Oracle Private Cloud Appliance

Upgrade Guide for Release 2.4.4.1

F57213-02
November 2022

ORACLE

Oracle Private Cloud Appliance Upgrade Guide for Release 2.4.4.1,

F57213-02

Contents

Preface

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

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

The documentation set consists of the following items:

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

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

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

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

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

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

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

Audience

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

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

Related Documentation

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

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

- Oracle Rack Cabinet 1242

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

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

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

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

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

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

Feedback

Provide feedback about this documentation at:

https://www.oracle.com/goto/docfeedback

Conventions

The following text conventions are used in this document:

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

Documentation Accessibility

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

Access to Oracle Support for Accessibility

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

Diversity and Inclusion

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

1

Updating Oracle Private Cloud Appliance

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 describes the sequence to perform Oracle Private Cloud Appliance updates.

For additional information about using the Upgrader Tool with software release 2.4.4.1, see the support note Upgrader Tool - Prechecks and Postchecks (Doc ID 2877541.1).

Table 1-1 Sequential Break-Down of an Appliance Update

Order	Component	Description
1.	management nodes software	Install updated management software on both management nodes (`mn05` and `mn06`). See Upgrading the Management Node Controller Software.
2.	all firmware, in this order 1. management node firmware 2. internal ZFS storage firmware 3. switch firmware • Firmware for Cisco leaf, spine, and management switches • EPLD image for Cisco leaf, spine, and management switches 4. compute node firmware	See Upgrading Component Firmware.
3.	compute node software updates	See Upgrading the Virtualization Platform

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.

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

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

To view supported firmware versions for all releases of Oracle Private Cloud Appliance, see support note Doc ID 2877541.1.

Warnings and Cautions

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

NOT_SUPPORTED:

Minimum Release

In this version of the Oracle Private Cloud Appliance Administrator's Guide, it is assumed that your system is currently **running Controller Software release 2.4.4 prior to this software update**.

If your system is currently running an earlier version, refer to the Updating Oracle Private Cloud Appliance chapter in Oracle Private Cloud Appliance Administration Guide for Release 2.4.4. Follow the appropriate procedures and make sure that your appliance configuration is valid for the release 2.4.4 update before you continue.

NOT_SUPPORTED:

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.

NOT_SUPPORTED:

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.

Caution:

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 Firmware Policy.

Caution:

No Backup

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

Caution:

CA Certificate and Keystore

If you have generated custom keys using `ovmkeytool.sh` in a previous version of the 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 Creating a Keystore.

Caution:

Proxy Settings

If direct public access is not available within your data center and you make use of proxy servers to facilitate HTTP, HTTPS and FTP traffic, it may be necessary to edit the 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 Adding Proxy Settings for more information.

Caution:

Custom LUNs on Internal Storage

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

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

Caution:

Oracle VM Availability During Update to Release 2.4.x

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

NOT_SUPPORTED:

Compute Node Upgrade ONLY Through Oracle Private Cloud Appliance

Compute nodes cannot be upgraded to the appropriate Oracle VM Server Release 3.4.x with the Oracle VM Manager web UI. You must upgrade them using the `pca-admin update compute-node` CLI command within the Oracle Private Cloud Appliance.

To perform this upgrade procedure, follow the specific instructions in Upgrading the Virtualization Platform.

NOT_SUPPORTED:

Do Not Override Oracle VM Global Update Settings

As stated in the Guidelines section in the Managing the Oracle VM Virtual Infrastructure chapter of the Oracle Private Cloud Appliance Administration Guide for Release 2.4.4, 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.

> **Caution:**
>
> **Post-Update Synchronization**
>
> Once you have confirmed that the update process has completed, it is advised that you wait a further 30 minutes before starting another compute node or management node software update. This allows the necessary synchronization tasks to complete.
>
> If you ignore the recommended delay between these update procedures there could be issues with further updating as a result of interference between existing and new tasks.

Backup Local Customizations

An update of the 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.

For detailed instructions, refer to the Agent Recovery section in the Oracle Enterprise Manager Plug-in documentation.

Auto Service Request (ASR) Users

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

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

Confirm your system is configured properly after an upgrade by following the Oracle Support Document 2560988.1 (How to Install Auto Service Request (ASR) on Private Cloud Appliance (PCA) 2.4.1 or Later).

Determine Firmware Versions

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

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

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

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

   - compute/management nodes

     ```
     → fwupdate list all
     ```

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

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

then determine the card firmware version with mstflint on the appropriate PCI bus:

```
[root@ovcamn05r1 ~]# mstflint -d /proc/bus/pci/3b/00.0 q
Image type:            FS4
FW Version:            16.29.1436
FW Release Date:       13.5.2021
Product Version:       16.29.1436
[...]
```

- ZFS Storage Appliances

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

- Cisco switches

  ```
  ovcasw21r1# show version
  ```

Upgrading the Management Node Controller Software

NOT_SUPPORTED:

UPGRADE BOTH MANAGEMENT NODES CONSECUTIVELY

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

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

NOT_SUPPORTED:

NO MANAGEMENT OPERATIONS DURING UPGRADE

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

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

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

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.
2. Run the command `pca-check-master` on both management nodes to verify which node owns the active role.
3. Reboot the management node that is **NOT** currently the active node. Enter `init 6` at the prompt.
4. Ping the machine you rebooted. When it comes back online, reconnect using SSH and monitor system activity to determine when the secondary management node takes over the active role. Enter this command at the prompt: `tail -f /var/log/messages`. New system activity notifications will be output to the screen as they are logged.
5. In the other SSH console, which is connected to the current active management node, enter `init 6` to reboot the machine and initiate management node failover.

   The log messages in the other SSH console should now indicate when the secondary management node takes over the active role.

