Oracle Private Cloud Appliance

Patching Guide for Release 3.0.1

F49450-09
December 2022

Oracle Private Cloud Appliance Patching Guide for Release 3.0.1,

F49450-09

Contents

Preface

This publication is part of the customer documentation set for Oracle Private Cloud Appliance Release 3.0.2. Note that the documentation follows the release numbering scheme of the appliance software, not the hardware on which it is installed. All Oracle Private Cloud Appliance product documentation is available at https://docs.oracle.com/en/engineered-systems/private-cloud-appliance/index.html.

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

Audience

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

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

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

Feedback

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

Conventions

The following text conventions are used in this document:

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

Documentation Accessibility

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

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

Access to Oracle Support for Accessibility

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

Diversity and Inclusion

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

1

Patching Your Oracle Private Cloud Appliance

This document describes the patching process for your Oracle Private Cloud Appliance. Upgrading your appliance is a different process, refer to the System Upgrade chapter of the Oracle Private Cloud Appliance Administrator Guide for those directions.

Starting with release 3.0.1, Oracle Private Cloud Appliance supports patching updates for security fixes and software errata between major releases. To take advantage of this feature you must configure your environment to support channel updates.

Patches are delivered as RPM packages through a series of dedicated channels on the Unbreakable Linux Network (ULN). To gain access to these channels, you need a Customer Support Identifier (CSI) and a ULN subscription.

Oracle Private Cloud Appliance is not allowed to connect directly to Oracle ULN servers. You must use a ULN mirror on a system inside the data center. The patch channels are then synchronized on the ULN mirror, where the management nodes can access the RPMs. Compute nodes need access to a subset of the RPMs, which are copied to a designated location on the internal shared storage and kept up-to-date.

2
Configure Your Environment for Patching

1. Obtain a valid Customer Support Identifier (CSI).

   Your CSI is an identifier that is issued to you when you purchased the appliance. For more information, see CSI Administration.

2. Register both your mirror server and Oracle Private Cloud Appliance with ULN. See ULN Registration.

3. Create a local ULN mirror. For instructions, see Setting up a Local ULN Mirror. Complete these tasks as you set up your local mirror:

   a. Register your local mirror's hostname in your local DNS.

   b. Subscribe to the following ULN channels for Oracle Private Cloud Appliance. It is best to isolate Oracle Private Cloud Appliance ULN channels from other ULN channels. Reserve approximately 60Gb on your mirror for patches. Over time, you may need to increase this capacity.

      > **Note:**
      >
      > There is no need to subscribe to the * `src` channels. These channels contain source RPMs for the binary channels, which are not used for patching and can take up significant space on your mirror.

      - PCA 3.0.1 Container Images
      - PCA 3.0.1 Firmware
      - PCA 3.0.1 Hypervisor
      - PCA 3.0.1 MN
      - PCA 3.0.1 OCI Compute Images

      > **Caution:**
      >
      > Only install patches from the `pca*` channels. Manually updating the appliance using other channels and other methods is not supported. Security and other updates to Oracle Linux 7 will come through the `pca*` channels.

   c. Verify you have correctly subscribed to the Oracle Private Cloud Appliance channels using the `yum repolist` command.

   d. Optionally, you can add ULN channels from the command line. See Oracle Linux: Managing ULN Channel Subscriptions via Command Line.

4. In the `/etc/sysconfig/uln-yum-mirror` config file, set `ALL_PKGS=1`.

5. Confirm that you have uln mirror version `0.3.0-8.el7` or later installed.

```
#  yum --disablerepo=* --enablerepo=ol7_addons install uln-yum-mirror
Loaded plugins: langpacks, ulninfo
Resolving Dependencies
--> Running transaction check
---> Package uln-yum-mirror.noarch 0:0.3.0-8.el7 will be installed
--> Processing Dependency: hardlinkpy for package: uln-yum-
mirror-0.3.0-8.el7.noarch
--> Processing Dependency: yum-arch for package: uln-yum-
mirror-0.3.0-8.el7.noarch
--> Running transaction check
---> Package hardlinkpy.noarch 0:0.0.5-1.el7 will be installed
---> Package yum-arch.noarch 0:2.2.2-9.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
===
Package Arch Version Repository Size
================================================================================
===
Installing:
uln-yum-mirror noarch 0.3.0-8.el7 ol7_addons 30 k
Installing for dependencies:
hardlinkpy noarch 0.0.5-1.el7 ol7_addons 15 k
yum-arch noarch 2.2.2-9.el7 ol7_addons 311 k

Transaction Summary
================================================================================
===
Install 1 Package (+2 Dependent packages)

Total download size: 356 k
Installed size: 1.3 M
```

6. Create soft links for your local mirror directories.

   a. During the setup of your local mirror, a directory titled "`EngineeredSystems`" was created. The default location of this directory is `/var/www/html/yum/EngineeredSystems`. In order for the patching tool to locate the correct directories, create the following soft links in the `/var/www/html/yum` directory, which contains the `EngineeredSystems` directory:

```
ln -s EngineeredSystems/pca301/hypervisor/x86_64 pca301_x86_64_hypervisor
ln -s EngineeredSystems/pca301/containers/x86_64
pca301_x86_64_container_images
ln -s EngineeredSystems/pca301/fw/x86_64 pca301_x86_64_fw
ln -s EngineeredSystems/pca301/mn/x86_64 pca301_x86_64_mn
ln -s EngineeredSystems/pca301/oci/x86_64 pca301_x86_64_oci
```

   b. Verify that the correct repositories appear on your local mirror.

```
# sudo yum repolist
...
repo id                              repo
name                              status
pca301_x86_64_containers             PCA 3.0.1 Container
Images              39
pca301_x86_64_fw                     PCA 3.0.1
Firmware                          0
```

```
pca301_x86_64_hypervisor            PCA 3.0.1 Hypervisor                9
pca301_x86_64_mn                    PCA 3.0.1 MN                        0
pca301_x86_64_oci                   PCA 3.0.1 OCI Compute Images        3
```

c. Update the repositories. This could take an hour or more for the initial download.

```
# /usr/bin/uln-yum-mirror
```

> **Note:**
>
> For yum servers running Oracle Linux 8 use the `dnf reposync` command.

d. Verify a repodata directory was created at the location of a soft link.

```
# ls /var/www/html/yum/pca301_x86_64_hypervisor/
```

7. Configure the management nodes to receive yum updates from the local mirror.

   By design, compute nodes do not have access outside the appliance. To prepare your environment to patch compute nodes, do the following:

   a. Configure a repository inside the appliance that the compute nodes can reach.

   b. Configure synchronization between that repository and the mirror, through the management nodes.

