CBAC-D Installation and Upgrade Guide

CBAC-R4.1.0

September 2024

Radisys Corporation.
Headquarters: Hillsboro, Oregon
8900 NE Walker Rd. Suite 130
Hillsboro, OR 97006
United States
+1.503.615.1100
sales@radisys.com
+1.503.615.1115

Contents

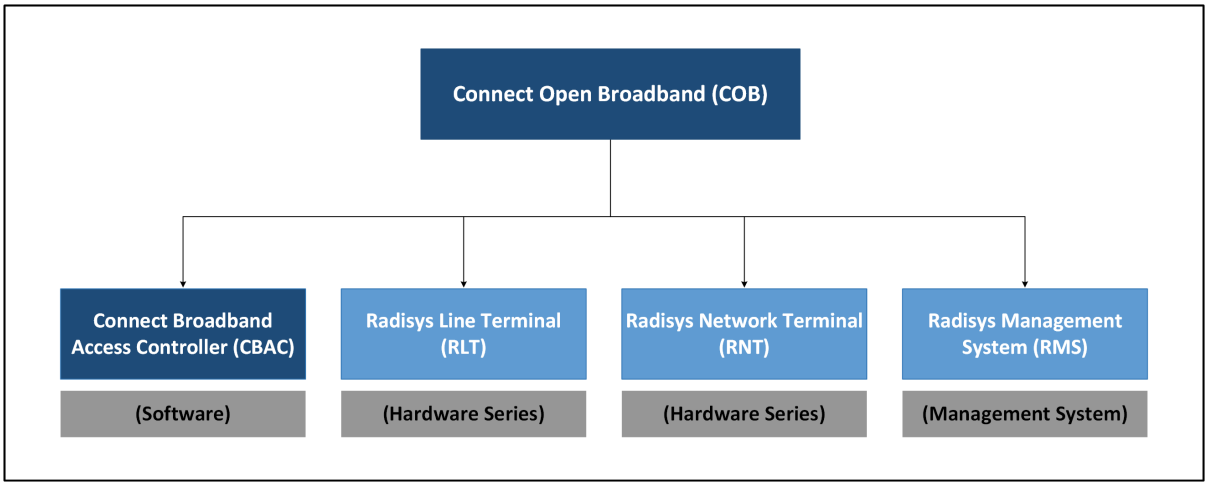
Preface

About this Guide

The Radisys Connect Open Broadband solution is a software-driven broadband access solution that simplifies fiber network management with a highly programmable framework based on open standards and disaggregated architecture.

The following figure illustrates various components of the Connect Open Broadband solution.

Figure 1. Connect Open Broadband Components



As highlighted in Figure 1: Connect Open Broadband Components *(on page 8)*, this guide describes the hardware and network requirements, and deployment procedure for the Connect Broadband Access Controller (CBAC) software.

For more information on the other components and their features, refer to the documents of the respective components.

Note: Internally we reference CBAC as SDPON and you may find instances of SDPON. These two terms refer to the same application.

Audience

This guide is intended for experienced network system administrators who are responsible for installing, configuring, and maintaining the COB solution.

What's New in this Manual

The following features are added or updated in this release.

For Information on...	See in this Manual...
FEC Enable/Disable Support for NNI Ports	Configuring FEC on NNI Port *(on page 49)*
Enable TACACS+ AAA in RMS and CBAC for Default User Roles	Configuring TACACS Server *(on page 240)*
Port Mirroring - Mirror Feature on OLT Data Ports	Mirroring on OLT Data Ports *(on page 257)*

Documentation Map

For more information on the tasks and corresponding documents, refer to the *Documentation Map*.

About Related Radisys Products

For information on Radisys CBAC and other Radisys products, see the Radisys Website at http://www.radisys.com

Notational Conventions

This manual uses the following conventions.

BoldText	A keyword.
ItalicText	File, function, and utility names.
`MonoText`	Screen text and syntax strings.
`BoldMonoText`	A command to enter.
ItalicMonoText	Variable parameters.
Brackets [ ]	Command options.
Curly braces { }	A grouped list of parameters.
Vertical line |	An *"OR"* in the syntax. Indicates a choice of parameters.

All numbers are decimal unless otherwise stated.

Deployment Requirements

This chapter provides information about the deployment requirements of the COB solution.

Hardware Requirements

The following hardware components are required for network connectivity.

- CBAC compliant white-box Optical Line Terminals (OLTs) with transceivers - Mandatory
- Optical Network Terminals (ONTs)/Residential Gateways (RGs) - Mandatory
- Passive Optical Network (PON) splitters - Mandatory
- Network switches - Optional
- Broadband Network Gateways (BNGs) - Optional
- A server with the following specifications:

Table 1. Server Specifications

Server	Specification
Log server	vCPU: 8 RAM: 8 GB Disk: 1 TB
Repository server and Docker registry	vCPU: 8 RAM: 8 GB Disk: 1 TB

Software Requirements

The CBAC components run as docker containers orchestrated by Kubernetes. The following tables show the version and various components of the COB solution.

Table 2. COB Solution Components

File Name	Content
CBAC-R4.1.0	A folder includes the following packages.
SDPON.1.21.133.tar.gz	Includes the CBAC-D release package.
ROLT.1.21.143.tar.gz	Includes the ONL image (Debian 10 - Buster) and OLT binaries.
RMS.15.9.19.tar.gz	Includes the RMS package. Image version–v15.9.19.

Component Name	Version
Kubernetes	1.28.6
Python	CBAC - 3.9.2 RMS - 3.6.9
Docker	20.10.20
BAL	3.12.11.11.17

System Requirements

The following are the system requirements for the Open Network Linux (ONL) installation.

- Hardware
  - Console cable
  - Network cable
- Software
  - DHCP server
  - Console utility such as Tera Term or PuTTY

Environment Setup

Perform the following steps to set up the environment for the ONL installation.

Hardware

1. Connect the console cable (serial port) to your PC/NB.
2. Connect the console cable to the port available on the front panel.
3. Connect the network cable to the server PC (DHCP/TFTP). The management port is available on the front panel.

Software

1. Launch the console utility.

   Baud rate: 115200

   Parity: None

   Data bit: 8

   Stop bit: 1

Note:

The MTU size of CBAC is configured as 9600 (Default value). This specific MTU setting is applicable to the IPv6 environments.

Verify the MTU settings across links for any communication issues between RMS and CBAC during the deployment or upgrade procedure.

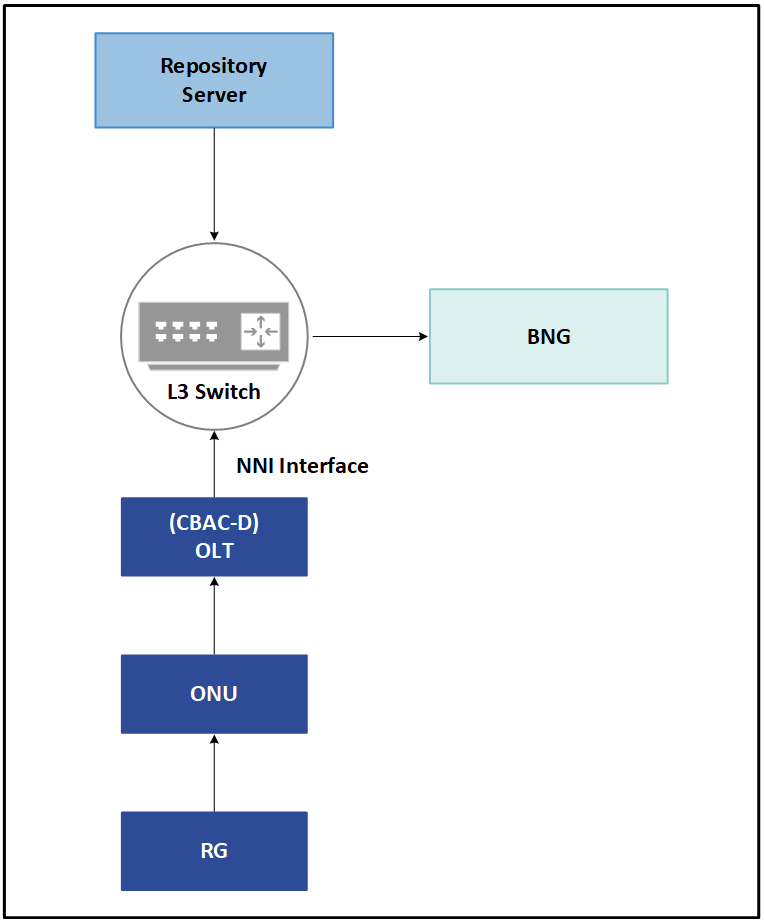
Configuring COB Solution

This chapter covers the network configuration of the COB solution.

In-band Configuration

The following figure shows the network configuration of the COB solution in-band management.

Figure 2. In-band Network Configuration



Deploying OLT and CBAC

This section covers the following.

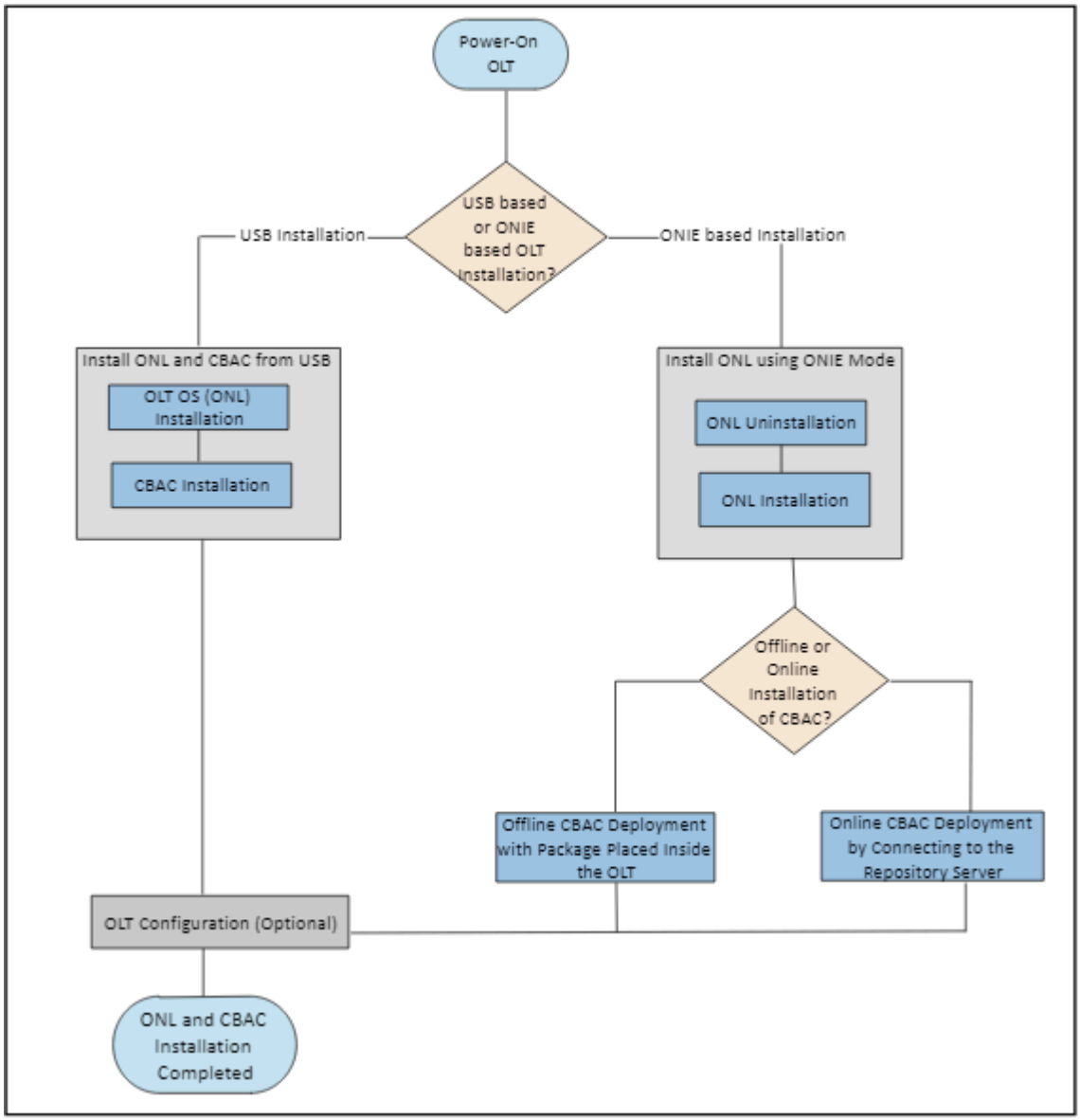
- OLT and CBAC Installation Flow
- Installation of ONL and CBAC using a USB Device
- Installation of ONL using ONIE Mode
- Verifying the ONL Installation and CBAC Installation

OLT and CBAC Installation Flow

This section covers the Installation of ONL (OS) and CBAC software.

The following figure illustrates the installation flow of the CBAC and ONL.

Figure 3. CBAC and ONL Installation Flow



1. Installing ONL and CBAC using USB Device *(on page 16)*
2. Installing CBAC Software *(on page 32)*
3. Uninstalling ONL *(on page 25)*
4. Installing ONL Image *(on page 27)*
5. Offline CBAC Deployment with Package Placed Inside OLT *(on page 32)*
6. Online CBAC Deployment by Connecting to Repository Server *(on page 36)*
7. Configuring the Radisys OLT *(on page 44)*

The installation consists of two steps, the installation of OS (ONL) followed by the CBAC software.

There are two ways to install the OS (ONL).

1. Installing ONL and CBAC using USB Device *(on page 16)*
2. Installing ONL using ONIE Mode *(on page 24)*

Prerequisites for Software Installation at Site

The field engineer must carry the following software installation kit before arriving at the site.

- Laptop (non-domain)
- Console cable compatible with the Radisys OLT
- USB device with the required software
- One working CAT5/6 cable
- Remote access software like Anydesk installed on the laptop
- Internet access to remotely connect to the laptop

The field engineer must perform the following steps.

1. Physically install the OLT and connect the DC power cables from the MCB (Miniature Circuit Breakers) to the power slots of the OLT.
2. Switch on the MCB so that power is applied to the OLT and wait for 4 minutes for the OLT to boot up.
3. The user can access the OLT through the serial console or SSH.
   a. To access the OLT through the serial console cable.

      Connect console to the laptop's CRAFT port and connect it to the OLT.

   b. To access using SSH (Accessing using SSH is applicable only for installing ONL and CBAC using a USB device).
      i. Connect the ethernet cable to the laptop and OLT’s out-of-band interface.
      ii. Assign the same subnet IP (192.168.1.0/24) address to the laptop.
      iii. Ssh from laptop to the OLT using default IP (192.168.1.1) .

Note: From release 4.0.0 onward, a default IP address is assigned to the out-of-band interface on factory installed OLT that can be used to connect to the OLT using SSH in field deployments. If the ONL version is below 4.0, use the console approach to access the OLT. When the ONL version is unknown, check for the installed ONL version on OLT using a console cable as mentioned below.

Installing ONL and CBAC using USB Device

This section covers the installation of ONL and CBAC.

Setting up an OLT in the field requires network connectivity and copying images from a remote location. This process can be time consuming and error prone. The USB based method provides faster and easier way of installation. This is an integrated installation method of ONL and CBAC.

The high-level steps are mentioned below.

1. Prepare a USB device with the necessary software files.
2. Copy the installation script to the OLT from the USB device (If the installed base ONL version on the OLT is R3.2.1 and above, then copying of the installation script is not required as the installation script is part of the ONL software build).
3. With the release of CBAC release 4.0, OLTs that are factory shipped have a default IP address of 192.168.1.1 on out-of-band interface. The user can access the OLT through the console or SSH using the default IP.

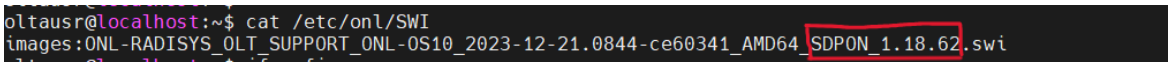
Prerequisites

The following prerequisites must be fulfilled to prepare the USB device for installation.

- **Check the ONL verison**. This step is applicable for the installation of any ONL version 2.9.x or above.

  The following screenshot shows how to check ONL version of the OLT.

  Figure 4. Installed Version of the ONL on the OLT



Note:

1. The installation engineer must format the USB device in FAT32 format. If the size of the USB device exceeds 32GB, Refer to Formatting the USB Device using Rufus Tool *(on page 266)* for formatting the USB device.
2. All partitions on the USB device must be in FAT32 format.
3. Only one copy of Figure 5: USB Device Installation Files *(on page 18)* must be present in the USB device, and they must be located in the same partition.
4. Any file other than the Figure 5: USB Device Installation Files *(on page 18)* can be stored on a USB device.

Copying Files to USB Device

This section covers the details of files that must be copied to the USB device.

- Copy the required ONL image to the USB device and change the name of the ONL image to *onie-installer* and ensure that the *onie-installer* image has executable permission.

  For example, if the original build image of R4.1.0 is *ONL-SDPON_ONL-OS11_2024-03-15.1217-f294004_AMD64_DSDPON_RSYS_1.19.143_INSTALLED_INSTALLER*, this software image has to be moved to the USB device, and then the software image name must be changed to *onie-installer*.

- Copy the required CBAC image in *tar.gz* format to the USB device.

  For example, if the R4.1.0 CBAC release has the version tag *SDPON.1.19.122.tar.gz*, copy the complete file to the USB device.

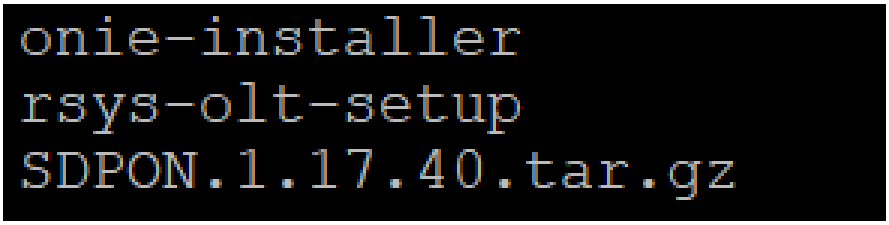
Important: The file name format must be strictly followed as SDPON.X.Y.Z.tar.gz.

- Copy the Installation script *rsys-olt-setup* to the USB device. Ensure that the script has executable permission. The *rsys-olt-setup* file is a bash script that performs the required installation on the OLT.

  Note: From 3.2.1, the base ONL image includes the *rsys-olt-setup* installation script. Hence, there is no need to copy the script from the USB to the OLT for an installation or update. The script is available in the */sbin* directory.

- The USB must contain the following three files.
  - *onie-installer* (This is the ONL installer image renamed as *onie-installer*)
  - *rsys-olt-setup* (Installation script)
  - The offline CBAC installation package in *tar.gz* format (For example, *SDPON.1.17.40.tar.gz*)

Figure 5. USB Device Installation Files



Copying Installation Script (rsys-olt-setup) to OLT from USB Device

If base ONL version is below 3.2.1, copy the installation script (*rsys-olt-setup*) to the OLT from the USB device as mentioned below.

Note: A few ONL versions below 3.2.1 contain an older version of *rsys-olt-setup* prepackaged in the ONL. Hence, it is recommended to copy the latest version from the USB device and use the same. If the *rsys-olt-setup* is not available in the package, contact the Radisys Support team.

An installation engineer must access the OLT before performing the following steps. For more information on steps to access OLT, see Prerequisites *(on page 17)*.

Perform the following steps to copy the installation script to the OLT from the USB storage device.

1. Connect the USB device to the OLT.

   The USB port is seen on the front panel of the OLT to which the USB device must be connected.

2. Login to the OLT.

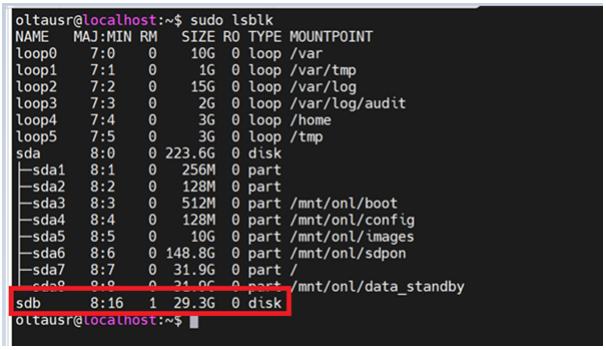
   For more information on the Connecting to the Serial Console Port, refer to the *RLT 1600G and 1600X Hardware and Installation Guide*.

- Execute the following command to find the USB device name.

```
sudo lsblk
```

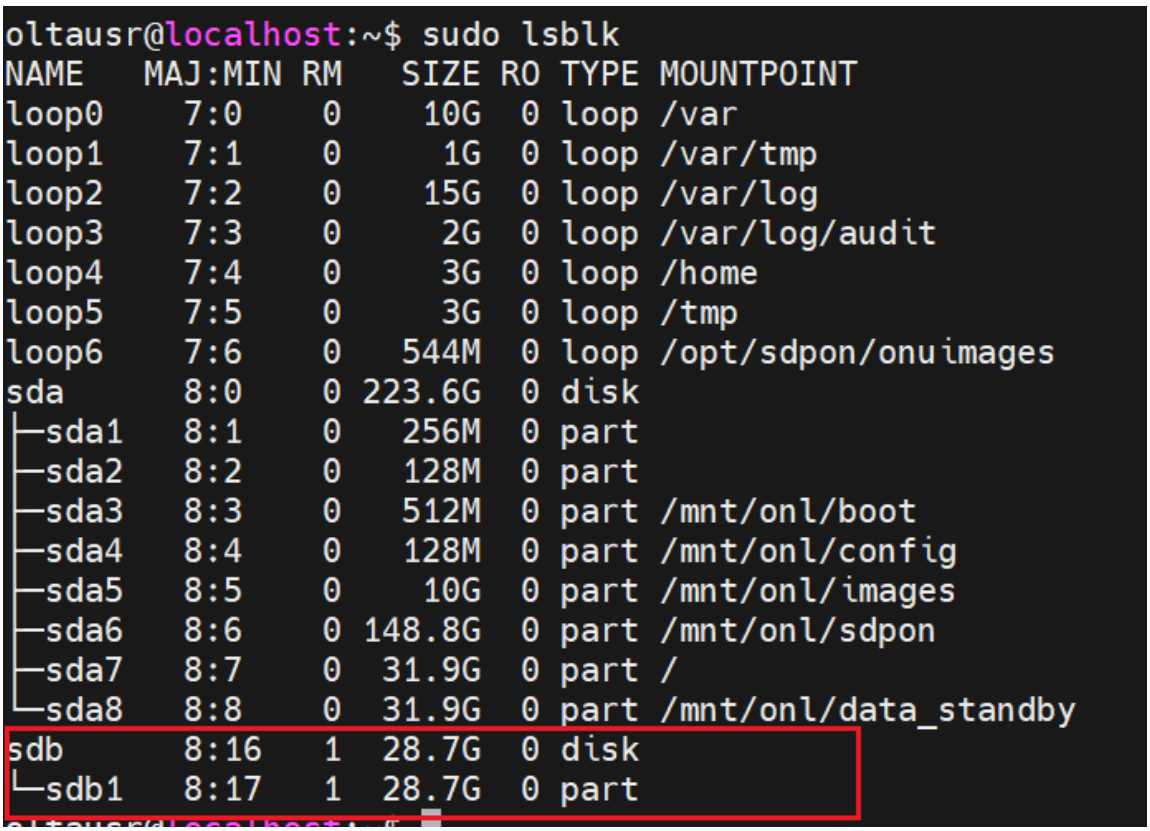
The following screenshot shows the detected USB device name on the OLT with the name *sdb*.

Figure 6. Detect USB Device



The **`lsblk`** output differs based on the number of partitions created in the USB device.

The following figure shows the lsblk output when the USB device is formatted with one partition */dev/sdb1*.



3. Execute the following command to check the file system type of the USB device.

```
sudo lsblk -f
```

The following figure shows the FSTYPE is **vfat** indicating that USB is formatted as FAT32.

```
oltausr@localhost:~$ sudo lsblk -f
NAME   FSTYPE FSVER LABEL           UUID                                 FSAVAIL FSUSE% MOUNTPOINT
loop0  ext4   1.0                   e7d44e2f-405b-4310-917a-e4d002f90b72      9G     2% /var
loop1  ext4   1.0                   3e55fee8-4421-4280-ae40-84d1ac347384  907.4M     0% /var/tmp
loop2  ext4   1.0                   849d7ac4-3d1a-4e29-b7a2-eb0f60080aaf   13.8G     0% /var/log
loop3  ext4   1.0                   187b967b-8da6-4d81-be0d-f9e45d4af748    1.8G     0% /var/log/audit
loop4  ext4   1.0                   6a56cc48-1912-4992-b2c7-f8bb3bf0e577    2.7G     0% /home
loop5  ext4   1.0                   83ad81ec-8777-49a4-b456-f9191c712c20    2.7G     0% /tmp
loop6  ext4   1.0                   45e985e7-2d78-41fd-aa0e-a09d6117634c  480.9M     0% /opt/sdpon/onuimages
sda
├─sda1 vfat   FAT16 ONIE-EFI        574A-B601
├─sda2 ext4   1.0   ONIE-BOOT       a191f16f-04da-4593-8361-c4d7e8ecb075
├─sda3 ext4   1.0   ONL-BOOT        ff9d9670-2aa9-4cd6-b72f-2bf073afda6d  391.1M    12% /mnt/onl/boot
├─sda4 ext4   1.0   ONL-CONFIG      e17418e0-f60b-4da1-a38b-2f4f791ba41c  109.4M     0% /mnt/onl/config
├─sda5 ext4   1.0   ONL-IMAGES      35bf470b-b335-4248-a6fa-2eb68d5dfaff    8.4G     8% /mnt/onl/images
├─sda6 ext4   1.0   SDPON           d94af3a3-cb55-4823-a0cb-d52890237d0a  123.3G    11% /mnt/onl/sdpon
├─sda7 ext4   1.0   ONL-DATA-ACTIVE caacad09-b259-4021-9882-eb4b8320bc84    8.4G    68% /
└─sda8 ext4   1.0   ONL-DATA-STANDBY 644c9abb-9e50-408e-aff1-ef8daef2e89a   27.2G     8% /mnt/onl/data_standby
sdb
└─sdb1 vfat   FAT32 USB1            D666-CD65
```

4. Execute the following command to create a directory to mount the USB device on the OLT.

```
sudo mkdir /tmp/usb
```

5. Execute the following command to mount the USB device to the directory created in step 4 *(on page 20)*.

```
sudo mount /dev/sdb  /tmp/usb
```

Note: If a different USB name is detected or different partitions are listed, then substitute it under *sdb* as per the output of the *lsblk* command in step 2 *(on page 18)*.

6. Execute the following command to check the contents of the USB device and ensure the *rsys-olt-setup* script is available.

```
ls -l /tmp/usb
```

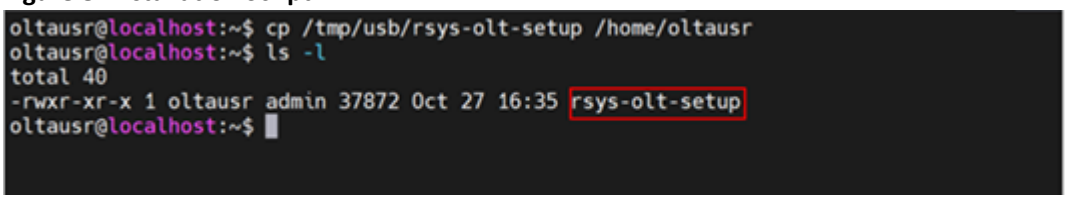
Figure 7. Contents of the USB Device

```
oltausr@localhost:~$ sudo mkdir /tmp/usb
oltausr@localhost:~$ sudo mount /dev/sdb  /tmp/usb
oltausr@localhost:~$ ls -l /tmp/usb
total 4524640
-rwxr-xr-x 1 root root  734549321 Oct 27 14:23 onie-installer
-rwxr-xr-x 1 root root      37872 Oct 27 14:23 rsys-olt-setup
-rwxr-xr-x 1 root root 3898614448 Oct 27 14:25 SDPON.1.14.183.tar.gz
oltausr@localhost:~$
```

7. Execute the following command to copy the script from the USB device to the OLT and ensure the script has executable permission.

```
cp /tmp/usb/rsys-olt-setup /home/oltausr
```

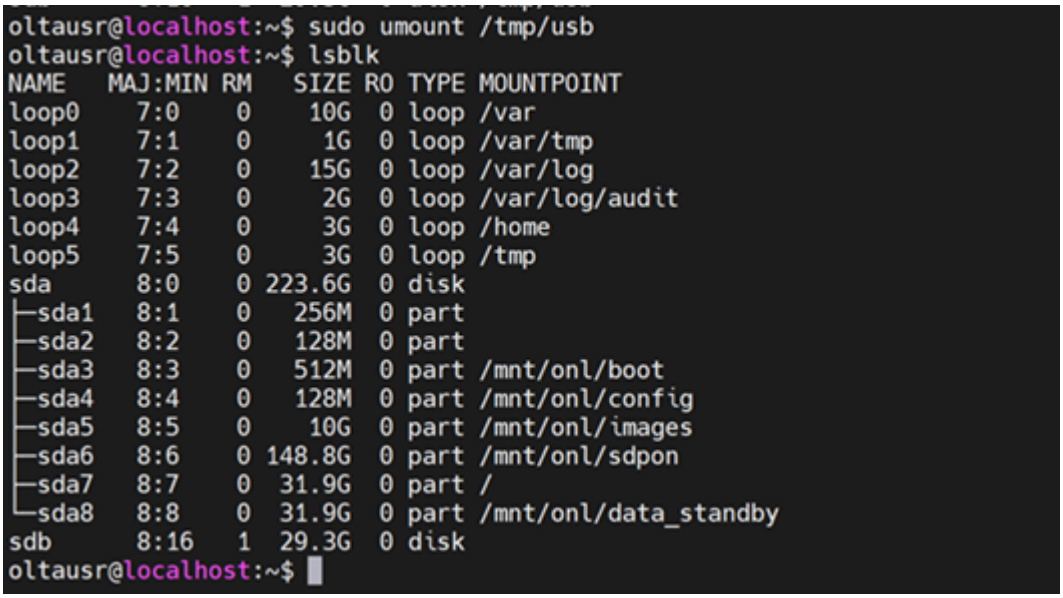
Figure 8. Installation Script



8. Execute the following command to unmount the USB and ensure that the unmount is successful.

```
sudo umount /tmp/usb
```

Figure 9. Unmount the USB



9. Execute the following command to remove the directory created to mount the USB device.

```
sudo rm -rf /tmp/usb
```

Installing CBAC and ONL using USB device

Once the USB contains the required software and is connected to OLT, perform the following steps to install the ONL and CBAC. The script provides two ways of installing the OS (ONL) either using the install or update option.

The criteria for choosing USB-based installation are based on the version of the ONL image in the OLT.

- Execute the following command to check the ONL version.

```
cat /etc/onl/SWI
```

Figure 10. ONL Version

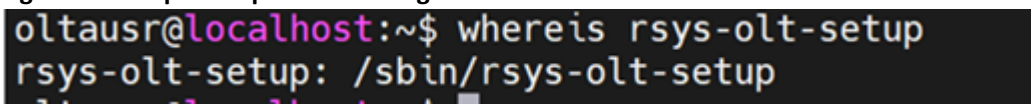
- If the factory shipped ONL version is 2.9 or lower (1.12.xx or lower), then install the 4.1.0 ONL using the ONIE-based installation method.
- If the factory shipped ONL version is higher than 2.9 (1.13.xx or higher), then ONL can be upgraded to 4.1.0 using the update option, as explained in 2.b *(on page 22)*.

1. Check for the installation script *rsys-olt-setup* on the OLT.
   - Execute the following command to check the installation script.

     ```
     whereis rsys-olt-setup
     ```

     The following output shows that the script is already packaged with the existing ONL.

     Figure 11. Output Script with Existing ONL

     If the script is not packaged in the ONL, the command output shows blank.
2. Install or update the ONL on the OLT.
   a. Perform the following steps for the fresh installation of the ONL image. A fresh installation can only be performed if the user wants to remove all the OLT configurations and then freshly bring up the OLT.
      - Execute the following command to install the ONL image.

        ```
        sudo /sbin/rsys-olt-setup -m install
        ```

        Note: The *rsys-olt-setup* script is already packaged in the ONL image if the OLT has an ONL version of 3.2.1 onwards.

      - Execute the following command if the *rsys-olt-setup* script is not packaged in the ONL image in the OLT.

        ```
        sudo /home/oltausr/rsys-olt-setup -m install
        ```

        Note: It is assumed that the user copied the script from the USB device to the */home/oltausr* path, if not, provide the path appropriately.

   b. Perform the following steps to update the ONL image. If the user requires the previous ONL configurations (IP address, user credentials and so on) even after the upgrade, the user can select the update option.
      - Execute the following command to update the ONL image.

        ```
        sudo /sbin/rsys-olt-setup -m update
        ```

Note: The *rsys-olt-setup* script is already packaged in the ONL image if the OLT has a base ONL version of 3.2.1 onwards.

- Execute the following command if the *rsys-olt-setup* script is not packaged in the ONL image in the OLT.

```
sudo /home/oltausr/rsys-olt-setup -m update
```

Note: It is assumed that the user copied the script from the USB device to the */home/altar* path; if not, provide the path appropriately.

When the ONL image in the OLT matches the image on the USB device, the user is prompted to continue. The installation proceeds or aborts based on the input. Once the installation is started, the OLT reboots automatically.

3. Set the time zone value on the OLT.
   - Execute the following commands to configure the time zone on the OLT to IST after the OLT is booted up with the required ONL version.

```
sudo timedatectl set-timezone Asia/Kolkata
sudo timedatectl set-time 2022-08-23
sudo timedatectl set-time 19:07:53
```

   - Replace the date and time with actual values at the time of installation.
4. CBAC deployment on the OLT.
   - Execute the following command to trigger the CBAC deployment.

```
sudo /sbin/rsys-olt-setup -m cbac
```

Note: The *rsys-olt-setup* script is already packaged in the ONL image if the OLT has an ONL version of 3.2.1 onwards.

   - Execute the following command if the *rsys-olt-setup* script is not packaged in the ONL image in the OLT.

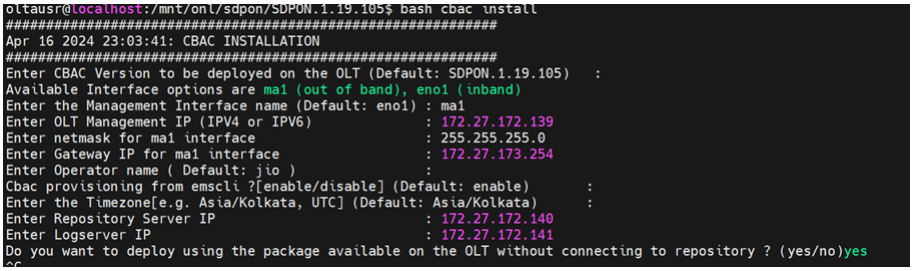
```
sudo /home/oltausr/rsys-olt-setup -m cbac
```

Note: It is assumed that the user copied the script to */home/oltausr*, if not, provide the path appropriately.

   - The user is prompted to enter more information. From release version 4.0.0 onward, the CBAC deployment can also be enabled on the out-of-band interface. The user can choose either in-band or out-of-band to manage CBAC. Depending on the interface selected, the user is prompted to enter the additional information.

The following screenshot shows a sample configuration for enabling CBAC management on an out-of-band interface.

Figure 12. Sample Configuration

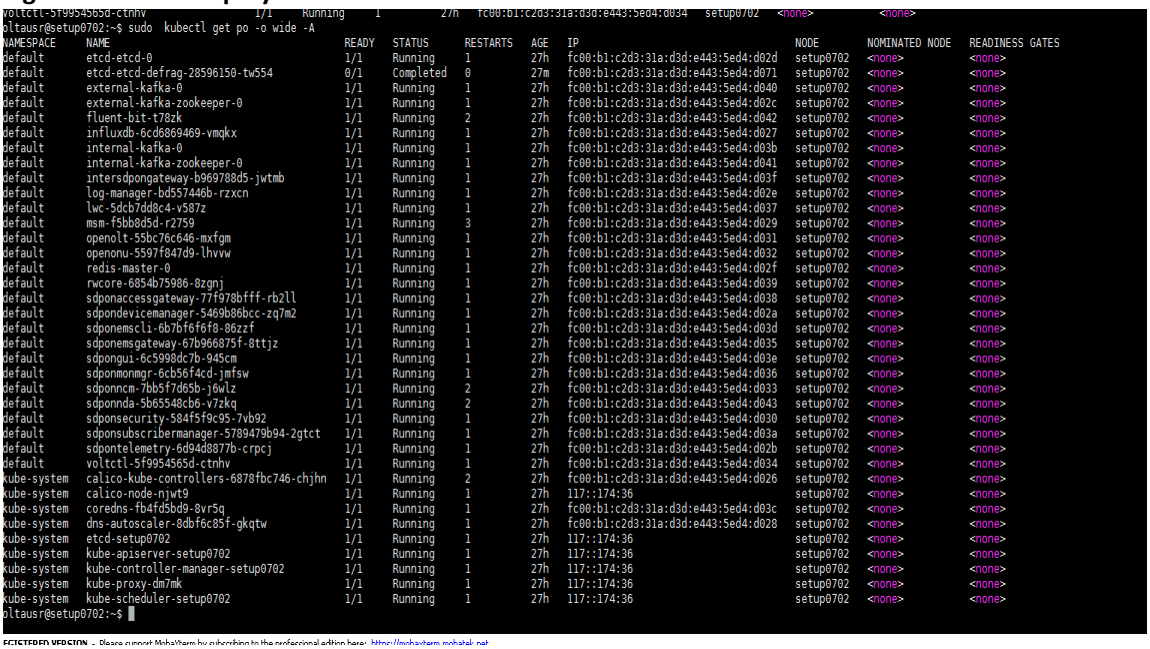


Note: When the in-band IP address is selected, the script prompts for additional information such as NNI and VLAN.

5. Execute the following command to verify the CBAC deployment after successful CBAC deployment.

```
sudo kubectl get pods -o wide -A
```

Figure 13. CBAC Deployment Verification



For any advanced configuration of the OLT, see Configuring Radisys OLT *(on page 44)*.

Installing ONL using ONIE Mode

This section covers the new provisioning of CBAC that installs and provisions the OLT without configuration and installation done at the factory. Power on the nodes and perform the following steps after enabling network connectivity. The ONIE method can also be used when a USB device is not

available for installation. The default IP address on the out-of-band interface is removed in the ONIE mode.

ONIE Grub Menu

After selecting the main ONIE from the Grub menu, the ONIE grub menu appears as follows.

```
GNU GRUB  version 2.02
 /-----------------------------------------------------------------------------\
 | ONIE: Install OS                                                            |
 | ONIE: Rescue                                                                |
 |*ONIE: Uninstall OS                                                          |
 | ONIE: Update ONIE                                                           |
 | ONIE: Embed ONIE                                                            |
 |                                                                             |
 |                                                                             |
 |                                                                             |
 |                                                                             |
 |                                                                             |
 |                                                                             |
 |                                                                             |
 |                                                                             |
 \-----------------------------------------------------------------------------/
      Use the ^ and v keys to select which entry is highlighted.
      Press enter to boot the selected OS, `e' to edit the commands
      before booting or `c' for a command-line.
```

Prerequisites for Installing ONL Using ONIE

The following requirements must be fulfilled before installing ONL using ONIE.

- If the firmware versions of OLT show as mentioned in the table below, the CPLD watchdog must be disabled before proceeding with the ONL installation.

Table 3. BIOS/CPLD Versions

Platform	BIOS	CPLD
RLT 1600G, RLT-1600X, and RLT-3200G	1.0.11	0x66
RLT-1600C and RLT-3200C	1.0.08	0x12

- The Grub password lock restricts editing the Grub menu and accessing the ONIE menu. Contact the Radisys Support team for details about username and password.

Note: Once the ONL installation is complete, enable the CPLD watchdog. See Enabling CPLD Watchdog *(on page 27)*.

Uninstalling ONL

The existing network operating system image is uninstalled by selecting ONIE from the main Grub menu and **ONIE:Uninstall OS** mode from the ONIE Grub menu.

Installing ONIE Through Console

Perform the following steps to install the ONIE through the console.

1. Reboot the OLT.
2. The Grub menu is displayed after the OLT reboot.

   Note: Editing the grub menu or accessing the ONIE menu is protected by a grub password lock. Contact the Radisys Support team for the username and password.

3. Select the **ONIE** mode and enter the grub username and password of the OLT.
4. Select the **ONIE > Rescue** mode from the ONIE Grub Menu *(on page 25)*.
5. Add the management IP address required to download the ONIE image from the repository server.
6. Add the **Eth4** configuration and netmask details.

   ```
   ONIE:/ # ifconfig eth4 <ip address> netmask <mask>
   ```

7. Add the route.

   ```
   ONIE:/ # route add default gw <gateway ip> 172.27.174.254
   ```

8. Execute the following commands to check the connectivity by pinging the gateway IP from the terminal.

   ```
   ONIE:/ # ip addr show eth4
   ONIE:/ # ip route
   ```

9. Execute the following command to copy the ONIE image file from the shared release package.

   Example:

   ```
   ONIE:/ # scp sdpon@172.27.172.75:/home1/sdpon/SDPON/build_packages/Release/olt/
   onie-updater-x86_64-phoenix-r0 .
   ```

   or

   ```
   ONIE:/ # scp sdpon@172.27.172.75:/home1/sdpon/SDPON/build_packages/Release/olt/
   onie-updater-x86_64-europa-r0 .
   ```

10. Execute the following command to modify the `machine.conf` file.

    ```
    ONIE:/ # vi /etc/machine.conf
    ```

    Note:

    - For RLT-1600C or RLT-3200C, replace **europa** with **radisys_europa**
    - For RLT-3200G, RLT-1600G, or RLT-1600X, replace **phoenix** with **radisys_phoenix**

11. Execute the following command to install ONIE.

```
ONIE:/ # onie-self-update onie-updater-x86_64-phoenix-
```

or

```
ONIE:/ # onie-self-update onie-updater-x86_64-europa-r0
```

Disabling CPLD Watchdog

Perform the following steps to disable the CPLD watchdog.

1. Log in to the ONL to disable the CPLD watchdog.
2. Execute the following command to disable the CPLD watchdog.

```
sudo /sbin/rsys-cpld-watchdog disable
```

Note: The CPLD watchdog is enabled by default. If it is disabled for ONL installation, enable it again. See Enabling CPLD Watchdog *(on page 27)*.

Related information

Deploying OLT and CBAC *(on page 14)*

Enabling CPLD Watchdog

Perform the following steps to enable the CPLD watchdog.

1. Log in to the ONL to enable the CPLD watchdog.
2. Execute the following command to enable CPLD watchdog.

```
sudo /sbin/rsys-cpld-watchdog enable
```

Related information

Deploying OLT and CBAC *(on page 14)*

Installing ONL Image

The subsequent methods are used to install the ONL image on an OLT from ONIE. All the methods require the OLT to have serial connectivity.

The following are the ONL installation methods from ONIE.

Note: The user can follow any one of the following methods to install ONL from ONIE based on the availability of the resources, such as the TFTP server and SCP server.

- Installing ONL on OLT Using TFTP *(on page 28)*
- Installing ONL on OLT Using SCP *(on page 29)*

Installing ONL on OLT Using TFTP

You can install the ONL on the OLT by copying the image to the Trivial File Transfer Protocol (TFTP) server.

Perform the following steps to install the ONL on OLT using TFTP.

1. Set up the DHCP and TFTP server.
2. Execute the following command in the TFTP server to place the ONIE installer file from the source folder.

   Example:

   ```
   $ sudo cp <Radisys-ONL path>  /tftpboot/onie-installer
   ```

3. Connect the network cable to the management port of the OLT.
4. Power ON the OLT, and if required, uninstall the ONL. See Uninstalling ONL *(on page 25)*.

   Note:

   Any existing ONL image is uninstalled, the uninstallation process may take some time. After the completion of uninstallation, the OLT reboots, and the user is shown the ONIE Grub Menu *(on page 25)*. For more information on the ONL uninstallation, see ONL Uninstallation *(on page 25)*.

   Or

   If the OS is not uninstalled, the user is shown the main grub menu. Select **ONIE** from the GRUB menu and enter the grub username and password of the OLT.

5. Select **ONIE > Install OS** from the ONIE Grub Menu *(on page 25)*.
6. When the device locates the ONL installer file, the ONL installation starts automatically.
7. After the installation, the OLT reboots automatically, and the main grub menu is displayed. Log into the OLT using the following default account credentials.

   ```
   Username: oltausr
   Password: OLTuser@12
   ```

   You need to modify the password at first login.

8. Assign an IP address for the management interface.

Installing ONL on OLT Using SCP

Perform the following steps to install the ONL on OLT using Secure Copy Protocol (SCP).

1. Set up the repository server.
2. Power ON the OLT, and if required, uninstall the ONL. See ONL Uninstallation *(on page 25)*.

   Note:

   Any existing ONL image is uninstalled, the uninstallation process may take some time. After the completion of uninstallation, the OLT reboots, and the user is shown the ONIE Grub Menu *(on page 25)*. For more information on the ONL uninstallation, see ONL Uninstallation *(on page 25)*.

   Or

   If the OS is not uninstalled, the user is shown the main grub menu. Select **ONIE** from the GRUB menu and enter the grub username and password of the OLT.

3. Select **ONIE > Rescue** from the ONIE Grub Menu *(on page 25)*.
4. Add the management IP address required to download the ONL image from the repository server.
5. Add the Eth4 configuration and netmask details.

```
ONIE:/ # ifconfig eth4 <ip address> netmask <mask>
```

6. Add the route.

```
ONIE:/ # route add default gw <gateway ip>
```

7. Execute the following commands to check the connectivity by pinging the gateway IP from the terminal.

```
ONIE:/ # ip addr show eth4
ONIE:/ # ip route
```

8. Verify the following details before downloading the ONL image from the repository server.
   a. Verify the latest repository server with access information such as username.

      Example:

      ```
      vmauser@172.27.182.25
      ```

   b. Verify the ONL image path for the new build.

      Example:

      ```
      /var/www/html
      ```

Note: The path may change for every release.

c. Verify the latest image details.

Example:

```
ONL-SDPON_ONL-OS10_2022-10-14.1244-47eb736_AMD64_DSDPON_RSYS_1.14.180_INSTALLED_I
NSTALLER
```

9. Download the ONL image from the repository server.
10. Execute the following command and provide the repository server password.

Example:

```
ONIE:/ # scp -r vmauser@172.27.182.25:/opt/CBAC-R2.10.0-
r1.14.166/ROLT.1.14.180/ONL-SDPON_ONL-OS10_2022-10-14.1244-
47eb736_AMD64_DSDPON_RSYS_1.14.180_INSTALLED_INSTALLER .
```

11. Execute the following command in the ONIE mode to retrieve the details of all the files, including the ONL image.

```
ONIE:/ # ls
```

Command Output:

```
ONL-SDPON_ONL-OS10_2022-10-14.1244-
47eb736_AMD64_DSDPON_RSYS_1.14.180_INSTALLED_INSTALLER
bin
boot
dev
etc
init
lib
mnt
proc
root
run
sbin
sys
tmp
usr
var
ONIE:/ #
```

12. Execute the following command to install the ONL image.

```
onie-nos-install <image name>
```

Note: The image details copied in step 10 *(on page 30)* are used to install the ONL image.

Example:

```
ONIE:/ # onie-nos-install ONL-SDPON_ONL-OS10_2022-10-14.1244-
47eb736_AMD64_DSDPON_RSYS_1.14.180_INSTALLED_INSTALLER
```

13. After installation, the OLT reboots automatically, and the Grub menu is displayed.
14. Login to the OLT using the following default login credentials.

```
Username: oltausr
Password: OLTuser@12
```

You must change the password when you first log in.

15. After the successful installation of ONL, verify if the build, image, and repository server versions are correct.

Note:

- If you want to upgrade the ONL, install the ONL again.
- If the OLT contains a different version of firmware (BIOS, CPLD, or FPGA), the firmware is upgraded automatically after an ONL upgrade when the OLT is rebooted, and another reboot is triggered for the firmware changes to be effective.

Related information

Deploying OLT and CBAC *(on page 14)*

Verifying ONL Installation

Perform the following steps to verify that the ONL operating system is properly installed on your device.

- Execute the following command to verify the ONL kernel version.

```
oltausr@localhost:~$ uname -a
```

Command Output:

```
Linux localhost 5.10.201-OpenNetworkLinux #1 SMP Fri Jan 5 10:07:23 UTC 2024 x86_64
 GNU/Linux
```

- Execute the following command to verify the ONL version and distribution-specific information.

```
oltausr@localhost:~$ cat /etc/os-release
```

Command Output:

```
PRETTY_NAME="Debian GNU/Linux 11 (bullseye)"
NAME="Debian GNU/Linux"
VERSION_ID="11"
```

```
VERSION="11 (bullseye)"
VERSION_CODENAME=bullseye
ID=debian
HOME_URL="https://www.debian.org/"
SUPPORT_URL="https://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
```

After the ONL installation, the user follows the CBAC-D installation and activation procedure mentioned in the following sections.

Note:

- By default, the ONL uses localhost as its hostname. To modify the hostname, execute the following command.

  ```
  sudo update_hostname <hostname>
  ```

- Hostnames can contain up to 64 characters, including uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and hyphen (-).
- The first character cannot be a hyphen.
- The **update_hostname** command throws an error if the hostname does not meet the above criteria.

Installing CBAC Software

This chapter provides information about deploying the CBAC software solution on the OLT.

There are two ways to deploy CBAC on the OLT.

1. Offline CBAC Deployment with Package Placed Inside OLT *(on page 32)*
2. Online CBAC Deployment by Connecting to the Repository Server *(on page 36)*

Related information

Deploying OLT and CBAC *(on page 14)*

Offline CBAC Deployment with Package Placed Inside OLT

The following procedure is an interactive script that takes inputs from the user and supports the CBAC deployment without connecting to the repository server. This automated deployment does not require any manual update of network or ansible inventory files.

Prerequisites

1. Install ONL and bring up the OLT.
2. Assign the out-of-band IP address, add the default gateway, and execute the following commands to enable SSH to the OLT.

a. Execute the following command to assign the out-of-band IP.

```
sudo ifconfig ma1 <OLT_IP>
```

b. Execute the following optional command to add the default gateway.

```
sudo route add default gw <Gateway_IP> via ma1
```

3. Perform SSH to the OLT using the temporary IP address assigned from the previous step.

Note: If the ONL is installed in the field using the ONIE mode, the default IP address is removed permanently.

4. Copy the release package to the */mnt/onl/sdpon* folder using scp.
5. Execute the following commands to untar the package and copy the installation script *SDPON.X.XX.XXX/cbac* to the */mnt/onl/sdpon* directory.

```
cd /mnt/onl/sdpon
sudo tar -xvf SDPON.X.X.X.tar
sudo cp SDPON.X.X.X/cbac /mnt/onl/sdpon/
```

6. To install CBAC, ensure that the above untarred SDPON package is present at the */mnt/onl/sdpon* directory.
7. Set the time zone value on the OLT.
   - Execute the following commands to configure the time zone on the OLT.

```
sudo timedatectl set-timezone Asia/Kolkata
sudo timedatectl set-time 2022-08-23
sudo timedatectl set-time 19:07:53
```

Note: Replace the date and time with actual values at the time of installation.

Offline Installation of CBAC

Note:

- If any incorrect inputs are provided, press Ctrl+C and start the process from the beginning.
- OLT reboots post installation if VLAN or NNI is different.

Perform the following procedure to install CBAC offline.

1. Execute the following command to change the directory to */mnt/onl/sdpon*.

```
$ cd /mnt/onl/sdpon
```

2. Execute the following command to install CBAC.

```
$ bash cbac install
```

Note:

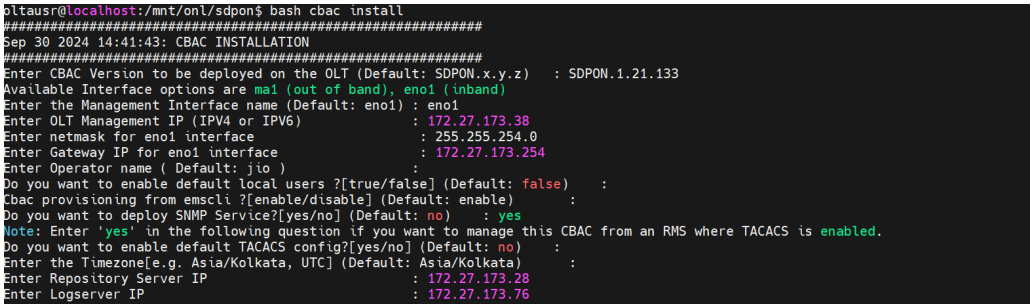
- CBAC script allows additional features where the user can manually perform network configuration and trigger CBAC install with --skip-network-setup option, for example, “bash cbac install --skip-network-setup”.
- Default values are hardcoded for fields such as operator, timezone, SDPON package, enabling SNMP service, and so on.
- By default, the SNMP service is disabled, and the SNMP service is deployed based on the user (**Yes/No**) input during installation. If the option is selected as **Yes**, a new service called "snmp-agent" starts and provides an SNMP interface to monitor faults and KPIs of **CBAC** using the SNMP protocol. For more information, refer to the *CBAC SNMP MIB* section in the *CBAC SNMP User Guide*.
- If the OLT is not connected to RMS and has configurations that must be enabled through the CBAC CLI, set the *enable_default_local_users* parameter to **True**. After that, the *cliadmin, clioperator, cliviewer* users are enabled in the CBAC CLI and the operators can log in to the CBAC CLI using the following login credentials.

Username	Password
cliadmin	CLIadmin@123
clioperator	CLIoperator@123
cliviewer	CLIviewer@123

- You can either press enter to obtain the default values or enter your preferred valid values.
- Select either in-band or out-of-band interface for managing the CBAC.
- For the operator, the default value is **JIO**. Press **Enter** to take the default value or any other value entered internally makes the operator value as **admin**.
- The default value of the CBAC package differs in different releases.
- If an in-band IP address is selected, ensure to enter VLAN and NNI values as permitted by the OLT model, otherwise, OLT restarts continuously.
- Do you want to deploy using the package available on the OLT without connecting to the repository? (**yes/no**)

- By entering **yes**, you can deploy CBAC without connecting to the repository and using the CBAC package stored at */mnt/onl/sdpon* path.

Figure 14. CBAC Offline Deployment Connecting to Repository server



Note: After the successful deployment, you can verify the deployment. See Verifying CBAC Deployment Setup *(on page 39)*.

Running Diagnostic Test

This section covers the steps to run the diagnostic script after commissioning.

1. Execute the following command in your home directory to copy the *diagnostic.sh* script from the CBAC package placed in your OLT at */mnt/onl/sdpon* location.

   ```
   sudo cp /mnt/onl/sdpon/SDPON.x.x.x/setup_repo/diagnostic.sh .
   ```

   Example:

   ```
   sudo cp /mnt/onl/sdpon/SDPON.1.14.183/setup_repo/diagnostic.sh .
   ```

2. Execute the following command to run the diagnostic script. Ensure that all the tests are passed.

   ```
   $ sudo /home/oltausr/diagnostic.sh
   ```

   If you want to remove the CBAC software for any reason, see Partial and Complete Clean Up of CBAC *(on page 35)*.

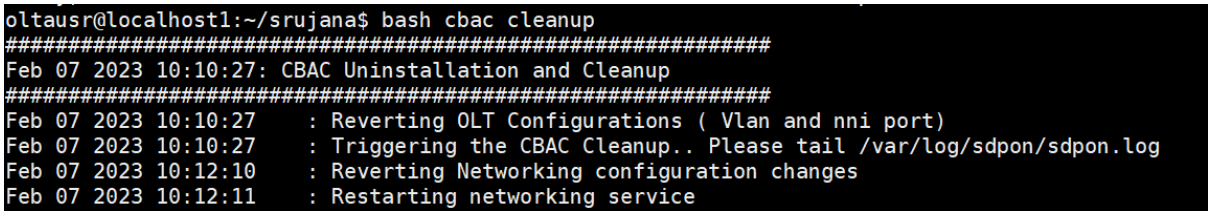
Partial and Complete Clean Up of CBAC

Perform the following steps to clean up the CBAC services completely.

Execute the following command to uninstall all the components of CBAC.

```
$ bash cbac cleanup
```

Figure 15. CBAC Cleanup



Execute the following commands to clean up the complete CBAC deployment without reverting the networking configurations followed by deployment. This procedure is needed if you want to bring up CBAC again without changing the existing network.

```
cd /mnt/onl/sdpon
sudo ansible-playbook cleanup_services.yml
sudo ansible-playbook deploy_services.yml
```

Note: Perform the following steps only if partial cleanup is required, such as removal and deployment of microservices only.

Execute the following commands to cleanup the CBAC services and redeployment.

```
cd /mnt/onl/sdpon
sudo ansible-playbook cleanup_services.yml
sudo ansible-playbook deploy_services.yml
```

Related information

Deploying OLT and CBAC *(on page 14)*

Online CBAC Deployment by Connecting to Repository Server

If the OLT and other CBAC components such as repository server are connected to the production network, the following method can be used to install the CBAC.

Prerequisites

The following requirements must be fulfilled before you trigger the CBAC deployment.

- The repository server is set up successfully with the relevant release package. For more information, see Repository Server *(on page 54)*.
- The OLT is reachable over the network. Ensure that the in-band or out-of-band management network and the OLT time zone are set as per the requirement. See Configuring Radisys OLT *(on page 44)* section for other optional configurations such as banner update and advanced configurations.
- If you want to use out-of-band interface for CBAC management, ensure you overwrite the default IP address with desired network details in the `/etc/network/interfaces` file.

```
#interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

auto ma1
iface ma1 inet static
address 192.168.1.1
netmask 255.255.255.0

auto eno1
iface eno1 inet dhcp

~
```

- Set the new IP address, netmask, and Gateway for out-of-band interface and restart the network service. Ensure that the OLT is reachable over the network with the new IP address on the out-of-band interface.

```
oltausr@localhost:~$ ifconfig ma1
ma1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.27.172.139  netmask 255.255.254.0  broadcast 0.0.0.0
        inet6 fe80::2ab9:d9ff:fee3:6ac6  prefixlen 64  scopeid 0x20<link>
        ether 28:b9:d9:e3:6a:c6  txqueuelen 1000  (Ethernet)
        RX packets 4207192  bytes 312821734 (298.3 MiB)
        RX errors 0  dropped 267  overruns 0  frame 0
        TX packets 37660  bytes 3129260 (2.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- **Note:** The network settings need not be modified if the in-band option is selected

- The Rsyslog server must be up and running. For more information, see Centralized Log Server *(on page 67)*.
- The NTP server must be up and reachable from the OLT. For more information, see Configuring NTP Client and Server Parameters *(on page 238)*.
- Ensure that the OLT time is synchronized with NTP.

  Set the timezone on the CBAC system or the OLT before the CBAC deployment to receive the CBAC service or deployment logs in the required timezone.

  Note: You cannot modify the timezone after the CBAC deployment. Influxdb and logstash logs are in Universal Time Coordinated (UTC), even after changing to another timezone. For example, IST.

Activating Deployment Environment

This section covers the procedure to activate the deployment environment.

Perform the following steps for CBAC deployment.

1. Copy the CBAC script from the package to the OLT `/mnt/onl/sdpon` path.
2. Execute the following command to change the directory to the `/mnt/onl/sdpon` path.

```
$ cd /mnt/onl/sdpon
```

3. Execute the following command to install CBAC.

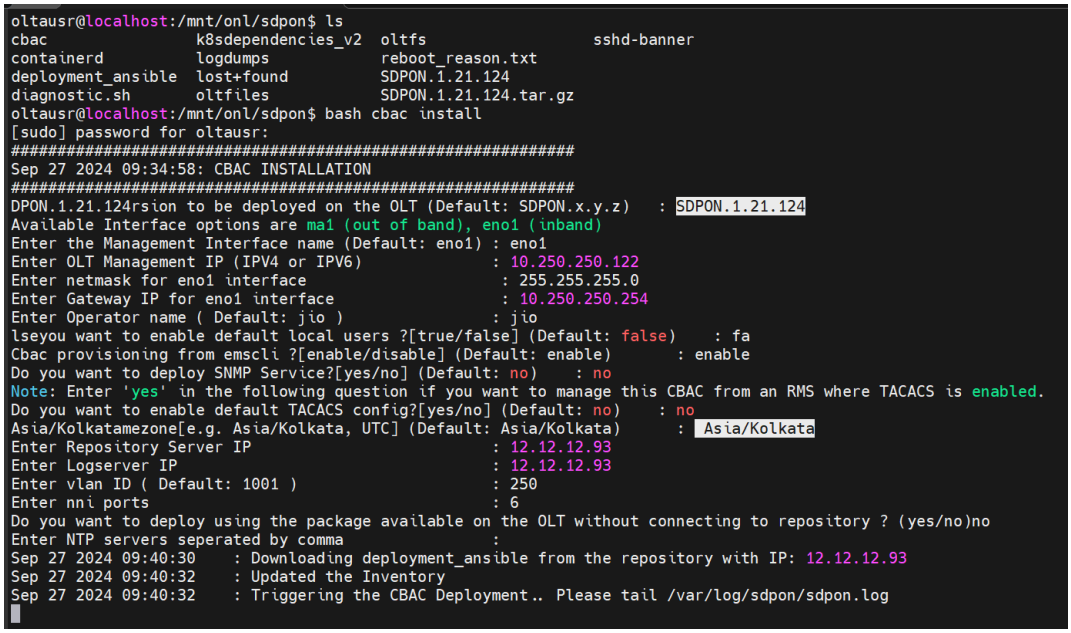
```
$ bash cbac install
```

Note: CBAC script allows additional feature where the user can manually perform network configuration and trigger CBAC install with --skip-network-setup option, for example, “bash cbac install --skip-network-setup”

- Default values are hardcoded for fields like operator, timezone, CBAC package, SNMP service, and so on.
- As a default, the SNMP service is not enabled, and SNMP deploys depending on the user's (Yes/No) choice.
- You can either press enter to obtain the default values or enter your preferred valid values.
- Select either in-band or out-of-band interface for managing the OLT.
- For the operator the default value is **JIO**. Press **Enter** to take the default value or any other value entered internally makes the operator value as **admin**.
- The default value of the SDPON package differs in different releases.
- If in-band IP address is selected, ensure to enter VLAN and NNI values as permitted by the OLT model, otherwise, OLT restarts continuously.
- Do you want to deploy using the package available on the OLT without connecting to the repository? (**yes/no**)

- By entering **no**, you can deploy CBAC by connecting to the repository.

Figure 16. CBAC Offline Deployment Without Connecting Repository



Verifying CBAC Deployment Setup

All the deployment logs are available at `/var/log/sdpon` folder. For CBAC deployment details, see the `/var/log/sdpon/sdpon.log` file.

Execute the following command to verify if the CBAC setup is successfully deployed.

Note: When the **kubectl get pods** command is executed, all the PODs must be running other than the *etcd-etcd-defrag-xxxxxxxx-xxxx* POD, which is already in a completed state.

```
$ sudo kubectl get pods
```

Command Output:

```
NAME                                  READY   STATUS      RESTARTS   AGE
etcd-etcd-0                           1/1     Running     0          4d15h
etcd-etcd-defrag-1642476660-jvtjm     0/1     Completed   0          4m38s
external-kafka-0                      1/1     Running     1          4d15h
external-kafka-zookeeper-0            1/1     Running     0          4d15h
influxdb-7f5b484848-lxbzz             1/1     Running     0          4d15h
internal-kafka-0                      1/1     Running     0          4d15h
internal-kafka-zookeeper-0            1/1     Running     0          4d15h
intersdpongateway-5f95d7fc6b-cv98s    1/1     Running     0          4d15h
log-manager-555dd4bc98-js54q          1/1     Running     0          4d15h
logstash-55685989d6-2g69w             1/1     Running     0          4d15h
lwc-74dd7765d4-cx8l8                  1/1     Running     0          4d15h
msm-56cf685b9d-pvrkk                  1/1     Running     0          4d15h
openolt-5dc7db9bfc-vswn2              1/1     Running     0          4d15h
openonu-fb94d6775-pklg9               1/1     Running     0          4d15h
```

```
redis-master-0                              1/1     Running     0          4d15h
rwcore-f6bf4767-dpc2t                       1/1     Running     0          4d15h
sdponaccessgateway-7c75c77498-dklx8         1/1     Running     0          4d15h
sdpondevicemanager-7b65d54557-9ctbl         1/1     Running     0          4d15h
sdponemscli-789fdfc958-8bslr                1/1     Running     0          4d15h
sdponemsgateway-59f979cb-qx66b              1/1     Running     0          4d15h
sdponmonmgr-7cfc7d6d44-r7rnm                1/1     Running     0          4d15h
sdponncm-764df7749c-xh84z                   1/1     Running     0          4d15h
sdponnda-7c6d59cff5-trmmp                   1/1     Running     0          4d15h
sdponsecurity-76c4cd6f56-zbvx9              1/1     Running     0          4d15h
sdponsubscribermanager-7c5df9f8d9-bhg8w     1/1     Running     0          4d15h
sdpontelemetry-64df666dfd-b7vlg             1/1     Running     0          4d15h
voltctl-889bf955b-qz9f9                     1/1     Running     0          4d15h
```

Note: During the CBAC deployment, if the SNMP service value is set to **Yes**, an extra POD of SNMP agent is seen as part of the output as shown in the below screenshot.

Figure 17. SNMP Service Output

```
oltausr@localhost:~$ sudo kubectl get pods
[sudo] password for oltausr:
NAME                                        READY   STATUS      RESTARTS   AGE
etcd-etcd-0                                 1/1     Running     0          94m
etcd-etcd-defrag-28679761-dv462             0/1     Completed   0          3m24s
external-kafka-0                            1/1     Running     0          93m
external-kafka-zookeeper-0                  1/1     Running     0          93m
fluent-bit-qmssx                            1/1     Running     0          92m
influxdb-758778b88d-gtdl4                   1/1     Running     0          94m
internal-kafka-0                            1/1     Running     0          94m
internal-kafka-zookeeper-0                  1/1     Running     0          94m
intersdpongateway-7dc6995c68-87gdh          1/1     Running     0          92m
log-manager-7c7d5df556-zbh6m                1/1     Running     0          91m
lwc-5788545c84-xqb74                        1/1     Running     0          91m
msm-7664546cdc-56l69                        1/1     Running     0          92m
openolt-bd8b4c8c9-bgjn4                     1/1     Running     0          91m
openonu-6fb9d95784-2nzjc                    1/1     Running     0          91m
redis-master-0                              1/1     Running     0          91m
rwcore-85b764f5b5-gnlpc                     1/1     Running     0          91m
sdponaccessgateway-5d4594b44b-4lgv6         1/1     Running     0          92m
sdpondevicemanager-766d488979-2zp4f         1/1     Running     0          92m
sdponemscli-7bd96b554c-whpcv                1/1     Running     0          92m
sdponemsgateway-5ff964d789-hl6z7            1/1     Running     0          92m
sdpongui-7878dd49f9-wttqn                   1/1     Running     0          92m
sdponmonmgr-b49d6fd95-w8dl7                 1/1     Running     0          91m
sdponncm-79d4cbb777-pnw9n                   1/1     Running     0          92m
sdponnda-f9f97ffc-vp5tq                     1/1     Running     0          92m
sdponsecurity-6bc845f7c6-rkv2j              1/1     Running     0          91m
sdponsnmpagent-6f864f6c48-2c997             1/1     Running     0          89m
sdponsubscribermanager-7df78bcf5f-4r2bp     1/1     Running     0          92m
sdpontelemetry-7d8f9dbd47-5bnpn             0/1     Running     0          91m
voltctl-778f5c6d77-ggg49                    1/1     Running     0          91m
oltausr@localhost:~$
```

Running Diagnostic Test

This section covers the steps to run the diagnostic script after commissioning.

1. Execute the following command to copy the diagnostic script *diagnostic.sh* from the repository server onto the OLT.

```
$ scp
 <repo_user_name>@<repo_ip>:/
var/www/html/sdpon/SDPON.x.x.x/diagnostic/diagnostic.sh .
```

   Example.

```
$ scp
 demo@172.27.172.77:/var/www/html/sdpon/SDPON.1.3.100/diagnostic/diagnostic.sh .
```

2. Execute the following command to run the diagnostic script. Ensure that all the tests are passed.

```
$ sudo /home/oltausr/diagnostic.sh
```

   If you want to uninstall the CBAC software completely, see Cleaning Up CBAC Deployment Environment *(on page 41)*.

Cleaning Up CBAC Deployment Environment

Perform the following steps to clean up the deployment environment.

1. Execute the following command to change the directory to *deployment_ansible* in the Ansible controller.

```
$ cd /mnt/onl/sdpon/deployment_ansible
```

2. Execute the following command to clean up the CBAC deployment logs. By default, logs are appended to the */var/log/sdpon/sdpon.log* file.

```
$ bash cbac cleanup
```

   Note: Kubernetes uninstallation logs are stored at `/var/log/sdpon/Kubernetes_cleanup.log`.

```
PLAY RECAP
 ********************************************************************************
**************************************************************

No task should be failed for successful cleanup.
```

   Note: Reboot the OLT after the cleanup operation.

   If you want to partially uninstall the CBAC software such as removal of micro services, see Cleaning Up Services and Data *(on page 42)*.

Cleaning Up Services and Data

Execute the *cleanup_services.yml* ansible playbook to clean up the services and provisioning data without deleting the Kubernetes cluster and docker images.

Note: During the cleanup process, services are impacted temporarily.

Perform the following to clean up services and data.

1. Execute the following command to change the directory to *deployment_ansible* in the Ansible controller node.

```
$ cd /mnt/onl/sdpon/deployment_ansible
```

2. Execute the following command to maintain separate logs for deployment and cleanup.

```
$ export ANSIBLE_LOG_PATH=/var/log/sdpon/cleanup.log
$ sudo ansible-playbook cleanup_services.yml
```

3. By default, logs get appended to `/var/log/sdpon/sdpon.log` by executing the following command.

```
$ sudo ansible-playbook cleanup_services.yml
```

Note: Reboot the OLT after the cleanup operation.

After the partial removal of CBAC software, if you want to bring-up the microservices again, see Redeploying All Services *(on page 42)*.

Redeploying All Services

After performing the service and data cleanup operation, you can choose to redeploy the services by executing the *deploy_services.yml* playbook.

Perform the following steps to redeploy the services.

1. Execute the following command to change the directory to *deployment_ansible* in the ansible controller node.

```
$ cd /mnt/onl/sdpon/deployment_ansible
```

2. Execute the following command to maintain separate logs for deployment and cleanup.

```
$ export ANSIBLE_LOG_PATH=/var/log/sdpon/deployment.log
$ ansible-playbook deploy_services.yml
```

3. Execute the following command. The logs are appended to the `/var/log/sdpon/sdpon.log` file by default.

```
$ sudo ansible-playbook deploy_services.yml
```

Note:

If the CBAC deployment was brought up without enabling SNMP service, then execute the following command to bring up SNMP service after the CBAC deployment.

```
sudo ansible-playbook deployment.yml --tags snmp -e "enable_snmp=yes"
```

Related information

Deploying OLT and CBAC *(on page 14)*

Configuring Radisys OLT

This section covers In-band management configuration, updating the OLT time zone, OLT security banner, and NNI port speed.

Configuring In-band Management

The following requirements must be fulfilled for the Radisys OLT configuration.

- For in-band management, ensure that the `olt_config` file is present in the */broadcom* folder with the following values.

```
{
"_comments" : "This is a comment. For making changes in this file, user is advised
 to go through CBACd_Installation_Guide of Release documentation.Please execute
 validate_olt_config to validate if JSON is valid",
"vlan" : 100,
"nni" : [1,3,4,5],
"pon_device_mode0" : "gpon",
"iwf_mode0" : "per_flow",
"pon_device_mode1" : "gpon",
"iwf_mode1" : "per_flow",
"inband_storm_control_rate" : 100000,
"version" : "v.0.0.01",
"alarmthreshold_max_events" : 10,
"alarmthreshold_window_time" : 5
}
```

Note:

- The NNI port represents the list of ports that can be used for in-band connectivity.
- The default NNI ports are NNI-1 and NNI-3.
- Update the in-band port list as per the topology requirement and perform an OLT reboot to take effect.

Figure 18. Current In-band Port List

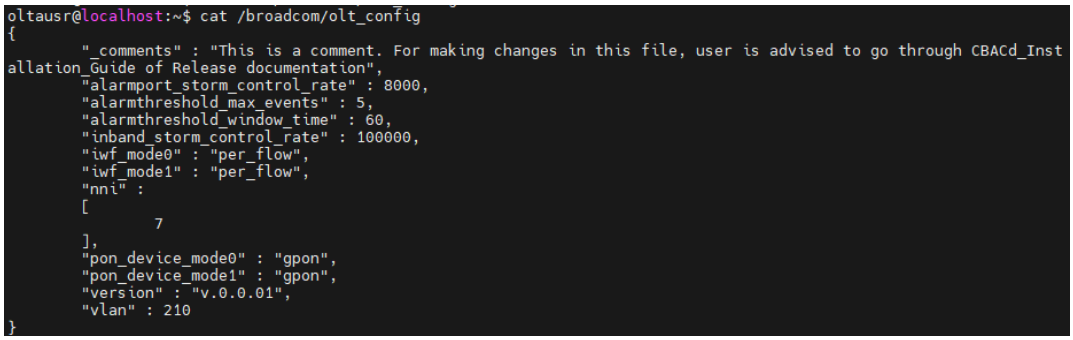
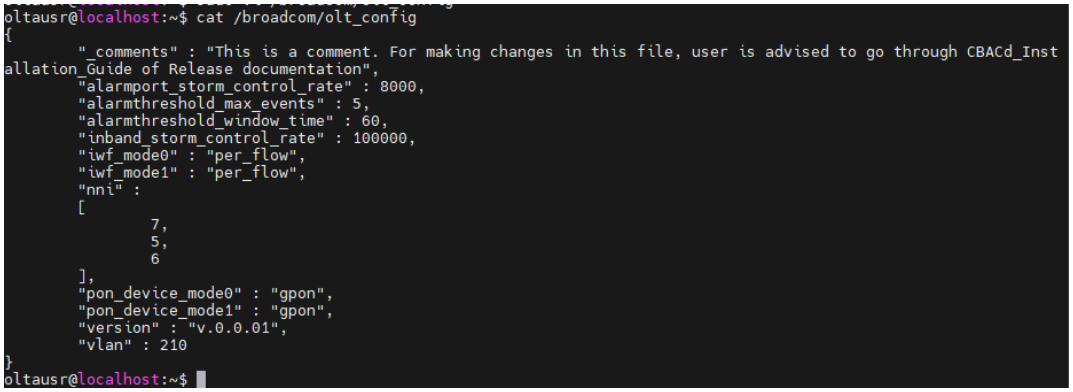


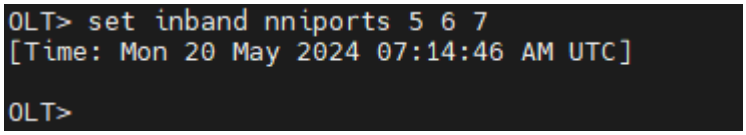
Figure 19. Target In-band Port List



- Execute the following command to modify the NNI in-band port list at runtime.

```
set inband nniports 5 6 7  //make sure that mentioned NNI port is up and not
 part of LAG
```

Figure 20. In-band Port Update



- In-band Management VLAN can be configured from RMS or SDPON CLI with the port information provided by the user.
- The *pon_device_mode* field is set to **gpon** by default. However, the user can configure the field value to **gpon**, **xgspon**, or **cpon** if the device supports it.
- The *vlan* field is set to 100. However, the user can change it to any preferred valid vlan-id.
- If any of the above fields are changed, the user needs to reboot the OLT to make these changes effective.
- To set up the DHCPv6 server and enable IPv6 on the eno1 interface, see Setting Up DHCPv6 Server *(on page 238)*.
- To configure the NTP client and server, see Configuring NTP Client and Server Parameters *(on page 238)*.
- By default, the OLT internally configures storm control objects for in-band VLAN with 1,00,000 kbps.
  - Execute the following command to modify the *inband_storm_control_rate* in the *oltconfig* utility to change the traffic rate.

    ```
    set inband storm_control_rate $storm_control_rate_value
    ```

  - If the user configures a storm with in-band VLAN, it is treated with higher priority. The range of *inband_storm_control_rate* is between 1 to 5,00,000 kbps (500 Mbps).
- By default, the OLT internally configures Alarm port and management interface storm control objects 100 kbps.

- Execute the following command to modify the *alarmport_storm_control_rate* in the *oltconfig* utility to change the traffic rate.

```
set alarmport storm_control_rate $storm_control_rate_value
```

- The range of alarmport *storm_control_rate* is between 12 kbps to 1,20,000 kbps (120 Mbps).

Updating OLT Time Zone

By default, the OLT has an Etc/UTC time zone.

Perform the following steps to update the OLT time zone.

1. Execute the following command to display the supported time zone.

```
sudo timedatectl list-timezones
```

2. Execute the following command to update the time zone to a different time zone.

```
sudo timedatectl set-timezone <new timezone>
```

Example:

```
sudo timedatectl set-timezone Asia/Kolkata
```

Note: Do not change the time zone using any other method, as it may result in unwanted behaviour.

Updating OLT Security Banner

By default, the OLT has a Radisys security banner.

Perform the following steps to update the OLT security banner.

1. Log in to the repository server.
2. Create the *config-files* directory in `/var/www/html/`, if the *config-files* directory is not present.
3. Execute the following command to move into the `/var/www/html/config-files` directory.

```
$ cd /var/www/html/config_files
```

4. If the *sshd-banner* file exists, open the file, remove all the content, update operator-specific content, and save the file.
5. If the *sshd-banner* file does not exist, create the *sshd-banner* file, add operator-specific banner content, and save the file.

The following is an example of the *sshd-banner* file content.

Example:

```
$ cat sshd-banner
```

```
################################################################################################
####
                            ## DO NOT LOGON WITHOUT AUTHORIZATION ##
You are attempting to log in to a system owned and operated by Radisys
 If you are not authorized to access this system, please cancel your login attempt
immediately
                        All activities on this system may be monitored
                    All data residing on this system is a property of Radisys
       Any unauthorized use, duplication, or disclosure of this device or its
 contents
     and/or the attempt to gain unauthorized access is strictly prohibited and
 unlawful
                                 and may lead to legal prosecution
################################################################################################
####
```

6. Log in to the OLT as an olt user.
7. Enter the following command to update the OLT security banner.

```
sudo update_banner http://<REPO_IP>/config-files/sshd-banner
```

Note: The OLT banner must be updated before the CBAC deployment to update the CBAC CLI banner. If the user wants to update the banner on the fly after the CBAC deployment, refer to the Creating Task for Banner Update section in the *RMS User Guide*.

Updating NNI Port Speed

By default, all the NNI ports are configured to run in 10G speed mode except the NNI1 and NNI2 ports, which always run in 40G mode for Europa and Phoenix setups.

Following are the steps to configure 100G/25G/1G port.

1. Run *oltconfig* utility in the OLT.
2. Execute the following command to set the NNI port speed.