6. Verify that both management nodes have come back online after reboot and that the active role has been transferred to the other manager. Run the command `pca-check-master` on both management nodes.

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

Installing the Oracle Private Cloud Appliance Upgrader

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

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

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

   ```
   [root@ovcamn05r1 ~]# yum search pca_upgrader
   pca_upgrader-2.4.4.1-31.el7.noarch
   ```

2. Log into My Oracle Support and download the latest version of the Oracle Private Cloud Appliance Upgrader to a secure location, if it is newer than the version on your system.

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

   To obtain the Upgrader package, download this zip file and extract the file `pca_upgrader-2.4.4.1-31.el7.noarch.rpm`.

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

3. If you downloaded a newer version of the Oracle Private Cloud Appliance Upgrader, you must upgrade to the newer version. From the directory where the `*.rpm` package was saved, run the command `yum update pca_upgrader-2.4.4.1-31.el7.noarch.rpm`.

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

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

   ```
   [root@ovcamn05r1 ~]# pca-check-master
   NODE: 192.168.4.3  MASTER: True
   root@ovcamn05r1 tmp]# yum install pca_upgrader-2.4.4.1-31.el7.noarch.rpm
   Preparing..########################################### [100%]
   1:pca_upgrader############################################ [100%]
   ```

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

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

Verifying Upgrade Readiness

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

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

   For help resolving issues to correct the compute node status, refer to the support note with Doc ID 2245197.1 or contact Oracle Support.

2. Perform the required manual pre-upgrade checks. For instructions, see "Running Manual Pre- and Post-Upgrade Checks in Combination with Oracle Private Cloud Appliance Upgrader" in the Troubleshooting chapter in Oracle Private Cloud Appliance Administration Guide for Release 2.4.4.

3. 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.

4. 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.

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

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

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

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

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

root@ovcamn05r1 ~]# pca_upgrader -V -t management -c ovcamn06r1 -g 2.4.4.1 \
-l http://<path-to-iso>/ovca-2.4.4.1-b000.iso.zip

PCA Rack Type: PCA X8_BASE.

Please refer to log file
/nfs/shared_storage/pca_upgrader/log/pca_upgrader_<date>-
<time>_<hostname_<action>.log
for more details.

Beginning PCA Management Node Pre-Upgrade Checks...

Validate the Image Provided                                    1/51
Rack Type Check                                                2/51
OVMM Model DB Check                                            3/51
ONF Check                                                      4/51
[...]
Password Check                                                48/51
OSA Disabled Check                                            49/51
Storage Network Upgrade Check                                 50/51
ZFSSA Network Configuration Check                             51/51

PCA Management Node Pre-Upgrade Checks completed after 2 minutes


Beginning PCA Health Checks...

Check Management Nodes Are Running                             1/19
Oracle VM Manager Default Networks                             2/19
Repositories Defined in Oracle VM Manager                      3/19
[...]
All Compute Nodes Running                                     16/19
Test for Shares Mounted on Compute Nodes                      17/19
Test for ovs-agent Service on Compute Nodes                   18/19
Check Compute Node's Active Network Interfaces                19/19
```

```
PCA Health Checks completed after 1 minutes

--------------------------------------------------------------------------------
PCA Management Node Pre-Upgrade Checks                                  Passed
--------------------------------------------------------------------------------
Validate the Image Provided                                        Not Required
Rack Type Check                                                         Passed
OVMM Model DB Check                                                     Passed
[...]
Storage Network Upgrade Check                                           Passed
ZFSSA Network Configuration Check                                       Passed
--------------------------------------------------------------------------------
PCA Health Checks                                                       Passed
--------------------------------------------------------------------------------
Check Management Nodes Are Running                                      Passed
Oracle VM Manager Default Networks                                      Passed
Repositories Defined in Oracle VM Manager                               Passed
Check Support Packages                                                  Passed
[...]
Test for Shares Mounted on Compute Nodes                                Passed
Test for ovs-agent Service on Compute Nodes                             Passed
Check Compute Node's Active Network Interfaces                          Passed
--------------------------------------------------------------------------------
Overall Status                                                          Passed
--------------------------------------------------------------------------------
PCA Management Node Pre-Upgrade Checks                                  Passed
PCA Health Checks                                                       Passed
Please refer to log file /nfs/shared_storage/pca_upgrader/log/pca_upgrader_<date>-
<time>_<hostname_<action>.log
for more details.
```

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

Executing a Controller Software Update

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

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

NOT_SUPPORTED:

NO MANAGEMENT OPERATIONS DURING UPGRADE

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

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

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

root@ovcamn05r1 ~]# pca_upgrader -U -t management -c ovcamn06r1 -g 2.4.4.1 \
-l http://<path-to-iso>/ovca-2.4.4.1-b132.iso.zip

PCA Rack Type: PCA X8_BASE.

Please refer to log file
/nfs/shared_storage/pca_upgrader/log/pca_upgrader_<date>-
<time>_<hostname_<action>.log
for more details.

Beginning PCA Management Node Pre-Upgrade Checks...
Validate the Image Provided                                          1/51
Rack Type Check                                                      2/51
OVMM Model DB Check                                                  3/51
[...]

PCA Management Node Pre-Upgrade Checks completed after 2 minutes


Beginning PCA Health Checks...

Check Management Nodes Are Running                                   1/19
Check PCA DBs Exist                                                  2/19
Check Support Packages                                               3/19
[...]

PCA Health Checks completed after 1 minutes

**********************************************************************
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 ovcamn06r1
Disable PCA Backups                                                  1/18
Download ISO                                                         2/18
Setup Yum Repo                                                       3/18
Take OVM Backup                                                      4/18
[…]
Restore PCA Backups                                                 17/18
Upgrade is complete                                                 18/18
PCA Management Node upgrade of ovcamn06r1 completed after 88 minutes
```

```
Beginning PCA Post-Upgrade Checks...

OVM Manager Cache Size Check                                          1/1

PCA Post-Upgrade Checks completed after 1 minutes

--------------------------------------------------------------------------------
PCA Management Node Pre-Upgrade Checks                                Passed
--------------------------------------------------------------------------------
Validate the Image Provided                                           Passed
Rack Type Check                                                       Passed
OVMM Model DB Check                                                   Passed
[…]
Storage Network Upgrade Check                                         Passed
ZFSSA Network Configuration Check                                     Passed
--------------------------------------------------------------------------------
PCA Health Checks                                                     Passed
--------------------------------------------------------------------------------
Check Management Nodes Are Running                                    Passed
Check PCA DBs Exist                                                   Passed
[…]
Test for Shares Mounted on Compute Nodes                              Passed
Check Compute Node's Active Network Interfaces                        Passed
--------------------------------------------------------------------------------
PCA Management Node Upgrade                                           Passed
--------------------------------------------------------------------------------
Disable PCA Backups                                                   Passed
Download ISO                                                          Passed
Setup Yum Repo                                                        Passed
[…]
Restore PCA Backups                                                   Passed
Upgrade is complete                                                   Passed
--------------------------------------------------------------------------------
PCA Post-Upgrade Checks                                               Passed
--------------------------------------------------------------------------------
OVM Manager Cache Size Check                                          Passed
--------------------------------------------------------------------------------
Overall Status                                                        Passed
--------------------------------------------------------------------------------
PCA Management Node Pre-Upgrade Checks                                Passed
PCA Health Checks                                                     Passed
PCA Management Node Upgrade                                           Passed
PCA Post-Upgrade Checks                                               Passed

Broadcast message from root@ovcamn05r1 (pts/3) (Wed Mar 23 11:44:23 2022):

Management Node upgrade succeeded. The master manager will be rebooted to
initiate failover in one minute.
```

