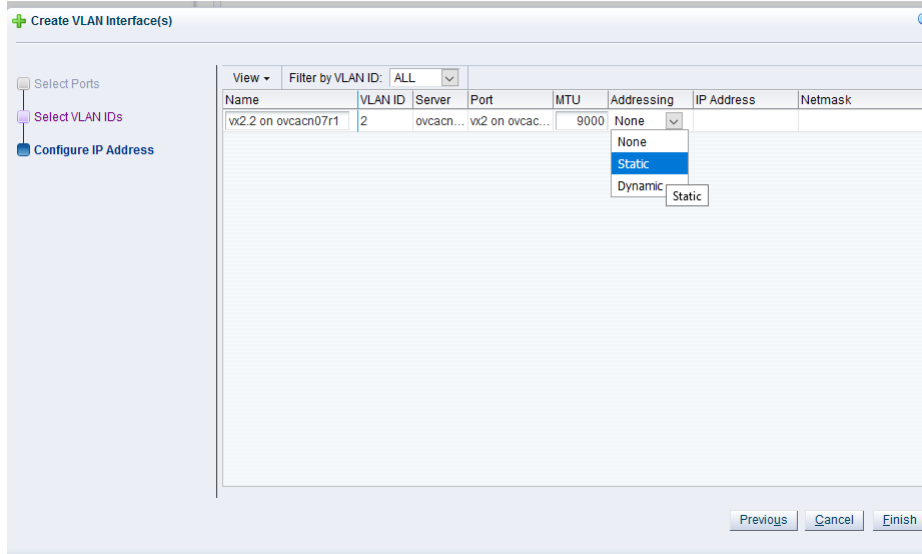
Ethernet-based systems can have NFS shares created on the internal ZFS storage appliance using VM Storage Networks for the Oracle VM Exporter Appliance *nfs share path*. The corresponding VM Storage network must be added to the Exporter Appliance for mounting the nfs share created on the internal ZFS storage appliance.

**Figure 5.6 Creating a VLAN**



3. Select a VLAN ID and click Next.
4. Choose static from the Addressing column, assign an IP Address and Netmask, then click Finish.

**Figure 5.7 Selecting a VLAN**

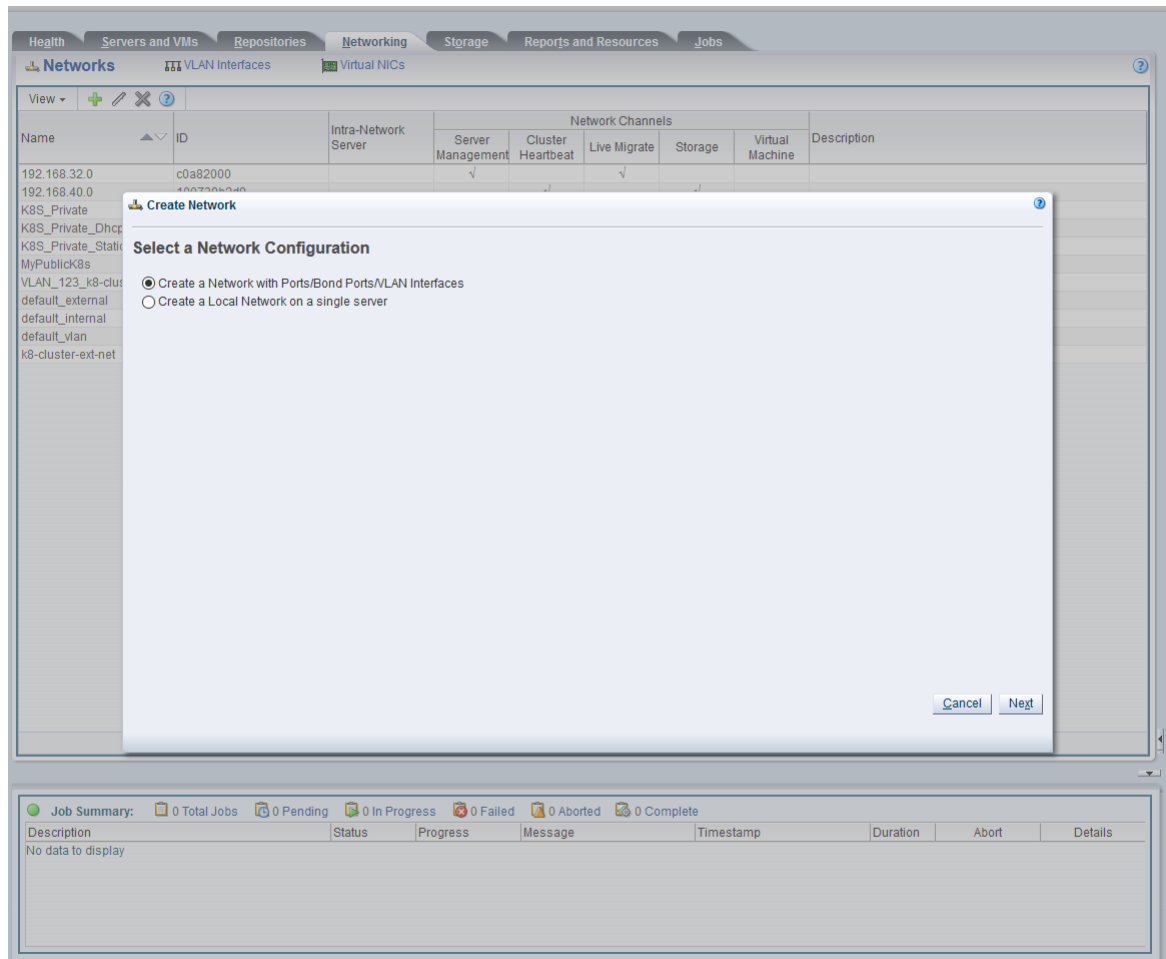


#### 5.10.4 Create a Network for the Oracle VM Exporter Appliance VM

This section describes Oracle Private Cloud Appliance specific considerations to export a VM created on Rack1-Repository.

1. From the Networking tab, select Networks, then click the Create New Network icon.

Figure 5.8 Create a Network



2. Select Create a Network with Port/Bonds Ports/VLAN interfaces, and click Next.

3. Enter the network name, select Virtual Machine for Network Uses, and click Next.

**Figure 5.9 Create a Network**

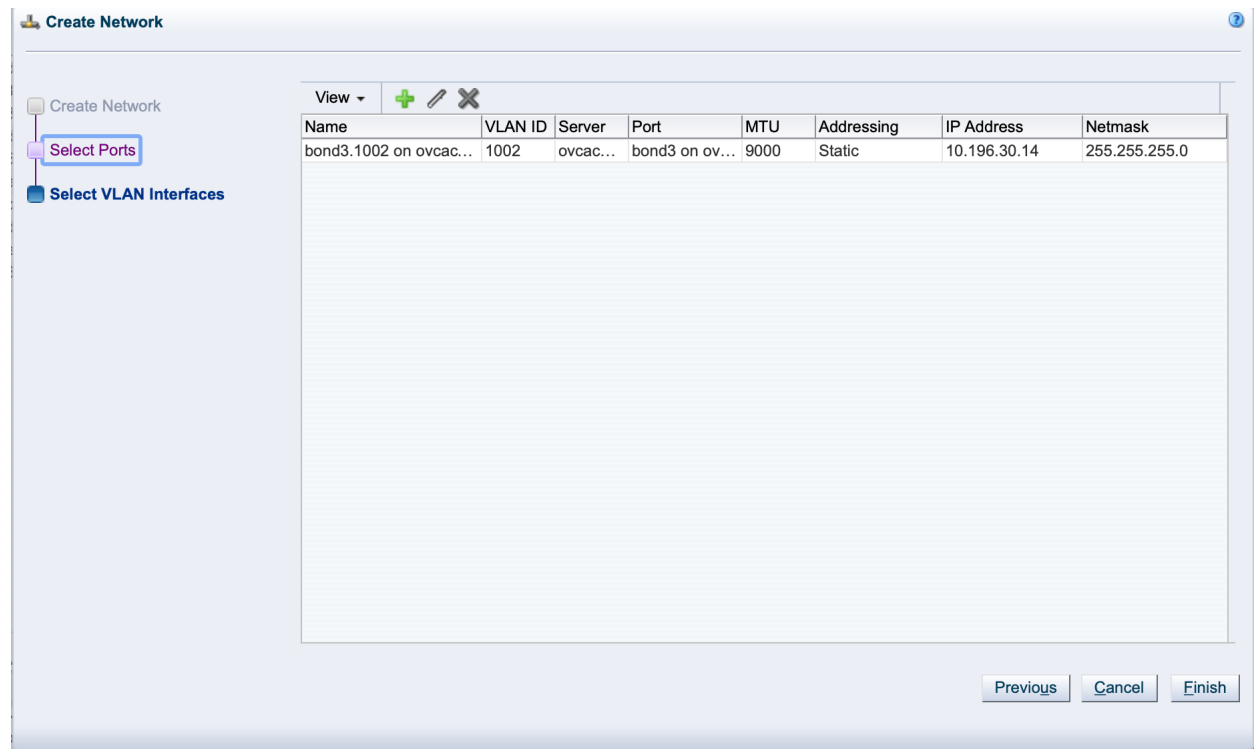
The screenshot shows a 'Create Network' wizard window. On the left, a vertical navigation pane contains three steps: 'Create Network' (selected), 'Select Ports', and 'Select VLAN Interfaces'. The main area is titled 'Enter Network Name and Use.' and contains the following fields and options:

- \* Name:** A text input field containing 'ServiceVMOnly'.
- Description:** A large empty text area.
- Network Uses:** A list of radio buttons with the following options:
  - Management
  - Live Migrate
  - Cluster Heartbeat
  - Virtual Machine
  - Storage

At the bottom right of the window, there are two buttons: 'Cancel' and 'Next'.

4. Select the VLAN interface you just created, then click Finish.

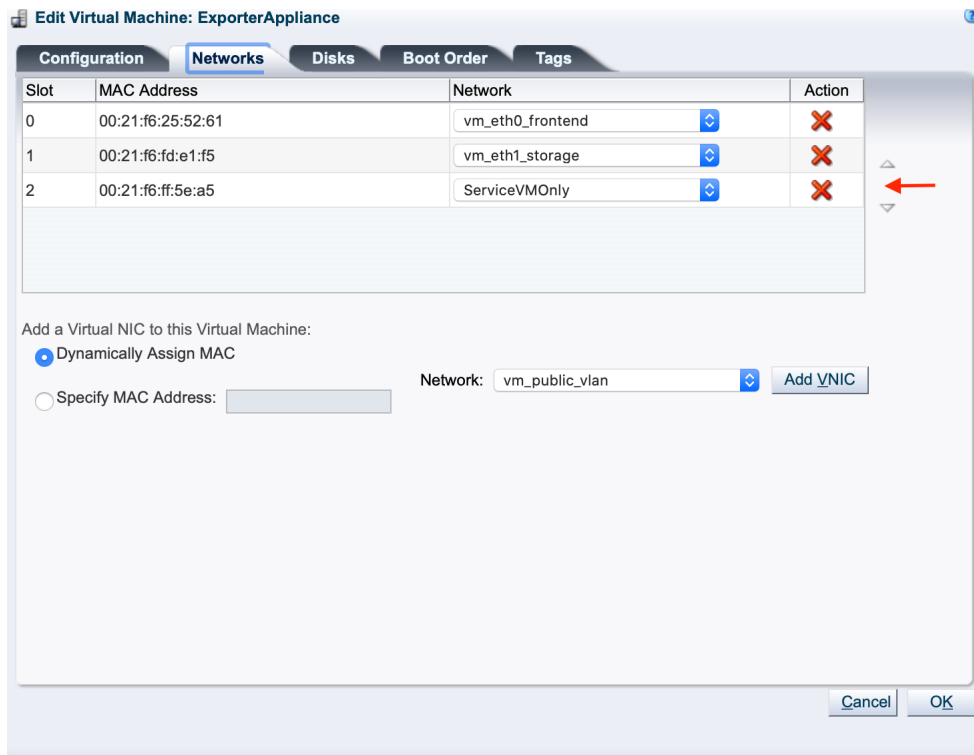
**Figure 5.10 Select Network Ports**



### 5.10.5 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 5.11 Select Network Ports**



3. Manually assign an IP address to the *ServiceVMOnly* interface on the Exporter Appliance that is from the same subnet as the VLAN interface you created earlier.

### 5.10.6 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 exports 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





---

# Chapter 6 Servicing Oracle Private Cloud Appliance Components

## Table of Contents

6.1 Oracle Auto Service Request (ASR) .....	230
6.1.1 Understanding Oracle Auto Service Request (ASR) .....	230
6.1.2 ASR Prerequisites .....	231
6.1.3 Setting Up ASR and Activating ASR Assets .....	232
6.2 Replaceable Components .....	232
6.2.1 Rack Components .....	232
6.2.2 Oracle Server X8-2 Components .....	233
6.2.3 Oracle Server X7-2 Components .....	234
6.2.4 Oracle Server X6-2 Components .....	235
6.2.5 Oracle Server X5-2 Components .....	236
6.2.6 Sun Server X4-2 Components .....	237
6.2.7 Sun Server X3-2 Components .....	238
6.2.8 Oracle ZFS Storage Appliance ZS7-2 Components .....	238
6.2.9 Oracle ZFS Storage Appliance ZS5-ES Components .....	240
6.2.10 Oracle ZFS Storage Appliance ZS3-ES Components .....	241
6.2.11 Sun ZFS Storage Appliance 7320 Components .....	242
6.2.12 Oracle Switch ES1-24 Components .....	243
6.2.13 NM2-36P Sun Datacenter InfiniBand Expansion Switch Components .....	244
6.2.14 Oracle Fabric Interconnect F1-15 Components .....	244
6.3 Preparing Oracle Private Cloud Appliance for Service .....	245
6.4 Servicing the Oracle Private Cloud Appliance Rack System .....	246
6.4.1 Powering Down Oracle Private Cloud Appliance (When Required) .....	246
6.4.2 Service Procedures for Rack System Components .....	247
6.5 Servicing an Oracle Server X8-2 .....	248
6.5.1 Powering Down Oracle Server X8-2 for Service (When Required) .....	248
6.5.2 Service Procedures for Oracle Server X8-2 Components .....	250
6.6 Servicing an Oracle Server X7-2 .....	250
6.6.1 Powering Down Oracle Server X7-2 for Service (When Required) .....	250
6.6.2 Service Procedures for Oracle Server X7-2 Components .....	252
6.7 Servicing an Oracle Server X6-2 .....	252
6.7.1 Powering Down Oracle Server X6-2 for Service (When Required) .....	253
6.7.2 Service Procedures for Oracle Server X6-2 Components .....	254
6.8 Servicing an Oracle Server X5-2 .....	255
6.8.1 Powering Down Oracle Server X5-2 for Service (When Required) .....	255
6.8.2 Service Procedures for Oracle Server X5-2 Components .....	256
6.9 Servicing a Sun Server X4-2 .....	257
6.9.1 Powering Down Sun Server X4-2 for Service (When Required) .....	257
6.9.2 Service Procedures for Sun Server X4-2 Components .....	259
6.10 Servicing a Sun Server X3-2 .....	260
6.10.1 Powering Down Sun Server X3-2 for Service (When Required) .....	260
6.10.2 Service Procedures for Sun Server X3-2 Components .....	261
6.11 Servicing the Oracle ZFS Storage Appliance ZS7-2 .....	262
6.11.1 Powering Down the Oracle ZFS Storage Appliance ZS7-2 for Service (When Required) ....	262
6.11.2 Service Procedures for Oracle ZFS Storage Appliance ZS7-2 Components .....	264
6.12 Servicing the Oracle ZFS Storage Appliance ZS5-ES .....	265
6.12.1 Powering Down the Oracle ZFS Storage Appliance ZS5-ES for Service (When Required) .	265
6.12.2 Service Procedures for Oracle ZFS Storage Appliance ZS5-ES Components .....	266

6.13 Servicing the Oracle ZFS Storage Appliance ZS3-ES .....	267
6.13.1 Powering Down the Oracle ZFS Storage Appliance ZS3-ES for Service (When Required) .	268
6.13.2 Service Procedures for Oracle ZFS Storage Appliance ZS3-ES Components .....	270
6.14 Servicing the Sun ZFS Storage Appliance 7320 .....	271
6.14.1 Powering Down the Sun ZFS Storage Appliance 7320 for Service (When Required) .....	271
6.14.2 Service Procedures for Sun ZFS Storage Appliance 7320 Components .....	272
6.15 Servicing an Oracle Switch ES1-24 .....	273
6.15.1 Powering Down the Oracle Switch ES1-24 for Service (When Required) .....	273
6.15.2 Service Procedures for Oracle Switch ES1-24 Components .....	274
6.16 Servicing an NM2-36P Sun Datacenter InfiniBand Expansion Switch .....	274
6.16.1 Powering Down the NM2-36P Sun Datacenter InfiniBand Expansion Switch for Service (When Required) .....	274
6.16.2 Service Procedures for NM2-36P Sun Datacenter InfiniBand Expansion Switch Components .....	275
6.17 Servicing an Oracle Fabric Interconnect F1-15 .....	275
6.17.1 Powering Down the Oracle Fabric Interconnect F1-15 for Service (When Required) .....	275
6.17.2 Service Procedures for Oracle Fabric Interconnect F1-15 Components .....	276
6.18 Servicing a Cisco Nexus 9336C-FX2 Switch .....	277
6.18.1 Powering Down the Cisco Nexus 9336C-FX2 Switch for Service (When Required) .....	277
6.18.2 Service Procedures for Cisco Nexus 9336C-FX2 Switch Components .....	277
6.19 Servicing a Cisco Nexus 9348GC-FXP Switch .....	278
6.19.1 Powering Down the Cisco Nexus 9348GC-FXP Switch for Service (When Required) .....	278
6.19.2 Service Procedures for Cisco Nexus 9348GC-FXP Switch Components .....	278

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 malfunction. Certain components of Oracle Private Cloud Appliance are customer-replaceable. These are listed in this chapter, along with the necessary instructions.