```
set nni_speed <nni_port_id> <nni_speed>
```

The following configuration shows how 100G/25G/1G speed is configured using the *oltconfig* utility and 100G/25G/1G configuration is supported only for Europa OLTs.

```
{
"_comments": "This is a comment. For making changes in this file, user is
advised to go through CBACd_Installation_Guide of Release documentation",
```

```
    "vlan": 231,
    "nni": [4,5,6],
    "pon_device_mode0": "gpon",
    "iwf_mode0": "per_flow",
    "pon_device_mode1": "gpon",
    "iwf_mode1": "per_flow",
    "inband_storm_control_rate": 100000,
    "version": "v.0.0.01",
    "alarmthreshold_max_events": 10,
    "alarmthreshold_window_time": 5,
    "nni_port_speed_25g" : [3, 4, 5, 6],
    "nni_port_speed_100g" : [1, 2],
    "nni_port_speed_1g" : [7, 8]
}
```

Note:

- By default, NNI-1 and NNI-2 are configured in 40G mode and other NNI ports in 10G mode.
- The *nni_port_speed_100g* tag lists NNI ports configured for 100G mode. The speed of NNI-1 and NNI-2 ports on 1600G and 3200G platform cannot be changed and therefore ignored if added under the "nni_port_speed_100g" tag. This tag is absent in the default `olt_config` file.
- Configuring the 1G/25G speed is not supported on the NNI-1 and NNI-2 ports.
- The *nni_port_speed_25g* tag lists NNI ports configured for 25G mode in 1600C/3200C. The speed of NNI ports on 1600G and 3200G platform cannot be changed to 25G and therefore ignored, if added under the *nni_port_speed_25g* tag. This tag is absent in the default `olt_config` file.

  Note: In 25G mode, only NNI-3 to NNI-6 ports of 1600C/3200C OLT can be configured.

- Execute the following command to revert the NNI port to default port speeds from *oltconfig* with default port speed.

  ```
  set nni_speed <nni_port_id> 10
  ```

- If any one of the four NNI ports (3, 4, 5, 6) is configured to 25G, then all four NNI ports (3, 4, 5, 6) must be configured to 25G.

  A warning message appears when the *oltconfig* file is executed as follows.

  ```
  oltausr@localhost:~$ sudo oltconfig
  [sudo] password for oltausr:
  Shared memory already exist
  ****************************
  * Openolt Debug CLI *
  ****************************
  OLT> set nni_speed 3 25
  [Caution:]Setting port speed on NNI-3 to 25G will result in setting NNI-3,
   NNI-
  ```

```
4, NNI-5, NNI-6 into 25G
Port speed changes for the above port(s) will be effective after manual OLT
reboot.
Please confirm Yes or No ? [y/n]:y
[Time: Tue 23 Apr 2024 10:03:46 AM UTC]
Sucessfully set the NNI speed 25G
OLT>
```

- After the configuration change, reboot the OLT to bring the port speed changes into effect.

Configuring FEC on NNI Port

This section covers the procedure to configure the Forward Error Correction (FEC) on the NNI port.

Forward Error Correction (FEC) is a technique used to improve the reliability of data transmission by detecting and correcting errors in data packets on the NNI port and FEC reduces retransmits.

The supported FEC types are.

- CL74
- CL91
- CL108
- Off

Note: By default, the FEC is disabled on all the NNI ports, and you cannot access the `olt_config` file.

Perform the following steps to configure the FEC on the NNI port.

1. Run the *olt_config* utility on the OLT.
2. Execute the following command to configure FEC on the NNI port.

```
set fec <fec_type> port nni <nni_port_id>
```

3. The `olt_config` file or broadcom directory are updated after configuring FEC on a 100G, 40G, 25G, or 10G NNI port using the *olt_config* utility.

```
{
        "_comments" : "This is a comment. For making changes in this file, user
 is advised to go through CBACd_Installation_Guide of Release documentation.Please
 execute validate_olt_config to validate if JSON is valid",
        "alarmthreshold_max_events" : 10,
        "alarmthreshold_window_time" : 5,
        "inband_storm_control_rate" : 100000,
        "iwf_mode0" : "per_flow",
        "iwf_mode1" : "per_flow",
        "nni" : [1, 3],
        "nni_port_fec_cl74" : [2, 6, 7],
        "nni_port_fec_cl91" : [1],
        "nni_port_speed_100g" : [1],
```

```
        "nni_port_speed_25g" : [3, 4, 5, 6],
        "pon_device_mode0" : "gpon",
        "pon_device_mode1" : "gpon",
        "version" : "v.0.0.01",
        "vlan" : 24
```

Note:

- The following warning message appears when configuring FEC on the NNI port, and you can proceed by entering "yes" or "y".

```
Warning: Changing the NNI FEC configuration may cause the link to go down if
 there is a mismatch with the peer port's FEC settings.
Do you wish to proceed? Please confirm by typing 'Yes' or 'No' [Y/N]:
```

- The following message appears if FEC is configured successfully on the NNI port.

```
Successfully applied FEC <fec_type> on the device for NNI <nni_port_id>
```

- The following message appears if FEC configuration fails on the NNI port.

```
Failed to set FEC <fec_type> on the device for NNI <nni_port_id>
```

- If FEC is configured in the device but not updated in the `olt_config` file due to some issue, then the user must configure FEC on the NNI port again, see 2 *(on page 49)*.

```
Successfully applied FEC on the device, but failed to save in oltconfig file.
Please re-execute this command again
```

- The following message appears when FEC is configured on an invalid NNI port.

```
Please provide valid interface.
```

- If the NNI port speed changes after FEC is configured, the user must reconfigure FEC according to the new port speed.
- The FEC configuration in an OLT continues to persist after rebooting the OLT.

Verifying FEC Values in NNI Ports

Execute the following command to open the `olt_config` file.

```
sudo oltconfig
```

Figure 21. oltconfig

Execute the following command to view the current FEC values configured in the NNI ports.

```
show port nni all
```

Figure 22. NNI Ports

```
OLT> show port nni all
[Time: Tue 11 Jun 2024 01:24:03 PM UTC]
Id   Sfp_id  speed   fec      state          status    SFP status        rx_pkts       tx_pkts       linkFlapCount
0    0       100G    disable  Down           Down      not present       0             0             0
1    1       40G     cl74     Up             Up        FTL410QE2C        0             0             5
2    2       25G     disable  Up             Down      ET5402-SR         0             0             0
3    3       25G     disable  Down           Down      ET5402-SR         0             0             0
4    4       25G     cl74     Up             Up        SFP-25GBASE-SR-I  0             0             5
5    5       25G     disable  Down           Down      SFP-25GBASE-LR-I  0             0             0
6    6       10G     disable  Up             Up        SFP-10GBASE-SR-I  0             0             3
7    7       10G     cl74     Up             Up        SFP-10GBASE-LR-C  0             0             5

total nni ports: 8
```

Subtended OLT

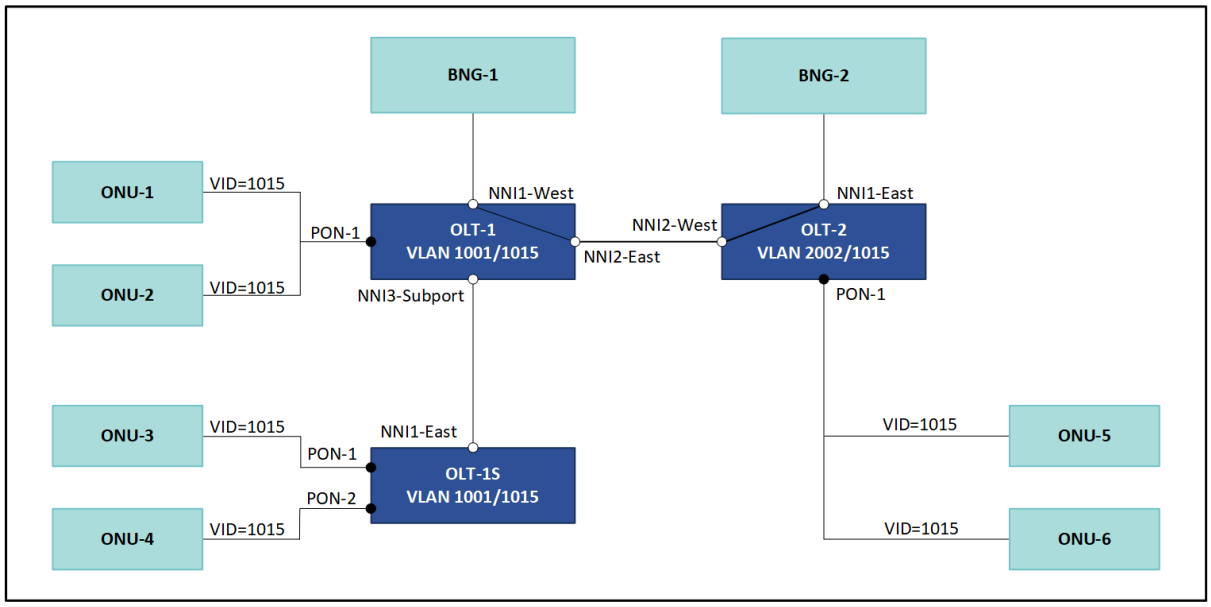
The cascaded OLT is known as a subtended OLT. RMS manages the subtended OLT like any other OLT and performs similar operations to handle it. To handle failure scenarios, LAG can be used as a connection between the cascaded OLTs.

Subtended OLT Topology Use-cases

Residential Use Case

The following figure illustrates the subtended OLT topology for the residential use case.

Figure 23. Subtended OLT–Residential Use Case

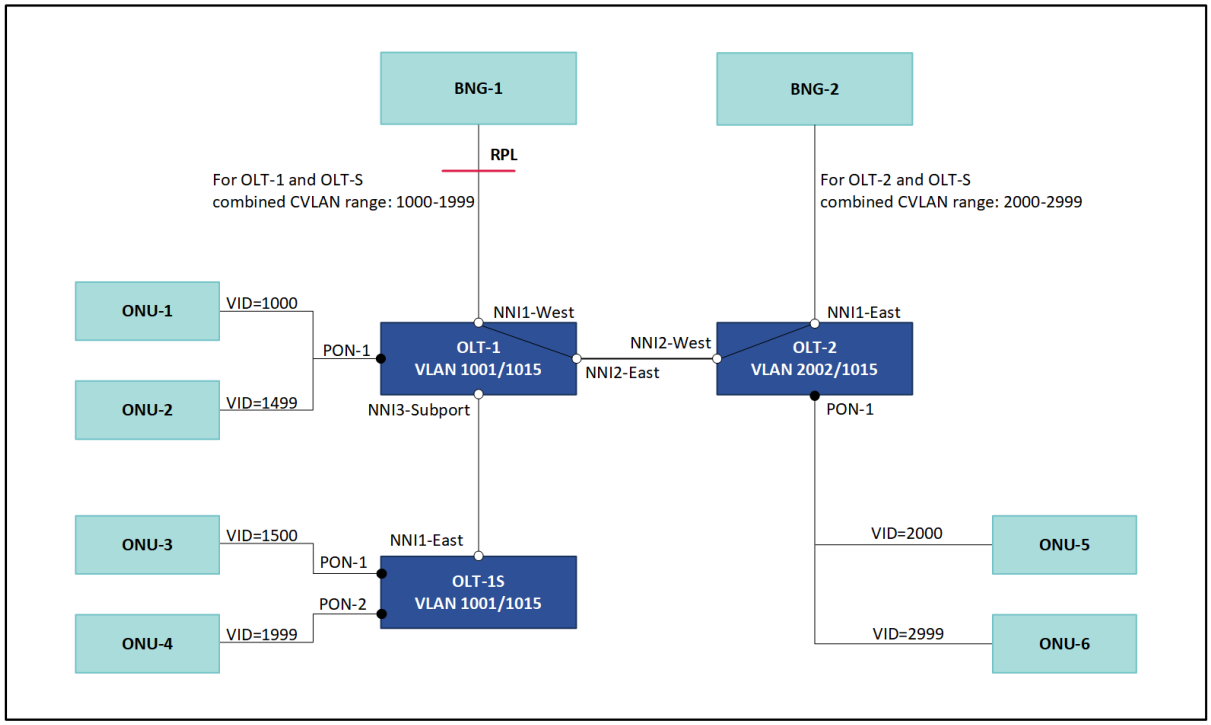


The in-band management channel in the parent OLT (OLT-1) shown in Figure 23: Subtended OLT–Residential Use Case *(on page 51)* must be autoconfigured on boot to enable the subtended OLT (OLT-1S) to reach the BNG.

Enterprise Use Case

The following figure illustrates the subtended OLT topology for the enterprise use case.

Figure 24. Subtended OLT–Enterprise Use Case



Configuring Subtended OLT

Scenario 1: Using Out-Of-band management interface (static/DHCP-based allocation) or static IP allocation for In-band management interface.

- In this scenario, the OLT must know the port that needs to be used to reach BNG. The user or factory configures the static IP and marks one of the NNI ports as ‘port connected’ or 'port reachable' to the router as part of the `olt_config` file.
- The following is an example configuration file where NNI3 is used to connect to BNG. This may be directly connected or connected through another OLT to the BNG. Users can find the following configuration in the `/broadcom$ cat olt_config` file.

```
{
   "vlan":257,
   "nni":[3],
   "pon_device_mode":"gpon",
   "iwf_mode":"per_flow",
   "inband_storm_control_rate":100000,
   "version":"v.0.0.01"
}
```

- On bootup, OLT considers the NNI port marked as the 'east' port, and all other rest NNI ports are marked as 'sub' ports for the management VLAN.
- E-LAN, E-LINE, or RING can be configured on any NNI or LAG ports in any sequence.
- Inband management VLAN can be configured from RMS or SDPON CLI with user provided port information and explicitly mentioned sub ports.

Scenario 2: DHCP used for the in-band management interface.

- By default, one 10G NNI port and 40G NNI port are configured as 'east/west' port for the management VLAN as shown in the following configuration. This enables the operator or the user to plug-in either NNI1 or NNI3 towards the BNG. This can be configured according to operator or user preference.

```
{
   "vlan":100,
   "nni":[1,3],
   "pon_device_mode":"gpon",
   "iwf_mode":"per_flow",
   "inband_storm_control_rate":100000,
   "version":"v.0.0.01"
}
```

- When the DHCP cycle is completed, the NNI port on which the DHCP offer is received is marked as the ‘east’ port. Referring to the above configuration, DHCP is expected on either the NNI1 or NNI3 interface and all other rest NNI ports are marked as sub ports.
- E-LAN, E-LINE, or RING can be configured on any NNI or LAG ports in any sequence.
- Inband management VLAN can be configured from RMS or SDPON CLI with user provided port information and explicitly mentioned sub ports.

Note:

- For the subtended OLT to be reachable from the BNG, ensure that the parent OLT user should provide a sub port list while configuring inband management VLAN from RMS or SDPON CLI. When parent OLT boots up, all the NNI ports act as sub ports except those mentioned in the `olt_config`. So, all the subtended OLTs are reachable to BNG in default cases.
- All the NNI ports, except which are mentioned in the `olt_config` file, are in the admin state as DOWN by default. Users must explicitly activate them.
- For the ERPS ring, both east and west ports must be identical. For example, both east and west ports must be NNI or LAG.
- Before upgrading ONL, if the user is using static in-band or out-of-band for management traffic, then ensure that the `olt_config` file contains only a single interface.
- The port configured as sub-port must be used only towards the subtended OLT.
- Subtended OLT uses the port connected towards the main OLT as its in-band port in the `olt_config` file.

Additional Procedures

This chapter provides information on the following procedures.

- **Repository Server**. Creating repository VM with the CBAC and RMS packages
- **SFTP Server**. Configuring the SFTP server on the repository server
- **Centralized Log Server**. Configuring the remote system log server and simulate the Centralized Log Management Server (CLMS)
- **Installing Keepalived**. Installing keepalived procedure, configuring of master server, configuring of backup server, and configuring of the (VRRP)

Repository Server

The repository server ensures the resiliency of all the data it hosts and restores them after a reboot.

Prerequisites

A hardened VM image from Radisys is used to install the repository server. The hardened image has OVA and QCOW2 formats and supports ESXi and KVM hypervisors. Optionally, the repository server can be installed on a regular Ubuntu 18.04.6 OS.

Note:

- Ensure that the `/var` partition has sufficient disk space.
- The hardened VMs partition contains 50 GB of disk space. For more information about the recommended size of the `/var` partition, refer to the *Disk Requirements* section in the following guides based on the RMS deployment type.
  - *Single Node RMS Installation and Upgrade Guide*
  - *Multinode RMS Installation and Upgrade Guide*
- Extend the partition to the recommended size. For more information about partition, see Extending Filesystem Size *(on page 237)*.

The following requirements must be fulfilled before you set up the repository server.

1. One `server/VM` is required with the specifications mentioned in the Hardware Requirements *(on page 10)* for the repository and log server. For more information about bringing up the VMs, see *Creating Guest VMs Using Virtual Machine Manager (on page 233)*.
2. Ensure that Internet connectivity is present for the package installation.

   Note: The installation fails without an internet connection.

Preparing Local Repository Server

This chapter provides information on how to set up the repository server. The repository server hosts a docker registry that contains all the CBAC docker images.

The following steps are valid for Radisys hardened image and regular Ubuntu 18.04.6. A user can bring up the virtual machine using ESXi or KVM. For more information about VM creation, refer to *Bringing Up Virtual Machine* section in the following guides based on the RMS deployment type.

- *Single Node RMS Installation and Upgrade Guide*
- *Multinode RMS Installation and Upgrade Guide*

Note:

- If the repository server exists for RMS, use the same for CBAC.
- Ensure that the */opt* has sufficient space to accommodate the CBAC release package.
- Ensure you delete the existing and unnecessary packages to accommodate the new package. Optionally, increase the */opt* partition space to the desired size. For more details on increasing partition details, see the Extending Filesystem Size *(on page 237)* section.

Perform the following steps to set up the repository server.

1. Execute the following command to copy the CBAC release version to the home directory of the newly created VM.

```
$ cd ~
$ sudo scp -r <build-server-username>@<build-server-ip>:<package-path> .
```

Example:

```
$ cd ~
$ sudo scp -r
 sdpon@172.27.172.75:/home1/sdpon/SDPON/build_packages/ROLT_Release/CBAC-R2.10.1-1.1
3.19/SDPON.1.13.19.tar.gz .
```

2. Execute the following command to untar the release package.

```
$ cd ~
$ sudo tar -zxvf <SDPON_Release>.tar.gz
```

Example:

```
$ cd ~
$ sudo tar -zxvf SDPON.1.13.19.tar.gz
```

3. Execute the following command to move the extracted folder to the */opt* directory.

```
$ sudo mv <SDPON_Release> /opt
```

Example:

```
$ sudo mv SDPON.1.13.19 /opt
```

4. Execute the following commands to change the directory to the CBAC release version directory.

```
$ cd /opt/<SDPON-Release>
```

5. Execute the following command to change the directory to the *setup_repo* directory.

```
$ cd setup_repo
```

6. Execute the following command to view the usage information of the *setup_local_repo.sh* script.

```
sudo ./setup_local_repo.sh -h
```

Setting Up Local Repository Server

This section describes how to set up the repository server.

Note: Operations such as setting up, updating, shutting down, and restarting the repository server are restricted to limited users such as admin and superuser.

Execute the following command to set up a repository server when a fresh VM is installed.

The command syntax is.

```
$ sudo ./setup_local_repo.sh --repo-ip <REPO_IP> --ntp-server-ip <NTP_SERVER_IP>
 --sdpon-version <SDPON_VERSION> --syslog_repo-ip <SYSLOG_REPO_IP>
```

Example:

```
$ sudo ./setup_local_repo.sh --repo-ip 172.27.173.67 --ntp-server-ip 172.24.100.50
 --sdpon-version SDPON.1.15.50 --syslog_repo-ip 172.27.173.76
```

Command Usage:

```
--repo-ip <REPO_IP>
Repo_IP is the address of the repository IP.
--ntp-server-ip <NTP_SERVER_IP>
NTP_server_IP is the address of the NTP server
--sdpon-version
SDPON release version number
--syslog_repo-ip <SYSLOG_REPO_IP>
SYSLOG_REPO_IP is the address of the Syslog server
--help
```

Note:

- Ensure that you delete the unnecessary packages to accommodate the new release package.
- The repository setup or update does not require system log repository IP as it is an optional parameter. Adding the system log repository IP to the repository setup configures a system log server and sends the repository audit logs to the configured system log server.

  Execute the following command to set up the repository server.

```
sudo ./setup_local_repo.sh --repo-ip 172.27.173.67 --ntp-server-ip
 172.24.100.50 --sdpon-version SDPON.1.15.50
```

Updating Repository Server with CBAC Package

This section describes how to update the repository server with the latest SDPON release package.

Execute the following command to update the existing repository server with the latest SDPON package. The command syntax is.

```
$ sudo ./setup_local_repo.sh  --sdpon-version <SDPON_VERSION> --repo-ip <REPO_IP>
 --syslog_repo-ip <SYSLOG_REPO_IP> --update-repo
```

Example:

```
$ sudo ./setup_local_repo.sh  --sdpon-version SDPON.1.15.50 --repo-ip 172.27.173.67
 --syslog_repo-ip 172.27.173.76 --update-repo
```

Note: The repository setup or update does not require system log repository IP as it is an optional parameter. Adding the system log repository IP to the repository setup configures a system log server and sends the repository audit logs to the configured system log server.

Example:

Execute the following command to set up the repository server.

```
sudo ./setup_local_repo.sh  --sdpon-version SDPON.1.15.50 --repo-ip 172.27.173.67
 --update-repo
```

Repository Server Redundancy

The repository server redundancy ensures high availability and prevents deployment failures. For more information, see Installing Keepalived *(on page 90)*.

The CBAC deployment fails if the master server fails. To avoid this, use the VIP configured on the redundant repository server instead of the original IP addresses of the repository servers. The redundant slave server acts as the repository server.

Viewing Repository Server Setup Logs

The setup logs are stored in the `var/log/sdpon/setup_local_repo.log` file.

1. Execute the following command to monitor the setup logs.

```
$ tail -f /var/log/sdpon/setup_local_repo.log
```

2. Execute the following command to monitor the update of the repository server logs.

```
$ tail -f /var/log/sdpon/update_docker_repo.log
```

Cleaning Up Repository Server

Note: This is not a part of the installation process.

This section describes the procedure to clean up the repository server.

The COB solution provides a cleanup script (*cleanup_repo.sh*) to clean up the repository server. The *cleanup_repo.sh* script is available in the respective release directory */opt/<SDPON_Release>*.

You can clean up a specific repository or all the repositories of the repository server using the *cleanup_repo.sh* script.

1. Execute the following commands to clean up all the repositories.

   Note: The following command removes all the repositories, including the RMS and system log configuration (if any) configured earlier when setting up the repository.

```
$ cd /opt/<SDPON_Release>/setup_repo
$ sudo chmod 777 cleanup_repo.sh
$ sudo ./cleanup_repo.sh --all
```

2. Execute the following commands to clean up a specific repository.

```
$ cd /opt/<SDPON_Release>/setup_repo
$ sudo chmod 777 cleanup_repo.sh
$ sudo ./cleanup_repo.sh --sdpon-version <SDPON_VERSION>
```

   Example:

```
$ sudo ./cleanup_repo.sh --sdpon-version sdpon.1.2.0023
```

Viewing Cleanup Logs

You can view the repository server cleanup logs in the `/var/log/sdpon/cleanup_repo.log` file.

Execute the following command to monitor the cleanup logs.

```
$ tail -f /var/log/sdpon/cleanup_repo.log
```

SFTP Server

This section explains how to configure the SFTP server on the repository server.

The login credentials of RMS and the SFTP server hosted on the repository server must be the same.

- The SFTP server hosted on the repository server is used for the OLT software upgrade.
- The SFTP server hosted on RMS is required for the backup and restore feature.
- The SFTP server hosted on the repository server needs to be configured manually.

Prerequisites

The following prerequisites must be fulfilled before setting up the SFTP server on the repository server.

- Ubuntu 18.04 servers.
- The user must have sudo permission.
- Internet access is needed to install prerequisite packages.

Setting Up SFTP Server

Perform the following steps to configure the SFTP server over SSH protocol.

1. Execute the following command to configure the SSH daemon.

   ```
   sudo apt install ssh
   ```

2. Execute the following command to edit the SSHD configuration directory.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

3. Enter the following at the end of the file.

   ```
   Match group sftp
   ChrootDirectory /home
   X11Forwarding no
   AllowTcpForwarding no
   ForceCommand internal-sftp
   AllowUsers vmauser sftpuser
   ```

   Note: If the SFTP server redundancy is implemented, remove the *ChrootDirectory /home* command from the above configuration.

4. Execute the following command to restart the SSH server and apply the changes.

   ```
   sudo service ssh restart
   ```

5. Execute the following command to create an SFTP user account.

```
radisys@jmapntp1: ~$ sudo addgroup sftp
```

Command Output:

```
Adding group `sftp' (GID 1001) ...
Done.
```

6. Execute the following command to create a new user and assign the user to the created SFTP group.

```
sudo useradd -m sftpuser -g sftp
```

7. The password for any user must meet the following requirements.
   - A minimum length of 8 characters.
   - At least two lowercase characters, two uppercase characters, one digit, and one special character.
   - Passwords for specific users must not include usernames.
   - Must not contain three consecutive alphabets or numbers, such as *"123"* and *"ABC"*.
   - Passwords must not be the same as the last seven passwords that you used.
8. Execute the following command to set a password for the SFTP user.

```
radisys@jmapntp1: ~$ sudo passwd sftpuser
```

Note: Enter the new SFTP password and retype it to confirm.

Command Output:

```
Enter new UNIX password:
Retype new UNIX password:
```

9. Execute the following command to change access permission for the user.

```
sudo chmod 700 /home/sftpuser/
```

10. Execute the following command to log in. Login through the SFTP server.

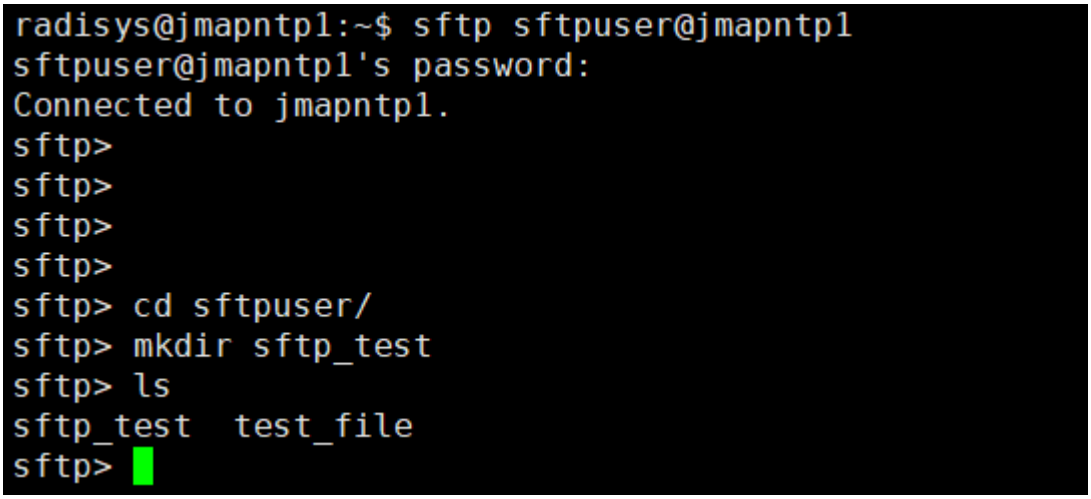
```
sftp sftpuser@jmapntp1
```

Figure 25. SFTP Server

```
radisys@jmapntp1:~$ sftp sftpuser@jmapntp1
The authenticity of host 'jmapntp1 (127.0.1.1)' can't be established.
ECDSA key fingerprint is SHA256:5ketu2gSgq2GIqTtWxP0D0pusAVAyVrgu9U92l+puuk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'jmapntp1' (ECDSA) to the list of known hosts.
sftpuser@jmapntp1's password:
Connected to jmapntp1.
sftp>
sftp>
```

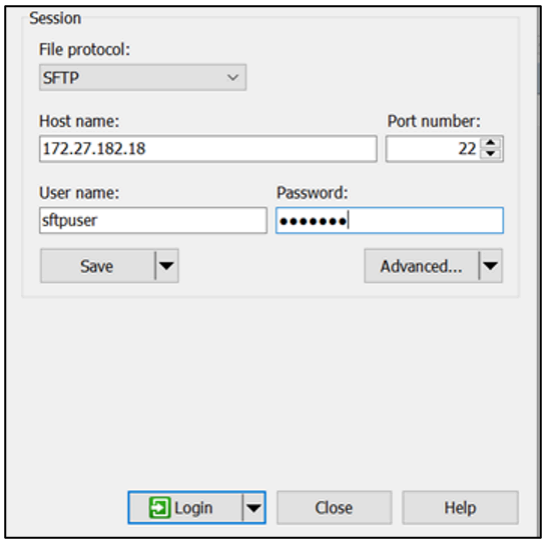
11. Execute the following command to check the "write" access for the user.

Figure 26. Write Access



12. Enter the following information to set up the SFTP connection through winscp or filezila.
    - **File Protocol**. Select SFTP from the drop-down.
    - **Host Name**. Enter the hostname, for example, 172.27.182.18.
    - **Port Number**. Enter the port number, for example, 22.
    - **Username**. Enter the username.
    - **Password**. Enter the password.

Figure 27. SFTP Server Connection



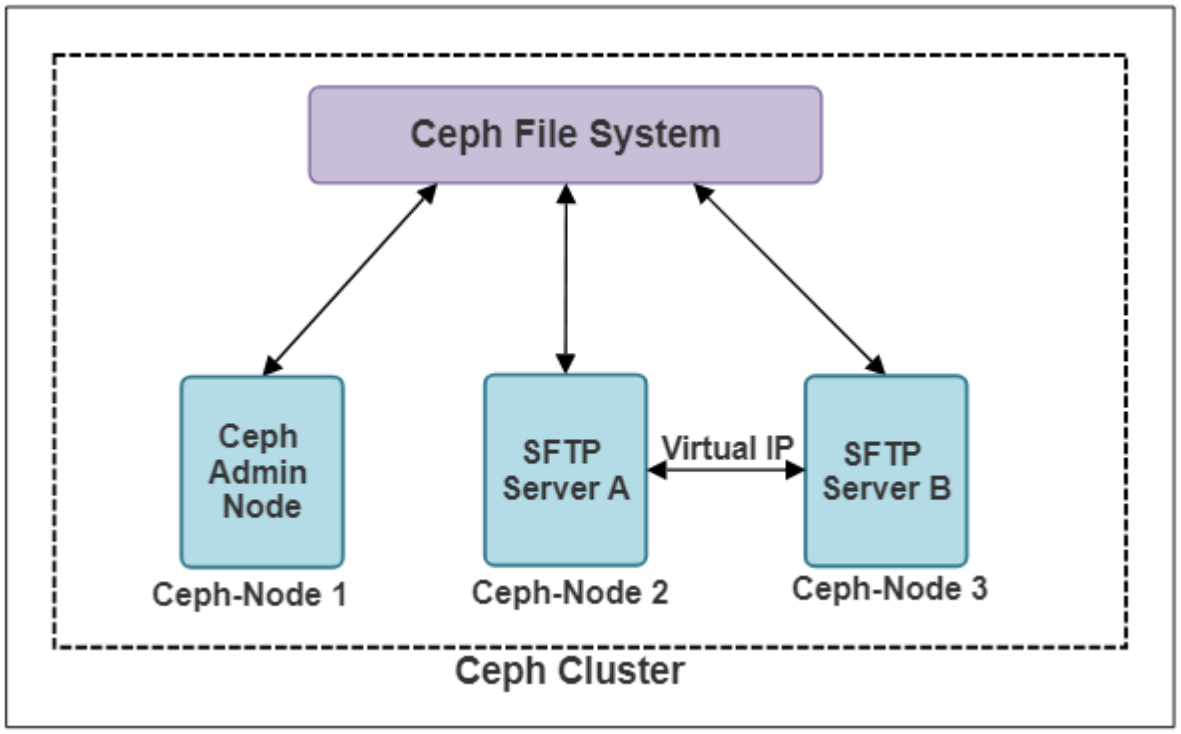
13. Execute the following command to start the SFTP server automatically during the host reboot.

```
sudo systemctl enable ssh
```

SFTP Server Redundancy

This section describes configuring the high-availability SFTP servers using CEPH as centralized storage. Thefollowing figure shows the two SFTP servers connected in a keepalived configuration, with the master holding the Virtual IP. SFTP server A and SFTP server B can read or write from the CEPH file system.

Figure 28. SFTP Server Redundancy



The Ceph is centralized storage, and data is written directly regardless of who writes it (SFTP server A or SFTP server B), so the data is persistent across both SFTP servers.

The code for setting up or cleaning up the SFTP ceph cluster is available in the RMS package under the *sftp-ceph-deployment* file.

The following prerequisites must be fulfilled before setting up the SFTP server redundancy.

- At least three Ubuntu 18.04 hardened OS servers.
- Configure keepalived on both SFTP servers and use the free IP address as a virtual IP address to maintain high availability. The virtual IP addresses of SFTP servers perform different operations. For more information, see the Installing Keepalived for Achieving Redundancy *(on page 90)* section.
- Add VRRP instances if the same SFTP cluster is used for OLT and RMS and if different IP protocols are implemented for each (IPv4/IPv6).
- A Ceph cluster requires three VMs. Two VMs are required to maintain SFTP server redundancy. Additionally, SFTP servers can be reused for ceph cluster setup.
- To create Object Storage Daemon (OSDs), the SFTP servers must be configured with an SFTP user, raw disks, or partitions, and required network interfaces. For more information, see the Setting Up SFTP Server *(on page 59)* section.

- The SFTP servers must be configured with the same SFTP credentials for successful login through the virtual IP address of the SFTP server.

- Ceph can use a raw disk or partition for OSDs. Refer to the *Adding Raw Disk for Ceph to VM in KVM and ESXi* section in the *Multinode RMS Installation and Upgrade Guide*.
- Internet access is required to install the ceph packages.

Note: You can replace the failed or unhealthy node with a new node when an SFTP server fails. For more information, see Replacing SFTP Server *(on page 277)* section.

Setting Up Ceph Cluster

This chapter provides information on how to set up the Ceph cluster.

Prerequisites

The following prerequisites must be fulfilled before setting up the Ceph cluster.

- Three Ubuntu 18.04 hardened VMs with free disk or partition to form a ceph cluster. Refer to the Adding Raw Disk for Ceph to VM section in the following guides based on the RMS deployment type.
  - *Single Node RMS Installation and Upgrade Guide*
  - *Multinode RMS Installation and Upgrade Guide*
- Three Ubuntu 18.04 hardened VMs. Two must be configured with sftp user, keepalived, and required network adapters.
- The SFTP VMs can be re-used as SFTP servers to form the Ceph cluster.

Perform the following steps to set up the Ceph cluster.

RMS software package has a *sftp-ceph-deployment* directory. Copy that directory to the ansible controller from where the ceph deployment is triggered.

1. Execute the following command to go to the RMS package path.

   ```
   $ cd <path/to/RMS_Release_path>/
   ```

2. Execute the following commands on the controller node where the user triggers the ansible-playbook commands.

   ```
   sudo apt-get update
   sudo apt-get install sshpass
   sudo apt-get install python3-pip
   ```

3. Execute the following command to install the required pip packages.

   ```
   $ sudo pip3 install -r sftp-ceph-deployment/requirements.txt
   ```

4. Execute the following command to update the *inventory/hosts* file with the required parameters, hostnames, **ansible_ssh_user**, **ansible_ssh_pass**, **device_name**, and **ansible_ssh_host**.

```
$ sudo vi sftp-ceph-deployment/inventory/hosts
```

The inventory hosts file has two host groups **ceph_cluster**, and **sftp_server**.

- At least three VMs are required to form a **Ceph cluster**.
- Each of the VMs must have a free disk or partition used by ceph to create OSDs.
- SFTP servers can be re-used as ceph VMs by creating a raw disk before performing the ceph installation.
- Provide the **device_name** parameter with the complete device path.

  Example: /dev/sdb

Figure 29. Sample Inventory for SFTP Ceph Deployment

```
# details of all the nodes in the cluster
<host1>    ansible_ssh_pass=<ssh_password>     ansible_ssh_user=<username>    ansible_ssh_host=<IPV4/IPV6>   device_name=<device_name>
<host2>    ansible_ssh_pass=<ssh_password>     ansible_ssh_user=<username>    ansible_ssh_host=<IPV4/IPV6>   device_name=<device_name>
<host3>    ansible_ssh_pass=<ssh_password>     ansible_ssh_user=<username>    ansible_ssh_host=<IPV4/IPV6>   device_name=<device_name>

# Update the below section with the ceph cluster hostnames provided in the section [all]
# 3 hosts are required to form ceph_cluster.
# sftp_server nodes can be re-used for deploying ceph.
[ceph_cluster]
<host1>
<host2>
<host3>

# Update the below section with the sftp hostnames provided in the section [all]
# 2 hosts are required for SFTP Server redundancy
# Can be a subset of ceph_cluster nodes
[sftp_server]
<host2>
<host3>
```

Note:

- Ensure that the correct hostname is used for your system.
- Do not give any blank lines between host group names ([**ceph_cluster**] or [**sftp_server**]) and the next entries (**hostnames**).
- **ansible_ssh_host**. Specifies the IP address of the VM (IPv4 or IPv6).
- **ansible_ssh_user**. Specifies the login username of the VM
- **ansible_ssh_pass**. Specifies the login password
- **device_name**. Specifies the device path of the raw disk or partition to be used for ceph OSDs. The hosts of the ceph cluster group must declare the device name. Example: `/dev/sdb`.

5. Execute the following command to edit the inventory or **group_vars** or all files.

```
$ sudo vi sftp-ceph-deployment/inventory/group_vars/all
```

Note: Enter the SFTP user and group names that are already configured on the SFTP servers.

Figure 30. Sample Group Variables for SFTP Ceph Deployment

```
# SFTP user that is already configured on both SFTP nodes
# Username (and password) should be same on both nodes
sftp_user: <SFTPuser>
sftp_group: <SFTPgroup>

#This option can be used, if we cannot restore the unreachable node, however want to cleanup the available nodes
force_cleanup: false
```

6. Execute the following command to save the ansible logs and create a directory on the ansible controller from where the deployment is triggered.

```
$ sudo mkdir /var/log/sftp_ceph
```

Note: This is required only in case of fresh deployment of ceph for SFTP servers.

7. Execute the following command to enter the **sftp-ceph-deployment** directory.

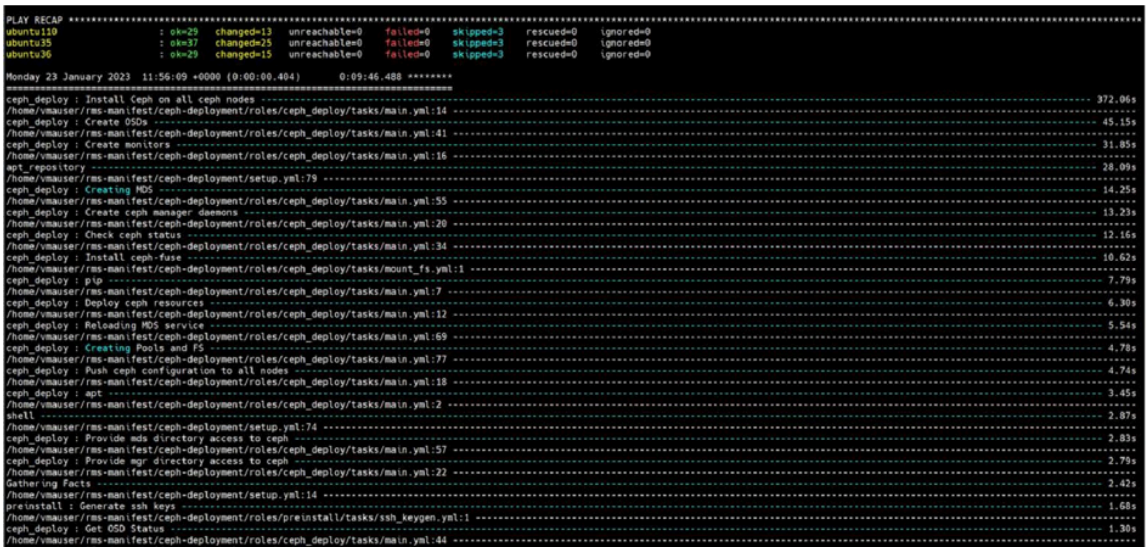
```
$ cd sftp-ceph-deployment
```

8. Execute the following command to setup the Ceph cluster.

```
$ sudo ansible-playbook setup.yml
```

The following screenshot shows the sample output of the SFTP Ceph deployment.

Figure 31. Sample Output of SFTP Ceph Deployment



9. Execute the following command on any of the Ceph cluster VMs to check the Ceph status after the successful deployment.

```
$ sudo ceph status
```

10. The redundant SFTP server must be reachable through a virtual IP address. All backup or restore file transfers must be performed to the default mount point, which is `/mnt/sftpstore`.

    Example: SFTP file path - `sftp://<vip-of-sftp-cluster>/mnt/sftpstore`

Cleaning Up Ceph Cluster

SFTP Ceph cluster cleanup removes data from the */mnt/sftpstore* and cleans up disks allocated as OSDs (**device_name** in inventory). Before proceeding with the cleanup, ensure that you back up any required data.

Note: Cleanup cannot be performed if any Ceph cluster VMs are unreachable.

Perform the following steps for force cleanup of the permanently unreachable Ceph cluster VMs.

1. Remove the unreachable hosts from the **ceph_cluster** group of inventory or hosts file.
2. Enable the **force_cleanup** parameter to clean up the Ceph cluster.
3. When one of the nodes in the cluster is unavailable and cannot be restored, set the **force_cleanup** parameter to *true* to clean up the available nodes for use in another cluster.
4. The console log displays the errors due to the failed node. The **force_cleanup** parameter is used only during cleanup.
5. Ceph deployment uses the first VM in the **ceph_cluster** host group as the base for setting up the cluster. Cleanup cannot be performed if the first host of the **ceph_cluster** used during deployment is unreachable. Perform the following to clean up the Ceph cluster

Perform the following steps to clean up the Ceph cluster.

1. To clean up the Ceph cluster, all servers under the Ceph cluster inventory group must be reachable. If any node is unreachable or permanently down, set the *force_cleanup = true* in the `inventory/group_vars/all` file and remove the unreachable host from the `inventory/hosts` file.

   The playbooks required for the cleanup of the Ceph cluster are available in the RMS package.

   a. Execute the following command to change the path to the RMS release directory.

   ```
   $ cd <path/to/RMS_Release_dir>
   ```

   b. Execute the following command to edit the `inventory/groups_vars/all` file.

   ```
   $ vi sftp-ceph-deployment/inventory/group_vars/all
   ```

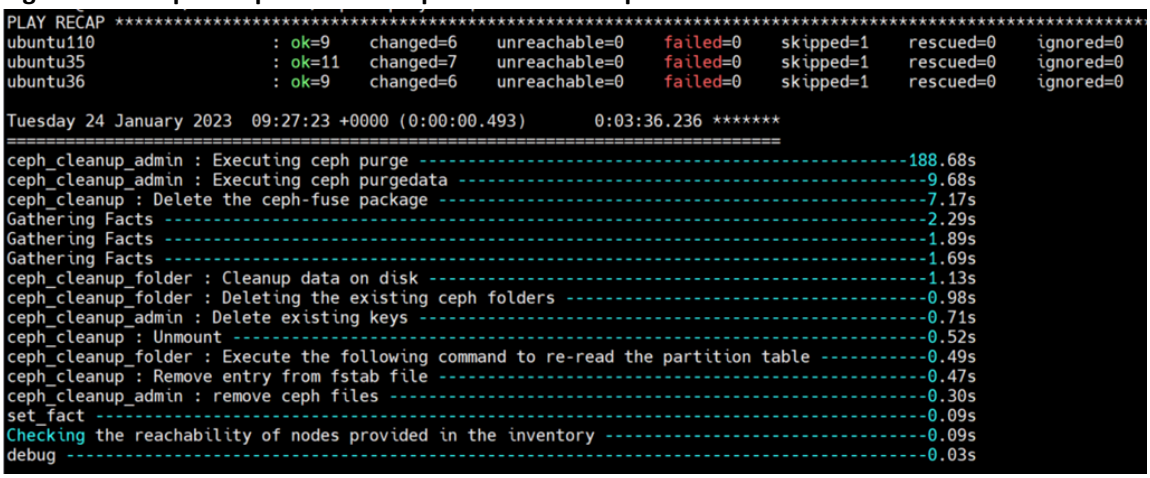
2. Execute the following command to navigate to the `sftp-ceph-deployment` directory.

   ```
   $ cd sftp-ceph-deployment
   ```

3. Execute the following command to set up the ceph cluster.

```
$ sudo ansible-playbook cleanup.yml
```

Figure 32. Sample output of SFTP Ceph Cluster Cleanup



4. Execute the following command to reboot all the VMs under the Ceph cluster section of inventory to complete the cleanup process.

```
$ sudo reboot
```

Centralized Log Server

Consider that the rsyslog server is the central server.

The following sections show how to configure the remote system log server and simulate the Centralized Log Management Server (CLMS).

Setting Up Log Server Using Rsyslog

Perform the following steps to configure the rsyslog server.

1. Execute the following command to back up the rsyslog file configuration.

```
demo@rsyslog-server:~$ sudo cp /etc/rsyslog.conf /etc/rsyslog.conf.orig
```

2. Open the rsyslog file configuration. Find and uncomment the following lines to enable the server to listen on the UDP and TCP ports.

```
demo@rsyslog-server:~$ sudo vi /etc/rsyslog.conf
...
#provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")
[...]
#provides TCP syslog reception
module(load="imtcp")
```

```
input(type="imtcp" port="514")
...
```

3. Add the value for the maximum size of the message.

```
#
# The Max size for a message
#
$MaxMessageSize 512k
```

4. Add the following lines to align the time zone of the logs with the system log server.

```
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$template myTemplate,"%timegenerated% %HOSTNAME% %syslogtag%%msg%\n"
$ActionFileDefaultTemplate myTemplate
```

5. Enter # in the beginning to disable the parameter.

Note: By default, the parameter is enabled.

```
#$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat
```

6. Execute the following command to create a template file under the `/etc/rsyslog.d/` directory. The file is used to define the new custom log format.

```
[demo@rsyslog-server ~]# sudo vi /etc/rsyslog.d/tmpl.conf
Add the following lines.
$template logFile, "/var/log/client_logs/CBAC-%fromhost-ip%/%programname%.log"
$template repologFile, "/var/log/client_logs/REPO-%fromhostip%/% programname%.log"
template(name="localCbacTemplateFb" type="list") {
    property(name="timegenerated")
    constant(value=" ")
    property(name="HOSTNAME")
    constant(value=" ")
    property(name="syslogtag")
    property(name="msg" spifno1stsp="on")
    property(name="msg" position.from="4")
    constant(value="\n")
}
template (name="cbacTemplateFb" type="list") {
        property(name="timegenerated" dateFormat="rfc3339")
        constant(value=" CBAC-[")
        property(name="fromhost-ip")
        constant(value="] ")
        property(name="programname")
        constant(value=":")
        property(name="msg" spifno1stsp="on")
        property(name="msg" position.from="4")
        constant(value="\n")
}
template (name="cbacTemplate" type="list") { property(name="timegenerated"
 dateFormat="rfc3339") constant(value=" CBAC-[")
```

```
property(name="fromhost-ip") constant(value="] ") property(name="programname")
 constant(value=":") property(name="msg" spifno1stsp="on" ) property(name="msg")
 constant(value="\n")
}
template (name="oltTemplate" type="list") { property(name="timegenerated"
 dateFormat="rfc3339") constant(value=" OLT-[")
property(name="fromhost-ip") constant(value="] ") property(name="programname")
 constant(value=":") property(name="msg" spifno1stsp="on" ) property(name="msg")
 constant(value="\n")
}
template (name="repoTemplate" type="list") { property(name="timegenerated"
 dateFormat="rfc3339") constant(value=" REPO-[")
property(name="fromhost-ip") constant(value="] ") property(name="programname")
 constant(value=":") property(name="msg" spifno1stsp="on" ) property(name="msg")
 constant(value="\n")
}
if ($fromhost-ip != "127.0.0.1") then {
if ($programname == 'repo_audit' or $programname == 'registry_audit' or
$programname == 'apache_audit' or $programname == 'nginx_audit' or $programname
== 'repo_registery_audit' or $programname == 'repo_notifier_audit') then
 { action(type="omfwd" target="172.27.172.120" port="514" protocol="udp"
 action.resumeRetryCount="-1" queue.type="linkedList" queue.size="10000"
 queue.filename="storage-buffer" queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off" template="repoTemplate")
*.* ?repologFile
} else {
if ( $programname == 'SDPONAuditLogs' or $programname == 'SDPONSecurityAuditLogs' or
 $syslogfacility-text == 'local5') then {
$template logFile, "/var/log/client_logs/CBAC-%fromhostip%/% programname%.log"

if ($msg startswith "\xef\xbb\xbf") then {
                                *.* -?logFile;cbacTemplateFb
                                action(type="omfwd" target="172.27.172.120"
                                port="514" protocol="udp"
 action.resumeRetryCount="-1"
                                queue.type="linkedList" queue.size="10000"
                                queue.filename="storage-buffer"
 queue.maxDiskSpace="1g"
                                queue.saveOnShutdown="on"
 action.execOnlyWhenPreviousIsSuspended="off"
                                template="cbacTemplateFb")
                        } else {
                                *.* -?logFile
                                action(type="omfwd" target="172.27.172.120"
                                port="514" protocol="udp"
 action.resumeRetryCount="-1"
                                queue.type="linkedList" queue.size="10000"
                                queue.filename="storage-buffer"
 queue.maxDiskSpace="1g"
                                queue.saveOnShutdown="on"
 action.execOnlyWhenPreviousIsSuspended="off"
                                template="cbacTemplate")
                        }
}
else {
if ($syslogfacility-text == 'local1' ) then {
$template logFile, "/var/log/client_logs/CBAC-%fromhostip%/% programname%.log"
```

```
action(type="omfwd" target="172.27.172.120" port="514" protocol="udp"
 action.resumeRetryCount="-1" queue.type="linkedList" queue.size="10000"
 queue.filename="storage-buffer" queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"  template="oltTemplate")
*.* -?logFile
}
*.* -?logFile
}
}
}
```

Where 172.27.172.120 is the sample IP address of the CLMS server to which the CBAC, OLT audit logs need to be relayed.

7. Save and close the template file.
8. Execute the following commands to allow the rsyslog default port 514 on your firewall. This opens the port through Uncomplicated Firewall (UFW).

```
[demo@rsyslog-server ~]# sudo ufw allow 514/tcp
[demo@rsyslog-server ~]# sudo ufw allow 514/udp
```

9. Execute the following command to restart the UFW service to apply the changes.

```
[demo@rsyslog-server ~]# sudo ufw reload
```

10. Execute the following command to reload the rsyslog service.

```
[demo@rsyslog-server ~]# sudo systemctl restart rsyslog
```

Note: You can also perform the above steps to configure a simulation of the CLMS. To do this, add the following commands in the `/etc/rsyslog.d/tmpl.conf` file on the CLMS. This redirects the audit logs that are forwarded from the rsyslog servers.

```
$template TmplTest, "/var/log/client_logs/%FROMHOST-IP%/security.log"
if ($fromhost-ip != "127.0.0.1") then {
*.* ?TmplTest
}
```

Validating Rsyslog Server

You can check the functioning of the rsyslog server by setting up one client-server.

A client-server is required with the following configuration.

- Operating System: Ubuntu 16.04 LTS
- RAM: 8 GB
- CPU: 4 cores
- Storage: 500 GB

- IP Address: 172.27.172.xyz
- Hostname: rsyslog-server

Perform the following steps to configure the client server.

1. Execute the following command to backup the rsyslog file configuration.

```
[root@rsyslog-client ~]# cp /etc/rsyslog.conf /etc/rsyslog.conf.orig
```

2. Execute the following command to open the rsyslog file configuration.

```
[root@rsyslog-client ~]# vi /etc/rsyslog.conf
Under the ##RULES## directive section, add the following line.
[...]
##RULES##
*.* @172.27.172.xyz:514
[...]
```

3. Execute the following command to reload the rsyslog service.

```
[root@rsyslog-client ~]# systemctl restart rsyslog
```

4. Execute the following command to log the message to the standard error (screen) and system log.

```
[root@rsyslog-client ~]# logger -s " This is my Rsyslog client "
```

5. Navigate to the rsyslog server under the `/var/log/Client_logs` directory. You must see a new folder named with the hostname of your rsyslog client.

Note: CBAC logs are placed under the `/var/log/Client_logs/SDPON-<IP>/` directory.

Example,

```
labadmin@labadmin:~$ ls /var/log/client_logs/SDPON-<IP>/
```

Retention and Log Rotation

CBAC supports the retention and rotation of the logs collected from different microservices and OLTs.

Retention: Time Series Database

- The default retention period for alarms and KPIs in the time series database is two days.
- Retention can be updated using the ***sdpon-settings update*** command through emscli.

Retention: Message Bus

- You can configure the retention of Kafka messages using Kafka-templates before the CBAC deployment.
- The retention is different for internal and external Kafka.
- **logRetentionHours.** Specifies the minimum age (in hours) of a log file that is eligible for deletion.
- **logRetentionMinutes.** Specifies the minimum age (in minutes) of a log file that is eligible for deletion.
- **logRetentionBytes.** Specifies the size-based retention policy for logs.
- **logSegmentBytes.** Specifies the maximum size of a log segment file. When the maximum size is reached, a new log segment is created.
- **For internal Kafka.**
  - The default retention period of Kafka messages is set to 30 minutes using the **logRetentionMinutes** variable.
  - **logRetentionHours.** The value is set to 0.
  - The default log retention size is set to 75 MB for C-SDPON and 30 MB for D-SDPON using the **logRetentionBytes** variable.
  - The default maximum size of a log segment file is set to 75 MB for C-SDPON and 30 MB for D-SDPON using the **logSegmentBytes** variable.
  - The log segment size must be less than the log retention size because the log removal starts only when the log segment is full.
- **For external Kafka.**
  - The default retention period of Kafka messages is set to 4 hours using the **logRetentionHours** variable.
  - The default log retention size is set to 150 MB using the **logRetentionBytes** variable.
  - The default maximum size of a log segment file is set to 150 MB using the **logSegmentBytes** variable.
  - The log segment size must be less than the log retention size because the log removal starts only when the log segment is full.

Retention: Docker Log

- Before the installation of CBAC, docker log rotation is configured through kubespray. This docker level setting rotates logs for all containers present in all the pods.
- The file for the docker log rotation configuration is present in the repository server at the following location.

```
/var/www/html/deployment-packages/kubespray/roles/kubespraydefaults/
defaults/main.yaml
```

- Update the following argument as follows:

```
docker_log_opts: "--log-opt max-size=50m --log-opt max-file=5"
```

Note: Any changes in the file must be performed before the CBAC deployment.

- The default logfile max size is set to 50 MB.
- The default logfile max file count is set to five.

Rotation of System Logs

The *logrotate* tool helps to configure the system logs that are captured in the system log file.

The following is the recommended configuration for the `/etc/logrotate.d/rsyslog` file.

```
/var/log/rsyslog
{
hourly
minsize 500M
rotate 10
missingok
notifempty
compress
delaycompress
postrotate
invoke-rc.d rsyslog rotate > /dev/null
endscript
}
```

Based on the configuration, the system log file is rotated hourly, when the file size increases beyond 500 MB. After the rotation, logs files are compressed to *.gz* files.

Note: During the rotation process, a maximum of ten log files can be generated and when a new log file is created, the oldest log file is deleted.

To disable remote logs to get written into `/var/log/syslog` file of the logserver, modify `/etc/rsyslog.d/50-default.conf` with following configuration.

```
if ($fromhost-ip == "127.0.0.1") then{
        *.*;auth,authpriv.none          -/var/log/syslog
}
```

Log Rotation at Rsyslog Server

Configuration can be applied at rsyslog for the log rotation. For example, if CBAC logs are pushed at the `/var/log/clientlogs/` directory of rsyslog, the following recommended configuration must be present in any file at the `/etc/logrotate.d/<any_file>` location.

For a `/etc/logrotate.d/sdponlogs` file, the following configuration must be present.

```
var/log/client_logs/CBAC*/[!EkL]*.log{
    weekly
```

```
    maxsize 50M
    maxage 30
    rotate 10
    missingok
    notifempty
    compress
    delaycompress
    postrotate
        invoke-rc.d rsyslog rotate > /dev/null
    endscript
}
/var/log/client_logs/CBAC*/EMSGW-LOG.log
/var/log/client_logs/CBAC*/ETCD0-LOG.log
/var/log/client_logs/CBAC*/kernel.log
/var/log/client_logs/CBAC*/LWC-LOGS.log
{
    weekly
    maxsize 150M
    maxage 30
    rotate 20
    missingok
    notifempty
    compress
    delaycompress
    postrotate
        invoke-rc.d rsyslog rotate > /dev/null
    endscript
}
/var/log/client_logs/CBAC*/EXTERNAL-KAFKA-LOG.log
/var/log/client_logs/CBAC*/EXTERNAL-KAFKA-ZOOKEEPER-LOG.log
/var/log/client_logs/CBAC*/EMSCLI-LOG.log
/var/log/client_logs/CBAC*/kdump-tools.log
/var/log/client_logs/CBAC*/kubelet.log
/var/log/client_logs/CBAC*/LOGMGR_LOG.log
/var/log/client_logs/CBAC*/LOGSTASH-LOG.log
{
    weekly
    maxsize 50M
    maxage 30
    rotate 10
    missingok
    notifempty
    compress
    delaycompress
    postrotate
        invoke-rc.d rsyslog rotate > /dev/null
    endscript
}
```

Since the value for logrotate configuration is set to hourly, ensure that the cron job logrotate configuration is also set to hourly. After updating the `/etc/logrotate.d/sdponlogs` file with the mentioned configuration, execute the following commands to apply the changes.

```
$ sudo service cron restart
$ sudo logrotate /etc/logrotate.conf -f
$ sudo service rsyslog restart
```

Relay Logs to Multiple Destinations from Central Log Server

Rsyslog forward logs to multiple log servers simultaneously. This can be achieved by defining many actions (with different targets) as needed. Queue filenames of each action must be unique and adhere to Linux filename rules.

Sample Configuration

You must set up the syslog server. For more information on setting up the syslog server, see the Centralized Log Server *(on page 67)* section.

Add multiple action directives with different targets (CLMS servers) to the existing template file as required.

Note:

- If one CLMS server is not reachable, the logs are forwarded to the remaining servers without interruption.
- Ensure that the *queue.filename* values for each CLMS server are different.

Perform the following to view the sample configuration.

1. Execute the following command to open the template file.

```
$ sudo vi /etc/rsyslog.d/tmpl.conf
```

2. Enter multiple action directives as required. In the following sample configuration, the logs are relayed to five CLMS servers.
   - Following is the sample to relay repo audit logs, all CBAC and OLT logs to multiple log servers.

```
$template logFile, "/var/log/client_logs/CBAC-%fromhostip%/%
programname%.log"
$template repologFile, "/var/log/client_logs/REPO-%fromhostip%/%
programname%.log"
template (name="cbacTemplate" type="list") {
property(name="timegenerated" dateFormat="rfc3339")
constant(value=" CBAC-[")
property(name="fromhost-ip")
constant(value="] ")
property(name="programname")
constant(value=":")
property(name="msg" spifno1stsp="on" )
property(name="msg")
constant(value="\n")
}
template (name="oltTemplate" type="list") {
property(name="timegenerated" dateFormat="rfc3339")
constant(value=" OLT-[")
property(name="fromhost-ip")
constant(value="] ")
property(name="programname")
constant(value=":")
```

```
property(name="msg" spifno1stsp="on" )
property(name="msg")
constant(value="\n")
}
template (name="repoTemplate" type="list") {
property(name="timegenerated" dateFormat="rfc3339")
constant(value=" REPO-[")
property(name="fromhost-ip")
constant(value="] ")
property(name="programname")
constant(value=":")
property(name="msg" spifno1stsp="on" )
property(name="msg")
constant(value="\n")
}
if ($fromhost-ip != "127.0.0.1") then {
if ($programname == 'repo_audit' or $programname == 'registry_audit' or
$programname == 'apache_audit' or $programname == 'nginx_audit' or
$programname == 'repo_registery_audit' or $programname ==
'repo_notifier_audit') then {
action(type="omfwd" target="172.27.172.42" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer1"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off" template
="repoTemplate")
action(type="omfwd" target="172.27.172.222" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer2"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="repoTemplate")
action(type="omfwd" target="172.27.172.239" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer3"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="repoTemplate")
action(type="omfwd" target="172.27.172.110" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer4"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="repoTemplate")
action(type="omfwd" target="172.27.172.219" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer5"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="repoTemplate")
*.* ?repologFile
} else {
if ($source startswith 'SDPON-') then {
$template logFile, "/var/log/client_logs/CBAC-%fromhostip%/%
```

```
programname%.log"
action(type="omfwd" target="172.27.172.42" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer1"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="repoTemplate")
action(type="omfwd" target="172.27.172.222" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer2"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="repoTemplate")
action(type="omfwd" target="172.27.172.239" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer3"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="repoTemplate")
action(type="omfwd" target="172.27.172.110" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer4"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="repoTemplate")
action(type="omfwd" target="172.27.172.219" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer5"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="repoTemplate")
*.* -?logFile
}
else {
$template logFile, "/var/log/client_logs/CBAC-%fromhostip%/%
programname%.log"
action(type="omfwd" target="172.27.172.42" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer1"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="oltTemplate")
action(type="omfwd" target="172.27.172.222" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer2"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="oltTemplate")
action(type="omfwd" target="172.27.172.239" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer3"
```

```
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="oltTemplate")
action(type="omfwd" target="172.27.172.110" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer4"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="oltTemplate")
action(type="omfwd" target="172.27.172.219" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer5"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="oltTemplate")
*.* -?logFile
}
}
}
```

- Following is the sample template to relay security audit logs to multiple log servers.

  Execute the following command to relay security audit logs to multiple log servers.

```
# /etc/rsyslog.d/tmpl.conf
$template logFile, "/var/log/client_logs/CBAC-%fromhostip%/%
programname%.log"
$template repologFile, "/var/log/client_logs/REPO-%fromhostip%/%
programname%.log"
template (name="cbacTemplate" type="list") {
property(name="timegenerated" dateFormat="rfc3339")
constant(value=" CBAC-[")
property(name="fromhost-ip")
constant(value="] ")
property(name="programname")
constant(value=":")
property(name="msg" spifno1stsp="on" )
property(name="msg")
constant(value="\n")
}
template (name="oltTemplate" type="list") {
property(name="timegenerated" dateFormat="rfc3339")
constant(value=" OLT-[")
property(name="fromhost-ip")
constant(value="] ")
property(name="programname")
constant(value=":")
property(name="msg" spifno1stsp="on" )
property(name="msg")
constant(value="\n")
}
template (name="repoTemplate" type="list") {
property(name="timegenerated" dateFormat="rfc3339")
constant(value=" REPO-[")
property(name="fromhost-ip")
constant(value="] ")
```

```
property(name="programname")
constant(value=":")
property(name="msg" spifno1stsp="on" )
property(name="msg")
constant(value="\n")
}
if ($fromhost-ip != "127.0.0.1") then {
if ($programname == 'repo_audit' or $programname == 'registry_audit' or
$programname == 'apache_audit' or $programname == 'nginx_audit' or
$programname == 'repo_registery_audit' or $programname ==
'repo_notifier_audit') then {
action(type="omfwd" target="172.27.172.42" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer1"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template ="repoTemplate")
action(type="omfwd" target="172.27.172.222" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer2"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="repoTemplate")
action(type="omfwd" target="172.27.172.239" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer3"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="repoTemplate")
action(type="omfwd" target="172.27.172.110" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer4"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="repoTemplate")
action(type="omfwd" target="172.27.172.219" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer5"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="repoTemplate")
*.* ?repologFile
} else {
if ( $programname == 'SDPONAuditLogs' or $programname ==
'SDPONSecurityAuditLogs' or $syslogfacility-text == 'local5') then {
$template logFile, "/var/log/client_logs/CBAC-%fromhostip%/%
programname%.log"
action(type="omfwd" target="172.27.172.42" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer1"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="cbacTemplate")
```

```
action(type="omfwd" target="172.27.172.222" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer2"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="cbacTemplate")
action(type="omfwd" target="172.27.172.239" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer3"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="cbacTemplate")
action(type="omfwd" target="172.27.172.110" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer4"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="cbacTemplate")
action(type="omfwd" target="172.27.172.219" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer5"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="cbacTemplate")
*.* -?logFile
}
else {
if ($syslogfacility-text == 'local1' ) then {
$template logFile, "/var/log/client_logs/CBAC-%fromhostip%/%
programname%.log"
action(type="omfwd" target="172.27.172.42" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer1"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="oltTemplate")
action(type="omfwd" target="172.27.172.222" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer2"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="oltTemplate")
action(type="omfwd" target="172.27.172.239" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer3"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="oltTemplate")
action(type="omfwd" target="172.27.172.110" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer4"
```

```
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="oltTemplate")
action(type="omfwd" target="172.27.172.219" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer5"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="oltTemplate")
*.* -?logFile
}
*.* -?logFile
}
}
}
```

where 172.27.172.42, 172.27.172.222, 172.27.172.239, 172.27.172.110 and 172.27.172.219 are the sample IP addresses of the 5 CLMS servers to which the CBAC, OLT audit logs need to be relayed.

- **Forwarding Logs Based on Filters**

  The following table explains the different topics used to control the relay of logs to the remote syslog server.

  In CBAC, logstash is responsible for reading all the logs from kafka and push them to the syslog server.

Table 4. Different Topics to Control the Relay of Logs to Remote Syslog Server

Topic Name	Decription	Required Code to Filter
LOGMGR_LOG	All logs generated by the **log manager** microservice are pushed to kafka with the topic name as *"LOGMGR_LOG"*. Logstash forwards all logs to the syslog server with topic name as *"LOGMGR_LOG"*.	if $programname=='LOGMGR_LOG'
TELEMETRY-LOG	All logs generated by the **telemetry** microservice are pushed to kafka with the topic name as *"TELEMETRYLOG"*.	if $programname=='TELEMETRY-LOG'

Topic Name	Decription	Required Code to Filter
	Logstash forwards all telemetry logs to the syslog server with program name as *"TELEMETRY-LOG"*.	
INFLUXDB-LOG	All logs generated by **InfluxDB** microservice are pushed to kafka with topic name as *"INFLUXDB-LOG"*. Logstash forwards all influxDB logs to the syslog server with program name as *"INFLUXDB-LOG"*.	if $programname=='INFLUXDB-LOG'
SubMgr-logs	All logs generated by the **sdpon subscriber manager** microservice are pushed to kafka with topic name as *"SubMgr-logs"*. Logstash forwards all submgr logs to the syslog server with program name as *"SubMgr-logs"*.	if $programname=='SubMgr-logs'
DEVICEMGR-LOG	All logs generated by the **sdpon device manager** microservice are pushed to kafka with topic name as *"DEVICEMGR-LOG"*. Logstash forwards all device manager logs to the syslog server with program name as *"DEVICEMGR-LOG"*.	if $programname=='DEVICEMGR-LOG'
AccGw-logs	All logs generated by the **sdpon access gateway** microservice are pushed to kafka	if $programname=='AccGw-logs'

Topic Name	Decription	Required Code to Filter
	with topic name as *"AccGw-logs"*. Logstash forwards all access gateway logs to the syslog server with program name as *"AccGw-logs"*.	
SECURITY-LOG	All logs generated by the **sdpon security** microservice are pushed to kafka with topic name as *"SECURITYLOG"*. Logstash forwards all sdpon security logs to the syslog server with program name as *"SECURITY-LOG"*.	if $programname=='SECURITY-LOG'
OPENOLT-LOG	All logs generated by the **OpenOLT** adapter microservice are pushed to kafka with topic name as *"OPENOLTLOG"*. Logstash forwards all openOLT logs to the syslog server with program name as *"OPENOLT-LOG"*.	if $programname=='OPENOLT-LOG'
OPENONU-LOG	All logs generated by the **OpenONU** adapter microservice are pushed to kafka with topic name as *"OPENONU-LOG"*. Logstash forwards all openONU logs to the syslog server with program name as *"OPENONU-LOG"*.	if $programname=='OPENONU-LOG'
RWCORE-LOG	All logs generated by the **rwcore**	if $programname=='RWCORE-LOG'

Topic Name	Decription	Required Code to Filter
	microservice are pushed to kafka with topic name as *"RWCORE-LOG"*. Logstash forwards all rwcore logs to the syslog server with program name as *"RWCORE-LOG"*.	
EXTERNALKAFKA- LOG	All logs generated by the **external kafka** are pushed to kafka with topic name as *"EXTERNAL-KAFKA-LOG"*. Logstash forwards all external kafka logs to the syslog server with program name as *"EXTERNAL-KAFKALOG"*.	if $programname=='EXTERNAL-KAFKALOG'
INTERNALKAFKA0- LOG	All logs generated by **internal kafka** are pushed to kafka with topic name as *"INTERNAL-KAFKA0-LOG"*. Logstash forwards all internal kafka logs to the syslog server with program name as *"INTERNAL-KAFKA0-LOG"*.	if $programname=='INTERNAL-KAFKA0-LOG'
ETCD0-LOG	All logs generated by the **etcd** are pushed to kafka with topic name as *"ETCD0-LOG"*. Logstash forwards all etcd logs to the syslog server with program name as *"ETCD0-LOG"*.	if $programname=='ETCD0-LOG'

Topic Name	Decription	Required Code to Filter
LOGSTASH-LOG	All logs generated by the **logstash** microservice are pushed to kafka with topic name as *"LOGSTASH-LOG"*. Logstash forwards all logstash logs to the syslog server with program name as *"LOGSTASH-LOG"*.	if $programname=='LOGSTASH-LOG'
FILEBEAT-LOG	Logs generated by third party services are consumed by file-beat, then formatted and pushed to kafka with topic name as *"FILEBEAT-LOG"*. Logstash forwards all **filebeat** logs to the syslog server with program name as *"FILEBEAT-LOG"*.	if $programname=='FILEBEAT-LOG'
LWC-LOGS	All logs generated by the **LWC** microservice are pushed to kafka with topic name as *"LWC-LOGS"*. Logstash forwards all LWC logs to the syslog server with program name as *"LWC-LOGS"*.	if $programname=='LWC-LOGS'
EXTERNALKAFKAZOOKEEPER-LOG	All logs generated by **external kafka zookeeper** are pushed to kafka with topic name as *"EXTERNALKAFKA-ZOOKEEPER-LOG"*. Logstash forwards all external kafka zookeeper logs to the	if $programname=='EXTERNAL-KAFKAZOOKEEPER- LOG'

Topic Name	Decription	Required Code to Filter
	syslog server with program name as *"EXTERNALKAFKA-ZOOKEEPER-LOG"*.	
INTERNALKAFKAZOOKEEPER-LOG	All logs generated by **internal kafka zookeeper** are pushed to kafka with topic name as *"INTERNAL-KAFKAZOOKEEPER0- LOG"*. Logstash forwards all internal kafka zookeeper logs to the syslog server with program name as *"INTERNALKAFKA-ZOOKEEPER0-LOG"*.	if $programname== 'INTERNAL-KAFKAZOOKEEPER0-LOG'
MONMGR-LOG	All logs generated by the **sdpon monitoring manager** microservice are pushed to kafka with topic name as *"MONMGR-LOG"*. Logstash forwards all monitoring manager logs to the syslog server with program name as *"MONMGR-LOG"*.	if $programname=='MONMGR-LOG'
NDA-LOG	All logs generated by the CBAC **NDA** microservice are pushed to kafka with topic name as *"NDA-LOG"*. Logstash forwards all NDA logs to the syslog server with program name as *"NDA-LOG"*.	if $programname=='NDA-LOG'
NCM-LOG	All logs generated by the **NCM** microservice	if $programname=='NCM-LOG'

Topic Name	Decription	Required Code to Filter
	are pushed to kafka with topic name as *"NCM-LOG"*. Logstash forwards all NCM logs to the syslog server with program name as *"NCM-LOG"*.	
REDIS-LOG	All logs generated by **redis** are pushed to kafka with topic name as "REDIS-LOG". Logstash forwards all redis logs to the syslog server with program name as *"REDIS-LOG"*.	if $programname=='REDIS-LOG'
VOLTHACTL-LOG	All logs generated by the **voltctl** microservice are pushed to kafka with topic name as *"VOLTHACTL-LOG"*. Logstash forwards all voltctl logs to the syslog server with program name as *"VOLTHACTL-LOG"*.	if $programname== 'VOLTHACTL-LOG'
MSM-LOG	All logs generated by the CBAC **msm** (microservice manager) are pushed to kafka with topic name as *"MSMLOG"*. Logstash forwards all msm logs to the syslog server with program name as *"MSM-LOG"*.	if $programname=='MSM-LOG'
INTERSDPONGWLOG	All logs generated by the **inter SDPON gateway** microservice are pushed to kafka with topic name as	if $programname== 'INTERSDPONGWLOG'

Topic Name	Decription	Required Code to Filter
	"INTERSDPONGW-LOG". Logstash forwards all inter CBAC gateway logs to the syslog server with program name as *"INTERSDPONGWLOG"*.	
EMSCLI-LOG	All logs generated by the **sdpon ems CLI** microservice are pushed to kafka with topic name as *"EMSCLI-LOG"*. Logstash forwards all ems CLI logs to the syslog server with program name as *"EMSCLI-LOG"*.	if $programname=='EMSCLI-LOG'
SDPONAuditLogs	All **sdpon audit logs** are pushed to kafka with the topic name as *"SDPONAuditLogs"*. Logstash forwards all sdpon audit logs to the syslog server with program name as *"SDPONAuditLogs"*.	if $programname=='SDPONAuditLogs'
SDPONSecurity AuditLogs	All audit logs generated by the **sdpon security** microservice are pushed to kafka with topic name as *"SDPONSecurityAuditLogs"*. Logstash forwards all sdpon security audit logs to the syslog server with program name as	if $programname== 'SDPONSecurityAuditLogs'

Topic Name	Decription	Required Code to Filter
	"SDPONSecurityAuditLogs".	
apache_audit	**Apache** service logs from the repo server are forwarded to the syslog server with program name as *"apache_audit"*.	if $programname=='apache_audit'
repo_audit	All **nginx** access logs from the repo server are forwarded to the syslog server with program name as *"repo_audit"*.	if $programname=='repo_audit'
nginx_audit	Audit logs of the **nginx-proxy** container are forwarded from the repo server to the syslog server with program name as *"nginx_audit"*.	if $programname=='nginx_audit'
repo_registery_audit	Audit logs of the **registry** container are forwarded from the repo server to the syslog server with program name as *"repo_registery_audit"*.	if $programname== 'repo_registery_audit'
repo_notifier_audit	Audit logs of the **repo-notifier** container are forwarded from the repo server to the syslog server with program name as *"repo_notifier_audit"*.	if $programname=='repo_notifier_audit'
OLTapplogs	All OLT logs except *"auth"*/*"authpriv"* can be forwarded to the syslog server.	-

Execute the following command to filter EMSGW , LOGMGR, and TELEMETRY logs based on the program name.

```
# /etc/rsyslog.d/tmpl.conf
# Below example configuration is to filter EMSGW log, LOGMGR log and
TELEMETRY log based on the programname
...
if ($programname == EMSGW-LOG" or $programname=="LOGMGR_LOG" or
$programname=="TELEMETRY-LOG") then {
$template logFile, "/var/log/client_logs/CBAC-%fromhostip%/%
programname%.log"
action(type="omfwd" target="172.x.y.z" port="514"
protocol="udp" action.resumeRetryCount="-1"
queue.type="linkedList"
queue.size="10000" queue.filename="storage-buffer2"
queue.maxDiskSpace="1g" queue.saveOnShutdown="on"
action.execOnlyWhenPreviousIsSuspended="off"
template="oltTemplate")
*.* -?logFile
}
# where 172.x.y.z is the CLMS server IP
...
```

3. Execute the following command to reload the rsyslog service.