   To enable synchronization between the repository and the mirror server, set the *fully qualified domain name* of the datacenter mirror server using the `setupstreamUlnMirror` command. Both HTTP and HTTPS protocols are supported. To use HTTPS, see Using HTTPS to Reach the ULN Mirror Server.

```
PCA-ADMIN> setupstreamUlnMirror ulnMirrorLocation=http://host.example.com/yum
Command: setupstreamUlnMirror ulnMirrorLocation=http://host.example.com/yum
Status: Success
Time: 2022-01-06 06:15:15,469 UTC
Data:
  upstream channels are set UpstreamMirror status = success
```

   Alternatively, you can set this parameter in the GUI.

> **Note:**
>
> You must use the fully qualified domain name to reference the datacenter mirror server, not the system IP address.

Using HTTPS to Reach the ULN Mirror Server

To use `https` protocol to reach the ULN mirror, add the TLS trust information for the ULN mirror server to the appliance. The TLS trust information to add to the appliance must contain only a CA chain or an x509 server certificate; the trust information on the appliance must not contain keys:

- If the server certificate is signed by a commercial CA, do not add anything to the appliance. Skip this procedure.
- If the server certificate is signed by a non-commercial CA, the TLS trust information to add to the appliance is the non-commercial CA chain file, in PEM or CRT format.

- If the server certificate is self-signed, the TLS trust information to add to the appliance is a copy of the server certificate, in PEM format.

Repeat this process whenever the X509 server certificate on the ULN mirror server is replaced, such as when the certificate expires:

1. On the first management node, create the following directory if it does not already exist:

   ```
   /etc/pca3.0/vault/customer_ca/
   ```

2. Copy the CA chain or x509 server certificate to the `/etc/pca3.0/vault/customer_ca/` directory.

   If the ULN server certificate is not self-signed, copy the CA chain. If the ULN server certificate is self-signed (the Subject Key Identifier is the same as the Authority Key Identifier), copy the server certificate.

3. Run the following command:

   ```
   python3 /usr/lib/python3.6/site-packages/pca_foundation/secret_service/
   cert_generator/cert_generator_app.py -copy_to_mns
   ```

   The resulting TLS trust/certificate bundle is in the following directory on each management node:

   ```
   /etc/pca3.0/vault/certs/ca_outside_bundle.crt
   ```

Using the Service Web UI

1. a. In the navigation menu, click ULN Mirror.

   b. In the top-right corner of the ULN Mirror page, click Set ULN Mirror.

   The ULN Mirror window appears.

   c. Fill out the parameters:

   - **ULN Mirror:** the fully qualified domain name of the ULN mirror in your datacenter.
   - **Proxy:** If your datacenter uses a proxy server as an intermediary for Internet access, specify that server here.

   d. Click Set ULN Mirror.

   The ULN mirror is set.

3
Prepare for Patching

Before you start a patching procedure, make sure that you have the correct permissions, that you refresh the local datacenter mirror and the secondary management node mirror, and that you have downloaded the RPM packages to the appropriate locations. You should also run health checks and perform a system backup before you begin patching procedures.

1. Verify you have permissions to perform patching operations. Log in to the Service Enclave with an administrator account and enter `showcustomcmds patchRequest` to ensure you have the correct permissions to use the patching commands.

   ```
   PCA-ADMIN> showcustomcmds patchRequest
       patchCN
       patchIlom
       patchOCIImages
       patchSwitch
       patchZfssa
       patchHost
       patchKubernetes
       patchVault
       patchPlatform
       patchMySQL
       patchEtcd
       setUpstreamUlnMirror
       syncUpstreamUlnMirror
       showUpstreamUlnMirror
   ```

   Patching permissions are available to these groups: SuperAdmin, Admin, and DR Admin. For more information, see the Administrator Account Management chapter of the Oracle Private Cloud Appliance Administrator Guide.

2. Log in to the local mirror server and update the Oracle Private Cloud Appliance repositories by entering the following command:

   ```
   # /usr/bin/uln-yum-mirror
   ```

3. Ensure the patch RPM files are updated and in the location you expect, and note the path.

4. After you have updated the local mirror server, update the local repository used for compute node patches by running the `syncUpstreamUlnMirror` command:

   ```
   PCA-ADMIN> syncUpstreamUlnMirror
   Command: syncUpstreamUlnMirror
   Status: Success
   Time: 2022-01-04 15:52:07,120 UTC
   Data:
     Upstream mirror sync started. UpstreamMirror status = success
   ```

   View the status of the update using the `showUpstreamUlnMirror` command.

   ```
   PCA-ADMIN> showupstreamUlnMirror
   Command: showupstreamUlnMirror
   Status: Success
   Time: 2022-01-24 17:29:48,965 UTC
   ```

```
Data:
  Mirror URI = https://host.example.com/yum
```

Alternatively, you can perform this step in the GUI.

Using the Service Web UI

1. In the navigation menu, click ULN Mirror.
2. In the top-right corner of the ULN Mirror page, click Update ULN Mirror.

   The ULN Mirror window appears.
3. Click Sync ULN Mirror.

   The ULN mirror is updated.
4. Ensure the system is in a ready state for patching by performing system health checks. Fix any errors before you proceed with patching a component.