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

Rollback works for errors that occur during these steps:

Table 1-2 Steps That Support Upgrader Rollback

Upgrading From Release 2.4.4
• downloading the ISO • setting up the YUM repository • taking an Oracle VM backup • breaking the Oracle Private Cloud Appliance HA model

> **Tip:**
>
> When the ISO is copied to the local file system of both management nodes, the management node upgrade time is shortened. The duration of the entire upgrade process depends heavily on the size of the environment: the number of compute nodes and their configuration, the size of the Oracle VM database, etc, and can take from 1.5 to several hours.
>
> If you choose to copy the ISO locally, replace the location URL in the `pca_upgrader` command with `-l file:///`***`<path-to-iso>`***`/ovca-2.4.4.1-bxxx.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>_<hostname_<action>`***`.log`.

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

```
# tail -f /nfs/shared_storage/pca_upgrader/log/pca_upgrader_<date>-
<time>_<hostname_<action>.log
```

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

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

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

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

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

[root@ovcamn06r1 ~]# head /etc/ovca-info
==== Begin build info ====
date: 2022-07-05
release: 2.4.4.1
build: 132
=== Begin compute node info ===
compute_ovm_server_version: 3.4.7
compute_ovm_server_build: 2.4.4-150
compute_rpms_added:
  osc-oracle-s7k-2.1.2-4.el7.noarch.rpm
  ovca-support-2.4.4-97.el7.noarch.rpm
```

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

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

```
root@ovcamn06r1 ~]# pca_upgrader -U -t management -c ovcamn05r1 -g 2.4.4.1 \
-l http://<path-to-iso>/ovca-2.4.4-b132.iso.zip

PCA Rack Type: PCA X8_BASE.

Please refer to log file
/nfs/shared_storage/pca_upgrader/log/pca_upgrader_<date>-
<time>_<hostname_<action>.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 Health Checks                                                     Passed
PCA Management Node Upgrade                                           Passed
PCA Post-Upgrade Checks                                               Passed

Broadcast message from root@ovcamn06r1 (pts/3) (Wed Mar 23 11:44:23 2022):
Management Node upgrade succeeded. The master manager will be rebooted to initiate
failover in one minute.
```

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

> **Tip:**
>
> If the first management node is inadvertently rebooted at this point, the upgrade fails on the second management node. For more information, see Inadvertent Reboot of Stand-by Management Node During Upgrade Suspends Upgrade.

6. Perform the required manual post-upgrade checks on management nodes.

   a. 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.

   b. 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

   c. 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.

   d. Check networks.

      Verify that all networks – factory default and custom – are present and correctly configured.

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/` .

NOT_SUPPORTED:

Do not perform any compute node provisioning operations during firmware upgrades.

Caution:

For certain services it is necessary to upgrade the Hardware Management Pack after a Controller Software update. For additional information, refer to "Some Services Require an Upgrade of Hardware Management Pack" in the Known Limitations and Workarounds section of 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.

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.

> **Caution:**
>
> **Interim Firmware Patches**
>
> Oracle periodically releases firmware patches for many products, for example to limit security vulnerabilities. It may occur that an important firmware patch is released for a component of 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.

Install the Current Firmware on the Management Nodes

To avoid compatibility issues with newer Oracle Private Cloud Appliance Controller Software and Oracle VM upgrades, you should always install the server ILOM firmware included in the ISO image of the current Oracle Private Cloud Appliance software release. When the ISO image is unpacked on the appliance internal storage, the firmware directory can be reached from the management nodes at this location: `/nfs/shared_storage/mgmt_image/firmware/`.

Installing the Current Firmware on the Management Nodes

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

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

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

   b. Extract the management node firmware.

   ```
   [root@ovcamn06r1 ~]# cd /nfs/shared_storage/mgmt_image/firmware/compute/
   X8-2_FIRMWARE/
   [root@ovcamn06r1 X8-2_FIRMWARE]# unzip p33540765_3221_Generic.zip
   ```

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

   ```
   [root@ovcamn06r1 ~]# ssh ilom-ovcamn06r1
   Password:
   Oracle(R) Integrated Lights Out Manager
   Version 5.1.0.20 r145377
   ```