```
[demo@rsyslog-server ~]# sudo systemctl restart rsyslog
```

Installing Keepalived

This section covers the procedure for keepalived installation, the configuration of master server, the configuration of backup server, and configuration of the (VRRP).

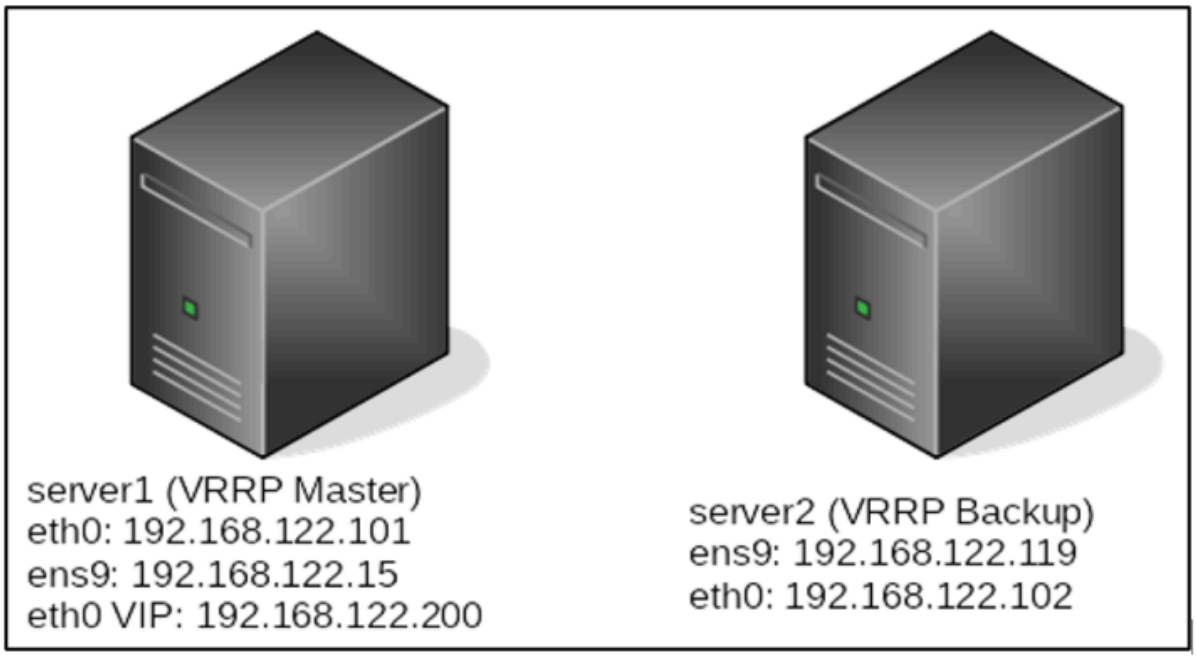
Installing Keepalived for Achieving Redundancy

To avoid deployment failures and offer high availability, the redundant servers are used instead of a single node for repository server, SFTP server, or log server. Redundant SFTP, repository, and log servers are preferred for high availability.

Keepalived is a Linux package that uses Virtual Router Redundancy Protocol (VRRP) to deliver high availability among Linux servers.

Keepalived provides redundancy through the VRRP protocol, which ensures that the redundant server prevents data loss when the primary server fails.

Figure 33. Keepalived Topology

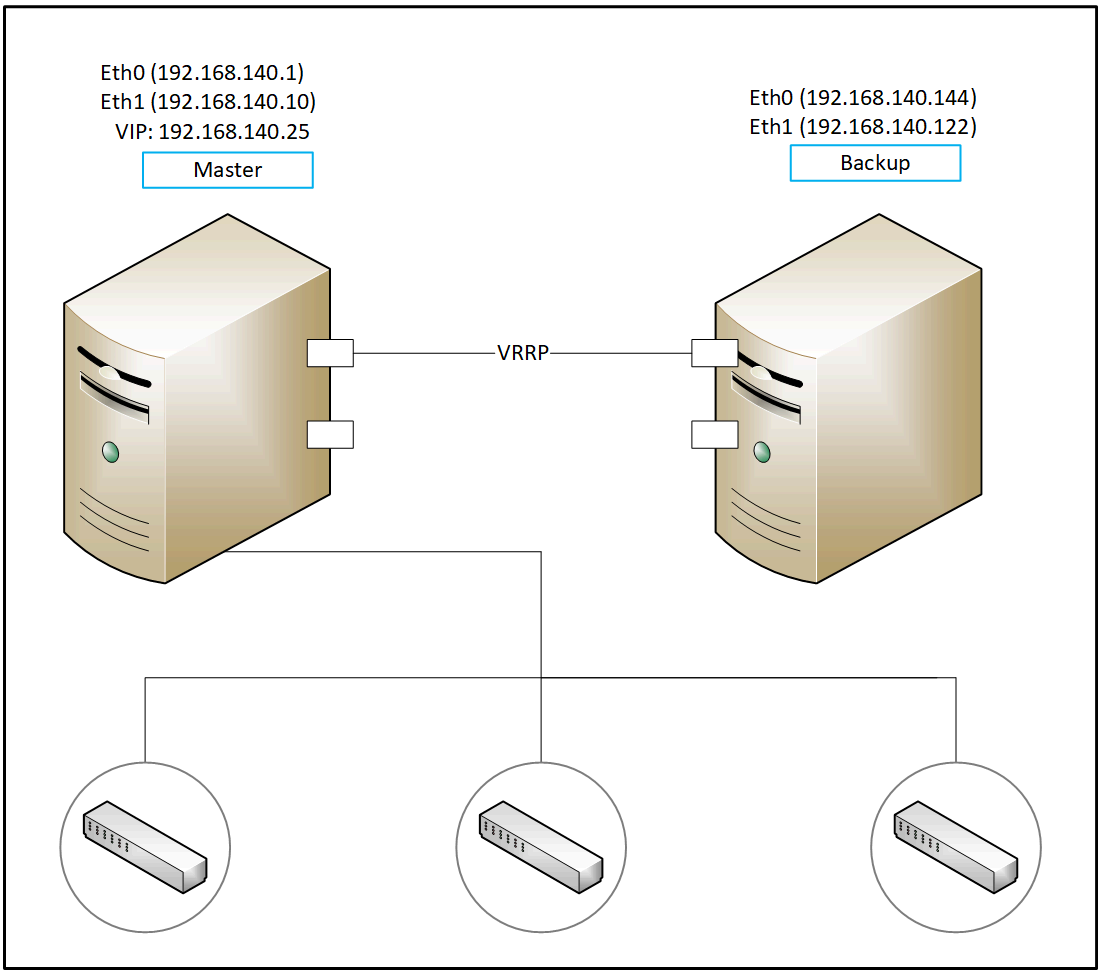


In the above keepalived topology, server 1 is the master and is responsible for the 192.168.122.200 IP address. If server 1 fails, then server 2 takes over this IP.

VRRP uses the concept of a virtual IP address (VIP). It determines which hosts (servers, routers, and so on) are responsible for controlling the VIP and only one host (the master) controls the VIP at a time. If the master fails, VRRP provides mechanisms for quickly switching to a standby host.

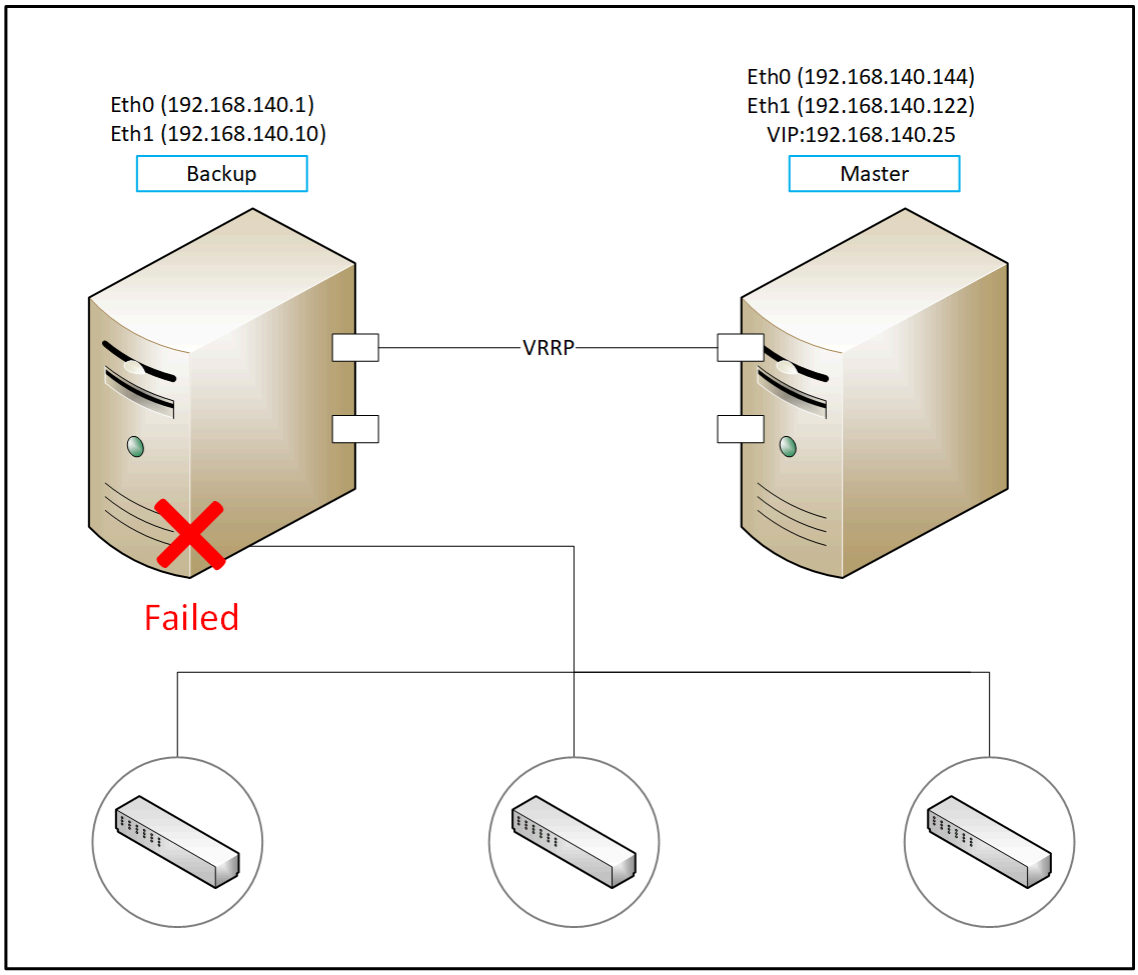
The following diagram represents the working of the system log server when the master and the backup servers are running.

Figure 34. System log Server Master and Backup



The following diagram represents when the master server is failed, the backup server is turned into the master server.

Figure 35. System log Server Master Failed



Installing Keepalived

1. Execute the following commands to install keepalived on both master and backup servers. Master server is the primary server, and the slave server is the backup server.

```
sudo apt-get update
sudo apt install keepalived
```

2. Execute the following command to view the keepalived version after installing it.

```
sudo keepalived --version
```

3. To configure keepalived, create and edit the `/etc/keepalived/keepalived.conf` file on both master and backup servers.
4. Execute the following command to create a directory.

```
sudo mkdir /etc/keepalived
```

Installing Keepalived with Offline Repository

Perform the following steps to install keepalived using the offline repository.

1. Remove nameservers from the `/etc/resolv.conf` and `/etc/netplan/01-netplan.yaml` files to ensure that it does not reach the Internet.
2. Remove all other sources pointing to the Internet including `/etc/apt/sources.list.d/mongodb-org-4.2.list`.
3. Execute the configure.sh command to install keepalived using an offline repository for apt and pip packages. The `configure.sh` file is included in the HDD offline package.

   For more information, refer to the Setting Up RMS Repository Server section in the following guides based on the RMS deployment type.

   - *Single Node RMS Installation and Upgrade Guide*
   - *Multinode RMS Installation and Upgrade Guide*

   Note: In case of failures of primary or secondary nodes, see Replacing SFTP Server *(on page 277)* section.

Configuring Master and Backup Server for VRRP

This section covers the configuration details of the master server and backup server.

Configuring Master Server for Server 1

Edit the keepalived.conf file for the master server and add the following lines.

```
sudo vi /etc/keepalived/keepalived.conf
global_defs
{
vrrp_version 2
vrrp_garp_master_delay 1
script_user root
enable_script_security
}
vrrp_instance VI_1
{
state BACKUP
interface ens256
virtual_router_id 51
priority 251
advert_int 1
nopreempt
authentication
{
auth_type PASS
auth_pass 12345
}
virtual_ipaddress
{
1212::1:13/64
```

```
}
track_interface
{
ens256 weight 5
}
}
```

Configuring Backup Server for Server 2

Edit the *keepalived.conf* file for the backup server and add the following lines.

```
sudo vi /etc/keepalived/keepalived.conf
global_defs
{
vrrp_version 2
vrrp_garp_master_delay 1
script_user root
enable_script_security
}
vrrp_instance VI_1
{
state BACKUP
interface ens256
virtual_router_id 51
priority 250
advert_int 1
nopreempt
authentication
{
auth_type PASS
auth_pass 12345
}
virtual_ipaddress
{
1212::1:13/64
}
track_interface
{
ens256 weight 5
}
}
```

Note:

- Virtual IP addresses that are used for the configuration must not be used for any other purpose.
- For VIPs on other interfaces, you must create a different VRRP instance with the different VIPs.

The following table explains the parameters used in the master and backup server configuration.

Table 5. Server Configuration Parameters

Configuration Parameter	Description
Global defs	
Vrrp version	Specifies the version of the virtual router redundancy protocol. For example, 2.
vrrp_garp_master_delay	Specifies the delay for the second set of gratuitous ARPs after the transition to MASTER.
script_user	Specifies the root user
enable_script_security	Keepalived does not allow a non-root user to modify the scripts, which means that a non root user cannot run a program with the root privileges.
vrrp_instance MAIN	
vrrp_instance	Specifies an individual instance of the VRRP protocol running on an interface.
state	Specifies both states as a backup because no pre-empt works only with state backup, and it helps prevent fallback.
interface	Specifies the interface that VRRP runs on.
virtual_router_id	Specifies the virtual router ID. The virtual router ID must be unique per the VRRP cluster. The same VRRP instances should have the same value.
priority	VRRP uses the concept of priority when determining the active master server. The server with the highest priority acts as the master, holding onto the VIP and servicing requests.
advert_int	Specifies the frequency at which the advertisements are sent. For example, 1 second.
nopreempt	Prevents fallback.
authentication	Specifies the information necessary for servers participating in VRRP to authenticate with each other.
virtual_ipaddress	Specifies the IP addresses (there can be multiple) that VRRP is responsible for.
track_interface	It is used to adjust the priority of the Keepalived instance based on the status of an interface. Once the interface is down, the priority of that configuration goes down by the weight mentioned.

Configuring Virtual Router Redundancy Protocol

The VRRP is a protocol that offers high availability for a network or subnetwork. This section covers the configuration steps for VRRP.

Prerequisites

The following requirements must be fulfilled before VRRP configuration.

- Install the Keepalived. For more information, see the Installing Keepalived *(on page 90)* section.
- Configure server 1 as a MASTER system log server and server 2 as a BACKUP system log server, which makes them the primary and backup log server.
- Place the configuration file for Keepalived at `/etc/keepalived/keepalived.conf` file.
- The virtual IP address of VRRP must be the same and free to use.

VRRP Configuration

Execute the following command to start the keepalived service after installing keepalived and ensuring that the required configurations have been completed on both master and backup servers.

```
sudo service keepalived start or sudo systemctl start keepalived
```

Useful Commands

The following commands are used to restart, stop, and check the status of keepalived.

- Execute the following command to check the status of keepalived service.

  ```
  sudo service keepalived status
  ```

- Execute the following command to restart the keepalived service.

  ```
  sudo service keepalived restart
  ```

- Execute the following command to stop the keepalived service.

  ```
  sudo service keepalived stop
  ```

Replacing Keepalived Cluster Node

This section explains the procedure to replace the failed keepalived cluster node with the new node.

The redundant (active and standby) servers are used instead of a single node for log server, repository server, and SFTP server.

The VIP is set to the active server. When the active server fails, VRRP switchover happens and the VIP moves to the standby server, which now serves as the active server.

Perform the following to replace the failed keepalived cluster node with the new node.

1. Execute the following commands to install the keepalived in the new node.

   Note: To install keepalived in the offline mode, see the Installing Keepalived with Offline Repository *(on page 94)* section.

   ```
   sudo apt-get update
   sudo apt install keepalived
   ```

2. Take the backup of the keepalived configuration of the failed node.

   Note: It is recommended to take the backup of the keepalived configuration for all the nodes. The same configuration can be used to replace a failed node. If the backup of the keepalived configuration is not available, you can copy the configuration from the other running server and assign the priority according to its role (active/standby).

3. Copy the keepalived configuration backup file to the new node in the `/etc/keepalived/keepalived.conf` file.
4. If the keepalived is still running on the failed node (VM or hardware failure, OS has not crashed), execute the following command to stop the keepalived.

   ```
   sudo service keepalived stop
   ```

   Note: The VIP switches over to the standby node if the active server is replaced.

5. Execute the following command to make the new node as a part of the keepalived cluster and start the keepalived service on the new node.

   ```
   sudo service keepalived start
   ```

6. Verify the keepalived service status of the nodes using any one of the following methods.
   - Execute the following commands on both the failed and new nodes.

     ```
     sudo service keepalived status
     ```

   - Execute the following command on the master node to check the VIP movement between the nodes.

     ```
     sudo service keepalived restart
     ```

   - Execute the following command to check the VIP presence on the master node.

     ```
     ip -a address
     ```

Upgrading OLT and CBAC Software

This chapter provides information on how to upgrade CBAC and OLT Software using RMS remotely.

Prerequisites

- Upgrade RMS to 4.1.0 version. For more information on RMS upgrade, refer to the *Upgrading RMS* section in the following guides based on the RMS deployment type.
  - *Single Node RMS Installation and Upgrade Guide*
  - *Multinode RMS Installation and Upgrade Guide*
- Before upgrading the CBAC software, disable the auto SSD firmware upgrade to prevent any deployment failures.

  Execute the following command to create an empty file in the OLT to disable the auto SSD Firmware upgrade.

  ```
  sudo touch /mnt/onl/config/no_auto_update_ssd_fw
  ```

Upgrade Sequence

CBAC and OLT must be upgraded to the new version as per the following sequence.

1. Upgrading CBAC Software *(on page 99)*
2. Upgrading OLT Software *(on page 105)*

Upgrading CBAC Software

The CBAC software can be upgraded to R4.1.0 from R4.0.0 or R4.0.1.

Before upgrading CBAC software, fulfill the prerequisites mentioned in the *OLT and CBAC Software Upgrade* section. See Prerequisites *(on page 99)*.

Perform the following steps to upgrade CBAC software.

1. Update the repository server with the *CBAC-R4.1.0* package.
2. After updating the R4.1.0 package in the repository server, the user has two options for proceeding with the CBAC upgrade.
   - If the NEW-SDPON-SOFTWARE-AVAILABLE event is reported in RMS, go to step 4 *(on page 100)* to proceed with the upgrade either from inventory or using a task.

     or

     CBAC checks the availability of the new software version between 0 and 60 minutes and notifies RMS. Once the event is reported, go to step 4 *(on page 100)* to proceed with the upgrade either from inventory or using a task.

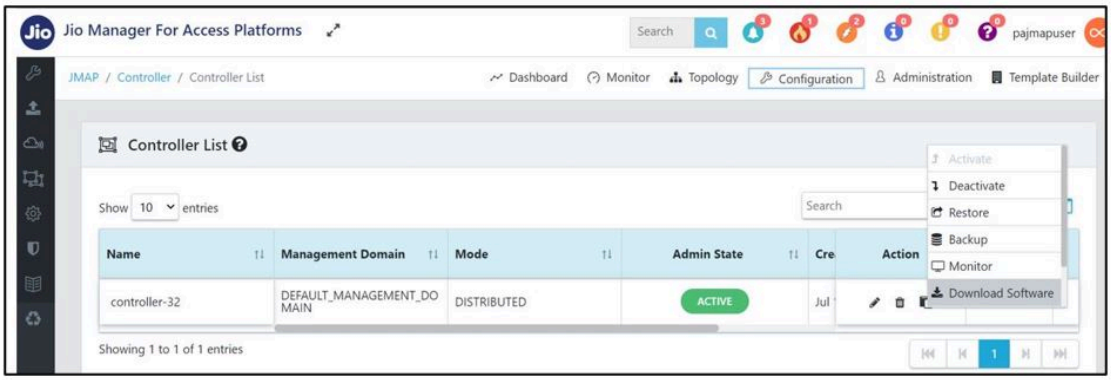
- Select the **Download Software** option in **Configuration > Controller > Action** page to proceed with the CBAC upgrade before the NEW-SDPON-SOFTWARE-AVAILABLE event is available in RMS. Go to step 3 *(on page 100)* and proceed with the on-demand software download.

  or

  When creating tasks, to perform download and upgrade actions together. See Upgrading CBAC Controller from Task *(on page 101)*.

3. Ignore this step if the NEW-SDPON-SOFTWARE-AVAILABLE notification is already noticed in the event.
   a. Click the **Download Software** option in the controller.

Figure 36. Download Software

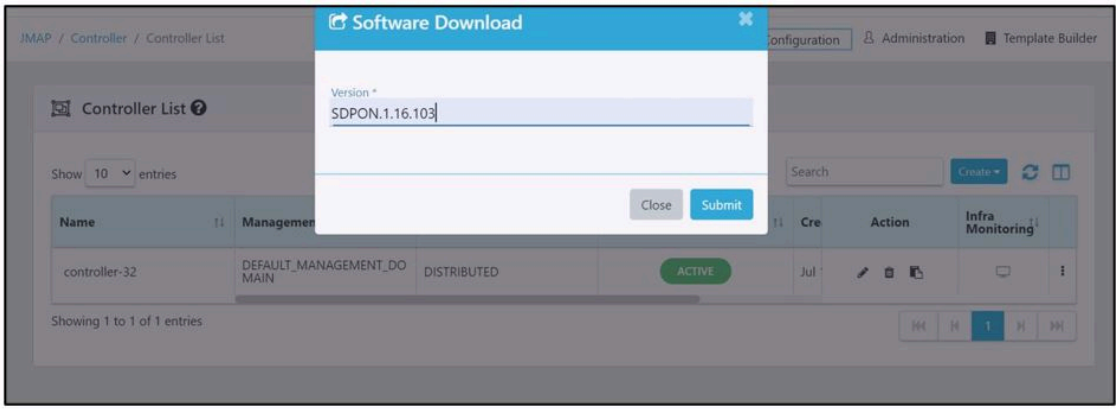


   b. As shown in the Figure 40 *(on page 100)*, provide the CBAC-R4.1.0 software version details that must be downloaded.

      Once the software download is successful, the SDPON-SOFTWARE-DOWNLOAD-SUCCESSFUL event is reported on the Monitor page.

   c. Upon receiving the event, proceed with the upgrade.

Figure 37. Software Version



4. Execute one of the following tasks to upgrade the CBAC software.
   - Upgrading CBAC from Inventory *(on page 101)*
   - Upgrading CBAC Controller from Task *(on page 101)*

Upgrading CBAC from Inventory

This section covers the procedure to upgrade CBAC from the inventory.

RMS enables the software upgrade option after receiving a NEW-SDPON-SOFTWARE-AVAILABLE event or SDPON-SOFTWARE-DOWNLOAD-SUCCESSFUL event.

Perform the following steps to upgrade the CBAC software.

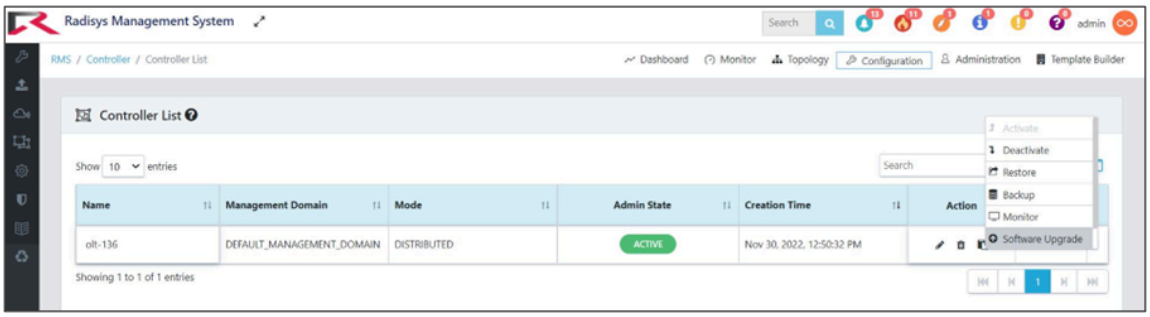
1. Navigate to the RMS GUI.
2. Click **Configuration**from the top right corner of the page.
3. Select **Maintenance** from the left-hand side of the menu.
4. Click **Task > Create**.
5. Select **Configuration > Controller**.

   The Controller List page appears.

6. Click on the three dots corresponding to the controller on which you want to upgrade the software and click the **Software Upgrade** option.

   The Software Upgrade page appears.

   Figure 38. Software Upgrade



7. Enter the SDPON build version corresponding to the CBAC version and click **Submit**.

   After the CBAC upgrade, RMS receives an SDPON-SOFTWARE-UPGRADE-SUCCESSFUL event.

Upgrading CBAC Controller from Task

This section covers the procedure to create a scheduled task for the bulk CBAC controller upgrade.

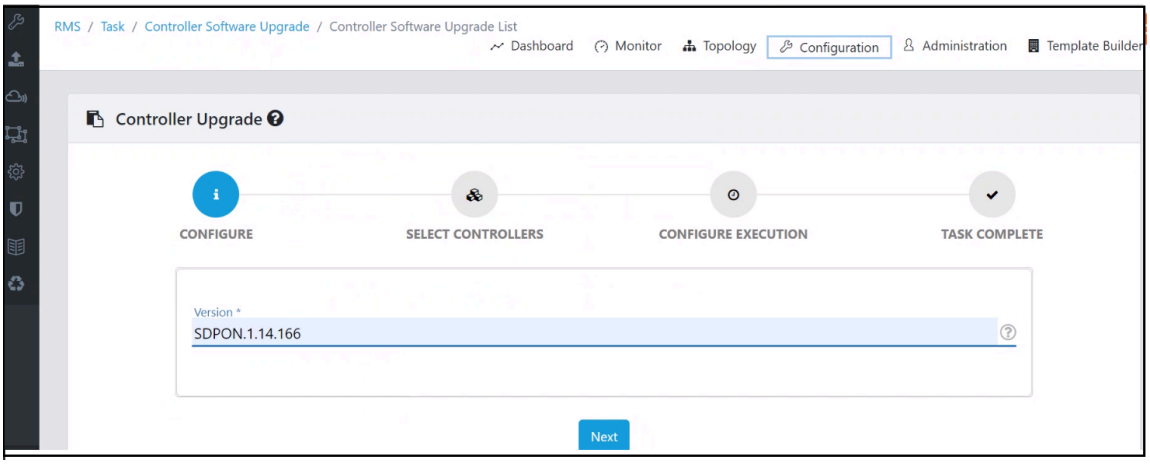
Perform the following steps to create a task for the controller software upgrade.

1. Navigate to the RMS GUI.
2. Click **Configuration** from the top right corner of the page.
3. Select **Maintenance** from the left-hand side of the menu.
4. Click **Task > Create**.
5. Enter the following details.

- **Name**. Enter a unique name for the task.
- **Type**. Select the task type as “Controller Software Upgrade”.
- **Short Description**. Enter a meaningful short description of the task.

6. Enter the SDPON version for the CBAC upgrade.

Figure 39. Controller Upgrade



7. Click **Next**.

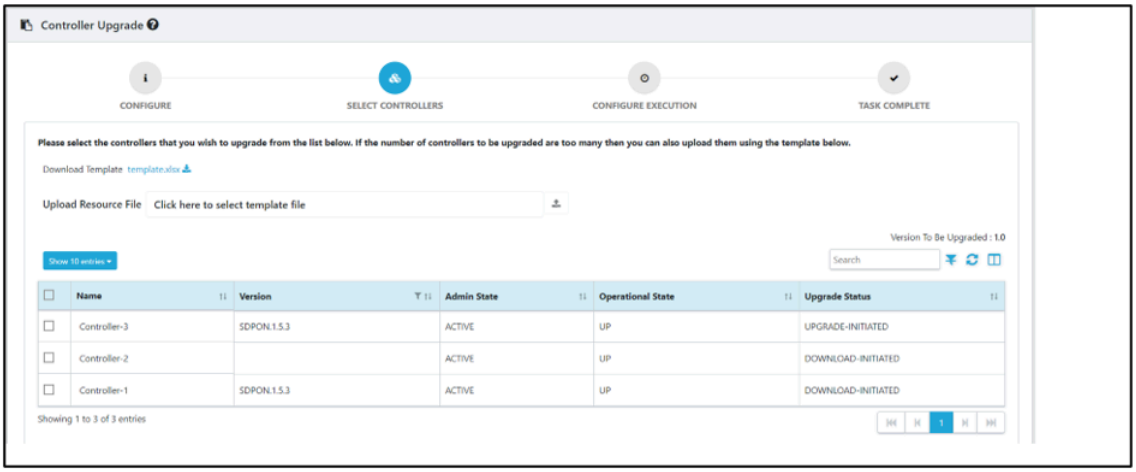
You can upgrade one or more controllers using the following two methods.

- Using Template Upload (CSV file) - This method is used for the bulk upgrade of the controller. Go to step 9 *(on page 102)*.
- Selecting controllers on GUI - This method is used for the single or bulk upgrade of the controller. Go to step 10 *(on page 103)*.

8. Select the **Controllers** page.

The Controller Upgrade page appears.

Figure 40. Controller Upgrade



9. Perform the following steps to upgrade the controller through template (CSV file).

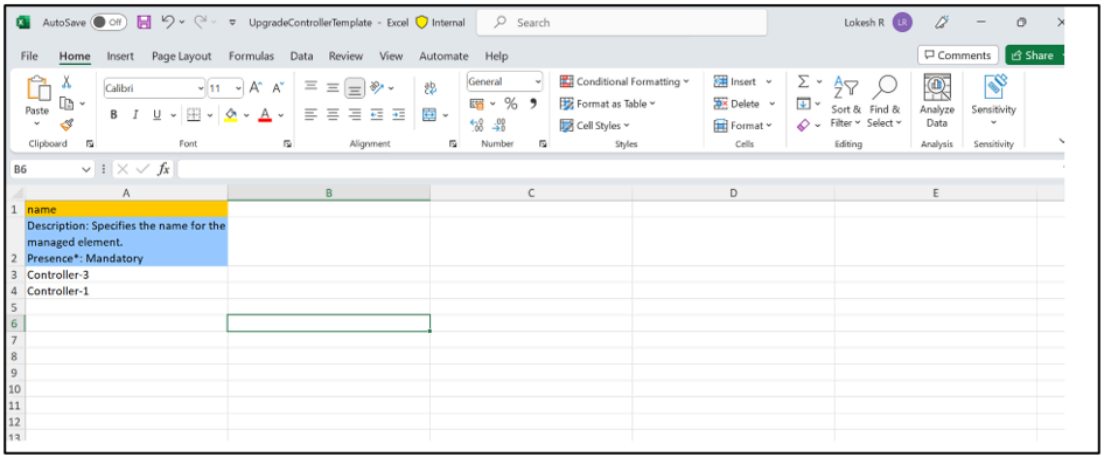
Note: Skip this step and see step 10 *(on page 103)* to upgrade the controller through controller selection.

a. Click on the **template.xlsx** file to download the template.

b. Enter the list of controllers and save the downloaded template.

Note: The user can provide maximum 100 entries in the CSV file at single task.

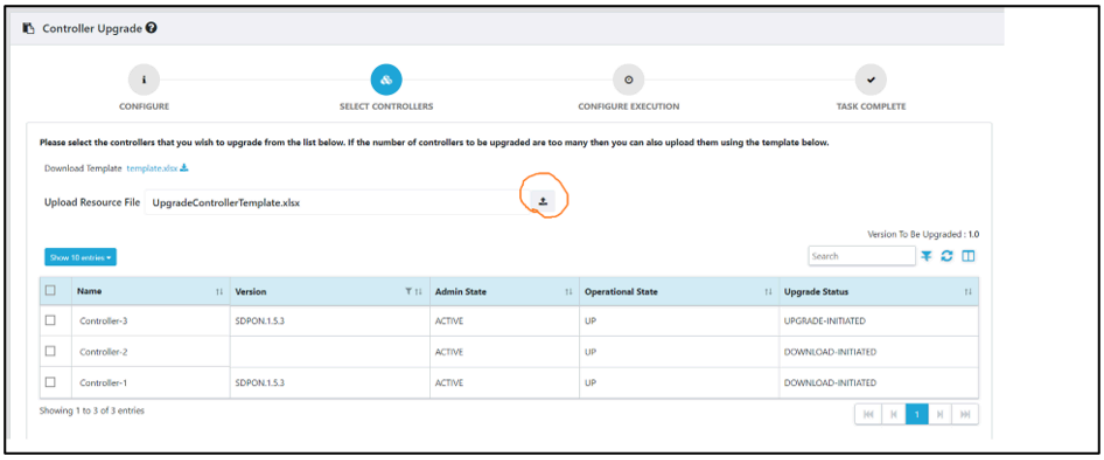
Figure 41. Sample CSV Template



c. Click on **Upload Resource File** and select the updated template. Continue with step 11 *(on page 104)* to upgrade the OLT software.

A confirmation message indicates that the upload is successful.

Figure 42. Upload CSV file

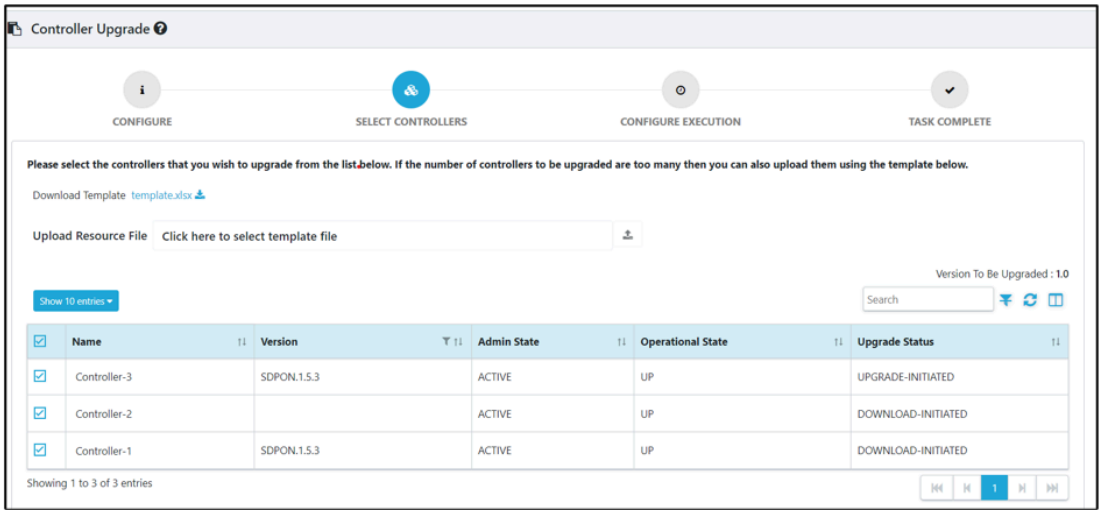


10. Perform the following steps to upgrade the controller through controller selection on RMS GUI.

Note: Skip this step and see step 9 *(on page 102)* to upgrade the OLT through template (CSV file).

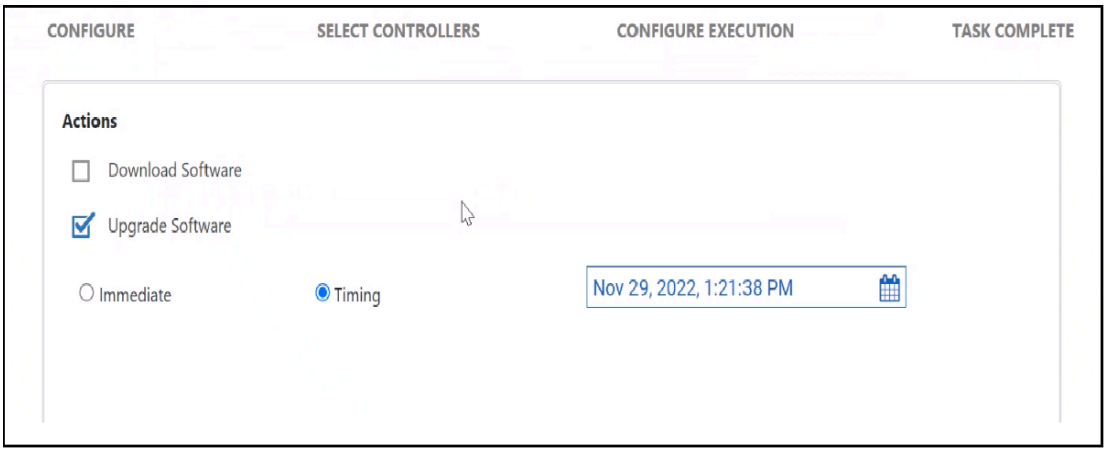
a. Select the checkbox for the applicable controllers for which the upgrade status is *NEW-SDPON-SOFTWARE-AVAILABLE* and click **Next**.

Figure 43. Controllers Selection



11. Select **Upgrade Software** and time (Immediate/Timing) for CBAC upgrade.
    - Select **Download Software** if *NEW-SDPON-SOFTWARE-AVAILABLE* notification is not listed in the controller.

Figure 44. Upgrade Software



12. Click **SUBMIT**.
13. The **TASK COMPLETE** tab is enabled and changed to green color.

    A confirmation message appears, indicating the software upgrade task status (completed/failed) based on the CBAC response.

    After the CBAC upgrade, RMS receives an SDPON-SOFTWARE-UPGRADE-SUCCESSFUL event.

Enabling SNMP Service

This section covers the procedure to enable the SNMP service.

Perform the following steps to enable the SNMP service post CBAC 4.1.0 upgrade.

1. Check the **enable_snmp** parameter in the `inventory/group_vars/all` file from the *deployment_ansible* folder in the OLT.
2. Add the **enable_snmp: yes** parameter to the `inventory/group_vars/all` file if the entry is absent.
3. The **enable_snmp** parameter value must be changed from **no** to **yes** if the parameter exists in the file.

   For example, **enable_snmp: yes**.

4. Execute the following command to bring up SNMP after modifying the **enable_snmp** parameter to ***yes*** in the `inventory/group_vars/all` file.

   ```
   sudo ansible-playbook deployment.yml --tags snmp
   ```

5. Execute the following command to verify SNMP status once the SNMP bring up is complete.

   ```
   sudo kubectl get pods | grep snmp
   ```

   Figure 45. SNMP Status

   ```
   oltausr@localhost:~$ sudo kubectl get pods | grep snmp
   sdponsnmpagent-5959fbf457-xbcl8           1/1     Running     0              136m
   oltausr@localhost:~$
   ```

   An SNMP agent is automatically configured for further upgrades.

Upgrading OLT Software

The OLT software can be upgraded to R4.1.0 from R4.0.0 or R4.0.1.

Before upgrading OLT software, fulfill the prerequisites mentioned in the *OLT and CBAC Software Upgrade* section. See Prerequisites *(on page 99)*.

The OLT software is divided into multiple layers, such as Network Operating System (NOS), the application layer, and firmware, and it supports the upgrade of all these components.

In addition to supporting the upgrade of a single OLT from RMS, the solution also supports bulk upgrades of OLTs from RMS. The OLT software upgrade (ONL or OLT BINS) is a three-step upgrade process involving the following.

- Download the OLT software to the OLT first from a centralized location.
- Activate the downloaded software on the OLT.
- Commit the software to the OLT.

The upgrade process allows backing out from an upgrade and returning to the previous version using a rollback procedure.

Note: If the OLT contains a different version of firmware (BIOS, CPLD, or FPGA), the firmware is upgraded automatically after an ONL upgrade when the OLT is rebooted, and another reboot is triggered for the firmware changes to be effective.

Perform one of the following tasks to upgrade the OLT software from RMS.

- Upgrading OLT Software from Inventory *(on page 106)*
- Upgrading OLT Software from Task *(on page 108)*

Upgrading OLT Software from Inventory

You can upgrade the OLT software from the current version to the latest version.

You can either perform the complete ONL upgrade or only the OLT applications upgrade.

Use the ONL image for the complete ONL upgrade and the OLT BINS image for the OLT applications upgrade.

Note: Before you download the OLT software (ONL or OLT BINS), you must specify the OLT software version. For more information on the Creating Model Version Configuration, refer to the Creating Model Version Configuration in the *RMS User Guide*.

Prerequisites

- The user must upgrade the controller software first and then proceed with the OLT software upgrade. For more information, see Upgrading CBAC Software *(on page 99)*.
- If the upgrade is only for the OLT applications, ensure that the OLT is upgraded to R4.1.0 version before upgrading the OLT BINS image.
- Add the new R4.1.0 ONL version to the RMS model with ONL image HTTP location and md5sum.

The OLT software upgrade (ONL or OLT BINS) process involves the following steps.

- Download the OLT software
- Activate the OLT software
- Commit the OLT software
- Rollback the OLT software to previous version if there is any malfunction during the upgrade process

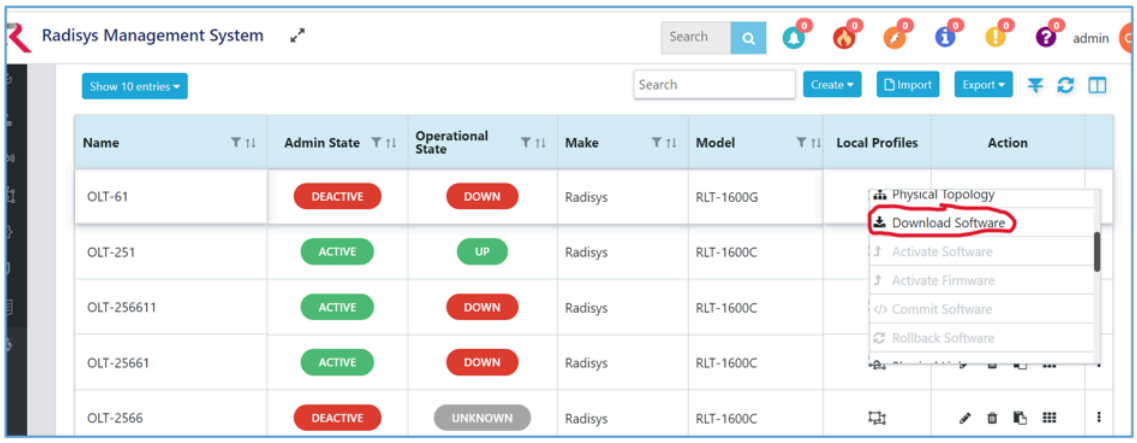
Perform the following steps to upgrade the OLT software (ONL or OLT BINS) immediately.

1. Select **Configuration > Inventory**.

   The Inventory List page appears.

2. Navigate to the **OLT** tab.
3. Click on the three dots corresponding to the OLT for which you want to upgrade the software.

Figure 46. OLT Software Upgrade



4. Click the **Download Software** option.

   The Download Software page appears.

5. Select the OLT software version that must be downloaded from the list.
6. Click **Download**.

   A confirmation message appears that the OLT software download is success.

   Note:

   - If the ONL download fails for some issues, the subsequent ONL download request resumes the ONL download from where it stopped.
   - By default, the options **Activate Software**, **Commit Software**, and **Rollback Software** are disabled, and these options are enabled only when the OLT download operation is success.

   After the OLT software download, RMS receives an ME-SOFTWARE-DOWNLOAD-SUCCESSFUL event.

7. Click the **Activate Software** option to activate the OLT software.

   After the OLT activate software, RMS receives an ME-SOFTWARE-ACTIVATION-SUCCESSFUL event.

8. Once the OLT activation is success, click the **Commit** Software option to commit the software.

   After the OLT commit software, RMS receives an ME-SOFTWARE-COMMIT-SUCCESSFUL event.

   A confirmation message appears that the OLT is upgraded with the new software.

If you want to schedule the OLT software update for a later date and time, you must create a task. For more information, see Upgrading OLT Software from Task *(on page 108)*.

Upgrading OLT Software from Task

When many OLTs are deployed in a network and a limited number of subscribers are connected to each OLT, physically accessing each OLT's software is not an efficient way to upgrade it.

RMS marks the status of the OLT software upgrade as COMPLETED when the upgrade request is initiated successfully for all the selected devices in the task.

OLT also has auto-recovery procedures in the event of an upgrade failure during activation. After three unsuccessful attempts, if the OLT does not come up with the new release, it automatically goes back to the previous release and notifies the upgrade failure as an alarm.

Note: Before you upgrade the software, you can verify the current version of the OLT software (ONL) from the **Monitor > Inventory > OLT** page.

Prerequisites

The following prerequisites must be fulfilled before creating task for OLT software upgrade.

- Create model version configuration. For more information on Creating Model Version Configuration, refer to the Creating Model Version Configuration in the *RMS User Guide*.
- The user must upgrade the controller software first and then proceed with the OLT software upgrade. For more information on the Creating Task for Controller Software Upgrade, see Upgrading CBAC Controller from Task *(on page 101)*.
- If the upgrade is only for the OLT applications, ensure that the OLT is upgraded to the R4.1.0 version before upgrading the OLT (ONL or OLT BINS) image.
- Create a site group, and the OLT must be part of the site group. For more information on Creating Site Group Configuration, refer to the Creating Site Group Configuration in the *RMS User Guide*.

Perform the following steps to create a task for the OLT software upgrade (ONL or OLT BINS).

1. Click **Configuration**from the top right corner of the page.
2. Select **Maintenance** from the left-hand side of the menu.
3. Click **Task**.

   The Task List page appears.

4. Click **Create**.

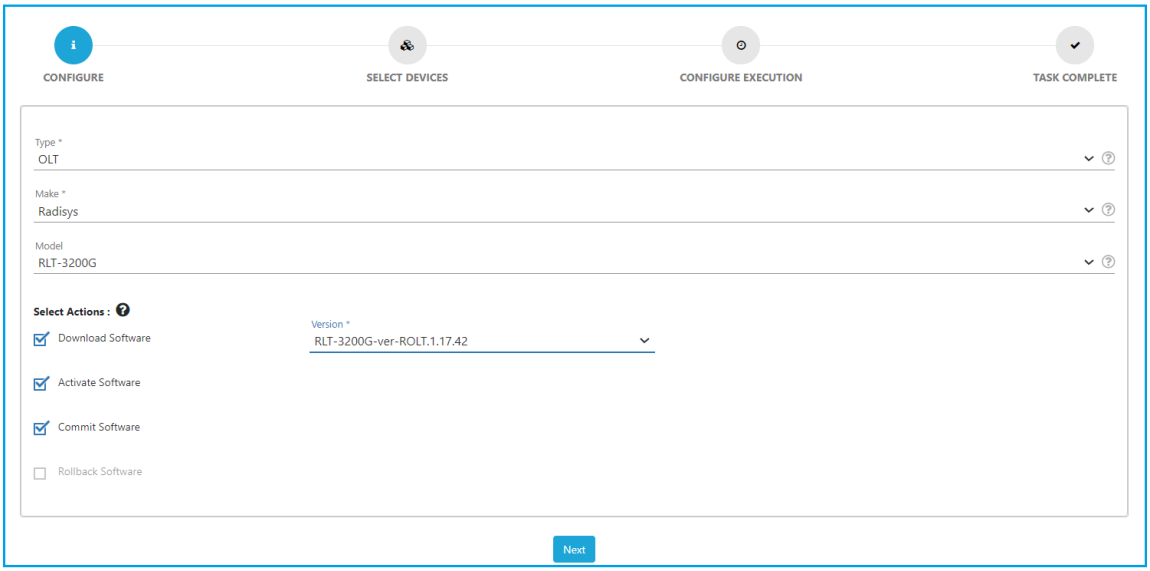
   The Task Configuration page appears.

Figure 47. OLT Upgrade Task

5. Complete the task configuration.
6. Click **Create**.

   The ME Software Upgrade page appears.

Figure 48. ME Software Upgrade



7. Complete the configuration.
8. Click **Next**.

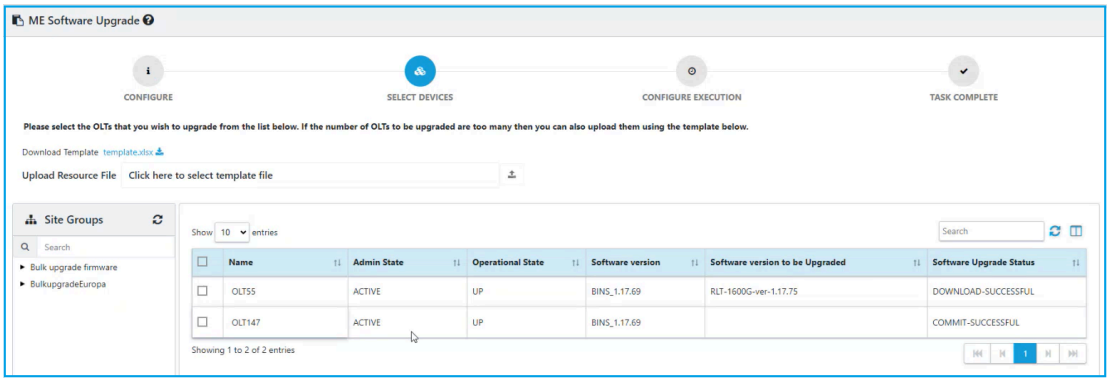
   The Select Device page appears.

OLT Bulk Upgrade

You can upgrade one or more OLTs using the following two methods.

- Template Upload (CSV file) - This method is used for the bulk upgrade of the OLT. Go to Step 7 *(on page 110)*.
- Selecting OLT on GUI - This method is used for the single or bulk upgrade of the OLT. Go to Step 8 *(on page 111)*.

Figure 49. OLT Device



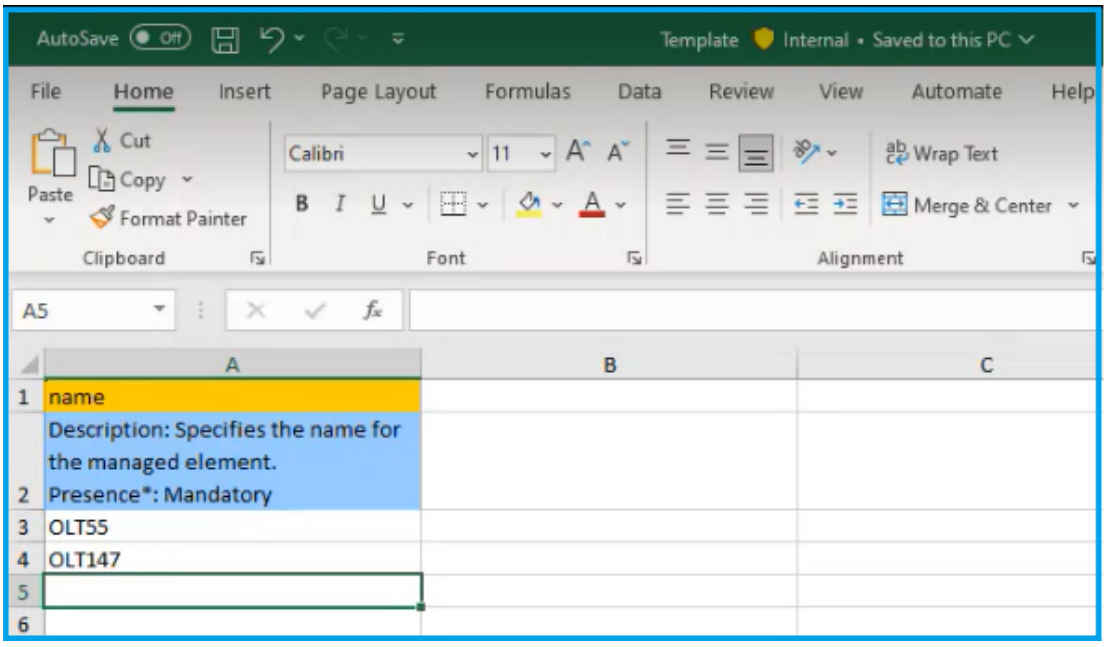
9. Perform the following steps to upgrade the OLT through template (CSV file).
   a. Click on the *template.xlsx* file to download the template.

> **Note:** Ensure that only same make or model OLTs must be a part of the CSV file.

   b. Enter the OLT name and save the downloaded template.

> **Note:** Do not remove or edit the yellow row and blue row in the template file.

Figure 50. Sample Template



c. Click on **Upload Resource File** and select the updated template. Continue with step 11 *(on page 112)* to upgrade the OLT software.

A confirmation message indicates that the upload is successful.

Figure 51. CSV File Upload

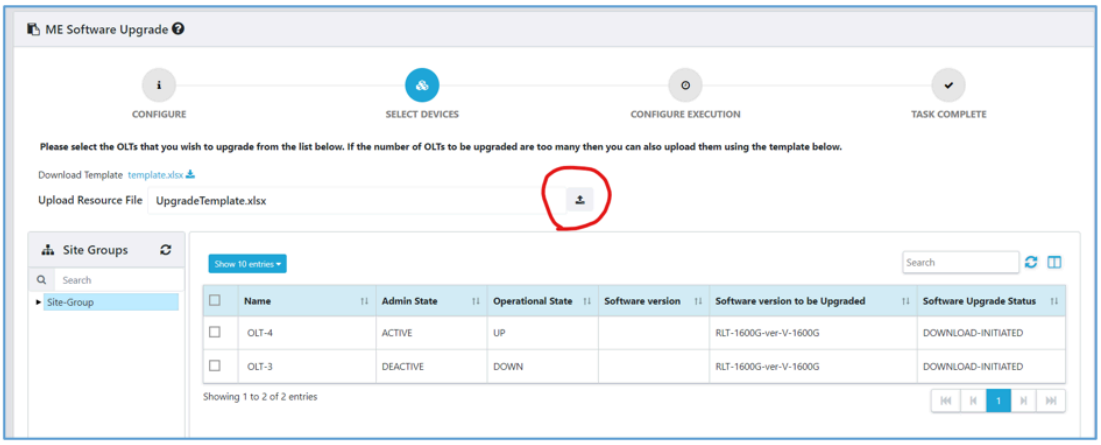
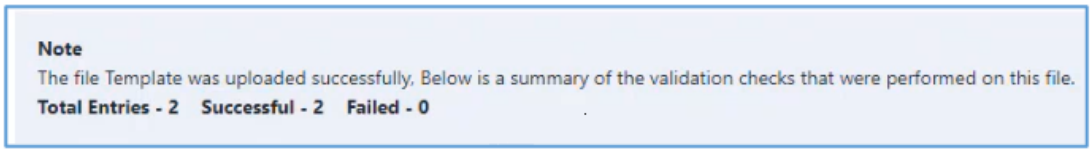


Figure 52. Upload Success



d. Click **Next** and skip to step 12 *(on page 112)* to upgrade the OLT software.

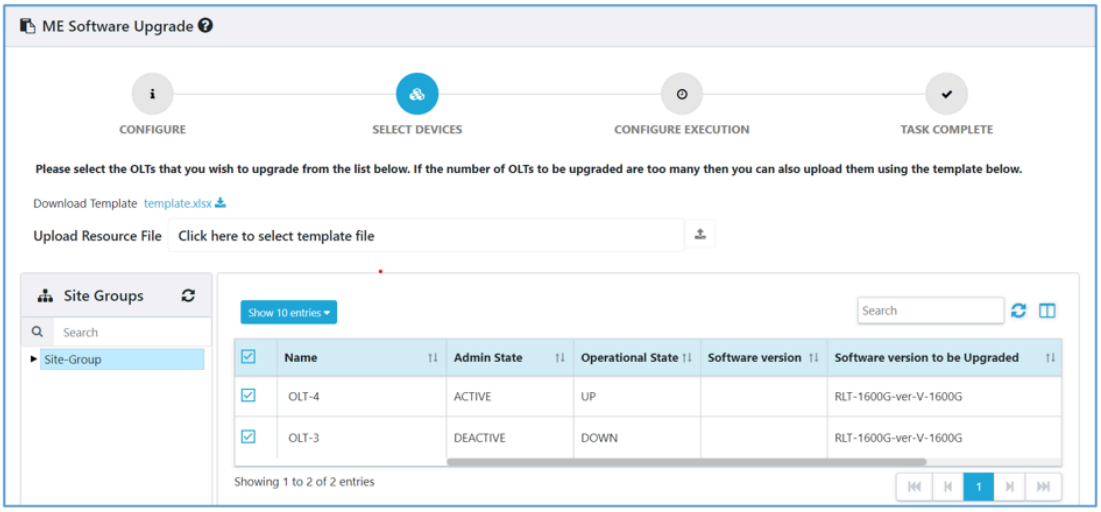
The CONFIGURE EXECUTION page appears.

10. Perform the following steps to upgrade the OLT through OLT selection on RMS GUI.

Note: Skip this step and see step 9 *(on page 110)* to upgrade the OLT through template (CSV file).

a. Select the checkbox for the applicable OLT/OLTs. Continue with step 11 *(on page 112)* to upgrade the OLT software.

Figure 53. OLT Selection

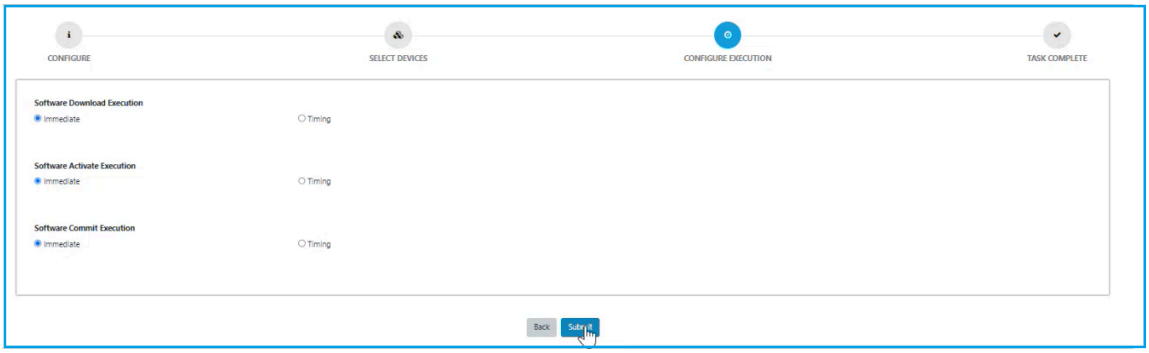


11. Click **Next**.

    The CONFIGURE EXECUTION page appears.

12. Complete the configuration.

Figure 54. ME Configure Execution



13. Click **Submit**.

    A confirmation message appears, indicating that the task request is created successfully and you are taken to the Task List page.

    - Click three dots on the corresponding task and then click **Monitor** or navigate to **Monitor > Task** page to view the status of the task. For more information on monitor section, refer to the OLT Software Upgrade section under Tasks in the *RMS User Guide*.

Upgrading OLT Firmware

The following section describes the upgrade procedure of the OLT firmware components (BIOS, CPLD, and FPGA) over the IP network.

- The firmware updates automatically with ONL updates, and the following step is not required. However, if the firmware has to be upgraded before connecting OLT to RMS, see Firmware Upgrade Procedure *(on page 113)*.
- The firmware upgrade bundle is provided as a Linux self-extractable installer and is packaged in the ONL image as */sbin/sdpon-firmware-install*.
- The ONL installer image is bundled with all the upgrade tools and the firmware files required to perform the firmware upgrade procedure.
- Trigger the firmware upgrade self-extractable binary from the SSH session over IP (on management port ma1 or in-band port eno1) or through the serial console interface.

Note: The complete upgrade takes approximately 8 to 10 minutes to complete.

How OLT Firmware Upgrade Works

The following steps describe how the OLT firmware upgrade works.

1. For each firmware component (BIOS, FPGA, and CPLD), the component version in the OLT and the component version in the upgrade bundle are compared.
2. The specific component upgrade is skipped if the component versions are the same.
3. If any of the components (BIOS, FPGA, and CPLD) versions are different, then an upgrade is performed for that specific component.

   Note: Ensure that you upgrade the BIOS first and then CPLD without manual reboots. If the BIOS is already upgraded, you can skip the upgrade and only upgrade the CPLD.

4. After an upgrade, the system reboots automatically.

   Note: Firmware upgrade logs are available in the `/var/log/sdpon-upgrade-firmware.log` file.

Firmware Upgrade Procedure

The following section describes the firmware upgrade procedure.

Note: While the upgrade procedure is in progress, do not disrupt or reboot the OLT. Ensure you have an uninterrupted power supply to the OLT.

Upgrading OLT Firmware from ONL

Perform the following steps for firmware upgrade.

1. Login to the OLT over the IP network.
2. Execute the following command to check the current firmware installed on the OLT and the firmware versions packaged into the ONL. This step is optional, and the user can skip this.

Figure 55. Upgrading from ONL

```
oltausr@localhost:~$  sudo /sbin/sdpon-firmware-install --version

Platform        : x86-64-radisys-phoenix-r0
Build Date      : 30/01/24

 Component      Current Version     Upgrade Bundle Version
------------------------------------------------------------
 BIOS               1.0.11              1.0.11
 MB FPGA            20110520            20110520
 DB FPGA            20110520            20110520
 CPLD               66                  66
 SSDFW              S23A25T             S23A25T
```

3. Execute the following command to trigger the firmware components installation.

```
oltausr@localhost:~$ sudo sdpon-firmware-install
```

4. The firmware upgrade procedure begins, and the system automatically reboots at the end of the upgrade operation. Once the system is up and running, execute the following command to retrieve the firmware versions and status of the upgrade operation.

```
oltausr@localhost:~$ cat /mnt/onl/config/sdpon-upgrade-firmware.cfg
ROOT= /dev/sda7
STATE= ACTIVATION_COMPLETE
PACKAGE= /mnt/onl/images/firmware/ SDPON-EU-FW_BIOS-1.0.01_CPLD-0c_FPGA-
21052713
BIOS= PASS
BIOS_VERSION= 21052713
FPGA= PASS
FPGA_VERSION= 21052713
CPLD= PASS
CPLD_VERSION= 0c
```

Note: Power cycle the board manually if the board does not boot for any reason after the upgrade.

Manually Downgrading Support on CBAC-D

This section covers the procedure to downgrade CBAC-D from version "n+1" to "n" using the Backup and Restore mechanism. If post upgrade the OLT goes down due to some hardware or some unforeseen issues, follow the below mentioned procedure.

Prerequisites

Perform the following steps before the CBAC-D downgrade.

1. The user must take an CBAC backup of the OLT on an existing version “n+1” before initiating an upgrade to version “n”. For more information on CBAC backup, refer to the *Backup Controller Configuration* section in the *RMS User Guide*.
2. Ensure the CBAC backup file has been copied to the SFTP server.

   Take a snapshot or output of the following files on OLT, as they need to be updated in case of a downgrade.

   a. `cat /etc/network/interface`
   b. `cat /broadcom/olt_config`

3. Check for the following parameters to ensure that the software upgrade status is not in a progress state while creating the CBAC backup file.
   a. Unzip the CBAC backup config zip file.
   b. The zip file contains a JSON file with the CBAC database backup data.
   c. Check for the key path in the file `/devices/Olts/v1/<olt-NB-ID>`.

      The olt-NB-ID is the OLT resource ID as displayed in RMS-GUI.

   d. Check the olt-NB-ID status for the parameter *“OperInProgress”*. If the status shows *“SWUpgrading”*, contact the product development team for further assistance before proceeding with the next steps.

Downgrading OLT Manually

Perform the following steps to downgrade the OLT from version “n+1” to version “n”.

1. Install ONL and CBAC version “n”. For more information on installation of ONL and CBAC, see Installing ONL and CBAC using USB Device *(on page 16)*.
2. Navigate to **Monitor > Inventory > Controller** page in the RMS GUI.

Note: For the applicable controller, the admin state must be ACTIVE, and the Operational state, Rest, and Kafka must be UP.

3. Perform the following steps from RMS to replace the OLT.
   a. Navigate to **Configuration > Controller**.
   b. Select the controller associated with the OLT, click on the three dots icon, and click **Replace** to synchronize the user credentials.
   c. Restore the SDPON database. For more information on restoring the SDPON database, refer to the Restore Controller Configuration section in the *RMS User Guide*.

      Note: Enter the absolute path of the backup file during the restore operation and wait for 10 minutes to allow OLT to reboot and replay the database.

   d. Trigger reconciliation from RMS to sync pending configurations, resolve conflicts, and delete orphan resources. For more information on reconciliation, refer to the Reconciliation section in the *RMS User Guide*.
   e. Perform alarm purge and fetch operations. For more information on these operations, refer to the *Purge and Fetch* section in the *RMS User Guide*.

Firewall Port Requirements

The following port access is required for communication between the mentioned components.

Table 6. Port Activity–ROLT to /from Repository Server

Port	Protocol	Service	Notes
80	TCP	HTTP	1. Download CBAC packages from the repository server. 2. Download ONL packages from the repository server.
5000	TCP	HTTPS	Download CBAC docker images from the repository server.
22	TCP	SFTP	Download ONL from the repository server.
3000	TCP	HTTP	Notification for new CBAC package availability in repository server.
443	TCP	HTTPS	Download the artifacts from the repo to OLTs securely.

Table 7. Port Activity–ROLT to /from NTP Server

Port	Protocol	Service	Notes
123	UDP	NTP	Time synchronization.

Table 8. Port Activity–ROLT to /from System log Server

Port	Protocol	Service	Notes
514	TCP	Syslog	R-OLT and CBAC logs are uploading to the system log server.

Table 9. Port Activity–ROLT to /from SEIM Tool

Port	Protocol	Service	Notes
514	UDP	Syslog	Security/Audit log synchronization.

Converting NNI Ports to LAG Ports in Live Deployment

This section covers the procedures to convert the NNI port to LAG port in the OLT live deployment.

OLTs are deployed in live networks based on the bandwidth requirements. Sometimes, there is a need to convert a single NNI port to a LAG port, and in some scenarios, the LAG port is required for redundancy, especially between the main and subtended OLT.

In some scenarios, where the microwave link is used between the OLT and BNG, and the dynamic LAG is required for redundancy to handle the link failure.

The following prerequisites must be fulfilled to ensure all the above scenarios are configurable fields of live OLTs.

1. OLT must be reachable (in band connection available)
2. OLTs must be running on residential or enterprise traffic (ERPS and so on)
3. Service impact must be avoided or at least reduced to the maximum extent

This section covers the following procedures to convert the NNI ports to LAG ports in the OLT live deployment.

- Example: Converting OLT Ring Ports from NNI to Static LAG - Enterprise *(on page 118)*
- Example: Converting OLT Ring Ports from NNI to Static LAG - Residential *(on page 137)*
- Example: Converting Subtended OLT Connection from NNI to LAG - Enterprise *(on page 148)*
- Example: Converting Subtended OLT Connection from NNI to LAG - Residential *(on page 160)*
- Example: Subtended OLT (Fresh Install) to Parent OLT with LAG *(on page 173)*
- Example: Connecting OLT Ring Ports with Eband Device Using Dynamic LAG - Enterprise *(on page 180)*
- Example: Connecting OLT Ring Ports with Eband Device Using Dynamic LAG - Residential *(on page 196)*
- Example: Converting Two Port Dynamic LAG to Single Port Static LAG - Enterprise *(on page 207)*
- Example: Converting Two Port Dynamic LAG to Single Port Static LAG - Residential *(on page 221)*

Example: Converting OLT Ring Ports from NNI to Static LAG - Enterprise

Overview

This section covers the procedure to convert the OLT ring ports from the NNI port to static LAG port for enterprise customers using the RMS GUI.

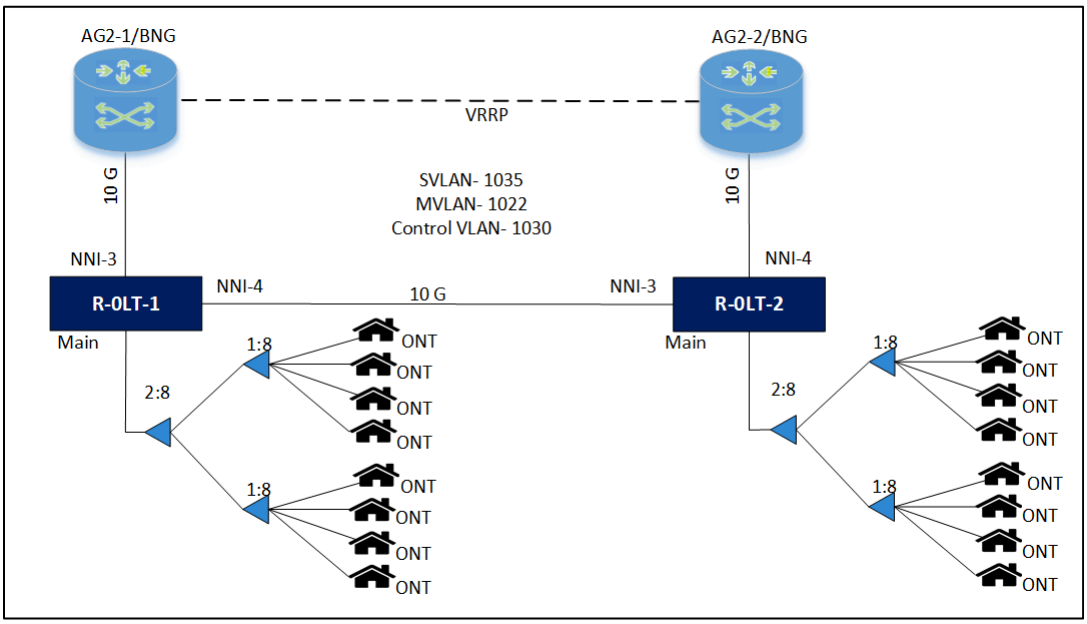
Topology 1

The following topology diagram shows the configurations and connections between main OLTs.

- **R-OLT-1** is **MAIN/Parent** OLT and part of the ring
- **R-OLT-2** is part of the ring

Note: It is assumed that all the OLTs are upgraded from R2.9.3/older version to R2.10.2/latest version. Ensure that the in-band port (port mentioned in the `olt_config` file) is UP and receives the traffic.

Figure 56. Topology



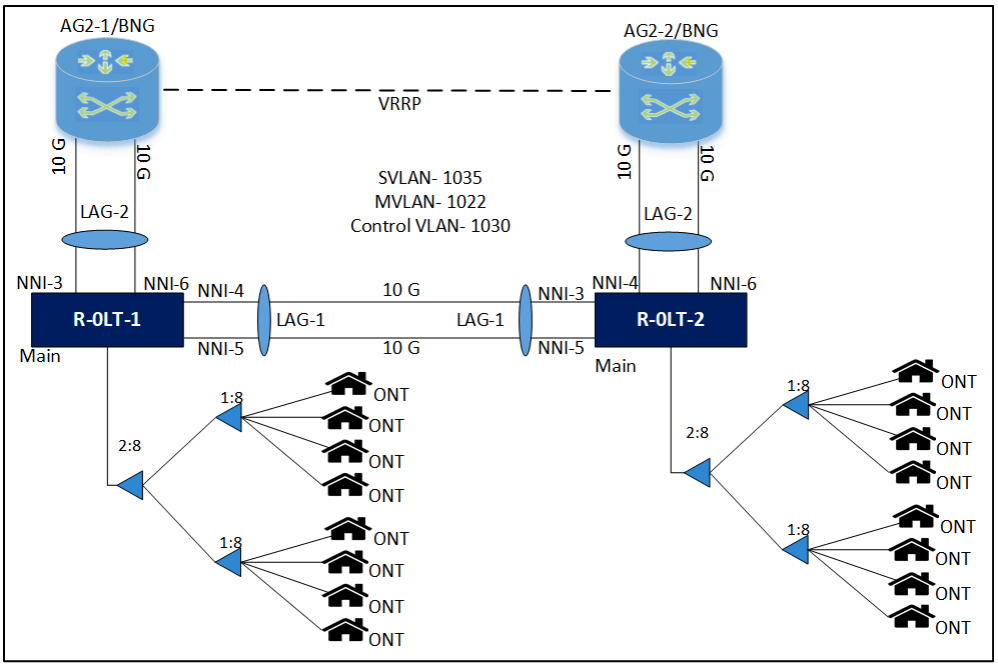
Following ELANs are used as part of the topology.

- Control VLAN **(ELAN1030)**
- Data VLAN **(ELAN1035)**
- Multicast VLAN **(ELAN1022)**

Topology 2

The following diagram shows the topology for converting the OLT ring ports from the NNI port to static LAG port.

Figure 57. Topology - OLT Ring Port (NNI to Static LAG)



R-OLT-1 Configuration

Perform the following steps to apply the force switch on the NNI-3 port for R-OLT-1.

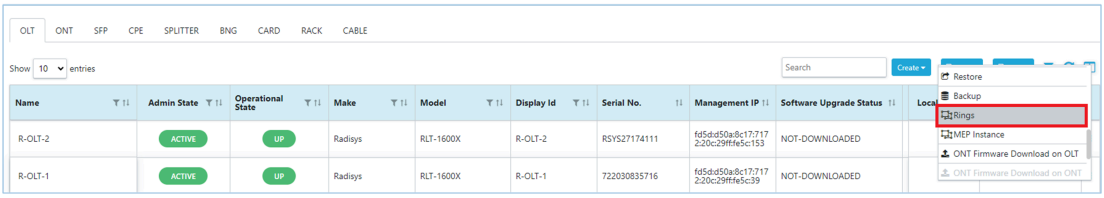
1. Apply the force switch on the NNI-3 port.
   a. Navigate to **Configuration > Inventory > OLT**.

      The OLT page appears.

   b. Click on the three dots and click the **Rings** option.

      The Rings page appears.

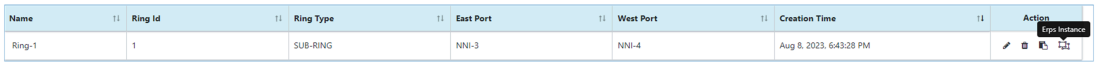
      Figure 58. Rings



   c. Click on **ERPS Instance** under the **Action** column.

      The ERPS instance page appears.

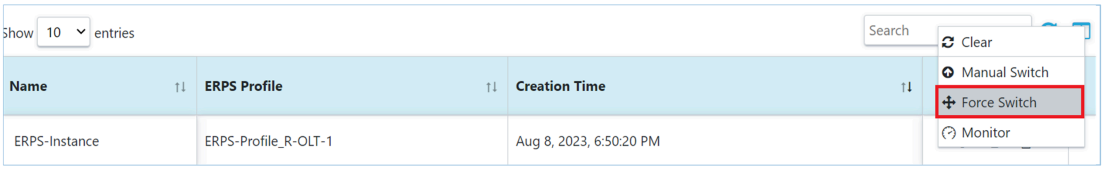
      Figure 59. ERPS Instance



   d. Click on the three dots corresponding to the ERPS Instance on which you want to apply the force switch and click **Force Switch**.

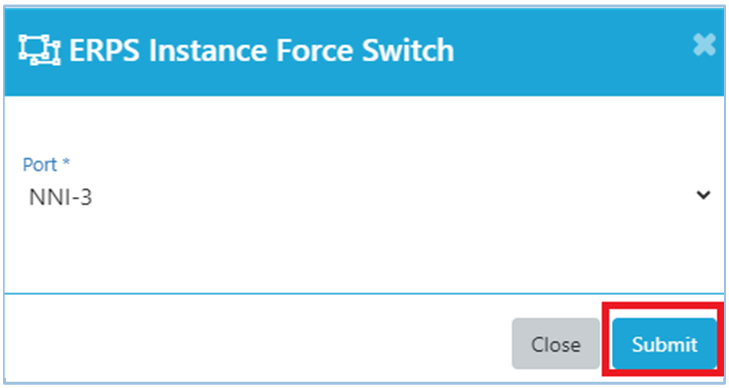
The ERPS Instance Force Switch window appears.

Figure 60. Force Switch



e. Select the Port NNI-3 from list and click **Submit**.

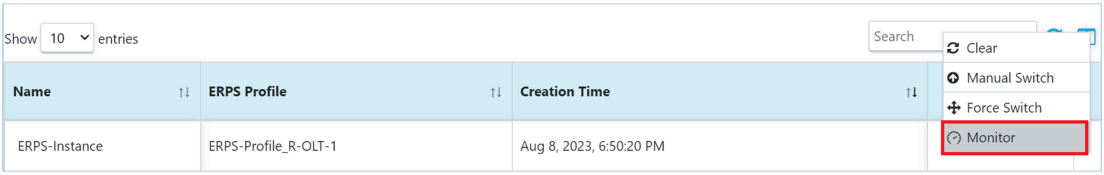
Figure 61. ERPS Instance Force Switch



Perform the following steps to check if both the OLTs are moved to the FORCE SWITCH state.

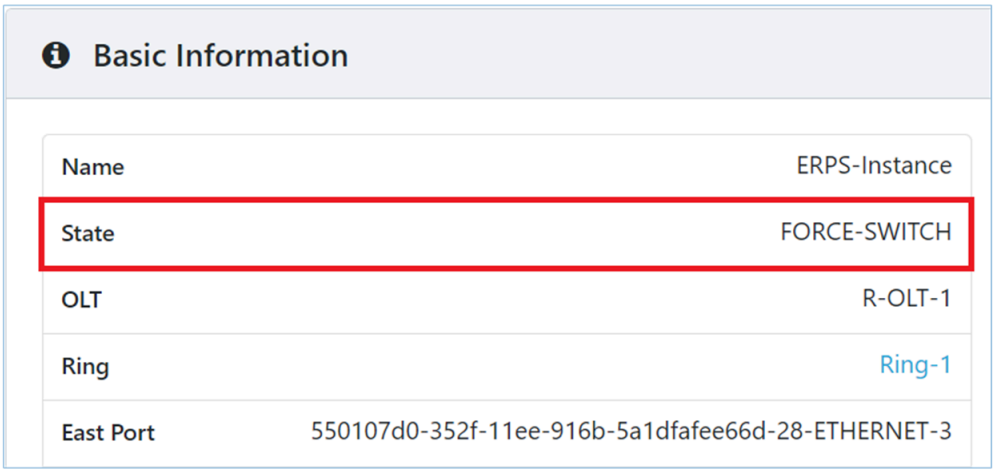
f. In the **ERPS Instance** page, click on three dots and click **Monitor** corresponding to the ERPS Instance on which you want to check the ERPS instance state.

Figure 62. OLT Monitor



g. In the Monitor page, under Basic Information, check for the state, which should reflect as FORCE-SWITCH.

Figure 63. Basic Information



Note: Check the same on R-OLT-2 if the state moved to FORCE-SWITCH.

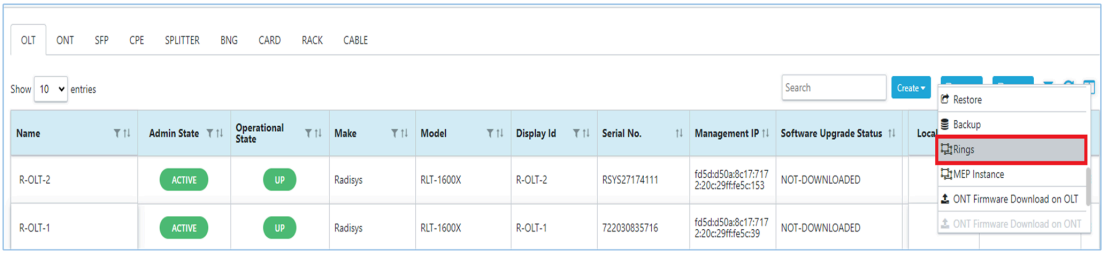
2. Delete the ERPS instance.
   a. Navigate to **Configuration > Inventory > OLT**.

      The OLT page appears.

   b. Click on three dots and click **Rings**.

      The Rings page appears.

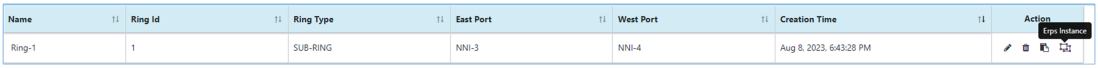
Figure 64. Rings



   c. Click on the **ERPS Instance** icon from the **Action** column.

      The ERPS Instance page appears.

Figure 65. ERPS Instance



   d. Click the delete icon from the **Action** column.

      An alert message appears, asking you to confirm the delete operation.

Figure 66. Delete ERPS Instance

e. Click **Confirm** to delete the ERPS instance.

A confirmation message appears, indicating the status of the delete operation.

3. Delete the MEP instance.

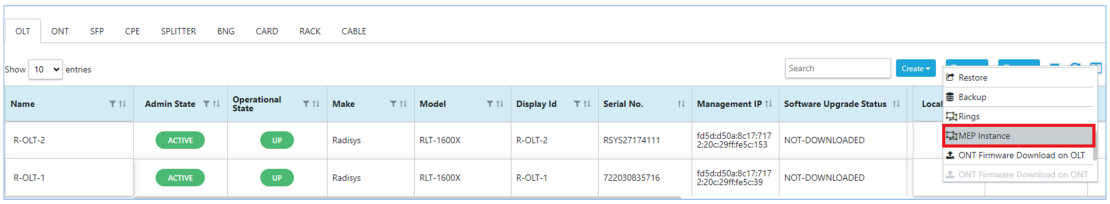
a. Navigate to **Configuration > Inventory > OLT**.

The OLT page appears.

b. Click on three dots and click **MEP Instance**.

The MEP Instance list page appears.

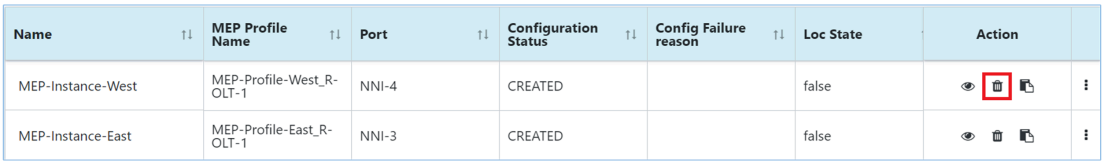
Figure 67. MEP Instance



c. Click the delete icon from the **Action** column.

An alert message appears, asking you to confirm the delete operation.

Figure 68. Delete MEP Instance



d. Click **Confirm** to delete the MEP instance.

A confirmation message appears, indicating the status of the delete operation.

4. Disable and delete the existing ELANs (ELAN1030, ELAN1035, and ELAN1022).

Note: You must disable the ELANs before you delete them.

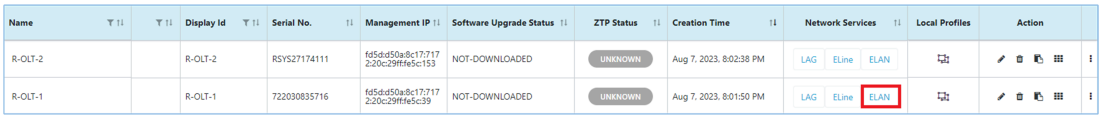
a. Navigate to **Configuration > Inventory > OLT**.

The OLT page appears.

b. Click ELAN from the **Network Services** column.

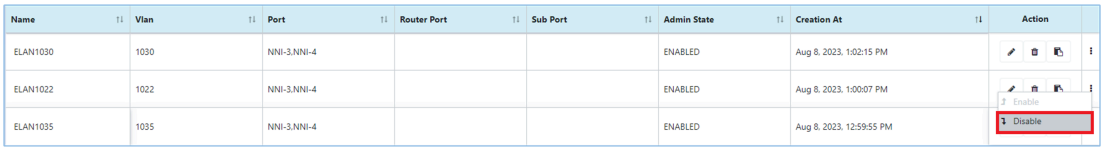
The ELAN list page appears.

Figure 69. ELAN



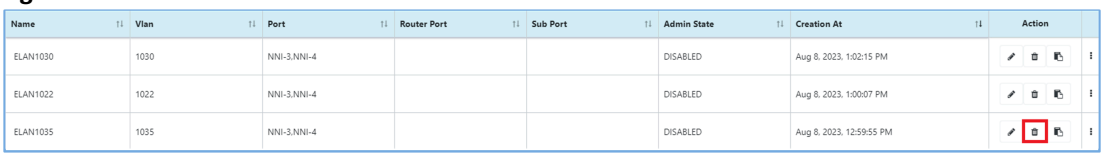
c. Click on three dots and select the **Disable** option to disable the ELAN1035. Repeat the steps to disable the ELAN1030 and ELAN1022.

Figure 70. Disable ELAN1035



d. Click on three dots and select the **Delete** icon to delete ELAN1035. Repeat the steps to delete the ELAN1030 and ELAN1022.

Figure 71. Delete ELAN1035



5. Delete the ring.

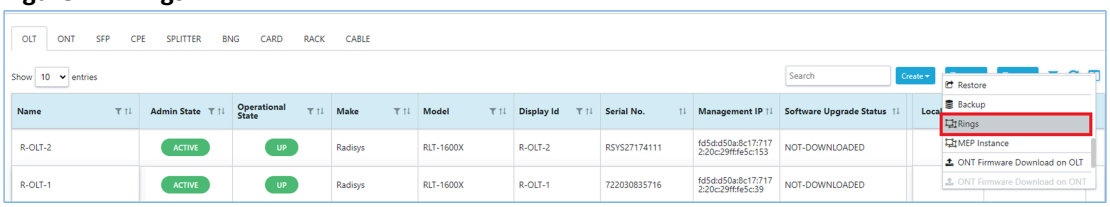
a. Navigate to **Configuration > Inventory > OLT**.

The OLT page appears.

b. Click on three dots and click the **Rings** option.

The Rings page appears.

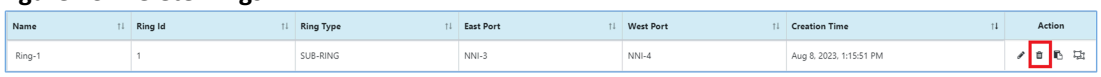
Figure 72. Rings



c. Click the delete icon from the **Action** column.

An alert message appears, asking you to confirm the delete operation.

Figure 73. Delete Rings

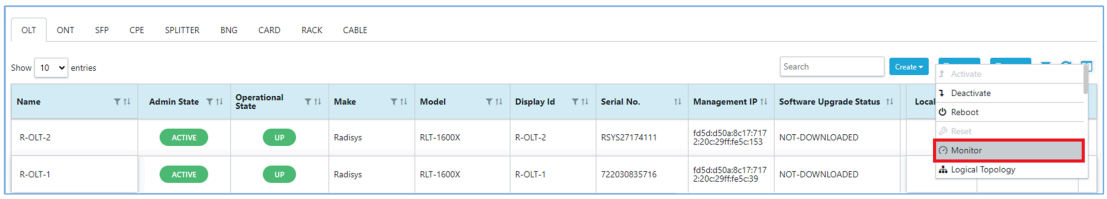


d. Click **Confirm** to delete the ring.

A confirmation message appears, indicating the status of the delete operation.

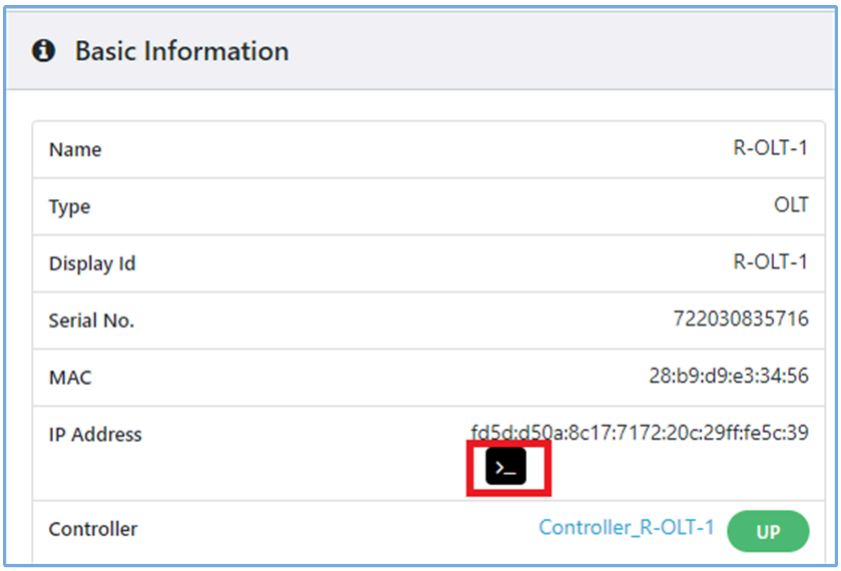
6. Log in to the OLT terminal and remove the *olt_hidden_config* json file.
   a. Navigate to **Configuration > Inventory > OLT**.
   b. Click on three dots and select **Monitor**.

Figure 74. OLT Monitor



   c. Under the **Basic Information**, click on the terminal in the IP Address.

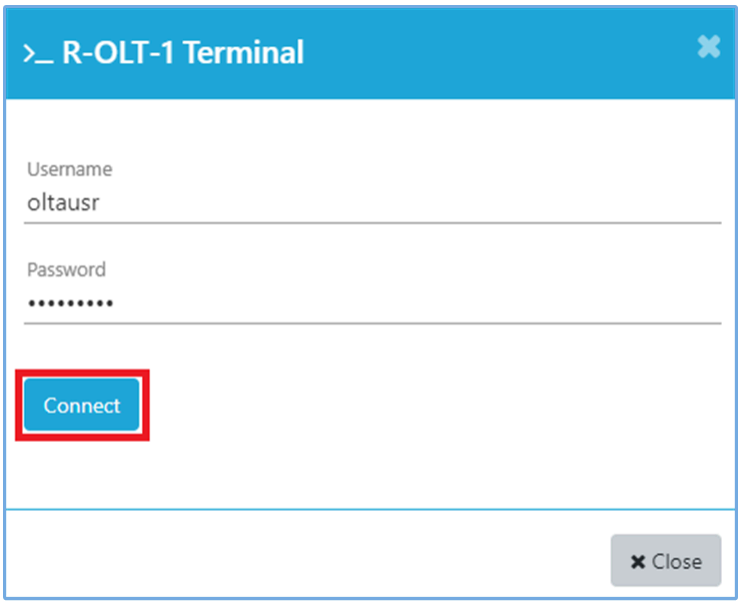
Figure 75. OLT Basic Information



   d. Enter the username and password for the OLT.
   e. Click **Connect**.

   The OLT Terminal page appears.

Figure 76. Connect R-OLT-1 Terminal



f. Execute the following command to remove the `olt_hidden_config` json file.