   See the Status and Health Monitoring chapter of the Oracle Private Cloud Appliance Administrator Guide.
5. Perform a system backup before you apply a patch.

   See the Backup and Restore chapter of the Oracle Private Cloud Appliance Administrator Guide.

4
Patching Individual Components

The granular patching mechanism allows you to perform patching procedures for individual hardware and software components. Besides the components included in the management node patch, you can also patch different categories of firmware, the operating system and appliance-specific software on the compute nodes, and Oracle Cloud Infrastructure images.

When you are installing multiple patches at the same time perform the patching operations in this order:

1. Compute nodes
2. Management nodes
3. MySQL cluster database
4. EtcD
5. Vault
6. Kubernetes cluster
7. Platform
8. Firmware

Patching a Compute Node

The compute node patching is similar to the management node host operating system patching: it ensures that the latest Oracle Linux kernel and user space packages are installed, as well as the `ovm-agent` package with appliance-specific optimizations. Compute nodes must be provisioned and locked, then patched one at a time, concurrent patches are not supported. After a successful patch, when a compute node has rebooted, the administrator must manually remove the locks to allow the node to return to normal operation.

Ensure synchronization of the mirror on the shared storage is complete prior to compute node patching by issuing the `syncUpstreamUlnMirror` command. For more information, see Prepare for Patching.

Using the Service Web UI

1. Set the provisioning and maintenance locks for the compute node you are about to patch.

   For more information, refer to "Performing Compute Node Operations" in the Hardware Administration section of the Oracle Private Cloud Appliance Administrator Guide.

   a. In the navigation menu, click Rack Units. In the Rack Units table, click the name of the compute node you want to patch to display its detail page.

   b. In the top-right corner of the compute node detail page, click Controls and select the Provisioning Lock command.

   c. When the provisioning lock is set, click Controls again and select the Maintenance Lock command.

2. In the navigation menu, click Upgrade & Patching.

3. In the top-right corner of the Upgrade Jobs page, click Create Upgrade or Patch.

   The Create Request window appears. Choose *Patch* as the Request Type.

4. Select the appropriate patch request type: Patch CN.

5. If required, fill out the request parameters:

   - **Host IP:** Enter the compute node's assigned IP address in the internal administration network. This is an IP address in the internal 100.96.2.0/23 range.
   - **ULN:** Enter the fully qualified domain name of the ULN mirror in your datacenter: `uln=https://host.example.com/yum`.
   - **Log Level:** Optionally, select a specific log level for the upgrade log file. The default log level is "Information". For maximum detail, select "Debug".
   - **Advanced Options JSON:** Not available.

6. Click Create Request.

   The new patch request appears in the Upgrade Jobs table.

7. When the compute node has been patched successfully, release the provisioning and maintenance locks.

   For more information, refer to "Performing Compute Node Operations" in Hardware Administration.

   a. Open the compute node detail page.

   b. In the top-right corner of the compute node detail page, click Controls and select the Maintenance Unlock command.

   c. When the maintenance lock has been released, click Controls again and select the Provisioning Unlock command.

Using the Service CLI

1. Gather the information that you need to run the command:

   - the fully qualified domain name of the ULN mirror in your datacenter:
   - the IP address of the compute node you intend to patch

2. Set the provisioning and maintenance locks for the compute node you are about to patch.

   For more information, refer to "Performing Compute Node Operations" in the Hardware Administration section of the Oracle Private Cloud Appliance Administrator Guide.

```
PCA-ADMIN> list ComputeNode
Data:
  id                                     name       provisioningState
provisioningType
  --                                     ----       -----------------
----------------
  363a26f4-fa34-4e4c-8e17-a1671a0b77d1   pcacn001   Provisioned         KVM
  9e8745c7-52e3-4aae-984c-e198869ee2cc   pcacn002   Provisioned         KVM
  56a9ecda-2402-427f-92d1-7f9be57dba36   pcacn003   Provisioned         KVM

PCA-ADMIN> provisioningLock id=363a26f4-fa34-4e4c-8e17-a1671a0b77d1

PCA-ADMIN> maintenanceLock id=363a26f4-fa34-4e4c-8e17-a1671a0b77d1
```

3. Enter the patch command.

   Syntax (entered on a single line):

   ```
   patchCN
   hostIp=<compute-node-ip>
   uln=<http|https>://<hostname.domainname>/<sub-directories>
   ```

   Example:

   ```
   PCA-ADMIN> patchCN hostIp=100.96.2.64 ULN=http://host.example.com/yum
   ```

4. Use the request ID and the job ID to check the status of the patching process.

   ```
   PCA-ADMIN> getUpgradeJobs
   ```

5. When the compute node patch has completed successfully and the node has rebooted, release the locks.

   For more information, refer to "Performing Compute Node Operations" in the Hardware Administration section of the Oracle Private Cloud Appliance Administrator Guide.

   ```
   PCA-ADMIN> maintenanceUnlock id=363a26f4-fa34-4e4c-8e17-a1671a0b77d1
   PCA-ADMIN> provisioningUnlock id=363a26f4-fa34-4e4c-8e17-a1671a0b77d1
   ```

6. Proceed to the next compute node and repeat this procedure.

Patching the Management Node Operating System

The Oracle Linux host operating system of the management nodes must be patched one node at a time; a rolling patch of all management nodes is not possible. This patching process, which involves updating the kernel and system packages, must always be initiated from the management node that holds the cluster virtual IP. Thus, in a three-management-node cluster, when you have patched two management nodes, you must reassign the cluster virtual IP to one of the patched management nodes and execute the final patch command from that node. Each management node must be rebooted after a patch is applied.

You must patch management nodes one at a time, using each one's internal IP address as a command parameter. To obtain the host IP addresses, use the Service CLI command `show ManagementNode name=<pcamn01>` and look for the `Ip Address` in the output.

You cannot complete all of the patching tasks required in the Service Web UI for this component. Use the Service CLI to patch the management nodes.