## 6.1 Oracle Auto Service Request (ASR)

Oracle Private Cloud Appliance is qualified for Oracle Auto Service Request (ASR), a software feature for support purposes. It is integrated with My Oracle Support and helps resolve problems faster by automatically opening service requests when specific hardware failures occur. Using ASR is optional: the components must be downloaded, installed and configured in order to enable ASR for your appliance.



### Caution

Oracle Auto Service Request (ASR) must be installed by an **authorized Oracle Field Engineer**. Request installation of ASR at the time of system install. Installation at a later date will be a Time and Materials charge.

Oracle is continuously analyzing and improving the ASR fault rules to enhance the Oracle support experience. This includes adding, modifying and removing rules to focus on actionable events from ASR assets while filtering non-actionable events. For up-to-date fault coverage details, please refer to the [Oracle Auto Service Request documentation page](#).

### 6.1.1 Understanding Oracle Auto Service Request (ASR)

To enable the automated service request feature, the Oracle Private Cloud Appliance components must be configured to send hardware fault telemetry to the ASR Manager software. ASR Manager must be installed

on the master management node, which needs an active outbound Internet connection using HTTPS or an HTTPS proxy.

When a hardware problem is detected, ASR Manager submits a service request to Oracle Support Services. In many cases, Oracle Support Services can begin work on resolving the issue before the administrator is even aware the problem exists.

ASR detects faults in the most common hardware components, such as disks, fans, and power supplies, and automatically opens a service request when a fault occurs. ASR does not detect all possible hardware faults, and it is not a replacement for other monitoring mechanisms, such as SMTP and SNMP alerts, within the customer data center. It is a complementary mechanism that expedites and simplifies the delivery of replacement hardware. ASR should not be used for downtime events in high-priority systems. For high-priority events, contact Oracle Support Services directly.

An email message is sent to both the My Oracle Support email account and the technical contact for Oracle Private Cloud Appliance to notify them of the creation of the service request. A service request may not be filed automatically on some occasions. This can happen because of the unreliable nature of the SNMP protocol or a loss of connectivity to ASR Manager. Oracle recommends that customers continue to monitor their systems for faults and call Oracle Support Services if they do not receive notice that a service request has been filed automatically.

For more information about ASR, consult the following resources:

- Oracle Auto Service Request web page: <https://www.oracle.com/support/premier/auto-service-request.html>.
- Oracle Auto Service Request user documentation: [http://docs.oracle.com/cd/E37710\\_01/index.htm](http://docs.oracle.com/cd/E37710_01/index.htm).

## 6.1.2 ASR Prerequisites

Before you install ASR, make sure that the prerequisites in this section are met.

- Make sure that you have a valid My Oracle Support account.  
If necessary, create an account at <https://support.oracle.com>.
- Ensure that the following are set up correctly in My Oracle Support:
  - technical contact person at the customer site who is responsible for Oracle Private Cloud Appliance
  - valid shipping address at the customer site where the Oracle Private Cloud Appliance is located, so that parts are delivered to the site where they must be installed
- Make sure that Oracle Java - JDK 7 (1.7.0\_13 or later) or Oracle Java 8 (1.8.0\_25 or later) is installed on both management nodes in your Oracle Private Cloud Appliance. Check the version installed on the system by entering the following command at the Oracle Linux prompt: `java -version`.

If the installed version does not comply with the ASR prerequisites, download a compatible Java version, unpack the archive in `/opt/` and install it on both management nodes.



### Note

OpenJDK is not supported by ASR.

If necessary, you can download the latest version from the Java SE Downloads page: <http://www.oracle.com/technetwork/java/javase/downloads/>.

- Verify connectivity to the Internet using HTTPS.

For example, try `curl` to test whether you can access <https://support.oracle.com>.

### 6.1.3 Setting Up ASR and Activating ASR Assets

The necessary packages for ASR Manager must first be downloaded and stored in an installation directory that is accessible from both management nodes. For ASR Manager to work on Oracle Private Cloud Appliance, it must be installed on both management nodes, and failover must be configured so that the ASR Manager role is always fulfilled by the management node that also has the master role.

ASR Manager (ASRM) can be registered as a stand-alone ASRM, pointing directly to My Oracle Support, or as a relay to another ASRM in your network. Even if other systems at your site already use an ASRM, you can choose to register the Oracle Private Cloud Appliance ASRM as stand-alone. This means it communicates directly with the Oracle backend systems, which is the standard registration method.

The Oracle Private Cloud Appliance components that are qualified as ASR assets are the compute nodes and the ZFS Storage Appliance. The two management nodes must not be activated.

The ASR activation mechanism for compute nodes requires operations in two separate locations. First the compute node ILOMs are configured to send SNMP traps to the ASR Manager when a failure occurs. Then the ASR Manager is configured to recognize the ILOMs as assets and accept their input.

The ZFS Storage Appliance runs its own ASR Manager, and relays its ASR data to the Oracle backend systems through the outbound connection of the master management node. To achieve this, Oracle Private Cloud Appliance relies on the `tinyproxy` HTTP and HTTPS proxy daemon. ASR requires `tinyproxy` version 1.8.3 or later to be installed and properly configured on both management nodes.

Detailed installation and configuration instructions are available from My Oracle Support. Refer to the support note with [Doc ID 2560988.1](#).

## 6.2 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.

All CRUs and FRUs are listed and identified in this chapter, but the servicing instructions included in this Oracle Private Cloud Appliance Administrator's Guide are focused primarily on CRUs. For FRU replacement, please contact Oracle.

### 6.2.1 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/](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	FRU/CRU	Hot-Swap
<i>Oracle Rack Cabinet 1242:</i>		
Jumper Cable C13-C14, 2m	FRU	Yes
Ethernet Cable, Category 5/5E, 10ft, Black	FRU	Yes
Ethernet Cable, Category 5/5E, 10ft, Blue	FRU	Yes
Ethernet Cable, Shielded, Category 5E, 1m, Grey	FRU	Yes
Ethernet Cable, Category 5, 8ft, Black	FRU	Yes
Ethernet Cable, Category 5, 8ft, Green	FRU	Yes
Ethernet Cable, Category 5, 8ft, Yellow	FRU	Yes
Active Optical Cable, Blue, 3m	FRU	Yes
10Gbps QSFP to QSFP Cable, Passive Copper, 3m	FRU	Yes
QSFP28 Cable, 30AWG, Passive Copper, 3m	FRU	Yes
QSFP28 Cable, 30AWG, Passive Copper, 1m	FRU	Yes
1U/2U Screw-Mount Slide Rail Kit	FRU	
1U/2U Cable Management Arm (Snap-in)	FRU	
<i>Power Distribution Units (PDUs):</i>		
15KVA Single-Phase PDU, North America	FRU	Yes
15KVA Three-Phase PDU, North America	FRU	Yes
15KVA Three-Phase PDU, International	FRU	Yes
22KVA Single-Phase PDU, North America	FRU	Yes
22KVA Single-Phase PDU, International	FRU	Yes
24KVA Three-Phase PDU, North America	FRU	Yes
24KVA Three-Phase PDU, International	FRU	Yes

For rack-level component servicing instructions, see [Section 6.4, “Servicing the Oracle Private Cloud Appliance Rack System”](#).

## 6.2.2 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/](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 X8-2 Components**

Component Description	FRU/CRU	Hot-Swap
Motherboard Assembly	FRU	No
Quad Counter Rotating Fan Module	CRU	Yes
1-Slot PCI Express Riser Assembly	FRU	No
2-Slot PCI Express Riser Assembly	FRU	No
Type A266 800/1200 Watt AC Input Power Supply	FRU	Yes
Sixteen-core Intel Xeon G-5218 processor (2.3 GHz), 125W	FRU	No
Twenty-four-core Intel Xeon P-8260 processor (2.4 GHz), 165W	FRU	No
CPU Heatsink	FRU	No
2.5" Disk Cage Front Indicator Module	FRU	No
8-Slot 2.5" Disk Backplane Assembly	FRU	No
1.2TB - 10000 RPM SAS-3 Disk Assembly with 1 bracket	FRU	Yes
DDR4 DIMM, 32GB	FRU	No
DDR4 DIMM, 64GB	FRU	No
Dual port 100Gbps Ethernet PCI Express 3.0 Host Channel Adapter (CX-5) (only appliance with Ethernet-based network architecture)	FRU	No
Dual port 80Gbps InfiniBand QDR PCI Express 3.0 Host Channel Adapter M3 (CX-3) (only appliance with InfiniBand-based network architecture)	FRU	No
Dual port 32Gbps Fibre Channel PCI Express 3.0 Host Bus Adapter (optional component)	FRU	No
8-Port 12Gbps SAS-3 RAID PCI Express HBA	FRU	No
System Battery	CRU	No
Cable Kit	FRU	No

For Oracle Server X8-2 component servicing instructions, see [Section 6.5, "Servicing an Oracle Server X8-2"](#).

### 6.2.3 Oracle Server X7-2 Components

The following table lists the replaceable components of the Oracle Server X7-2 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/](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 X7-2 Components**

Component Description	FRU/CRU	Hot-Swap
Motherboard Assembly	FRU	No
Dual Counter Rotating Fan Module	CRU	Yes
1-Slot PCI Express Riser Assembly	FRU	No
2-Slot PCI Express Riser Assembly	FRU	No
A266 1200 Watt AC Input Power Supply	CRU	Yes
Twenty-four-core Intel Xeon P-8160 processor (2.1 GHz), 150W	FRU	No
CPU Heatsink	FRU	No
2.5" Disk Cage Front Indicator Module	FRU	No
4-Slot 2.5" Disk Backplane Assembly	FRU	No
1.2TB - 10000 RPM SAS Disk Assembly with 1 bracket	CRU	Yes
DDR4 DIMM	FRU	No
Dual port 80Gbps InfiniBand QDR PCI Express 3.0 Host Channel Adapter M3 (CX-3)	FRU	No
8-Port 12Gbps SAS-3 RAID PCI Express HBA	FRU	No
System Battery	CRU	No
Cable Kit	FRU	No

For Oracle Server X7-2 component servicing instructions, see [Section 6.6, "Servicing an Oracle Server X7-2"](#).

## 6.2.4 Oracle Server X6-2 Components

The following table lists the replaceable components of the Oracle Server X6-2 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/](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 Server X6-2 Components**

Component Description	FRU/CRU	Hot-Swap
System Board Assembly	FRU	No
Dual Counter Rotating Fan Module	CRU	Yes
1-Slot PCI Express Riser Assembly	FRU	No
2-Slot PCI Express Riser Assembly	FRU	No
A256 600 Watt AC Input Power Supply	CRU	Yes

Component Description	FRU/CRU	Hot-Swap
Twenty-two-core Intel Xeon processor E5-2699 v4 series (2.2 GHz), 145W	FRU	No
Pre-Greased CPU Heatsink	FRU	No
2.5" Disk Cage Front Indicator Module	FRU	No
4-Slot 2.5" Disk Backplane Assembly	FRU	No
1.2TB - 10000 RPM SAS Disk Assembly with 1 bracket	CRU	Yes
32GB DDR4-2400 Load Reduced DIMM	FRU	No
Dual port 80Gbps InfiniBand QDR PCI Express 3.0 Host Channel Adapter M3 (CX-3)	FRU	No
8GB USB 2.0 Flash Drive	FRU	No
8-Port 12Gbps SAS-3 RAID PCI Express HBA	FRU	No
1U/2U Remote Battery Assembly	CRU	No
Cable Kit	FRU	No

For Oracle Server X6-2 component servicing instructions, see [Section 6.7, "Servicing an Oracle Server X6-2"](#).

## 6.2.5 Oracle Server X5-2 Components

The following table lists the replaceable components of the Oracle Server X5-2 management and 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/](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 6.5 Replaceable Oracle Server X5-2 Components**

Component Description	FRU/CRU	Hot-Swap
System Board Assembly	FRU	No
Dual Counter Rotating Fan Module	CRU	Yes
1-Slot PCI Express Riser Assembly	FRU	No
2-Slot PCI Express Riser Assembly	FRU	No
A256 600 Watt AC Input Power Supply	CRU	Yes
Eighteen-core Intel Xeon processor E5-2699 v3 series (2.3 GHz), 145W	FRU	No
Pre-Greased CPU Heatsink	FRU	No
2.5" Disk Cage Front Indicator Module	FRU	No
4-Slot 2.5" Disk Backplane Assembly	FRU	No



Component Description	FRU/CRU	Hot-Swap
1.2TB - 10000 RPM SAS Disk Assembly with 1 bracket	CRU	Yes
32GB DDR4-2133 Load Reduced DIMM	FRU	No
Dual port 80Gbps InfiniBand QDR PCI Express 3.0 Host Channel Adapter M3 (CX-3)	FRU	No
8GB USB 2.0 Flash Drive	FRU	No
8-Port 12Gbps SAS-3 RAID PCI Express HBA	FRU	No
1U/2U Remote Battery Assembly	CRU	No
Cable Kit	FRU	No

For Oracle Server X5-2 component servicing instructions, see [Section 6.8, “Servicing an Oracle Server X5-2”](#).

## 6.2.6 Sun Server X4-2 Components

The following table lists the replaceable components of the Sun Server X4-2 management and 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/](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 6.6 Replaceable Sun Server X4-2 Components**

Component Description	FRU/CRU	Hot-Swap
System Board Assembly	FRU	No
Dual Counter Rotating Fan Module	CRU	Yes
1-Slot PCI Express Riser Assembly	FRU	No
2-Slot PCI Express Riser Assembly	FRU	No
A256 600 Watt AC Input Power Supply	CRU	Yes
2.6GHz Intel 8-core Xeon E5-2650, 95W	FRU	No
Pre-Greased CPU Heatsink	FRU	No
2.5" Disk Cage Front Indicator Module	FRU	No
4-Slot 2.5" Disk Backplane Assembly	FRU	No
1.2TB - 10000 RPM SAS Disk Assembly with 1 bracket	CRU	Yes
16GB DDR3-1600 DIMM, 1.35V	FRU	No
Dual port 80Gbps InfiniBand QDR PCI Express 3.0 Host Channel Adapter M3 (CX-3)	FRU	No
4GB USB 2.0 Flash Drive	FRU	No

Component Description	FRU/CRU	Hot-Swap
8-Port 6Gbps SAS-2 RAID PCI Express HBA, B4 ASIC	FRU	No
1U/2U Remote Battery Assembly	CRU	No
Cable Kit	FRU	No

For Sun Server X4-2 component servicing instructions, see [Section 6.9, “Servicing a Sun Server X4-2”](#).