```
sudo rm -rf /mnt/onl/sdpon/oltfiles/olt_hidden_config.json
```

Figure 77. Remove JSON File

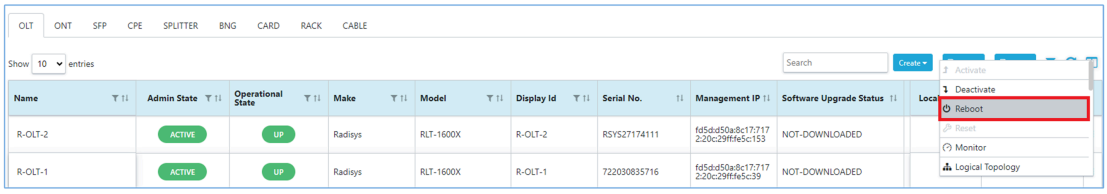
```
oltausr@localhost:~$ sudo rm -rf /mnt/onl/sdpon/oltfiles/olt_hidden_config.json
```

7. Reboot the OLT.

a. Navigate to **Configuration > Inventory > OLT**.

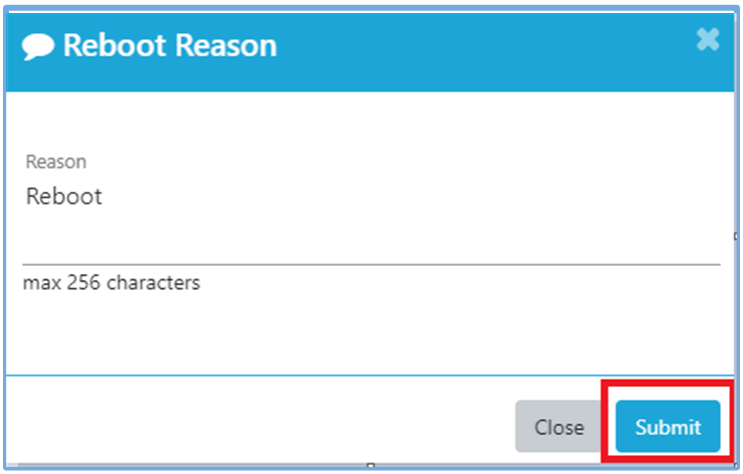
b. Click on three dots and select the **Reboot** option.

Figure 78. Reboot OLT



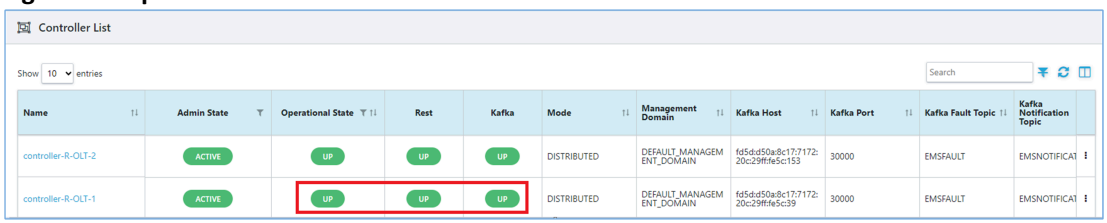
c. Enter the reason for the OLT reboot and click **Submit**.

Figure 79. OLT Reboot Reason



8. Check if the OLT is UP.
   a. Check if the "ME-REBOOTED" event is raised in the **Monitor > Events** page.
   b. Once the "ME-REBOOTED" event is raised, go to **Monitor > Inventory > Controller** and check if the Operational State of Rest and Kafka is UP.

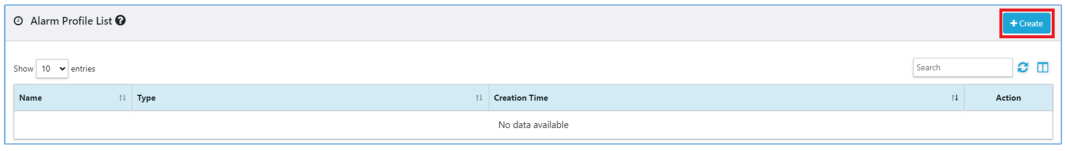
Figure 80. Operational State of Rest and Kafka are UP



9. Create LAGs and add the member ports to LAGs.
   a. Create a LAG alarm profile.
      i. Navigate to **Configuration > Profile > Alarm Profile**.
      ii. Click **Create**.

      The Alarm Profile Configuration page appears.

Figure 81. Create Alarm Profile

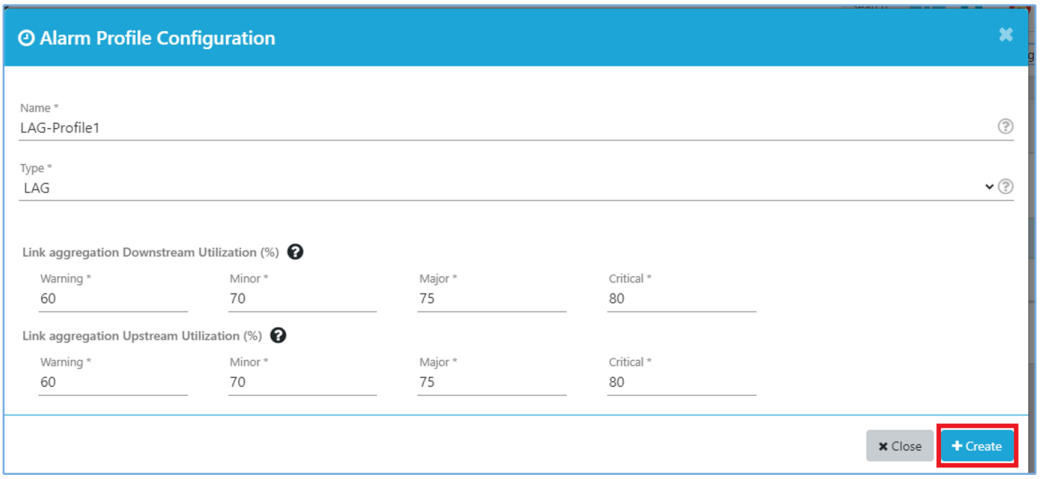


      iii. Enter the alarm profile configuration and click **Create**.

Note:

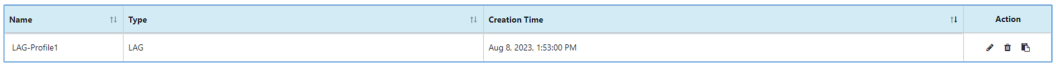
- The space as delimiter is not accepted in RMS for the profile names.
- Change the utilization values for downstream and upstream from the default to the required value (The minimum and maximum values are set to 60).

Figure 82. Alarm Profile Configuration



The following screenshot shows the status of the alarm profile created for LAG.

Figure 83. Alarm Profile Status

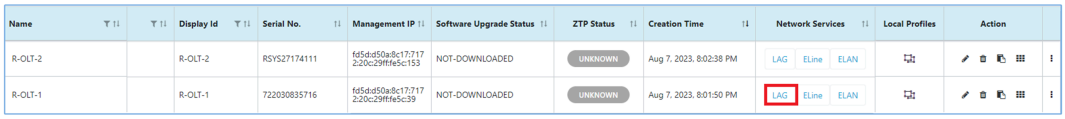


Perform the following steps to create LAG-1.

i. Navigate to **Configuration > Inventory > OLT**.

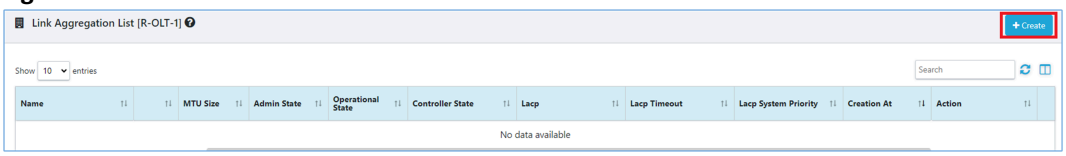
ii. Click on the LAG from the **Network Services** column.

Figure 84. LAG



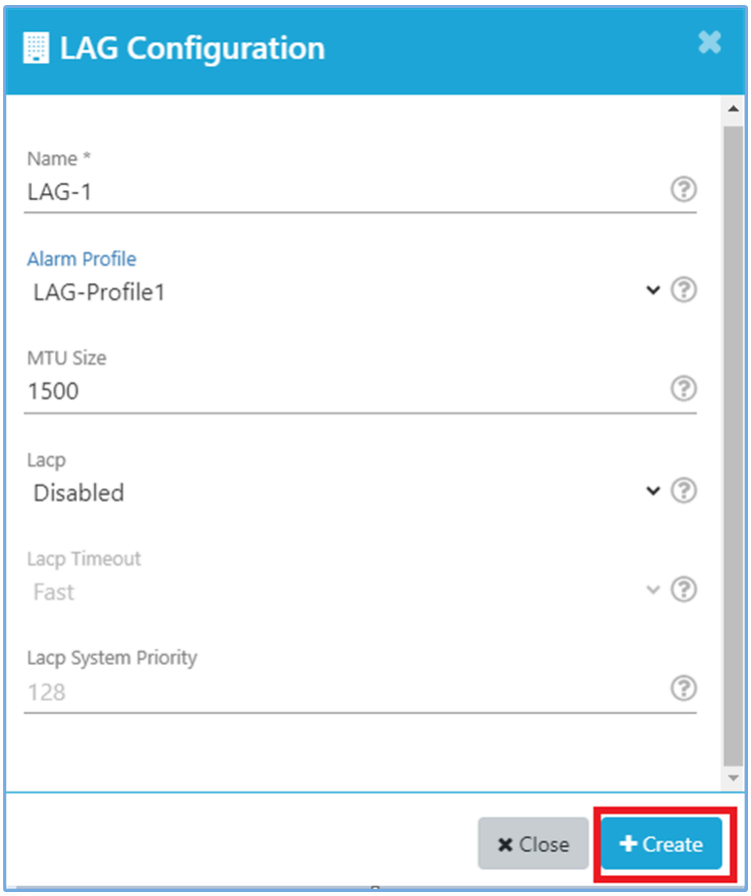
iii. Click **Create**.

Figure 85. Create LAG



iv. Enter the LAG configuration and click **Create**.

Figure 86. LAG Configuration



v. A LAG is created and the administrative state shows as ACTIVE.

Figure 87. LAG Status

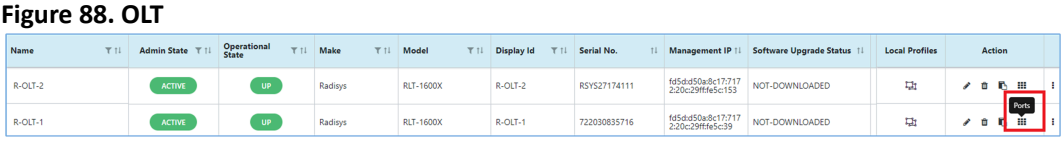
Perform the following steps to associate the NNI-4 and NNI-5 ports to the LAG-1.

Note: When configured, the LAG configuration must only have one active member port. In this scenario, NNI-4 is active and up while NNI-5 is down, and NNI-5 may be active and brought up once the LAG configuration is finished, preventing packet looping.

i. Navigate to **Configuration > Inventory > OLT**.

ii. Click on nine dots.

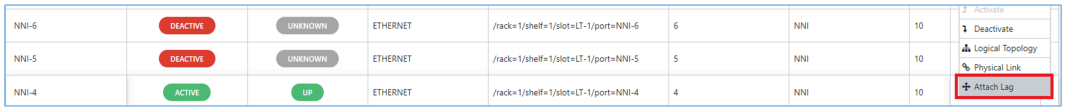
Figure 88. OLT



iii. Navigate to the **NNI-4** Port.

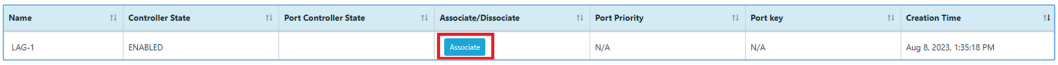
iv. Click on three dots and select the **Attach Lag** option.

Figure 89. Attach LAG



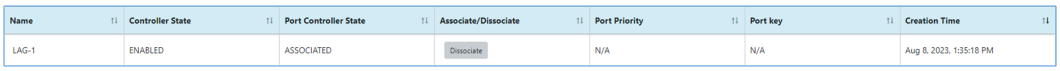
v. Click the **Associate** option from the Associate/Dissociate column.

Figure 90. Associate LAG



The NNI-4 port is associated to LAG-1 and a confirmation message appears, indicating the status of the associate operation. Repeat the steps to associate the NNI-5 port with LAG-1.

Figure 91. Status of the LAG-1



vi. Repeat the same steps to create the LAG-2 and associate NNI-3 and NNI-6 port to the LAG-2.

10. Create a ring with LAGs.

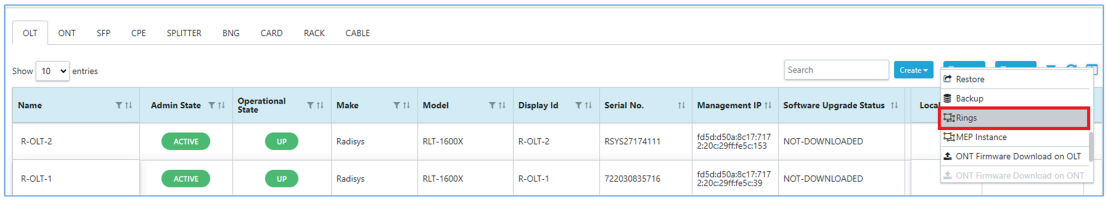
a. Create a Ring with LAG-1 as west port and LAG-2 as east port.

b. Navigate to **Configuration > Inventory > OLT**.

c. Click on three dots and click the **Rings** option.

The Rings page appears.

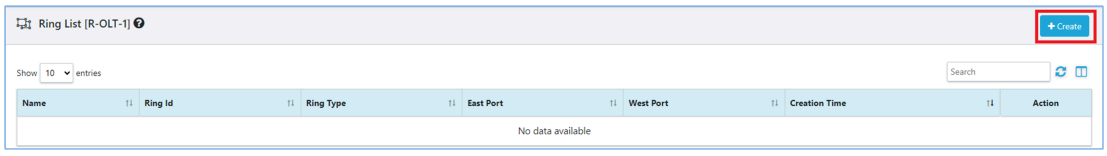
Figure 92. Rings



d. Click **Create**.

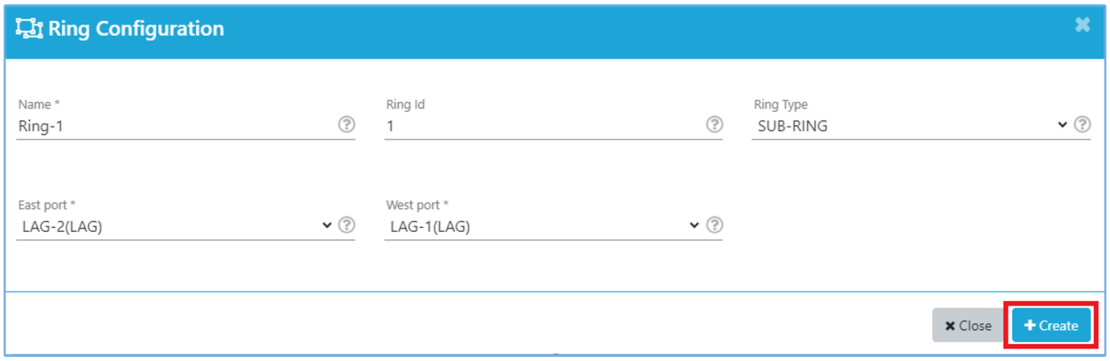
The Ring Configuration page appears.

Figure 93. Create Ring



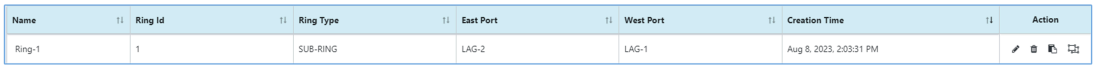
e. Enter the ring configuration and click **Create**.

Figure 94. Ring Configuration



A confirmation message appears indicating the status of the ring.

Figure 95. Status of the Ring



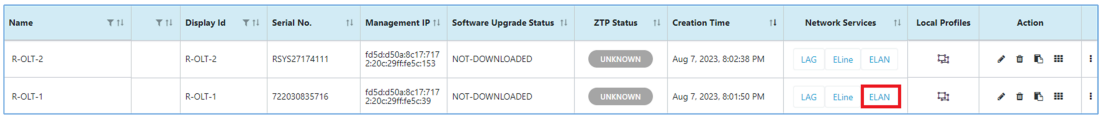
11. Create and enable ELANs with the LAGs

    a. Create an ELAN1035 with port list as LAG-1 and LAG-2 and enable the ELAN1035.

    b. Navigate to **Configuration > Inventory > OLT**.

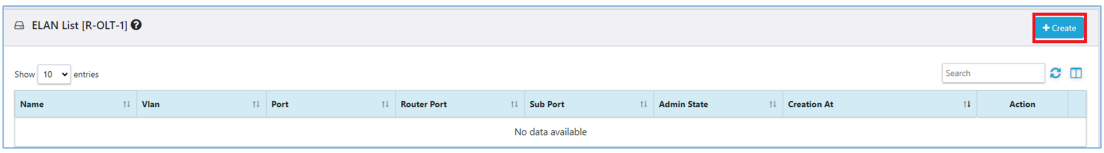
    c. Click on the ELAN from the **Network Services** column.

Figure 96. ELAN



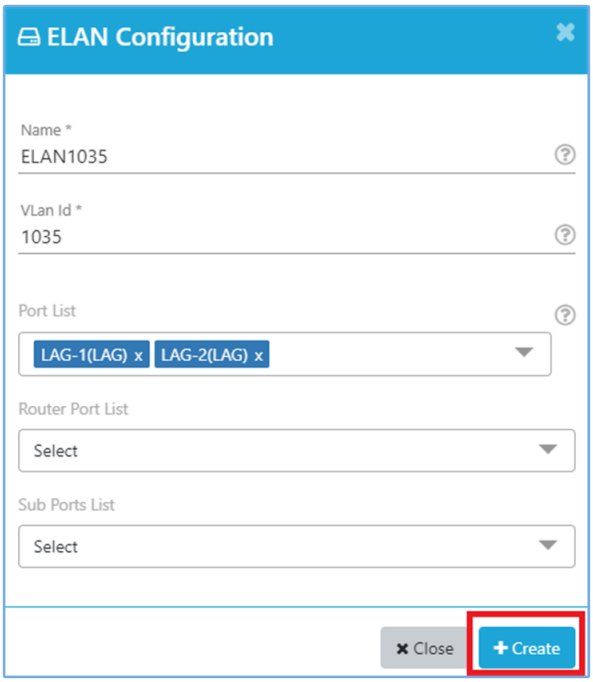
    d. Click **Create**.

Figure 97. Create ELAN



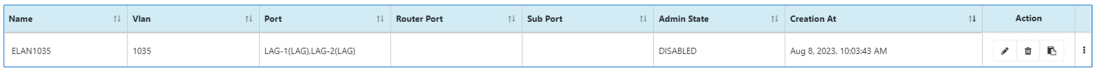
    e. Enter the ELAN configuration and click **Create**.

Figure 98. ELAN Configuration



The following screenshot shows the status of the ELAN1035.

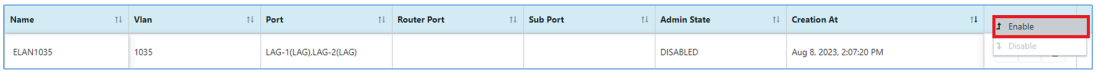
Figure 99. Status of the ELAN1035



Note: The ELAN1035 is in the Disable state.

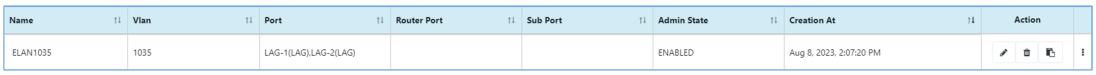
f. Click on three dots and select **Enable** option to enable the ELAN1035.

Figure 100. Enable ELAN1035



The following screenshot shows the status of the ELAN1035.

Figure 101. Status of the ELAN1035



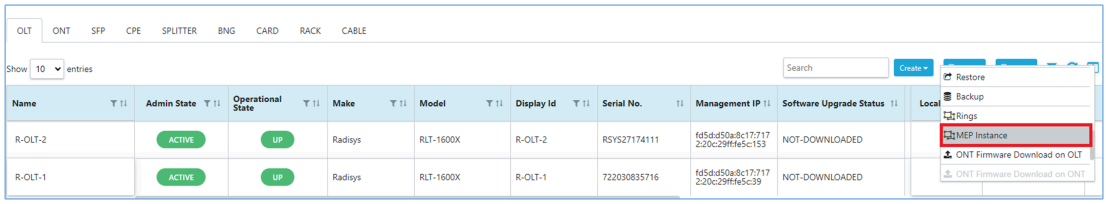
g. Repeat the same steps to create and enable the ELAN1022 and ELAN1030 with port list as LAG-1 and LAG-2.

12. Create the MEP instance.

a. Navigate to **Configuration > Inventory > OLT**.

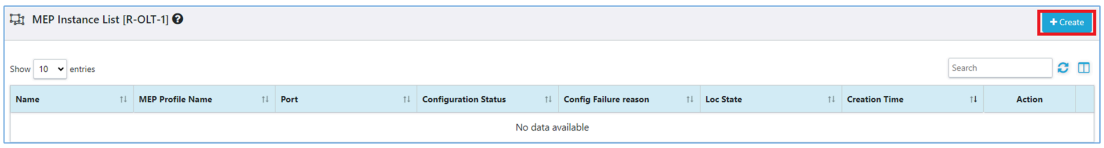
b. Click on three dots and select the **MEP Instance**.

Figure 102. MEP Instance



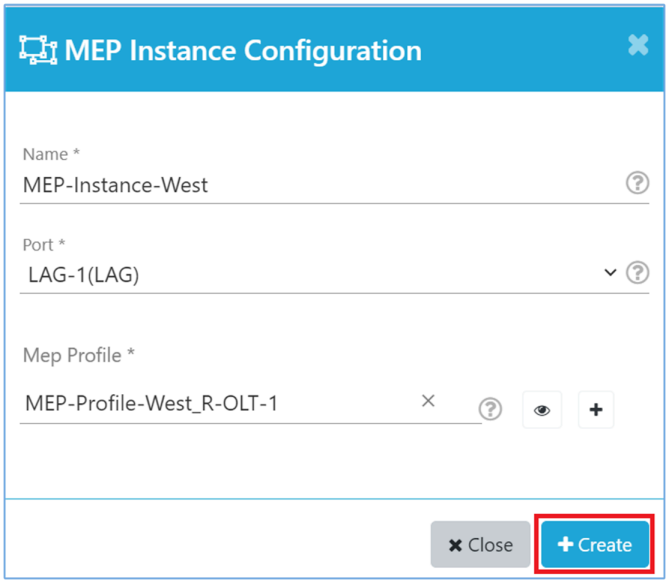
c. Click **Create**.

Figure 103. Create MEP Instance



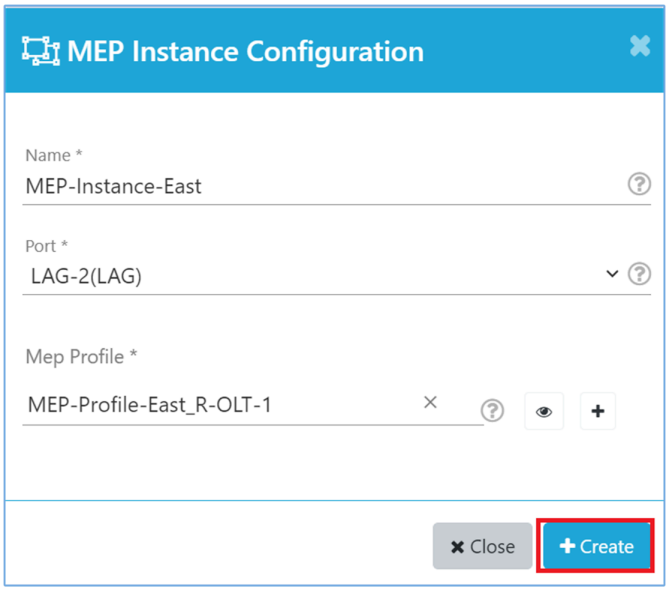
d. Enter the MEP instance configuration (use the previously used MEP Profile) and click **Create**.

Figure 104. MEP Instance Configuration - West



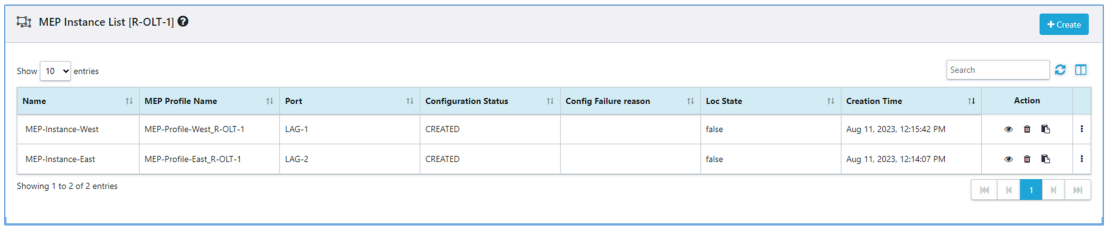
e. Repeat the same steps to create an another MEP instance configuration.

Figure 105. MEP Instance Configuration - East



The following screenshot shows the status of the MEP instances.

Figure 106. Status of the MEP Instances

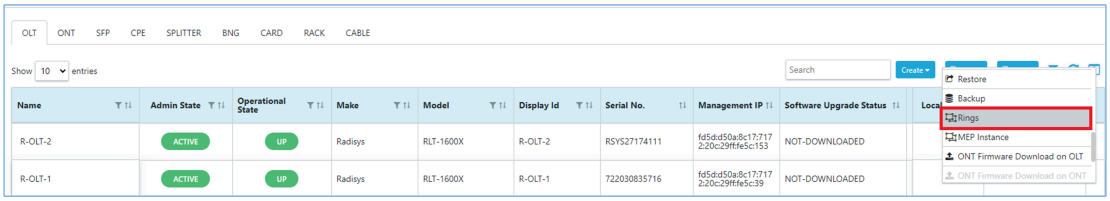


13. Create the ERPS instance.

    a. Navigate to **Configuration > Inventory > OLT**.

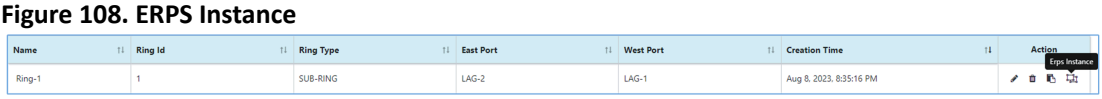
    b. Click on three dots and select **Rings**.

Figure 107. Rings



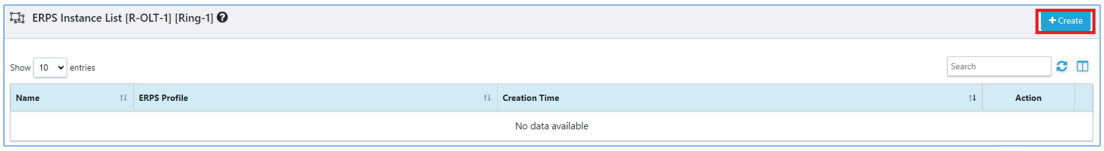
    c. Click on the **ERPS Instance** from the **Action** column.

Figure 108. ERPS Instance



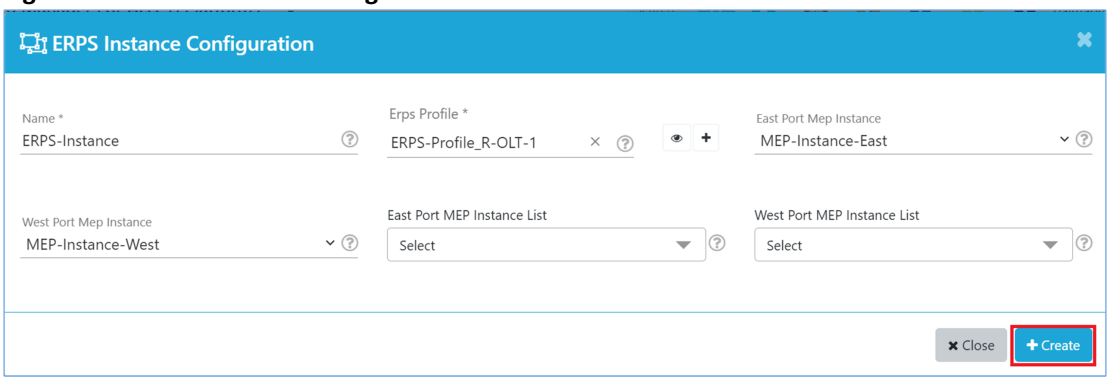
    d. Click **Create**.

Figure 109. Create ERPS



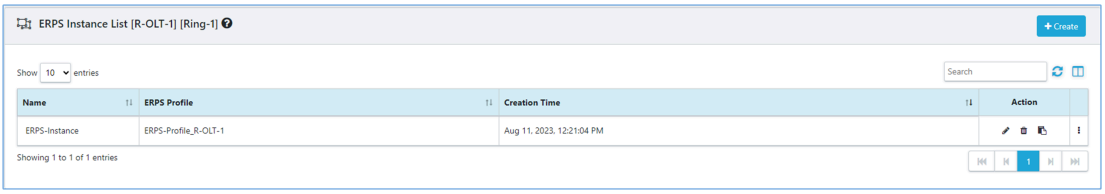
e. Enter ERPS instance configurations (use the previously used ERPS Profile) and click **Create**.

Figure 110. ERPS Instance Configuration



The following screenshot shows the status of the ERPS instance.

Figure 111. Status of the ERPS Instance



f. Navigate to **Monitor > Events** page and check for the "CREATE-ERPS-INSTANCE-SUCCESSFUL" event.

R-OLT-2 Configuration

This section covers the configuration for converting OLT ring ports from NNI to static LAG for enterprise customers for R-OLT-2.

1. Delete the ERPS Instance. See step 2 *(on page 122)*.
2. Delete the MEP Instance. See step 3 *(on page 123)*.
3. Disable the ELANs and delete the ELANs. See step 4 *(on page 123)*.

- Disable the ELAN1030, ELAN1035, and ELAN1022.

Figure 112. Disable ELANs

Name	Vlan	Port	Router Port	Sub Port	Admin State	Creation At	Action
ELAN1030	1030	NNI-3,NNI-4			DISABLED	Jul 31, 2023, 10:08:11 AM	
ELAN1022	1022	NNI-3,NNI-4			DISABLED	Jul 31, 2023, 10:07:33 AM	
ELAN1035	1035	NNI-3,NNI-4			DISABLED	Jul 31, 2023, 10:07:05 AM	

- Delete the ELAN1030, ELAN1035, and ELAN1022.

4. Delete the ring. See step 5 *(on page 124)*.
5. Log in to OLT terminal and remove the *olt_hidden_config* json file. See step 6 *(on page 125)*.
6. Reboot the OLT. See step 7 *(on page 126)*.
7. Check if the OLT is UP. See step 8 *(on page 127)*.
8. Create the LAGs and add the member ports. See step 9 *(on page 127)*.
   - Create the **LAG-1** and associate **NNI-3** and **NNI-5** to the LAG-1
   - Create the **LAG-2** and associate **NNI-4** and **NNI-6** to the LAG-2

Figure 113. Create LAG and Associate NNI

Name	Ports	MTU Size	Admin State	Operational State	Controller State	Lacp	Lacp Timeout	Lacp System Priority	Action
LAG-2	NNI-4,NNI-6	1500	ACTIVE	UP	ENABLED	disabled	fast	128	
LAG-1	NNI-3,NNI-5	1500	ACTIVE	UP	ENABLED	disabled	fast	128	

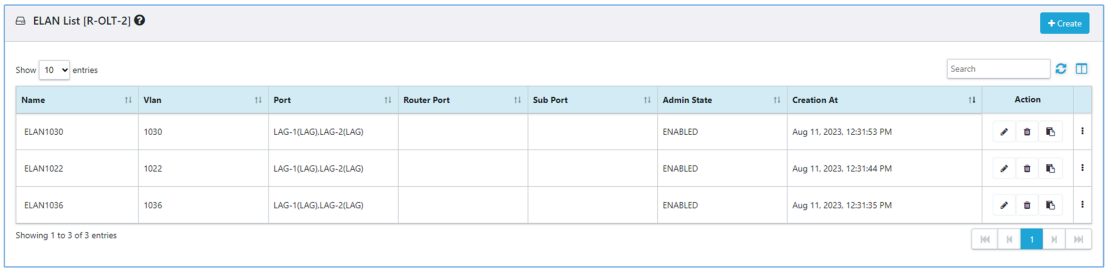
9. Create the Ring with the LAGs. See step 9.a.vi *(on page 130)*.
   - Create the Ring with LAG-1 as east port and LAG-2 as west Port.

Figure 114. Create Ring

Name	Ring Id	Ring Type	East Port	West Port	Creation Time	Action
Ring-1	1	SUB-RING	LAG-1	LAG-2	Aug 11, 2023, 12:32:32 PM	

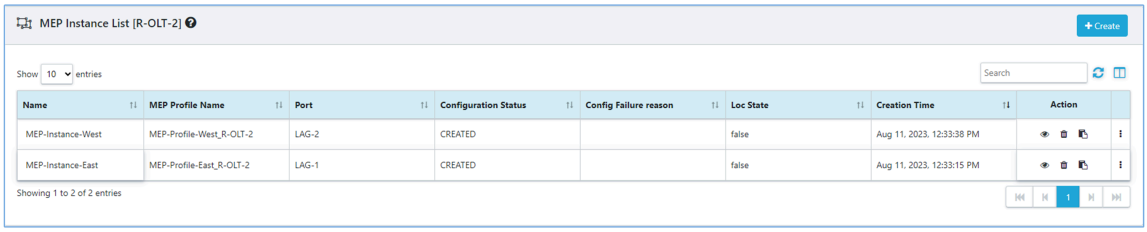
10. Create and enable ELANs with the ELANs. See step 11 *(on page 131)*.
    - Create the control VLAN (ELAN1030) with port list as **LAG-1** and **LAG-2** and enable the ELAN1030.
    - Create the data VLAN (ELAN1035) with port list as **LAG-1** and **LAG-2** and enable the ELAN1035.
    - Create the MCAST VLAN (ELAN1022) with port list as **LAG-1** and **LAG-2** and enable the ELAN1022.

Figure 115. Create and Enable ELANs with the LAGs



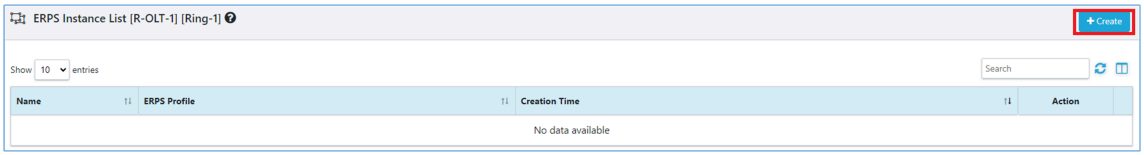
11. Create MEP Instance. See step 12 *(on page 132)*.

Figure 116. MEP Instance



12. Create the ERPS Instance. See step 13 *(on page 134)*.

Figure 117. ERPS Instance



Example: Converting OLT Ring Ports from NNI to Static LAG - Residential

Overview

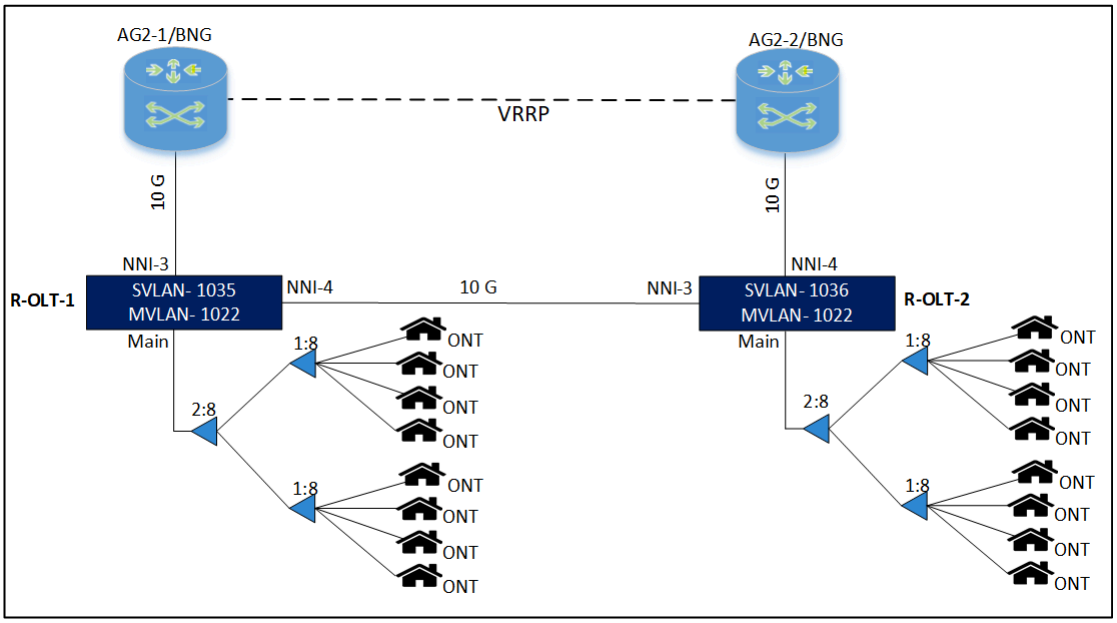
This section covers the procedures to convert the OLT ring ports from the NNI port to the static LAG port for residential customers using the RMS GUI.

Topology 1

The following topology diagram shows the configurations and connections between main OLTs.

- R-OLT-1
- R-OLT-2

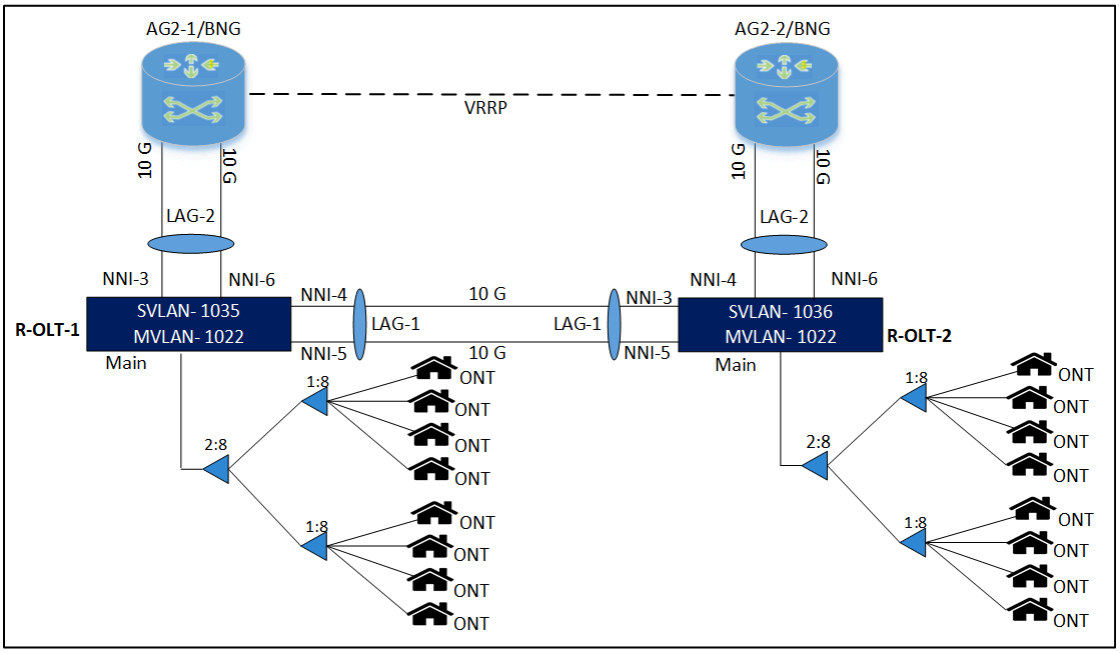
Note: It is assumed that all the OLTs are upgraded from R2.9.3/older version to R2.10.2/latest version. Ensure that the in-band port (port mentioned in the `olt_config` file) is UP and receives the traffic.



Topology 2

The following diagram shows the topology for converting the OLT ring ports from the NNI port to the static LAG port.

Figure 118. Topology - OLT Ring Port (NNI to Static LAG)



R-OLT-1 Configuration

Perform the following steps to convert the OLT ring ports from the NNI port to the static LAG port.

1. Disable and delete the existing ELANs.

   Note: You must disable ELANs before you delete.

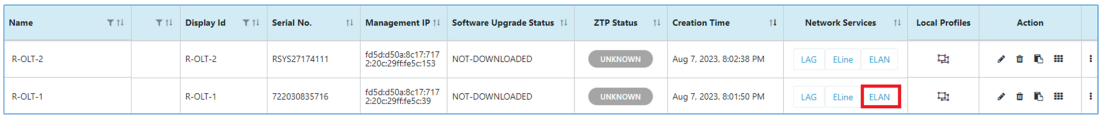
   a. Navigate to **Configuration > Inventory > OLT**.

      The OLT page appears.

   b. Click on the ELAN from the **Network Services** column.

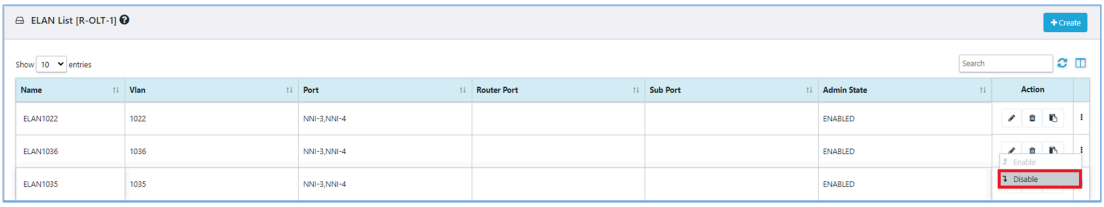
      The ELAN list page appears.

      Figure 119. ELAN



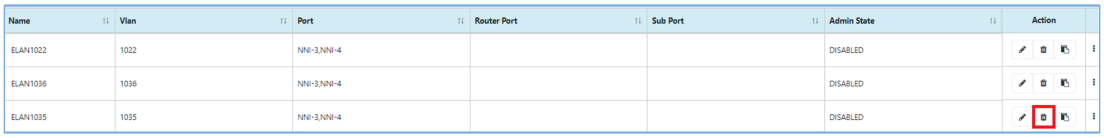
   c. Click on three dots and select the **Disable** option to disable the ELAN1035. Repeat the steps to disable the ELAN1022 and ELAN1036.

      Figure 120. Disable ELAN1035



   d. Click on three dots and select the **Delete** icon to delete theELAN1035. Repeat the steps to delete the ELAN1022 and ELAN1036.

      Figure 121. Delete ELAN1035



2. Delete the ring.

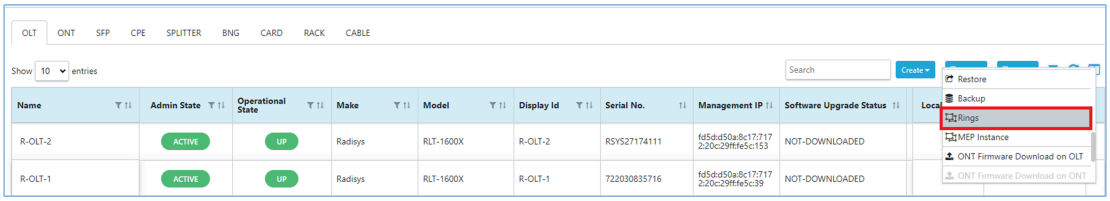
   a. Navigate to **Configuration > Inventory > OLT**.

      The OLT page appears.

   b. Click on three dots and click the **Rings** option.

      The Rings page appears.

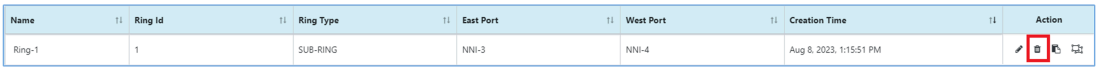
Figure 122. Rings



c. Click the delete icon from the **Action** column.

An alert message appears, asking you to confirm the delete operation.

Figure 123. Delete Ring



d. Click **Confirm** to delete the ring.

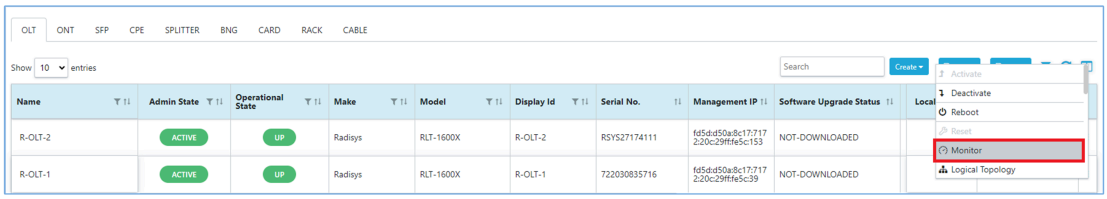
A confirmation message appears, indicating the status of the delete operation.

3. Log in to the OLT terminal and remove the *olt_hidden_config* file.

a. Navigate to **Configuration > Inventory > OLT**.

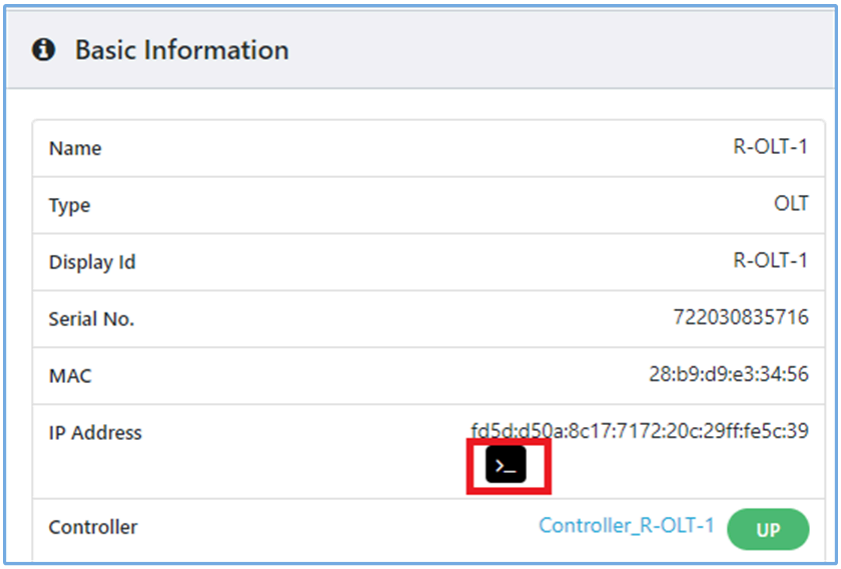
b. Click on three dots and select **Monitor**.

Figure 124. OLT Monitor



c. Under the **Basic Information**, click on the terminal in the IP Address.

Figure 125. OLT Basic Information

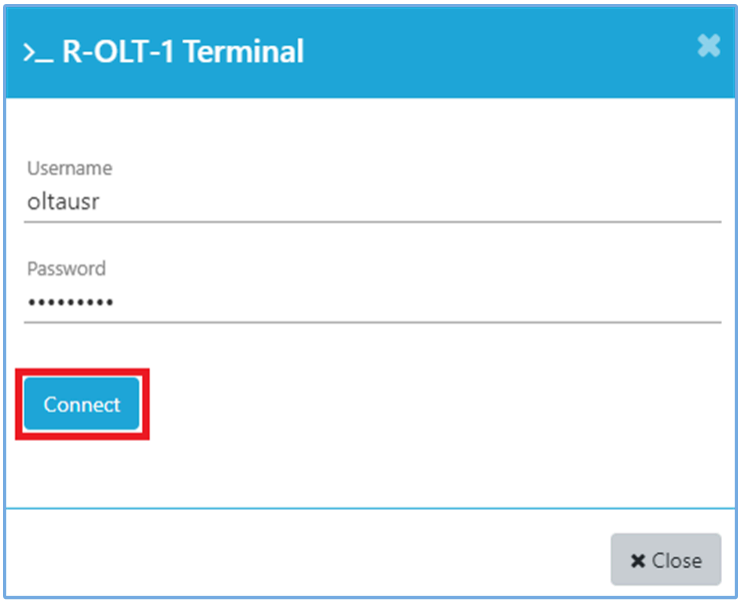


d. Enter the username and password.

e. Click **Connect**.

The OLT Terminal page appears.

Figure 126. R-OLT-1 Terminal



f. Execute the following command to remove the `olt_hidden_config` json file.