Using the Service CLI

1. Gather the information that you need to run the command:
   - the fully qualified domain name of the ULN mirror in your datacenter
   - the IP address of the management node for which you intend to patch the host operating system
2. Run the Service CLI from the management node that holds the management cluster virtual IP.
   a. Log on to one of the management nodes and check the status of the cluster.

      ```
      # ssh root@pcamn01
      # pcs status
      Cluster name: mncluster
      Stack: corosync
      Current DC: pcamn02 (version 1.1.23-1.0.1.el7-9acf116022) - partition with
      ```

```
quorum

Online: [ pcamn01 pcamn02 pcamn03 ]

Full list of resources:

 scsi_fencing         (stonith:fence_scsi):          Stopped (disabled)
 Resource Group: mgmt-rg
     vip-mgmt-int     (ocf::heartbeat:IPaddr2):      Started    pcamn02
     vip-mgmt-host    (ocf::heartbeat:IPaddr2):      Started    pcamn02
     vip-mgmt-ilom    (ocf::heartbeat:IPaddr2):      Started    pcamn02
     vip-mgmt-lb      (ocf::heartbeat:IPaddr2):      Started    pcamn02
     vip-mgmt-ext     (ocf::heartbeat:IPaddr2):      Started    pcamn02
     l1api            (systemd:l1api):               Started    pcamn02
     haproxy          (ocf::heartbeat:haproxy):      Started    pcamn02
     pca-node-state   (systemd:pca_node_state):      Started    pcamn02
     dhcp             (ocf::heartbeat:dhcpd):        Started    pcamn02
     hw-monitor       (systemd:hw_monitor):          Started    pcamn02

Daemon Status:
  corosync: active/enabled
  pacemaker: active/enabled
  pcsd: active/enabled
```

In this example, the command output indicates that the node with host name `pcamn02` currently holds the cluster virtual IP.

3. Log in to the management node virtual IP and launch the Service CLI.

```
# ssh -l admin 100.96.2.32 -p 30006
```

4. Enter the patch command.

Choose one of the management nodes that is not currently hosting the virtual IP. In the prior example, `pcamn02` holds the cluster virtual IP, so choose either `pcamn01` or `pcamn03` as your patch target.

Syntax (entered on a single line):

```
patchHost
ULN=<http|https>://<hostname.domainname>/<sub-directories>
hostIp=<management-node-ip>
```

Example:

```
PCA-ADMIN> patchHost ULN=http://host.example.com/yum \
patchHost hostIp=100.96.2.33 \
Command: patchHost ULN=http://host.example.com/yum hostIp=100.96.2.33
Status: Success
Time: 2022-01-01 21:06:56.849 UTC
Data: Service request has been submitted.  Upgrade Job ID = 1632990827394-
host-56156 \
Upgrade Request ID = UWS-1a97a8d9-54ef-478d-a0c0-348a17ba6755
```

5. Use the job ID to check the status of the patch process. The job ID is listed in the output of the patch command.

```
PCA-ADMIN> getUpgradeJob upgradeJobId=1632990827394-host-56156
```

6. Exit the Service CLI and reboot the management node you just patched.

```
PCA-ADMIN> exit
Connection to 100.96.2.32 closed.
# ssh root@pcamn01
```

```
root@pcamn01's password:
Last login: Mon Jan 10 20:50:28 2022
# /sbin/reboot
Connection to 100.96.2.33 closed by remote host.
Connection to 100.96.2.33 closed.
```

Wait approximately 5 minutes until the management node restarts.

7. When the first management node host operating system patch has completed successfully, execute the same command for the next management node.

```
PCA-ADMIN> patchHost hostIp=100.96.2.35 \
ULN=http://host.example.com/yum \
```

8. Exit the Service CLI and reboot the management node you just patched.

```
PCA-ADMIN> exit
Connection to 100.96.2.32 closed.
# ssh root@pcamn03
root@pcamn03's password:
Last login: Mon Jan 10 20:50:28 2022
# /sbin/reboot
Connection to 100.96.2.35 closed by remote host.
Connection to 100.96.2.35 closed.
```

Wait approximately 5 minutes until the management node restarts.

9. When the second management node host operating system patch has completed successfully, move the cluster virtual IP to one of the upgraded management nodes.

```
# ssh root@pcamn01
root@pcamn01's password:
Last login: Mon Jan 10 20:50:28 2022
# pcs resource move mgmt-rg pcamn01
# pcs status
Cluster name: mncluster
Stack: corosync
[...]
 scsi_fencing   (stonith:fence_scsi):   Stopped (disabled)
 Resource Group: mgmt-rg
     vip-mgmt-int       (ocf::heartbeat:IPaddr2):       Started pcamn01
     vip-mgmt-host      (ocf::heartbeat:IPaddr2):       Started pcamn01
[...]
```

Moving the cluster virtual IP to another management node should only take a number of seconds and will close your current connection.

10. Log in to the management node virtual IP and launch the Service CLI to execute the host operating system patch for the final management node.

```
# ssh -l admin 100.96.2.32 -p 30006
PCA-ADMIN> patchHost hostIp=100.96.2.34 \
ULN=http://host.example.com/yum \
```

11. Exit the Service CLI and reboot the management node you just patched.

```
PCA-ADMIN> exit
Connection to 100.96.2.32 closed.
# ssh root@pcamn02
root@pcamn02's password:
Last login: Mon Jan 10 21:09:28 2022
# /sbin/reboot
```

Wait approximately 5 minutes until the management node restarts.

When this patch has completed successfully, the operating system on all management nodes is up-to-date.

Patching the MySQL Cluster Database

The MySQL Cluster database is patched independently of the management node host operating system; the MySQL packages are deliberately kept separate from the Oracle Linux upgrade.

Ensure you perform a system backup before you apply a patch. See the Backup and Restore section of the Oracle Private Cloud Appliance Administrator Guide.

Using the Service Web UI

1. In the navigation menu, click Upgrade & Patching.
2. In the top-right corner of the Upgrade Jobs page, click Create Upgrade or Patch.