## 6.2.7 Sun Server X3-2 Components

The following table lists the replaceable components of the Sun Server X3-2 management and 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/](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 6.7 Replaceable Sun Server X3-2 Components**

Component Description	FRU/CRU	Hot-Swap
System Board Assembly	FRU	No
Dual Counter Rotating Fan Module	CRU	Yes
1-Slot PCI Express Riser Assembly	FRU	No
2-Slot PCI Express Riser Assembly	FRU	No
A256 600 Watt AC Input Power Supply	CRU	Yes
2.2GHz Intel 8-core Xeon E5-2660, 95W	FRU	No
Pre-Greased CPU Heatsink	FRU	No
2.5" Disk Cage Front Indicator Module	FRU	No
4-Slot 2.5" Disk Backplane Assembly	FRU	No
900GB - 10000 RPM SAS Disk Assembly with 1 bracket	CRU	Yes
16GB DDR3-1600 DIMM, 1.35V	FRU	No
Dual 40Gbps InfiniBand 4x QDR PCI Express Low Profile Host Channel Adapter	FRU	No
4GB USB 2.0 Flash Drive	FRU	No
8-Port 6Gbps SAS-2 RAID PCI Express HBA, B4 ASIC	FRU	No
1U/2U Remote Battery Assembly	CRU	No

For Sun Server X3-2 component servicing instructions, see [Section 6.10, “Servicing a Sun Server X3-2”](#).

## 6.2.8 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/](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 6.8 Replaceable Oracle ZFS Storage Appliance ZS7-2 Components**

Component Description	FRU/CRU	Hot-Swap
<i>Oracle ZFS Storage Appliance ZS7-2 Storage Head:</i>		
2.3GHz Intel 18-Core Xeon G-6140, 140W	FRU	No
Pre-greased CPU Heatsink	FRU	No
64GB DDR4 DIMM	FRU	No
7.68TB SAS-3 Disk Assembly	CRU	Yes
1.2TB - 10000 RPM SAS-3 Disk Assembly	CRU	Yes
Fortville dual PCIe 40Gb Ethernet Adapter	FRU	No
2.5" Disk Cage Front Indicator Module	FRU	No
12-Slot 2.5" Disk Backplane Assembly	FRU	No
Interlock Cable, 125mm	FRU	No
Cable Kit	FRU	No
Dual Counter Rotating Fan Module	CRU	Yes
System Board Assembly	FRU	No
3V lithium coin cell battery	CRU	No
Type A266 800/1200 Watt AC Input Power Supply	CRU	Yes
Cluster Heartbeat Assembly	FRU	No
8-Port 12Gbps SAS HBA	CRU	No
4x4 Port 12Gbps SAS-3 PCI Express HBA	CRU	No
<i>Oracle Storage DE3-24C Disk Shelf:</i>		
580 Watt AC Input Power Supply	CRU	Yes
12Gbps SAS-3 I/O Controller Module	CRU	Yes
4RU Chassis Assembly with Midplane	FRU	No
36-Pin Mini SAS3 HD Cable, SFF-8644 to SFF-8644, 3M	FRU	Yes
DE3-24C Mounting Rail Kit	CRU	No
14TB - 7200 RPM SAS-3 Disk Drive Assembly	CRU	Yes
200GB SAS-3 Solid State Drive Assembly	CRU	Yes

For Oracle ZFS Storage Appliance ZS7-2 component servicing instructions, see [Section 6.11, "Servicing the Oracle ZFS Storage Appliance ZS7-2"](#).

## 6.2.9 Oracle ZFS Storage Appliance ZS5-ES Components

The following table lists the replaceable components of the Oracle ZFS Storage Appliance ZS5-ES.



### 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/](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 6.9 Replaceable Oracle ZFS Storage Appliance ZS5-ES Components**

Component Description	FRU/CRU	Hot-Swap
<i>Oracle ZFS Storage Appliance ZS5-ES Storage Head:</i>		
2.3GHz Intel 18-Core Xeon E5-2699 V3, 145W	FRU	No
Pre-greased CPU Heatsink	FRU	No
16GB DDR4-2133 DIMM	FRU	No
3.2TB SAS-3 Solid State Drive Assembly	CRU	Yes
1.2TB - 10000 RPM SAS-3 Disk Assembly	CRU	Yes
Dual 40Gbps InfiniBand 4x QDR PCI Express Low Profile Host Channel Adapter	FRU	No
2-Slot PCI Express Riser Assembly	FRU	No
1-Slot PCI Express Riser Assembly	FRU	No
2.5" Disk Cage Front Indicator Module	FRU	No
8-Slot 2.5" Disk Backplane Assembly	FRU	No
Interlock Cable, 125mm	FRU	No
Cable Kit	FRU	No
Dual Counter Rotating Fan Module	CRU	Yes
System Board Assembly	FRU	No
3V lithium coin cell battery	CRU	No
Type A256 600 Watt AC Input Power Supply	CRU	Yes
Cluster Heartbeat Assembly	FRU	No
8-Port 12Gbps SAS HBA	FRU	No
4x4 Port 12Gbps SAS-3 PCI Express HBA	FRU	No
<i>Oracle Storage DE3-24P Disk Shelf:</i>		
580 Watt AC Input Power Supply	FRU	Yes
12Gbps SAS-3 I/O Controller Module	FRU	Yes
2RU Chassis Assembly with Midplane	FRU	No
36-Pin Mini SAS3 HD Cable, SFF-8644 to SFF-8644, 3M	FRU	Yes

Component Description	FRU/CRU	Hot-Swap
DE3-24P Mounting Rail Kit	FRU	No
1.2TB - 10000 RPM SAS-3 Disk Drive Assembly	CRU	Yes
200GB SAS-3 Solid State Drive Assembly	CRU	Yes

For Oracle ZFS Storage Appliance ZS5-ES component servicing instructions, see [Section 6.12, “Servicing the Oracle ZFS Storage Appliance ZS5-ES”](#).

## 6.2.10 Oracle ZFS Storage Appliance ZS3-ES Components

The following table lists the replaceable components of the Oracle ZFS Storage Appliance ZS3-ES.



### 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/](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 6.10 Replaceable Oracle ZFS Storage Appliance ZS3-ES Components**

Component Description	FRU/CRU	Hot-Swap
<i>Oracle ZFS Storage Appliance ZS3-ES Storage Head:</i>		
2.1GHz Intel 8-Core Xeon E5-2658, 95W	FRU	No
Pre-greased CPU Heatsink	FRU	No
16GB DDR-1600 DIMM, 1.35V	FRU	No
1.6TB SAS Solid State Drive Assembly	CRU	Yes
900GB - 10000 RPM SAS Disk Assembly	CRU	Yes
Dual 40Gbps InfiniBand 4x QDR PCI Express Low Profile Host Channel Adapter	FRU	No
2-Slot PCI Express Riser Assembly	FRU	No
1-Slot PCI Express Riser Assembly	FRU	No
2.5" Disk Cage Front Indicator Module	FRU	No
4-Slot 2.5" Disk Backplane Assembly	FRU	No
Cable Kit	FRU	No
Dual Counter Rotating Fan Module	CRU	Yes
System Board Assembly	FRU	No
3V lithium coin cell battery	CRU	No
Type A256 600 Watt AC Input Power Supply	CRU	Yes
Cluster Heartbeat Assembly	FRU	No
8-Port 6Gbps SAS-2 RAID HBA	FRU	No
8-Port 6Gbps SAS-2 PCI Express HBA (LSI)	FRU	No

Component Description	FRU/CRU	Hot-Swap
<i>Oracle Storage DE2-24P Disk Shelf:</i>		
580 Watt AC Input Power Supply	FRU	Yes
6Gbps SAS-2 I/O Controller Module	FRU	Yes
2RU Chassis Assembly with Midplane	FRU	No
4X Mini SAS Cable, SFF-8088 to SFF-8088, 2M	FRU	Yes
DE2-24P Mounting Rail Kit	FRU	No
900GB 10000 RPM SAS Disk Drive Assembly	CRU	Yes
200GB SAS Solid State Drive Assembly	CRU	Yes

For Oracle ZFS Storage Appliance ZS3-ES component servicing instructions, see [Section 6.13, “Servicing the Oracle ZFS Storage Appliance ZS3-ES”](#).

## 6.2.11 Sun ZFS Storage Appliance 7320 Components

The following table lists the replaceable components of the Sun ZFS Storage Appliance 7320.



### 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/](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 6.11 Replaceable Sun ZFS Storage Appliance 7320 Components**

Component Description	FRU/CRU	Hot-Swap
<i>Sun ZFS 7320 Storage Head:</i>		
2.4GHz Intel Quad-Core Xeon E5620, 12MB, 80W	FRU	No
Xeon Heatsink	FRU	No
8GB Registered DDR3L-1333/DDR3L-1600 DIMM, 1.35V	FRU	No
512GB Solid State Drive SATA-2 Assembly	CRU	Yes
500GB - 10000 RPM SATA Disk Assembly with 1 bracket	CRU	Yes
USB Assembly	FRU	Yes
Dual 40Gbps InfiniBand 4x QDR PCI Express Low Profile Host Channel Adapter	FRU	No
4GB USB 2.0 Flash Drive	FRU	No
1-Slot x8 PCI Express Riser Assembly	FRU	No
1-Slot x16 PCI Express Riser Assembly	FRU	No
Power Distribution Board	FRU	No
8-Slot Disk Backplane, SATA DVD	FRU	No
PDB to System Board Ribbon Cable	FRU	

Component Description	FRU/CRU	Hot-Swap
SFF8087 to SFF8087 Mini-SAS Cable, 690mm	FRU	
6-Pin Fan Power Cable	FRU	
Fan Data Ribbon Cable	FRU	
Bus Bar Set	FRU	
Fan Board Assembly	FRU	
Connector Board Assembly, SATA DVD	FRU	
Fan Module	CRU	Yes
System Board Assembly	FRU	No
3V Lithium Coin Cell Battery	FRU	No
Type A247A 760 Watt AC Input Power Supply	CRU	Yes
Cluster Heartbeat Assembly	FRU	
8-Port 6Gbps SAS-2 RAID HBA	FRU	No
<i>Oracle Storage DE2-24P Disk Shelf:</i>		
580 Watt AC Input Power Supply	CRU	Yes
6Gbps SAS-2 I/O Controller Module	FRU	Yes
2RU Chassis Assembly with Midplane	FRU	No
4X Mini SAS Cable, SFF-8088 to SFF-8088, 2M	FRU	
4X Mini SAS Cable, SFF-8088 to SFF-8088, 0.5M	FRU	
DE2-24P Mounting Rail Kit	FRU	
900GB 10000 RPM SAS Disk Drive Assembly	CRU	Yes
73GB SAS Solid State Drive Assembly	CRU	Yes

For Sun ZFS Storage Appliance 7320 component servicing instructions, see [Section 6.14, "Servicing the Sun ZFS Storage Appliance 7320"](#).

## 6.2.12 Oracle Switch ES1-24 Components

The following table lists the replaceable components of the Oracle Switch ES1-24.



### 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/](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 6.12 Replaceable Oracle Switch ES1-24 Components**

Component Description	FRU/CRU	Hot-Swap
24-Port ES1-24 Switch Assembly	FRU	No
Rear-to-Front Airflow Fan Module	CRU	Yes

Component Description	FRU/CRU	Hot-Swap
Type A247A 760 Watt AC Input Power Supply	CRU	Yes

For Oracle Switch ES1-24 component servicing instructions, see [Section 6.15, “Servicing an Oracle Switch ES1-24”](#).

## 6.2.13 NM2-36P Sun Datacenter InfiniBand Expansion Switch Components

The following table lists the replaceable components of the Sun Datacenter InfiniBand Expansion Switch NM2-36P.



### 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/](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 6.13 Replaceable NM2-36P Sun Datacenter InfiniBand Expansion Switch Components**

Component Description	FRU/CRU	Hot-Swap
Datacenter InfiniBand Switch 36 Subassembly	FRU	No
Type A247A 760 Watt AC Input Power Supply	CRU	Yes
Rear-to-Front Airflow Fan Module	CRU	Yes

For NM2-36P Sun Datacenter InfiniBand Expansion Switch component servicing instructions, see [Section 6.16, “Servicing an NM2-36P Sun Datacenter InfiniBand Expansion Switch”](#).

## 6.2.14 Oracle Fabric Interconnect F1-15 Components

The following table lists the replaceable components of the Oracle Fabric Interconnect F1-15.



### 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/](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 6.14 Replaceable Oracle Fabric Interconnect F1-15 Components**

Component Description	FRU/CRU	Hot-Swap
F1-15 Power Supply	FRU	Yes
QDR Fabric Board	FRU	No
2U/4U Front Panel G2 (Com-X i7)	FRU	No



Component Description	FRU/CRU	Hot-Swap
F1-15 I/O Management Module	FRU	No
F1-15 Fan Tray	FRU	Yes
Quad Port 10 Gigabit Ethernet (GbE) Module	FRU	Yes
Dual Port 2 × 8 Gigabit Fibre Channel I/O Module	FRU	Yes
F1-15 Chassis without Power Supply, Fan, Fabric Board, Front Panel	FRU	No

For Oracle Fabric Interconnect F1-15 component servicing instructions, see [Section 6.17, “Servicing an Oracle Fabric Interconnect F1-15”](#).

## 6.3 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 \(E88194-02\)](#)
- Follow the safety guidelines described in the [Oracle Private Cloud Appliance Installation Guide \(F28397-01\)](#):
  - [Electrical Power Requirements](#)
  - [Rack-mount Safety Precautions](#)
- 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)

## 6.4 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 [Section 6.3, “Preparing Oracle Private Cloud Appliance for Service”](#).

### 6.4.1 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 master 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.

## 6.4.2 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 6.15 Service Instructions for Rack System Components**

Replaceable Part(s)	Hot-Swap	Instructions
Power cables		
Ethernet cables		
Cable management arms (CMAs)  (Oracle-qualified service technician only)		<p>For removal and installation of a cable management arm, refer to the <a href="#">Oracle Server X8-2 Installation Guide (part no. E93391)</a>.</p> <ul style="list-style-type: none"> <li>• “Remove the Cable Management Arm”</li> <li>• “Install the Cable Management Arm”</li> </ul>
Slide rails  (Oracle-qualified service technician only)		<p>To service the slide rails, the server must be removed from the rack. For instructions, refer to the <a href="#">Oracle Server X8-2 Service Manual (part no. E93386)</a>.</p> <ul style="list-style-type: none"> <li>• “Remove the Server From the Rack”</li> <li>• “Reinstall the Server Into the Rack”</li> </ul> <p>For slide rail installation instructions, refer to the section <a href="#">Attach the Slide-Rails</a> in the <a href="#">Oracle Server X8-2 Installation Guide (part no. E93391)</a>. To remove the slide rails, reverse the installation steps.</p>

## 6.5 Servicing an Oracle Server X8-2

This section provides instructions to service replaceable components (CRUs/FRUs) in an Oracle Server X8-2 compute node. Before starting any service procedure, read and follow the guidelines in [Section 6.3, “Preparing Oracle Private Cloud Appliance for Service”](#).