```
Copyright (c) 2022, Oracle and/or its affiliates. All rights reserved.
Warning: HTTPS certificate is set to factory default.
Hostname: ilom-ovcamn06r1
->
```

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

```
-> load -source sftp://root@192.168.4.4/nfs/shared_storage/mgmt_image/
firmware/compute/X8-2_FIRMWARE/
Oracle_Server_X8-2-3.2.2.1.94534-FIRMWARE_PACK/Firmware/service-processor/
ILOM-5_0_2_24_a_r142555-ORACLE_SERVER_X8-2-rom.pkg
```

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

   The reboot should take about 10 minutes.

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

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

```
# cd /nfs/shared_storage/mgmt_image/firmware/compute/X8-2_FIRMWARE/ \
Oracle_Server_X8-2-3.2.2.1.94534-FIRMWARE_PACK/Firmware/SAS9361-16i

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

6. Once the stand-by management node comes back online, reboot the active management node and initiate failover to the newly-updated management node.
7. Log in to the newly-updated management node and run the `pca-check-master` command to confirm it is now the active node.
8. Now that one management node is upgraded and has assumed the active role, repeat this procedure to upgrade the firmware on the other management node.

Upgrading the Operating Software on the Oracle ZFS Storage Appliance

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

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

NOT_SUPPORTED:

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

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

Note:

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

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

Upgrading the ZFS Storage Appliance Operating Software

1. Before initiating the upgrade on the storage controllers, follow the instructions in "Preparing for a Software Upgrade" in Upgrading the Software in the Oracle ZFS Storage Appliance Customer Service Manual, Release OS8.8.x.
2. Log on to the active management node using SSH and an account with superuser privileges.
3. Select the appropriate software update package. The following examples show an upgrade to version *ak-nas-2013.06.05.8.43-1.1.3x-nondebug.pkg*.

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

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

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

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

   ```
   ovcasn01r1:> maintenance system updates
   ovcasn01r1:maintenance system updates> download
   ovcasn01r1:maintenance system updates download (uncommitted)> \
   set url=http://192.168.4.199/storage//FW_Updates/release_folders/
   2.4.4.1/zfs/8.8.43/ak-nas-2013.06.05.8.43-1.1.3x-nondebug.pkg
              url = http://192.168.4.199/storage//FW_Updates/release_folders/
   2.4.4.1/zfs/8.8.43/ak-nas-2013.06.05.8.43-1.1.3x-nondebug.pkg
   ovcasn01r1:maintenance system updates download (uncommitted)> commit
   ```

```
Transferred 2.01G of 2.01G (100%) ... done
Unpacking ... done
```

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

d. Repeat these steps for the second storage controller.

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

   Check the storage cluster configuration. If the storage cluster state is stripped, as shown in the following example, then you are logged in to the standby controller. Go to the next step in this procedure to begin upgrading the standby controller. In the following example, controller `ovcasn02r1` is the standby controller. Upgrade `ovcasn02r1` first.

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

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

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

Children:
                      resources => Configure resources
```

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

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

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

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

RESOURCE        OWNER           TYPE       LABEL         CHANGES  DETAILS
net/i40e4       ovcasn01r1      private    i40e4         no       192.168.4.1
net/ipmp1       ovcasn01r1      singleton  Management... no
192.168.4.100
net/vnic3       ovcasn01r1      singleton  Storage_In... no
192.168.40.1
```

```
net/vnic4       ovcasn01r1      singleton  Storage_In... no       192.168.235.200
net/vnic5       ovcasn01r1      singleton  Storage_In... no       192.168.236.200
zfs/OVCA_POOL   ovcasn01r1      singleton                no       110T
zfs/PCC_internal_pool_HC_01 ovcasn01r1      singleton                no       110T
```

The standby controller does not own any cluster/singleton resource. The standby controller reports only the name of the storage resource, not the size of the storage resource, as shown in the following example on `ovcasn02r1`. In the following example, controller `ovcasn02r1` is the standby controller. Upgrade `ovcasn02r1` first.

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

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

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

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

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

   UPDATE                                      RELEASE DATE              STATUS
   ak-nas@2013.06.05.8.0,1-1.28        2018-8-10 21:22:26   OS8.8.0
   previous
   ak-nas@2013.06.05.8.19,1-1.3        2020-3-2 16:33:02    OS8.8.19
   previous
   ak-nas@2013.06.05.8.20,1-1.3        2020-3-23 16:13:25   OS8.8.20
   waiting
   * ak-nas@2013.06.05.8.20,1-2.20.4392.1 2020-5-22 00:35:42   IDR OS8.8.20
   current
   ak-nas@2013.06.05.8.43,1-1.3        2022-2-25 13:52:55   OS8.8.43
   waiting
   ak-nas@2013.06.05.8.5,1-1.3         2019-3-30 07:27:20   OS8.8.5
   previous
   ak-nas@2013.06.05.8.9,1-1.1         2019-12-11 16:03:04  OS8.8.9
   previous

   [*] : Interim Diagnostics and Relief (IDR)

   Deferred updates:

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

   ovcasn01r1:maintenance system updates> select ak-nas@2013.06.05.8.43,1-1.3
   ```

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

   ```
   ovcasn01r1:maintenance system updates ak-nas@2013.06.05.8.43,1-1.3> check
   You have requested to run checks associated with waiting upgrade media. This
   ```

```
will execute the same
set of checks as will be performed as part of any upgrade attempt to
this media, and will
highlight conditions that would prevent successful upgrade. No actual
upgrade will be attempted,
and the checks performed are of static system state and non-invasive. Do
you wish to continue?