   The Create Request window appears. Choose *Patch* as the Request Type.
3. Select the appropriate patch request type: Patch MySQL.
4. If required, fill out the patch request parameters:
   - **ULN:** the fully qualified domain name of the ULN mirror in your datacenter.
   - **Advanced Options JSON:** Not available.
   - **Log Level:** Optionally, select a specific log level for the upgrade log file. The default log level is "Information". For maximum detail, select "Debug".
5. Click Create Request.

   The new patch request appears in the Upgrade Jobs table.

Using the Service CLI

1. Gather the information that you need to run the command:
   - the fully qualified domain name of the ULN mirror in your datacenter
2. Enter the patch command.

   Syntax (entered on a single line):

   ```
   patchMySQL
   ULN=<http|https>://<hostname.domainname>/<sub-directories>
   ```

   Example:

   ```
   PCA-ADMIN> patchMySQL ULN=http://host.example.com/yum
   ```
3. Use the request ID and the job ID to check the status of the patch process.

   ```
   PCA-ADMIN> getupgradejobs
   Command: getupgradejobs
   Status: Success
   Time: 2022-01-24 18:53:22,117 UTC
   Data:
     id
   upgradeRequestId                          commandName   result
     --
   ----------------                          -----------   ------
     1642593347925-mysql-40566        UWS-1ee38895-dedf-41c5-ab77-
   eebe294707ed   mysql         Passed
   ```

```
PCA-ADMIN> getupgradejobs requestid=UWS-1ee38895-dedf-41c5-ab77-eebe294707ed
Command: getupgradejobs requestid=UWS-1ee38895-dedf-41c5-ab77-eebe294707ed
Status: Success
Time: 2022-01-24 18:54:05,408 UTC
Data:
  id                              upgradeRequestId
commandName   result
  --                              ----------------
-----------   ------
  1642593347925-mysql-40566       UWS-1ee38895-dedf-41c5-ab77-eebe294707ed
mysql         Passed
```

Patching Etcd and Vault

The secret service contains two components that need to be patched separately: Etcd and Vault. The order in which you patch them is not relevant.

The Etcd and Vault patches are rolling patches: each patch is executed on all three management nodes with one command.

Ensure you perform a system backup before you apply a patch. See the Backup and Restore section of the Oracle Private Cloud Appliance Administrator Guide.

Using the Service Web UI

1. In the navigation menu, click Upgrade & Patching.
2. In the top-right corner of the Upgrade Jobs page, click Create Upgrade or Patch.

   The Create Request window appears. Choose *Patch* as the Request Type.
3. Select the appropriate patch request type: Patch Etcd.
4. If required, fill out the patch parameters:
   - **ULN:** Enter the fully qualified domain name of the ULN mirror in your datacenter.
   - **Advanced Options JSON:** Not available.
   - **Log Level:** Optionally, select a specific log level for the upgrade log file. The default log level is "Information". For maximum detail, select "Debug".
5. Click Create Request.

   The new patch request appears in the Upgrade Jobs table.
6. When the Etcd patch has completed successfully, repeat this procedure to create a patch for Vault.

Using the Service CLI

1. Gather the information that you need to run the command:
   - the fully qualified domain name of the ULN mirror in your datacenter
2. Enter the patch command.

   Syntax (entered on a single line):

   ```
   patchVault
   uln=<http|https>://<hostname.domainname>/<sub-directories>
   ```

```
patchEtcd
uln=<http|https>://<hostname.domainname>/<sub-directories>
```

Example:

```
PCA-ADMIN> patchVault ULN=http://host.example.com/yum

PCA-ADMIN> patchEtcd ULN=http://host.example.com/yum
```

3. Use the request ID and the job ID to check the status of the upgrade process.

```
PCA-ADMIN> getupgradejobs
Command: getupgradejobs
Status: Success
Time: 2022-01-24 18:53:22,117 UTC
Data:
  id
upgradeRequestId                          commandName   result
  --
----------------                          -----------   ------
  1642594274785-vault-29202       UWS-1ee38895-dedf-41c5-ab77-
eebe294707ed   vault         Passed
  1642593966208-etcd-6066         UWS-1ee38895-dedf-41c5-ab77-
eebe294707ed   etcd          Passed

PCA-ADMIN> getupgradejobs requestid=UWS-1ee38895-dedf-41c5-ab77-eebe294707ed
Command: getupgradejobs requestid=UWS-1ee38895-dedf-41c5-ab77-eebe294707ed
Status: Success
Time: 2022-01-24 18:54:05,408 UTC
Data:
  id
upgradeRequestId                          commandName   result
  --
----------------                          -----------   ------
  1642594274785-vault-29202       UWS-1ee38895-dedf-41c5-ab77-
eebe294707ed   vault         Passed
  1642593966208-etcd-6066         UWS-1ee38895-dedf-41c5-ab77-
eebe294707ed   etcd          Passed
```

Patching the Kubernetes Cluster

The Kubernetes container orchestration environment patching is also kept separate from the operating system. With a single command, all Kubernetes packages, such as kubeadm, kubectl and kubelet, are patched on the three management nodes and all the compute nodes. Note that this patching does not include the microservices running in Kubernetes containers.

Ensure synchronization of the mirror on the shared storage is complete prior to Kubernetes patching by issuing the `syncUpstreamUlnMirror` command. For more information, see Prepare for Patching.

Using the Service Web UI

1. In the navigation menu, click Upgrade & Patching.
2. In the top-right corner of the Upgrade Jobs page, click Create Upgrade or Patch.

   The Create Request window appears. Choose *Patch* as the Request Type.
3. Select the appropriate patch request type: Patch Kubernetes.

4. If required, fill out the patch parameters:
   - **ULN:** Enter the fully qualified domain name of the ULN mirror in your datacenter.
   - **Advanced Options JSON:** Not available.
   - **Log Level:** Optionally, select a specific log level for the upgrade log file. The default log level is "Information". For maximum detail, select "Debug".
5. Click Create Request.