### 6.5.1 Powering Down Oracle Server X8-2 for Service (When Required)

If you need to execute a service procedure that requires the Oracle Server X8-2 to be powered down, follow these instructions:

#### Placing a compute node into maintenance mode

Before an Oracle Server X8-2 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 “[Section 5.2, “Logging in to the Oracle VM Manager Web UI”](#)” in the [Oracle Private Cloud Appliance Administrator's Guide](#).

- 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 Oracle Server X8-2 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 the chapter “[Preparing for Service](#)” in the [Oracle Server X8-2 Service Manual \(part no. E93386\)](#).

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 and data cables from the server.
4. Extend the server to the maintenance position.
5. Most service operations can be performed while the server is in the maintenance position.

However, if necessary, remove the cable management arm (CMA) and pull the server out of the rack.



#### Caution

The server weighs approximately 15.9 kg (35.0 lb). Two people are required to dismount and carry the chassis.

### Returning the system to operation

These steps briefly describe the procedure. For detailed instructions, refer to the chapter “[Returning the Server to Operation](#)” in the [Oracle Server X8-2 Service Manual \(part no. E93386\)](#).

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.

## 6.5.2 Service Procedures for Oracle Server X8-2 Components

For parts that are not hot-swappable, power down the Oracle Server X8-2 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 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 6.16 Service Procedures for Oracle Server X8-2 Components**

Replaceable Part(s)	Hot-Swap	URL
Storage drives	Yes	<a href="https://docs.oracle.com/cd/E93359_01/html/E93386/gquak.html#scrolltoc">https://docs.oracle.com/cd/E93359_01/html/E93386/gquak.html#scrolltoc</a>
Fan Modules	Yes	<a href="https://docs.oracle.com/cd/E93359_01/html/E93386/gquhg.html#scrolltoc">https://docs.oracle.com/cd/E93359_01/html/E93386/gquhg.html#scrolltoc</a>
Power supplies	Yes	<a href="https://docs.oracle.com/cd/E93359_01/html/E93386/gqunc.html#scrolltoc">https://docs.oracle.com/cd/E93359_01/html/E93386/gqunc.html#scrolltoc</a>
DIMMs (Oracle-qualified service technician only)	No	<a href="https://docs.oracle.com/cd/E93359_01/html/E93386/gqvkr.html#scrolltoc">https://docs.oracle.com/cd/E93359_01/html/E93386/gqvkr.html#scrolltoc</a>
PCI Express risers (Oracle-qualified service technician only)	No	<a href="https://docs.oracle.com/cd/E93359_01/html/E93386/gqvft.html#scrolltoc">https://docs.oracle.com/cd/E93359_01/html/E93386/gqvft.html#scrolltoc</a>
PCI Express cards (Oracle-qualified service technician only)	No	<a href="https://docs.oracle.com/cd/E93359_01/html/E93386/gqvjk.html#scrolltoc">https://docs.oracle.com/cd/E93359_01/html/E93386/gqvjk.html#scrolltoc</a>
Battery	No	<a href="https://docs.oracle.com/cd/E93359_01/html/E93386/gqviw.html#scrolltoc">https://docs.oracle.com/cd/E93359_01/html/E93386/gqviw.html#scrolltoc</a>

## 6.6 Servicing an Oracle Server X7-2

This section provides instructions to service replaceable components (CRUs/FRUs) in an Oracle Server X7-2 compute node. Before starting any service procedure, read and follow the guidelines in [Section 6.3, "Preparing Oracle Private Cloud Appliance for Service"](#).

### 6.6.1 Powering Down Oracle Server X7-2 for Service (When Required)

If you need to execute a service procedure that requires the Oracle Server X7-2 to be powered down, follow these instructions:

#### Placing a compute node into maintenance mode

Before an Oracle Server X7-2 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 “[Section 5.2, “Logging in to the Oracle VM Manager Web UI”](#)” in the [Oracle Private Cloud Appliance Administrator's Guide](#).

- 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 Oracle Server X7-2 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 the chapter “[Preparing for Service](#)” in the [Oracle Server X7-2 Service Manual \(part no. E72445\)](#).

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 and data cables from the server.
4. Extend the server to the maintenance position.
5. Most service operations can be performed while the server is in the maintenance position.

However, if necessary, remove the cable management arm (CMA) and pull the server out of the rack.



#### Caution

The server weighs approximately 15.9 kg (35.0 lb). Two people are required to dismount and carry the chassis.

### Returning the system to operation

These steps briefly describe the procedure. For detailed instructions, refer to the chapter “[Returning the Server to Operation](#)” in the [Oracle Server X7-2 Service Manual \(part no. E72445\)](#).

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.

## 6.6.2 Service Procedures for Oracle Server X7-2 Components

For parts that are not hot-swappable, power down the Oracle Server X7-2 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 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 6.17 Service Procedures for Oracle Server X7-2 Components**

Replaceable Part(s)	Hot-Swap	URL
Storage drives	Yes	<a href="http://docs.oracle.com/cd/E72435_01/html/E72445/gquak.html#scrolltoc">http://docs.oracle.com/cd/E72435_01/html/E72445/gquak.html#scrolltoc</a>
Fan Modules	Yes	<a href="http://docs.oracle.com/cd/E72435_01/html/E72445/gquhg.html#scrolltoc">http://docs.oracle.com/cd/E72435_01/html/E72445/gquhg.html#scrolltoc</a>
Power supplies	Yes	<a href="http://docs.oracle.com/cd/E72435_01/html/E72445/gqunc.html#scrolltoc">http://docs.oracle.com/cd/E72435_01/html/E72445/gqunc.html#scrolltoc</a>
DIMMs (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E72435_01/html/E72445/gqvkr.html#scrolltoc">http://docs.oracle.com/cd/E72435_01/html/E72445/gqvkr.html#scrolltoc</a>
PCI Express risers (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E72435_01/html/E72445/gqvft.html#scrolltoc">http://docs.oracle.com/cd/E72435_01/html/E72445/gqvft.html#scrolltoc</a>
PCI Express cards (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E72435_01/html/E72445/gqvjk.html#scrolltoc">http://docs.oracle.com/cd/E72435_01/html/E72445/gqvjk.html#scrolltoc</a>
Battery	No	<a href="http://docs.oracle.com/cd/E72435_01/html/E72445/gqviw.html#scrolltoc">http://docs.oracle.com/cd/E72435_01/html/E72445/gqviw.html#scrolltoc</a>

## 6.7 Servicing an Oracle Server X6-2

This section provides instructions to service replaceable components (CRUs/FRUs) in an Oracle Server X6-2 compute node. Before starting any service procedure, read and follow the guidelines in [Section 6.3, "Preparing Oracle Private Cloud Appliance for Service"](#).



## 6.7.1 Powering Down Oracle Server X6-2 for Service (When Required)

If you need to execute a service procedure that requires the Oracle Server X6-2 to be powered down, follow these instructions:

### Placing a compute node into maintenance mode

Before an Oracle Server X6-2 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 “[Section 5.2, “Logging in to the Oracle VM Manager Web UI”](#)” in the [Oracle Private Cloud Appliance Administrator's Guide](#).

- 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 Oracle Server X6-2 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 the chapter “[Preparing for Service](#)” in the [Oracle Server X6-2 Service Manual \(part no. E62171\)](#).

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

System data may become corrupted during an immediate power down. Use this task only after attempting to power down the server gracefully.

3. Disconnect the power cables and data cables from the server.
4. Extend the server to the maintenance position.
5. Most service operations can be performed while the server is in the maintenance position.

However, if necessary, remove the cable management arm (CMA) and pull the server out of the rack.



### Caution

The server weighs approximately 18.1 kg (39.9 lb). Two people are required to dismount and carry the chassis.

### Returning the system to operation

These steps briefly describe the procedure. For detailed instructions, refer to the chapter “[Returning the Server to Operation](#)” in the [Oracle Server X6-2 Service Manual \(part no. E62171\)](#).

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.

## 6.7.2 Service Procedures for Oracle Server X6-2 Components

For parts that are not hot-swappable, power down the Oracle Server X6-2 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 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 6.18 Service Procedures for Oracle Server X6-2 Components**

Replaceable Part(s)	Hot-Swap	URL
Storage drives	Yes	<a href="http://docs.oracle.com/cd/E62159_01/html/E62171/z40000091011460.html#scrolltoc">http://docs.oracle.com/cd/E62159_01/html/E62171/z40000091011460.html#scrolltoc</a>
Fan Modules	Yes	<a href="http://docs.oracle.com/cd/E62159_01/html/E62171/z40000091014194.html#scrolltoc">http://docs.oracle.com/cd/E62159_01/html/E62171/z40000091014194.html#scrolltoc</a>
Power supplies	Yes	<a href="http://docs.oracle.com/cd/E62159_01/html/E62171/z40000091014153.html#scrolltoc">http://docs.oracle.com/cd/E62159_01/html/E62171/z40000091014153.html#scrolltoc</a>
DIMMs (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E62159_01/html/E62171/z40003f01425075.html#scrolltoc">http://docs.oracle.com/cd/E62159_01/html/E62171/z40003f01425075.html#scrolltoc</a>
PCI Express risers (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E62159_01/html/E62171/z40000f91037394.html#scrolltoc">http://docs.oracle.com/cd/E62159_01/html/E62171/z40000f91037394.html#scrolltoc</a>

Replaceable Part(s)	Hot-Swap	URL
PCI Express cards  (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E62159_01/html/E62171/z40000f91037409.html#scrolltoc">http://docs.oracle.com/cd/E62159_01/html/E62171/z40000f91037409.html#scrolltoc</a>
Internal USB flash drives  (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E62159_01/html/E62171/z4000a6d1442801.html#scrolltoc">http://docs.oracle.com/cd/E62159_01/html/E62171/z4000a6d1442801.html#scrolltoc</a>
Battery	No	<a href="http://docs.oracle.com/cd/E62159_01/html/E62171/z40003f01423753.html#scrolltoc">http://docs.oracle.com/cd/E62159_01/html/E62171/z40003f01423753.html#scrolltoc</a>

## 6.8 Servicing an Oracle Server X5-2

This section provides instructions to service replaceable components (CRUs/FRUs) in an Oracle Server X5-2 management node or compute node. Before starting any service procedure, read and follow the guidelines in [Section 6.3, “Preparing Oracle Private Cloud Appliance for Service”](#).

### 6.8.1 Powering Down Oracle Server X5-2 for Service (When Required)

If you need to execute a service procedure that requires the Oracle Server X5-2 to be powered down, follow these instructions:



#### Note

The management nodes are not placed in maintenance mode for servicing. If you need to power down the master management node, bring it offline as described below and wait for the other management node to take over the master role. If you need to power down the secondary management node, no additional steps are required.

#### Placing a compute node into maintenance mode

Before an Oracle Server X5-2 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 “[Section 5.2, “Logging in to the Oracle VM Manager Web UI”](#)” in the [Oracle Private Cloud Appliance Administrator's Guide](#).

- 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 Oracle Server X5-2 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 the chapter “[Preparing for Service](#)” in the [Oracle Server X5-2 Service Manual \(part no. E48320\)](#).

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

System data may become corrupted during an immediate power down. Use this task only after attempting to power down the server gracefully.

3. Disconnect the power cables and data cables from the server.
4. Extend the server to the maintenance position.
5. Most service operations can be performed while the server is in the maintenance position.

However, if necessary, remove the cable management arm (CMA) and pull the server out of the rack.



#### Caution

The server weighs approximately 18.1 kg (39.9 lb). Two people are required to dismount and carry the chassis.

### Returning the system to operation

These steps briefly describe the procedure. For detailed instructions, refer to the chapter “[Returning the Server to Operation](#)” in the [Oracle Server X5-2 Service Manual \(part no. E48320\)](#).

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.

## 6.8.2 Service Procedures for Oracle Server X5-2 Components

For parts that are not hot-swappable, power down the Oracle Server X5-2 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 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 6.19 Service Procedures for Oracle Server X5-2 Components**

Replaceable Part(s)	Hot-Swap	URL
Storage drives	Yes	<a href="http://docs.oracle.com/cd/E41059_01/html/E48320/z40000091011460.html#scrolltoc">http://docs.oracle.com/cd/E41059_01/html/E48320/z40000091011460.html#scrolltoc</a>
Fan Modules	Yes	<a href="http://docs.oracle.com/cd/E41059_01/html/E48320/z40000091014194.html#scrolltoc">http://docs.oracle.com/cd/E41059_01/html/E48320/z40000091014194.html#scrolltoc</a>
Power supplies	Yes	<a href="http://docs.oracle.com/cd/E41059_01/html/E48320/z40000091014153.html#scrolltoc">http://docs.oracle.com/cd/E41059_01/html/E48320/z40000091014153.html#scrolltoc</a>
DIMMs (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E41059_01/html/E48320/z40003f01425075.html#scrolltoc">http://docs.oracle.com/cd/E41059_01/html/E48320/z40003f01425075.html#scrolltoc</a>
PCI Express risers (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E41059_01/html/E48320/z40000f91037394.html#scrolltoc">http://docs.oracle.com/cd/E41059_01/html/E48320/z40000f91037394.html#scrolltoc</a>
PCI Express cards (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E41059_01/html/E48320/z40000f91037409.html#scrolltoc">http://docs.oracle.com/cd/E41059_01/html/E48320/z40000f91037409.html#scrolltoc</a>
Internal USB flash drives (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E41059_01/html/E48320/z4000a6d1442801.html#scrolltoc">http://docs.oracle.com/cd/E41059_01/html/E48320/z4000a6d1442801.html#scrolltoc</a>
Battery	No	<a href="http://docs.oracle.com/cd/E41059_01/html/E48320/z40003f01423753.html#scrolltoc">http://docs.oracle.com/cd/E41059_01/html/E48320/z40003f01423753.html#scrolltoc</a>

## 6.9 Servicing a Sun Server X4-2

This section provides instructions to service replaceable components (CRUs/FRUs) in a Sun Server X4-2 management node or compute node. Before starting any service procedure, read and follow the guidelines in [Section 6.3, “Preparing Oracle Private Cloud Appliance for Service”](#).

### 6.9.1 Powering Down Sun Server X4-2 for Service (When Required)

If you need to execute a service procedure that requires the Sun Server X4-2 to be powered down, follow these instructions:



**Note**

The management nodes are not placed in maintenance mode for servicing. If you need to power down the master management node, bring it offline as described

below and wait for the other management node to take over the master role. If you need to power down the secondary management node, no additional steps are required.

### Placing a compute node into maintenance mode

Before a Sun Server X4-2 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. For details, refer to the section “[Placing an Oracle VM Server into Maintenance Mode](#)” in the [Oracle VM Manager User's Guide](#).

1. Log in to the Oracle VM Manager Web UI.

For details, refer to the section “[Section 5.2, “Logging in to the Oracle VM Manager Web UI”](#)” in the [Oracle Private Cloud Appliance Administrator's Guide](#).

- 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 Sun Server X4-2 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 the chapter “[Preparing for Service](#)” in the [Sun Server X4-2 Service Manual \(part no. E38041\)](#).

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

System data may become corrupted during an immediate power down. Use this task only after attempting to power down the server gracefully.

3. Disconnect the power cables and data cables from the server.
4. Extend the server to the maintenance position.
5. Most service operations can be performed while the server is in the maintenance position.

However, if necessary, remove the cable management arm (CMA) and pull the server out of the rack.



### Caution

The server weighs approximately 18.1 kg (39.9 lb). Two people are required to dismount and carry the chassis.

### Returning the system to operation

These steps briefly describe the procedure. For detailed instructions, refer to the chapter “[Returning the Server to Operation](#)” in the [Sun Server X4-2 Service Manual \(part no. E38041\)](#).

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.