```
sudo rm -rf /mnt/onl/sdpon/oltfiles/olt_hidden_config.json
```

Figure 127. Remove JSON File

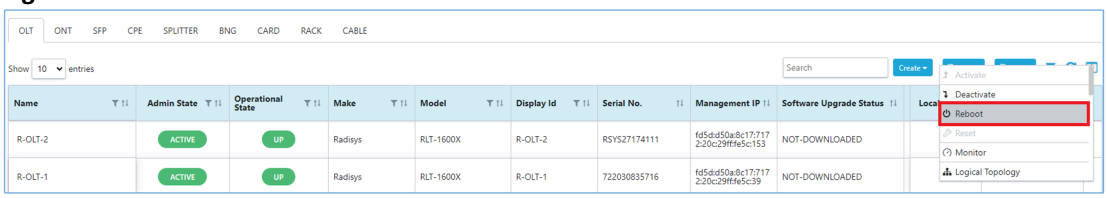
```
oltausr@localhost:~$ sudo rm -rf /mnt/onl/sdpon/oltfiles/olt_hidden_config.json
```

4. Reboot the OLT.

a. Navigate to **Configuration > Inventory > OLT**.

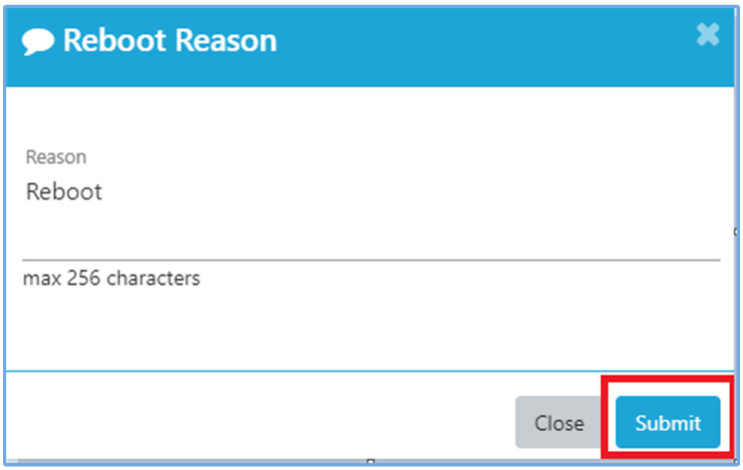
b. Click on three dots and select the **Reboot** option.

Figure 128. OLT Reboot



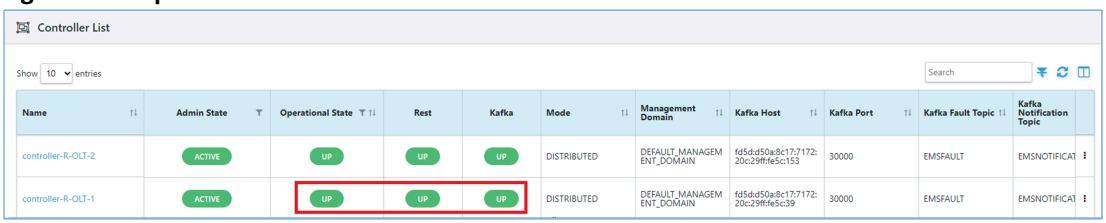
c. Enter the reason for the OLT reboot and click **Submit**.

Figure 129. OLT Reboot Reason



5. Check if the OLT is UP.
   a. Check if the "ME-REBOOTED" event is raised in the **Monitor > Events** page.
   b. Once the "ME-REBOOTED" event is raised, go to **Monitor > Inventory > Controller** and check if the Operational State of Rest and Kafka is UP.

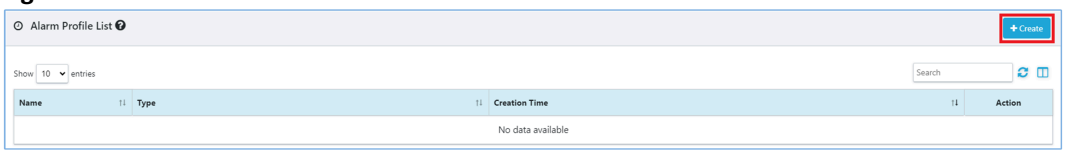
Figure 130. Operational State of Rest and Kafka



6. Create LAGs and add the member ports to LAGs.
   a. Create a LAG alarm profile.
      i. Navigate to **Configuration > Profile > Alarm Profile**.
      ii. Click **Create**.

      The Alarm Profile Configuration page appears.

Figure 131. Create Alarm Profile

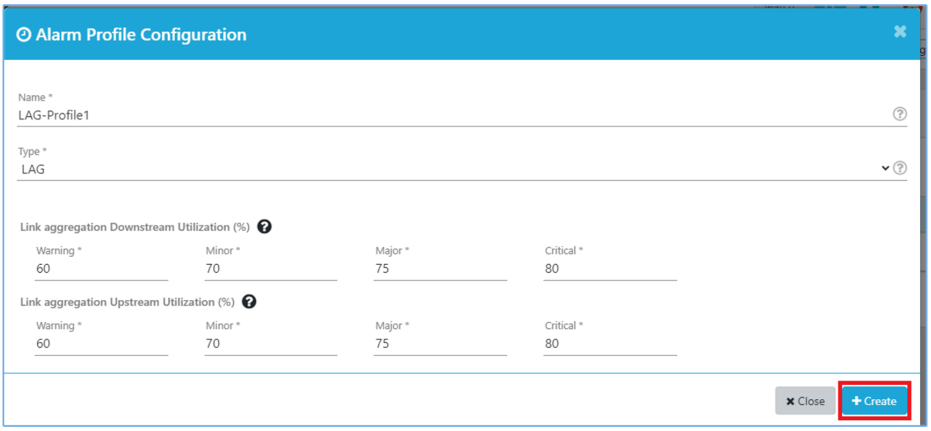


      iii. Enter the alarm profile configuration and click **Create**.

Note:

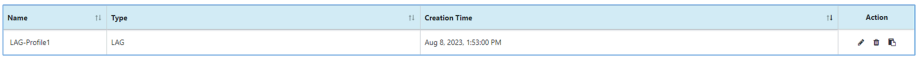
- The space as delimiter is not accepted in RMS for the profile names.
- Change the utilization values for downstream and upstream from the default to the required value (The minimum and maximum values are set to 60). A new LAG alarm profile is created on the Alarm Profile List page.

Figure 132. Alarm Profile Configuration



The following screenshot shows the status of the alarm profile created for LAG.

Figure 133. Alarm Profile Status

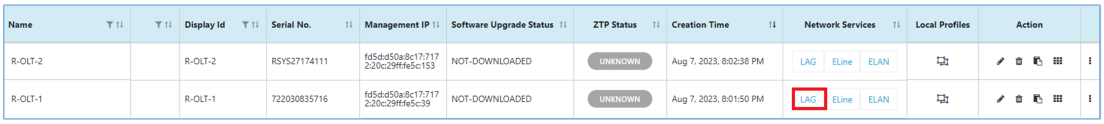


Perform the following steps to create LAG-1.

a. Navigate to **Configuration > Inventory > OLT**.

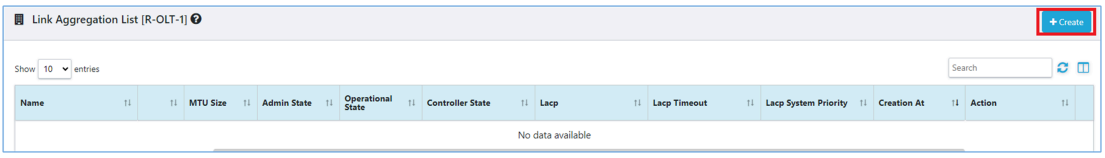
b. Click on the LAG from the **Network Services** column.

Figure 134. LAG



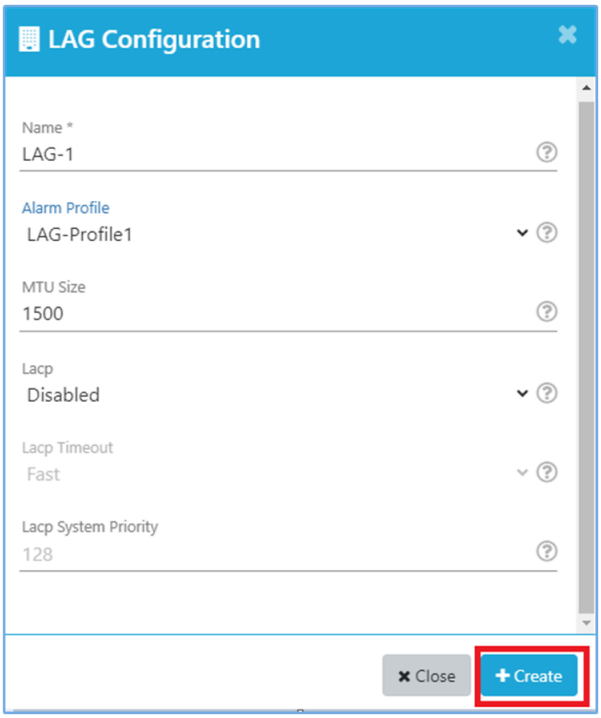
c. Click **Create**.

Figure 135. Create LAG



d. Enter the LAG configuration and click **Create**.

Figure 136. LAG Configuration



e. A LAG is created and the administrative state shows as ACTIVE.

Figure 137. Status of LAG

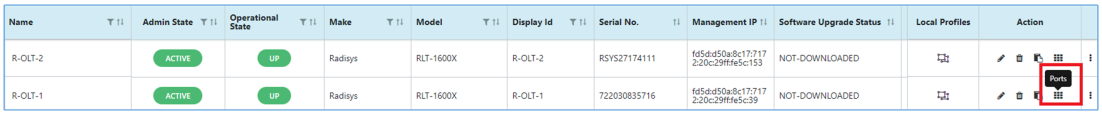
Perform the following steps to associate the NNI-4 and NNI-5 ports to the LAG-1.

Note: When configured, the LAG configuration must only have one active member port. In this scenario, NNI-4 is active and up while NNI-5 is down, and NNI-5 may be active and brought up once the LAG configuration is finished, preventing packet looping.

a. Navigate to **Configuration > Inventory > OLT**.

b. Click on nine dots.

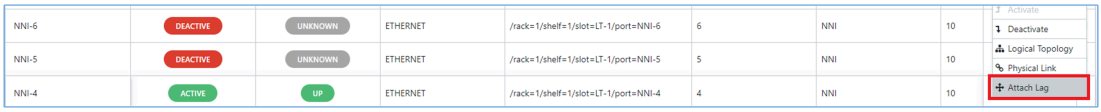
Figure 138. OLT



c. Navigate to the **NNI-4** Port.

d. Click on three dots and select the **Attach Lag** option.

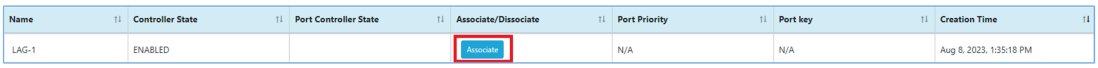
Figure 139. Attach LAG



e. Click the **Associate** option from the Associate/Dissociate column.

The NNI-4 port is associated to LAG-1 and a confirmation message appears, indicating the status of the associate operation. Repeat the steps to associate the NNI-5 port with LAG-1.

Figure 140. Associate LAG



f. Repeat the same steps to create the LAG-2 and associate NNI-3 and NNI-6 ports to the LAG-2

7. Create a ring with LAGs.

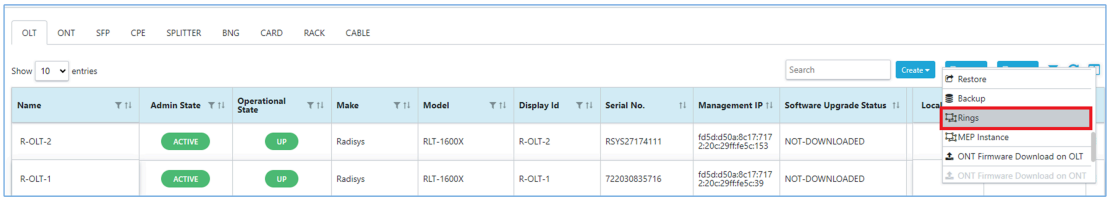
a. Create a ring with LAG-1 as west port and LAG-2 as east port.

b. Navigate to **Configuration > Inventory > OLT**.

c. Click on three dots and click the **Rings** option.

The Rings page appears.

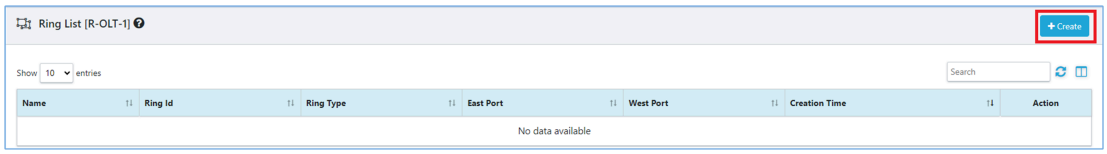
Figure 141. Rings



d. Click **Create**.

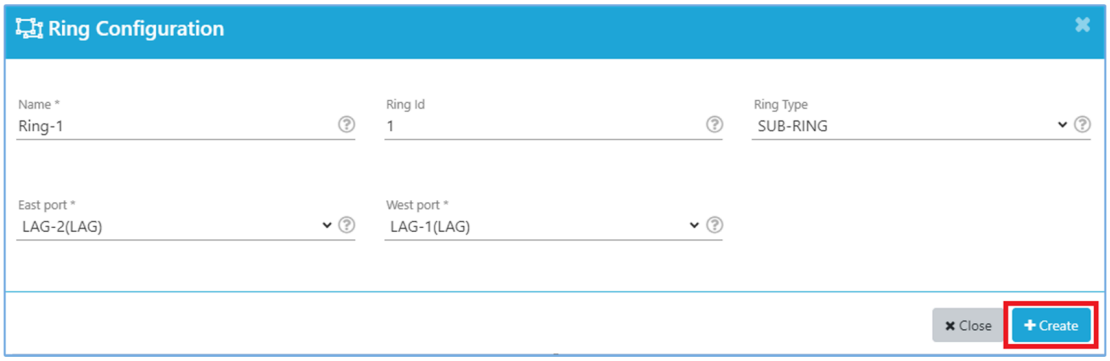
The Ring Configuration page appears.

Figure 142. Create Ring



e. Enter the ring configuration and click **Create**.

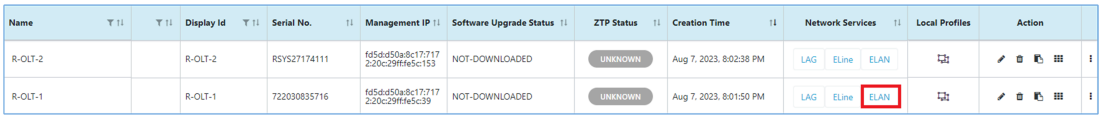
Figure 143. Ring Configuration



A confirmation message appears indicating the status of the ring.

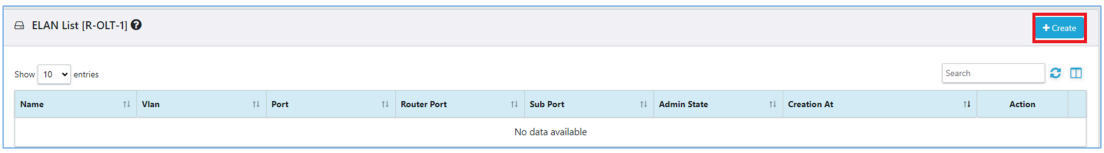
8. Create and enable ELANs with the LAGs.
   a. Create an ELAN1035 with port list as LAG-1 and LAG-2 and enable the ELAN1035.
   b. Navigate to **Configuration > Inventory > OLT**.
   c. Click on the ELAN from the **Network Services** column.

Figure 144. ELAN



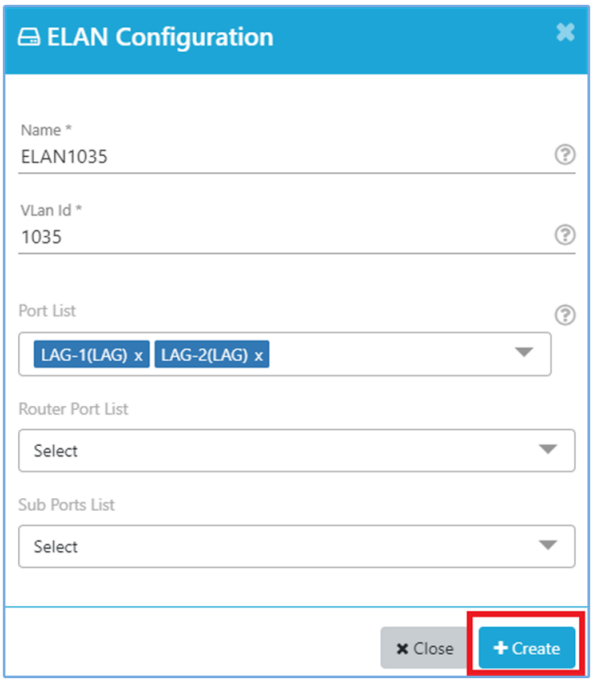
   d. Click **Create**.

Figure 145. Create ELAN



   e. Enter the ELAN configuration and click **Create**.

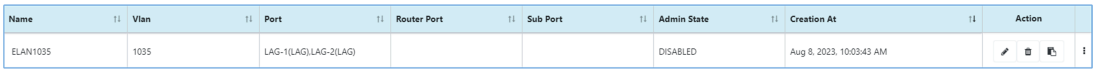
Figure 146. ELAN Configuration



The following screenshot shows the status of the ELAN 1035.

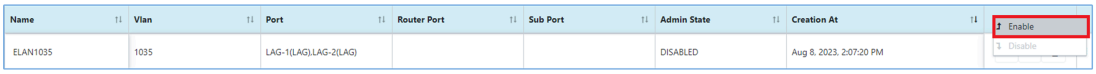
Note: The ELAN1035 is in the **Disable** state.

Figure 147. Status of ELAN1035



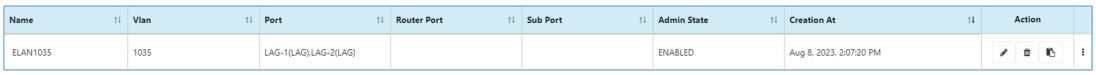
f. Click on three dots and select **Enable** option to enable the ELAN1035.

Figure 148. Enable ELAN



The following screenshot shows the status of the ELAN1035.

Figure 149. Status of ELAN1035



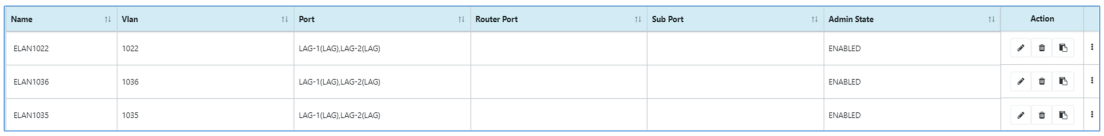
g. Repeat the same steps to create and enable the ELAN1036 and ELAN 1022 with port list as LAG-1 and LAG-2.

R-OLT-2 Configuration

This section covers the configuration for converting OLT ring ports from NNI to static LAG for residential customers for R-OLT-2.

1. Disable and delete the existing ELANs. See step 1 *(on page 139)*.
   - Disable the ELAN1035, ELAN1036, and ELAN1022.

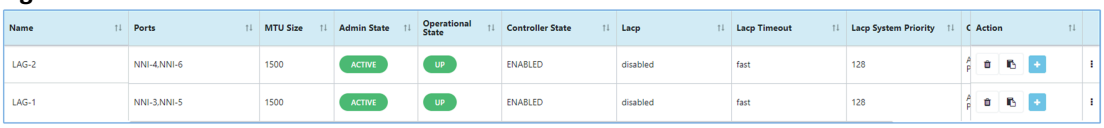
     Figure 150. Disable ELAN

Name	Vlan	Port	Router Port	Sub Port	Admin State	Action
ELAN1022	1022	LAG-1(LAG),LAG-2(LAG)			ENABLED	
ELAN1036	1036	LAG-1(LAG),LAG-2(LAG)			ENABLED	
ELAN1035	1035	LAG-1(LAG),LAG-2(LAG)			ENABLED	

   - Delete the ELAN1035, ELAN1036, and ELAN1022.
2. Delete the Ring. See step 2 *(on page 139)*.
3. Log in to the OLT terminal and remove the *olt_hidden_config* json file. See step 3 *(on page 140)*.
4. Reboot the OLT. See step 4 *(on page 141)*.
5. Check if the OLT is UP. See step 5 *(on page 142)*.
6. Create the LAGs and add the member ports. See step 6 *(on page 142)*.
   - Create the **LAG-1** and associate **NNI-3** and **NNI-5** to the LAG-1.
   - Create the **LAG-2** and associate **NNI-4** and **NNI-6** to the LAG-2, as shown in the below figure.

     Figure 151. Create LAG and Associate NNI

Name	Ports	MTU Size	Admin State	Operational State	Controller State	Lacp	Lacp Timeout	Lacp System Priority	Action
LAG-2	NNI-4,NNI-6	1500	ACTIVE	UP	ENABLED	disabled	fast	128	
LAG-1	NNI-3,NNI-5	1500	ACTIVE	UP	ENABLED	disabled	fast	128	

7. Create the Ring with the LAGs. See step 7 *(on page 145)*.
8. Create and enable ELANs with the LAGs. See step 8 *(on page 146)*.
   - Create the **ELAN1035**, **ELAN1036**, and **ELAN1022** with port list as **LAG-1** and **LAG-2** and enable the **ELAN1035**, **ELAN1036**, and **ELAN1022**.

Example: Converting Subtended OLT Connection from NNI to LAG - Enterprise

Overview

This section covers the procedure to convert the subtended OLT connection from the NNI port to LAG port for enterprise customers using the RMS GUI.

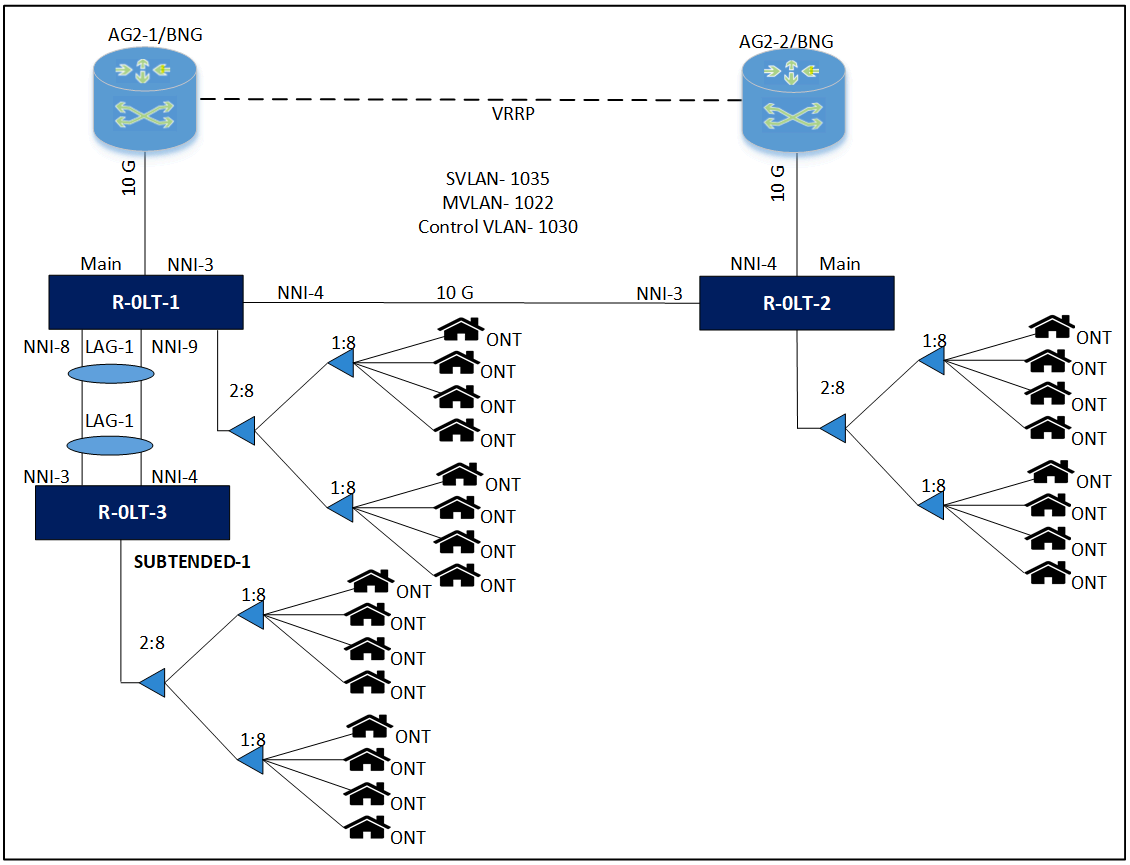
Topology

The following topology diagram shows the configurations and connections between main OLTs and subtended OLT.

- R-OLT-1 is main/parent OLT and part of the ring
- R-OLT-2 is part of the ring
- R-OLT-3 is SUBTENDED-1 OLT

Note: It is assumed that all the OLTs have been upgraded from R2.9.3/older version to R2.10.2/ later version.

Figure 152. Topology



Migrating the SUBTENDED-1 OLT (R-OLT-3) NNI configuration to LAG configuration without impacting the traffic of parent OLT (R-OLT-1). The LAG between parent OLT and subtended OLT has two NNI ports as member ports.

Ideal or Expected Case. The traffic must not be impacted to the main OLT when the SUBTENDED OLT NNI configuration is migrated to LAG.

Configuration for R-OLT-3 (Subtended OLT)

This section covers the configuration for converting the subtended OLT connection from the NNI port to LAG port for enterprise customers for R-OLT-3 (subtended OLT).

1. Disable and delete the existing ELINEs/ELANs.

   Note: You must disable the ELINEs/ELANs before you delete them.

   Perform the following steps to disable and delete the ELINE1035.

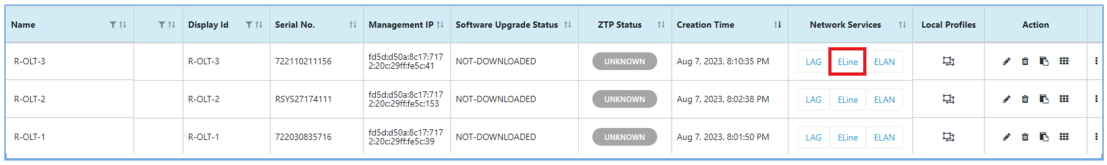
a. Navigate to **Configuration > Inventory > OLT**.

The OLT page appears.

b. Click on the ELINE from the **Network Services** column.

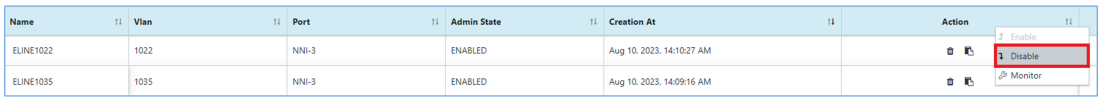
The ELINE list page appears.

Figure 153. ELINE



c. Click on three dots and select the **Disable** option to disable the ELINE1035. Repeat the steps to disable the ELINE1022.

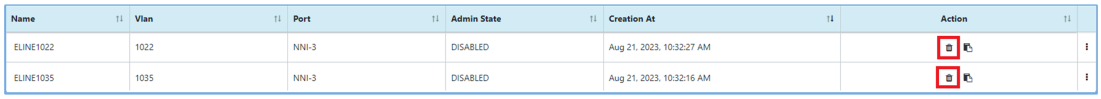
Figure 154. Disable ELINE1035



d. Click the delete icon from the **Action** column.

An alert message appears, asking you to confirm the delete operation.

Figure 155. Delete ELINE



e. Click **Confirm** to delete the ELINE1035.

A confirmation message appears, indicating the status of the delete operation.

Perform the following steps to disable and delete the ELAN1035, if you have configured ELANs.

Note: You must disable the ELANs before you delete them.

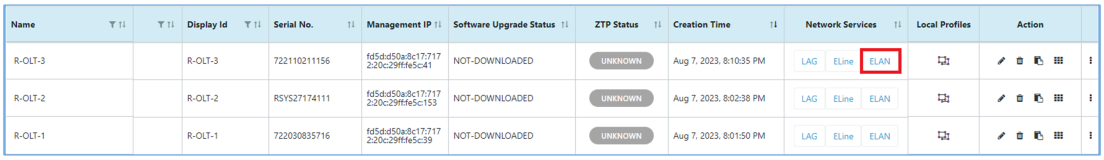
a. Navigate to **Configuration > Inventory > OLT**.

The OLT page appears.

b. Click on the ELAN from the **Network Services** column.

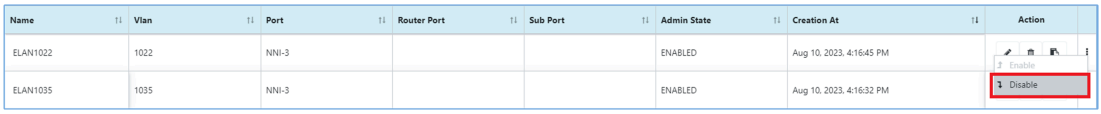
The ELAN list page appears.

Figure 156. Click ELAN



c. Click on three dots and select the **Disable** option to disable the ELAN1035. Repeat the steps to disable the ELAN1022.

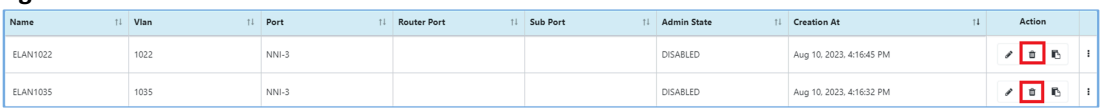
Figure 157. Disable ELAN1022



d. Click the delete icon from the **Action** column.

An alert message appears, asking you to confirm the delete operation.

Figure 158. Delete ELAN



e. Click **Confirm** to delete the ELAN1035.

A confirmation message appears, indicating the status of the delete operation.

2. Create the LAG and add the member ports.

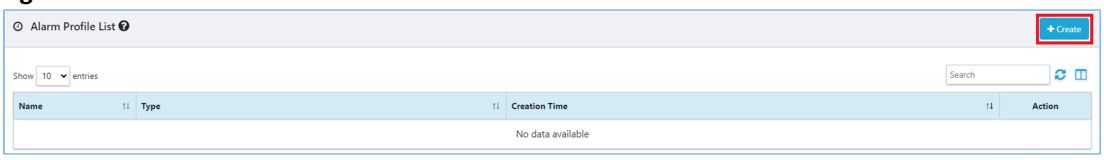
Perform the following steps to create the Alarm Profile for the LAG

a. Navigate to **Configuration > Profile > Alarm Profile**.

b. Click **Create**.

The Alarm Profile Configuration page appears.

Figure 159. Create

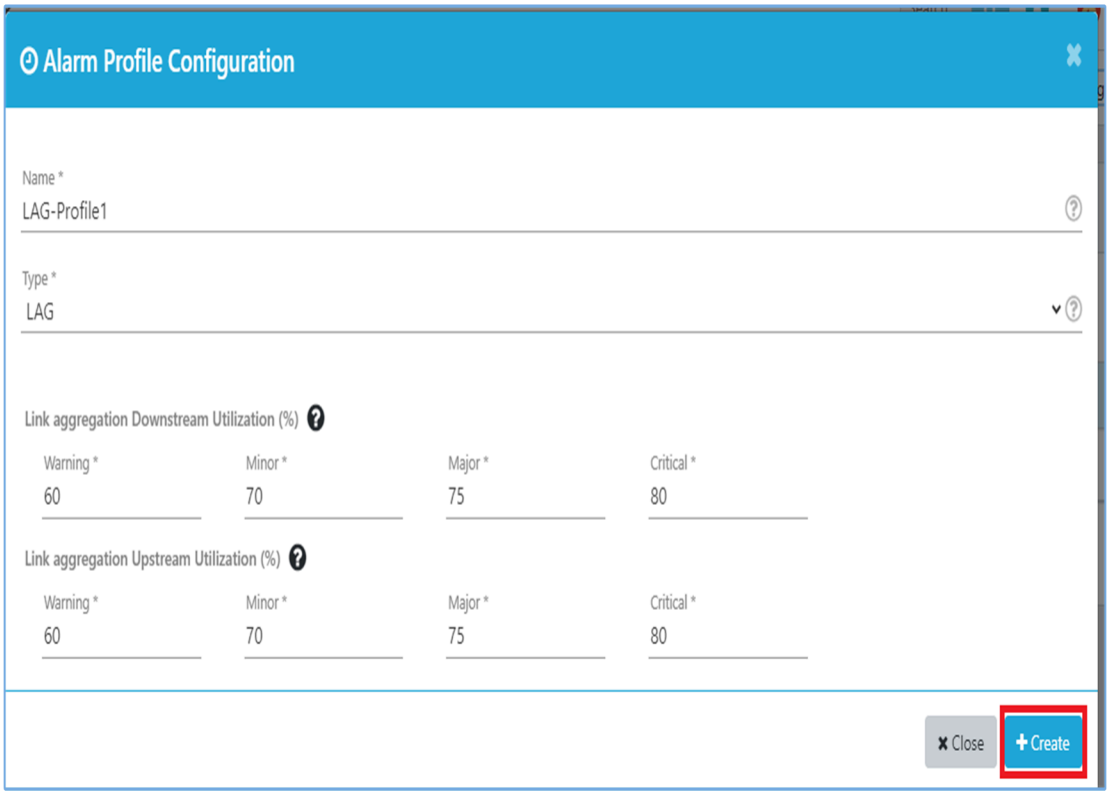


c. Enter the alarm profile configuration and click **Create**.

Note:

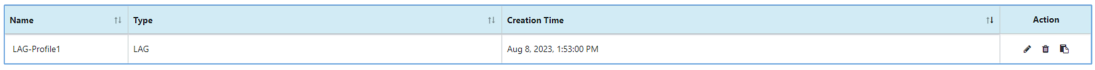
- The space as delimiter is not accepted in RMS for the profile names.
- Change the utilization values for downstream and upstream from the default to the required value (The minimum and maximum values are set to 60).

Figure 160. Alarm Profile Configuration



The following screenshot shows the status of the alarm profile created for LAG.

Figure 161. Status of the LAG

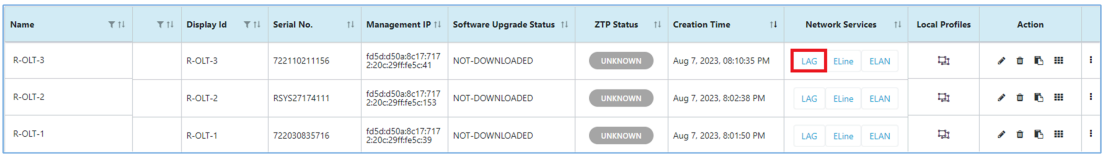


Perform the following steps to create the LAG-1.

a. Navigate to **Configuration > Inventory > OLT**.

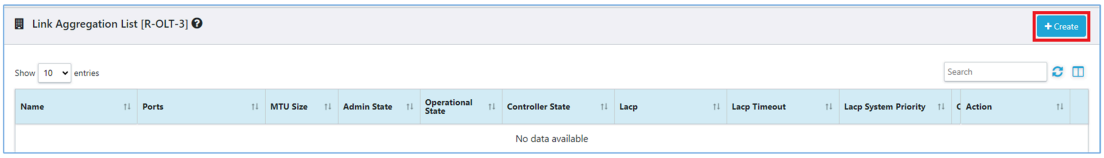
b. Click on the LAG from the **Network Services** column.

Figure 162. LAG



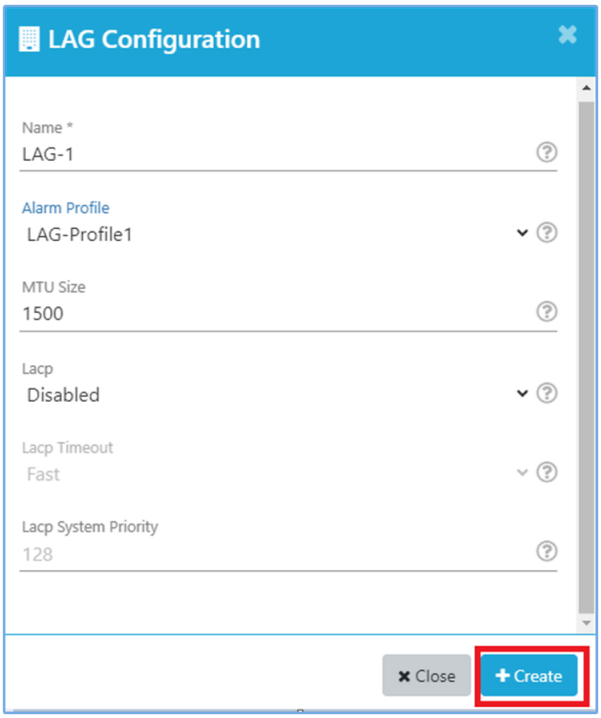
c. Click **Create**.

Figure 163. Create LAG



d. Enter the LAG configuration and click **Create**.

Figure 164. LAG Configuration



e. A LAG is created and the administrative state shows as ACTIVE.

Figure 165. Status of the LAG

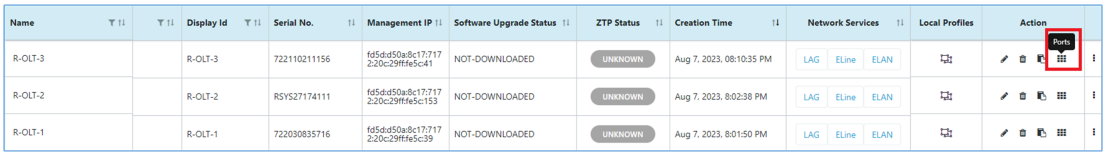
Perform the following steps to associate the NNI-3 and NNI-4 ports to the LAG-1.

Note: When configured, the LAG configuration must only have one active member port. In this scenario, NNI-3 is active and up while NNI-4 is down, and NNI-4 may be active and brought up once the LAG configuration is finished, preventing packet looping.

a. Navigate to **Configuration > Inventory > OLT**.

b. Click on nine dots.

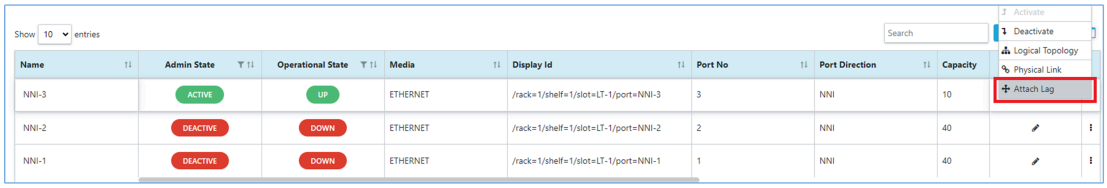
Figure 166. OLT



c. Navigate to the **NNI-4** Port.

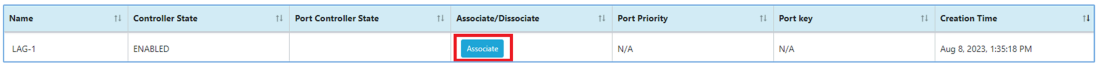
d. Click on three dots and select the **Attach Lag** option.

Figure 167. Attach Lag



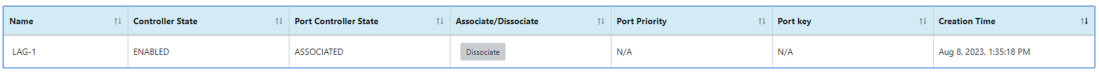
e. Click the **Associate** option from the Associate/Dissociate column.

Figure 168. Associate LAG



The following screenshot shows the NNI-3 port associated with the LAG-1. Repeat the steps to associate the NNI-4 for LAG-1.

Figure 169. Status of the LAG



f. Repeat the same steps to associate NNI-4 to the LAG-1.

3. Create ELINEs or ELANs with the LAG

Perform the following steps to create and enable the ELINE1035 with the port list as LAG-1.

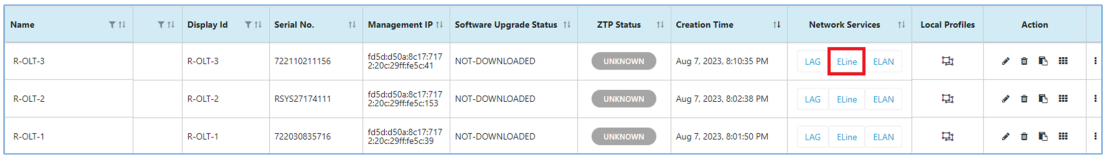
a. Navigate to **Configuration > Inventory > OLT**.

The OLT page appears.

b. Click on the ELINE from the **Network Services** column.

The ELINE list page appears.

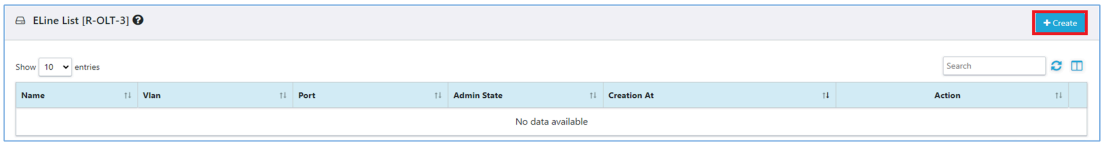
Figure 170. ELINE



c. Click **Create**.

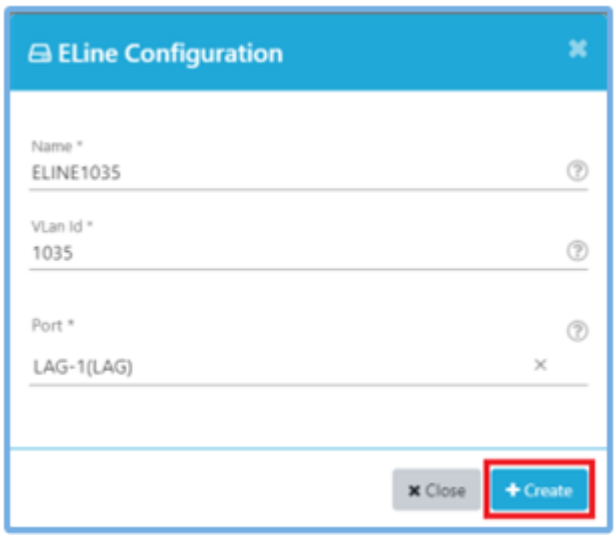
The ELINE Configuration page appears.

Figure 171. Create Eline



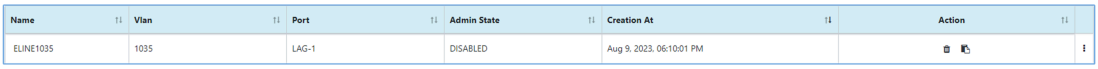
d. Enter the ELINE configuration and click **Create**.

Figure 172. Eline Configuration



The following screenshot shows the status of the ELINE1035.

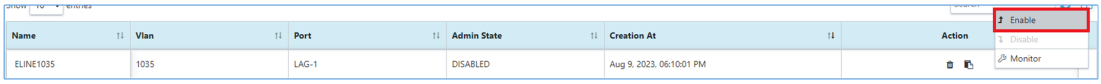
Figure 173. Status of the ELINE1035



Note: The ELINE1035 is in the **Disable** state.

e. Click on three dots and select **Enable** option to enable the ELINE1035.

Figure 174. Enable ELINE1035



The following screenshot shows the status of the ELINE1035.

Figure 175. Status of the ELINE1035

f. Repeat the same steps to create and enable the ELINE1022 with port list as LAG-1.

Perform the following steps to create and enable the ELAN1035 with port list as LAG-1, if you need to configure ELANs.

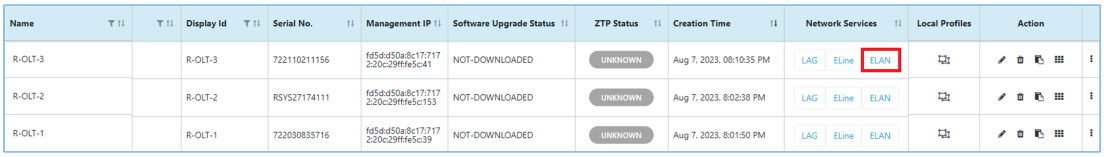
a. Navigate to **Configuration > Inventory > OLT**.

The OLT page appears.

b. Click on the ELAN from the **Network Services** column.

The ELAN list page appears.

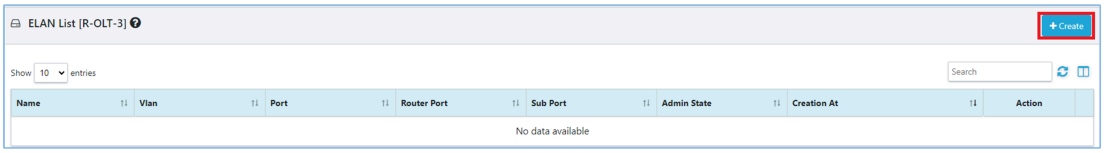
Figure 176. ELAN



c. Click **Create**.

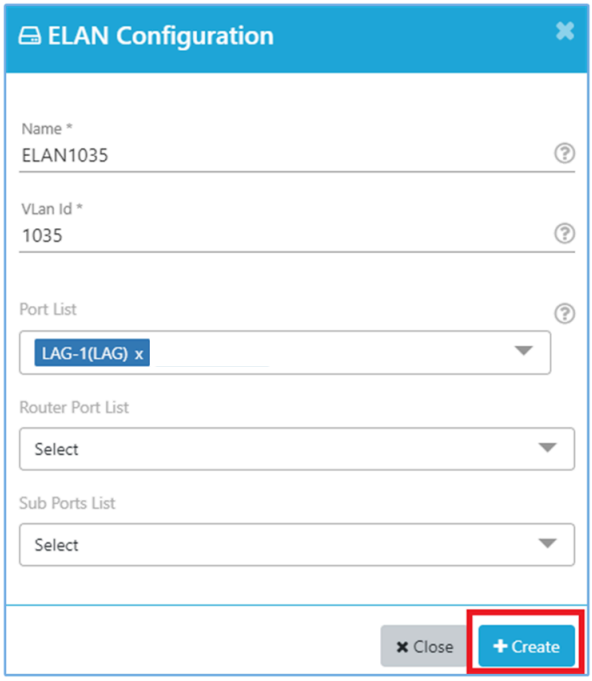
The ELAN Configuration page appears.

Figure 177. Create ELAN



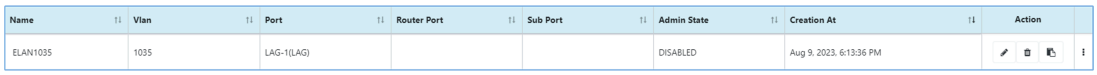
d. Enter the ELAN configuration and click **Create**.

Figure 178. ELAN Configuration



The following screenshot shows the status of the ELAN1035.

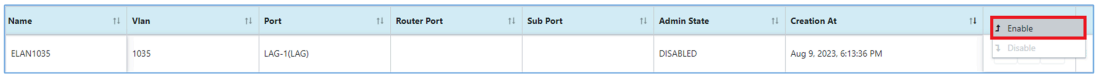
Figure 179. Status of the ELAN1035



Note: The ELAN1035 is in the Disable state.

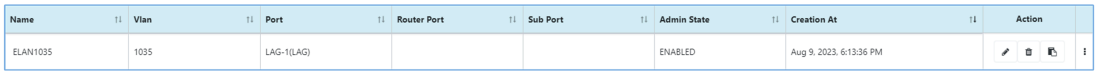
e. Click on three dots and select **Enable** option to enable the ELAN1035.

Figure 180. Enable ELAN1035



The following screenshot shows the status of the ELAN1035.

Figure 181. Status of ELAN1035



f. Repeat the same steps to create and enable the ELAN1022 with port list as LAG-1.

R-OLT-1 (Parent OLT) Configuration

This section covers the configuration for converting subtended OLT connection from NNI to LAG for enterprise customers for R-OLT-1 (Parent OLT).

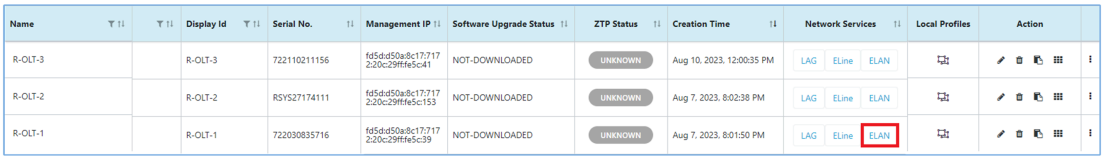
1. Go to the parent OLT (R-OLT-1) and remove the NNI-8 from the existing ELANs.
   a. Navigate to **Configuration > Inventory > OLT**.

      The OLT page appears.

   b. Click on the ELAN from the **Network Services** column.

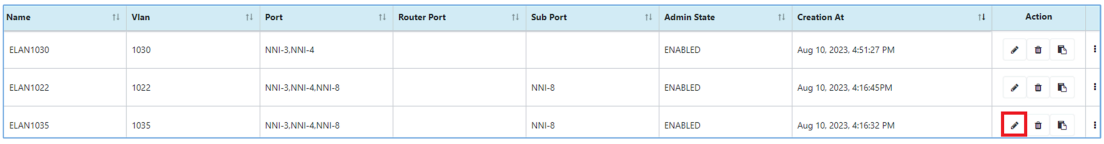
      The ELAN list page appears.

Figure 182. ELAN



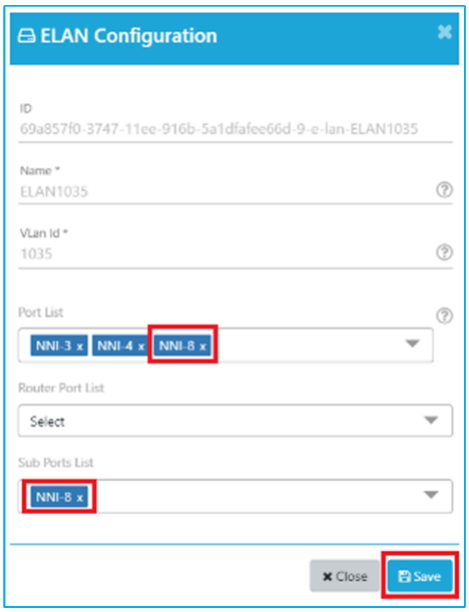
   c. Click the **edit** button to remove the NNI-8.

Figure 183. Edit ELAN



   d. Remove the NNI-8 from the ELAN1035 port and sub port, and then click **Save**.

Figure 184. ELAN1035



The following screenshot shows the status of the removing NNI-8 from the ELAN1035 port.

Figure 185. Status of the ELAN

Name	Vlan	Port	Router Port	Sub Port	Admin State	Creation At	Action
ELAN1030	1030	NNI-3,NNI-4			ENABLED	Aug 10, 2023, 4:51:27 PM	
ELAN1022	1022	NNI-3,NNI-4,NNI-8		NNI-8	ENABLED	Aug 10, 2023, 4:16:45PM	
ELAN1035	1035	NNI-3,NNI-4			ENABLED	Aug 10, 2023, 4:16:32 PM	

e. Repeat the same steps to remove the NNI-8 from the ELAN1022 port and sub port.

f. The following screenshot shows the status of the removed NNI-8 from the ELAN1022 port.

Figure 186. Status of the ELAN1022

Name	Vlan	Port	Router Port	Sub Port	Admin State	Creation At	Action
ELAN1030	1030	NNI-3,NNI-4			ENABLED	Aug 10, 2023, 4:51:27 PM	
ELAN1022	1022	NNI-3,NNI-4			ENABLED	Aug 10, 2023, 4:16:45 PM	
ELAN1035	1035	NNI-3,NNI-4			ENABLED	Aug 10, 2023, 4:16:32 PM	

2. Create the LAG and add the member ports.

a. Create the LAG-1 and associate NNI-8 and NNI-9 to the LAG. See step 2 *(on page 151)*.

Figure 187. Create LAG

Name	Ports	MTU Size	Admin State	Operational State	Controller State	Lacp	Lacp Timeout	Lacp System Priority	Action
LAG-1	NNI-8,NNI-9	1500	ACTIVE	UP	ENABLED	disabled	fast	128	

3. Update the ELANs port list and sub port list with LAG-1

a. Update the ELAN1035 with port list and sub port list as LAG-1.

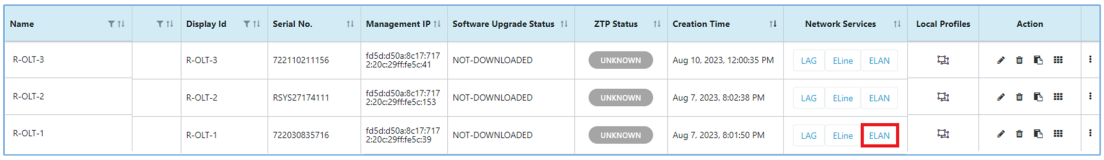
b. Navigate to **Configuration > Inventory > OLT**.

The OLT page appears.

c. Click on the ELAN from the **Network Services** column.

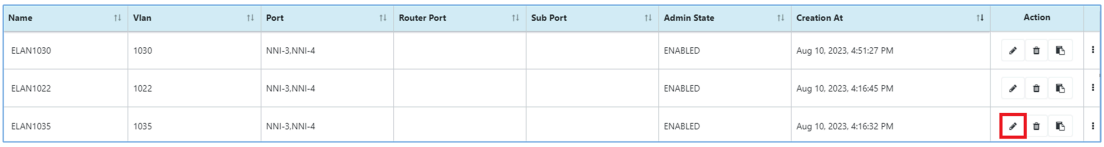
The ELAN list page appears.

Figure 188. ELAN



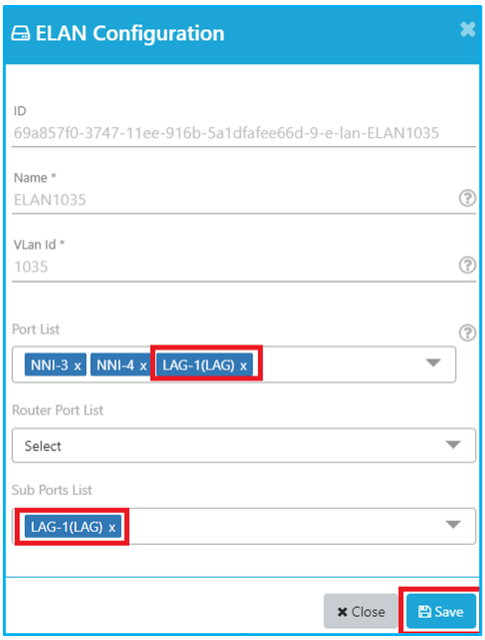
d. Click the **edit** button to update the ELAN1035.

Figure 189. Update ELAN1035



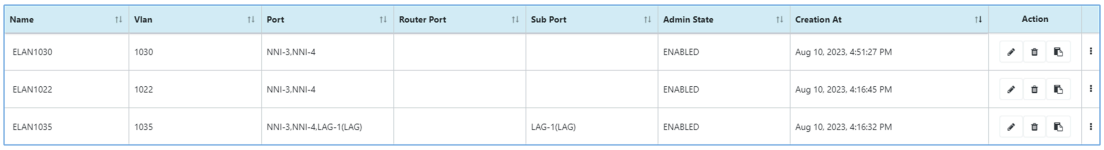
e. Update the ELAN1035 port and sub port with LAG-1, and then click **Save**.

Figure 190. ELAN Configuration



The following screenshot shows the status of the updated ELAN1035 port.

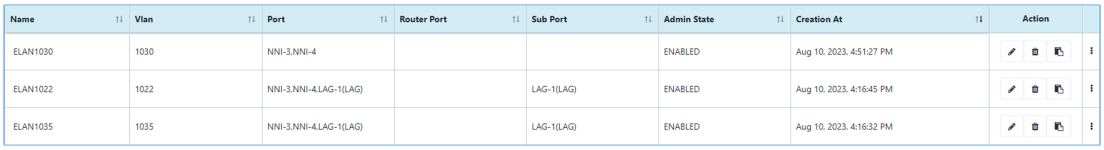
Figure 191. Status of the ELAN1035



f. Repeat the same steps to update the ELAN1022 port and sub port list as LAG-1.

g. Now the ELAN1035 and ELAN1022 port list is NNI-3, NNI-4, and LAG-1 ports and sub port list is LAG-1.

Figure 192. Status of the ELANs



Name	Vlan	Port	Router Port	Sub Port	Admin State	Creation At	Action
ELAN1030	1030	NNI-3,NNI-4			ENABLED	Aug 10, 2023, 4:51:27 PM	
ELAN1022	1022	NNI-3,NNI-4,LAG-1(LAG)		LAG-1(LAG)	ENABLED	Aug 10, 2023, 4:16:45 PM	
ELAN1035	1035	NNI-3,NNI-4,LAG-1(LAG)		LAG-1(LAG)	ENABLED	Aug 10, 2023, 4:16:32 PM	

Example: Converting Subtended OLT Connection from NNI to LAG - Residential

Overview

This section covers the procedure to convert the subtended OLT connection from the NNI port to LAG port for residential customers using the RMS GUI.

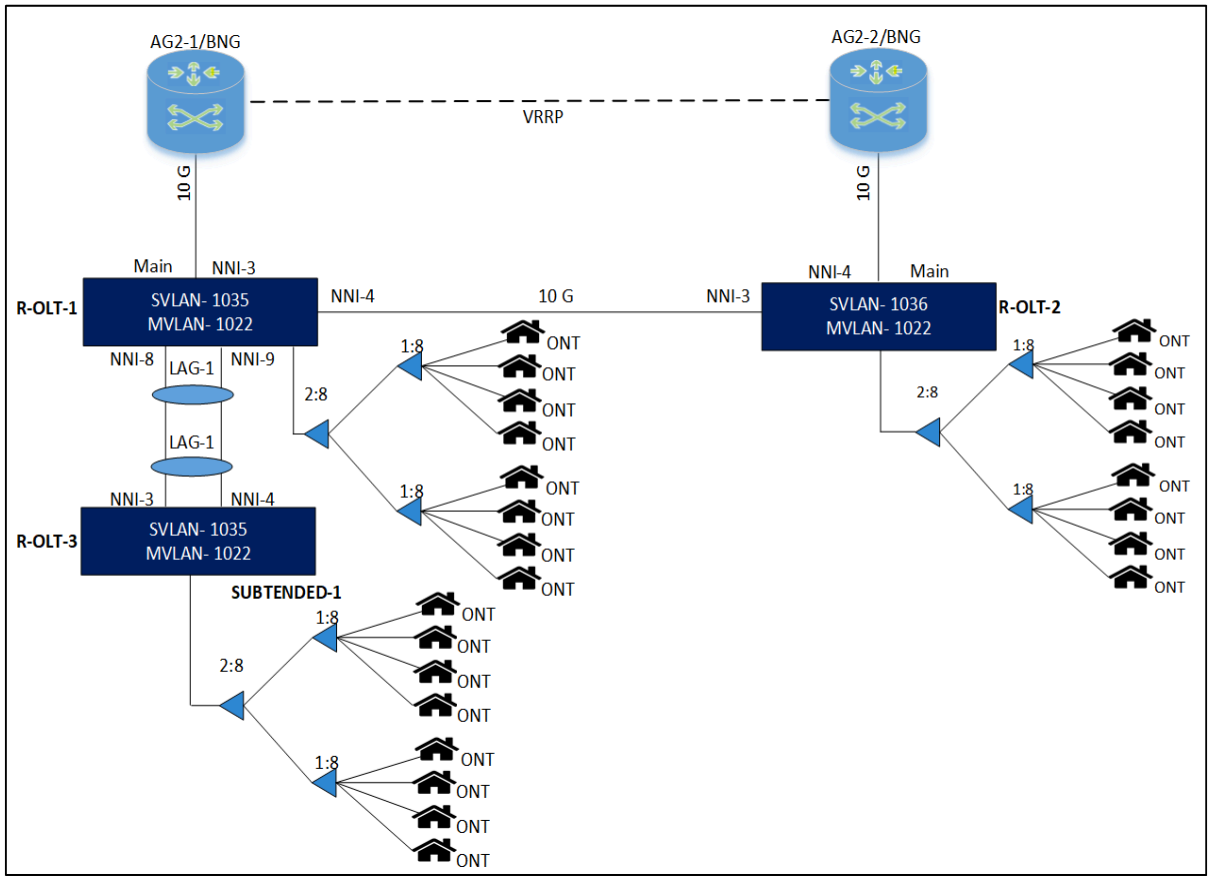
Topology

The following topology diagram shows the configurations and connections between main OLTs and subtended OLTs.

- R-OLT-1 is MAIN/Parent OLT
- R-OLT-2
- R-OLT-3 is SUBTENDED-1 OLT

Note: It is assumed that all the OLTs have been upgraded from R2.9.3/older version to R2.10.2/ later version.

Figure 193. Topology



Migrating the SUBTENDED-1 OLT (R-OLT-3) NNI configuration to LAG configuration without impacting the traffic of parent OLT (R-OLT-1). The LAG between parent OLT and subtended OLT has two NNI ports as member ports.

Ideal/Expected Case. The traffic must not be impacted to the main OLT when the subtended OLT NNI configuration is migrated to LAG.

Configuration for R-OLT-3 (Subtended OLT)

This section covers the configuration for converting the subtended OLT connection from the NNI port to LAG port for residential customers for R-OLT-3 (subtended OLT).

1. Disable and delete the existing ELINE's/ELAN's.

   Note: You must disable the ELINE's/ELAN's before you delete them.

   Perform the following steps to disable and delete the ELINE1035.

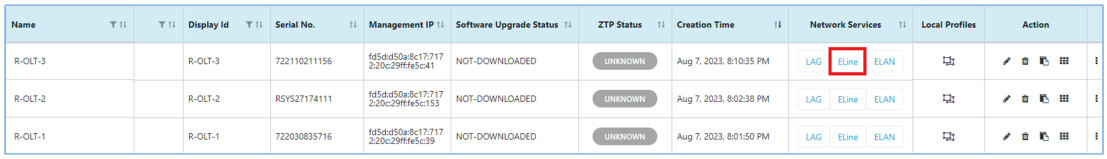
   a. Navigate to **Configuration > Inventory > OLT**.

      The OLT page appears.

   b. Click on the ELINE from the **Network Services** column.

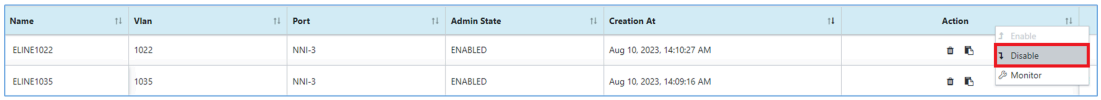
The ELAN list page appears.

Figure 194. ELINE



c. Click on three dots and select the **Disable** option to disable the ELINE1035. Repeat the steps to disable the ELINE1022.

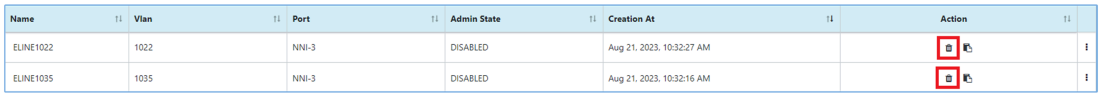
Figure 195. Disable ELINE1035



d. Click the delete icon from the **Action** column.

An alert message appears, asking you to confirm the delete operation.

Figure 196. Delete ELINE



e. Click **Confirm** to delete the ELINE1035.

A confirmation message appears, indicating the status of the delete operation.

Perform the following steps to disable and delete the ELAN1035, if you have configured ELANs.

Note: You must disable the ELANs before you delete them.

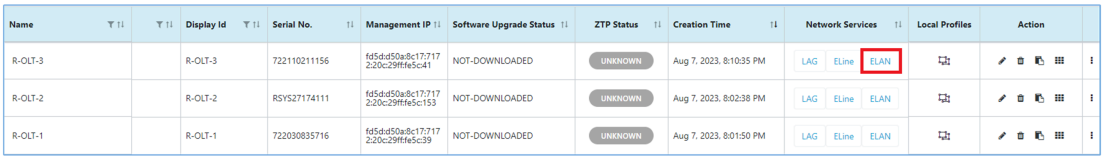
a. Navigate to **Configuration > Inventory > OLT**.

The OLT page appears.

b. Click on the ELAN from the **Network Services** column.

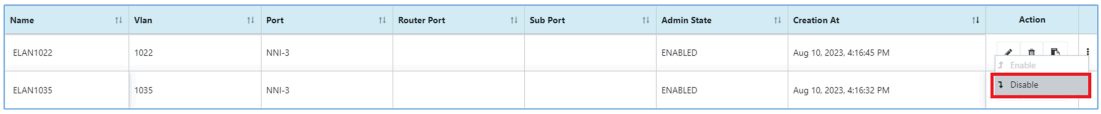
The ELAN list page appears.

Figure 197. ELAN



c. Click on three dots and select the **Disable** option to disable the ELAN1035. Repeat the steps to disable the ELAN1022.

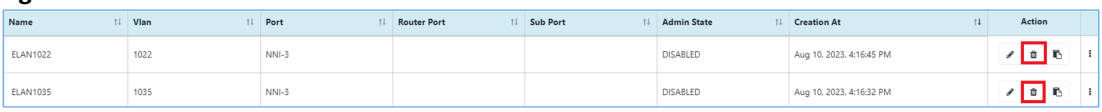
Figure 198. Disable ELAN1035



d. Click the delete icon from the **Action** column.

An alert message appears, asking you to confirm the delete operation.

Figure 199. Delete ELAN



e. Click **Confirm** to delete the ELAN1035.

A confirmation message appears, indicating the status of the delete operation.

2. Create the LAG and add the member ports.

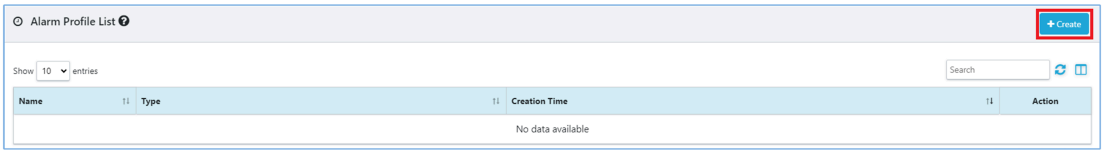
Perform the following steps to create the Alarm Profile for the LAG.

a. Navigate to **Configuration > Profile > Alarm Profile**.

b. Click **Create**.

The Alarm Profile Configuration page appears.

Figure 200. Create Alarm Profile

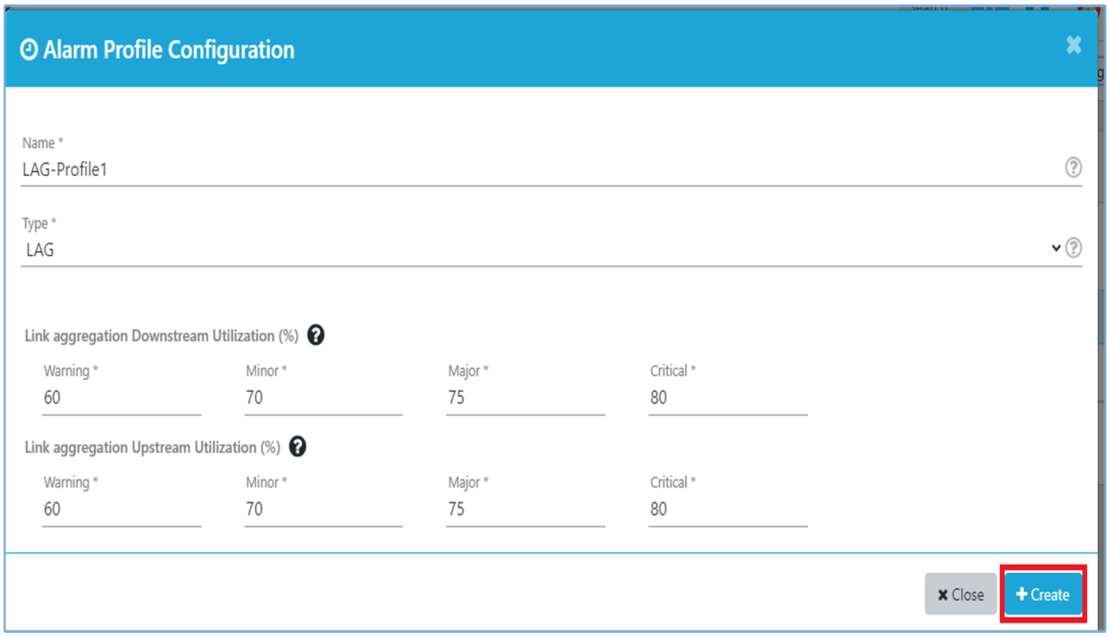


c. Enter the alarm profile configuration and click **Create**.

Note:

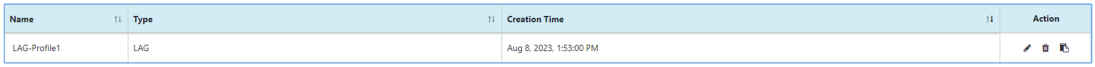
- The space as a delimiter is not accepted in RMS for the profile names.
- Change the utilization values for downstream and upstream from the default to the required value (The minimum and maximum values are set to 60).

Figure 201. Alarm Profile Configuration



The following screenshot shows the status of the alarm profile created for LAG.

Figure 202. Status of the Alarm Profile

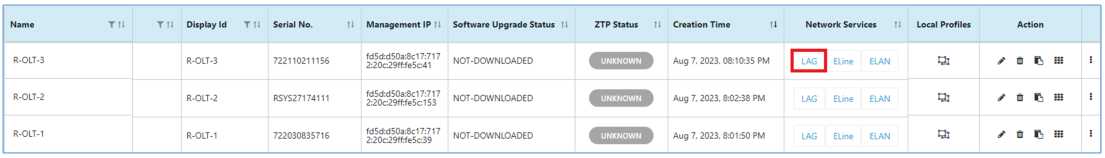


Perform the following steps to create the LAG-1.

a. Navigate to **Configuration > Inventory > OLT**.

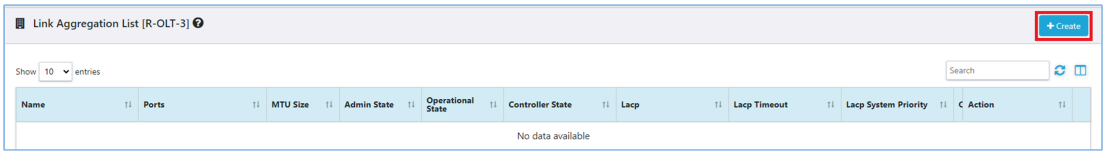
b. Click on the LAG from the **Network Services** column.

Figure 203. LAG



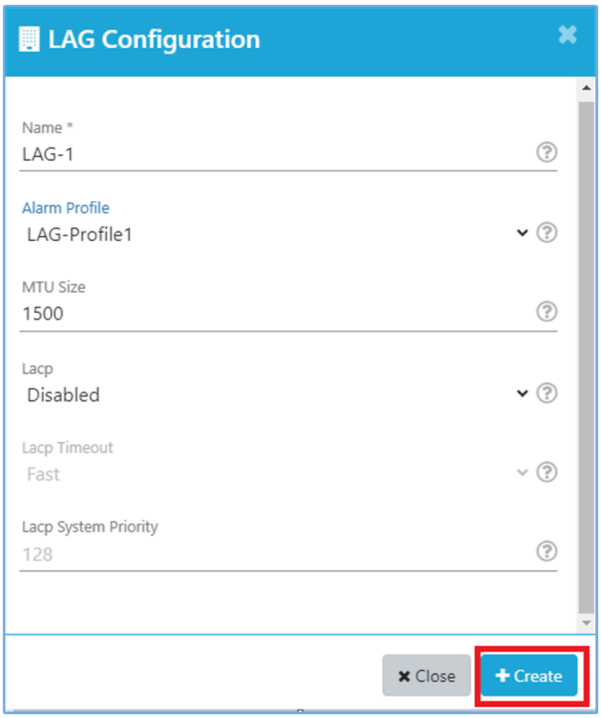
c. Click **Create**.

Figure 204. Create LAG



d. Enter the LAG configuration and click **Create**.

Figure 205. LAG Configuration



e. The LAG is created and the administrative state is ACTIVE.

Figure 206. Status of the LAG

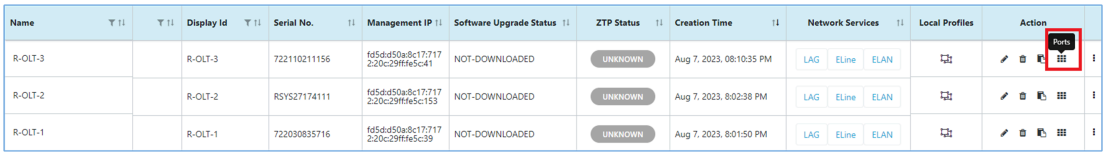
Perform the following steps to associate NNI-3 and NNI-4 ports to the LAG-1.

Note: When configured, the LAG configuration must only have one active member port. In this scenario, NNI-3 is active and up while NNI-4 is down, and NNI-4 may be active and brought up once the LAG configuration is finished, preventing packet looping.

a. Navigate to **Configuration > Inventory > OLT**.

b. Click on nine dots.

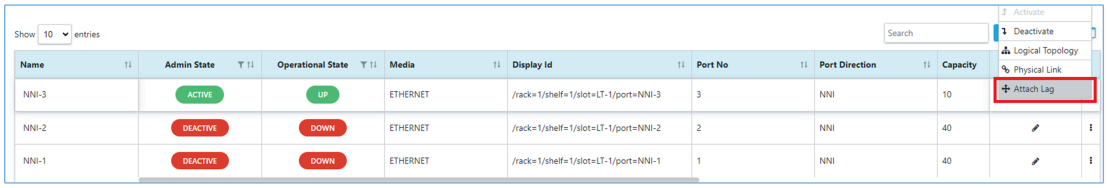
Figure 207. OLT



c. Navigate to the **NNI-3** Port.

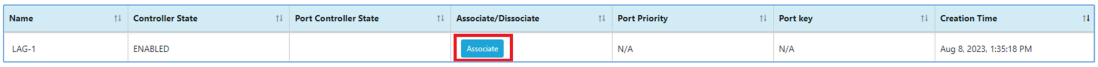
d. Click on three dots and select the **Attach LAG** option.

Figure 208. Attach LAG



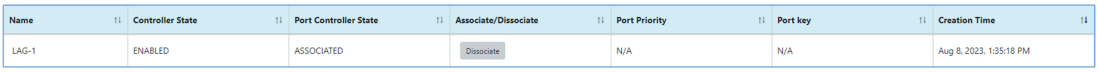
e. Click the **Associate** option from the Associate/Dissociate column.

Figure 209. Associate LAG



The following screenshot shows the associated NNI-3 port with LAG-1 port.

Figure 210. Associated Port to LAG-1



f. Repeat the same steps to associate NNI-4 port to the LAG-1 port.

3. Create ELINEs or ELANs with the LAG

Perform the following steps to create and enable the ELINE1035 with port list as LAG-1.

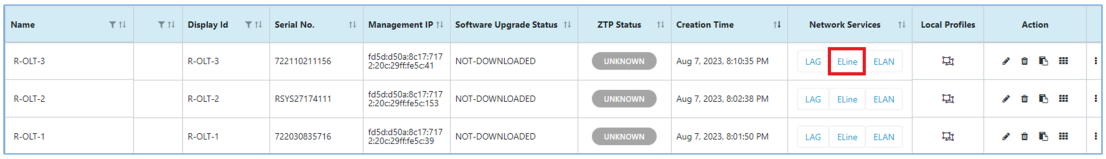
a. Navigate to **Configuration > Inventory > OLT**.

The OLT page appears.

b. Click on the ELINE from the **Network Services** column.

The ELINE list page appears.

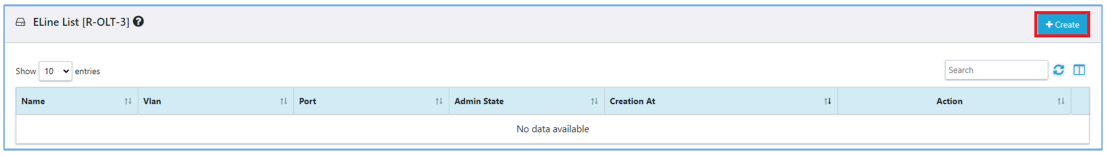
Figure 211. ELINE



c. Click **Create**.

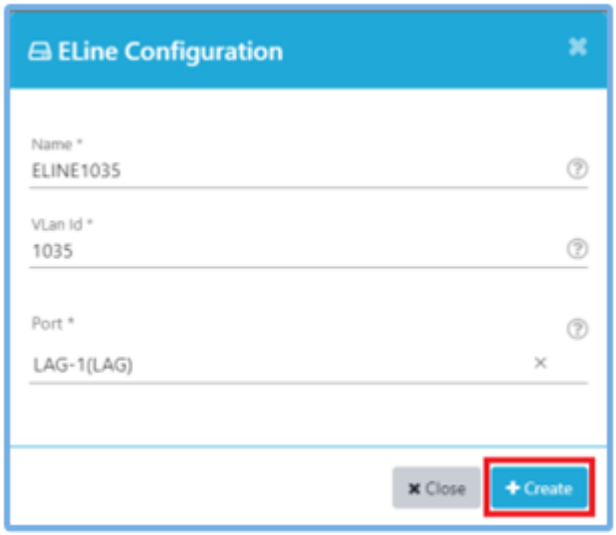
The ELINE Configuration page appears.

Figure 212. Create ELINE



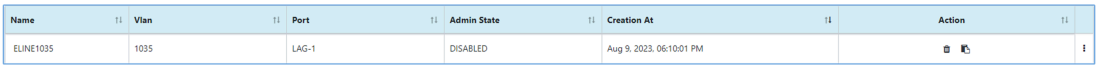
d. Enter the ELINE configuration and click **Create**.

Figure 213. ELINE Configuration



The following screenshot shows the status of the ELINE1035.

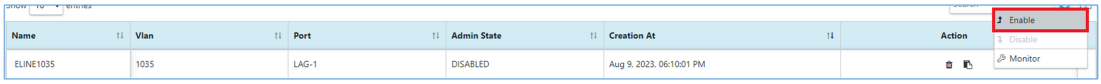
Figure 214. Status of the ELINE1035



Note: The ELINE1035 is in the **Disable** state.

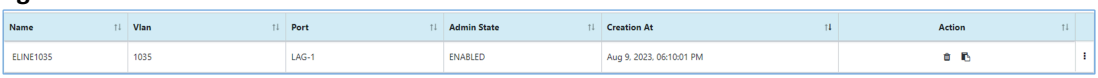
e. Click on three dots and select **Enable** option to enable the ELINE1035.

Figure 215. Enable ELINE1035



The following screenshot shows the status of the ELINE1035.

Figure 216. Status of the ELINE1035



f. Repeat the same steps to create and enable the ELINE1022 with port list as LAG-1.

Perform the following steps to create and enable the ELAN1035 with port list as LAG-1, if you need to configure ELANs.

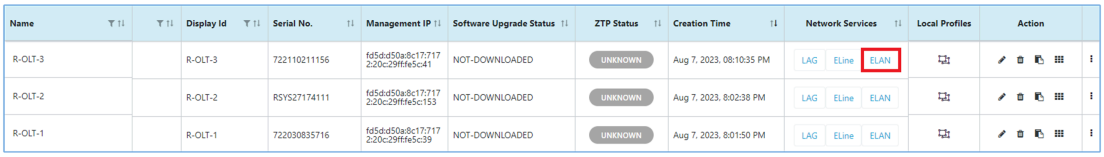
a. Navigate to **Configuration > Inventory > OLT**.

The OLT page appears.

b. Click on the ELAN from the **Network Services** column.

The ELAN list page appears.

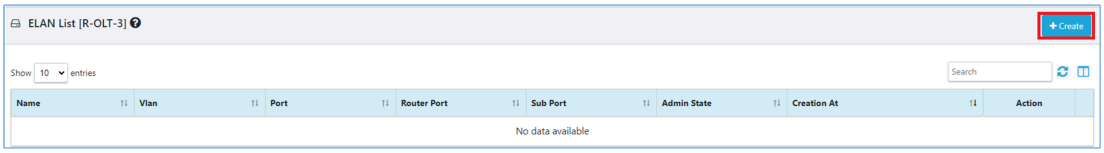
Figure 217. ELAN



c. Click **Create**.

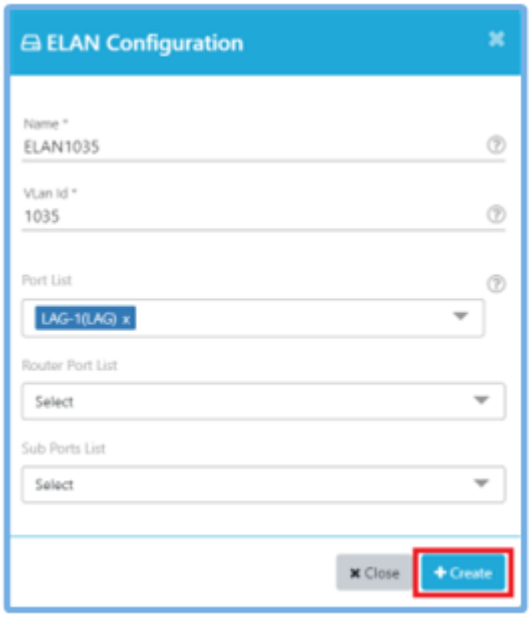
The ELAN Configuration page appears.

Figure 218. Create ELAN



d. Enter the ELAN configuration and click **Create**.

Figure 219. ELAN Configuration



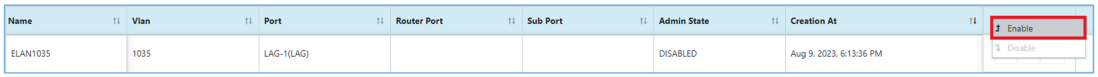
The following screenshot shows the status of the ELAN1035.

Figure 220. Status of ELAN1035

Note: The ELAN1035 is in the Disable state.

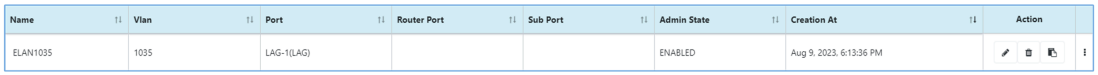
e. Click on three dots and select **Enable** option to enable the ELAN1035.

Figure 221. Enable ELAN1035



The following screenshot shows the status of the ELAN1035.

Figure 222. Status of the ELAN1035



f. Repeat the same steps to create and enable the ELAN1022 with port list as LAG-1.

R-OLT-1 (Parent OLT) Configuration

This section covers the configuration for converting the subtended OLT connection from the NNI port to LAG port for enterprise customers for R-OLT-1 (Parent OLT).

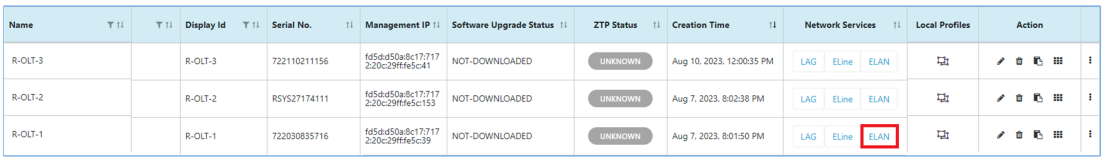
1. Go to the parent OLT (R-OLT-1) and remove the NNI-8 from the existing ELANs.
   a. Navigate to **Configuration > Inventory > OLT**.

      The OLT page appears.

   b. Click on the ELAN from the **Network Services** column.

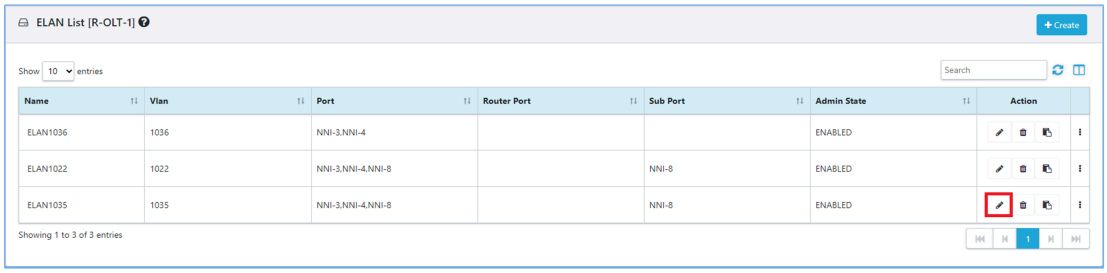
      The ELAN list page appears.

Figure 223. ELAN



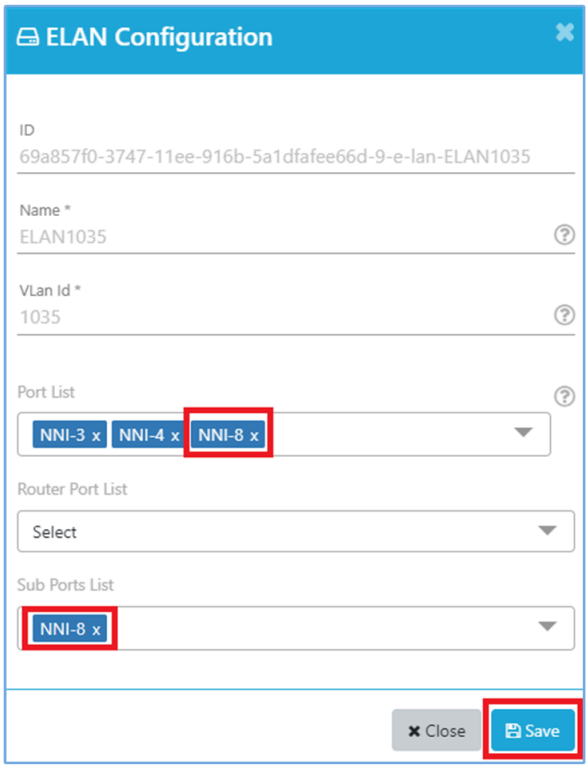
   c. Click the **edit** button to remove the NNI-8 port.

Figure 224. Edit ELAN1035



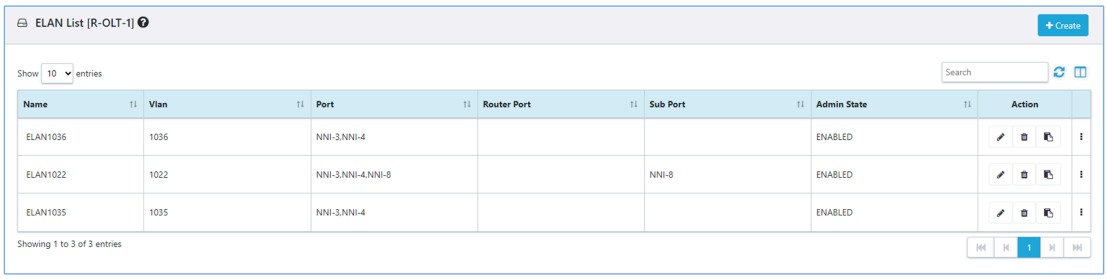
   d. Remove the NNI-8 port from the ELAN1035 port and sub port, and then click **Save**.

Figure 225. ELAN Configuration



The following screenshot shows the status of the removing NNI-8 port from the ELAN1035 port.

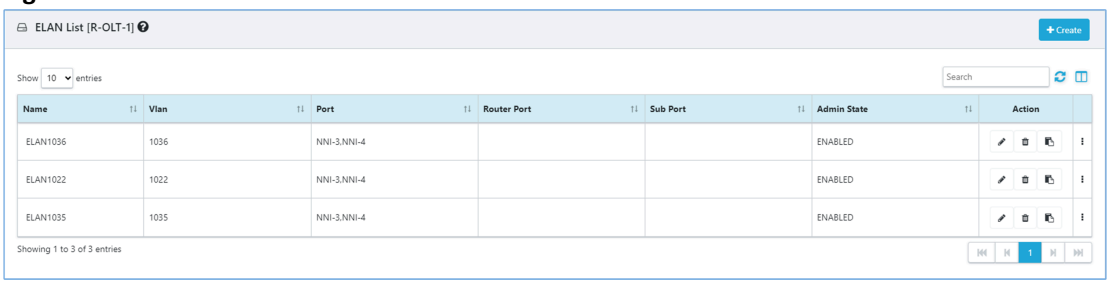
Figure 226. Status of the ELAN1035



e. Repeat the same steps to remove the NNI-8 port from the ELAN1022 port and sub port.

f. The following screenshot shows the status of the removed NNI-8 port from the ELAN1022 port.

Figure 227. Status of the ELAN1022



2. Create the LAG and add the member ports.

a. Create the LAG-1 and associate NNI-8 and NNI-9 ports to the LAG port. See step 2 *(on page 163)*.

Figure 228. Create LAG

3. Update the ELANs port list and sub-port list with LAG-1

a. Update the ELAN1035 with a port list and sub-port list as LAG-1.

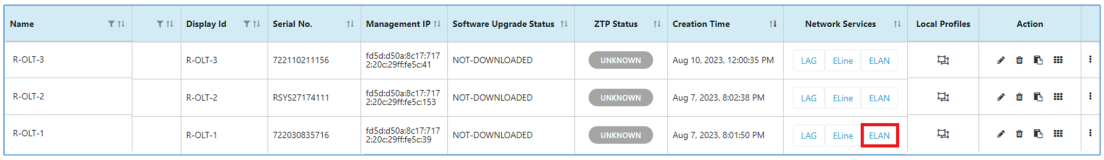
b. Navigate to **Configuration > Inventory > OLT**.

The OLT page appears.

c. Click on the ELAN from the **Network Services** column.

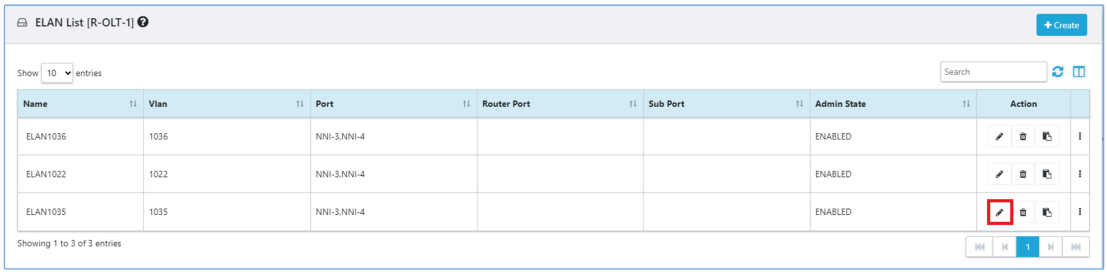
The ELAN list page appears.

Figure 229. ELAN



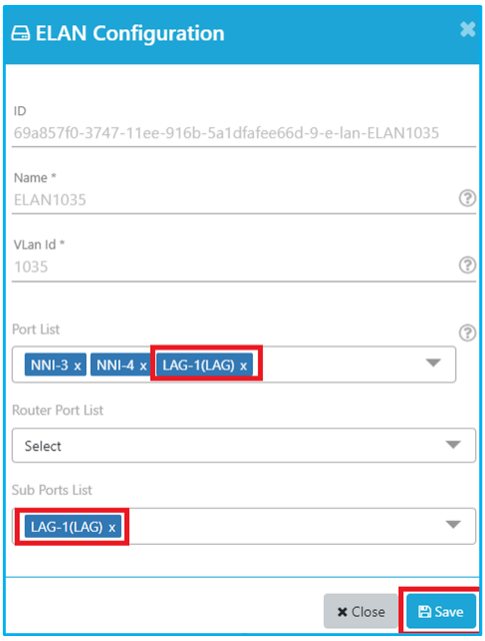
d. Click the **edit** button to update the ELAN1035.

Figure 230. Edit ELAN1035



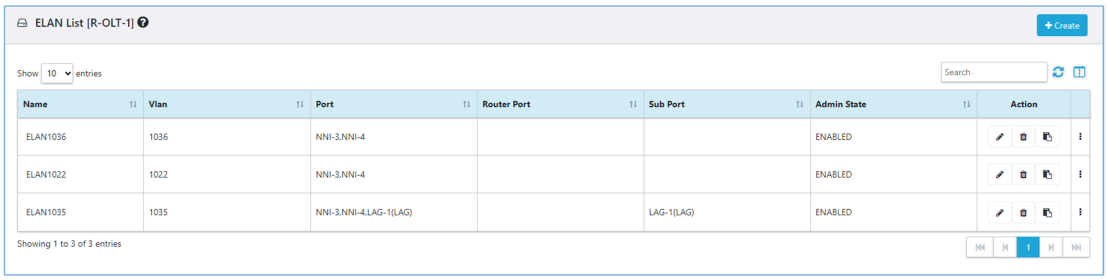
e. Update the ELAN1035 port and sub port with LAG-1, and then click **Save**.

Figure 231. ELAN Configuration



The following screenshot shows the status of the updated ELAN1035 port.

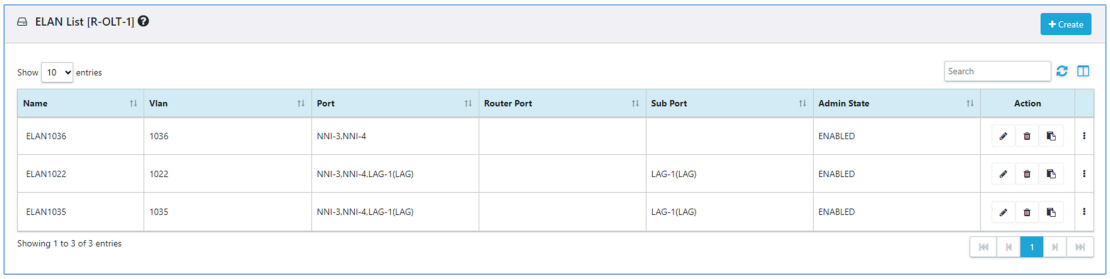
Figure 232. Status of the ELAN1035



f. Repeat the same steps to update the ELAN1022 port and sub port list as LAG-1.

g. Now the ELAN1035 and ELAN1022 port list is NNI-3, NNI-4, and LAG-1 and sub port list is LAG-1.

Figure 233. Status of the ELANs



Example: Subtended OLT (Fresh Install) to Parent OLT with LAG

Overview

This section covers the procedure to subtend fresh OLT to the parent OLT with LAG port using the RMS GUI.

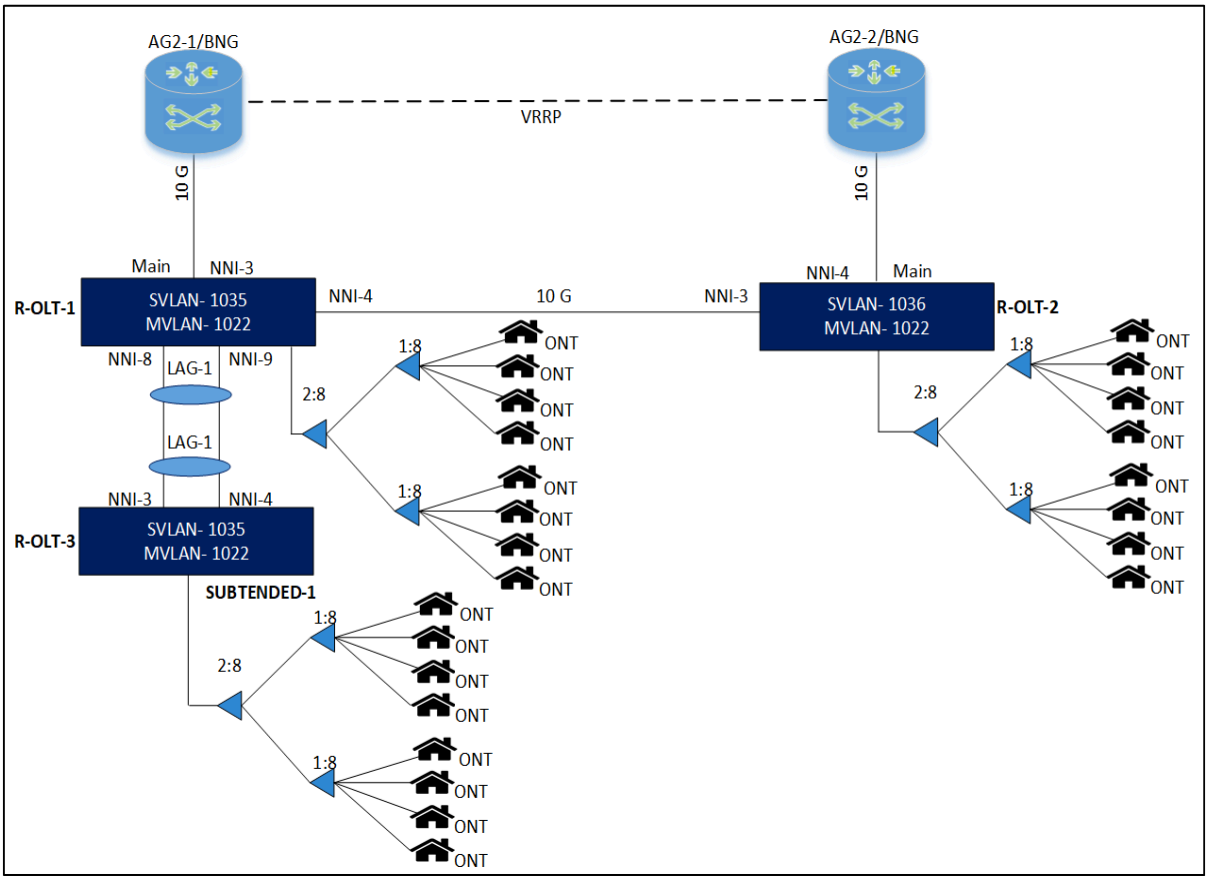
Topology

The following topology diagram shows the configurations and connections between main OLTs when subtended OLT is added freshly.

- R-OLT-1 is main/parent OLT and part of the ring
- R-OLT-2 is part of the ring
- R-OLT-3 is SUBTENDED-1 OLT

Note: It is assumed that the OLTs are installed with 2.10.2/latest version.

Figure 234. Topology



Connecting the SUBTENDED-1 OLT (R-OLT-3) to parent OLT (R-OLT-1) using LAG without impacting the traffic of parent the OLT (R-OLT-1).

Ideal or Expected Case. The traffic must not be impacted to the Main OLT when the ELAN is updated with the SUBTENDED OLT Ports with LAG.

Configuration to Connect the Subtended OLT (R-OLT-3) to the Main OLT (R-OLT-1)

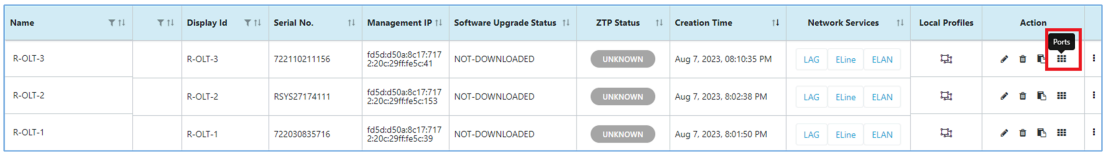
This section covers the procedure to connect the subtended OLT R-OLT-3 to the main OLT R-OLT-1.

1. Connect the SUBTENDED OLT R-OLT-3 to the main OLT R-OLT-1.
2. Activate the NNI ports.

   Perform the following steps to activate the NNI-3 port.

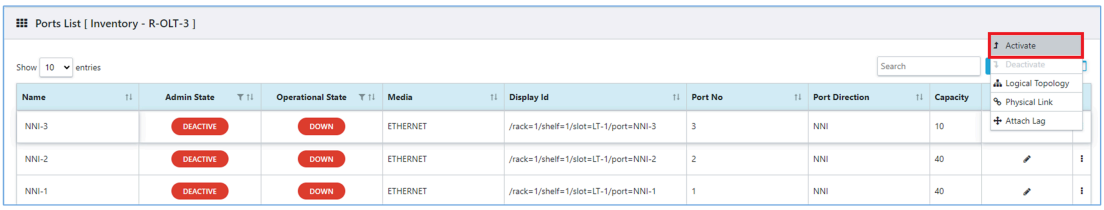
   a. Navigate to **Configuration > Inventory > OLT**.
   b. Click on nine dots.

   Figure 235. OLT



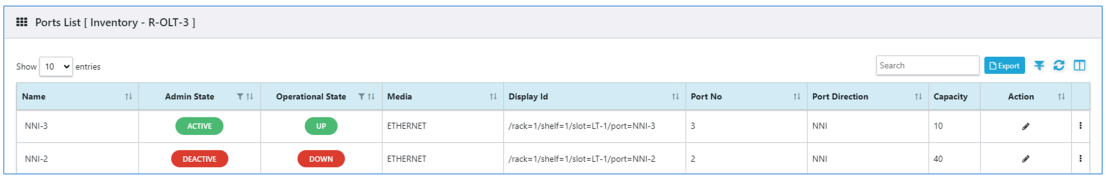
   c. Navigate to the NNI-3 Port
   d. Click on three dots and select the **Activate** option.

   Figure 236. Activate NNI-3 Port



   The following screenshot shows the status after activating the NNI-3 port.

   Figure 237. Status of the NNI-3 Port



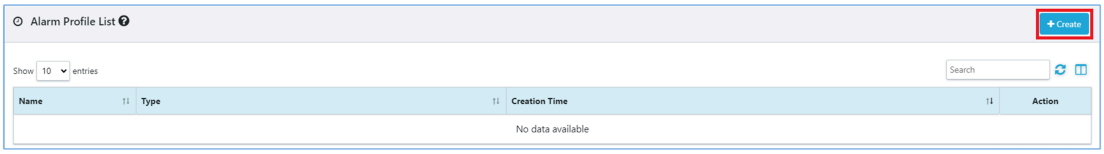
   e. Repeat the same steps to activate the NNI-4 port.
3. Create the LAG and add the member ports.

   Perform the following steps to create the Alarm Profile for the LAG.

   a. Navigate to **Configuration > Profile > Alarm Profile**.
   b. Click **Create**.

The Alarm Profile Configuration page appears.

Figure 238. Create Alarm Profile

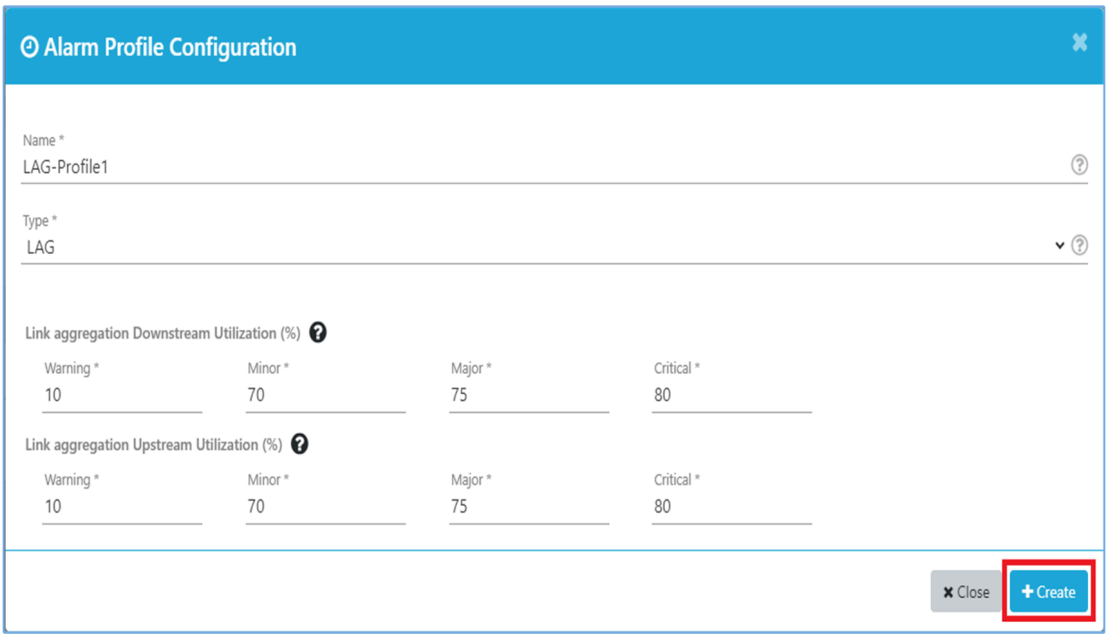


c. Enter the alarm profile configuration and click **Create**.

Note:

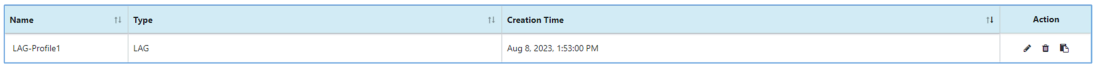
- The space as delimiter is not accepted in the RMS for the profile names.
- Change the utilization values for downstream and upstream from the default to the required value (The minimum and maximum values are set to 60).

Figure 239. Alarm Profile Configuration



The following screenshot shows the status of the alarm profile created for LAG.

Figure 240. Status of the Alarm Profile

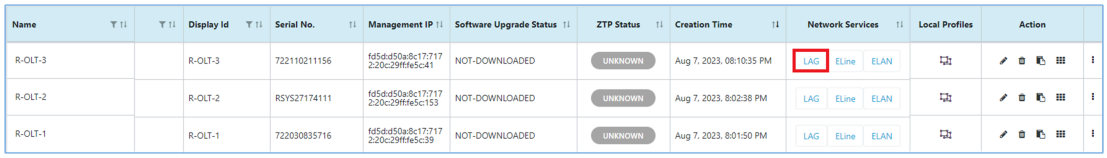


Perform the following steps to create the LAG-1.

a. Navigate to **Configuration > Inventory > OLT**.

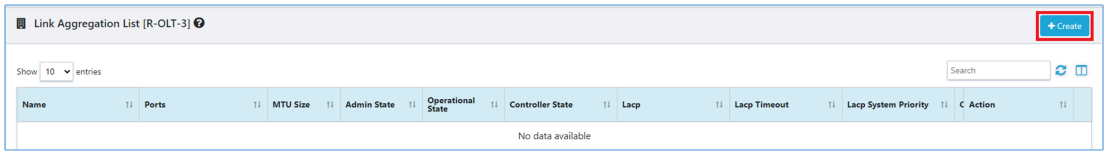
b. Click on the LAG from the **Network Services** column.

Figure 241. LAG



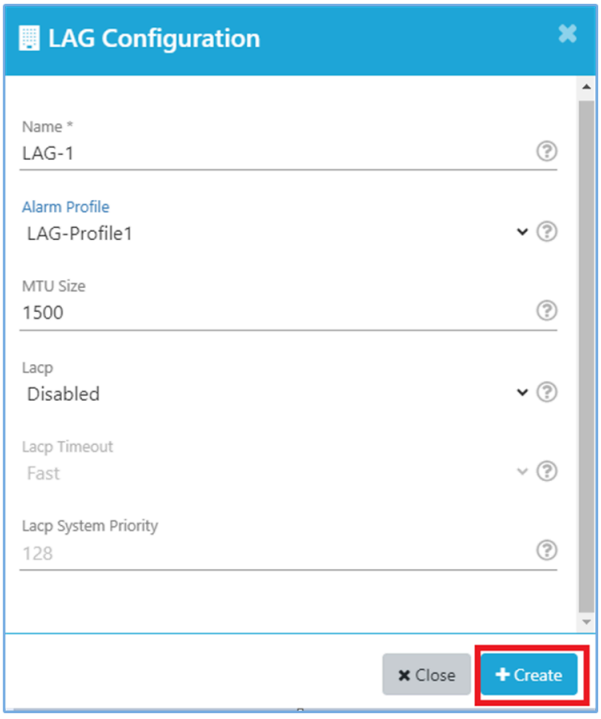
c. Click **Create**.

Figure 242. Create LAG



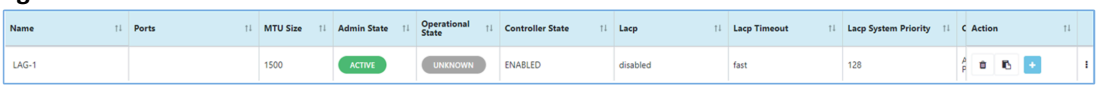
d. Enter the LAG configuration and click **Create**.

Figure 243. LAG Configuration



e. A LAG is created and the administrative state is ACTIVE.

Figure 244. Status of the LAG



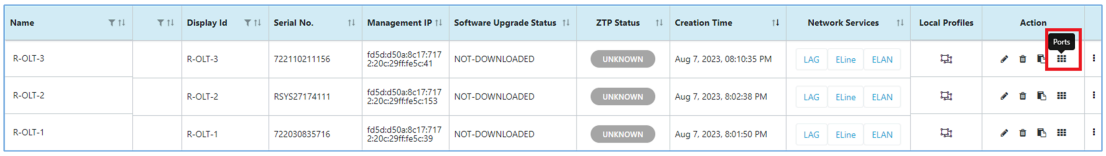
Perform the following steps to associate the NNI-3 and NNI-4 ports to the LAG-1.

Note: When configured, the LAG configuration must only have one active member port. In this scenario, NNI-3 is active and up while NNI-4 is down, and NNI-4 may be active and brought up once the LAG configuration is finished, preventing packet looping.

a. Navigate to **Configuration > Inventory > OLT**.

b. Click on nine dots.

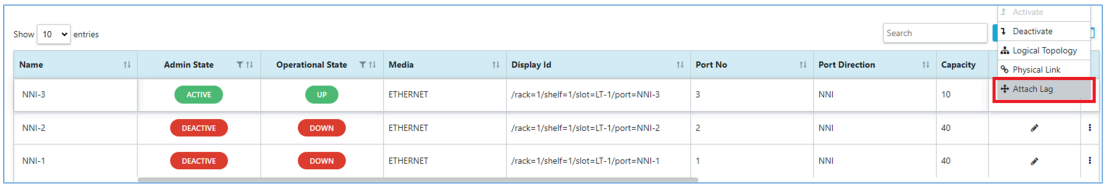
Figure 245. OLT



c. Navigate to the **NNI-3** Port.

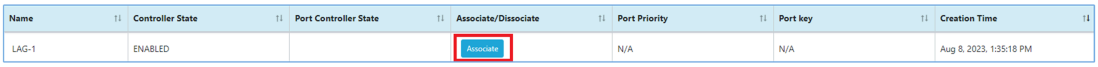
d. Click on three dots and select the **Attach Lag** option.

Figure 246. Attach Lag



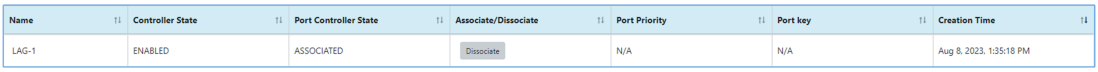
e. Click the **Associate** option from the Associate/Dissociate column.

Figure 247. Associate



The following screenshot shows the associated NNI-3 port to the LAG-1.

Figure 248. Status of the LAG



f. Repeat the same steps to associate NNI-4 port to the LAG-1 port.

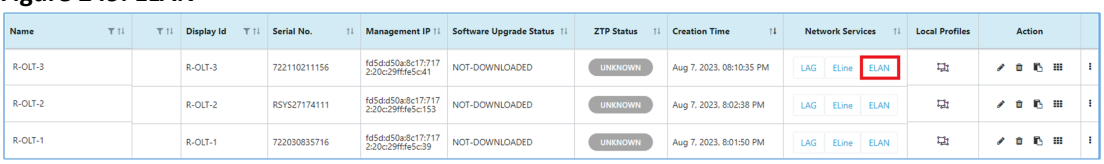
4. Create ELANs with the LAGs.

a. Create ELAN1035 with port list as LAG-1 and enable the ELAN1035.

b. Navigate to **Configuration > Inventory > OLT**.

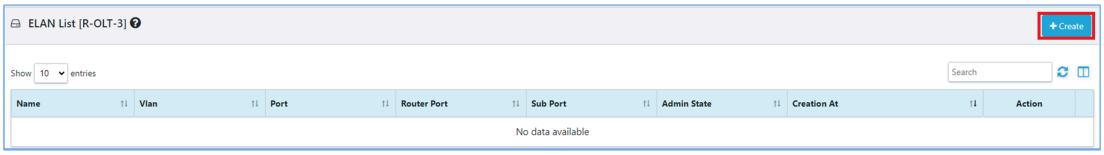
c. Click on the ELAN from the **Network Services** column.

Figure 249. ELAN



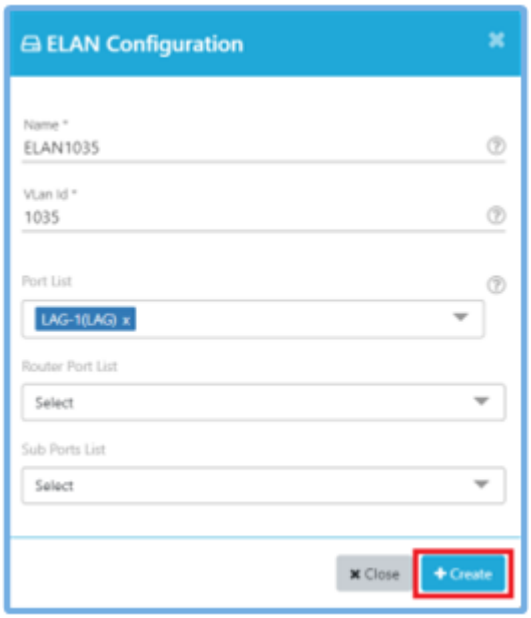
d. Click **Create**.

Figure 250. Create ELAN



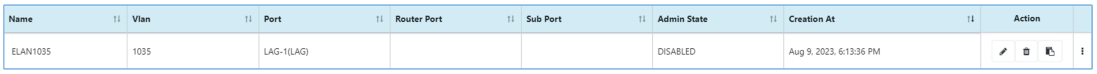
e. Enter the ELAN configuration and click **Create**.

Figure 251. ELAN Configuration



The following screenshot shows the status of the ELAN1035.

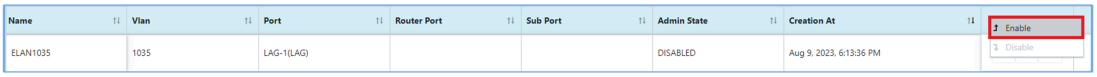
Figure 252. Status of the ELAN1035



Note: The ELAN1035 is in the **Disable** state.

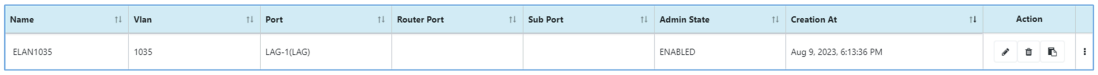
f. Click on three dots and select the **Enable** option to enable the ELAN1035.

Figure 253. Enable ELAN1035



The following screenshot shows the status of the ELAN1035.

Figure 254. Status of the ELAN1035



g. Create the ELAN1022 with port list as LAG-1 and enable the ELAN1022.

Configuration to Connect the Parent OLT (R-OLT-1)

This section covers the procedure to connect the parent OLT R-OLT-1.

1. Navigate to the parent OLT R-OLT-1.
2. Activate the NNI-8 and NNI-9 ports of R-OLT-1 which is connected to R-OLT-3. See step 2 *(on page 174)*.
3. Create the LAG-1 and associate NNI-8 and NNI-9 to the LAG-1. See step 3 *(on page 174)*.

Figure 255. Create LAG-1 and Associate NNI-8 and NNI-9

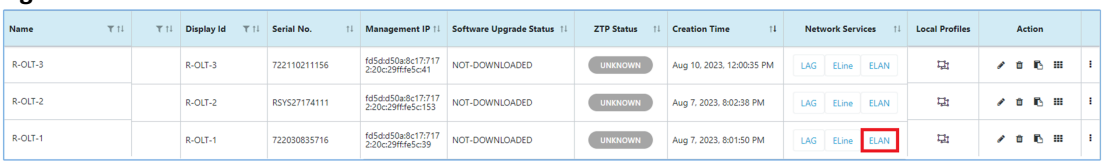
4. Update the ELANs port list and sub-port list with LAG-1.
   a. Update the ELAN1035 with a port list and sub-port list as LAG-1.
   b. Navigate to **Configuration > Inventory > OLT**.

      The OLT page appears.

   c. Click on the ELAN from the **Network Services** column.

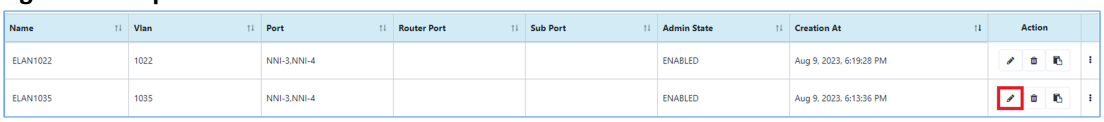
      The ELAN list page appears.

Figure 256. ELAN



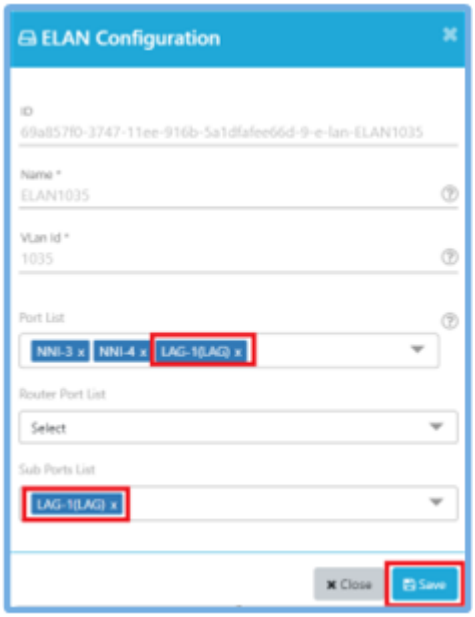
   d. Click the **edit** button to update the ELAN1035.

Figure 257. Update ELAN1035



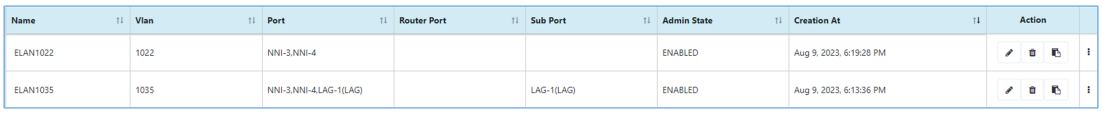
   e. Update the ELAN1035 port and sub port with LAG-1, and then click **Save**.

Figure 258. ELAN Configuration



The following screenshot shows the status of the updated ELAN1035 port.

Figure 259. Status of the ELAN1035

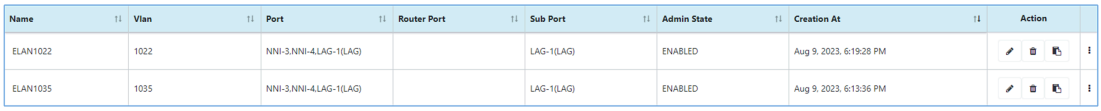


Name	Vlan	Port	Router Port	Sub Port	Admin State	Creation At	Action
ELAN1022	1022	NNI-3,NNI-4			ENABLED	Aug 9, 2023, 6:19:28 PM	
ELAN1035	1035	NNI-3,NNI-4,LAG-1(LAG)		LAG-1(LAG)	ENABLED	Aug 9, 2023, 6:13:36 PM	

f. Repeat the same steps to update the ELAN1022 port and sub port list as LAG-1.

g. Now the ELAN1035 and ELAN1022 port list is NNI-3, NNI-4, and LAG-1 and sub-port list is LAG-1.

Figure 260. Status of the ELANs



Name	Vlan	Port	Router Port	Sub Port	Admin State	Creation At	Action
ELAN1022	1022	NNI-3,NNI-4,LAG-1(LAG)		LAG-1(LAG)	ENABLED	Aug 9, 2023, 6:19:28 PM	
ELAN1035	1035	NNI-3,NNI-4,LAG-1(LAG)		LAG-1(LAG)	ENABLED	Aug 9, 2023, 6:13:36 PM	

Example: Connecting OLT Ring Ports with Eband Device Using Dynamic LAG - Enterprise

Overview

This section covers the procedure to connect the OLT Ring ports with Eband device using dynamic LAG port for enterprise customers using the RMS GUI.

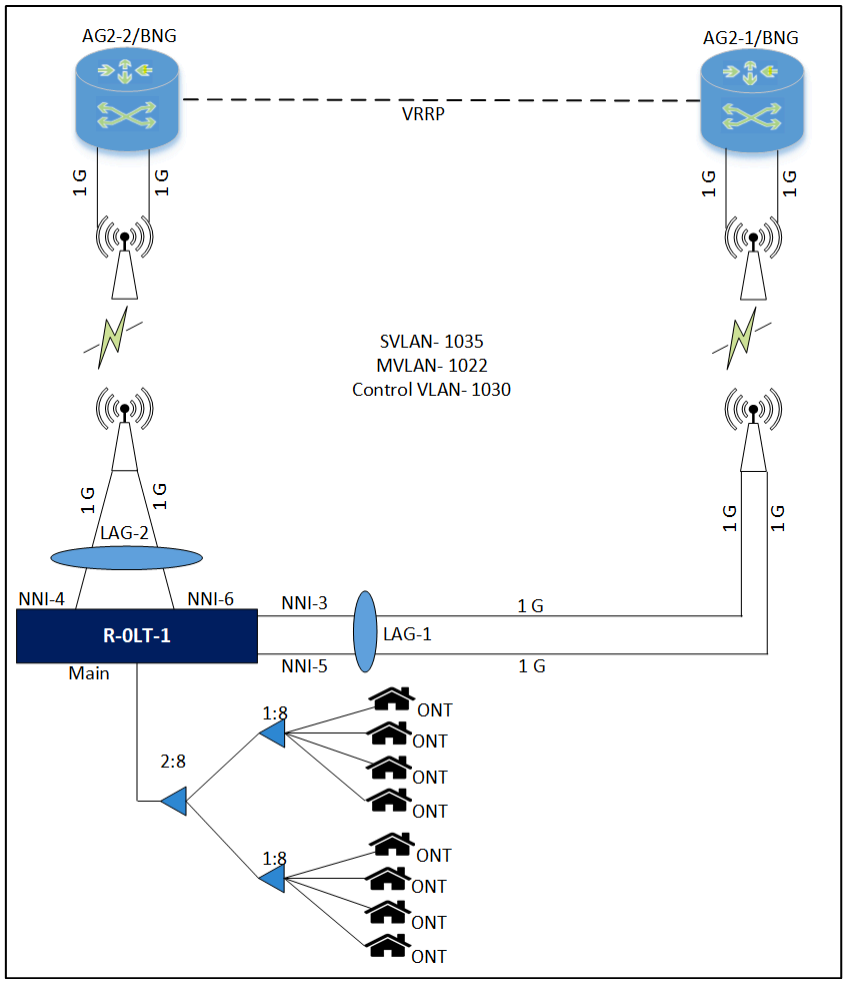
Topology

The following topology diagram shows the configurations and connections between the main OLT and Eband device.

- R-OLT-1 is the main or parent OLT

Note: It is assumed that the OLTs are installed with 2·10·2/latest version.

Figure 261. Topology

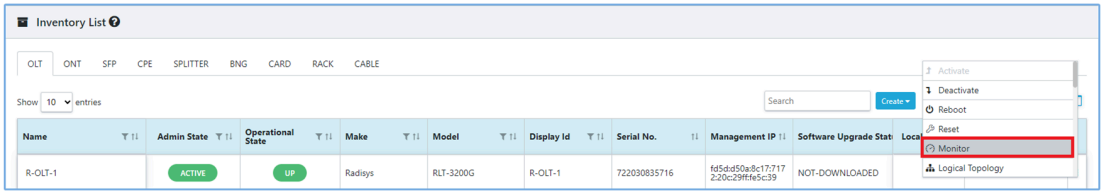


Configuration

This section covers the procedure to connect the OLT with Eband device using dynamic LAG port for enterprise customers for R-OLT-1.

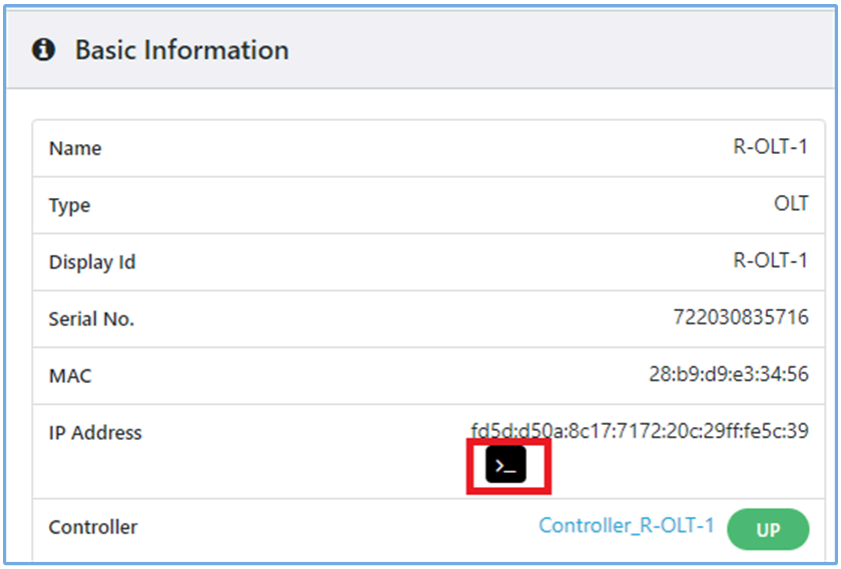
1. Log in to the OLT terminal, edit the `olt_config` file with "*nni_port_speed_1g": [3,4,5,6]* field.
   a. Navigate to **Configuration > Inventory > OLT**.
   b. Click on three dots and select **Monitor**.

Figure 262. OLT Monitor



c. Under the **Basic Information**, click on the terminal in the IP Address.

Figure 263. OLT Basic Information

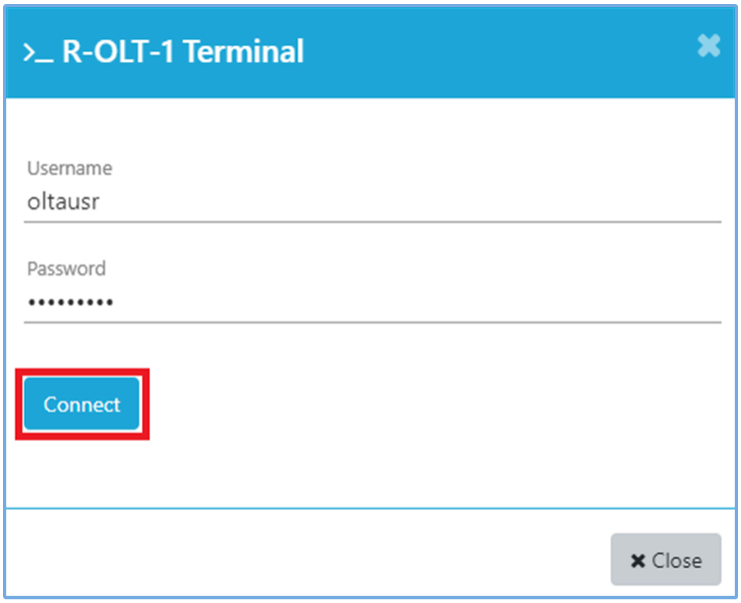


d. Enter the username and password.

e. Click **Connect**.

The OLT Terminal page appears.

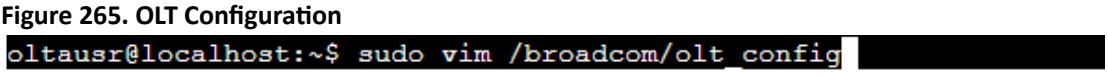
Figure 264. R-OLT-1 Terminal



f. Execute the following command to edit the `olt_config` file.

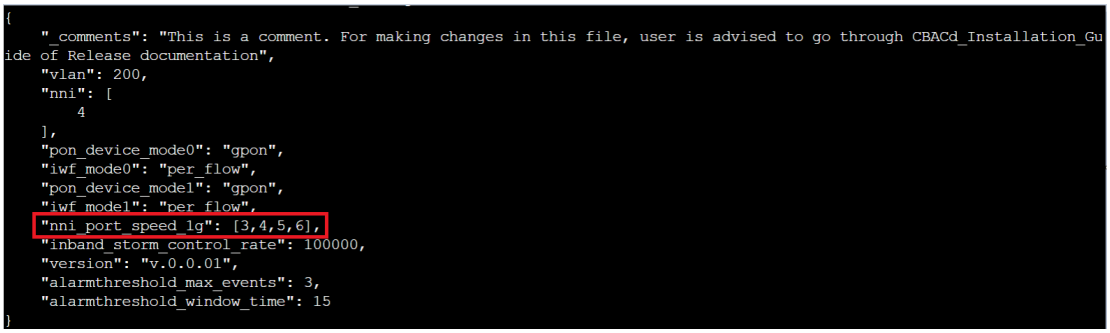
```
sudo vim /broadcom/olt_config
```

Figure 265. OLT Configuration



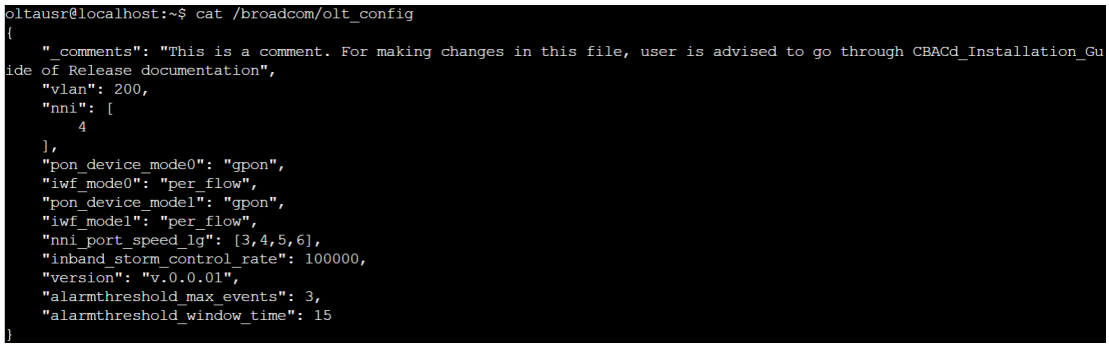
g. Add the *"nni_port_speed_1g": [3,4,5,6]*, field from the `olt_config` file.

Figure 266. NNI Port Speed



h. Status of the `olt_config` file after adding the field.

Figure 267. OLT Configuration File

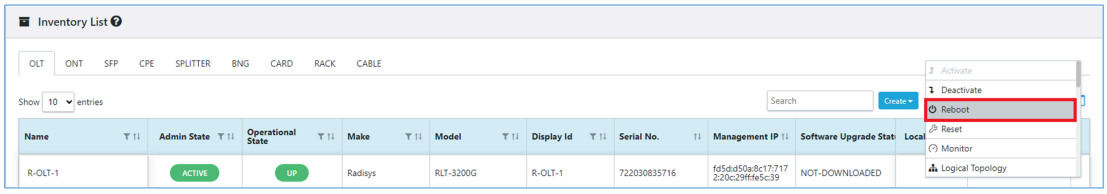


2. Reboot the OLT.

a. Navigate to **Configuration > Inventory > OLT**.

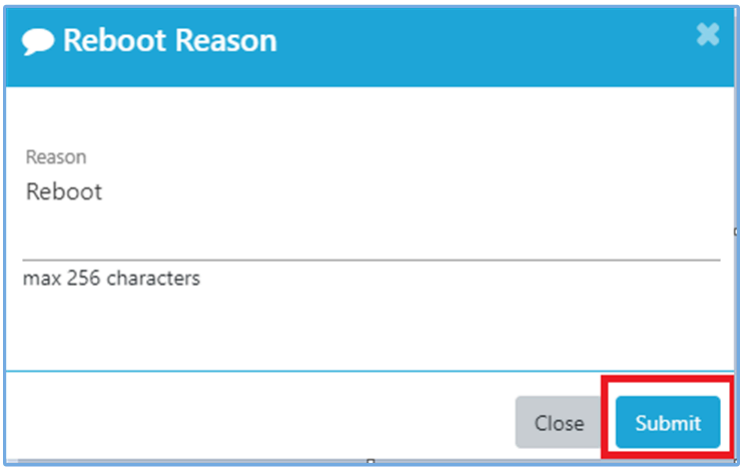
b. Click on three dots and select the **Reboot** option.

Figure 268. OLT Reboot



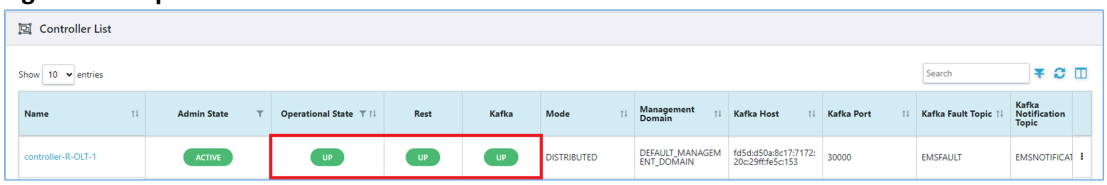
c. Enter the reason for the OLT reboot and click **Submit**.

Figure 269. OLT Reboot Reason



3. Check if the OLT is UP.
   a. Check if the "ME-REBOOTED" event is raised in the **Monitor > Events** page.
   b. Once the "ME-REBOOTED" event is raised, go to **Monitor > Inventory > Controller** and check if the Operational State of Rest and Kafka is UP.

Figure 270. Operational State of Rest and Kafka



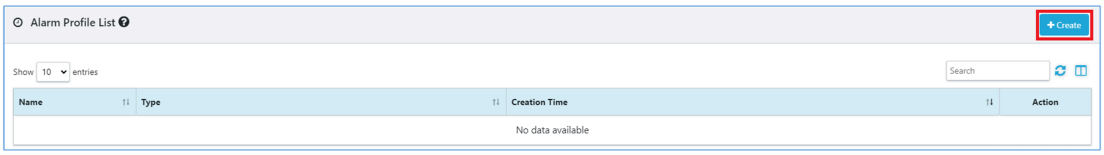
4. Create LAGs with LACP and add the member ports.

   Perform the following steps to create the Alarm Profile for the LAG.

   a. Navigate to **Configuration > Profile > Alarm Profile**.
   b. Click **Create**.

      The Alarm Profile Configuration page appears.

Figure 271. Create Alarm Profile

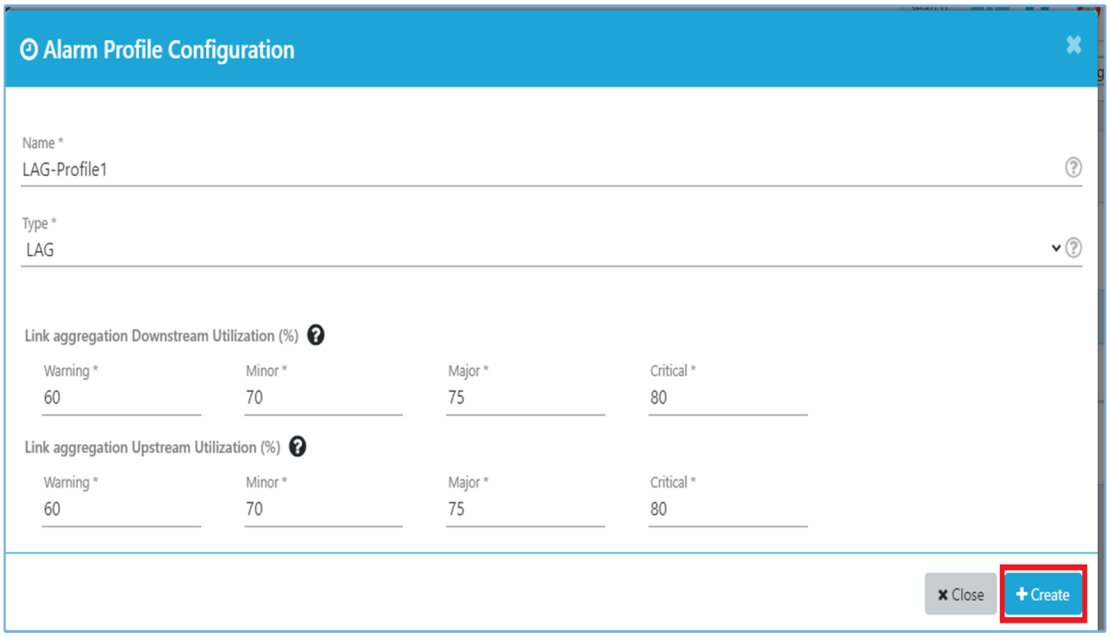


   c. Enter the alarm profile configuration and click **Create**.

Note:

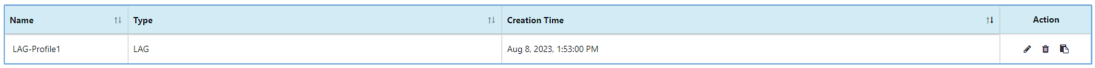
- The space as delimiter is not accepted in RMS for the profile names.
- Change the utilization values for downstream and upstream from the default to the required value (The minimum and maximum values are set to 60).

Figure 272. Alarm Profile Configuration



The following screenshot shows the status of the alarm profile created for LAG.

Figure 273. Status of the Alarm Profile

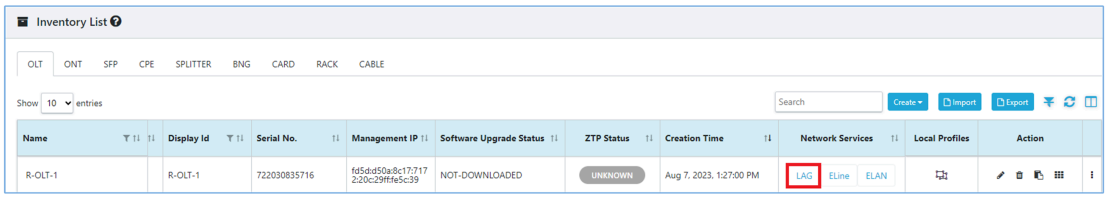


Perform the following steps to create the LAG-2 with LACP as active.

a. Navigate to **Configuration > Inventory > OLT**.

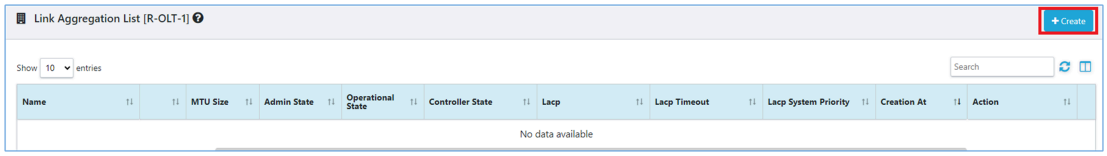
b. Click on the LAG from the **Network Services** column.

Figure 274. LAG



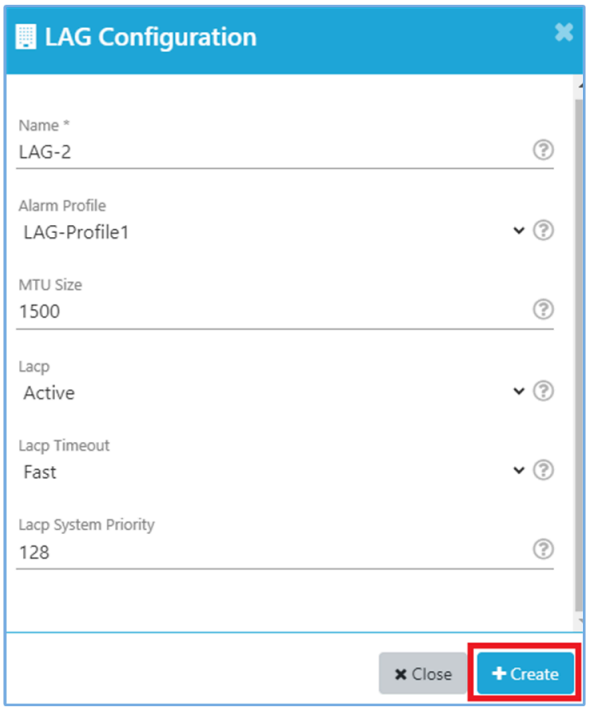
c. Click **Create**.

Figure 275. Create LAG



d. Enter the LAG configuration and click **Create**.

Figure 276. LAG Configuration



Note: LACP timeout must be changed to the required value as per the peer configuration.

e. The LAG-2 is created and the administrative state shows as ACTIVE.

Figure 277. Status of the LAG

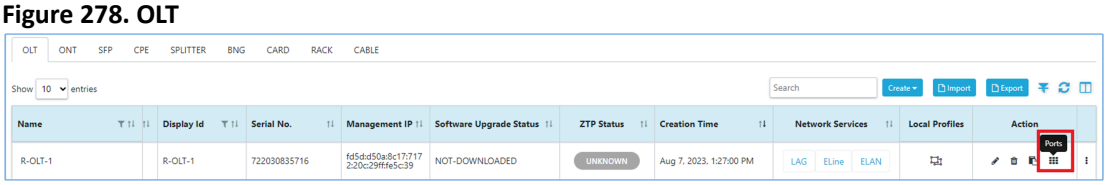
Perform the following steps to associate the NNI-4 port to the LAG-2 port and check for LACP BPDUs.

Note: The IN-BAND NNI port must be added to the LAG port first and NNI-4 port is the IN-BAND NNI Port

a. Navigate to **Configuration > Inventory > OLT**.

b. Click on nine dots.

Figure 278. OLT

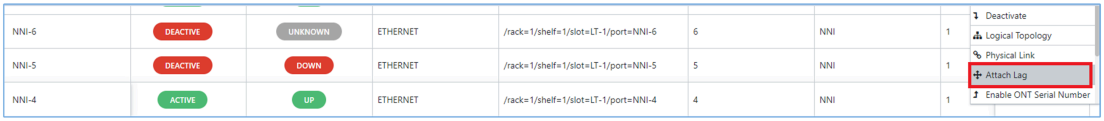


c. Navigate to the **NNI-4** port

Note: When configured, the LAG configuration must only have one active member port. In this scenario, the NNI-4 port is active and up while the NNI-6 port is down. The NNI-6 port maybe active and brought up once the LAG configuration is finished, preventing packet looping.

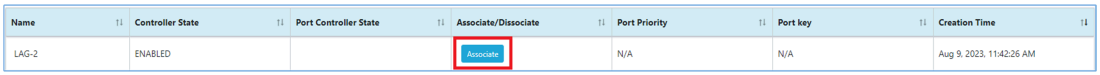
d. Click on three dots and select the **Attach Lag** option.

Figure 279. Attach Lag



e. Click the **Associate** option from the Associate/Dissociate column.

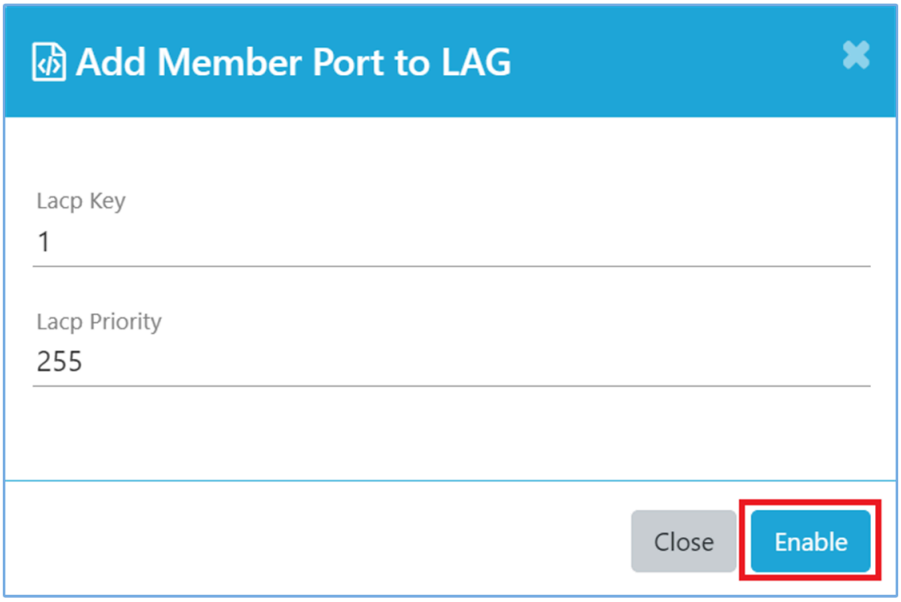
Figure 280. Associate LAG



f. Enter the LACP key and LACP priority and Click **Enable**.

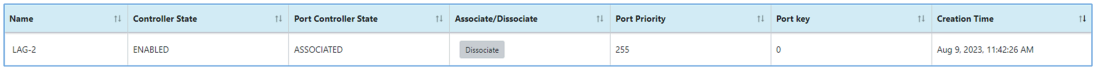
Note: LACP key must be changed to the required value as per the peer configuration.

Figure 281. Add Member Port to LAG



The following screenshot shows the status of the attached NNI-4 port to the LAG-2.

Figure 282. Status of the LAG



g. Log in to the OLT terminal. See Step 1 *(on page 181)*.

h. Execute the following command to check for the LACP BPDUs.