   The new patch request appears in the Upgrade Jobs table.

Using the Service CLI

1. Gather the information that you need to run the command:
   - the fully qualified domain name of the ULN mirror in your datacenter
2. Enter the patch command.

   Syntax (entered on a single line):

   ```
   patchKubernetes
   uln=<http|https>://<hostname.domainname>/<sub-directories>
   ```

   Example:

   ```
   PCA-ADMIN> patchKubernetes ULN=http://host.example.com/yum
   ```
3. Use the request ID and the job ID to check the status of the upgrade process.

```
PCA-ADMIN> getupgradejobs
Command: getupgradejobs
Status: Success
Time: 2022-01-18 20:11:16,398 UTC
Data:
  id                                upgradeRequestId
commandName   result
  --                                ----------------
-----------   ------
  1642509549088-kubernetes-51898   UWS-4f0d9e99-a515-4170-ab35-9f8bdcbdb2b5
kubernetes    Passed
  1642492793827-oci-12162          UWS-6e06bbb7-16b8-49ba-9c33-f42fffbe1323
oci           Failed
PCA-ADMIN> getupgradejobs requestid=UWS-4f0d9e99-a515-4170-ab35-9f8bdcbdb2b5
Status: Success
Time: 2022-01-18 20:12:52,760 UTC
Data:
  id                                upgradeRequestId
commandName   result
  --                                ----------------
-----------   ------
  1642509549088-kubernetes-51898   UWS-4f0d9e99-a515-4170-ab35-9f8bdcbdb2b5
kubernetes    Passed
PCA-ADMIN>
```

Patching the Platform

The platform patching covers both the internal services of the platform layer, and the administrative and user-level services exposed through the infrastructure services layer.

The containerized microservices have their own separate patching mechanism. A service is patched if a new Helm deployment chart and container image are found in the `pca301_containers` ULN channel. When a new deployment chart is detected during the patching process, the pods running the services are restarted with the new container image.

Using the Service Web UI

1. In the navigation menu, click Upgrade & Patching.
2. In the top-right corner of the Upgrade Jobs page, click Create Upgrade or Patch.

   The Create Request window appears. Choose *Patch* as the Request Type.
3. Select the appropriate patch request type: Patch Platform.
4. If required, fill out the patch parameters:
   - **ULN:** Enter the fully qualified domain name of the ULN mirror in your datacenter.
   - **Advanced Options JSON:** Not available.
   - **Log Level:** Optionally, select a specific log level for the upgrade log file. The default log level is "Information". For maximum detail, select "Debug".
5. Click Create Request.

   The new patch request appears in the Upgrade Jobs table.

Using the Service CLI

1. Gather the information that you need to run the command:
   - the fully qualified domain name of the ULN mirror in your datacenter
2. Enter the patch command.

   Syntax (entered on a single line):

   ```
   patchPlatform uln=<http|https>://<hostname.domainname>/<sub-
   directories>
   ```

   Example:

   ```
   PCA-ADMIN> patchplatform ULN=http://host.example.com/yum
   Command: patchplatform ULN=http://host.example.com/yum
   Status: Success
   Time: 2021-12-08 17:36:12,217 UTC
   Data:
     Service request has been submitted. Upgrade Job Id = 1638984971208-
   platform-79257 \
   Upgrade Request Id = UWS-39f3f08f-b2d1-4804-8185-2dd3af60dd41
   ```
3. Use the request ID and the job ID to check the status of the upgrade process.

   ```
   PCA-ADMIN> getupgradejobs
   Command: getupgradejobs
   Status: Success
   Time: 2021-12-08 17:36:34,657 UTC
   Data:
     id
   upgradeRequestId                          commandName   result
     --
   ----------------                          -----------   ------
   ```

```
  1638984971208-platform-79257     UWS-39f3f08f-b2d1-4804-8185-2dd3af60dd41
platform      None

PCA-ADMIN> getupgradejob upgradeJobId=1638984971208-platform-79257
Command: getupgradejob upgradeJobId=1638984971208-platform-79257
Status: Success
Time: 2021-12-08 17:36:19,385 UTC
Data:
  Upgrade Request Id = UWS-39f3f08f-b2d1-4804-8185-2dd3af60dd41
  Name = platform
  Start Time = 2021-12-08T17:36:11
  Pid = 79257
  Host = pcamn02
  Log File = /nfs/shared_storage/pca_upgrader/log/pca-
upgrader_platform_services_2021_12_08-17.36.11.log
  Arguments =
{"component_names":null,"diagnostics":false,"display_task_plan":false,"dry_run_task
s":false, \

"expected_iso_checksum":null,"fail_halt":false,"fail_upgrade":null,"image_location"
:null, \
[...]
  Process = alive
  Tasks 1 - Name = Validate ULN Channel URL
  Tasks 1 - Description = Verify that the ULN channel URL is accessible
  Tasks 1 - Time = 2021-12-08T17:36:12
[...]
```

Patching Firmware

Firmware is included in the ISO image for all component ILOMs, for the Oracle ZFS Storage Appliance, and for the switches. Select the instructions below for the component type you want to patch.

Obtaining an ILOM IP Address

Using the Service Web UI

1. In the navigation menu, click Rack Units.
2. Click on the name of the component you are patching.
3. Select the Rack Unit Information tab.
4. Record the IP Address listed under ILOM IPs.