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

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

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

```
ovcasn01r1:maintenance system updates ak-nas@2013.06.05.8.43,1-1.3>
upgrade
The system is currently running an IDR. You might negate the fix
provided with the current IDR.
You may still continue. This procedure will consume several minutes and
requires a system reboot
upon successful update, but can be aborted at any time prior to reboot.
A health check will
validate system readiness before an update is attempted, and may also be
executed independently by
clicking the Check button.

Are you sure? (Y/N) y
Loading media metadata ... done.
Selecting alternate product ... SUNW,maguroZ7
Installing Oracle ZFS Storage ZS7-2 2013.06.05.8.43,1-1.3
pkg://sun.com/ak/SUNW,maguroZ7@2013.06.05.8.43,1-1.3:20220225T135239Z
Creating system/ak-nas-2013.06.05.8.43_1-1.3 ... done.
Creating system/ak-nas-2013.06.05.8.43_1-1.3/install ... done.
Creating system/ak-nas-2013.06.05.8.43_1-1.3/boot ... done.
Creating system/ak-nas-2013.06.05.8.43_1-1.3/root ... done.
Creating system/ak-nas-2013.06.05.8.43_1-1.3/install/svc ... done.
Creating system/ak-nas-2013.06.05.8.43_1-1.3/install/var ... done.
Creating system/ak-nas-2013.06.05.8.43_1-1.3/install/home ... done.
Creating system/ak-nas-2013.06.05.8.43_1-1.3/install/stash ... done.
Creating system/ak-nas-2013.06.05.8.43_1-1.3/wiki ... done.
Creating system/VARSHARE/kvol ... done.
Extracting os image ... done.
Customizing Solaris ... done.
Creating driver_aliases.addendum... done.
Updating vfstab ... done.
Generating usr/man windex ... done.
Generating usr/gnu/share/man windex ... done.
Generating usr/perl5/man windex ... done.
Preserving ssh keys ... done.
Configuring smf(5) ... done.
Extracting appliance kit ... Creating private passwd and shadow
files ... done.
Creating private smbshadow file ... done.
Creating product symlink ... done.
Registering update job 3aaf864a-0e90-47ea-b682-9793e81aa5c7 ... done.
Creating install profile ... done.
Assigning appliance serial number ... d34980cd-703f-4375-823f-
e5cfeff0985d
Determining chassis serial number ... 1830XC200F
Setting appliance product string ... SUNW,maguroZ7
```

```
Setting appliance product class ... nas
Setting install timestamp ... done.
Setting virtualization status ... done.
Saving SSL keys ... done.
Updating phone-home key ... done.
Saving currently running profile ... done.
Installing firmware ... done.
Installing device links ... done.
Installing device files ... done.
Updating device links ... done.
Updating /etc ... done.
Creating /.domainroot ... done.
Installing boot amd64/unix ... done.
Assembling etc/system.d ... done.
Creating factory reset boot archive ... done.
Generating GRUB2 configuration ...  done.
Installing GRUB2 configuration ... done.
Snapshotting zfs filesystems ...  done.
Preserving hostid ... done.
Installation complete - unmounting datasets ...
Creating boot archive ...
done.
Update completed; rebooting.
Connection to 192.168.4.2 closed.
```

d. Update the Oracle ILOM version on the controller.

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

DO NOT INTERRUPT THIS PROCESS.

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

e. At the end of the upgrade, when the controller has fully rebooted and rejoined the cluster, log back in and check the cluster configuration. This can take about 30 minutes. The upgraded controller must still be in the state "Ready (waiting for failback)".

```
Appliance Name: ovcasn02r1
Appliance Product: Oracle ZFS Storage ZS7-2
Appliance Type: Sun ZFS Storage 7370
Appliance Version: 2013.06.05.8.43,1-1.3
First Installed: Sun Sep 23 2018 18:17:48 GMT+0000 (UTC)
Last Updated: Tue Apr 05 2022 05:09:38 GMT+0000 (UTC)
Last Booted: Tue Apr 05 2022 05:41:41 GMT+0000 (UTC)
Appliance Serial Number: dxxxxxx-x03f-433as-8x3f-e5cf9ff0xxd
Chassis Serial Number: 1xxxxxxxxx
Software Part Number: Oracle 000-0000-00
Vendor Product ID: ORACLE-ZFS-ZS7-2
Browser Name: aksh 1.0
Browser Details: aksh
```

```
HTTP Server: Apache/2.4.52 (Unix)
SSL Version: OpenSSL 1.0.2za-fips  24 Aug 2021
Appliance Kit: ak/SUNW,maguroZ7@2013.06.05.8.43,1-1.3
Release Name: OS8.8.43
Operating System: SunOS 5.11 11.4.43.113.3 64-bit
BIOS: American Megatrends Inc. (BIOS)42060700 (BIOS)11.18.2019
Service Processor: 4.0.4.52 r133103
```

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

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

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

7. 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_STRIPPED
                    description = Ready (waiting for failback)
                       peer_asn = 07119e39-af6a-45e4-9c01-8c68ca98db1e
                  peer_hostname = ovcasn01r1
                     peer_state = AKCS_OWNER
               peer_description = Active (takeover completed)
```

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