```
sudo tcpdump -x -v -i nni3 (Interface starts from 0, so NNI-4 is NNI-3 here)
```

```
oltausr@localhost:~$ sudo tcpdump -x -v -i nni3
tcpdump: listening on nni3, link-type EN10MB (Ethernet), capture size 262144 bytes
11:39:00.659627 LACPv1, length 110
        Actor Information TLV (0x01), length 20
```

i. Repeat the same steps to associate the NNI-6 port for LAG-2 and check for the LACP BPDUs.

Create the LAG-1 with LACP as active, see Perform the following steps to create the LAG-2 with LACP as active.

- Associate NNI-3 to the LAG-1 and check for LACP BPDUs
- Associate NNI-5 to the LAG-1 and check for LACP BPDUs

5. Create the Ring with the LAGs.

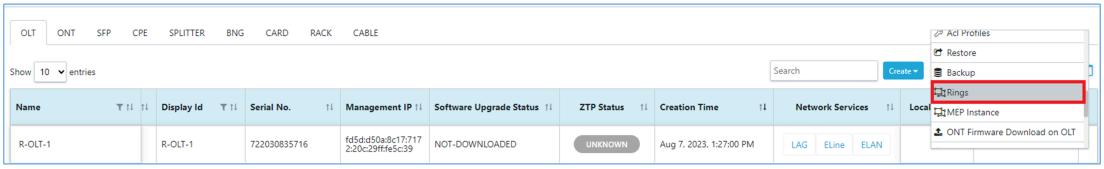
a. Create the Ring with LAG-1 as west port and LAG-2 as east port.

b. Navigate to **Configuration > Inventory > OLT**.

c. Click on three dots and click the **Rings** option.

The Rings page appears.

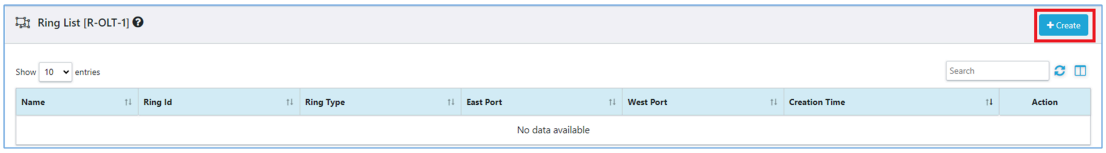
Figure 283. Rings



d. Click **Create**.

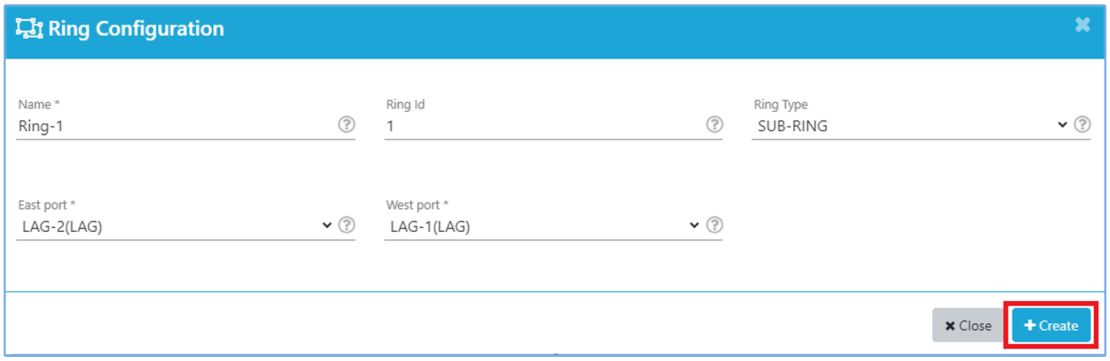
The Ring Configuration page appears.

Figure 284. Create Ring



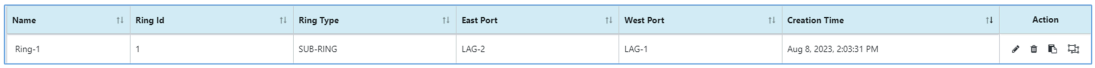
e. Enter the Ring configuration and click **Create**.

Figure 285. Ring Configuration



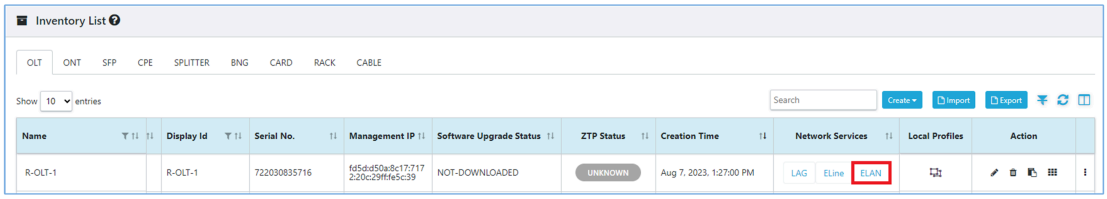
A confirmation message appears indicating the status of the Ring.

Figure 286. Status of the Ring



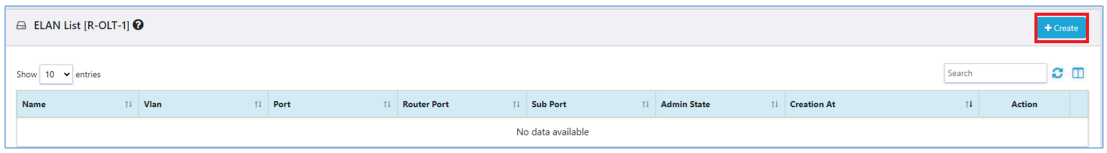
6. Create ELANs with the LAGs.
   a. Create ELAN1035 with port list as LAG-1 and LAG-2 and enable the ELAN1035.
   b. Navigate to **Configuration > Inventory > OLT**.
   c. Click on the ELAN from the **Network Services** column.

Figure 287. ELAN



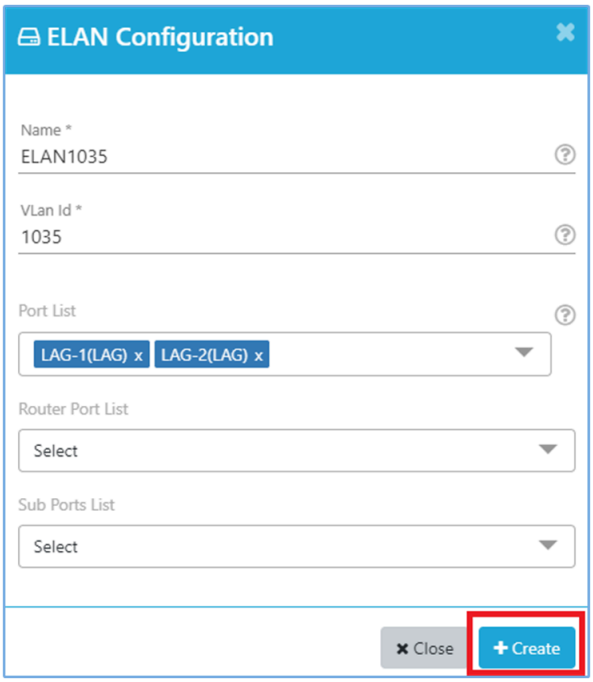
   d. Click **Create**.

Figure 288. Create ELAN



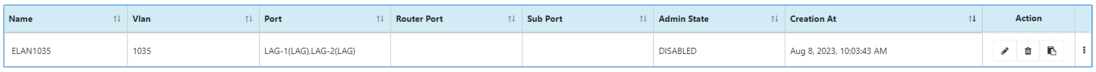
   e. Enter the ELAN configuration and click **Create**.

Figure 289. ELAN Configuration



The following screenshot shows the status of the ELAN1035.

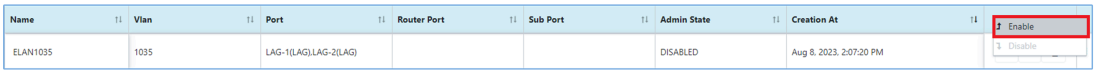
Figure 290. Status of the ELAN1035



Note: The ELAN1035 is in the Disable state.

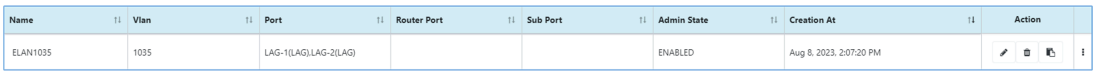
f. Click on three dots and select **Enable** option to enable the ELAN1035.

Figure 291. Enable ELAN1035



The following screenshot shows the status of the ELAN1035.

Figure 292. Status of the ELAN1035



g. Repeat the same steps to create the ELAN1022 with port list as LAG-1 and LAG-2 and enable the ELAN1022.

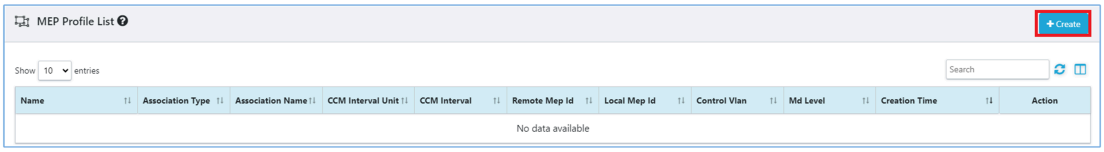
h. Repeat the same steps to create the ELAN1030 with port list as LAG-1 and LAG-2 and enable the ELAN1030.

7. Create the MEP profile.

a. Navigate to **Configuration > Profile > MEP Profile**.

b. Click **Create**.

Figure 293. Create MEP Profile

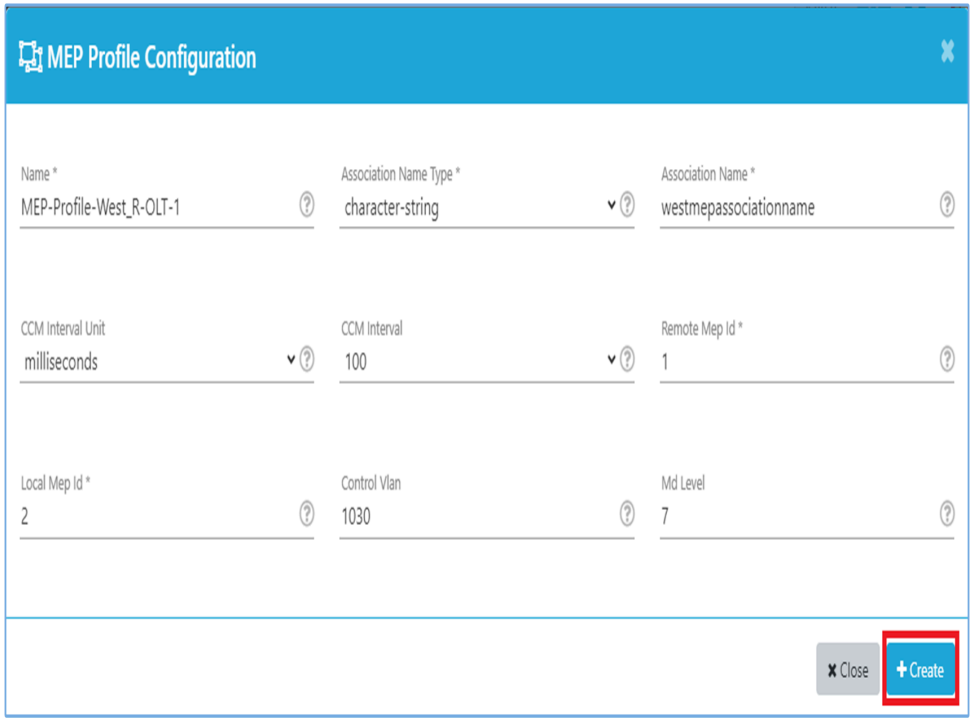


c. Enter the MEP profile configuration and click **Create**.

Note:

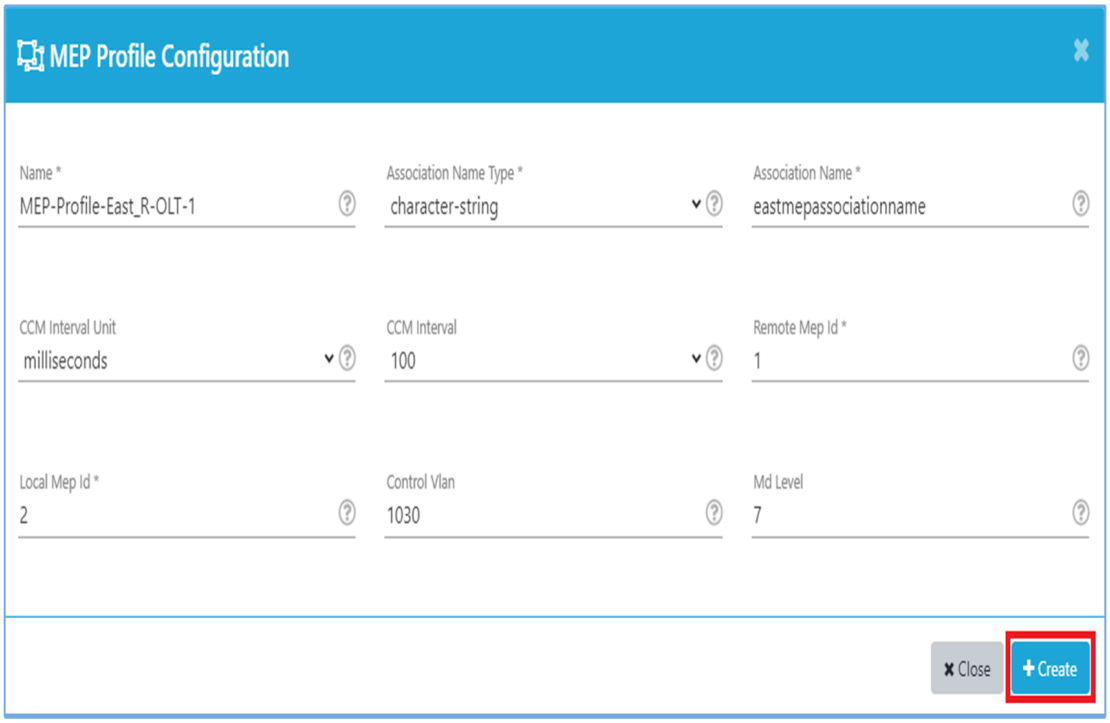
- Change the Association Name, Remote Mep Id, and Local Mep Id values from the default values to the required values as per the peer configuration (EBAND Device).
  - The "Remote Mep Id" must be same as the value given as "Local Mep Id" in the remote device.
  - The "Remote Mep Id" must be same as the value given as "Local Mep Id" in the remote device.
  - The "Local Mep Id" should be same as the value given as "Remote Mep Id" in the remote device.
- The space as delimiter is not accepted in RMS for the profile names.

Figure 294. MEP Profile Configuration



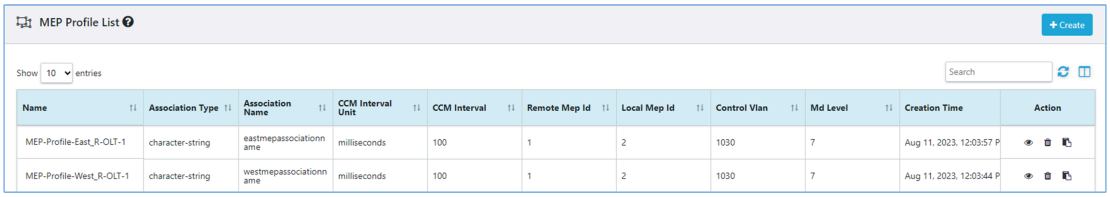
d. Repeat the same steps to create MEP-Profile-East_R-OLT-1.

Figure 295. MEP Profile Configuration



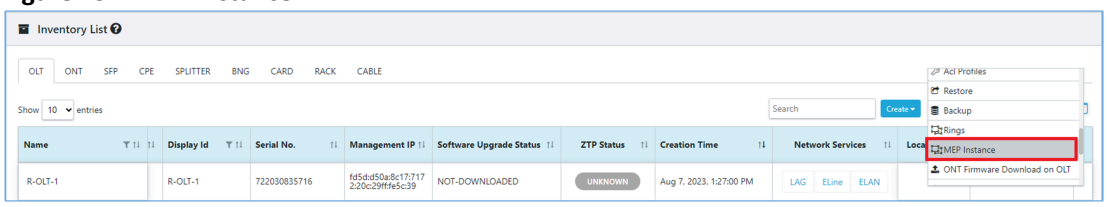
The following screenshot shows the status of the MEP profiles.

Figure 296. Status of the MEP Profiles



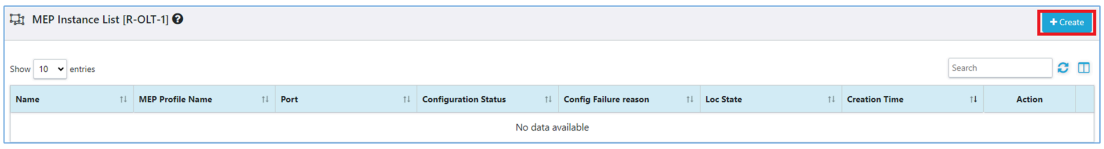
8. Create the MEP instance.
   a. Navigate to **Configuration > Inventory > OLT**.
   b. Click on three dots and select the **MEP Instance**.

Figure 297. MEP Instance



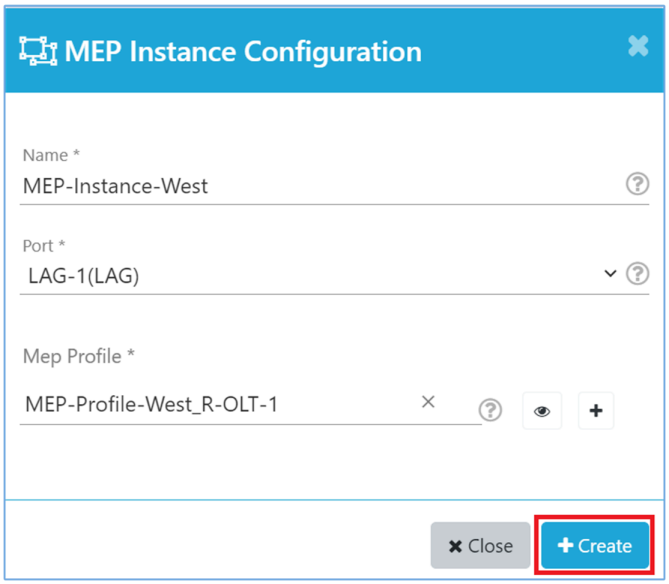
   c. Click **Create**.

Figure 298. Create MEP Instance



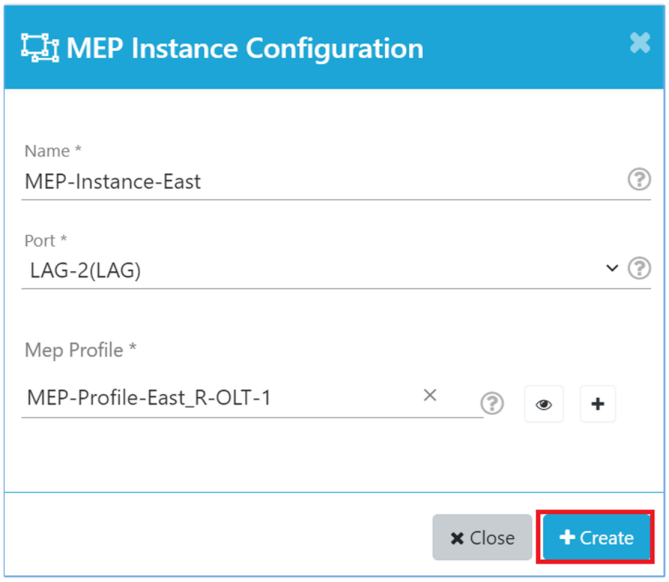
d. Enter the MEP instance configuration (use the previously used MEP Profile) and click **Create**.

Figure 299. MEP Instance Configuration - West



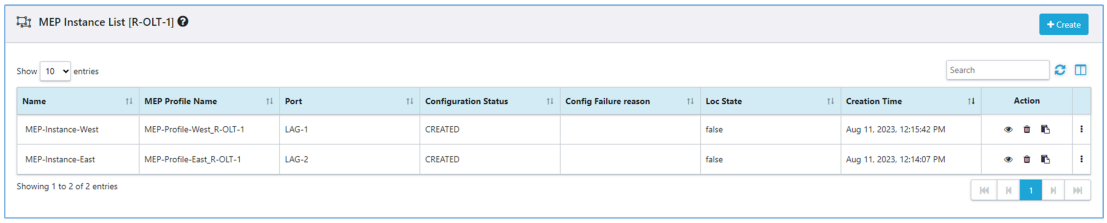
e. Repeat the same steps to create another MEP instance configuration.

Figure 300. MEP Instance Configuration - East



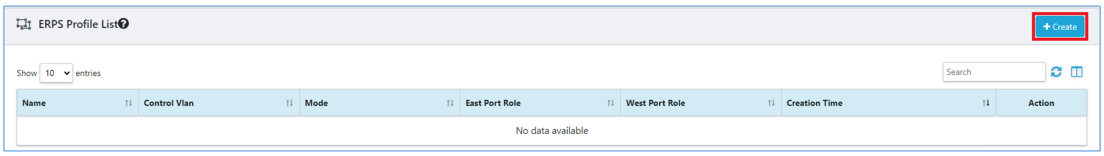
The following screenshot shows the status of the MEP instances.

Figure 301. Status of the MEP Instances



9. Create the ERPS profile.
   a. Navigate to **Configuration > Profile > ERPS Profile**.
   b. Click **Create**.

Figure 302. Create ERPS Profile

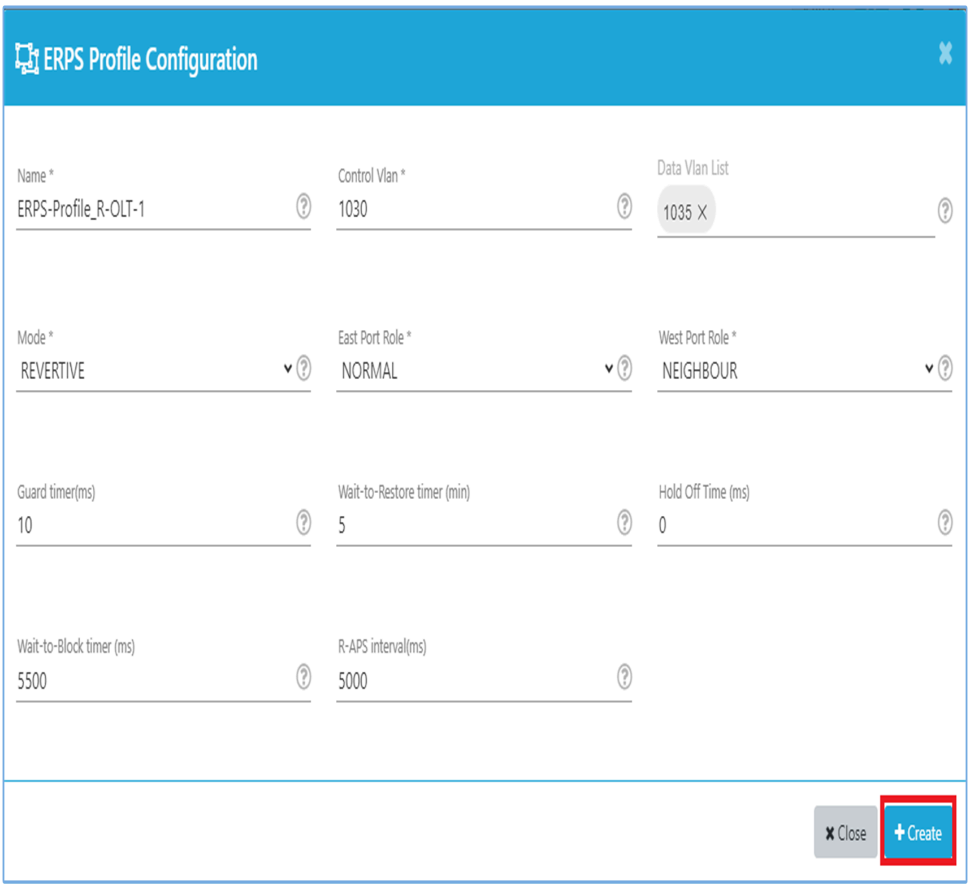


   c. Enter ERPS profile configurations and click **Create**.

Note:

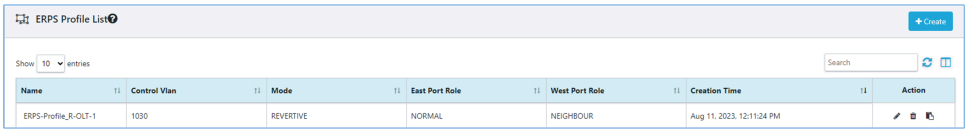
- Change the Guard, Wait-to-Restore, Hold Off, Wait-to-Block, and R-APS interval values from the default to the required values (Match the values provided at BNG side).
- The space as delimiter is not accepted in RMS for the profile names.

Figure 303. ERPS Profile Configuration



The following screenshot shows the status of the ERPS profile.

Figure 304. Status of the ERPS Profile

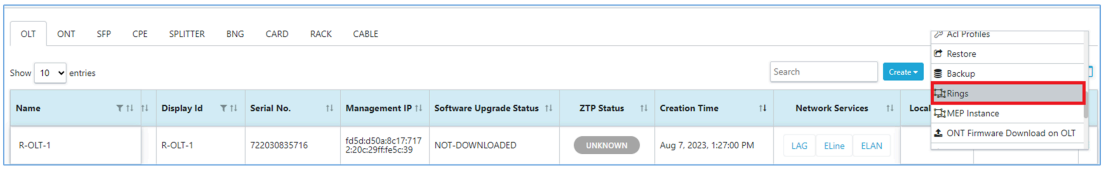


10. Create the ERPS instance.

a. Navigate to **Configuration > Inventory > OLT**.

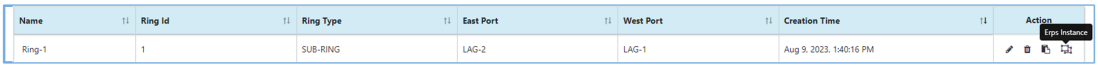
b. Click on three dots and select **Rings**.

Figure 305. Rings



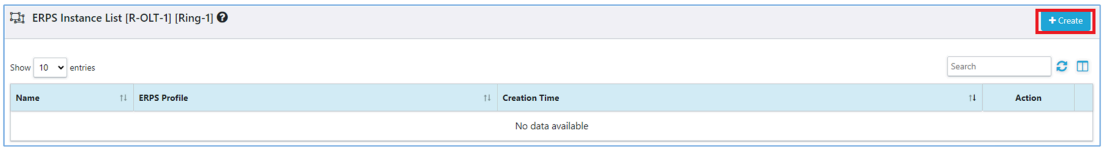
c. Click on the **ERPS Instance** from the **Action** column.

Figure 306. ERPS Instance



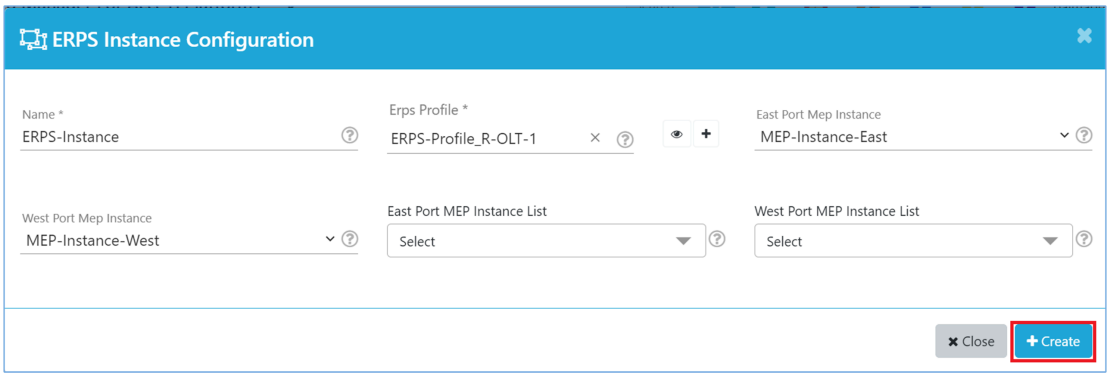
d. Click **Create**.

Figure 307. Create ERPS Instance



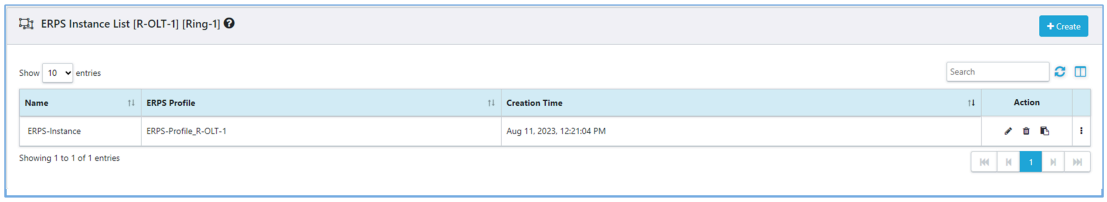
e. Enter ERPS instance configurations and click **Create**.

Figure 308. ERPS Instance Configuration



The following screenshot shows the status of the ERPS instance.

Figure 309. Status of the ERPS Instance



Navigate to **Monitor > Events** page and check for the "CREATE-ERPS-INSTANCE-SUCCESSFUL" event.

Note: Add the service configuration and check if the traffic is running.

Example: Connecting OLT Ring Ports with Eband Device Using Dynamic LAG - Residential

Overview

This section covers the procedure to connect the OLT Ring ports with Eband device using dynamic LAG for residential customers using the RMS GUI.

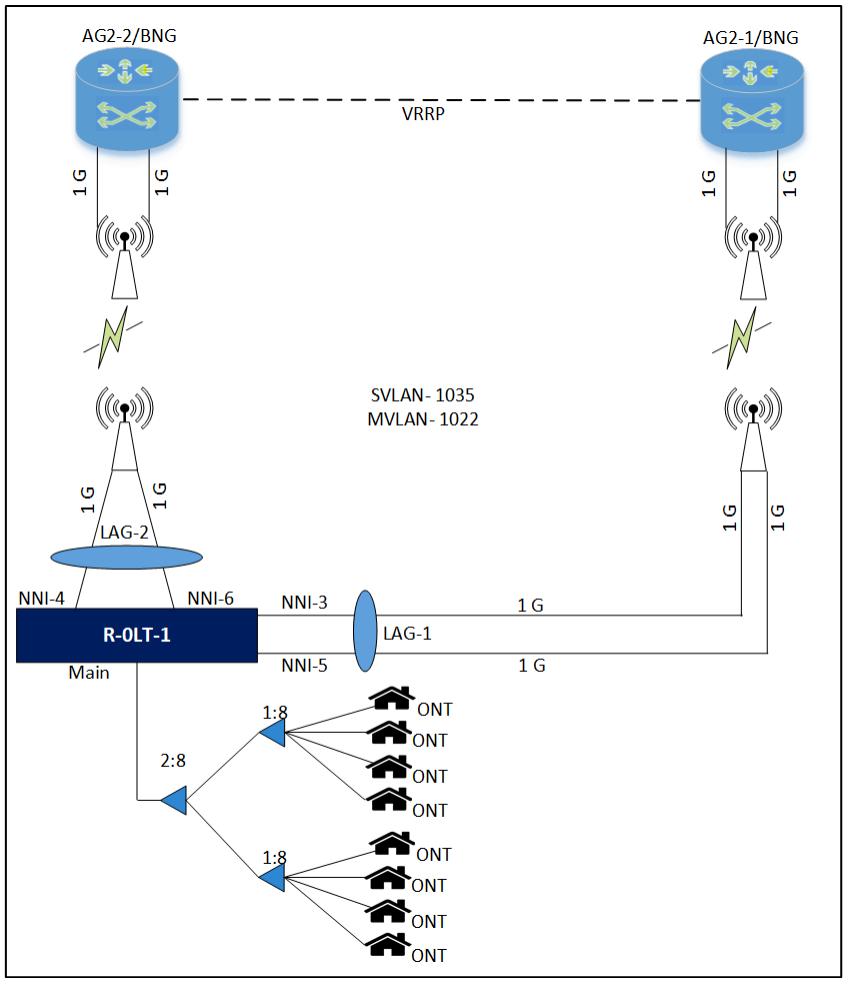
Topology

The following topology diagram shows the configurations and connections between the main OLT and Eband device.

- R-OLT-1 is the main or parent OLT

Note: It is assumed that the OLTs are installed with 2.10.2/latest version.

Figure 310. Topology

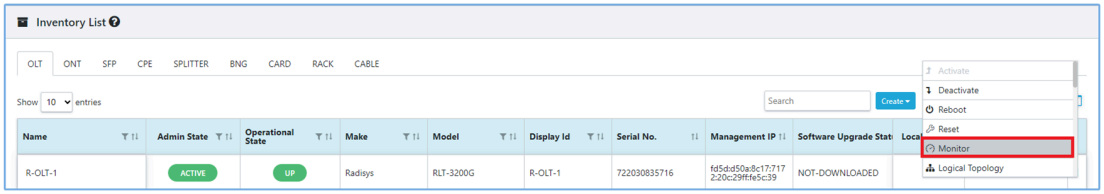


Configuration

This section covers the procedure to connect the OLT with Eband device using dynamic LAG port for residential customers for R-OLT-1.

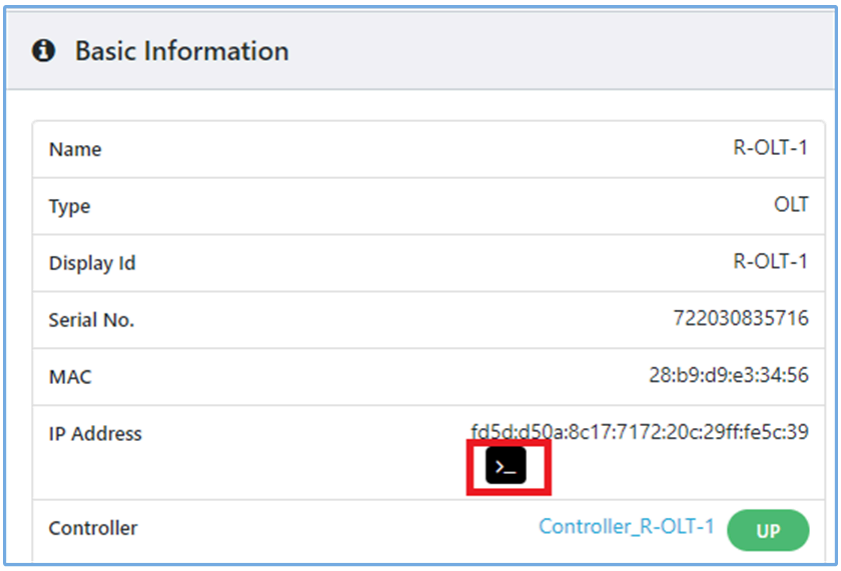
1. Log in to the OLT terminal, edit the `olt_config` file with *"nni_port_speed_1g": [3,4,5,6]* field.
   a. Navigate to **Configuration > Inventory > OLT**.
   b. Click on three dots and select **Monitor**.

Figure 311. OLT Monitor



   c. Under the **Basic Information**, click on the terminal in the IP Address.

Figure 312. OLT Basic Information

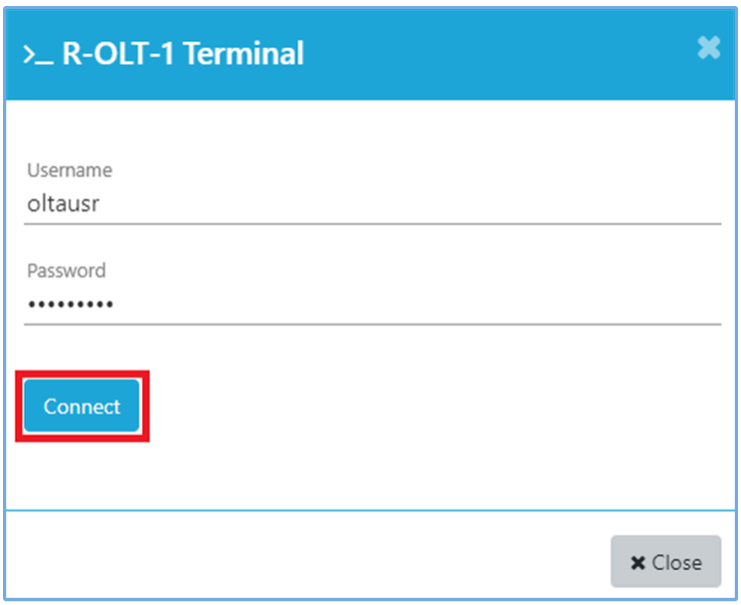


d. Enter the username and password.

e. Click **Connect**.

The OLT Terminal page appears.

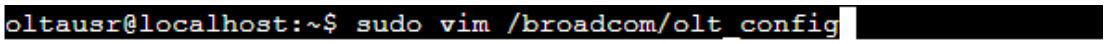
Figure 313. R-OLT-1 Terminal



f. Execute the following command to edit the `olt_config` file.