Using the Service CLI

1. Find the component ID:

   Syntax (entered on a single line):

   ```
   list <component>
   ```

   Example:

   ```
   PCA-ADMIN> list computeNode
   Command: list computeNode
   Status: Success
   Time: 2021-12-17 21:30:41,064 UTC
   ```

```
Data:
  id                                     name       provisioningState
provisioningType
  --                                     ----       -----------------
----------------
  03111396-bb33-4249-9561-b921387c6f3a   pcacn003   Provisioned         KVM
  1600443b-00f3-4424-946d-bd52df778aaf   pcacn001   Provisioned         KVM
  69e4e3b7-9390-4283-b246-49ebedccac95   pcacn002   Provisioned         KVM
```

2. Use the component ID to show the details of that component.

```
PCA-ADMIN> show computeNode id=03111396-bb33-4249-9561-b921387c6f3a
Command: show computeNode id=03111396-bb33-4249-9561-b921387c6f3a
Status: Success
Time: 2021-12-17 21:42:47,724 UTC
Data:
  Id = 03111396-bb33-4249-9561-b921387c6f3a
  Type = ComputeNode
  Provisioning State = Provisioned
[...]
  Ip Address = 100.96.2.64
  ILOM Ip Address = 100.96.0.64
  Hostname = pcacn001
[...]
```

Patching ILOMs

ILOM patches can be applied to management nodes and compute nodes. Firmware packages may be different per component type, so make sure you select the correct one from the firmware directory. You must patch ILOMs one at a time, using each one's internal IP address as a command parameter.

> **Caution:**
>
> You must NOT patch the ILOM of the management node that holds the management virtual IP address, and thus the primary role in the cluster. To patch its ILOM, first reboot the management node in question so that another node in the cluster takes over the primary role. Once the node has rebooted completely, you can proceed with the ILOM patch.
>
> To determine which management node has the primary role in the cluster, log in to any management node and run the command `pcs status`.

Using the Service Web UI

1. In the navigation menu, click Upgrade & Patching.
2. In the top-right corner of the Upgrade Jobs page, click Create Upgrade or Patch.

   The Create Request window appears. Choose *Patch* as the Request Type.
3. Select the appropriate patch request type: Patch ILOM.
4. Fill out the patch parameters:
   - **ULN:** Enter the fully qualified domain name of the ULN mirror in your datacenter.
   - **Host IP:** Enter the component's assigned IP address in the ILOM network.

- **Advanced Options JSON:** Not available.
- **Log Level:** Optionally, select a specific log level for the upgrade log file. The default log level is "Information". For maximum detail, select "Debug".

5. Click Create Request.

   The new patch request appears in the Upgrade Jobs table.

Using the Service CLI

1. Gather the information that you need to run the command:
   - the IP address of the ILOM for which you intend to patch the firmware
   - the fully qualified domain name of the ULN mirror in your datacenter
2. Enter the patch command.

   Syntax (entered on a single line):

   ```
   patchIlom
   hostIp=<ilom-ip>
   uln=<http|https>://<hostname.domainname>/<sub-directories>
   ```

   Example:

   ```
   PCA-ADMIN> patchIlom hostIp=100.96.4.62 \
   ULN=http://host.example.com/yum \
   ```

3. Use the request ID and the job ID to check the status of the upgrade process.

   ```
   PCA-ADMIN> getUpgradeJobs
     id                              upgradeRequestId
   commandName   result
     --                              ----------------
   -----------   ------
     1620921089806-ilom-21480        UWS-732d6fce-9f06-4329-b972-d093bee40010
   ilom          Passed

   PCA-ADMIN> getupgradejobs requestid=UWS-732d6fce-9f06-4329-b972-d093bee40010
   Command: getupgradejobs requestid=UWS-732d6fce-9f06-4329-b972-d093bee40010
   Status: Success
   Time: 2022-01-24 18:23:39,690 UTC
   Data:
     id                              upgradeRequestId
   commandName   result
     --                              ----------------
   -----------   ------
     1620921089806-ilom-21480        UWS-732d6fce-9f06-4329-b972-d093bee40010
   ilom          Passed
   ```

4. Use the `syncHardwareData` command to update the hardware attributes in the system hardware database.

> **Note:**
>
> The `syncHardwareData` command is also used for internal automated system tasks. If this automated task is running when you issue the `syncHardwareData` command manually, a lock will prevent your command from running and you could see this error:
>
> ```
> This command cannot be performed at this time. Please try
> again.
> ```
>
> Wait a few moments, then re-issue the `syncHardwareData` command.

At the end of the patch, the ILOM itself is rebooted automatically. However, the server component also needs to be rebooted for all changes to take effect.

Patching the ZFS Storage Appliance Operating Software

To patch the operating software of the system's ZFS Storage Appliance, you only need to provide the path to the ULN mirror. The IP addresses of the storage controllers are known, and a single command initiates a rolling patch of both controllers.

> **Caution:**
>
> Ensure users are not logged in to the ZFS Storage Appliance or the ZFS Storage Appliance ILOM during the upgrade process.

> **Caution:**
>
> Do not make storage configuration changes while an upgrade is in progress. While controllers are running different software versions, configuration changes made to one controller are not propagated to its peer controller.

> **Note:**
>
> ZFS Storage Appliance updates may include ILOM and or BIOS firmware. If an update to the BIOS firmware is required, there will be a note in the Upgrader log indicating that the BIOS will be updated the next time the storage head is shut down.

Using the Service Web UI

1. In the navigation menu, click Upgrade & Patching.
2. In the top-right corner of the Upgrade Jobs page, click Create Upgrade or Patch.

   The Create Request window appears. Choose *Patch* as the Request Type.

3. Select the appropriate patch request type: Patch Zfssa.
4. Fill out the patch parameters:
   - **ULN:** Enter the fully qualified domain name of the ULN mirror in your datacenter.
   - **Advanced Options JSON:** Not available.
   - **Log Level:** Optionally, select a specific log level for the upgrade log file. The default log level is "Information". For maximum detail, select "Debug".
5. Click Create Request.

   The new patch request appears in the Upgrade Jobs table.

Using the Service CLI

1. Gather the information that you need to run the command: the path to the AK-NAS firmware package in the ULN mirror.
2. Enter the patch command.