```
ovcasn01r1:> maintenance system updates
ovcasn01r1:maintenance system updates> list
UPDATE                                RELEASE DATE         RELEASE NAME
STATUS
ak-nas@2013.06.05.8.0,1-1.28          2018-8-10 21:22:26   OS8.8.0
previous
ak-nas@2013.06.05.8.19,1-1.3          2020-3-2 16:33:02    OS8.8.19
previous
ak-nas@2013.06.05.8.20,1-1.3          2020-3-23 16:13:25   OS8.8.20
waiting
* ak-nas@2013.06.05.8.20,1-2.20.4392.1 2020-5-22 00:35:42   IDR
OS8.8.20    current
ak-nas@2013.06.05.8.43,1-1.3          2022-2-25 13:52:55   OS8.8.43
waiting
ak-nas@2013.06.05.8.5,1-1.3           2019-3-30 07:27:20   OS8.8.5
previous
ak-nas@2013.06.05.8.9,1-1.1           2019-12-11 16:03:04  OS8.8.9
previous
ovcasn01r1:maintenance system updates> select ak-
nas@2013.06.05.8.43,1-1.3
ovcasn01r1:maintenance system updates ak-nas@2013.06.05.8.43,1-1.3>
```

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

```
ovcasn01r1:maintenance system updates ak-nas@2013.06.05.8.43,1-1.3> upgrade
The system is currently running an IDR. You might negate the fix provided with
the current IDR.
You may still continue. This procedure will consume several minutes and
requires a system
reboot upon successful update, but can be aborted at any time prior to reboot.
A health check
will validate system readiness before an update is attempted, and may also be
executed
independently by clicking the Check button.

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

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 = d34980cd-703f-4375-823f-e5cfeff0985d
                  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.

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

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

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

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

b. Reboot the active management node.

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

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

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

Verify the status of the services:

```
[root@ovcamn06r1 ~]# service ovca status
Checking Oracle Fabric Manager: Running
MySQL running (70254)                                      [  OK  ]
Oracle VM Manager is running...
Oracle VM Manager CLI is running...
tinyproxy (pid 71315 71314 71313 71312 71310 71309 71308 71307 71306
71305 71301) is running...
dhcpd (pid  71333) is running...
snmptrapd (pid  71349) is running...
log server (pid 6359) is running...
remaster server (pid 6361) is running...
http server (pid 71352) is running...
taskmonitor server (pid 71356) is running...
xmlrpc server (pid 71354) is running...
nodestate server (pid 71358) is running...
sync server (pid 71360) is running...
monitor server (pid 71363) is running...
```

10. 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@2013.06.05.8.43,1-1.3x-nondebug.pkg OS8.8.43_Readme.html
# rm ak-nas@2013.06.05.8.43,1-1.3x-nondebug.pkg OS8.8.43_Readme.html
rm: remove regular file `ak-nas-2013.06.05.8.43-1.1.3x-nondebug.pkg'? yes
rm: remove regular file `OS8.8.43_Readme.html'? yes
# cd ..
# rmdir ak
```

Upgrading the Cisco Switch Firmware

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

> **Caution:**
>
> When upgrading to Controller Software release 2.4.4.1, it is critical that you perform the upgrade operations in the correct order. This means the Cisco switch firmware must be upgraded after the management node upgrade, but before the storage network upgrade.
>
> Do not make any spine switch configuration changes until you have completed **all** the upgrade operations. If you make any spine switch configuration changes before all upgrade operations are complete, you could lose access to the storage network. See "Loading Incompatible Spine Switch Configuration Causes Storage Network Outage" in Known Limitations and Workarounds in the *Oracle Private Cloud Appliance Release Notes*.

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

1. Log on to the active management node using SSH and an account with superuser privileges.
2. Verify that the new Cisco NX-OS software image is available on the appliance shared storage. During the Controller Software upgrade, the Oracle Private Cloud Appliance Upgrader copies the file to the following location:

   ```
   /nfs/shared_storage/mgmt_image/firmware/ethernet/Cisco/nxos.9.3.8.bin
   ```

3. Upgrade the switches, one at a time, in the following order.
   a. Leaf Cisco Nexus 9336C-FX2 Switches: ovcasw15r1, ovcasw16r1

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

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

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

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

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

Determining Which Switch is Primary or Operational Primary

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

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

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

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

```
ovcasw15r1(config)# show vpc role

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

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

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

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

```
ovcasw16r1# show vpc role

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

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

```
ovcasw16r1# show vpc role

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

```
vPC local config role-priority  : 2
vPC peer system-mac             : d4:e8:80:87:eb:4b
vPC peer role-priority          : 1
vPC peer config role-priority   : 1
```

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

```
ovcasw15r1# show vpc role

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

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

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

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

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

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

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

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

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

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

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

   - Leaf and spine switches.

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

     ```
     ovcasw15r1# copy scp://root@192.168.4.216//nfs/shared_storage/mgmt_image/
     firmware/ethernet/Cisco/nxos.9.3.8.bin \
     bootflash:nxos.9.3.8.bin vrf management
     root@192.168.4.216's password:
     nxos.9.3.8.bin                                100%  937MB  16.2MB/s   00:58
     Copy complete, now saving to disk (please wait)...
     Copy complete.
     ```

   - Management switch.

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

     ```
     ovcasw21r1# copy scp://root@192.168.4.216//nfs/shared_storage/mgmt_image/
     firmware/ethernet/Cisco/nxos.9.3.8.bin \
     bootflash:nxos.9.3.8.bin vrf default
     root@192.168.4.216's password:
     nnxos.9.3.8.bin                               100%  937MB  16.2MB/s   00:58
     Copy complete, now saving to disk (please wait)...
     Copy complete.
     ```
4. Verify the impact of the software upgrade.

   ```
   ovcasw15r1# show install all impact nxos bootflash:nxos.9.3.8.bin
   Installer will perform impact only check. Please wait.