```
sudo vim /broadcom/olt_config
```

Figure 314. OLT Configuration File



g. Add the *"nni_port_speed_1g": [3,4,5,6]*, field from the `olt_config` file.

Figure 315. NNI Port Speed


```
{
    "_comments": "This is a comment. For making changes in this file, user is advised to go through CBACd_Installation_Gu
ide of Release documentation",
    "vlan": 200,
    "nni": [
        4
    ],
    "pon_device_mode0": "gpon",
    "iwf_mode0": "per_flow",
    "pon_device_mode1": "gpon",
    "iwf_mode1": "per_flow",
    "nni_port_speed_1g": [3,4,5,6],
    "inband_storm_control_rate": 100000,
    "version": "v.0.0.01",
    "alarmthreshold_max_events": 3,
    "alarmthreshold_window_time": 15
}
```


h. Status of the `olt_config` file after adding the field.

Figure 316. Status of the OLT Configuration File

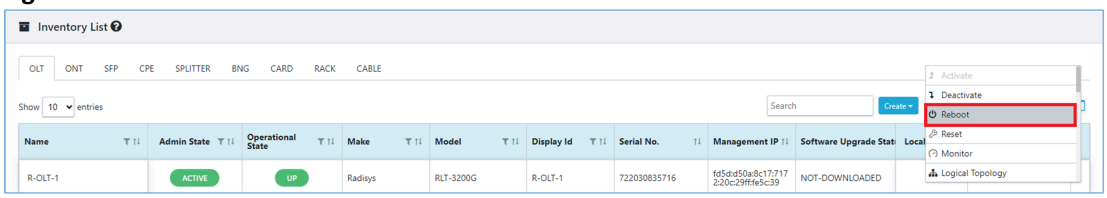

```
oltausr@localhost:~$ cat /broadcom/olt_config
{
    "_comments": "This is a comment. For making changes in this file, user is advised to go through CBACd_Installation_Gu
ide of Release documentation",
    "vlan": 200,
    "nni": [
        4
    ],
    "pon_device_mode0": "gpon",
    "iwf_mode0": "per_flow",
    "pon_device_mode1": "gpon",
    "iwf_mode1": "per_flow",
    "nni_port_speed_1g": [3,4,5,6],
    "inband_storm_control_rate": 100000,
    "version": "v.0.0.01",
    "alarmthreshold_max_events": 3,
    "alarmthreshold_window_time": 15
}
```


2. Reboot the OLT.

a. Navigate to **Configuration > Inventory > OLT**.

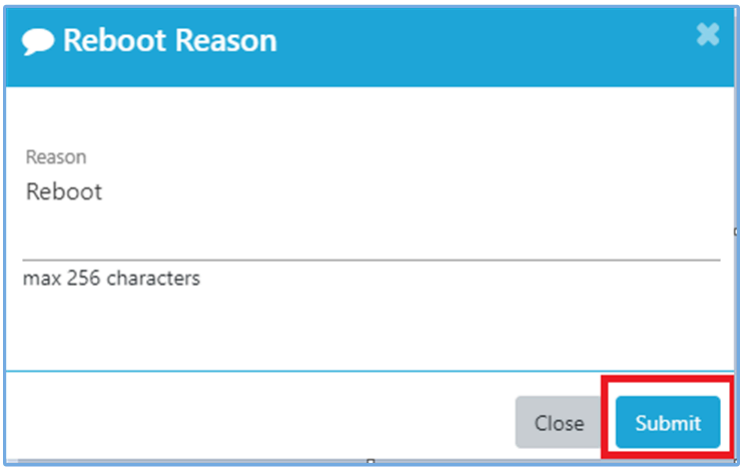
b. Click on three dots and select the **Reboot** option.

Figure 317. OLT Reboot



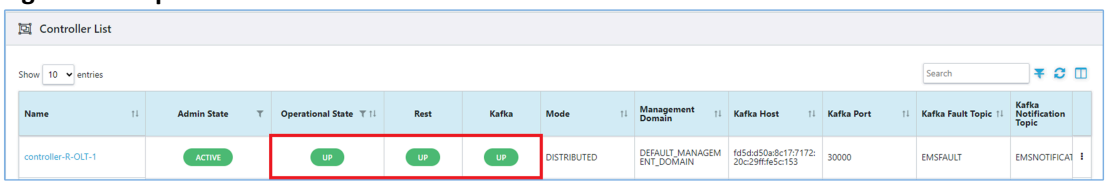
c. Enter the reason for the OLT reboot and click **Submit**.

Figure 318. OLT Reboot Reason



3. Check if the OLT is UP.
   a. Check if the "ME-REBOOTED" event is raised in the **Monitor > Events** page.
   b. Once the "ME-REBOOTED" event is raised, go to **Monitor > Inventory > Controller** and check if the Operational State of Rest and Kafka is UP.

Figure 319. Operational State of Rest and Kafka



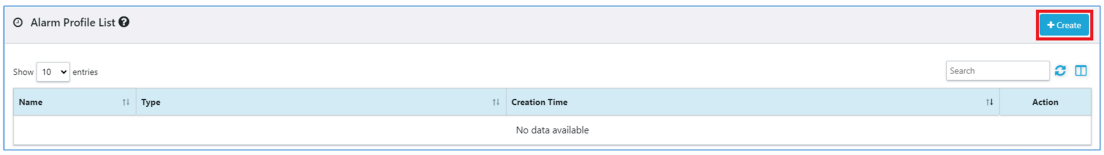
4. Create LAGs with LACP and add the member ports.

   Perform the following steps to create the Alarm Profile for the LAG.

   a. Navigate to **Configuration > Profile > Alarm Profile**.
   b. Click **Create**.

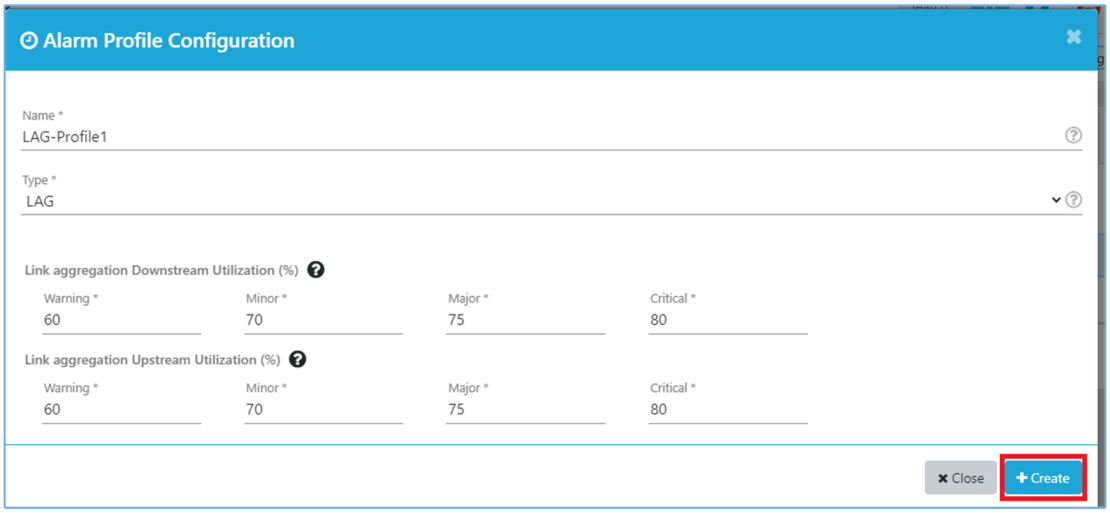
      The Alarm Profile Configuration page appears.

Figure 320. Create Alarm Profile



   c. Enter the alarm profile configuration and click **Create**.

Figure 321. Alarm Profile Configuration

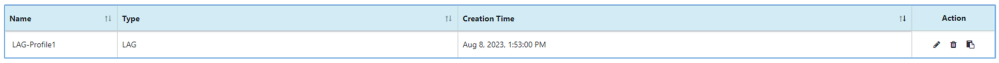


The following screenshot shows the status of the alarm profile created for LAG.

Note:

- The space as delimiter is not accepted in RMS for the profile names.
- Change the utilization values for downstream and upstream from the default to the required value (The minimum and maximum values are set to 60).

Figure 322. Status of the Alarm Profile

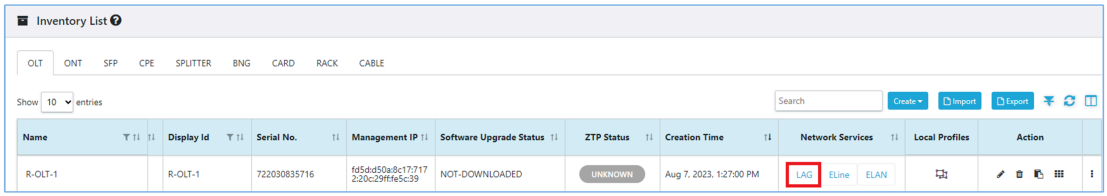


Perform the following steps to create the LAG-2 with LACP as active.

a. Navigate to **Configuration > Inventory > OLT**.

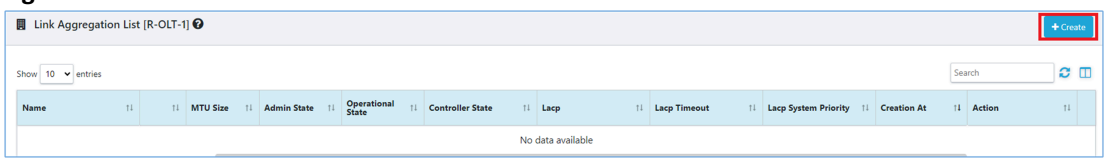
b. Click on the LAG from the **Network Services** column.

Figure 323. LAG



c. Click **Create**.

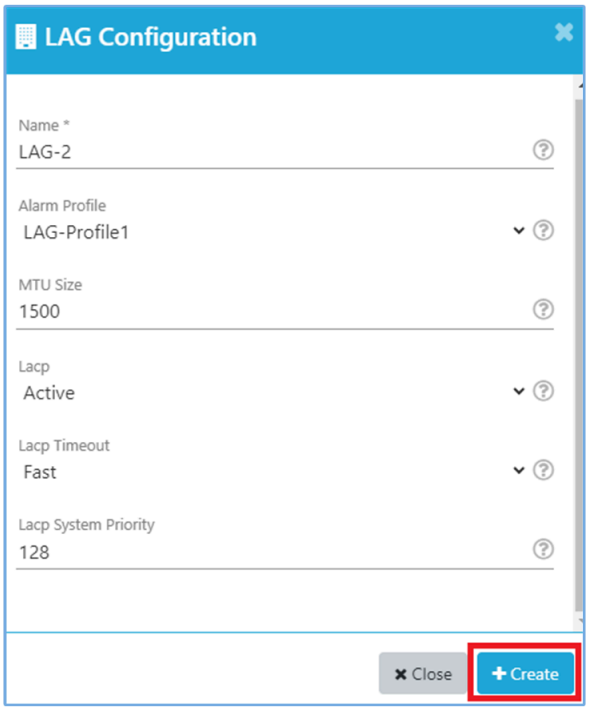
Figure 324. Create LAG



d. Enter the LAG configuration and click **Create**.

Note: LACP timeout must be changed to the required value as per the peer configuration.

Figure 325. LAG Configuration



e. The LAG-2 is created and the administrative state shows as ACTIVE.

Figure 326. Status of the LAG

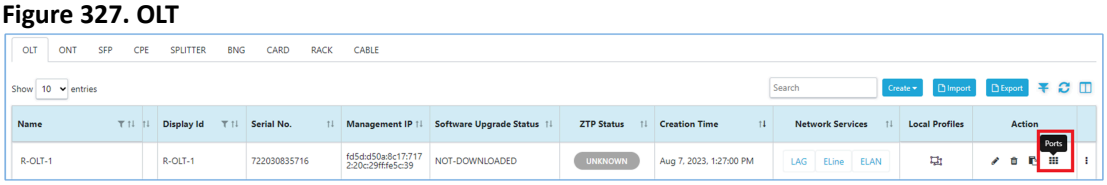
Perform the following steps to associate NNI-4 port to the LAG-2 port and check for LACP BPDUs.

Note: The IN-BAND NNI port must be added to the LAG first and NNI-4 is the IN-BAND NNI Port.

a. Navigate to **Configuration > Inventory > OLT**.

b. Click on nine dots.

Figure 327. OLT

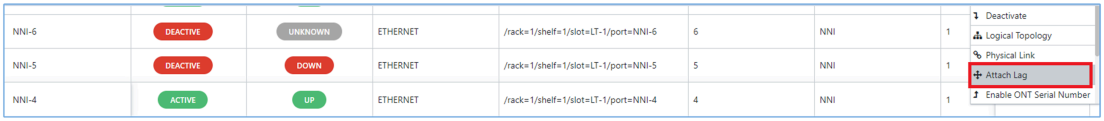


c. Navigate to the **NNI-4** port.

Note: When configured, the LAG configuration must only have one active member port. In this scenario, NNI-4 port is active and up while NNI-6 port is down, and NNI-6 port may be active and brought up once the LAG configuration is finished, preventing packet looping.

d. Click on three dots and select the **Attach Lag** option.

Figure 328. Attach Lag

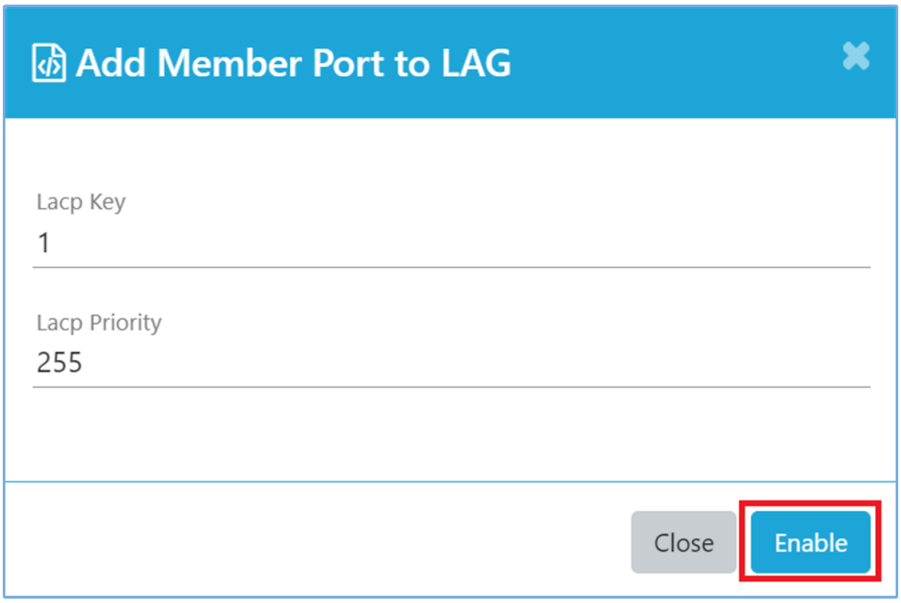


e. Click the **Associate** option from the Associate/Dissociate column.

Figure 329. Associate LAG

f. Enter the LACP key and LACP priority and Click **Enable**.

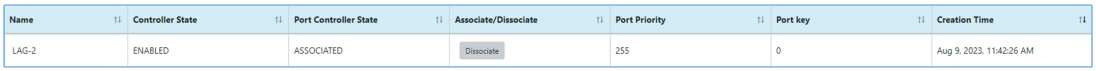
Figure 330. Add Member Port to LAG



Note: LACP key must be changed to the required value as per the peer configuration.

The following screenshot shows the status of the attached NNI-4 port to the LAG-2 port.

Figure 331. Status of the LAG



g. Log in to the OLT terminal. See step 1 *(on page 197)*.

h. Execute the following command to check for the LACP BPDUs.

```
sudo tcpdump -x -v -i nni3 (Interface starts from 0, so NNI-4 is NNI-3 here)
```

Figure 332. Command to check the LACP BPDUs

```
oltausr@localhost:~$ sudo tcpdump -x -v -i nni3
tcpdump: listening on nni3, link-type EN10MB (Ethernet), capture size 262144 bytes
11:39:00.659627 LACPv1, length 110
        Actor Information TLV (0x01), length 20
```

i. Repeat the same steps to associate the NNI-6 port for LAG-2 port and check for the LACP BPDUs.

Create the LAG-1 with LACP as active. See Perform the following steps to create the LAG-2 with LACP as active.

- Associate NNI-3 to the LAG-1 and check for LACP BPDUs
- Associate NNI-5 to the LAG-1 and check for LACP BPDUs

5. Create the Ring with the LAGs.

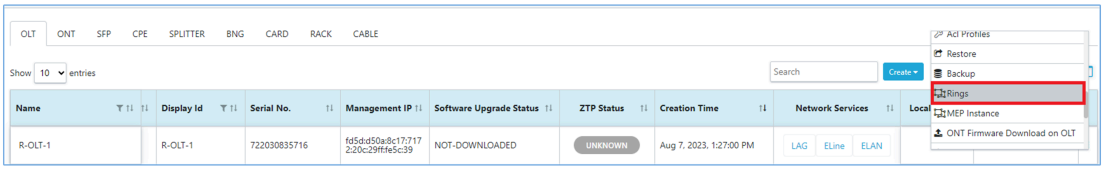
a. Create the Ring with LAG-1 as west port and LAG-2 as east port

b. Navigate to **Configuration > Inventory > OLT**.

c. Click on three dots and click the **Rings** option.

The Rings page appears.

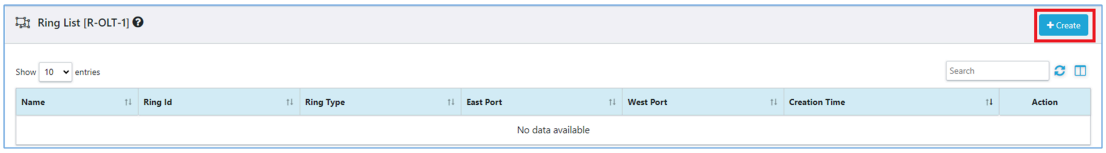
Figure 333. Rings



d. Click **Create**.

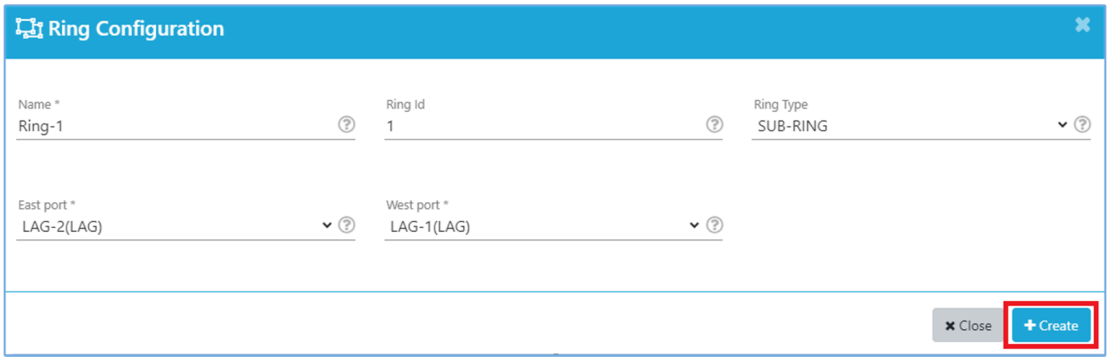
The Ring Configuration page appears.

Figure 334. Create Ring



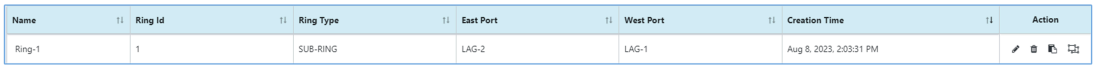
e. Enter the Ring configuration and click **Create**.

Figure 335. Ring Configuration



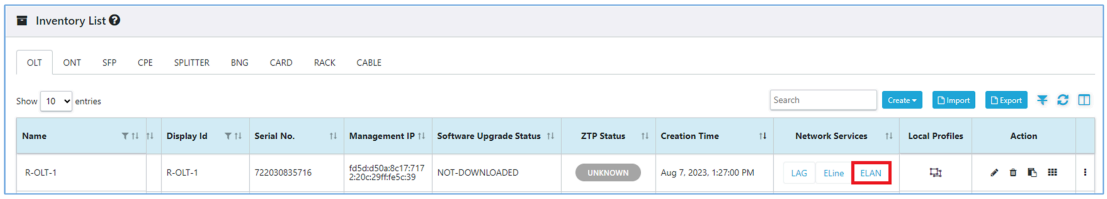
A confirmation message appears indicating the status of the Ring.

Figure 336. Status of the Ring



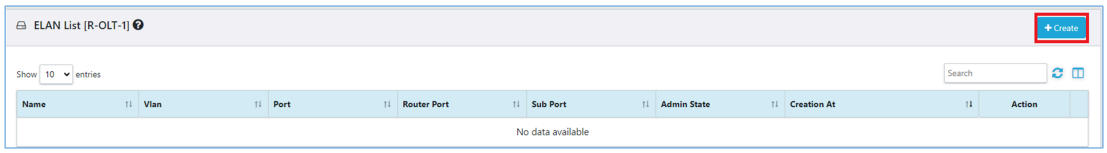
6. Create ELANs with the LAGs.
   a. Create ELAN1035 with port list as LAG-1 and LAG-2 and enable the ELAN1035.
   b. Navigate to **Configuration > Inventory > OLT**.
   c. Click on the ELAN from the **Network Services** column.

Figure 337. ELAN



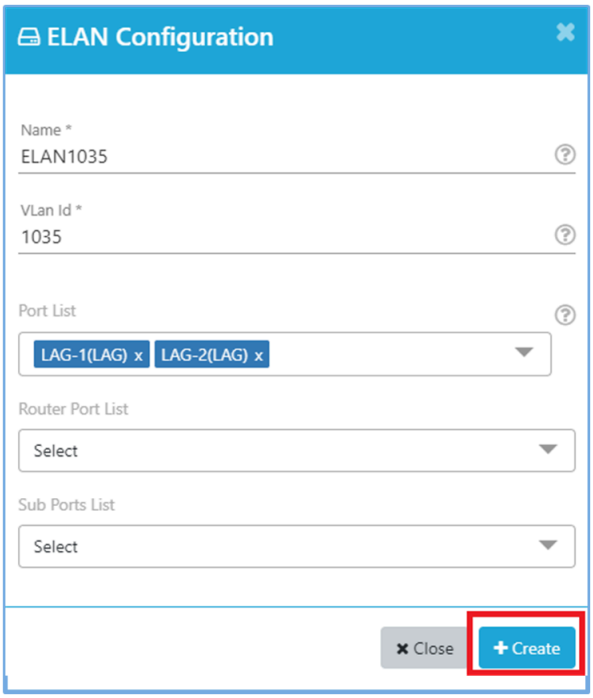
   d. Click **Create**.

Figure 338. Create ELAN



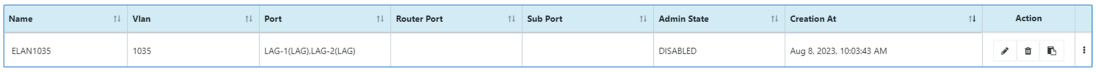
   e. Enter the ELAN configuration and click **Create**.

Figure 339. ELAN Configuration



The following screenshot shows the status of the ELAN1035.

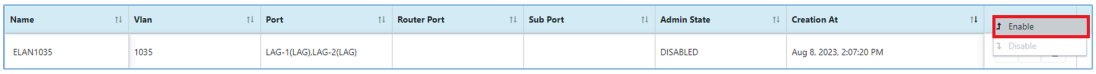
Figure 340. Status of the ELAN1035



Note: The ELAN1035 is in the **Disable** state.

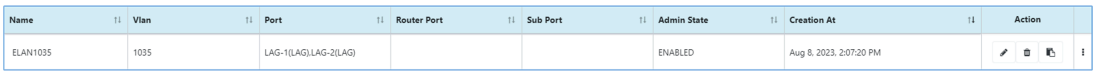
f. Click on three dots and select **Enable** option to enable the ELAN1035.

Figure 341. Enable ELAN1035



The following screenshot shows the status of the ELAN1035.

Figure 342. Status of the ELAN1035



g. Repeat the same steps to create the ELAN1022 with port list as LAG-1 and LAG-2 and enable the ELAN1022.

Note: Add the service configuration and check if the traffic is running.

Example: Converting Two Port Dynamic LAG to Single Port Static LAG - Enterprise

Overview

This section covers the procedure to convert the two-port dynamic LAG to single port static LAG for enterprise customers using the RMS GUI.

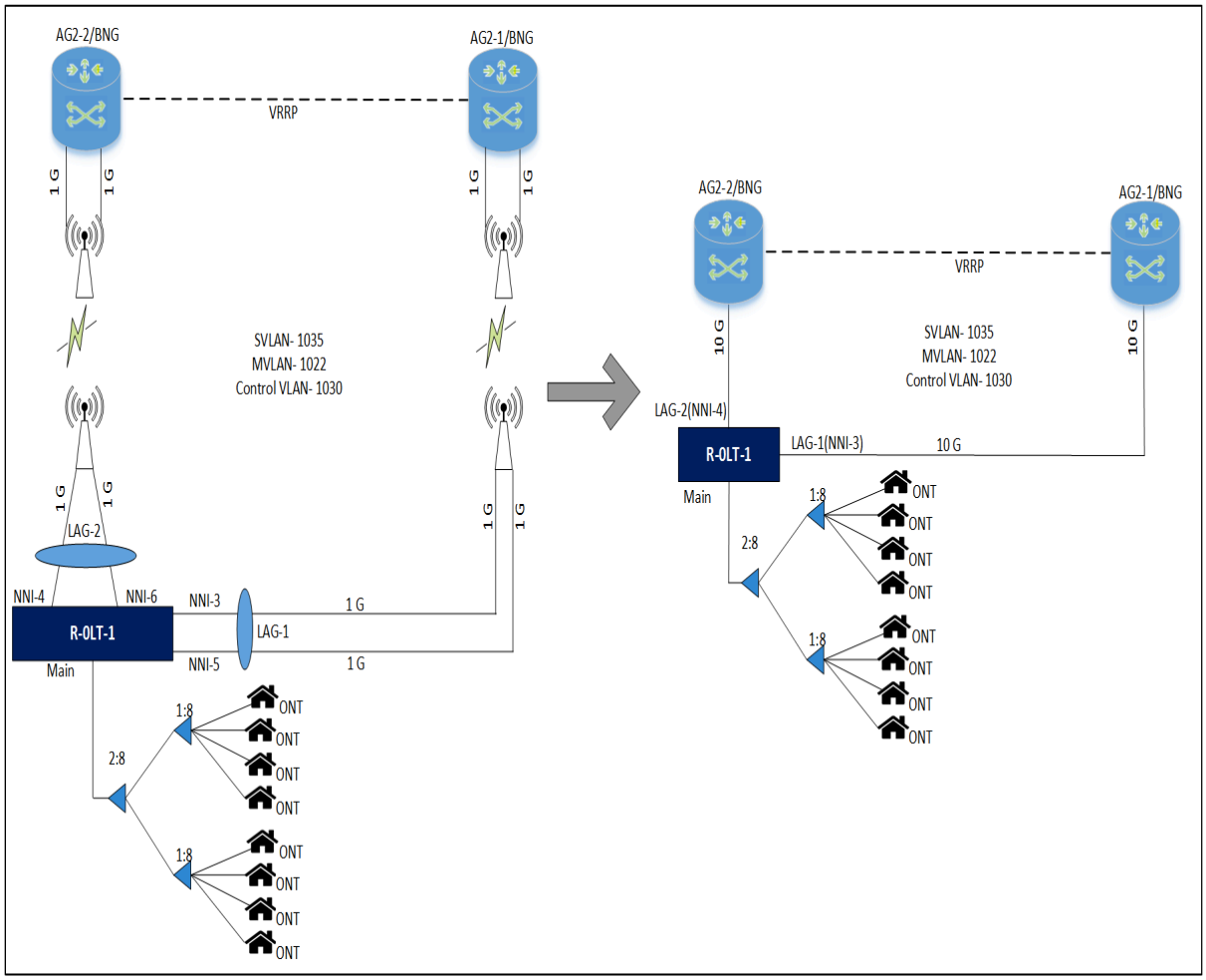
Topology

The following topology diagram shows the configurations and connections between the main OLTs.

- R-OLT-1 is the main or parent OLT and part of the ring

Note: It is assumed that the OLTs are installed with 2.10.2/latest version and required configurations are done at the BNG side.

Figure 343. Topology



Configuration

This section covers the configuration for converting two port based dynamic LAG to single port based static LAG for enterprise customers.

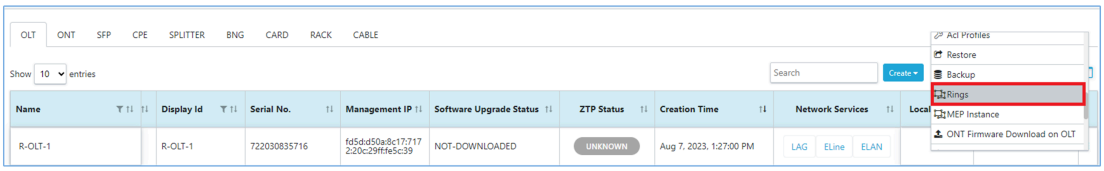
1. Delete the ERPS instance.
   a. Navigate to **Configuration > Inventory > OLT**.

      The OLT page appears.

   b. Click on three dots and click the **Rings** option.

      The Rings page appears.

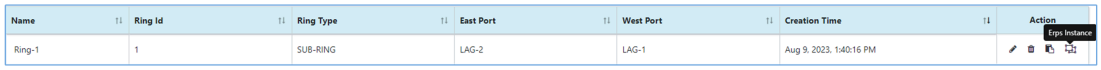
      Figure 344. Rings

   c. Click on the **ERPS Instance** icon from the **Action** column.

      The ERPS Instance page appears.

      Figure 345. ERPS Instance

   d. Click the delete icon from the **Action** column.

      An alert message appears, asking you to confirm the delete operation.

   e. Click **Confirm** to delete the ERPS instance.

      A confirmation message appears, indicating the status of the delete operation.

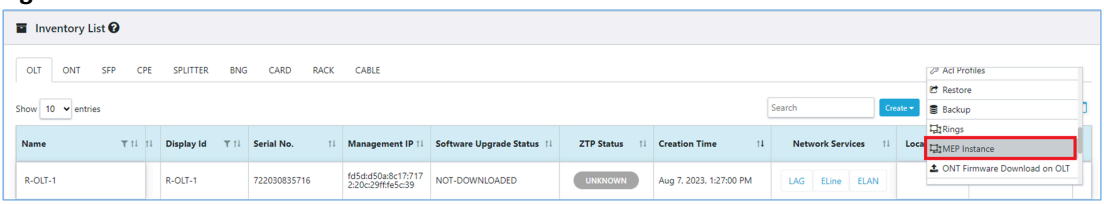
2. Delete the MEP instance.
   a. Navigate to **Configuration > Inventory > OLT**.

      The OLT page appears.

   b. Click on three dots and click the **MEP Instance** option.

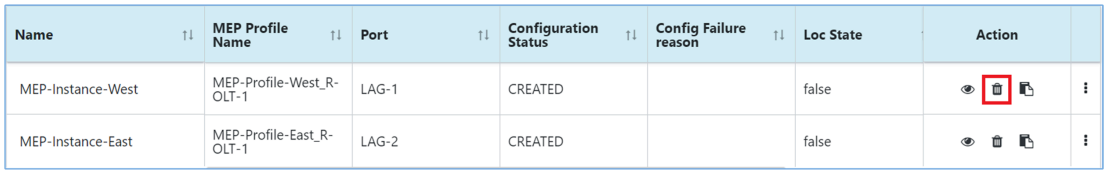
      The MEP Instance list page appears.

      Figure 346. MEP Instance

c. Click the delete icon from the **Action** column.

Figure 347. Delete MEP Instance



An alert message appears, asking you to confirm the delete operation.

d. Click **Confirm** to delete the MEP instance.

A confirmation message appears, indicating the status of the delete operation.

3. Disable and delete the existing ELANs (ELAN1030, ELAN1035, and ELAN1022)

Note: You must disable the ELANs before you delete them.

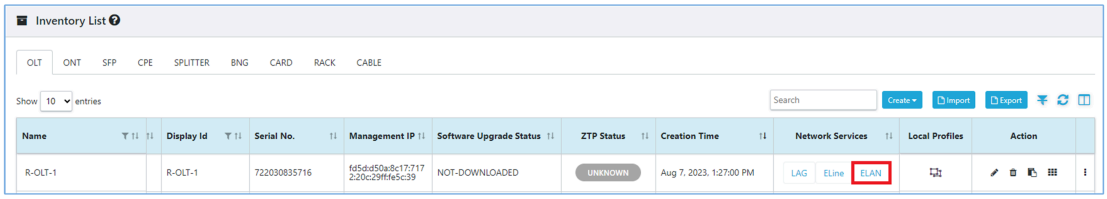
a. Navigate to **Configuration > Inventory > OLT**.

The OLT page appears.

b. Click on the ELAN from the **Network Services** column.

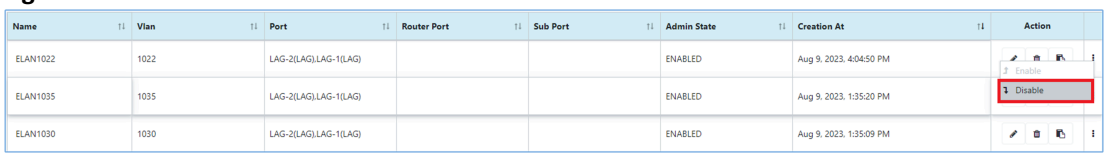
The ELAN list page appears.

Figure 348. ELAN



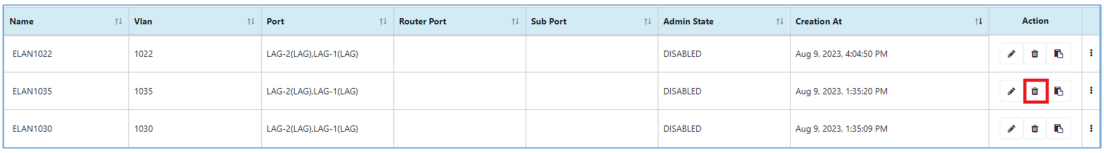
c. Click on three dots and select the **Disable** option to disable the ELAN1035. Repeat the steps to disable the ELAN1030 and ELAN1022.

Figure 349. Disable ELANs



d. Click on three dots and select the **Delete** icon to delete theELAN1035. Repeat the steps to delete the ELAN1030 and ELAN1022.

Figure 350. Delete ELANs



4. Delete the ring.

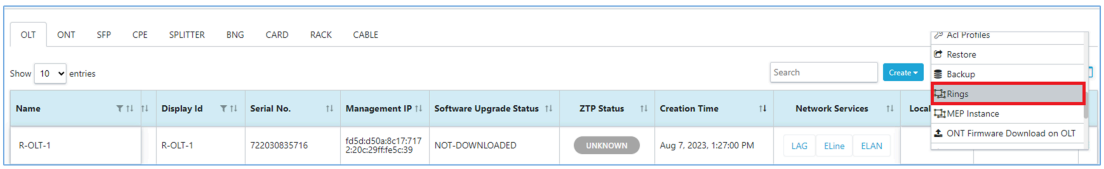
a. Navigate to **Configuration > Inventory > OLT**.

The OLT page appears.

b. Click on three dots and click the **Rings** option.

The Rings page appears.

Figure 351. Rings



c. Click the delete icon from the **Action** column.

An alert message appears, asking you to confirm the delete operation.

d. Click **Confirm** to delete the ring.

A confirmation message appears, indicating the status of the delete operation.

5. Dissociate the member ports from the LAG-1 and delete the LAG.

Note: NNI-4 is the IN-BAND port. Except the IN-BAND port, deactivate all the other ports and then dissociate from the LAG to avoid looping.

a. Navigate to **Configuration > Inventory > OLT**.

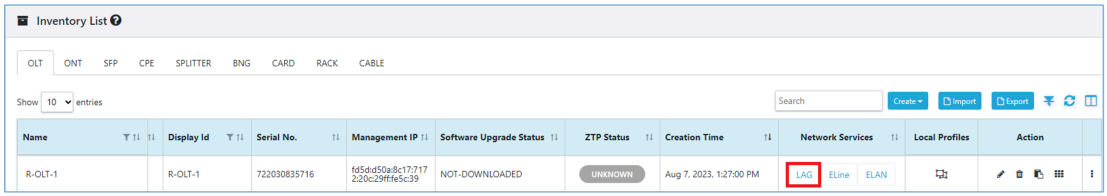
The OLT page appears.

b. Click on the ELAN from the **Network Services** column.

The LAG list page appears.

c. Check the ports that must be dissociated from LAG-1.

Figure 352. LAG

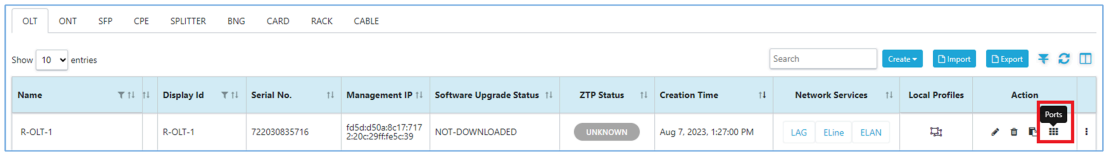


d. Dissociate NNI-3 port from the LAG-1.

e. Navigate to **Configuration > Inventory > OLT**.

f. Click on nine dots icon (port) from the **Action** column.

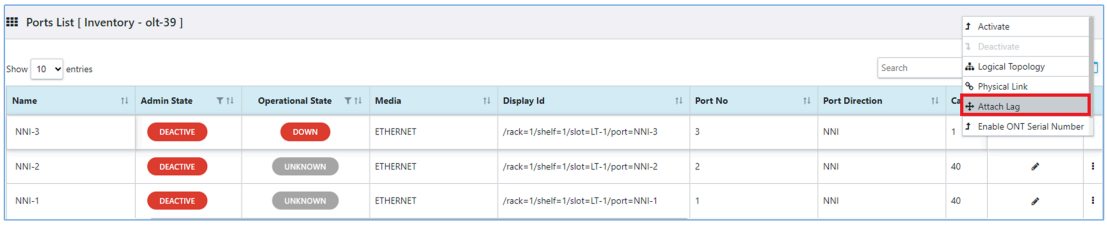
Figure 353. OLT



g. Click on the NNI-3 port.

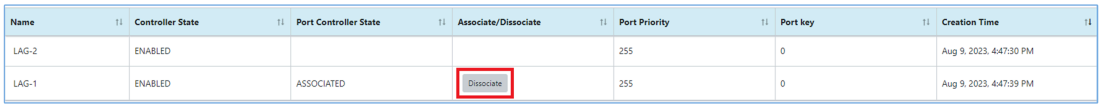
h. Click on three dots and select the **Attach Lag** option to attach LAG to the NNI-3 port.

Figure 354. Attach LAG



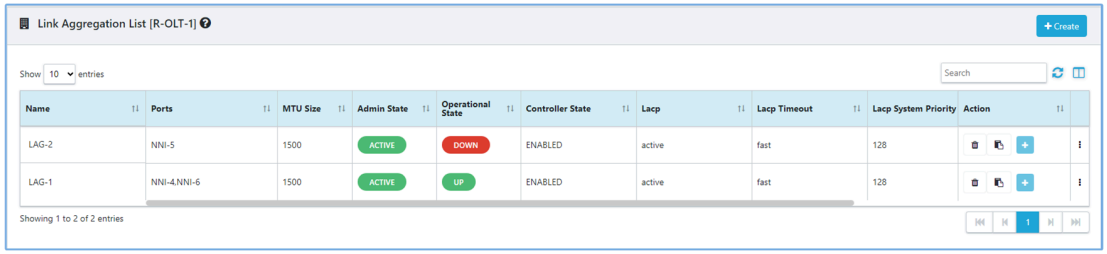
i. Dissociate the NNI-3 port from the LAG-1 and repeat the same for the NNI-5 port.

Figure 355. Dissociate LAG



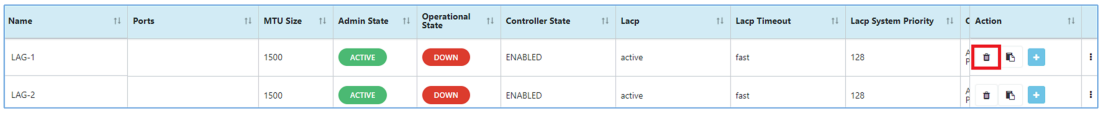
j. Dissociate the member ports from the LAG-2.

Figure 356. Dissociate Member Port



k. Delete LAG-1 and LAG-2.

Figure 357. Delete LAG

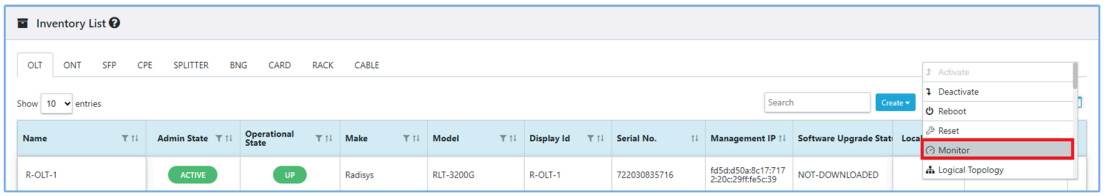


6. Log in to the OLT terminal, edit the `olt_config` file and remove the *"nni_port_speed_1g": [3,4,5,6]* field.

a. Navigate to **Configuration > Inventory > OLT**.

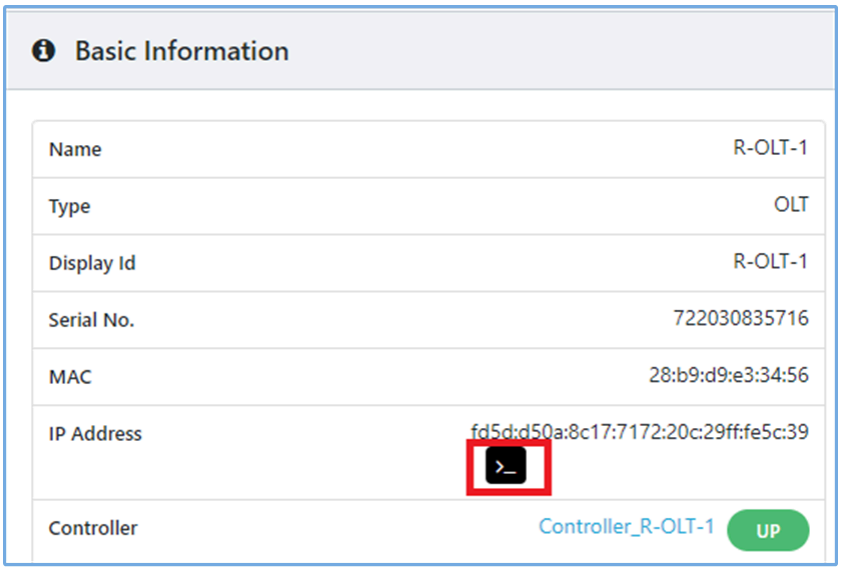
b. Click on three dots and select **Monitor**.

Figure 358. Monitor OLT



c. Under the **Basic Information**, click on the terminal in the IP Address.

Figure 359. OLT Basic Information

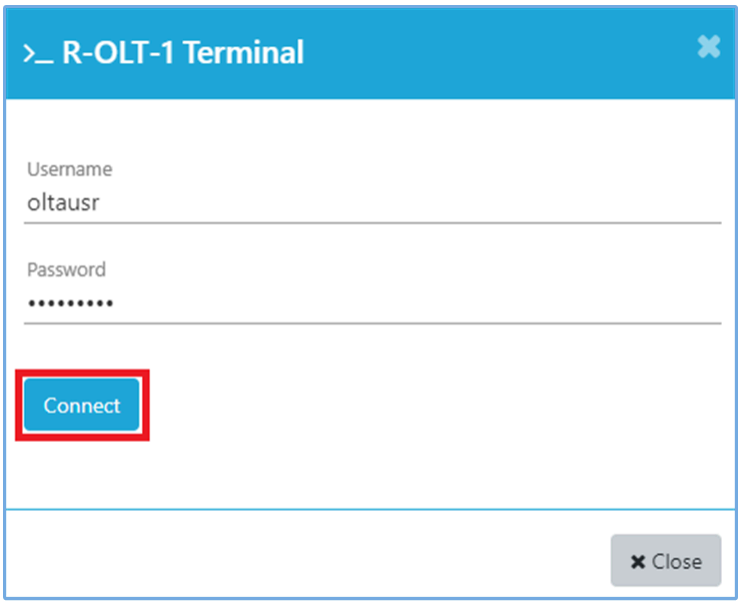


d. Enter the username and password.

e. Click **Connect**.

The OLT Terminal page appears.

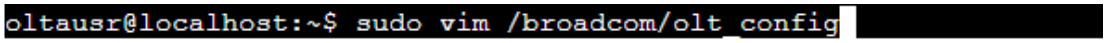
Figure 360. OLT Terminal



f. Execute the following command to edit the `olt_config` file.

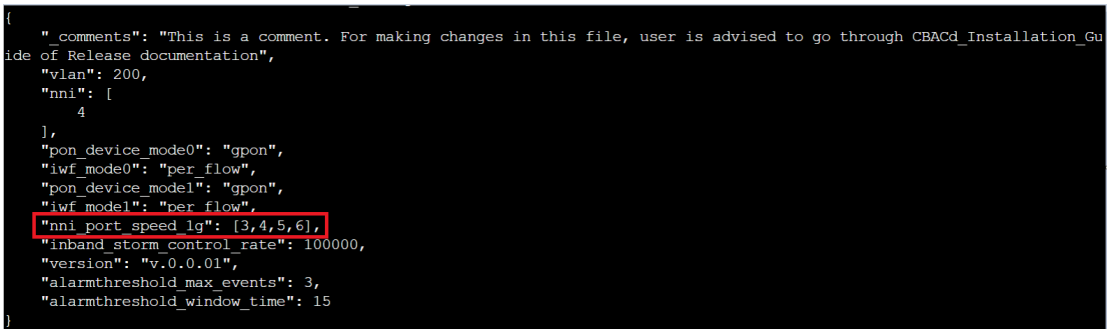
```
sudo vim /broadcom/olt_config
```

Figure 361. OLT Configuration File



g. Remove the *"nni_port_speed_1g": [3,4,5,6]*, field from the `olt_config` file.

Figure 362. NNI Port Speed



h. Status of the `olt_config` file after removing the field.

Figure 363. OLT Configuration File

```
oltausr@localhost:~$ cat /broadcom/olt_config
{
    "_comments": "This is a comment. For making changes in this file, user is advised to go through CBACd_Installation_Gu
ide of Release documentation",
    "vlan": 200,
    "nni": [
        4
    ],
    "pon_device_mode0": "gpon",
    "iwf_mode0": "per_flow",
    "pon_device_mode1": "gpon",
    "iwf_mode1": "per_flow",
    "inband_storm_control_rate": 100000,
    "version": "v.0.0.01",
    "alarmthreshold_max_events": 3,
    "alarmthreshold_window_time": 15
}
```

7. Execute the following command to check and delete the `olt_hidden_config` json file from the same OLT terminal if the field name exists.

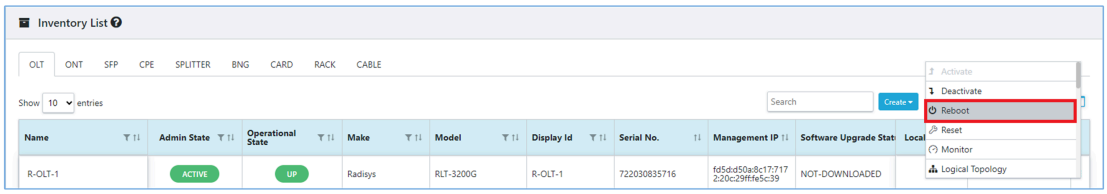
```
sudo rm -rf /mnt/onl/sdpon/oltfiles/olt_hidden_config.json
```

Figure 364. OLT JSON File

```
oltausr@localhost:~$ sudo rm -rf /mnt/onl/sdpon/oltfiles/olt_hidden_config.json
```

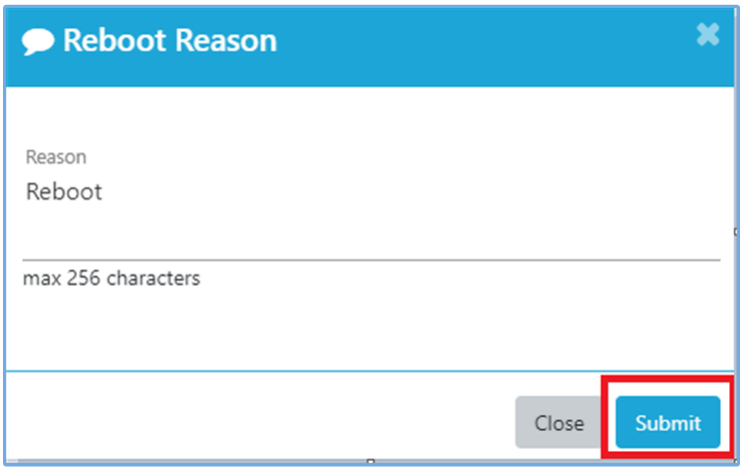
8. Reboot the OLT.
   a. Navigate to **Configuration > Inventory > OLT**.
   b. Click on three dots and select the **Reboot** option.

Figure 365. OLT Reboot



   c. Enter the reason for the OLT reboot and click **Submit**.

Figure 366. OLT Reboot Reason



9. Check if the OLT is UP.

a. Check if the "ME-REBOOTED" event is raised in the **Monitor > Events** page.

b. Once the "ME-REBOOTED" event is raised, go to **Monitor > Inventory > Controller** and check if the Operational State of Rest and Kafka is UP.

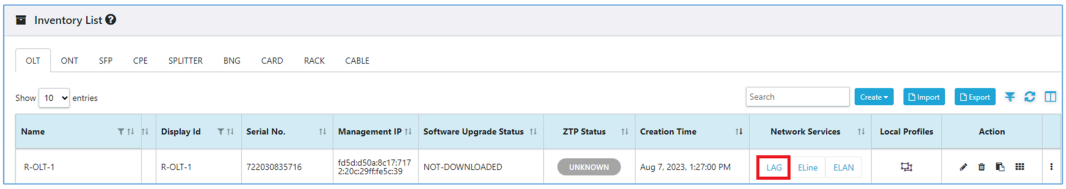
10. Create a LAG with LACP **Disabled** and add the member ports.

a. Create LAG-1.

i. Navigate to **Configuration > Inventory > OLT**.

ii. Click on the LAG from the **Network Services** column.

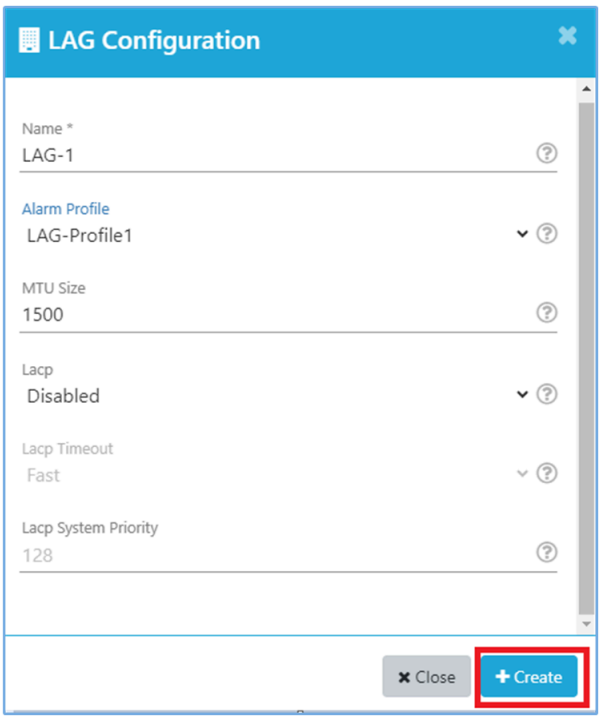
Figure 367. LAG



iii. Click **Create**.

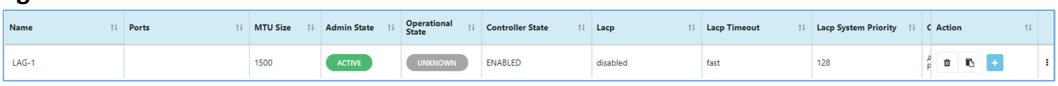
iv. Enter the LAG configuration and click **Create**.

Figure 368. LAG Configuration



v. The following screenshot shows the status of the LAG.

Figure 369. Status of the LAG



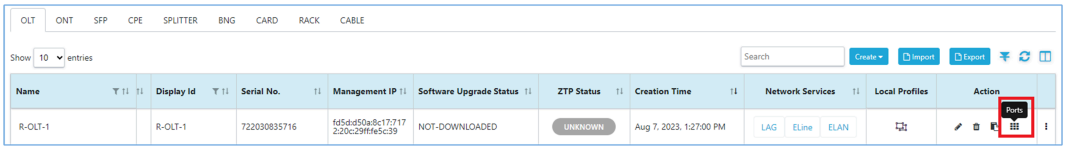
b. Associate NNI-3 to the LAG-1.

i. Navigate to **Configuration > Inventory > OLT**.

ii. Click on nine dots.

Note: If NNI-3 is not activated, then activate the NNI-3 port.

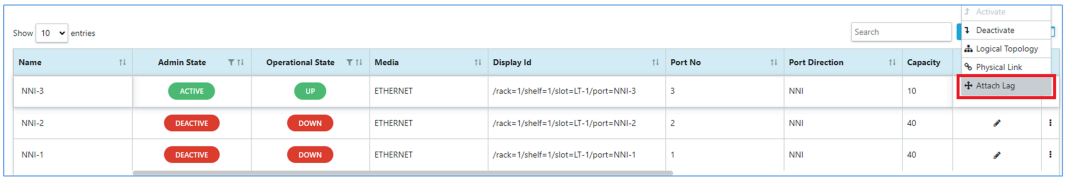
Figure 370. OLT



iii. Navigate to the **NNI-4** Port

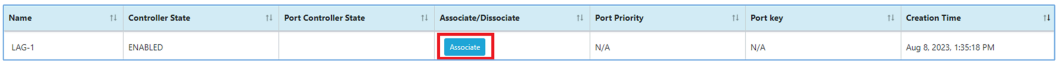
iv. Click on three dots and select the **Attach Lag** option.

Figure 371. Attach Lag



v. Click the **Associate** option from the Associate/Dissociate column.

Figure 372. Associate LAG



The NNI-3 port is associated to LAG-1 and a confirmation message appears, indicating the status of the associate operation. Repeat the same steps to associate the NNI-4 port for LAG-2.

11. Create the Ring with the LAGs.

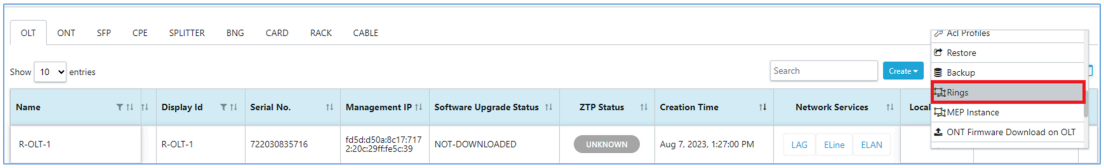
a. Create the Ring with LAG-1 as west port and LAG-2 as east port.

b. Navigate to **Configuration > Inventory > OLT**.

c. Click on three dots and click the **Rings** option.

The Rings page appears.

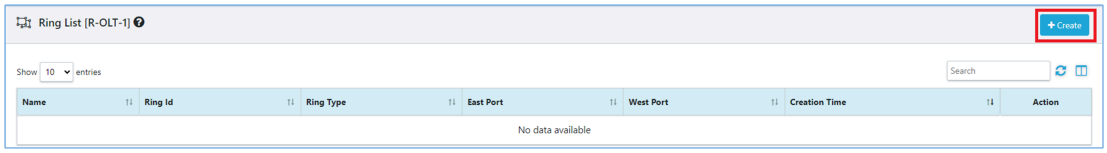
Figure 373. Rings



d. Click **Create**.

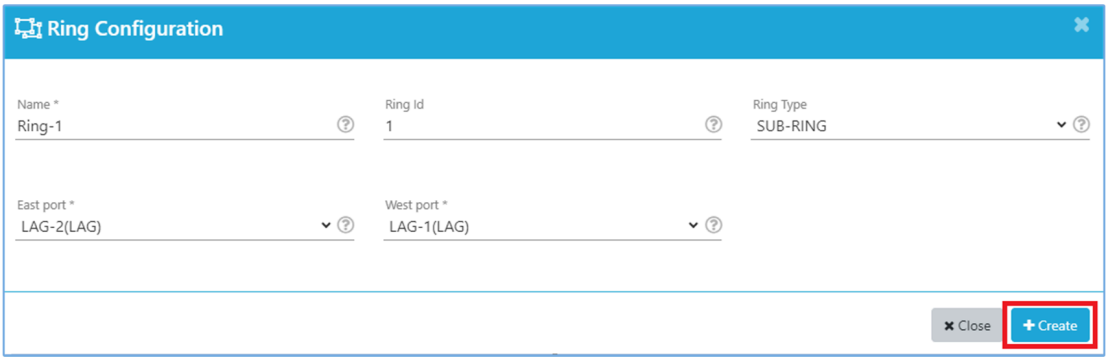
The Ring Configuration page appears.

Figure 374. Create Ring



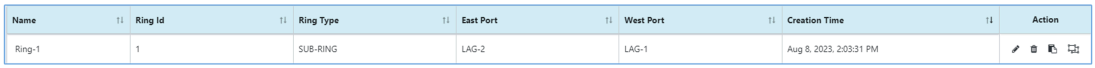
e. Enter the Ring configuration and click **Create**.

Figure 375. Ring Configuration



A confirmation message appears indicating the status of the Ring.

Figure 376. Status of the Ring

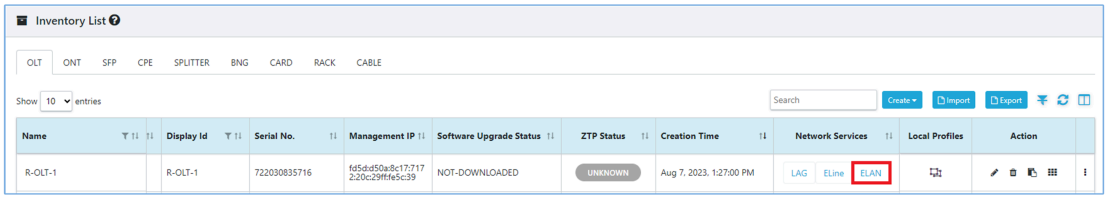


12. Create ELANs with the LAGs.

a. Navigate to **Configuration > Inventory > OLT**.

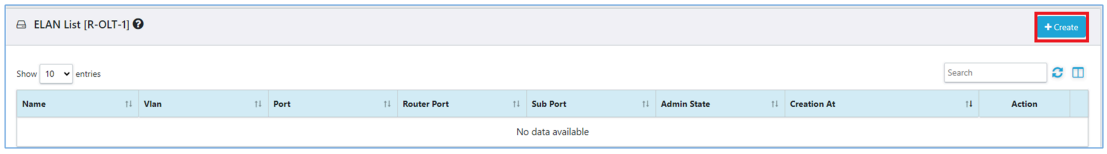
b. Click on the ELAN from the **Network Services** column.

Figure 377. ELAN



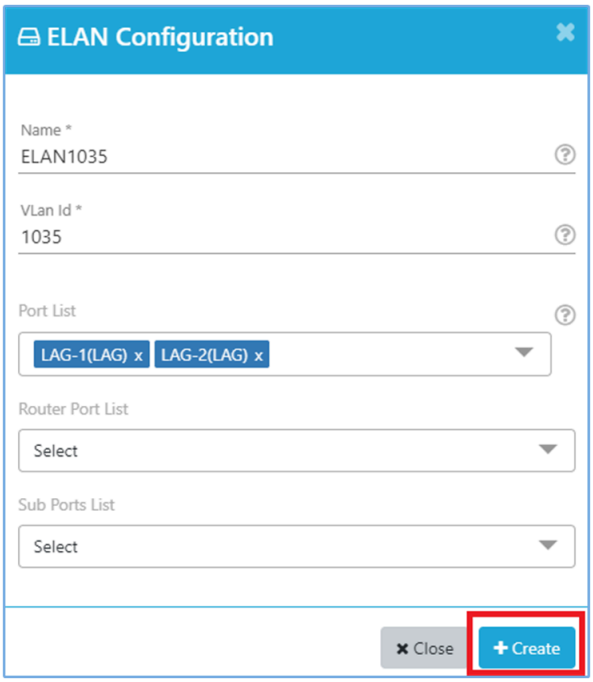
c. Click **Create**.

Figure 378. Create ELAN



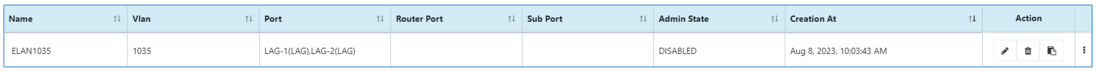
d. Enter the ELAN configuration and click **Create**.

Figure 379. ELAN Configuration



The following screenshot shows the status of the ELAN1035.

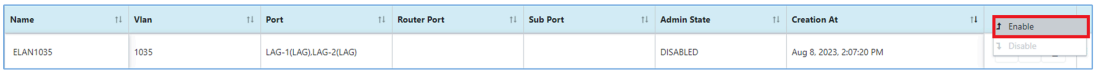
Figure 380. Status of the ELAN1035



Note: The ELAN1035 is the **Disable** state.

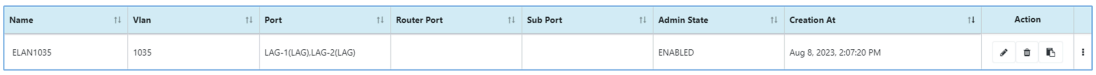
e. Click on three dots and select **Enable** option to enable ELAN1035.

Figure 381. Enable ELAN1035



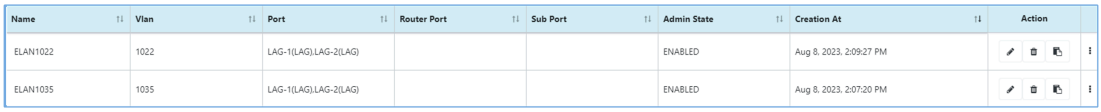
The following screenshot shows the status of ELAN1035.

Figure 382. Status of the ELAN1035



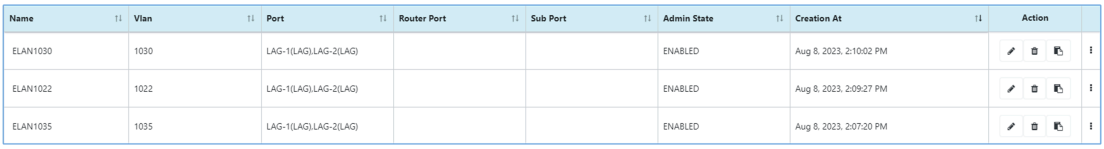
f. Create the ELAN1022 with port list as LAG-1 and LAG-2 as and enable the ELAN1022.

Figure 383. Create and Enable ELAN1022



g. Create the ELAN1030 with port list as LAG-1 and LAG-2 and enable the ELAN1030.

Figure 384. Create and Enable ELAN1030

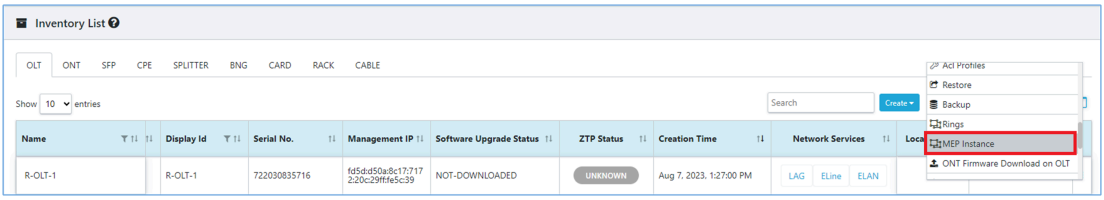


13. Create the MEP instance.

a. Navigate to **Configuration > Inventory > OLT**.

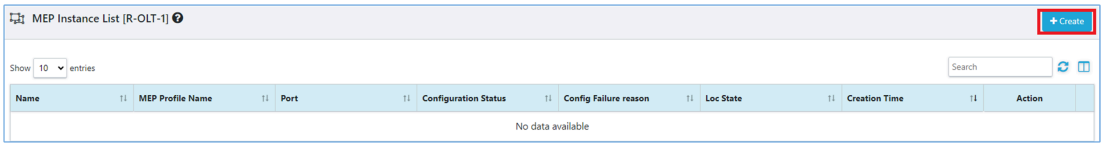
b. Click on three dots and select the **MEP Instance**.

Figure 385. MEP Instance



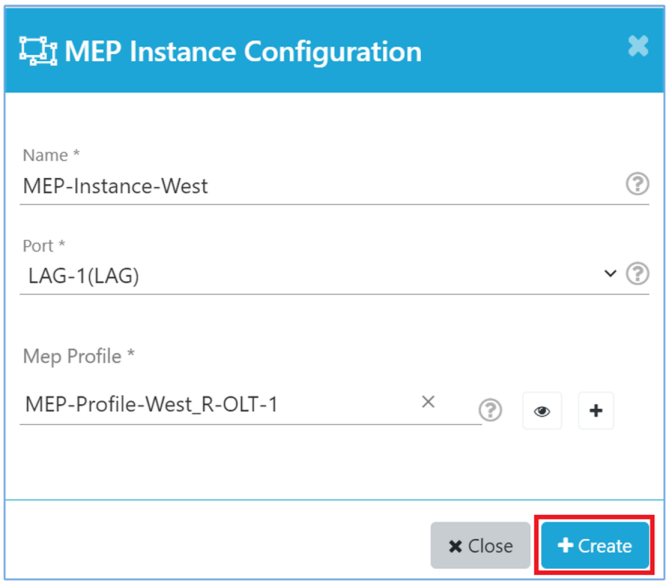
c. Click **Create**.

Figure 386. Create MEP Instance



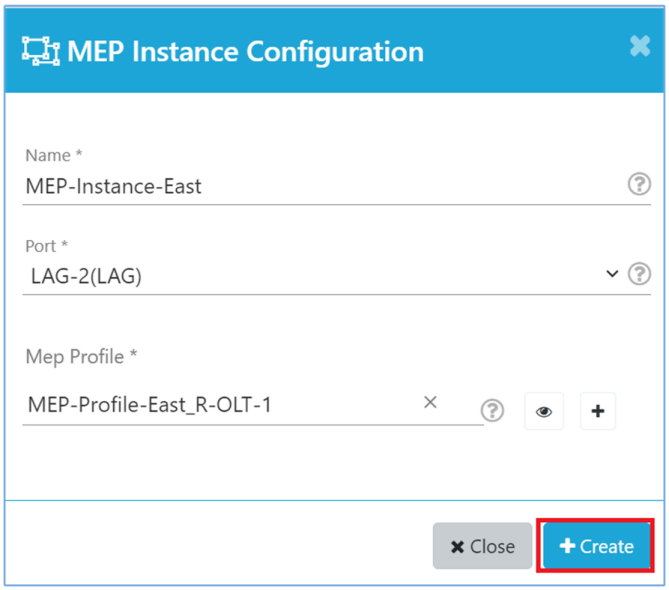
d. Enter the MEP instance configuration (Use the previously used MEP Profile) and click **Create**.

Figure 387. MEP Instance Configuration - West



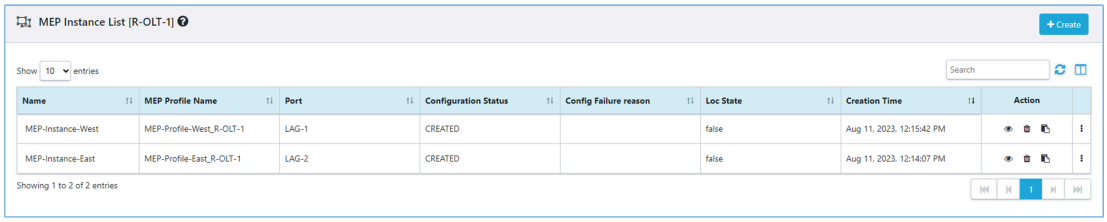
e. Repeat the same steps to create MEP-Instance-East.

Figure 388. MEP Instance Configuration - East



The following screenshot shows the status of the MEP instances.

Figure 389. Status of the MEP Instances

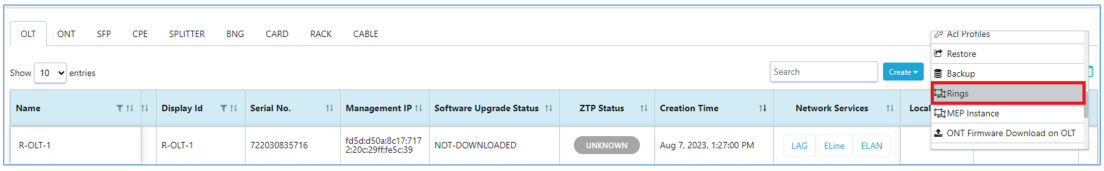


14. Create the ERPS instance.

    a. Navigate to **Configuration > Inventory > OLT**.

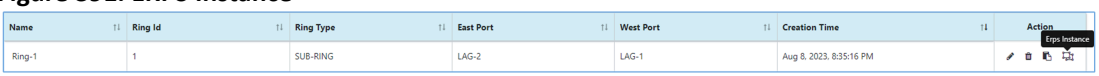
    b. Click on three dots and select **Rings**.

Figure 390. Rings



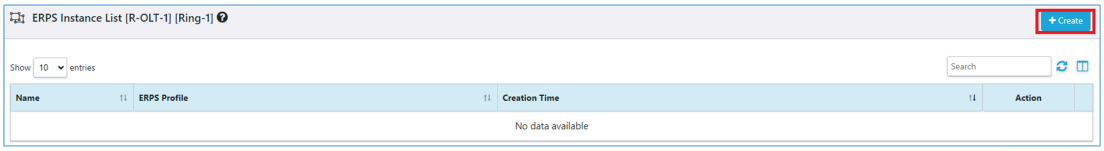
    c. Click on the **ERPS Instance** from the **Action** column.

Figure 391. ERPS Instance



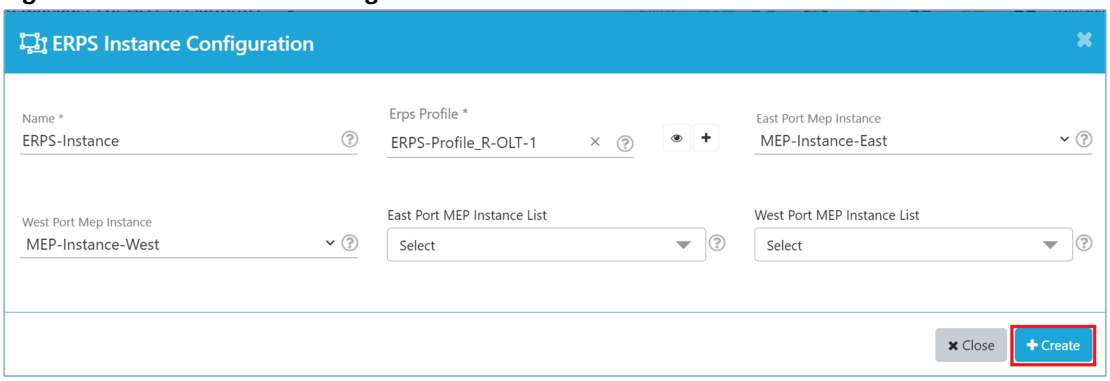
    d. Click **Create**.

Figure 392. Create ERPS Instance



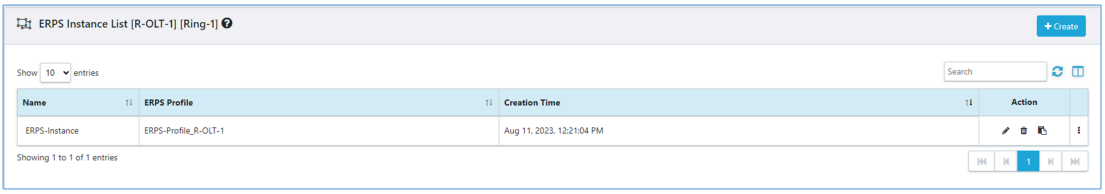
e. Enter ERPS instance configurations (Use the previously used ERPS Profile) and click **Create**.

Figure 393. ERPS Instance Configuration



The following screenshot shows the status of the ERPS instance.

Figure 394. Status of the ERPS Instance



f. Navigate to **Monitor > Events** page and check for the "CREATE-ERPS-INSTANCE-SUCCESSFUL" event.

Note: The traffic must resume.

Example: Converting Two Port Dynamic LAG to Single Port Static LAG - Residential

Overview

This section covers the procedure to convert the two-port dynamic LAG to single port static LAG for residential customers using the RMS GUI.

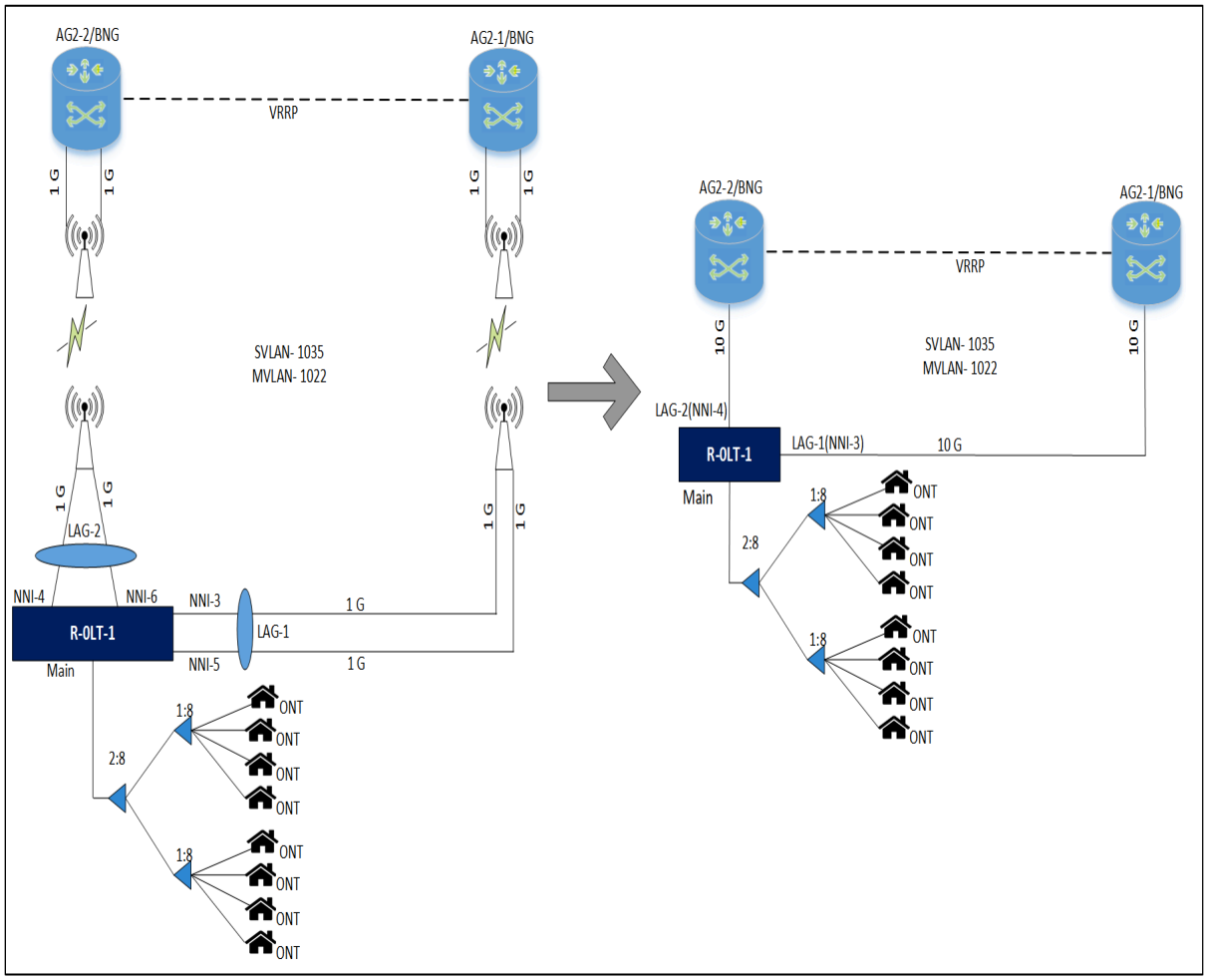
Topology

The following topology diagram shows the configurations and connections between the main OLTs.

- R-OLT-1 is the main or parent OLT

Note: It is assumed that the OLTs are installed with 2·10·2/latest version and required configurations are done at the BNG side.

Figure 395. Topology



Configuration

This section covers the configuration for converting two port based dynamic LAG to single port based static LAG for residential customers.

1. Disable and delete the existing ELANs (ELAN1035 and ELAN1022)

   Note: You must disable the ELANs before you delete them.

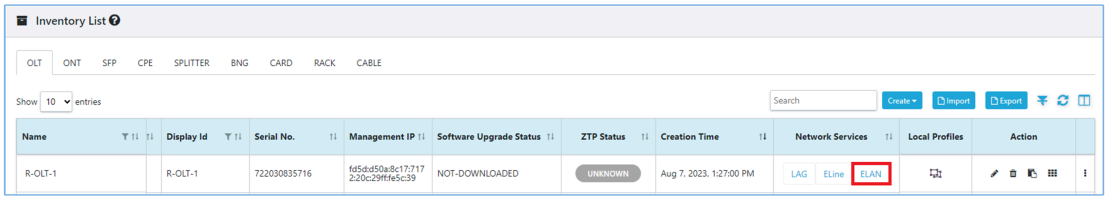
   a. Navigate to **Configuration > Inventory > OLT**.

      The OLT page appears.

   b. Click on the ELAN from the **Network Services** column.

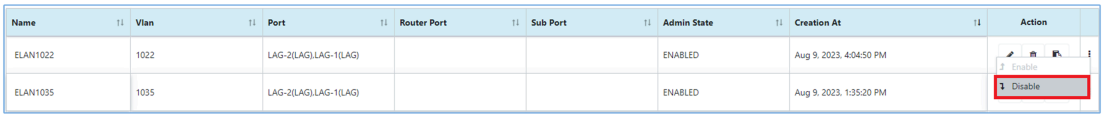
The ELAN list page appears.

Figure 396. ELAN



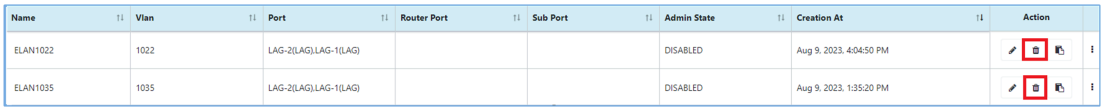
c. Click on three dots and select the **Disable** option to disable the ELAN1035. Repeat the steps to disable the ELAN1022.

Figure 397. Disable ELAN1035



d. Click on three dots and select the **Delete** icon to delete the ELAN1035. Repeat the steps to delete the ELAN1022.

Figure 398. Delete ELAN1035



2. Delete the ring.

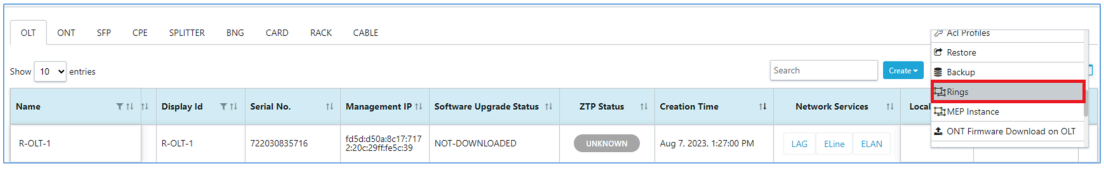
a. Navigate to **Configuration > Inventory > OLT**.

The OLT page appears.

b. Click on three dots and click the **Rings** option.

The Rings page appears.

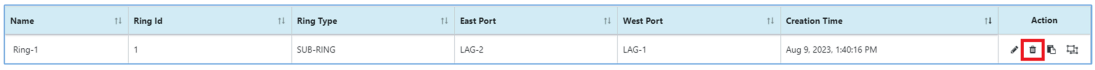
Figure 399. Rings



c. Click the delete icon from the **Action** column.

An alert message appears, asking you to confirm the delete operation.

Figure 400. Delete Ring



d. Click **Confirm** to delete the ring.

A confirmation message appears, indicating the status of the delete operation.

3. Dissociate the member ports from the LAG-1 and delete the LAG.

Note: The NNI-4 port is the IN-BAND port. Deactivate all the other ports except the IN-BAND port and then dissociate from the LAG to avoid looping.

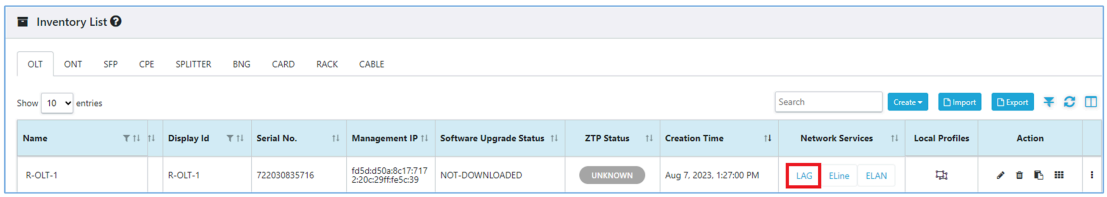
a. Navigate to **Configuration > Inventory > OLT**.

The OLT page appears.

b. Click on the LAG from the **Network Services** column.

The LAG list page appears.

Figure 401. LAG



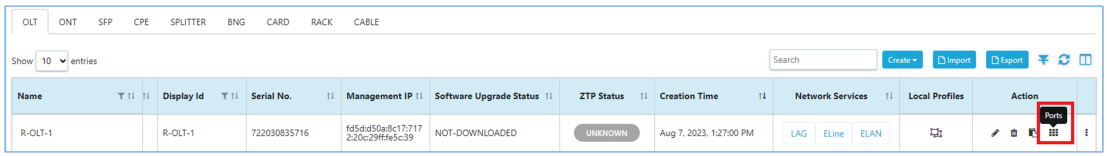
c. Check the ports that must be dissociated from LAG-1.

d. Dissociate NNI-3 from the LAG-1.

e. Navigate to **Configuration > Inventory > OLT**.

f. Click on nine dots icon (port) from the **Action** column.

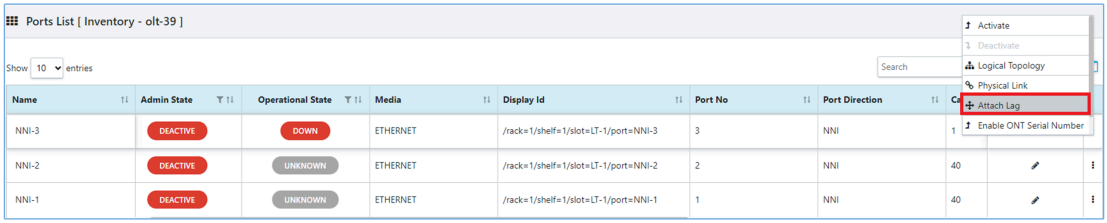
Figure 402. OLT



g. Click on the NNI-3 port.

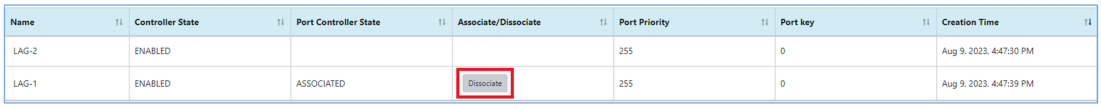
h. Click on three dots and select the **Attach Lag** option to attach LAG to the NNI-3 port.

Figure 403. Attach LAG



i. Dissociate the NNI-3 port from the LAG-1 and repeat the same for the NNI-5 port.

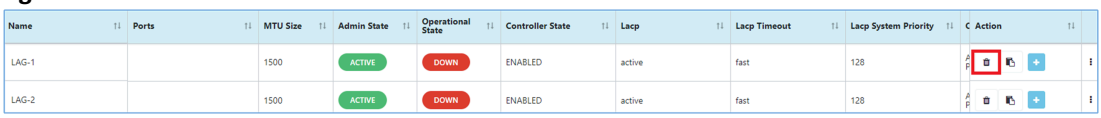
Figure 404. Dissociate LAG



j. Dissociate the member ports from the LAG-2.

k. Delete LAG-1 and LAG-2.

Figure 405. Delete LAG

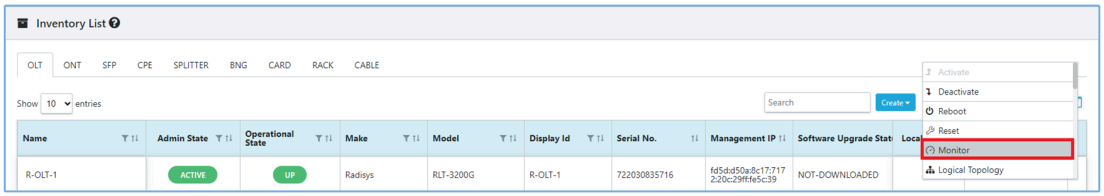


4. Log in to the OLT terminal, edit the `olt_config` file and remove the *"nni_port_speed_1g": [3,4,5,6]* field.

a. Navigate to **Configuration > Inventory > OLT**.

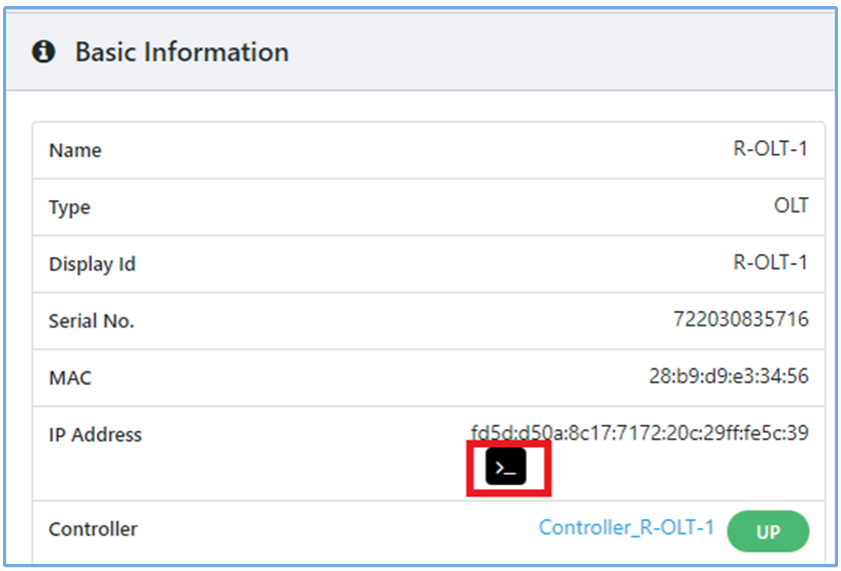
b. Click on three dots and select **Monitor**.

Figure 406. OLT Monitor



c. Under the **Basic Information**, click on the terminal in the IP Address.

Figure 407. OLT Basic Information

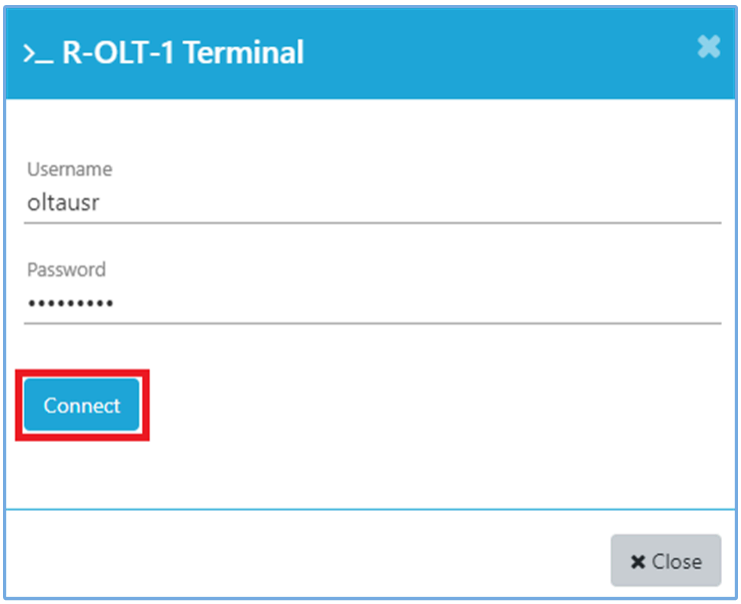


d. Enter the username and password.

e. Click **Connect**.

The OLT Terminal page appears.

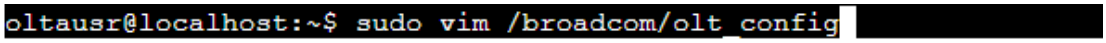
Figure 408. R-OLT-1 Terminal



f. Execute the following command to edit the `olt_config` file.

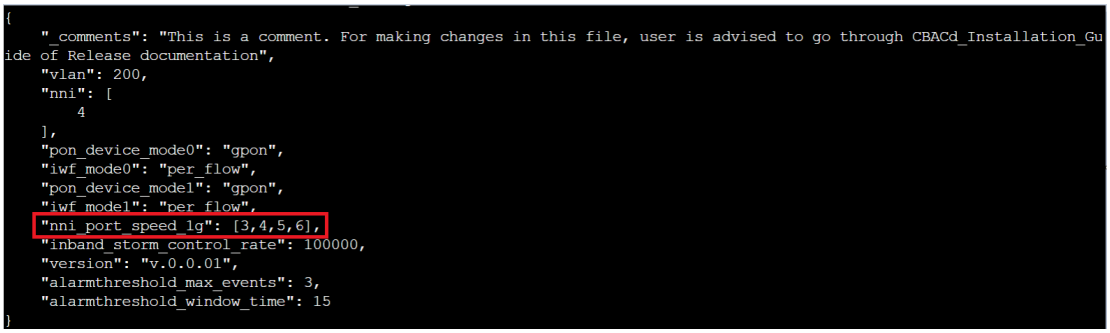
```
sudo vim /broadcom/olt_config
```

Figure 409. OLT Configuration File



g. Remove the *"nni_port_speed_1g": [3,4,5,6]*, field from the `olt_config` file.

Figure 410. NNI Port Speed



h. Status of the `olt_config` file after removing the field.

Figure 411. Status of the OLT Configuration File