   Syntax:

   ```
   patchZfssa uln=<http|https>://<hostname.domainname>/<sub-
   directories>
   ```

   Example:

   ```
   PCA-ADMIN> patchZfssa ULN=http://host.example.com/yum
   ```

3. Use the request ID and the job ID to check the status of the upgrade process.

   ```
   PCA-ADMIN> getUpgradeJobs
   Status: Success
   Time: 2022-01-24 18:19:29,731 UTC
   Data:
     id                                upgradeRequestId
   commandName   result
     --                                ----------------
   -----------   ------
     1643035466051-zfssa-62915         UWS-831fd008-cc32-428d-8e76-91c43081f6e7
   zfssa         Passed

   PCA-ADMIN> getupgradejobs requestid=UWS-831fd008-cc32-428d-8e76-91c43081f6e7
   Command: getupgradejobs requestid=UWS-831fd008-cc32-428d-8e76-91c43081f6e7
   Status: Success
   Time: 2022-01-24 18:27:52,083 UTC
   Data:
     id                            upgradeRequestId
   commandName   result
     --                            ----------------
   -----------   ------
     1643035466051-zfssa-62915     UWS-831fd008-cc32-428d-8e76-91c43081f6e7
   zfssa         Passed
   ```

Patching the Switch Software

The appliance rack contains three categories of Cisco Nexus switches: a management switch, two leaf switches, and two spine switches. They all run the same Cisco NX-OS network operating software. There is no preferred patching order for the switches.

When patching their firmware, use the same binary file with each patch command. Only one command per switch category is required, meaning that the leaf switches and the spine switches are patched in pairs.

Using the Service Web UI

1. In the navigation menu, click Upgrade & Patching.
2. In the top-right corner of the Upgrade Jobs page, click Create Upgrade or Patch.

   The Create Request window appears. Choose *Patch* as the Request Type.
3. Select the appropriate patch request type: Patch Switch.
4. Fill out the patch parameters:
   - **ULN:** Enter the fully qualified domain name of the ULN mirror in your datacenter.
   - **Advanced Options JSON:** Not available.
   - **Log Level:** Optionally, select a specific log level for the upgrade log file. The default log level is "Information". For maximum detail, select "Debug".
   - **Switch Type:** Select the switch type you intend to patch. The preferred order is as follows: leaf switches first, then spine switches, and finally the management switch.
5. Click Create Request.

   The new patch request appears in the Upgrade Jobs table.
6. When the patch has completed successfully, but other switches in the system still need to be patched, repeat this procedure for any other type of switch that requires patching.

Using the Service CLI

1. Gather the information that you need to run the command:
   - the type of switch to patch (spine, leaf, management)
   - the fully qualified domain name of the ULN mirror in your datacenter
2. Enter the patch command.

   Syntax (entered on a single line):

   ```
   patchSwitch
   switchType=[MGMT, SPINE, LEAF]
   imageLocation=<http|https>://<hostname.domainname>/<sub-
   directories>
   ```

   Example:

   ```
   PCA-ADMIN> patchSwitch switchType=LEAF \
   imageLocation=http://host.example.com/yum \
   ```
3. Use the request ID and the job ID to check the status of the upgrade process.

   ```
   PCA-ADMIN> getUpgradeJobs
   ```
4. Use the `syncHardwareData` command to update the hardware attributes in the system hardware database.

> **Note:**
>
> The `syncHardwareData` command is also used for internal automated system tasks. If this automated task is running when you issue the `syncHardwareData` command manually, a lock will prevent your command from running and you could see this error:
>
> ```
> This command cannot be performed at this time. Please try again.
> ```
>
> Wait a few moments, then re-issue the `syncHardwareData` command.

Patching Oracle Cloud Infrastructure Images

When new Oracle Cloud Infrastructure Images become available and supported for Oracle Private Cloud Appliance between major releases, you can pick up these images using the patching process.

Oracle Cloud Infrastructure Images installed using the patching method are stored in the `/nfs/shared_storage/oci_compute_images` directory on the ZFS storage appliance.

Using the Service Web UI

1. In the navigation menu, click Upgrade & Patching.
2. In the top-right corner of the Upgrade Jobs page, click Create Upgrade or Patch.

   The Create Request window appears. Choose *Patch* as the Request Type.
3. Select the appropriate patch request type: Patch OCIImages.
4. If required, fill out the request parameters:
   - **ULN:** Enter the path to the shared storage.
   - **Advanced Options JSON:** Not available.
   - **Log Level:** Optionally, select a specific log level for the upgrade log file. The default log level is "Information". For maximum detail, select "Debug".
5. Click Create Request.

   The new patch request appears in the Upgrade Jobs table.

Using the Service CLI

1. Gather the information that you need to run the command:
   - the fully qualified domain name of the ULN mirror in your datacenter
2. Enter the patch command.

   Syntax (entered on a single line):

   ```
   patchOCIimages
   uln=<http|https>://<hostname.domainname>/<sub-directories>
   ```

   Example:

   ```
   PCA-ADMIN> patchOCIimages ULN=http://host.example.com/yum
   ```

3. Use the request ID and the job ID to check the status of the patching process.

```
PCA-ADMIN> getupgradejobs
Command: getupgradejobs
Status: Success
Time: 2022-01-18 19:58:34,745 UTC
Data:
  id                              upgradeRequestId
commandName   result
  --                              ----------------
-----------   ------
  1641839285475-oci-94665         UWS-778b08bc-f579-492b-993d-915dcf581374
oci           Passed
  1641838937541-platform-56313    UWS-bc4372ae-8f51-4b40-9306-992fb6459878
platform      Failed

PCA-ADMIN> getupgradejobs requestid=UWS-778b08bc-f579-492b-993d-915dcf581374
Command: getupgradejobs requestid=UWS-778b08bc-f579-492b-993d-915dcf581374
Status: Success
Time: 2022-01-18 20:00:43,804 UTC
Data:
  id                          upgradeRequestId
commandName   result
  --                          ----------------
-----------   ------
  1641839285475-oci-94665     UWS-778b08bc-f579-492b-993d-915dcf581374
oci           Passed
PCA-ADMIN>
```