   Verifying image bootflash:/nxos.9.3.8.bin for boot variable "nxos".
   [####################] 100% -- SUCCESS

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

   Preparing "nxos" version info using image bootflash:/nxos.9.3.8.bin.
   ```

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

Preparing "bios" version info using image bootflash:/nxos.9.3.8.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 the following table:
Module       Image                 Running-Version(pri:alt)           New-
Version  Upg-Required
------  ----------  ----------------------------------------
--------------------  ------------
     1        nxos                                7.0(3)I7(9)
9.3(8)           yes
     1        bios     v05.44(04/02/2021):v05.33(09/08/2018)
v05.44(04/02/2021)            no
```

5. Save the current running configuration as the startup configuration.

```
ovcasw15r1# copy running-config startup-config
[########################################] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
```

6. Install the Cisco NX-OS software that was copied to the bootflash location. When prompted about the disruptive upgrade, enter `y` to continue with the installation.

```
ovcasw15r1# install all nxos bootflash:nxos.9.3.8.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.9.3.8.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

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

Preparing "nxos" version info using image bootflash:/nxos.9.3.8.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.3.8.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 the following table:
Module       Image                 Running-Version(pri:alt)           New-
Version  Upg-Required
```

```
------  ----------  ----------------------------------------
--------------------  ------------
     1        nxos                                7.0(3)I7(9)
9.3(8)           yes
     1        bios     v05.44(04/02/2021):v05.33(09/08/2018)
v05.44(04/02/2021)            no

Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)?  [n] y

Install is in progress, please wait.

Performing runtime checks.
[####################] 100% -- SUCCESS

Setting boot variables.
[####################] 100% -- SUCCESS

Performing configuration copy.
[####################] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Finishing the upgrade, switch will reboot in 10 seconds.
```

7. After switch reboot, confirm the install succeeded.

```
ovcasw15r1# show install all status
This is the log of last installation.

Verifying image bootflash:/nxos.9.3.8.bin for boot variable "nxos".
 -- SUCCESS

Verifying image type.
 -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.3.8.bin.
 -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.3.8.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 the following table:
Module       Image                 Running-Version(pri:alt)           New-
Version  Upg-Required
------  ----------  ----------------------------------------
--------------------  ------------
     1        nxos                                7.0(3)I7(9)
```

```
9.3(8)           yes
     1        bios     v05.44(04/02/2021):v05.33(09/08/2018)
v05.44(04/02/2021)            no

Switch will be reloaded for disruptive upgrade.

Install is in progress, please wait.

Performing runtime checks.
 -- SUCCESS

Setting boot variables.
 -- SUCCESS

Performing configuration copy.
 -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
 -- SUCCESS

Finishing the upgrade, switch will reboot in 10 seconds.
```

8. Verify that the correct software version is active on the switch.

```
ovcasw15r1# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
[...]

Software
  BIOS: version 05.44
  NXOS: version 9.3(8)
  BIOS compile time:  04/02/2021
  NXOS image file is: bootflash:///nxos.9.3.8.bin
  NXOS compile time:  8/4/2021 13:00:00 [08/04/2021 22:25:26]
[...]

ovcasw15r1#
```

9. Verify the vPC status.

> **Note:**
>
> This step does not apply to the appliance internal management network switch (Cisco Nexus 9348GC-FXP Switch). Proceed to the next step.

Use the command shown below. The output values should match this example.

```
ovcasw15r1# show vpc brief
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link

vPC domain id                     : 2
Peer status                       : peer adjacency formed ok <---- verify this
field
vPC keep-alive status             : peer is alive <----- verify this field
```

```
Configuration consistency status  : success <----- verify this field
Per-vlan consistency status       : success <----- verify this field
Type-2 consistency status         : success <----- verify this field
vPC role                          : primary, operational secondary
Number of vPCs configured         : 27
Peer Gateway                      : Enabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Disabled
Delay-restore status              : Timer is off.(timeout = 30s)
Delay-restore SVI status          : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router    : Enabled
```

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

```
ovcasw15r1# exit
Connection to ovcasw15r1 closed
```

Repeat this procedure for the next switch to be upgraded.

Upgrading the Electronic Programmable Logic Device (EPLD) of all Cisco Leaf, Spine, and Management Switches

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

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

1. Log on to the active management node using SSH and an account with superuser privileges.
2. Verify that the new Cisco NX-OS EPLD firmware image is available on the appliance shared storage. During the Controller Software upgrade, the Oracle Private Cloud Appliance Upgrader copies the file to the following location:

   ```
   /nfs/shared_storage/mgmt_image/firmware/ethernet/Cisco/n9000-epld.9.3.8.img
   ```

3. Log on as `admin` to the first switch to be upgraded.

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

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

   Complete this entire procedure for one switch, then return to this step to upgrade the next switch.

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

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

   - Leaf and spine switches.

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

     ```
     ovcasw15r1# copy scp://root@192.168.4.216//nfs/shared_storage/mgmt_image/
     firmware/ethernet/Cisco/n9000-epld.9.3.8.img \
     bootflash:n9000-epld.9.3.8.img vrf management
     root@192.168.4.216's password:
     n9000-epld.9.3.8.img                          100%  142MB  15.8MB/s   00:09
     Copy complete, now saving to disk (please wait)...
     Copy complete.
     ```

   - Management switch.

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

     ```
     ovcasw21r1# copy scp://root@192.168.4.216//nfs/shared_storage/mgmt_image/
     firmware/ethernet/Cisco/n9000-epld.9.3.8.img \
     bootflash:n9000-epld.9.3.8.img vrf default
     root@192.168.4.216's password:
     n9000-epld.9.3.8.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.9.3.8.img

   Retrieving EPLD versions.... Please wait.
   Images will be upgraded according to the following table:
   Module  Type   EPLD             Running-Version   New-Version  Upg-Required
   ------  ----  -------------      ---------------   -----------  ------------
        1   SUP  MI FPGA                   0x04         0x05            Yes
        1   SUP  IO FPGA                   0x11         0x13            Yes

   Compatibility check:
   Module        Type         Upgradable        Impact   Reason
   -----------------------------------------------
        1            SUP           Yes       disruptive   Module Upgradable
   ```

6. Save the current running configuration as the startup configuration.

   ```
   ovcasw15r1# copy running-config startup-config
   [########################################] 100%
   Copy complete, now saving to disk (please wait)...
   Copy complete.
   ```

> **Note:**
>
> You must upgrade both the primary and golden regions of the FPGA. However, only one upgrade is allowed per reload to avoid programming errors. The next steps describe how to upgrade both regions of the FPGA.

7. Install the Cisco EPLD software that was copied to the bootflash location **to the primary region of the FPGA**. When prompted about the switch reload, enter `y` to continue with the installation.

> **Caution:**
>
> Do not interrupt, power cycle, or reload the switch during the upgrade.