## 6.9.2 Service Procedures for Sun Server X4-2 Components

For parts that are not hot-swappable, power down the Sun Server X4-2 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 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 6.20 Service Procedures for Sun Server X4-2 Components**

Replaceable Part(s)	Hot-Swap	URL
Storage drives	Yes	<a href="http://docs.oracle.com/cd/E36975_01/html/E38045/z40000091011460.html#scrolltoc">http://docs.oracle.com/cd/E36975_01/html/E38045/z40000091011460.html#scrolltoc</a>
Fan Modules	Yes	<a href="http://docs.oracle.com/cd/E36975_01/html/E38045/z40000091014194.html#scrolltoc">http://docs.oracle.com/cd/E36975_01/html/E38045/z40000091014194.html#scrolltoc</a>
Power supplies	Yes	<a href="http://docs.oracle.com/cd/E36975_01/html/E38045/z40000091014153.html#scrolltoc">http://docs.oracle.com/cd/E36975_01/html/E38045/z40000091014153.html#scrolltoc</a>
DIMMs (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E36975_01/html/E38045/z40003f01425075.html#scrolltoc">http://docs.oracle.com/cd/E36975_01/html/E38045/z40003f01425075.html#scrolltoc</a>
PCI Express risers (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E36975_01/html/E38045/z40000f91037394.html#scrolltoc">http://docs.oracle.com/cd/E36975_01/html/E38045/z40000f91037394.html#scrolltoc</a>

Replaceable Part(s)	Hot-Swap	URL
PCI Express cards (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E36975_01/html/E38045/z40000f91037409.html#scrolltoc">http://docs.oracle.com/cd/E36975_01/html/E38045/z40000f91037409.html#scrolltoc</a>
Internal USB flash drives (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E36975_01/html/E38045/z4000a6d1442801.html#scrolltoc">http://docs.oracle.com/cd/E36975_01/html/E38045/z4000a6d1442801.html#scrolltoc</a>
Battery	No	<a href="http://docs.oracle.com/cd/E36975_01/html/E38045/z40003f01423753.html#scrolltoc">http://docs.oracle.com/cd/E36975_01/html/E38045/z40003f01423753.html#scrolltoc</a>

## 6.10 Servicing a Sun Server X3-2

This section provides instructions to service replaceable components (CRUs/FRUs) in a Sun Server X3-2 management node or compute node. Before starting any service procedure, read and follow the guidelines in [Section 6.3, “Preparing Oracle Private Cloud Appliance for Service”](#).

### 6.10.1 Powering Down Sun Server X3-2 for Service (When Required)

If you need to execute a service procedure that requires the Sun Server X3-2 to be powered down, follow these instructions:



#### Note

The management nodes are not placed in maintenance mode for servicing. If you need to power down the master management node, bring it offline as described below and wait for the other management node to take over the master role. If you need to power down the secondary management node, no additional steps are required.

#### Placing a compute node into maintenance mode

Before a Sun Server X3-2 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. For details, refer to the section “[Placing an Oracle VM Server into Maintenance Mode](#)” in the [Oracle VM Manager User's Guide](#).

1. Log in to the Oracle VM Manager Web UI.

For details, refer to the section “[Section 5.2, “Logging in to the Oracle VM Manager Web UI”](#)” in the [Oracle Private Cloud Appliance Administrator's Guide](#).

- 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 Sun Server X3-2 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 the chapter “[Preparing for Service](#)” in the [Sun Server X3-2 Service Manual \(part no. E22313\)](#).

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

System data may become corrupted during an immediate power down. Use this task only after attempting to power down the server gracefully.

3. Extend the server to the maintenance position.
4. Disconnect the power cables and data cables from the server.
5. Most service operations can be performed while the server is in the maintenance position.

However, if necessary, remove the cable management arm (CMA) and pull the server out of the rack.



#### Caution

The server weighs approximately 18.1 kg (39.9 lb). Two people are required to dismount and carry the chassis.

### Returning the system to operation

These steps briefly describe the procedure. For detailed instructions, refer to the chapter “[Returning the Server to Operation](#)” in the [Sun Server X3-2 Service Manual \(part no. E22313\)](#).

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. Reconnect data cables and power cords.
4. Return the server to its normal operational position in the rack, making sure the CMA is correctly installed.
5. Power on the server.

## 6.10.2 Service Procedures for Sun Server X3-2 Components

For parts that are not hot-swappable, power down the Sun Server X3-2 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 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 6.21 Service Procedures for Sun Server X3-2 Components**

Replaceable Part(s)	Hot-Swap	URL
Storage drives	Yes	<a href="http://docs.oracle.com/cd/E22368_01/html/E27242/z40000091011460.html#scrolltoc">http://docs.oracle.com/cd/E22368_01/html/E27242/z40000091011460.html#scrolltoc</a>
Fan Modules	Yes	<a href="http://docs.oracle.com/cd/E22368_01/html/E27242/z40000091014194.html#scrolltoc">http://docs.oracle.com/cd/E22368_01/html/E27242/z40000091014194.html#scrolltoc</a>
Power supplies	Yes	<a href="http://docs.oracle.com/cd/E22368_01/html/E27242/z40000091014153.html#scrolltoc">http://docs.oracle.com/cd/E22368_01/html/E27242/z40000091014153.html#scrolltoc</a>
DIMMs (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E22368_01/html/E27242/z40003f01425075.html#scrolltoc">http://docs.oracle.com/cd/E22368_01/html/E27242/z40003f01425075.html#scrolltoc</a>
PCI Express risers (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E22368_01/html/E27242/z40000f91037394.html#scrolltoc">http://docs.oracle.com/cd/E22368_01/html/E27242/z40000f91037394.html#scrolltoc</a>
PCI Express cards (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E22368_01/html/E27242/z40000f91037409.html#scrolltoc">http://docs.oracle.com/cd/E22368_01/html/E27242/z40000f91037409.html#scrolltoc</a>
Internal USB flash drives (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E22368_01/html/E27242/z4000a6d1442801.html#scrolltoc">http://docs.oracle.com/cd/E22368_01/html/E27242/z4000a6d1442801.html#scrolltoc</a>
Battery	No	<a href="http://docs.oracle.com/cd/E22368_01/html/E27242/z40003f01423753.html#scrolltoc">http://docs.oracle.com/cd/E22368_01/html/E27242/z40003f01423753.html#scrolltoc</a>

## 6.11 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 [Section 6.3, “Preparing Oracle Private Cloud Appliance for Service”](#).

### 6.11.1 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.



#### 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.

## 6.11.2 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.



**Warning**

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 6.22 Service Procedures for Oracle ZFS Storage Appliance ZS7-2 Components**

Replaceable Part(s)	Hot-Swap	URL
Storage head hard drives	Yes	<a href="https://docs.oracle.com/cd/F13758_01/html/F13771/gtbno.html#scrolltoc">https://docs.oracle.com/cd/F13758_01/html/F13771/gtbno.html#scrolltoc</a>
Disk shelf drives	Yes	<a href="https://docs.oracle.com/cd/F13758_01/html/F13771/goxds.html#scrolltoc">https://docs.oracle.com/cd/F13758_01/html/F13771/goxds.html#scrolltoc</a>
Fan modules	Yes	<a href="https://docs.oracle.com/cd/F13758_01/html/F13771/gtboxa.html#scrolltoc">https://docs.oracle.com/cd/F13758_01/html/F13771/gtboxa.html#scrolltoc</a>
Storage head power supplies	Yes	<a href="https://docs.oracle.com/cd/F13758_01/html/F13771/gtbon.html#scrolltoc">https://docs.oracle.com/cd/F13758_01/html/F13771/gtbon.html#scrolltoc</a>
Disk shelf power supplies	Yes	<a href="https://docs.oracle.com/cd/F13758_01/html/F13771/goxbs.html#scrolltoc">https://docs.oracle.com/cd/F13758_01/html/F13771/goxbs.html#scrolltoc</a>
Memory modules (Oracle-qualified service technician only)	No	<a href="https://docs.oracle.com/cd/F13758_01/html/F13771/gtbou.html#scrolltoc">https://docs.oracle.com/cd/F13758_01/html/F13771/gtbou.html#scrolltoc</a>
PCI Express cards	No	<a href="https://docs.oracle.com/cd/F13758_01/html/F13771/gtbnz.html#scrolltoc">https://docs.oracle.com/cd/F13758_01/html/F13771/gtbnz.html#scrolltoc</a>

Replaceable Part(s)	Hot-Swap	URL
(Oracle-qualified service technician only)		
Battery	No	<a href="https://docs.oracle.com/cd/F13758_01/html/F13771/gtbwl.html#scrolltoc">https://docs.oracle.com/cd/F13758_01/html/F13771/gtbwl.html#scrolltoc</a>
Disk shelf I/O modules (Oracle-qualified service technician only)	Yes	<a href="https://docs.oracle.com/cd/F13758_01/html/F13771/goxeo.html#scrolltoc">https://docs.oracle.com/cd/F13758_01/html/F13771/goxeo.html#scrolltoc</a>
Disk shelf SIM boards (Oracle-qualified service technician only)	Yes	<a href="https://docs.oracle.com/cd/F13758_01/html/F13771/goxef.html#scrolltoc">https://docs.oracle.com/cd/F13758_01/html/F13771/goxef.html#scrolltoc</a>

## 6.12 Servicing the Oracle ZFS Storage Appliance ZS5-ES

This section provides instructions to service replaceable components (CRUs/FRUs) in the Oracle ZFS Storage Appliance ZS5-ES. Before starting any service procedure, read and follow the guidelines in [Section 6.3, “Preparing Oracle Private Cloud Appliance for Service”](#).

### 6.12.1 Powering Down the Oracle ZFS Storage Appliance ZS5-ES for Service (When Required)

If you need to execute a service procedure that requires the Oracle ZFS Storage Appliance ZS5-ES 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.

**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.

## 6.12.2 Service Procedures for Oracle ZFS Storage Appliance ZS5-ES Components

For parts that are not hot-swappable, power down the Oracle ZFS Storage Appliance ZS5-ES before starting the service procedure.



**Warning**

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 6.23 Service Procedures for Oracle ZFS Storage Appliance ZS5-ES Components**

Replaceable Part(s)	Hot-Swap	URL
Storage head hard drives	Yes	<a href="https://docs.oracle.com/cd/E59597_01/html/E59600/gqloy.html#scrolltoc">https://docs.oracle.com/cd/E59597_01/html/E59600/gqloy.html#scrolltoc</a>
Disk shelf drives	Yes	<a href="https://docs.oracle.com/cd/E79446_01/html/E79459/goxds.html#scrolltoc">https://docs.oracle.com/cd/E79446_01/html/E79459/goxds.html#scrolltoc</a>
Fan modules	Yes	<a href="https://docs.oracle.com/cd/E59597_01/html/E59600/gqlib.html#scrolltoc">https://docs.oracle.com/cd/E59597_01/html/E59600/gqlib.html#scrolltoc</a>
Storage head power supplies	Yes	<a href="https://docs.oracle.com/cd/E59597_01/html/E59600/gqlfa.html#scrolltoc">https://docs.oracle.com/cd/E59597_01/html/E59600/gqlfa.html#scrolltoc</a>
Disk shelf power supplies	Yes	<a href="https://docs.oracle.com/cd/E79446_01/html/E79459/goxbs.html#scrolltoc">https://docs.oracle.com/cd/E79446_01/html/E79459/goxbs.html#scrolltoc</a>
Memory modules (Oracle-qualified service technician only)	No	<a href="https://docs.oracle.com/cd/E59597_01/html/E59600/gqlgl.html#scrolltoc">https://docs.oracle.com/cd/E59597_01/html/E59600/gqlgl.html#scrolltoc</a>
PCI Express risers (Oracle-qualified service technician only)	No	<a href="https://docs.oracle.com/cd/E59597_01/html/E59600/gqllep.html#scrolltoc">https://docs.oracle.com/cd/E59597_01/html/E59600/gqllep.html#scrolltoc</a>
PCI Express cards (Oracle-qualified service technician only)	No	<a href="https://docs.oracle.com/cd/E59597_01/html/E59600/gqlkc.html#scrolltoc">https://docs.oracle.com/cd/E59597_01/html/E59600/gqlkc.html#scrolltoc</a>
Battery	No	<a href="https://docs.oracle.com/cd/E59597_01/html/E59600/gqlfu.html#scrolltoc">https://docs.oracle.com/cd/E59597_01/html/E59600/gqlfu.html#scrolltoc</a>
Disk shelf I/O modules (Oracle-qualified service technician only)	Yes	<a href="https://docs.oracle.com/cd/E79446_01/html/E79459/goxeo.html#scrolltoc">https://docs.oracle.com/cd/E79446_01/html/E79459/goxeo.html#scrolltoc</a>
Disk shelf SIM boards (Oracle-qualified service technician only)	Yes	<a href="https://docs.oracle.com/cd/E79446_01/html/E79459/goxef.html#scrolltoc">https://docs.oracle.com/cd/E79446_01/html/E79459/goxef.html#scrolltoc</a>

## 6.13 Servicing the Oracle ZFS Storage Appliance ZS3-ES

This section provides instructions to service replaceable components (CRUs/FRUs) in the Oracle ZFS Storage Appliance ZS3-ES. Before starting any service procedure, read and follow the guidelines in [Section 6.3, “Preparing Oracle Private Cloud Appliance for Service”](#).

## 6.13.1 Powering Down the Oracle ZFS Storage Appliance ZS3-ES for Service (When Required)

If you need to execute a service procedure that requires the Oracle ZFS Storage Appliance ZS3-ES to be powered down, follow these instructions:

### Powering down the storage head/controller

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. This is the preferred method for powering down a controller for component replacement.

1. Ensure that Ethernet cables are connected from your network to the **NET-0** port on the back of each server.
2. Direct your web browser to the server to be serviced by using either the IP address or host name assigned to the NET-0 port as follows: `https://ipaddress:215`.
3. Log in as root, using the system-wide Oracle Private Cloud Appliance password.
4. Go to **Maintenance**, then select **Hardware**.
5. Click the **Show Details** link for the server.
6. Click the Power icon for the server and select **Power off** from the pull-down list.

If graceful shutdown is not possible, use the power button.



### Caution

This task forces the main power off. You might corrupt or lose system data, or lose the server configuration (the resources assigned to it) during an immediate power down.

1. Press and quickly release the Power button on the front panel.

This action causes an orderly shutdown of the operating system, and the server enters the standby power mode.

2. If the server did not respond or you need a more immediate shutdown, press and hold the Power button for four seconds.

This forces the main power off and enters the standby power mode immediately. When the main power is off, the Power/OK LED on the front panel begins flashing, indicating that the server is in standby power mode.

If neither graceful shutdown nor emergency shutdown using the power button is possible, for example because you are not physically located at the system, use the ILOM to perform an emergency shutdown. Choose one of the following options:



### Caution

This task forces the main power off. You might corrupt or lose system data, or lose the server configuration (the resources assigned to it) during an immediate power down.



- Log in to the **Oracle ILOM web interface**.

In the left pane, click Host Management > Power Control, and in the Actions list click **Immediate Power Off**.

Click Save, and then click OK.

- Log in to the **Oracle ILOM command-line interface (CLI)**.

At the CLI prompt, type the following command: `stop -f /System`.

### Powering down the disk shelf

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 down or removing all SAS chains from a disk shelf will cause the controllers to panic to prevent data loss. To avoid this, shut down the controllers before decommissioning the shelf.

1. Stop all input and output to and from the disk shelf.
2. Wait approximately two minutes until all disk activity indicators have stopped flashing.
3. Place the power supply on/off switches to the "O" off position.
4. Disconnect the power cords from the external power source.

### Powering on the storage appliance

The disk shelf must not be operated without all components in place.

1. Reconnect the disk shelf power and data cables you removed to service a component.
2. Place the power supply on/off switches on the disk shelf to the "I" on position.
3. Wait several minutes until the boot process is complete, at which time the Power LED should be solid green.
4. Connect the storage head power and data cables you removed to service a component.
5. 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**.

In the left pane, 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`.

6. Wait approximately two minutes until the power-on self-test (POST) code checkpoint tests have completed, and the Power/OK LED on the front panel lights and remains lit.
7. 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.

## 6.13.2 Service Procedures for Oracle ZFS Storage Appliance ZS3-ES Components

For parts that are not hot-swappable, power down the Oracle ZFS Storage Appliance ZS3-ES before starting the service procedure.



#### Warning

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 6.24 Service Procedures for Oracle ZFS Storage Appliance ZS3-ES Components**

Replaceable Part(s)	Hot-Swap	URL
Storage head hard drives	Yes	<a href="http://docs.oracle.com/cd/E37831_01/html/E48559/z40000091011460.html#scrolltoc">http://docs.oracle.com/cd/E37831_01/html/E48559/z40000091011460.html#scrolltoc</a>
Disk shelf drives	Yes	Refer to the section “Replacing a Drive” on this page: <a href="http://docs.oracle.com/cd/E27998_01/html/E48492/maintenance__hardware__procedures__shelf.html#scrolltoc">http://docs.oracle.com/cd/E27998_01/html/E48492/maintenance__hardware__procedures__shelf.html#scrolltoc</a>
Fan modules	Yes	<a href="http://docs.oracle.com/cd/E37831_01/html/E48559/z40000091014194.html#scrolltoc">http://docs.oracle.com/cd/E37831_01/html/E48559/z40000091014194.html#scrolltoc</a>
Storage head power supplies	Yes	<a href="http://docs.oracle.com/cd/E37831_01/html/E48559/z40000091014153.html#scrolltoc">http://docs.oracle.com/cd/E37831_01/html/E48559/z40000091014153.html#scrolltoc</a>
Disk shelf power supplies	Yes	Refer to the section “Replacing a Power Supply” on this page: <a href="http://docs.oracle.com/cd/E27998_01/html/E48492/maintenance__hardware__procedures__shelf.html#scrolltoc">http://docs.oracle.com/cd/E27998_01/html/E48492/maintenance__hardware__procedures__shelf.html#scrolltoc</a>
Memory modules (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E37831_01/html/E48559/z40003f01425075.html#scrolltoc">http://docs.oracle.com/cd/E37831_01/html/E48559/z40003f01425075.html#scrolltoc</a>
PCI Express risers (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E37831_01/html/E48559/z40000f91037394.html#scrolltoc">http://docs.oracle.com/cd/E37831_01/html/E48559/z40000f91037394.html#scrolltoc</a>
PCI Express cards	No	<a href="http://docs.oracle.com/cd/E37831_01/html/E48559/z40000f91037409.html#scrolltoc">http://docs.oracle.com/cd/E37831_01/html/E48559/z40000f91037409.html#scrolltoc</a>

Replaceable Part(s)	Hot-Swap	URL
(Oracle-qualified service technician only)		
Internal USB flash drive	No	<a href="http://docs.oracle.com/cd/E37831_01/html/E48559/z4000a6d1442801.html#scrolltoc">http://docs.oracle.com/cd/E37831_01/html/E48559/z4000a6d1442801.html#scrolltoc</a>
(Oracle-qualified service technician only)		
Battery	No	<a href="http://docs.oracle.com/cd/E37831_01/html/E48559/z40003f01423753.html#scrolltoc">http://docs.oracle.com/cd/E37831_01/html/E48559/z40003f01423753.html#scrolltoc</a>
Disk shelf I/O modules	Yes	Refer to the section “Replacing an I/O Module” on this page: <a href="http://docs.oracle.com/cd/E27998_01/html/E48492/maintenance__hardware__procedures__shelf.html#scrolltoc">http://docs.oracle.com/cd/E27998_01/html/E48492/maintenance__hardware__procedures__shelf.html#scrolltoc</a>
(Oracle-qualified service technician only)		
Disk shelf SIM boards	Yes	Refer to the section “Replacing a SIM Board” on this page: <a href="http://docs.oracle.com/cd/E27998_01/html/E48492/maintenance__hardware__procedures__shelf.html#scrolltoc">http://docs.oracle.com/cd/E27998_01/html/E48492/maintenance__hardware__procedures__shelf.html#scrolltoc</a>
(Oracle-qualified service technician only)		

## 6.14 Servicing the Sun ZFS Storage Appliance 7320

This section provides instructions to service replaceable components (CRUs/FRUs) in the Sun ZFS Storage Appliance 7320. Before starting any service procedure, read and follow the guidelines in [Section 6.3, “Preparing Oracle Private Cloud Appliance for Service”](#).

### 6.14.1 Powering Down the Sun ZFS Storage Appliance 7320 for Service (When Required)

If you need to execute a service procedure that requires the Sun ZFS Storage Appliance 7320 to be powered down, follow these instructions:

#### Powering down the storage head/controller

Powering down or removing all SAS chains from a disk shelf will cause the controllers to panic to prevent data loss. To avoid this, shut down the controllers before decommissioning the shelf.

1. Log in to the BUI.
2. Click the Power icon on the left side of the masthead.

If the BUI is not accessible, select one of the following options:



#### Note

In a configuration with clustered storage heads, always shut down the standby head before the active head.

- SSH into the appliance and issue the `maintenance system poweroff` command.
- SSH or serial console into the service processor (SP) and issue the `stop /SYS` command.
- Use a pen or non-conducting pointed object to press and release the Power button on the front panel.



#### Caution

To initiate emergency shutdown during which all applications and files will be closed abruptly without saving, 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.

### Powering down the disk shelf

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 down or removing all SAS chains from a disk shelf will cause the controllers to panic to prevent data loss. To avoid this, shut down the controllers before decommissioning the shelf.

1. Stop all input and output to and from the disk shelf.
2. Wait approximately two minutes until all disk activity indicators have stopped flashing.
3. Place the power supply on/off switches to the "O" off position.
4. Disconnect the power cords from the external power source.

### Powering on the storage appliance

The disk shelf must not be operated without all components in place.

1. Reconnect the disk shelf power and data cables you removed to service a component.
2. Place the power supply on/off switches on the disk shelf to the "I" on position.
3. Wait several minutes until the boot process is complete, at which time the Power LED should be solid green.
4. Connect the storage head power cables and wait approximately two minutes until the Power/OK LED on the front panel next to the Power button lights and remains lit.

## 6.14.2 Service Procedures for Sun ZFS Storage Appliance 7320 Components

For parts that are not hot-swappable, power down the Sun ZFS Storage Appliance 7320 before starting the service procedure.



### Warning

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 6.25 Service Procedures for Sun ZFS Storage Appliance 7320 Components**

Replaceable Part(s)	Hot-Swap	URL
Storage head HDDs or SSDs	Yes	<a href="http://docs.oracle.com/cd/E28317_01/html/E38247/maintenance__hardware__details__7x20.html#maintenance__hardware__details__7x20">http://docs.oracle.com/cd/E28317_01/html/E38247/maintenance__hardware__details__7x20.html#maintenance__hardware__details__7x20</a>
Disk shelf drives	Yes	Refer to the section "Replacing a Drive" on this page: <a href="http://docs.oracle.com/cd/E27998_01/html/E48492/maintenance__hardware__procedures__shelf.html#scrolltoc">http://docs.oracle.com/cd/E27998_01/html/E48492/maintenance__hardware__procedures__shelf.html#scrolltoc</a>

Replaceable Part(s)	Hot-Swap	URL
Fan modules	Yes	<a href="http://docs.oracle.com/cd/E28317_01/html/E38247/maintenance__hardware__details__7x20.html#maintenance__har">http://docs.oracle.com/cd/E28317_01/html/E38247/maintenance__hardware__details__7x20.html#maintenance__har</a>
Storage head power supplies	Yes	<a href="http://docs.oracle.com/cd/E28317_01/html/E38247/maintenance__hardware__details__7x20.html#maintenance__har">http://docs.oracle.com/cd/E28317_01/html/E38247/maintenance__hardware__details__7x20.html#maintenance__har</a>
Disk shelf power supplies	Yes	Refer to the section “Replacing a Power Supply” on this page: <a href="http://docs.oracle.com/cd/E27998_01/html/E48492/maintenance__hardware__procedures__shelf.html#scrolltoc">http://docs.oracle.com/cd/E27998_01/html/E48492/maintenance__hardware__procedures__shelf.html#scrolltoc</a>
Memory modules (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E28317_01/html/E38247/maintenance__hardware__details__7x20.html#maintenance__har">http://docs.oracle.com/cd/E28317_01/html/E38247/maintenance__hardware__details__7x20.html#maintenance__har</a>
PCI Express risers and cards (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E28317_01/html/E38247/maintenance__hardware__details__7x20.html#maintenance__har">http://docs.oracle.com/cd/E28317_01/html/E38247/maintenance__hardware__details__7x20.html#maintenance__har</a>
Battery	No	<a href="http://docs.oracle.com/cd/E28317_01/html/E38247/maintenance__hardware__details__7x20.html#maintenance__har">http://docs.oracle.com/cd/E28317_01/html/E38247/maintenance__hardware__details__7x20.html#maintenance__har</a>
System indicator boards (Oracle-qualified service technician only)	Yes	<a href="http://docs.oracle.com/cd/E26765_01/html/E26399/maintenance__hardware__details__7x20.html#maintenance__har">http://docs.oracle.com/cd/E26765_01/html/E26399/maintenance__hardware__details__7x20.html#maintenance__har</a>
Disk shelf I/O modules (Oracle-qualified service technician only)	Yes	Refer to the section “Replacing an I/O Module” on this page: <a href="http://docs.oracle.com/cd/E27998_01/html/E48492/maintenance__hardware__procedures__shelf.html#scrolltoc">http://docs.oracle.com/cd/E27998_01/html/E48492/maintenance__hardware__procedures__shelf.html#scrolltoc</a>
Disk shelf SIM boards (Oracle-qualified service technician only)	Yes	Refer to the section “Replacing a SIM Board” on this page: <a href="http://docs.oracle.com/cd/E27998_01/html/E48492/maintenance__hardware__procedures__shelf.html#scrolltoc">http://docs.oracle.com/cd/E27998_01/html/E48492/maintenance__hardware__procedures__shelf.html#scrolltoc</a>

## 6.15 Servicing an Oracle Switch ES1-24

This section provides instructions to service replaceable components (CRUs/FRUs) in an Oracle Switch ES1-24. Before starting any service procedure, read and follow the guidelines in [Section 6.3, “Preparing Oracle Private Cloud Appliance for Service”](#).

### 6.15.1 Powering Down the Oracle Switch ES1-24 for Service (When Required)

If you need to execute a service procedure that requires the Oracle Switch ES1-24 to be powered down, follow these instructions:

#### Powering down the switch

1. To power down an individual power supply, remove its power cord.
2. To power down the switch, remove the power cords from both power supplies.

#### Returning the switch to operation

1. Reconnect the power cords to both power supplies.
2. Verify that the switch has power by checking the status LEDs.

The AC LED lights green to indicate the power supply is connected to line power. A moment later, the OK LED lights green to indicate the power supply is fully operational.

## 6.15.2 Service Procedures for Oracle Switch ES1-24 Components

For parts that are not hot-swappable, power down the Oracle Switch ES1-24 before starting the service procedure.



### Warning

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 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 6.26 Service Procedures for Oracle Switch ES1-24 Components**

Replaceable Part(s)	Hot-Swap	URL
Power supplies	Yes	<a href="http://docs.oracle.com/cd/E39109_01/html/E39116/z40000349112.html#scrolltoc">http://docs.oracle.com/cd/E39109_01/html/E39116/z40000349112.html#scrolltoc</a>
Fan module	Yes	<a href="http://docs.oracle.com/cd/E39109_01/html/E39116/z40000369112.html#scrolltoc">http://docs.oracle.com/cd/E39109_01/html/E39116/z40000369112.html#scrolltoc</a>

## 6.16 Servicing an NM2-36P Sun Datacenter InfiniBand Expansion Switch

This section provides instructions to service replaceable components (CRUs/FRUs) in a NM2-36P Sun Datacenter InfiniBand Expansion Switch. Before starting any service procedure, read and follow the guidelines in [Section 6.3, "Preparing Oracle Private Cloud Appliance for Service"](#).

### 6.16.1 Powering Down the NM2-36P Sun Datacenter InfiniBand Expansion Switch for Service (When Required)

If you need to execute a service procedure that requires the NM2-36P Sun Datacenter InfiniBand Expansion Switch to be powered down, follow these instructions:

#### Powering down the switch

1. To power down an individual power supply, remove its power cord.
2. To power down the switch, remove the power cords from both power supplies.

#### Returning the switch to operation

1. Reconnect the power cords to both power supplies.

2. Verify that the switch has power by checking the status LEDs.

The AC LED lights green to indicate the power supply is connected to line power. A moment later, the OK LED lights green to indicate the power supply is fully operational.

## 6.16.2 Service Procedures for NM2-36P Sun Datacenter InfiniBand Expansion Switch Components

For parts that are not hot-swappable, power down the NM2-36P Sun Datacenter InfiniBand Expansion Switch before starting the service procedure.



### Caution

InfiniBand connectivity may be 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 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 6.27 Service Procedures for NM2-36P Sun Datacenter InfiniBand Expansion Switch Components**

Replaceable Part(s)	Hot-Swap	URL
Power supplies	Yes	<a href="http://docs.oracle.com/cd/E26698_01/html/E26434/z40001f49112.html#scrolltoc">http://docs.oracle.com/cd/E26698_01/html/E26434/z40001f49112.html#scrolltoc</a>
Fans	Yes	<a href="http://docs.oracle.com/cd/E26698_01/html/E26434/z40001f59112.html#scrolltoc">http://docs.oracle.com/cd/E26698_01/html/E26434/z40001f59112.html#scrolltoc</a>
Data cables	Yes	<a href="http://docs.oracle.com/cd/E26698_01/html/E26434/z40001f69112.html#scrolltoc">http://docs.oracle.com/cd/E26698_01/html/E26434/z40001f69112.html#scrolltoc</a>

## 6.17 Servicing an Oracle Fabric Interconnect F1-15

This section provides instructions to service replaceable components (CRUs/FRUs) in an Oracle Fabric Interconnect F1-15. Before starting any service procedure, read and follow the guidelines in [Section 6.3, "Preparing Oracle Private Cloud Appliance for Service"](#).

### 6.17.1 Powering Down the Oracle Fabric Interconnect F1-15 for Service (When Required)

If you need to execute a service procedure that requires the Fabric Interconnect to be powered down, follow these instructions:

#### Powering down the Oracle Fabric Interconnect F1-15

1. Press the Power button to power down the Fabric Interconnect gracefully.
2. Wait for the Status LED to switch off, indicating that the component has been powered down successfully.

**Returning the Oracle Fabric Interconnect F1-15 to operation**

1. Press the Power button to power on the Fabric Interconnect.

The Status LED blinks green, indicating that the system control processor is booting.

2. Wait until the Status LED is solid green.

This indicates that the system control processor has finished booting and the Fabric Interconnect is ready for operation.

**6.17.2 Service Procedures for Oracle Fabric Interconnect F1-15 Components**

For parts that are not hot-swappable, power down the Oracle Fabric Interconnect F1-15 before starting the service procedure.



**Caution**

Management, storage, VM and external network connectivity may be affected while the Fabric Interconnect 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 6.28 Service Procedures for Oracle Fabric Interconnect F1-15 Components**

Replaceable Part(s)	Hot-Swap	URL
Power supplies (Oracle-qualified service technician only)	Yes	<a href="http://docs.oracle.com/cd/E38500_01/html/E50997/z40004411020156.html#scrolltoc">http://docs.oracle.com/cd/E38500_01/html/E50997/z40004411020156.html#scrolltoc</a>
Fan modules (Oracle-qualified service technician only)	Yes	<a href="http://docs.oracle.com/cd/E38500_01/html/E50997/z40004411020136.html#scrolltoc">http://docs.oracle.com/cd/E38500_01/html/E50997/z40004411020136.html#scrolltoc</a>
Fabric board (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E38500_01/html/E50997/z40004411020657.html#scrolltoc">http://docs.oracle.com/cd/E38500_01/html/E50997/z40004411020657.html#scrolltoc</a>
Management module (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E38500_01/html/E50997/z40004411020369.html#scrolltoc">http://docs.oracle.com/cd/E38500_01/html/E50997/z40004411020369.html#scrolltoc</a>  <a href="http://docs.oracle.com/cd/E38500_01/html/E50997/z40004411020375.html#scrolltoc">http://docs.oracle.com/cd/E38500_01/html/E50997/z40004411020375.html#scrolltoc</a>
I/O modules	Yes	<a href="http://docs.oracle.com/cd/E38500_01/html/E50997/z40004411020323.html#scrolltoc">http://docs.oracle.com/cd/E38500_01/html/E50997/z40004411020323.html#scrolltoc</a>



Replaceable Part(s)	Hot-Swap	URL
(Oracle-qualified service technician only)		<a href="http://docs.oracle.com/cd/E38500_01/html/E50997/z400037d1022426.html#scrolltoc">http://docs.oracle.com/cd/E38500_01/html/E50997/z400037d1022426.html#scrolltoc</a>
Front panel assembly, including system control processor  (Oracle-qualified service technician only)	No	<a href="http://docs.oracle.com/cd/E38500_01/html/E50997/z40004411020496.html#scrolltoc">http://docs.oracle.com/cd/E38500_01/html/E50997/z40004411020496.html#scrolltoc</a>

## 6.18 Servicing a Cisco Nexus 9336C-FX2 Switch

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 [Section 6.3, "Preparing Oracle Private Cloud Appliance for Service"](#).