```
ovcasw15r1# install epld bootflash:n9000-epld.9.3.8.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 the following table:
Module  Type   EPLD             Running-Version   New-Version  Upg-Required
------  ----  -------------      ---------------   -----------  ------------
     1   SUP  MI FPGA                   0x04        0x05            No
     1   SUP  IO FPGA                   0x09        0x11           Yes
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ?  [n] y

Proceeding to upgrade Modules.

 Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (     64 of      64 sectors)
Module 1 EPLD upgrade is successful.
Module        Type  Upgrade-Result
------  ------------------  --------------
     1         SUP         Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

Resetting Active SUP (Module 1) FPGAs. Please wait...
```

8. The switch reloads automatically and boots from the backup FPGA. Confirm the primary module upgrade succeeded.

```
ovcasw15r1# show version module 1 epld

EPLD Device                     Version
---------------------------------------
MI FPGA                          0x5
IO FPGA                          0x9
```

At this point, the `MI FPGA` version is upgraded, but the `IO FPGA` version is not upgraded.

9. Install the Cisco EPLD software that was copied to the bootflash location **to the golden region of the FPGA**. When prompted about the switch reload, enter `y` to continue with the installation.

> **Caution:**
>
> Do not interrupt, power cycle, or reload the switch during the upgrade.

```
ovcasw15r1# install epld bootflash:n9000-epld.9.3.8.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...
```

10. The switch reloads automatically and boots from the backup FPGA. Confirm the both upgrades succeeded.

```
ovcasw15r1# show version module 1 epld

EPLD Device                       Version
---------------------------------------
MI FPGA                            0x5
IO FPGA                            0x11
```

11. Verify the vPC status.

> **Note:**
>
> This step does not apply to the appliance internal management network switch (Cisco Nexus 9348GC-FXP Switch). Proceed to the next step.

Use the command shown below. The output values should match this example.

```
ovcasw15r1# show vpc brief
Legend:
                (*) - local vPC is down, forwarding via vPC peer-link
```

```
vPC domain id                     : 2
Peer status                       : peer adjacency formed ok <---- verify
this field
vPC keep-alive status             : peer is alive <----- verify this field
Configuration consistency status  : success <----- verify this field
Per-vlan consistency status       : success <----- verify this field
Type-2 consistency status         : success <----- verify this field
vPC role                          : primary, operational secondary
Number of vPCs configured         : 27
Peer Gateway                      : Enabled
Dual-active excluded VLANs        : -
Graceful Consistency Check        : Enabled
Auto-recovery status              : Disabled
Delay-restore status              : Timer is off.(timeout = 30s)
Delay-restore SVI status          : Timer is off.(timeout = 10s)
Operational Layer3 Peer-router    : Enabled
```

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

```
ovcasw15r1# exit
Connection to ovcasw15r1 closed
```

Repeat this procedure for the next switch to be upgraded.

Install the Current Firmware on All Compute Nodes

Always install the server ILOM and component firmware included in the ISO image of the current Oracle Private Cloud Appliance software release. When the 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. Supported firmware versions are listed in the Oracle Private Cloud Appliance Release Notes.

The following task map outlines the steps you should consider as you update compute node firmware.

Table 1-3 Compute Node Firmware Upgrade Task Map

Component	Resources
Migrate any VMs off of the compute nodes	See Migrate or Move Virtual Machines
Update CX5 card firmware	For general card update instructions, see: Oracle Support Document 2399803.1 • For Oracle Server X9-2 CX5 upgrades use the `Oracle_Dual_Port_CX5_100_Gb_OCP_Adapter` file. • For Oracle Server X8-2 CX5 upgrades use the `Oracle_Dual_Port_100_Gb_RoCE_Adapter` file.

Table 1-3 (Cont.) Compute Node Firmware Upgrade Task Map

Component	Resources
Update RAID Controller firmware	For general card update instructions, see: Oracle Support Document 2399803.1 For Oracle Server X9-2, the RAID firmware is upgraded when the ILOM/BIOS is upgraded, so no further action is necessary.
Update server ILOM/BIOS firmware	For general ILOM/BIOS firmware update instructions, see: Updating System Firmware Using Oracle ILOM
Proceed to Upgrading the Compute Node Software	Upgrading the Virtualization Platform

Upgrading the Virtualization Platform

For Oracle Private Cloud Appliance Controller Software release 2.4.4.1, the compute node upgrade procedure has been reverted to the methodology used in Software release 2.4.3, where 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 2.4.4.1, 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

Caution:

Do not make any management changes during the entire compute node upgrade procedure.

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.

> **Caution:**
>
> Do not use the `add network-to-tenant-group`, `add compute-node`, and `reprovision` CLI commands during the compute node upgrade procedure.

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

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

   ```
   # pca-admin
   Welcome to PCA! Release: 2.4.4.1
   PCA> show version

   ----------------------------------------
   Version              2.4.4.1
   Build                000
   Date                 2022-05-06
   ----------------------------------------

   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 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.

      > **Caution:**
      >
      > 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.

      > **Caution:**
      >
      > 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.