### 6.18.1 Powering Down the Cisco Nexus 9336C-FX2 Switch for Service (When Required)

If you need to execute a service procedure that requires the Cisco Nexus 9336C-FX2 Switch to be powered down, follow these instructions:

#### Powering down the Cisco Nexus 9336C-FX2 Switch

1. Unplug the power cord to power down the switch gracefully.
2. Wait for the Status LED to switch off, indicating that the component has been powered down successfully.

#### Returning the Cisco Nexus 9336C-FX2 Switch to operation

1. Plug in the power cord to power on the switch.

The STS LED blinks amber while booting, then turns green when ready.

2. Wait until the STS LED is solid green.

This indicates that the system control processor has finished booting and the switch is ready for operation.

### 6.18.2 Service Procedures for Cisco Nexus 9336C-FX2 Switch Components

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 6.29 Service Procedures for Cisco Nexus 9336C-FX2 Switch Components**

Replaceable Part(s)	Hot-Swap	URL
Power supplies (Oracle-qualified service technician only)	Yes	<a href="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#">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#</a>
Fan modules (Oracle-qualified service technician only)	Yes	<a href="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#">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#</a>

## 6.19 Servicing a Cisco Nexus 9348GC-FXP Switch

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 [Section 6.3](#), “Preparing Oracle Private Cloud Appliance for Service”.

### 6.19.1 Powering Down the Cisco Nexus 9348GC-FXP Switch for Service (When Required)

If you need to execute a service procedure that requires the Cisco Nexus 9348GC-FXP Switch to be powered down, follow these instructions:

#### Powering down the switch

1. To power down an individual power supply, remove its power cord.
2. To power down the switch, remove the power cords from both power supplies.

#### Returning the switch to operation

1. Reconnect the power cords to both power supplies.
2. Verify that the switch has power by checking the STS LEDs.

The STS LED blinks amber while booting, then turns solid green to indicate the power supply is fully operational.

### 6.19.2 Service Procedures for Cisco Nexus 9348GC-FXP Switch Components

For parts that are not hot-swappable, power down the Cisco Nexus 9348GC-FXP Switch before starting the service procedure.



#### Warning

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 6.30 Service Procedures for Cisco Nexus 9348GC-FXP Switch Components**

Replaceable Part(s)	Hot-Swap	URL
Power supplies	Yes	<a href="https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/n9348gcfxp_hig/guide/b_c9348gcfxp_nxos_mode_hardware_install_guide/b_c9348gcfxp_nxos_mode_hardware_install_guide_chapter_0101.html#conc">https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/n9348gcfxp_hig/guide/b_c9348gcfxp_nxos_mode_hardware_install_guide/b_c9348gcfxp_nxos_mode_hardware_install_guide_chapter_0101.html#conc</a>
Fan module	Yes	<a href="https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/n9348gcfxp_hig/guide/b_c9348gcfxp_nxos_mode_hardware_install_guide/b_c9348gcfxp_nxos_mode_hardware_install_guide_chapter_0101.html#conc">https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/n9348gcfxp_hig/guide/b_c9348gcfxp_nxos_mode_hardware_install_guide/b_c9348gcfxp_nxos_mode_hardware_install_guide_chapter_0101.html#conc</a>



---

## Chapter 7 Troubleshooting

### Table of Contents

7.1 Setting the Oracle Private Cloud Appliance Logging Parameters .....	281
7.2 Adding Proxy Settings for Oracle Private Cloud Appliance Updates .....	282
7.3 Configuring Data Center Switches for VLAN Traffic .....	283
7.4 Changing the Oracle VM Agent Password .....	284
7.5 Running Manual Pre- and Post-Upgrade Checks in Combination with Oracle Private Cloud Appliance Upgrader .....	284
7.6 Enabling Fibre Channel Connectivity on a Provisioned Appliance .....	286
7.7 Restoring a Backup After a Password Change .....	288
7.8 Enabling SNMP Server Monitoring .....	290
7.9 Using a Custom CA Certificate for SSL Encryption .....	291
7.9.1 Creating a Keystore .....	292
7.9.2 Importing a Keystore .....	293
7.10 Reprovisioning a Compute Node when Provisioning Fails .....	294
7.11 Deprovisioning and Replacing a Compute Node .....	295
7.12 Eliminating Time-Out Issues when Provisioning Compute Nodes .....	296
7.13 Returning Oracle VM Server Pool to Operation After Network Services Restart .....	297
7.14 Recovering from Tenant Group Configuration Mismatches .....	298
7.15 Configure Xen CPU Frequency Scaling for Best Performance .....	299

This chapter describes how to resolve a number of common problem scenarios.

## 7.1 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 [Chapter 4, The 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.

## 7.2 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 [Chapter 4, The 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.

## 7.3 Configuring Data Center Switches for VLAN Traffic



**Warning**

This section applies **only** to systems with an InfiniBand-based network architecture. The configuration described in this section is valid for the outbound connections through the Oracle Fabric Interconnect F1-15s .

The Oracle Private Cloud Appliance network infrastructure supports the use of VLANs by default. For this purpose, the Oracle Fabric Interconnect F1-15s are set to trunking mode to allow tagged data traffic.



**Caution**

Do not configure any type of link aggregation group (LAG) across the 10GbE ports: LACP, network/interface bonding or similar methods to combine multiple network connections are not supported.

To provide additional bandwidth to the environment hosted by the Oracle Private Cloud Appliance, create custom networks. For detailed information, see [Section 2.6, “Network Customization”](#).

You may implement VLANs for logical separation of different network segments, or to define security boundaries between networks with different applications – just as you would with physical servers instead of virtual machines.

However, to allow virtual machines hosted by the Oracle Private Cloud Appliance to communicate with systems external to the appliance, you must update the configuration of your next-level data center switches accordingly.

- The switch ports on the receiving end of the outbound appliance connections must be part of each VLAN used within the Oracle Private Cloud Appliance environment.
- The same ports must also be part of the network(s) connecting the external systems that your virtual machines need to access. For example, WAN connectivity implies that virtual machines are able to

reach the public gateway in your data center. As an alternative to VLAN tagging, Layer 3 routing can be used to connect to the Oracle Private Cloud Appliance.

## 7.4 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*.

## 7.5 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, please refer to the support note with [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.

Start by running the Oracle Private Cloud Appliance Upgrader in verify-only mode. The steps are described in [Section 3.2.3, "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 master 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 Oracle 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 with [Doc ID 2148589.1](#).

If your system is InfiniBand-based and there are no Fibre Channel cards installed in the Fabric Interconnects, you can skip this check.

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 master management node, download and run the script `number_of_jobs_and_objects.sh`. It is attached to the support note with [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. It 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 master management node to ensure that the standby management node is capable of taking over the master 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 [Section 3.2.4, "Executing a Controller Software Update"](#). 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 with [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 with [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.

## 7.6 Enabling Fibre Channel Connectivity on a Provisioned Appliance



### Warning

This section applies **only** to systems with an InfiniBand-based network architecture. The configuration described in this section is valid for the I/O modules in the Oracle Fabric Interconnect F1-15s .

However, for Oracle Server X8-2 and newer compute nodes, Fibre Channel connectivity through the Fabric Interconnects is **not** supported. Instead, you must use the (optional) physical FC HBA expansion cards. Refer to the section [Extending Storage Capacity of Ethernet-based Systems](#) in the *Oracle Private Cloud Appliance Installation Guide*.

If you ordered an Oracle Private Cloud Appliance without factory-installed Fibre Channel I/O modules and you decide to add external Fibre Channel storage at a later time, when the rack has already been provisioned, your installation must meet these requirements:

- The Oracle Private Cloud Appliance controller software must be at Release 2.1.1 or later.
- A total of four Fibre Channel I/O modules must be installed in slots 3 and 12 of each Oracle Fabric Interconnect F1-15.
- Storage clouds and vHBAs must be configured manually.

Installation information for the optional Fibre Channel I/O modules can be found in the section entitled [Installing Optional Fibre Channel I/O Modules](#) in the *Oracle Private Cloud Appliance Installation Guide*. This section provides detailed CLI instructions to configure the storage clouds and vHBAs associated with Fibre Channel connectivity.

### Configuring Storage Clouds and vHBAs for Fibre Channel Connectivity

1. Using SSH and an account with superuser privileges, log into the master 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. Launch the Oracle Private Cloud Appliance CLI in interactive mode.

```
# pca-admin
Welcome to PCA! Release: 2.3.2
PCA>
```

3. Verify that no storage clouds or vHBAs exist yet.

```
PCA> list storage-network
```

```
Network_Name          Description
-----
0 rows displayed
Status: Success
```

```
PCA> list wwpn-info
```

```
WWPN                  vHBA      Cloud_Name      Server      Type  Alias
-----
0 rows displayed
Status: Success
```

4. Configure the vHBAs on both management nodes.

```
PCA> configure vhbases ovcamn05r1 ovcamn06r1
```

```
Compute_Node          Status
-----
ovcamn05r1            Succeeded
ovcamn06r1            Succeeded
-----
2 rows displayed
Status: Success
```

5. Verify that the clouds have been configured.

```
PCA> list storage-network
```

```
Network_Name          Description
-----
Cloud_A               Default Storage Cloud ru22 port1 - Do not delete or modify
Cloud_B               Default Storage Cloud ru22 port2 - Do not delete or modify
Cloud_C               Default Storage Cloud ru15 port1 - Do not delete or modify
Cloud_D               Default Storage Cloud ru15 port2 - Do not delete or modify
-----
4 rows displayed
Status: Success
```

6. If the 4 storage clouds have been configured correctly, configure the vHBAs on all compute nodes.

```
PCA> configure vhbases ALL
```

```
Compute_Node          Status
-----
ovcacn07r1            Succeeded
ovcacn08r1            Succeeded
[...]
ovcacn36r1            Succeeded
ovcacn37r1            Succeeded
-----
20 rows displayed
Status: Success
```

7. Verify that all clouds and vHBAs have been configured correctly.

```
PCA> list wwpn-info
```

```
WWPN                  vHBA      Cloud_Name      Server      Type  Alias
-----
```

```

50:01:39:70:00:4F:91:00  vhba01  Cloud_A      ovcamn05r1  MN   ovcamn05r1-Cloud_A
50:01:39:70:00:4F:91:02  vhba01  Cloud_A      ovcamn06r1  MN   ovcamn06r1-Cloud_A
50:01:39:70:00:4F:91:04  vhba01  Cloud_A      ovcacn07r1  CN   ovcacn07r1-Cloud_A
50:01:39:70:00:4F:91:06  vhba01  Cloud_A      ovcacn08r1  CN   ovcacn08r1-Cloud_A
[...]
50:01:39:70:00:4F:F1:05  vhba04  Cloud_D      ovcacn35r1  CN   ovcacn35r1-Cloud_D
50:01:39:70:00:4F:F1:03  vhba04  Cloud_D      ovcacn36r1  CN   ovcacn36r1-Cloud_D
50:01:39:70:00:4F:F1:01  vhba04  Cloud_D      ovcacn37r1  CN   ovcacn37r1-Cloud_D
-----
88 rows displayed

Status: Success

```

```

PCA> show storage-network Cloud_A

-----
Network_Name      Cloud_A
Description       Default Storage Cloud ru22 port1 - Do not delete or modify
Ports             ovcasw22r1:12:1, ovcasw22r1:3:1
vHBAs             ovcacn07r1-vhba01, ovcacn08r1-vhba01, ovcacn10r1-vhba01, [...]
-----
Status: Success

PCA> show storage-network Cloud_B

-----
Network_Name      Cloud_B
Description       Default Storage Cloud ru22 port2 - Do not delete or modify
Ports             ovcasw22r1:12:2, ovcasw22r1:3:2
vHBAs             ovcacn07r1-vhba02, ovcacn08r1-vhba02, ovcacn10r1-vhba02, [...]
-----
Status: Success

PCA> show storage-network Cloud_C

-----
Network_Name      Cloud_C
Description       Default Storage Cloud ru15 port1 - Do not delete or modify
Ports             ovcasw15r1:12:1, ovcasw15r1:3:1
vHBAs             ovcacn07r1-vhba03, ovcacn08r1-vhba03, ovcacn10r1-vhba03, [...]
-----
Status: Success

PCA> show storage-network Cloud_D

-----
Network_Name      Cloud_D
Description       Default Storage Cloud ru15 port2 - Do not delete or modify
Ports             ovcasw15r1:12:2, ovcasw15r1:3:2
vHBAs             ovcacn07r1-vhba04, ovcacn08r1-vhba04, ovcacn10r1-vhba04, [...]
-----
Status: Success

```

The system is now ready to integrate with external Fibre Channel storage. For detailed information and instructions, refer to the section entitled [Adding External Fibre Channel Storage](#) in the *Oracle Private Cloud Appliance Installation Guide*.

## 7.7 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 change 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.

## 7.8 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-5.5-60.0.1.el6.x86_64.rpm`
- `net-snmp-libs-5.5-60.0.1.el6.x86_64.rpm`
- `net-snmp-utils-5.5-60.0.1.el6.x86_64.rpm`
- `ovca-snmp-0.9-3.el6.x86_64.rpm`
- `lm_sensors-libs-3.1.1-17.el6.x86_64.rpm`

3. Install these packages by running the following command:

```
# rpm -ivh ovca-snmp-0.9-3.el6.x86_64.rpm net-snmp-libs-5.5-49.0.1.el6.x86_64.rpm \
net-snmp-5.5-49.0.1.el6.x86_64.rpm lm_sensors-libs-3.1.1-17.el6.x86_64.rpm \
net-snmp-utils-5.5-49.0.1.el6.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.

```
# service snmpd start
```

6. If desired, enable the `snmpd` service on boot.

```
# chkconfig snmpd on
```

7. Open the SNMP ports on the firewall.

```
# iptables -I INPUT -p udp -m udp --dport 161 -j ACCEPT
```

```
# iptables -I INPUT -p udp -m udp --dport 162 -j ACCEPT
# iptables-save > /etc/sysconfig/iptables
```

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::ovcaSerial
- 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.

```
# service snmpd start
```

SNMP is now ready for use on this compute node.

4. If desired, enable the `snmpd` service on boot.

```
# chkconfig snmpd on
```

5. Repeat this procedure on all other compute nodes installed in your Oracle Private Cloud Appliance environment.

## 7.9 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.

## 7.9.1 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 Welcome1 -storetype jks -keystore mykeystore.jks -storepass Welcome1
# 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 Welcome1 -storetype jks -keystore mykeystore.jks -storepass Welcome1
# 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 Welcome1
```

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 Welcome1 -storetype jks -keystore mykeystore.jks \
-storepass Welcome1
```



- 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
```

- 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
```

- 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.

### 7.9.2 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 Oracle 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 Oracle Private Cloud Appliance software, you must regenerate the keys prior to updating the Controller Software. For instructions, refer to the support note with [Doc ID 2597439.1](#).

#### Importing a Keystore with an Existing CA and SSL Certificate

- 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 ~]#
```

- Import the keystore.

```
# /u01/app/oracle/java/bin/keytool -importkeystore -noprompt \
-srckeystore existing_keystore.jks -srcstoretype source_format -srcstorepass Welcome1
-destkeystore mykeystore.jks -deststoretype jks -deststorepass Welcome1
```

- 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
```

Where `/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.

## 7.10 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.



### Warning

Reprovisioning is to be applied *only* to compute nodes that fail to complete provisioning.

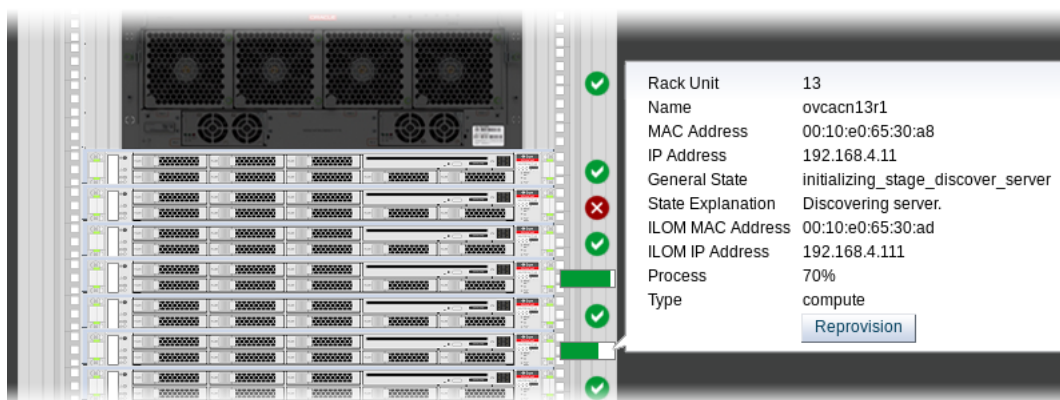
For correctly provisioned and running compute nodes, reprovisioning functionality is blocked in order to prevent incorrect use that could lock compute nodes out of the environment permanently or otherwise cause loss of functionality or data corruption.

### 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 master 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 [Section 5.2, “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.

## 7.11 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 [Section 5.2, “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.

- 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>
```

- Lock provisioning to make sure that the compute node cannot be reprovisioned immediately after deprovisioning.

```
PCA> create lock provisioning
Status: Success
```

- 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
```

- 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.

## 7.12 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.

## 7.13 Returning Oracle VM Server Pool to Operation After Network Services Restart



### Warning

This section applies **only** to systems with an InfiniBand-based network architecture. The use of the `bond0` interface described in this section is inherent to the network design based on the use of Oracle Fabric Interconnect F1-15s .

When network services are restarted on the master management node, the connection to the Oracle VM management network ( `bond0` ) is lost. By design, the `bond0` interface is not brought up automatically on boot, so that the virtual IP of the management cluster can be configured on the correct node, depending on which management node assumes the master role. While the master management node is disconnected from the Oracle VM management network, the Oracle VM Manager user interface reports that the compute nodes in the server pool are offline.

The management node that becomes the master, runs the Oracle VM services necessary to bring up the `bond0` interface and configure the virtual IP within a few minutes. It is expected that the compute nodes in the Oracle VM server pool return to their normal online status in the Oracle VM Manager user interface. If the master management node does not reconnect automatically to the Oracle VM management network, bring the `bond0` interface up manually from the Oracle Linux shell.



### Warning

Execute this procedure **ONLY** when so instructed by Oracle Support. This should only be necessary in rare situations where the master management node fails to connect automatically. You should never manually disconnect or restart networking on any node.

### Manually Reconnecting the Master Management Node to the Oracle VM Management Network

1. Using SSH and an account with superuser privileges, log into the disconnected master management node on the appliance management network.

```
# ssh root@192.168.4.3
root@192.168.4.3's password:
[root@ovcamn05r1 ~]#
```

2. Check the configuration of the `bond0` interface.

If the interface is down, the console output looks similar to this:

```
# ifconfig bond0
```

```
bond0    Link encap:Ethernet  HWaddr 00:13:97:4E:B0:02
         BROADCAST MULTICAST  MTU:1500  Metric:1
         RX packets:0 errors:0 dropped:0 overruns:0 frame:0
         TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

3. Bring the `bond0` interface up.

```
# ifconfig bond0 up
```

4. Check the configuration of the `bond0` interface again.

When the interface reconnects successfully to the Oracle VM management network, the console output looks similar to this:

```
# ifconfig bond0
bond0    Link encap:Ethernet  HWaddr 00:13:97:4E:B0:02
         inet addr:192.168.140.4  Bcast:192.168.140.255  Mask:255.255.255.0
         inet6 addr: fe80::213:97ff:fe4e:b002/64 Scope:Link
         UP BROADCAST RUNNING MASTER MULTICAST  MTU:1500  Metric:1
         RX packets:62191 errors:0 dropped:0 overruns:0 frame:0
         TX packets:9183 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:4539474 (4.33 MB)  TX bytes:1853641 (1.77 MB)
```

## 7.14 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 [Section 2.8.2, “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 server 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 [Section 2.8.2, “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.

## 7.15 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
cpufreq         : 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
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"
```

2. Rebuild `grub.cfg` by means of the following command:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```



---

# Index

## A

accessibility, 28

appliance

architecture, 1

backup, 22

hardware, 1, 2

high availability, 21

overview, 1, 1

provisioning, 1, 19

software, 1, 12

software update, 23

upgrader tool, 23

ASR

introduction, 230

prerequisites, 231

setup and asset activation, 232

understanding ASR, 230

authentication, 58

Auto Service Request

introduction, 230

prerequisites, 231

setup and asset activation, 232

understanding ASR, 230

## B

backup, 22, 25, 68

restore after password change, 288

## C

certificate

SSL encryption with custom CA certificate, 291

change password

Oracle VM Agent, 284

cloud backup, 68

configuration, 68

configure manually, 69

delete, 70

delete Oracle Cloud Infrastructure target, 71

cluster, 78

create on DHCP network, 74

create on static network, 75

delete, 79

compute node

deprovisioning, 295

failover, 22

provisioning, 19

provisioning failure, 294

replacement or repair, 295

server information, 206

time-outs when provisioning, 296

upgrade Oracle VM Server, 99

upgrade virtualization platform, 99

compute nodes

hardware, 5

configuration, 25

cloud backup, 68

DNS, 32

initial setup, 32

logging, 281

management network, 32

management node, 32

NTP, 32

proxy, 282

public network, 32

contrast, 28

CRU servicing

Cisco Nexus 9336C-FX2 Switch, 277

Cisco Nexus 9348GC-FXP Switch, 278

NM2-36P Sun Datacenter InfiniBand Expansion Switch, 274

Oracle Fabric Interconnect F1-15, 275

Oracle Server X5-2, 255

Oracle Server X6-2, 252

Oracle Server X7-2, 250

Oracle Server X8-2, 248

Oracle Switch ES1-24, 273

Oracle ZFS Storage Appliance ZS3-ES, 267

Oracle ZFS Storage Appliance ZS5-ES, 265

Oracle ZFS Storage Appliance ZS7-2, 262

rack parts, 246

Sun Server X3-2, 260

Sun Server X4-2, 257

Sun ZFS Storage Appliance 7320, 271

custom networking, 39

configure on Ethernet architecture, 40

configure on InfiniBand architecture, 44

create and delete custom network, 39

## D

Dashboard, 25, 32, 58

Hardware View, 28

login, 26

software, 12

database

failover, 21

databases

software, 14

deprovision compute node, 295

## E

electrostatic discharge safety, 245

ES1-24 switch

component servicing instructions, 273

---

external storage  
enable fibre channel on provisioned appliance, 286

## F

Fabric Interconnect F1-15  
component servicing instructions, 275  
replaceable components, 244

failover

compute node, 22  
database, 22  
management node, 21  
networking, 22  
storage, 22

fault, 64

monitoring, 64

fibre channel

enable on provisioned appliance, 286

font size, 28

## H

hardware, 2

compute nodes, 5  
health monitoring, 61  
identifying, 28  
management nodes, 4  
monitoring, 28  
networking, 8  
status, 28  
storage, 5  
view, 28

health monitoring, 61

high availability, 21

## I

InfiniBand switch

component servicing instructions, 274  
replaceable components, 244

initial setup, 25

## J

jobs and events, 219, 219

## K

Kubernetes, 71

cluster status, 79  
create cluster on DHCP network, 74  
create cluster on static network, 75  
dashboard, 77  
delete cluster, 79  
guidelines, 71  
maintain OS on virtual machines, 81  
prepare environment, 72  
resize virtual machine disk space, 80

## L

logging

configure, 281

## M

management node

failover, 21  
initial setup, 32  
provisioning, 19  
update appliance controller software, 86

management nodes

hardware, 4

managing, 78

manual cloud backup, 69

monitoring, 61, 64, 67

enabling SNMP, 290

hardware, 25, 28, 205

Oracle VM, 205

Oracle VM Events perspective, 205

Oracle VM Info perspective, 205

virtual machine, 205

## N

network

configuration, 25

functional limitations, 35

limitations Ethernet architecture, 36

limitations InfiniBand architecture, 38

monitoring, 25

network customization, 39

configure on Ethernet architecture, 40

configure on InfiniBand architecture, 44

create and delete custom network, 39

Network Environment, 32

networking

Ethernet architecture, 8

failover, 22

hardware, 8

InfiniBand architecture, 10

proxy, 282

server pool offline after network restart, 297

using VLANs, 283

NM2-36P InfiniBand switch

component servicing instructions, 274

replaceable components, 244

## O

OCI backup, 68

operating systems

software, 13

Oracle Cloud Infrastructure target

delete, 71

Oracle Server X5-2

---

- component servicing instructions, 255
- replaceable components, 236
- Oracle Server X6-2
  - component servicing instructions, 252
  - replaceable components, 235
- Oracle Server X7-2
  - component servicing instructions, 250
  - replaceable components, 234
- Oracle Server X8-2
  - component servicing instructions, 248
- Oracle VM, 201
  - Events, 219
  - Events perspective, 205
  - Exporter Appliance, 219
  - health, 205
  - Info perspective, 205
  - Jobs, 219
  - limitations, 202
  - login, 205
  - monitoring, 205
  - networking, 211
  - Reports and Resources, 219
  - repositories, 209
  - server pool offline after network restart, 297
  - Servers and VMs, 206
  - storage, 217
  - tagging, 219
- Oracle VM Agent
  - change password, 284
- Oracle VM Manager
  - adding expansion nodes, 20
  - restore backup after password change, 288
  - server pool, 20
  - server pool mismatch with tenant group, 298
  - software, 13
- Oracle ZFS Storage Appliance ZS3-ES
  - component servicing instructions, 267
- Oracle ZFS Storage Appliance ZS5-ES, 7
  - component servicing instructions, 265
- Oracle ZFS Storage Appliance ZS7-2, 5
  - component servicing instructions, 262

## P

- password, 58
  - change Oracle VM Agent password, 284
- password change
  - failure restoring backup, 288
- password management, 58
- password manager, 13
- phone home, 67
  - health monitoring, 67
- power off procedure
  - servicing, 246

- provisioning, 19
  - compute node discovery, 19
  - compute node failure, 294
  - eliminate time-out issues, 296
  - expansion node, 20
  - initialization, 19
  - server pool configuration, 20
- proxy
  - configure, 282

## R

- rack
  - component servicing instructions, 246
  - replaceable components, 232
- replaceable components
  - Cisco Nexus 9336C-FX2 Switch, 277
  - Cisco Nexus 9348GC-FXP Switch, 278
  - NM2-36P Sun Datacenter InfiniBand Expansion Switch, 244
  - Oracle Fabric Interconnect F1-15, 244
  - Oracle Server X5-2, 236
  - Oracle Server X6-2, 235
  - Oracle Server X7-2, 234
  - Oracle Server X8-2, 233
  - Oracle Switch ES1-24, 243
  - Oracle ZFS Storage Appliance ZS3-ES, 241
  - Oracle ZFS Storage Appliance ZS5-ES, 240
  - Oracle ZFS Storage Appliance ZS7-2, 238
- rack infrastructure, 232
- Sun Server X3-2, 238
- Sun Server X4-2, 237
- Sun ZFS Storage Appliance 7320, 242

reset, 58

## S

- safety
  - electrostatic discharge, 245
  - service precautions, 245
- screen reader, 28
- server pool
  - offline after network restart, 297
  - tenant group configuration mismatch, 298
- service, 230
  - ASR prerequisites, 231
  - ASR setup and asset activation, 232
  - Auto Service Request, 230
  - electrostatic discharge, 245
  - preparations, 245
  - replaceable components, 232
  - safety precautions, 245
  - servicing Cisco Nexus 9336C-FX2 Switch parts, 277
  - servicing Cisco Nexus 9348GC-FXP Switch parts, 278
  - servicing Fabric Interconnect parts, 275

---

- servicing NM2-36P Sun Datacenter InfiniBand Expansion Switch parts, 274
- servicing Oracle Server X5-2 parts, 255
- servicing Oracle Server X6-2 parts, 252
- servicing Oracle Server X7-2 parts, 250
- servicing Oracle Server X8-2 parts, 248
- servicing Oracle Switch ES1-24 parts, 273
- servicing Oracle ZFS Storage Appliance ZS3-ES parts, 267
- servicing Oracle ZFS Storage Appliance ZS5-ES parts, 265
- servicing Oracle ZFS Storage Appliance ZS7-2 parts, 262
- servicing rack parts, 246
- servicing Sun Server X3-2 parts, 260
- servicing Sun Server X4-2 parts, 257
- servicing Sun ZFS Storage Appliance 7320 parts, 271
- understanding ASR, 230
- servicing the system
  - powering down, 246
- SNMP
  - enable, 290
  - software, 12
    - Dashboard, 12
    - databases, 13
    - operating systems, 13
    - Oracle VM Manager, 13
    - wallet, 13
  - software update, 23, 83
    - update appliance controller software, 86
    - upgrade existing compute node with new Oracle VM Server, 99
    - upgrader tool, 23, 86
- SSL
  - using custom certificate, 291
- storage
  - adding, 217
  - configuration, 217
  - enable fibre channel on provisioned appliance, 286
  - failover, 22
  - hardware, 5
- Storage Appliance
  - component servicing instructions, 262, 265, 267, 271
  - replaceable components, 238, 240, 241, 242
- Sun Server X3-2
  - component servicing instructions, 260
  - replaceable components, 238
- Sun Server X4-2
  - component servicing instructions, 257
  - replaceable components, 237
- Sun ZFS Storage Appliance 7320
  - component servicing instructions, 271
- switch ES1-24
  - component servicing instructions, 273

- replaceable components, 243

## T

- tagging resources, 219
- tenant group
  - recovering from configuration mismatches, 298

## U

- update, 83
  - update appliance controller software, 86
  - upgrade Oracle VM Server, 99
  - upgrade virtualization platform, 99
  - upgrader tool, 23, 86
- upgrader tool, 23
  - installation, 88
  - pre-checks, 89
  - storage network, 97
  - update appliance controller software, 86, 91
  - upgrade readiness, 89
  - usage, 86

## V

- virtual machine
  - clone, 206
  - clone customizer, 209
  - console, 206
  - create, 206
  - delete, 206
  - import, 206
  - installation media, 209
  - ISOs, 209
  - management, 201, 206
  - messaging, 206
  - migrate, 206
  - resources, 209
  - templates, 209
  - virtual appliances, 209
  - virtual disks, 209
  - VNICs, 211
- VLAN
  - enabling VLAN traffic, 283
- vm storage
  - network, 50
- vm storage network, 50

## W

- wallet
  - software, 13

## Z

- ZFS Storage Appliance
  - component servicing instructions, 262, 265, 267, 271
  - replaceable components, 238, 240, 241, 242