```
oltausr@localhost:~$ cat /broadcom/olt_config
{
    "_comments": "This is a comment. For making changes in this file, user is advised to go through CBACd_Installation_Gu
ide of Release documentation",
    "vlan": 200,
    "nni": [
        4
    ],
    "pon_device_mode0": "gpon",
    "iwf_mode0": "per_flow",
    "pon_device_mode1": "gpon",
    "iwf_mode1": "per_flow",
    "inband_storm_control_rate": 100000,
    "version": "v.0.0.01",
    "alarmthreshold_max_events": 3,
    "alarmthreshold_window_time": 15
}
```

5. Execute the following command to check and delete the `olt_hidden_config` json file from the same OLT terminal if the field name exists.

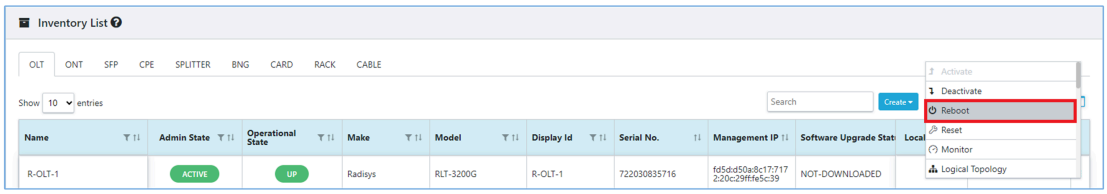
```
sudo rm -rf /mnt/onl/sdpon/oltfiles/olt_hidden_config.json
```

Figure 412. OLT Configuration JSON File

```
oltausr@localhost:~$ sudo rm -rf /mnt/onl/sdpon/oltfiles/olt_hidden_config.json
```

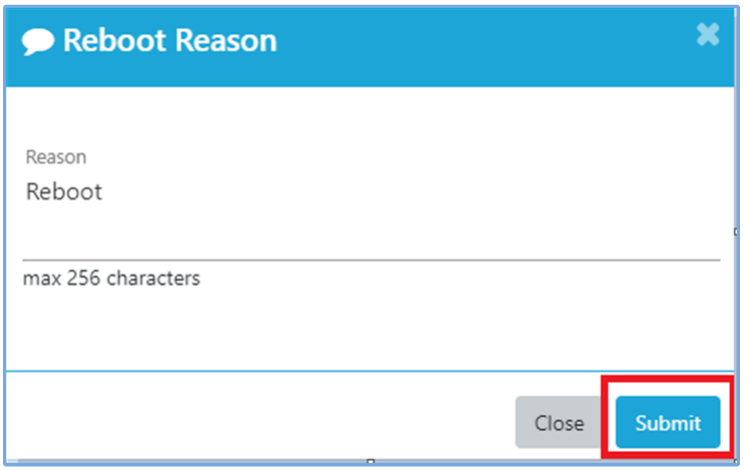
6. Reboot the OLT.
   a. Navigate to **Configuration > Inventory > OLT**.
   b. Click on three dots and select the **Reboot** option.

Figure 413. OLT Reboot



   c. Enter the reason for the OLT reboot and click **Submit**.

Figure 414. OLT Reboot Reason

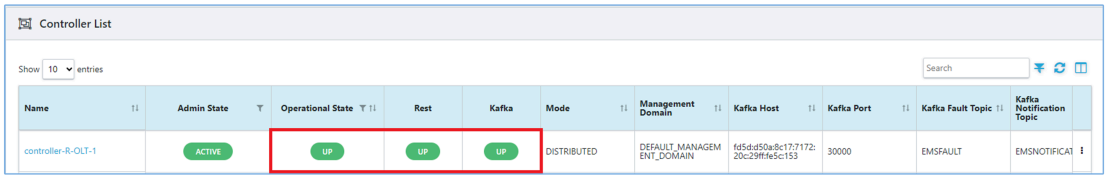


7. Check if the OLT is UP.

a. Check if the "ME-REBOOTED" event is raised in the **Monitor > Events** page.

b. Once the "ME-REBOOTED" event is raised, go to **Monitor > Inventory > Controller** and check if the Operational State of Rest and Kafka is UP.

Figure 415. Operational State of Rest and Kafka



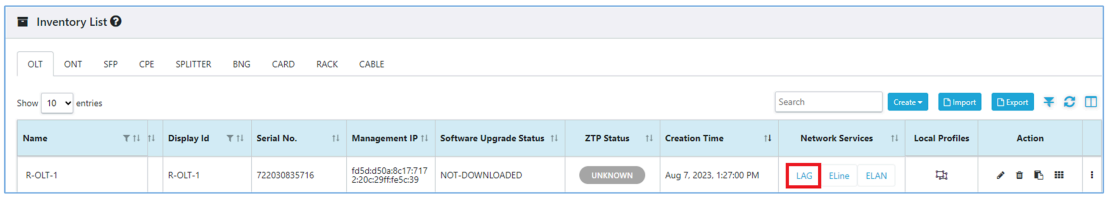
8. Create a LAG with LACP Disabled and add the member ports.

Perform the following steps to create the LAG-1.

a. Navigate to **Configuration > Inventory > OLT**.

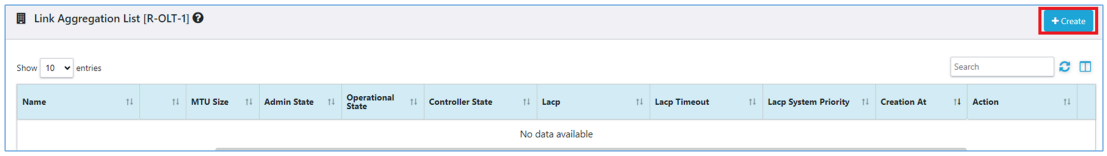
b. Click on the LAG from the **Network Services** column.

Figure 416. LAG



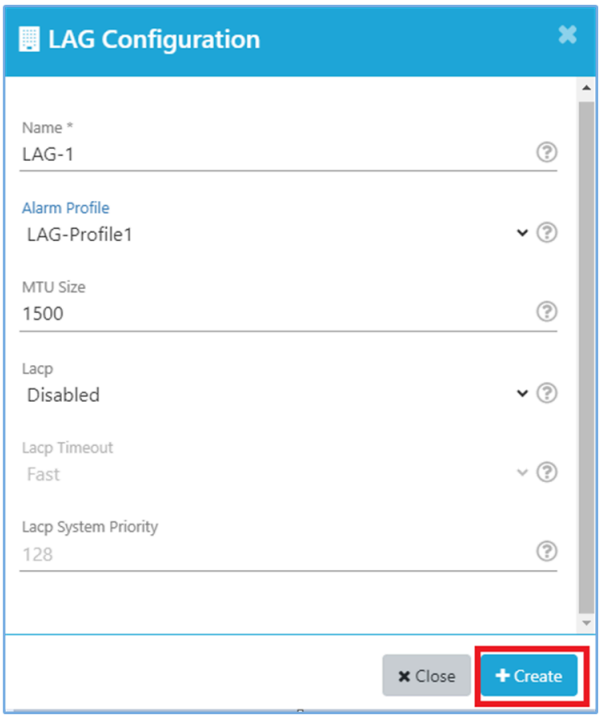
c. Click **Create**.

Figure 417. Create LAG



d. Enter the LAG Configuration and click **Create**.

Figure 418. LAG Configuration



The following screenshot shows the status of the LAG.

Figure 419. Status of the LAG

e. Repeat the same steps to create the LAG-2.

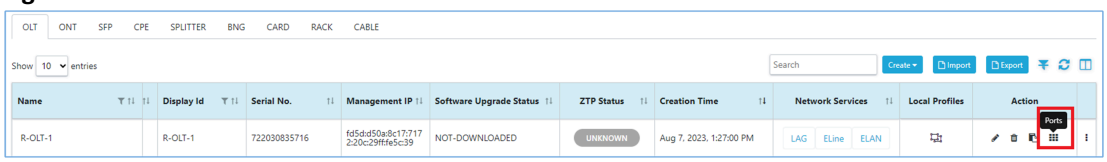
Perform the following steps to associate NNI-3 to the LAG-1.

a. Navigate to **Configuration > Inventory > OLT**.

b. Click on nine dots.

Note: If NNI-3 is not activated, then activate the NNI-3 port.

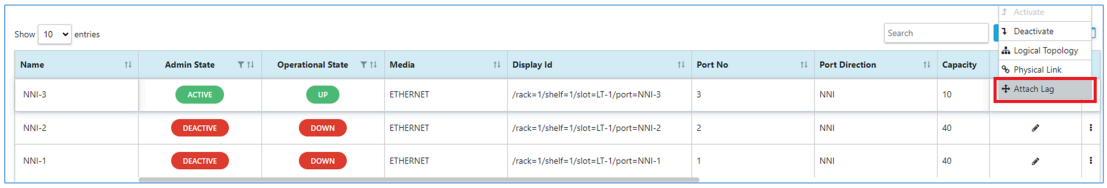
Figure 420. OLT



c. Navigate to the **NNI-4** Port

d. Click on three dots and select the **Attach Lag** option.

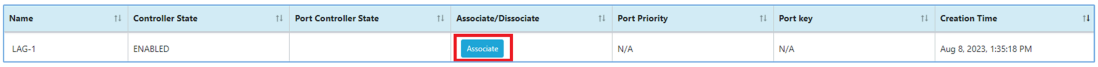
Figure 421. Attach LAG



e. Click the **Associate** option from the Associate/Dissociate column.

The NNI-3 port is associated to LAG-1, and a confirmation message indicates the status of the associate operation. Repeat the same steps to associate the NNI-4 port for LAG-2.

Figure 422. Associate LAG



9. Create the Ring with the LAGs

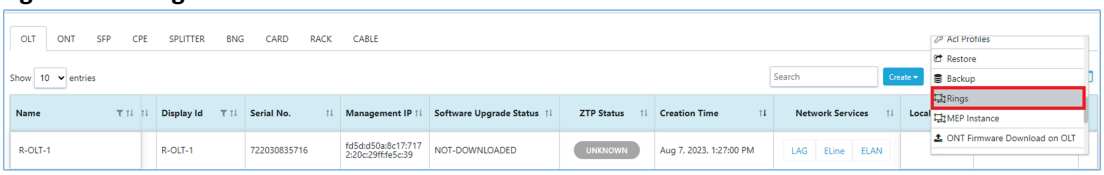
a. Create the Ring with LAG-1 as west port and LAG-2 as east port.

b. Navigate to **Configuration > Inventory > OLT**.

c. Click on three dots and click the **Rings** option.

The Rings page appears.

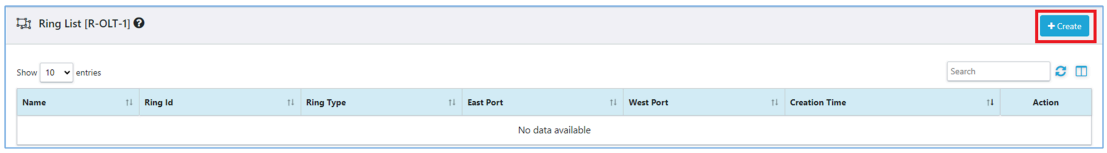
Figure 423. Rings



d. Click **Create**.

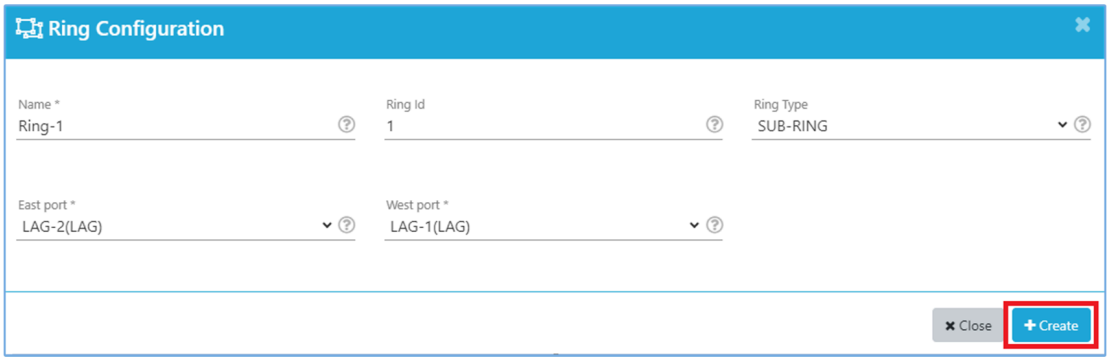
The Ring Configuration page appears.

Figure 424. Create Ring



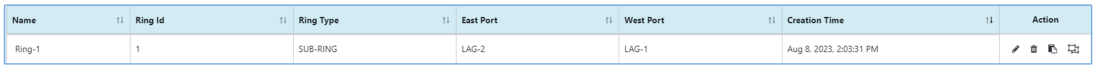
e. Enter the Ring configuration and click **Create**.

Figure 425. Ring Configuration



A confirmation message appears indicating the status of the Ring.

Figure 426. Status of the Ring



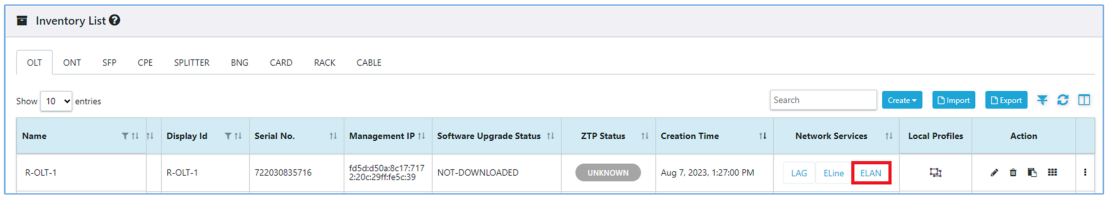
10. Create ELANs with the LAGs.

    a. Create ELAN1035 with port list as LAG-1 and LAG-2 and enable the ELAN1035.

    b. Navigate to **Configuration > Inventory > OLT**.

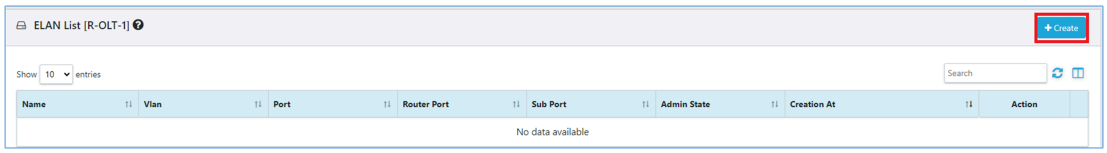
    c. Click on the ELAN from the **Network Services** column.

Figure 427. ELAN



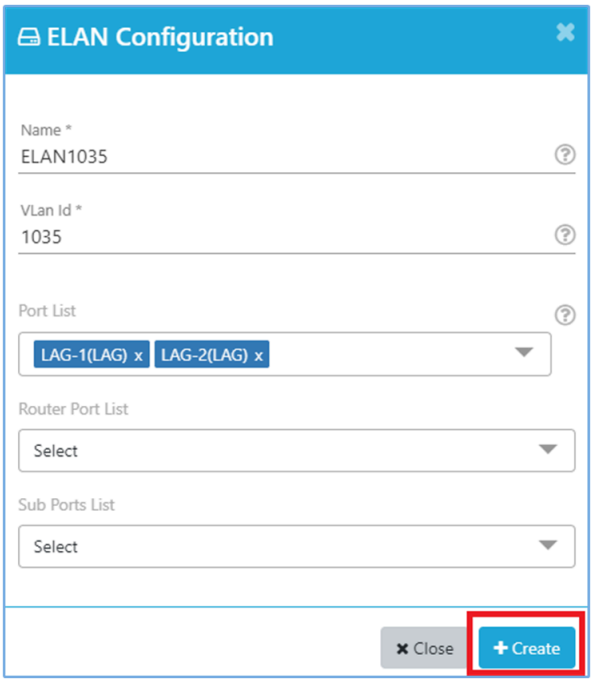
    d. Click **Create**.

Figure 428. Create ELAN



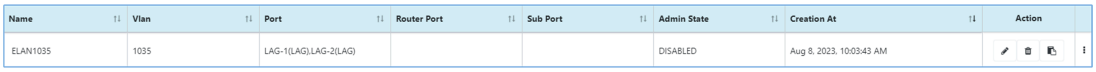
    e. Enter the ELAN configuration and click **Create**.

Figure 429. ELAN Configuration



The following screenshot shows the status of ELAN1035.

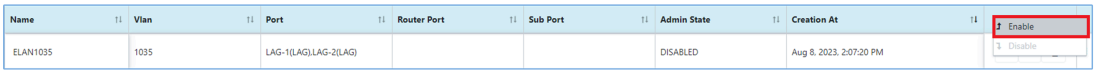
Figure 430. Status of the ELAN1035



Note: The ELAN1035 is in the Disable state.

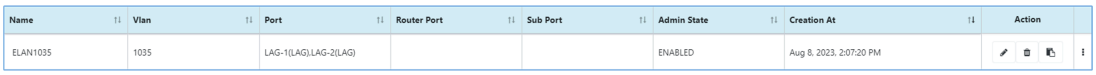
f. Click on three dots and select **Enable** option to enable ELAN1035.

Figure 431. Enable ELAN1035



The following screenshot shows the status of ELAN1035.

Figure 432. Status of the ELAN1035



g. Create the ELAN1022 with port list as LAG-1 and LAG-2 as and enable the ELAN1022.

Note: The traffic must resume.

Configuring DHCPv6 and NTP

This appendix provides information about the configuration of various servers such as the rsyslog server, retention of Kafka messages, retention on alarms and KPIs, log rotation on the host and remote system log servers, DHCPv6 server, NTP server, and so on.

Creating Guest VMs Using Virtual Machine Manager

The virt-manager is also known as Virtual Machine Manager and is a desktop user interface to create and manage the guest virtual machines.

Prerequisites

- Copy the *qcow2* image from the repository server to a location on the bare metal server, where you want to create the VMs.

  Example,

  ```
  scp -r /home1/sdpon/SDPON/VM_QCOW2/vm_image/vm1.qcow2 /var/lib/libvirt/images
  ```

- Rename the image to the required name.
- Radisys provided custom VM image login credentials are ***radisys/radisys***.
- For DHCP IP in Radisys custom VM, execute the ***sudo dhclient <interface-name>*** command if the configuration interface name is not present.
- Execute the IP command and activate the interface and execute the ***dhclient*** command.

  Note: To retrieve the DHCP IP address, the DHCP server must be running on the host machine.

- To install CBAC/RMS in a VM, the VM must have at least 8 GB RAM and CPU.
- Radisys provided custom VM image consists of 50 GB hard disk size by default. For extending hard disk, perform the following.

  1. Execute the following command to verify the custom image size before you extend the hard disk size. The vm1.qcow2 is the image name.

     ```
     sudo qemu-img info /var/lib/libvirt/images/vm1.qcow2
     image: /var/lib/libvirt/images/vm1.qcow2
     file format: qcow2
     virtual size: 50G (53687091200 bytes)
     disk size: 3.3G
     cluster_size: 65536
     Format specific information:
     compat: 1.1
     lazy refcounts: false
     refcount bits: 16
     corrupt: false
     ```

2. Extend the disk hard size to the desired size. Execute the following command to extend the disk size by 25 GB.

```
sudo qemu-img resize vm1.qcow2 +25G
```

3. After extending the hard disk size, execute the following command to verify the extended disk size.

```
sudo qemu-img info /var/lib/libvirt/images/vm1.qcow2
image: /var/lib/libvirt/images/vm1.qcow2
file format: qcow2
virtual size: 75G (80530636800 bytes)
disk size: 3.3G
cluster_size: 65536
Format specific information:
compat: 1.1
lazy refcounts: false
refcount bits: 16
corrupt: false
```

- Ensure that for each VM, a copy of qcow2 is present.
- Ensure that the KVM and *virt-manager* are installed.
- Ensure that the *virt-manager* can access the installation media, locally or over the network.

Launching the Virtual Machine Manager

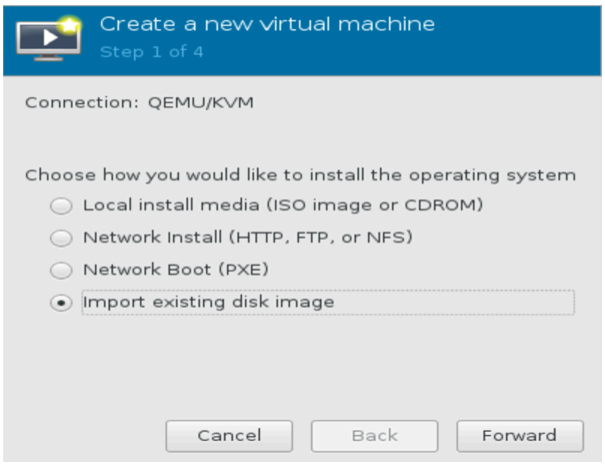
Execute the following command to start the virt-manager application.

```
sudo virt-manager
```

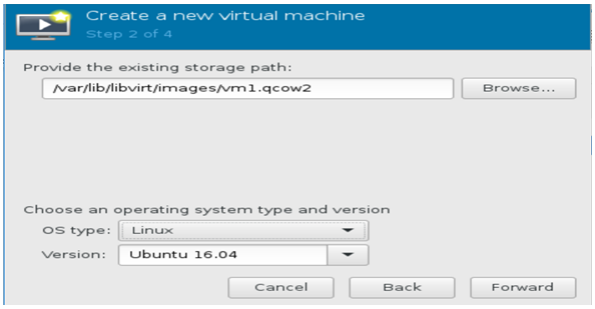
Creating VM

Perform the following steps to create the VM.

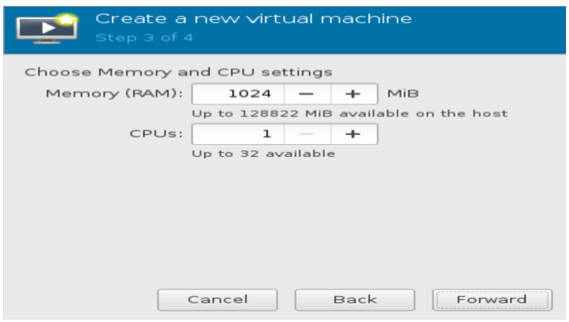
1. From the virt-manager Web GUI, select **File > New Virtual Machine**.
2. Select the **Import existing disk image** option to install the operating system, as shown in the following figure. This option allows you to create a new guest virtual machine and import a disk image to it. The disk image contains a pre-installed and bootable operating system.
3. Click **Forward**.



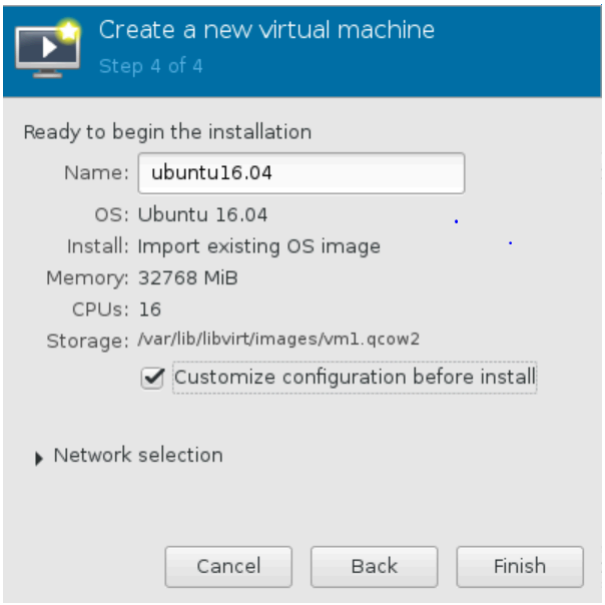
4. Browse to the location of the disk image. Select the required **OS type** and **Version** from the lists, as shown in the following figure. Click **Forward**.



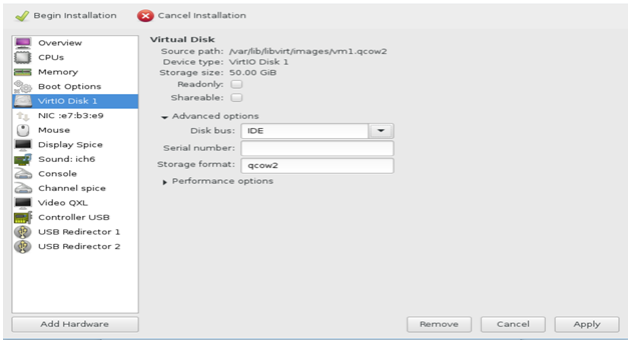
5. Configure the number of CPUs and memory (RAM) that you want to allocate to the virtual machine, as shown in the following figure. Click **Forward**.



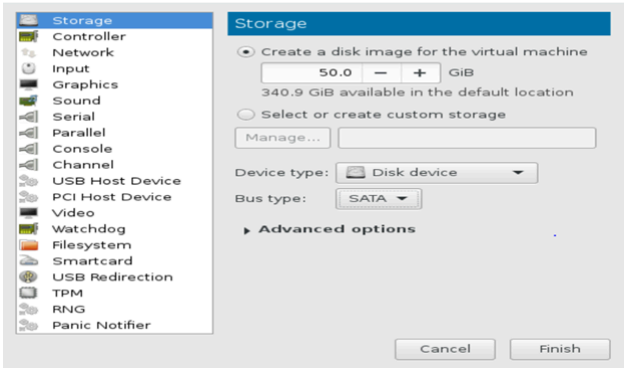
6. Select the *Customize configuration before install* option to configure the primary disk and storage details as shown in the following figure. Click **Finish**.



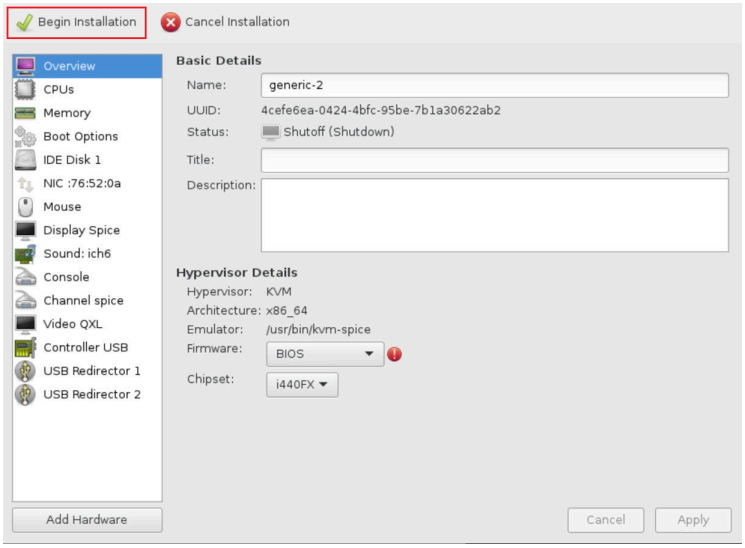
7. From the left menu, select **VirtIO Disk 1**, and the Virtual Disk page displays. Select *IDE* as a disk bus and *qcow2* as a storage format from the drop-down list, as shown in the figure. Click **Apply**.



8. If an additional disk is required, right-click on the Storage option and Select *Add Hardware*. Configure the required details as shown in the figure. Click **Finish**.



9. Click **Begin Installation** to create a VM.



The guest VM is created successfully.

Extending Filesystem Size

If you have extended the VM hard disk in the previous step, perform the following to increase the size of the filesystem to use the added capacity.

1. Log in to the VM created using the custom image and execute the following command to verify the size.

```
radisys@ubuntu:~$ sudo fdisk -l
[sudo] password for radisys:
Disk /dev/vda: 75 GiB, 80530636800 bytes, 157286400 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x7be9f1dc
Device Boot Start End Sectors Size Id Type
/dev/vda1 * 2048 146484375 146482328 69.9G 83 Linux
```

2. Execute the following command to increase the partition size.

```
radisys@ubuntu:~$ sudo parted
GNU Parted 3.2
Using /dev/vda
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted) resizepart 1
Warning: Partition /dev/vda1 is being used. Are you sure you want to continue?
Yes/No? Yes
End? [75.0GB]? 75GB
(parted) quit
```

3. Execute the following command to increase the filesystem size.

```
radisys@ubuntu:~$ sudo resize2fs /dev/vda1
```

4. Execute the following command to verify the increased filesystem size.

```
radisys@ubuntu:~$ df -h
```

Setting Up DHCPv6 Server

Perform the following steps to access the OLT IPv6 address from the DHCPv6 server dynamically.

1. Configure a DHCPv6 server in the BNG on the VLAN sub-interface connected to the NNI port of the OLT.
2. Ensure that the following dhclient configuration lines are present in the `/etc/network/interfaces` file.

```
allow-hotplug eno1
iface eno1 inet6 dhcp
```

3. Configure one subnet in the BNG DHCPv6 server to allocate an IPv6 address to the OLT **eno1** interface.

Configuring NTP Client and Server Parameters

This section covers the configuration of the NTP client and server on the devices.

NTP Server Configuration

The NTP server can be configured in two ways.

1. Using the local clock, configure the `/etc/ntp.conf` file of your server to synchronize with the primary server or directly assign a stratum to it by adding the following lines.

```
server  127.127.1.0  //the server takes it's local clock value to synchronize fudge
 127.127.1.0 stratum 2 //assigning statrum 2 to this server in case local clock has
 to be considered.
```

2. Using the other primary clock source, modify the `/etc/ntp.conf` file of the server to add the primary server as follows.

```
Sample file /etc/ntp.conf :
driftfile /var/lib/ntp/ntp.drift
tos maxdist 16

# Leap seconds definition provided by tzdata
leapfile /usr/share/zoneinfo/leap-seconds.list

# Enable this if you want statistics to be logged.
#statsdir /var/log/ntpstats/

statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
```

```
filegen clockstats file clockstats type day enable

# You do need to talk to an NTP server or two (or three).
#server ntp.your-provider.example

# Specify one or more NTP servers.
server 172.24.100.50 iburst
# pool.ntp.org maps to about 1000 low-stratum NTP servers. Your server will
# pick a different set every time it starts up. Please consider joining the
# pool: <http://www.pool.ntp.org/join.html>
pool 0.debian.pool.ntp.org iburst
pool 1.debian.pool.ntp.org iburst
pool 2.debian.pool.ntp.org iburst
pool 3.debian.pool.ntp.org iburst

# Access control configuration; see /usr/share/doc/ntp-doc/html/accopt.html for
# details.  The web page <http://support.ntp.org/bin/view/Support/AccessRestrictions>
# might also be helpful.
#
# Note that "restrict" applies to both servers and clients, so a configuration
# that might be intended to block requests from certain clients could also end
# up blocking replies from your own upstream servers.

# By default, exchange time with everybody, but don't allow configuration.
restrict -4 default kod notrap nomodify nopeer noquery limited
restrict -6 default kod notrap nomodify nopeer noquery limited

# Local users may interrogate the ntp server more closely.
restrict 127.0.0.1
restrict ::1

# Needed for adding pool entries
restrict source notrap nomodify noquery

# Clients from this (example!) subnet have unlimited access, but only if
# cryptographically authenticated.
#restrict 192.168.123.0 mask 255.255.255.0 notrust

# If you want to provide time to your local subnet, change the next line.
# (Again, the address is an example only.)
#broadcast 192.168.123.255

# If you want to listen to time broadcasts on your local subnet, de-comment the
# next lines.  Please do this only if you trust everybody on the network!
#disable auth
#broadcastclient
# fudge make sure that local clock will be used when no servers are available
fudge  127.127.1.0 stratum 10
restrict localhost
```

NTP Client Configuration

Perform the following steps to configure the Network Time Protocol [NTP] client.

1. Configure the NTP server IP in the `/etc/ntp.conf` file at the OLT, which is a client configuration file. For example, server xxx.xx.xxx.xx iburst

   NTP client configuration can be done through the CBAC configuration. Add the NTP profile while adding OLT from RMS, and the profile is added to the `/etc/ntp.conf` file upon OLT activation.

2. Execute the following command to restart the NTP service. This command synchronizes the time with the NTP server clock.

   ```
   service ntp restart
   ```

3. Use the **ntpq -p** command to view the remote servers configured for NTP.

   Note:

   - The command output displays the remote server IP followed by * symbol. This indicates that time synchronization is in progress.
   - If the offset value is too high in the **ntpq -p** command output, the time is not synchronized.
   - If the time difference between the client and server is more than 20 minutes, NTP does not function properly.
   - If the time difference between the client and server is less than 20 minutes, it requires approximately 15 to 20 minutes to synchronize with the server clock.

Configuring TACACS Server

This section covers the configuration of the TACACS server for remote Authentication, Authorization, and Accounting (AAA) of third-party users.

Remote AAA uses the TACACS protocol that is validated with the following configuration.

Ensure the services **exec** and **PPP** are configured on the TACACS server configuration file.

The following TACACS server configuration file can be used for reference.

- Define where to log the accounting data. Following is the default path for the accounting file.

  Accounting file = `/var/log/tac_plus.acct`

- The following key is used to access TACACS server.

  Key = **testkey123**

- The following are the configuration details for a third-party user with privilege level 15.

  ```
  user = testadmin
  {
  default service = permit
  pap = des "teKrj2bVdPy7." ## created using tac_pwd testkey123 (Password:
  ```

```
sdpon)
service = exec {
priv-lvl = 15
timeout = 15
idletime = 2
}
service = ppp protocol = ssh
{
default attribute = permit
addr=172.27.174.228 ##tacacs server address
priv-lvl = 15
timeout = 5
idletime = 2
Reply-Message = "Welcome to TACACS+ Auth"
}
}
```

The default TACACS is enabled during installation time.

1. CBAC is configured with the default TACACS configuration. Consequently, it allows CBAC to be onboarded onto an RMS that supports TACACS authentication.
2. Onboard the CBAC to RMS.
3. The TACACS profile must be configured from RMS using TACACS+ profiles and attached to the controller. For more information, refer to the *RMS User Guide*.

Note:

- For proper RMS and CBAC functionalities, TACACS+ authentication must be enabled on RMS and all the CBACs. Both RMS and CBAC must communicate with the same TACACS+ server. If different TACACS+ servers are configured for RMS and CBAC, they must have the same user configuration.
- TACACS configuration is only applicable for host SSH login for servers such as RMS master or worker nodes, OLT, repository server, log server, and NTP or SFTP server.

Configuring ACL File

This section covers the configuration of ACL files on the repository server.

The ACL file is present in the **setup_repo** section of the package. Ensure that the admin, operator, viewer groups, and associated users are on the repository server.

The following are the steps to create user groups, users, and passwords for each user.

1. Execute the following commands to create user groups for the admin, viewer, and operator.

```
sudo groupadd admin
sudo groupadd viewer
sudo groupadd operator
```

2. Execute the following commands to create users in the respective group.

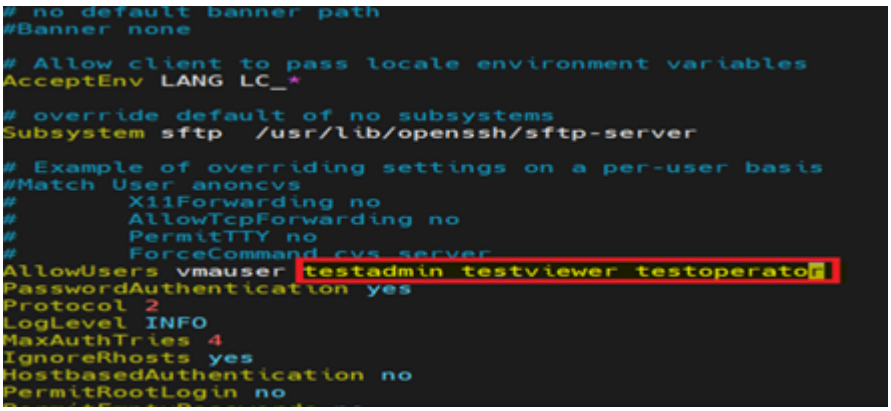
```
sudo useradd -g admin -m <admin-user>
sudo useradd -g operator -m <operator-user>
sudo useradd -g viewer -m <viewer-iuser>
```

3. Execute the following command to set the password for each user.

```
sudo passwd <admin-user>
sudo passwd <operator-user>
sudo passwd <viewer-user>
```

4. Execute the following command to modify `/etc/ssh/sshd_config` file and include newly created users as part of AllowUsers.

```
sudo vim /etc/ssh/sshd_config
```



Note: Ensure that the repository server is updated with the latest package.

5. Execute the following command to restart the service.

```
ssh restart
```

6. Execute the following commands to set the *CBAC_VERSION, RMS_VERSION,* and *ABSOLUTE_PACKAGE_PATH* in the root shell.

```
root@demor:~$ export CBAC_VERSION=<SDPON_Version>
root@demor:~$ export RMS_VERSION=<RMS_Version>
root@demor:~$ export
ABSOLUTE_PACKAGE_PATH=<Absolute_path_where_package_is_copied>
```

Example:

```
root@demor:~$ export CBAC_VERSION=SDPON.1.14.138
root@demor:~$ export RMS_VERSION=RMS.8.10.14
root@demor:~$ export ABSOLUTE_PACKAGE_PATH=/opt
```

7. Execute the following to configure the ACL file on the repository server.

```
root@demor:~# bash acl_rules.sh start
```

Command Output:

```
Synchronizing state of rsync.service with SysV service script with
/lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable rsync
acl_rules: Setting up ACL rules for the restricted files ...
acl_rules: ACL rules for Section 1: /var/www/html/sdpon/index.html set
successfully.
acl_rules: ACL rules for Section 2: deployment_ansible set successfully.
acl_rules: ACL rules for Section 3: deployment-packages set successfully.
acl_rules: ACL rules for Section 4: diagnostic set successfully.
acl_rules: ACL rules for Section 5: templates set successfully.
acl_rules: ACL rules for Section 6: /var/www/html/sdpon/SDPON.1.14.111 set
successfully.
acl_rules: ACL rules for Section 7: ~/SDPON.1.14.111 set successfully.
acl_rules: ACL rules for Section 8: ~/SDPON.1.14.111/k8sdependencies set
successfully.
acl_rules: ACL rules for Section 9: ~/SDPON.1.14.111/docker_images set
successfully.
acl_rules: ACL rules for Section 10: ~/SDPON.1.14.111/setup_repo set
successfully.
acl_rules: ACL rules for Section 11: ~/SDPON.1.14.111/setup_repo/certs set
successfully.
acl_rules: ACL rules for Section 12: ~/SDPON.1.14.111/diagnostic set
successfully.
acl_rules: ACL rules for Section 13: ~/RMS.8.10.4/certs set successfully.
acl_rules: ACL rules for Section 14: ~/RMS.8.10.4/common_docker_images set
successfully.
acl_rules: ACL rules for Section 15: ~/RMS.8.10.4/debian set successfully.
acl_rules: ACL rules for Section 16: ~/RMS.8.10.4/jmap_docker_images set
successfully.
acl_rules: ACL rules for Section 17: ~/RMS.8.10.4/deployment-packages set
successfully.
acl_rules: ACL rules for Section 18: ~/RMS.8.10.4/kubernetes-installation set
successfully.
acl_rules: ACL rules for Section 19:
/var/www/html/sdpon/SDPON.1.14.111/k8sdependencies set successfully.
acl_rules: ACL rules for Section 20: /var/www/html/rms/RMS.8.10.4/certs set
successfully.
acl_rules: ACL rules for Section
 21: /var/www/html/rms/RMS.8.10.4/deploymentpackages
set successfully.
acl_rules: ACL rules for Section 22: /var/www/html/rms/RMS.8.10.4/jmapdeployment-
dualstack set successfully.
acl_rules: ACL rules for Section 23:
/var/www/html/rms/RMS.8.10.4/monitor_deployment set successfully.
acl_rules: ACL rules for Section 24:
/var/www/html/rms/RMS.8.10.4/pon_monitoring_scripts set successfully.
acl_rules: ACL rules for Section
 25: /var/www/html/rms/RMS.8.10.4/kubernetesinstallation
set successfully.
acl_rules: ACL rules for Section 26:
/var/www/html/rms/RMS.8.10.4/monitor_templates set successfully.
acl_rules: ACL rules for Section Miscellaneous set successfully.
```

Troubleshooting

The CBAC architecture extends CLI and Radisys Management System (RMS) Web GUI capability to manage and troubleshoot the system in case of faults. All management functions in the vOLT solution are handled through RMS. It is integrated with CBAC through the REST APIs.

RMS handles various management functions such as configuration, fault, event handling, fetching performance KPIs, and reporting it to the OSS systems. CBAC reports alarms and KPIs to RMS for its consumption.

Accessing Kubectl CLI

Problem Description: kubectl commands throw a "server connection refused" error post-reboot.

Solution: The following steps are applicable if CBAC is installed on the OLT and PODs are running before reboot.

1. Ensure that the NTP synchronization is proper.
2. Date and time must be correct.
3. Execute the following command to restart the kubelet service.

```
sudo service kubelet restart
```

Collecting CBAC Logs

Problem Description: Log collection of all CBAC modules.

Solution: Collect the logs for analysis.

1. Execute the following command to collect the logs for analysis.

```
sudo kubectl get po -o wide
```

Command Output:

```
etcd-0 1/1 Running 0 1d 10.233.102.129 node1
etcd-etcd-defrag-27992880-b4t9x 0/1 Running
external-kafka-0 1/1 Running 1 1d 10.233.75.6 node2
external-kafka-zookeeper-0 1/1 Running 0 1d 10.233.71.4 node3
influxdb-6dbb6d468b-5rppl 1/1 Running 0 1d 10.233.102.137 node1
internal-kafka-0 1/1 Running 0 1d 10.233.71.3 node3
internal-kafka-zookeeper-0 1/1 Running 0 1d 10.233.102.130 node1
intersdpongateway-76475c6bc-26wzc 1/1 Running node1
log-manager-868c7b77d9-sjww5 1/1 Running node1
logstash-logstash-0 1/1 Running node1
lwc-b87bcc6f5-vqdk6 1/1 Running node1
msm-744b967dc6-n667n 1/1 Running node1
openolt-5b667f4c48-95k75 1/1 Running node1
```

```
openonu-85cc67895c-h7mpf 1/1 Running node1
redis-master-0 1/1 Running node1
rwcore-b79498768-gz52h 1/1 Running node1
sdponaccessgateway-dd4b9b55f-5zdhq 1/1 Running node1
sdpondevicemanager-67f8dfdbf8-7kkvx 1/1 Running node1
sdponemscli-557b75f567-w88l5 1/1 Running node1
sdponemsgateway-776cd6dc84-jntlj 1/1 Running node1
sdponmonmgr-7dd7cb798f-b69x2 1/1 Running node1
sdponncm-85cc88d76b-z55fb 1/1 Running node1
sdponnda-76f466574f-5ht9n 1/1 Running node1
sdponsecurity-6c9bc6b879-blkrq 1/1 Running node1
sdponsubscribermanager-b8dddd79c-vhl77 1/1 Running node1
sdpontelemetry-d58d686d4-z5p4h 1/1 Running node1
voltctl-5954d74fdf-5bm9s 1/1 Running node1
```

2. Execute the following command to collect the logs of all the services.

```
sudo kubectl logs <service-name> <service-name>.txt
```

where <*service-name*> is the name of the service identified by the **kubectl** command.

3. Collect the Kafka message logs.
Log in to the internal-kafka-0 and execute the following command in the Kafka POD on the corresponding topics to view the message logs of the topics.

```
sudo kubectl exec -it internal-kafka-0 bash
Config Logs:
a. AccGw:
/opt/bitnami/kafka/bin/kafka-console-consumer.sh --bootstrap-server
localhost:9092 --topic ACCESSGW --from-beginning
b. SubMgr:
/opt/bitnami/kafka/bin/kafka-console-consumer.sh --bootstrap-server
localhost:9092 --topic SUBMGR --from-beginning
c. EmsGw:
/opt/bitnami/kafka/bin/kafka-console-consumer.sh --bootstrap-server
localhost:9092 --topic EMSGW --from-beginning
d. DevMgr:
/opt/bitnami/kafka/bin/kafka-console-consumer.sh --bootstrap-server
localhost:9092 --topic DEVICEMGR --from-beginning
Alarms:
e. DeviceMgr:
/opt/bitnami/kafka/bin/kafka-console-consumer.sh --bootstrap-server
localhost:9092 --topic DEVMGR-ALARM --from-beginning
f. EmsGW:
/opt/bitnami/kafka/bin/kafka-console-consumer.sh --bootstrap-server
localhost:9092 --topic EMSGW-ALARM --from-beginning
g. Telemetry:
/opt/bitnami/kafka/bin/kafka-console-consumer.sh --bootstrap-server
localhost:9092 --topic SDPON-ALARM --from-beginning
KPIS:
h. DeviceMgr:
/opt/bitnami/kafka/bin/kafka-console-consumer.sh --bootstrap-server
localhost:9092 --topic DEVMGR-KPI --from-beginning
i. EmsGW:
/opt/bitnami/kafka/bin/kafka-console-consumer.sh --bootstrap-server
localhost:9092 --topic EMSGW-KPI --from-beginning
j. Telemetry:
```

```
/opt/bitnami/kafka/bin/kafka-console-consumer.sh --bootstrap-server
localhost:9092 --topic SDPON-KPI --from-beginning
```

4. Log in to any of the external-kafka-0 and execute the following command on the CBAC server.

```
sudo kubectl exec -it external-kafka-0 bash
Notification: /opt/bitnami/kafka/bin/kafka-console-consumer.sh --bootstrapserver
localhost:9092 --topic EMSNOTIFICATION --from-beginning
Alarms: /opt/bitnami/kafka/bin/kafka-console-consumer.sh --bootstrap-server
localhost:9092 --topic EMSFAULT--from-beginning
KPIS: /opt/bitnami/kafka/bin/kafka-console-consumer.sh --bootstrap-server
localhost:9092 --topic EMSKPINOTIFICATION--from-beginning
```

5. Collect the LWC logs. See the Accessing LWC *(on page 271)* section for the commands.
6. Collect the OLT logs.
   Log in to the OLT as the root user (root/ONL) and copy the following logs.

```
/var/log/*
```

7. Collect the ONT logs.
   Connect the serial console to the ONT and log in using the login credentials **(admin/admin)**.

```
GEN# cd log
Log# show log poncfg
Log# show log pondrv
Log# show log dsploam
Log# show log brmgr
Log# show log ploamevent
Log# show log omci_task
Log# show log omciagt_cfg
Log# show log omciagt_main
Log# cd omci
Omci# show omci receive packets
Omci# show omci transmit packets
Omci# show stream us
Omci# show stream ds
Omci# show me all
Omci# show ont running config
Omci# show omci receive packets
Omci# show omci transmit packets
Omci# igmp
Igmp# show table
Igmp# exit
GEN# linuxshell
# bs /b/e port/index=wan0
# bs /b/e gem
# bs /b/e ingress_class
# bs /b/e bridge
# bs /b/e port/index=lan0
```

Fetching Software Versions of OLT and ONU

Problem Description: To fetch the software versions of OLT.

Solution: Perform the following steps to retrieve the software versions of OLT and ONU.

1. After the OLT activation, you can view the OLT system information and version information using the ***oltcli*** command as shown below.

```
admin@localhost:/broadcom$ sudo oltcli
*****************************
* Openolt Debug CLI *
*****************************
```

2. Execute the following command to view the OLT system information.

```
OLT> show system
pon_dev_id device_mode iwf_mode state
  1          XGSPON      PER_FLOW UP
platform: phoenix
platform variant: 1RU x/gpon
board_technology: xgspon
serial_number: 722026030704
num_of_pon_ports: 16
num_of_nni_ports: 6
mac_address: 28:b9:d9:e3:28:90
inband_interface: eno1
inband_vlan: 222
system state: Active
Openolt Voltha state: Connected
Openolt agent uptime: 6:D 0:H 16:M 57:S
System Monitoring: Running
NS Service uptime: 6:D 0:H 16:M 59:S
NS NDA state: Connected
```

3. Execute the following command to view the OLT version information.

```
OLT> show version
software_version: SDPON_BINS_1.15.123
hardware_version: 3708-32-256
firmware_version: BAL.3.12.4
onl_version: ONL-OS10_2023-02-24.0611-3b26b77_AMD64
cpld_version: 6.3
mb_fpga_version: 0x20110520
db_fpga_version: 0x20110520
bios_version: 1.0.07
onie_version: mainlineONIE-202102251244-dirty
device0 chip_family: Aspen
device0 chip_revision: A1
device1 chip_family: Aspen
device1 chip_revision: A1
```

The software version for the ONU is maintained by Radisys. The software images shared by TWSH are in the following format.

```
BCM_XGSPON-BCM6858X_nand_cferom_fs_128-VB14_R1B01D173e69e6-
_secureboot_ram_kernel_fs
```

The software version of the ONU after an upgrade is always 1.0.0.

Rebooting OLT

Problem Description: After the OLT reboot, the **ma1** interface is not activated.

Solution: Execute the following commands to recover the **ma1** interface.

```
$ sudo ifconfig down
$ sudo ifconfig up
```

Reboot Reason

The following table explains different scenarios that can result in the reboot or halt of the OLT.

The table shows the reboot reason details in the OLT reboot notification.

Table 10. Reboot Reason

Scenario	Reboot Reason	Action
The audit logs are placed in the `/var/log/audit` partition location. The OLT is halted when the available space is less than 300MB in the partition. A manual power cycle is required to bring up the setup.	Audit initiated reboot due to audit logs size above the limit.	System Halt
CBAC monitors the temperature and initiates a system halt if the current temperature is more than the configured threshold value.	CBAC initiates shutdown due to high temperature.	System Halt
The user initiates a reboot from the OLT console. For example-reboot, shutdown, or power off Linux commands.	OLT initiated a reboot.	System Reboots
ONL image upgraded	ONL software upgrade process initiated the OLT reboot.	System Reboots
Any abrupt reboot is due to some issue in the system and the operating system is not responding.	• Hardware watchdog timeout issue initiated the OLT reboot. • Reboot due to CPLD watchdog timeout	System Reboots
Firmware upgraded (BIOS, CPLD, and FPGA)	The firmware upgrade process initiated the OLT reboot.	System Reboots
CBAC commands to reboot or reset the OLT.	SDPON initiated a reboot.	System Reboots

Table 10. Reboot Reason (continued)

Scenario	Reboot Reason	Action
The second level of temperature monitoring is by the platform software.	ONLPD initiated a reboot due to high temperature.	System Reboots
Software watchdog monitoring and recovery. For more information, see Monitoring Software Watchdog *(on page 249)*.	• Radisys watchdog initiated a reboot. • Radisys watchdog initiated a reboot and factory restore.	System Reboots
CMOS register cleared by software or manually	Reboot due to clearing Complementary Metal-Oxide-Semiconductor (CMOS).	System Reboots
Reboot initiated by software or manually by configuring CPLD registers	Reboot due to force power cycle.	System Reboots
Reboot due to any other reset triggered by software	Reboot due to soft reset.	System Reboots
A short press of the reset button or OS kernel panic	Reboot due to kernel panic or a short press of the reset button.	System Reboots
A long press of the reset button	• Cold reset • Global reset • A long press of the reset button	System Reboots
Power fluctuation or physical power cycle of OLT	OLT rebooted due to power interruption.	System reboots and hardware is rebooted
The OLT is rebooted due to the BAL disconnect	Reboot due to the BAL disconnect	System Reboots

Monitoring Software Watchdog

A software watchdog monitoring system is implemented to recover the system from issues related to OLT application failures. The software watchdog periodically monitors whether the main OLT software applications are up and running and performs the recovery action if any of them are not running.

The following recovery actions are available.

1. If any of the main applications are not running, the software watchdog restarts the application.
2. If the issue persists after an application restart, then OLT reboots with a reason as ***Rsys Watchdog Initiated Reboot***.
3. After the OLT reboot, if any OLT main applications still have issues, the software watchdog initiates a reboot and auto-updates the ONL image to the version updated through ONIE. Now, the OLT reboots from the other partition with a reason as ***Rsys Watchdog Initiated Reboot and Factory Restore***.

If the issue still exists in the other partition, repeat the above-mentioned recovery actions from step 1 to step 3.

Deploying CBAC

1. **Problem Description**: Kube-dns is going into a crashloop back state.

   Solution 1: Check all the nodes if *resolv.conf* file exists.

   ```
   cat /etc/resolv.conf
   nameserver 172.24.100.50
   ```

   Solution 2:

   Execute the following commands to check if the firewall is disabled on all the nodes.

   ```
   sudo systemctl disable firewalld
   sudo systemctl reboot
   sudo systemctl disable ufw
   sudo systemctl reboot
   ```

   Note: Ensure to run the cleanup command only if the Kubernetes is up and running.

2. **Problem Description**: The cleanup operation fails with !!! Kubernetes clean-up failed !!! error.

   Solution: Execute the **docker rm** command and check for the error driver "aufs" failed to remove the root filesystem

   ```
   sudo docker rm -f $(sudo docker ps -a -q)
   Error response from daemon: driver "aufs" failed to remove root filesystem
   for 380ca7ca6c894e54639740ad133e7514fcec386781dc445484c16335f68ffe70: no
   such file or directory
   ```

   Log in as a root user.

   ```
   $ sudo su,
   $ rm -rf /var/lib/docker/containers/*
   ```

   Execute the cleanup command.

   ```
   $ sudo ansible playbook cleanup.yml
   ```

3. **Problem Description**: Unable to install packages due to following error.

```
failed: E: Unable to correct problems, you have held broken packages.\n", "rc":
100, "stderr": "E: Unable to correct problems, you have held broken
packages.\n", "stderr_lines": ["E: Unable to correct problems, you have held
broken packages."], Depends: libcurl3-gnutls (= 7.47.0-1ubuntu2.9) but 7.47.0-
1ubuntu2.14 is to be installed\n", "stdout_lines": ["Reading package lists...",
"Building dependency tree...", "Reading state information...", "Some packages
could not be installed.
```

Solution: Execute the following commands to install the respective packages

```
$ sudo apt-get install libcurl3-gnutls=7.47.0-1ubuntu2
$ sudo apt install curl
```

4. **Problem Description**: Kubernetes activation fails while populating the inventory.

Solution: Update the gateway IP address in the interfaces file.

```
auto ma1
iface ma1 inet static
address 172.27.174.102
netmask 255.255.255.0
gateway 172.27.174.254
```

5. **Problem Description**: Kubespray updates the `/etc/hosts` file with the old IP address.

Solution: Execute the following command to perform the clean up operation and reboot the system.

```
$ ansible-playbook cleanup.yml
$ reboot
$ ansible-playbook deployment.yml
```

6. **Problem Description**: Kubespray cleanup fails with the following error.

```
"Unable to start service networking: Job for networking.service failed because
the control process exited with error code. \nSee \"systemctl status
networking.service\" and \"journalctl -xe\" for details.\n"}
```

Solution: The networking service is not running on the setup.

- Verify the entries in the `/etc/network/interfaces` file for invalid entries. Then, remove and restart the networking service.
- Execute the **sudo service networking** status command and check for more details using the **journalctl** command. If any of the interfaces are not coming up, reboot the system.

7. **Problem Description**: Kubernetes PODs that go to an evicted state or kubelet service do not come up with the following error.

```
“9175 event.go:265] Unable to write event: 'Post
https://[xx.xx.xx.xx]:6443/api/v1/namespaces/default/events: dial tcp
xx.xx.xx.xx:6443: connect: connection refused' (may retry after sleeping)
2021-09-17 10:37:16.6059 localhost kubelet[9175]: F0917 10:37:16.604801 9175
server.go:182] Failed to create listener for podResources endpoint: failed to
```

```
create temporary file: open /var/lib/kubelet/pod-resources/959020798: no space
left on device”
```

However,there is enough disk space available in the disk partition, but the number of inodes has crossed the disk pressure threshold value.

Solution: If the IUse% is more than 90%, check the inode consumption on the */var* in your system using *df—i*.

a. Execute the *freed_inode.sh* script, which is present in the CBAC release package. The CBAC release package is available at SDPON-`buildpackage/deployment/freed_inode.sh` path.

b. Copy the script from the release package to the home path on ROLT.

c. Execute the bash *freed_inode.sh* script.

Verifying IPtable SYN FLOOD Attack

Problem Description: The OLT IPtable rule to block TCP SYN flood attacks.

Solution: Perform the following steps.

Execute the **iptables -L** command to verify the pre-configured rules present in iptables.

```
root@localhost:~# sudo iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
syn_flood tcp -- anywhere 172.27.174.224 tcp
flags:FIN,SYN,RST,ACK/SYN
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
Chain syn_flood (1 references)
target prot opt source destination
ACCEPT all -- anywhere anywhere limit: avg 1/sec
burst 3
DROP all -- anywhere anywhere
```

To test syn flood attack, install the hping3 tool in a server and execute the following command.

```
$ sudo hping3 -V -c 1000 -d 100 -S -p 80 --flood 172.27.173.54
```

Where,

-V indicates verbose

-c indicates number of packet

-d indicates packet size

-p indicates destination port (here HTTP)

-S indicates syn flag set

-- indicates flooding packet

At the OLT side verify the accepted and dropped packet count with the following command *iptables -L -v -n*

Validating NTP Server Synchronization

Problem Description: To check whether the client (OLT) is synchronized with any of the NTP servers.

Solution. Perform the following steps.

- Execute the following command on the OLT:

```
admin@newhost:~$ ntpq -p
remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
172.27.172.148  .STEP.          16 u    -  512    0    0.000    0.000   0.000
*myhost          10.51.128.51     2 u   66   64  377    0.669  -55.610 1582.50
```

If the '*' symbol appears before the listed servers, the OLT is in synchronization with the NTP server.

Check the reach values if the OLT is not synchronized with any of the servers.If it is 0, perform the following steps.

1. Ping the NTP server to check if it is reachable.
2. If the NTP server is reachable, then access the NTP server and execute the **ntpq -p** command on the server to check if the NTP server is synchronized with the OLT. If not, restart the ntp daemon using the **sudo service ntp restart** command.
3. Recheck if the NTP server is synchronized and check the OLT again. Sometimes, the IT team synchronizes the NTP server. If not, we can restart the ntp daemon restart using the **sudo service ntp restart** command.
4. If the NTP server is not accessible, check the packets coming from the server using the **tcpdump** command. The command output shows whether the NTP server is synchronized.

```
E.g.
sdpon@ubuntu> sudo tcpdump -vvAs0 port 123
tcpdump: listening on enp8s0f0, link-type EN10MB (Ethernet), capture size 262144
bytes
10:57:06.620162 IP (tos 0xb8, ttl 64, id 16900, offset 0, flags [DF], proto UDP
(17), length 76)
172.27.172.197.ntp > indc05.radisys.com.ntp: [udp sum ok] NTPv4, length 48
Client, Leap indicator: clock unsynchronized (192), Stratum 0 (unspecified),
poll 6 (64s), precision -23
```

Problem Description: The NTP client is not able to resolve hostnames, that is, the server is not shown in the ntpq -p command output.

Solution. Perform the following steps.

1. Check if the hostname can be resolved using the **ping** command. If not, check if the hostname needs to be added in the *resolv.conf* or */etc/hosts* files.
2. If the hostname is resolved using the **ping** command, then check if ntp has permission to access */etc/hosts*. Execute the following command with strace and check the log.

```
sudo strace -f -o /tmp/ntp_trace /usr/sbin/ntpd -p /var/run/ntpd.pid -g -u 100:103
```

If appropriate permission is not there, add permission to the /etc/hosts file to be read by ntp daemon.

Validating Unicast Traffic

To verify the unicast traffic, you must install the DHCP server at the BNG gateway and create a VLAN tagged interface with CTag and STag.

At BNG:

Perform the following steps in the Border Network Gateway (BNG).

1. Execute the following commands to create a VLAN tagged network interface.

```
sudo vconfig add eth0 2
sudo ifconfig eth0.2 up
sudo vconfig add eth0.2 124
sudo ifconfig eth0.2.124 10.10.3.1/24 up
```

   For in-band management mode:

   a. Create a VLAN tagged network interface with the VLAN ID mentioned in the `/broadcom/olt_config` file.

```
sudo vconfig add eth0 100 (assuming eth0 is the interface, which is connected to
 the NNI port)
sudo ifconfig eth0.100 up
```

   b. Configure the DHCP server for the interface, which is created with the VLAN ID mentioned in the earlier step.

   c. If in-band interface of the OLT uses the fixed IP address, change the DHCP server configuration file with the MAC and IP mapping as follows:

      For example:

```
host localolt {
hardware ethernet b8:6a:97:54:e8:f8;
fixed-address 192.168.10.58;
}
```

2. Execute the following command to install the DHCP server.

```
sudo apt-get install isc-dhcp-server
```

3. Modify the following path in the */etc/default/isc-dhcp-server* file to specify the network interface for the DHCP server.

```
vim /etc/default/isc-dhcp-server
```

4. Configure the interface.

```
INTERFACES="eth0.2.124"
```

5. Modify the */etc/dhcp/dhcpd.conf* file to configure the subnet. The isc-dhcp-server requires the subnet that matches the interface IP address.

```
subnet 10.10.3.0 netmask 255.255.255.0
{
range 10.10.3.2 10.10.3.240;
option routers 10.10.3.1;
}
```

6. Restart the DHCP server.

```
sudo service isc-dhcp-server restart
```

At RG:

Perform the following steps in the RG.

1. Execute the following command to add the interface connected to the RG in the namespace.

```
sudo ip netns add rg
sudo ip link set eth0 netns rg
```

2. Execute the following command to assign the IP address to the RG interface.

```
sudo dhclient eth0
```

Validating IGMP and Multicast Traffic

At BNG, perform the following steps to verify the IGMP and multicast traffic.

1. Execute the following commands to create a VLAN tag interface with VLAN 4000 for the interface connected to the NNI port of OLT.

```
sudo vconfig add eth0 4000
sudo ifconfig eth0.4000 up
sudo ip link add veth10 type veth peer name veth11
sudo ip link set veth10 up
sudo ip link set veth11 up
```

2. Execute the following command to install the VLC player.

```
sudo apt-get install vlc
```

3. Execute the following commands to create a namespace and in the namespace add the interfaces created in step 1.

```
sudo ip netns add mcast
sudo ip link set eth0.4000 netns mcast
sudo ip link set veth11 netns mcast
```

4. Execute the following commands to configure the following settings in the namespace.

```
sudo ip netns exec mcast bash
sudo ifconfig eth0.4000 192.168.1.254/24 up
sudo ifconfig veth11 20.20.20.3/24 up
sudo echo "3" > /proc/sys/net/ipv4/conf/eth0.4000/force_igmp_version
sudo sysctl -w net.ipv4.ip_forward=1
sudo route -n add -net 224.0.0.0 netmask 240.0.0.0 dev eth0.4000
sudo sysctl -w net.ipv4.conf.eth0/4000.rp_filter=0
```

5. Execute the following commands to install the improxy package on the BNG.

```
git clone https://github.com/haibbo/improxy.git
cd improxy
make all
```

6. Execute the following command to configure the improxy application.

```
Edit sample.conf file with below lines
igmp enable version 3
upstream veth11
downstream eth0.4000
```

Note: You cannot achieve end-to-end automatic multicast from the BNG gateway due to some unknown issue. Hence, you can send the stream continuously at the eth0.4000 interface and test the control message flow for JOIN and LEAVE from the improxy application. Ideally, the multicast packet for a particular address must come from the upstream interface.

7. Execute the following command to start the improxy application.

```
./improxy -c sample.conf -d 5
```

8. Copy any video file from the system.
9. It is recommended to start the VLC multicast stream from the same namespace using the following command in a different terminal. This starts the video multicast stream in a loop.

```
vlc -vvv <video_file_name> --sout
'#duplicate{dst=rtp{mux=ts,dst=232.43.211.234,sdp=sap,name="TestStream"}}' --
ttl 32 -L
```

Note: You cannot execute the above command with root user permission. Ensure that you switch to another user other than the root user.

At RG, execute the following commands:

1. Execute the following command to install the VLC player.

```
sudo apt-get install vlc
```

2. Ensure that the IP address is assigned to the RG interface before you execute the following commands.

```
sudo ip netns exec rg bash
sudo ifconfig eth0 multicast
sudo sysctl -w net.ipv4.ip_forward=1
sudo echo "3" > /proc/sys/net/ipv4/conf/eth0/force_igmp_version
sudo route -n add -net 224.0.0.0 netmask 240.0.0.0 dev eth0
sudo sysctl -w net.ipv4.conf.eth0.rp_filter=0
```

3. Execute the following command at RG to send an IGMP join.

```
vlc rtp://232.43.211.234:5004
```

Note:

- Ensure that you execute the command in a VNC session. Otherwise, the video looks intermittent.
- You cannot execute the above command with the **root** user permission. Ensure that you switch to another user other than the root user.
- IGMP join is received at LWC and is sent further to the BNG. The traffic flow is pushed to the OLT for multicast after the video is seen on VLC, which is sent through the BNG gateway.

Mirroring on OLT Data Ports

CBAC supports mirror traffic passing through OLT of the ingress, egress, or both traffic on the specified PON or network ports.

Enabling Mirror on OLT Data Ports

Execute the following command to enable the mirror feature on data ports using the CBAC CLI.

```
SDPON#mirror-session mirror1
SDPON(mirror1)#destination-interface NNI-3
SDPON(mirror1)#source-interface PON-1 techtype gpon
SDPON(mirror1)#direction ingress
SDPON(mirror1)#vlan 100
SDPON(mirror1)#enable
SDPON(mirror1)#commit
```

Disabling Mirror on OLT Data Ports

Execute the following command to disable the mirror feature on data ports using the CBAC CLI.

```
SDPON#mirror-session mirror1
SDPON(mirror1)#disable
SDPON(mirror1)#commit
```

Deleting Mirror on OLT Data Ports

Execute the following command to delete the mirror feature on data ports using the CBAC CLI.

```
SDPON#no mirror-session mirror1
SDPON#commit
```

Uninstalling Microservices

This section covers the procedure to uninstall the CBAC microservices.

The following microservices are deployed in CBAC.

- **VOLTHA Service**
  - Consul stateful set and service
  - Rw-core
  - OpenOLT adapter
  - Open ONU adapter
  - voltctl
- **CBAC**
  - Access gateway deployment
  - EMS CLI deployment
  - EMS CLI node port service
  - Telemetry deployment
  - Device manager deployment
  - EMS gateway deployment and node port service
  - Subscriber manager deployment
  - Security deployment

- Log manager deployment
- Microservice-manager (MSM) agent

- **Platform**
  - Kafka
  - Zookeeper
  - etcd
  - Filebeat
  - Logstash
  - Influxdb
  - Redis

Perform the following steps, to uninstall or delete the services of the CBAC deployment.

1. Execute the following command to delete the CBAC release.

```
$ sudo helm delete <release-name>
```

2. Execute the following command to delete the CBAC release permanently.

```
$ sudo helm delete --purge <release-name>
```

Note: If you want to redeploy the microservices, you must clean up the persistent data.

Collecting CBAC Logs With or Without OLT Credentials

This section covers the CBAC log collection procedure with or without OLT user login credentials.

Collecting CBAC Log Using oltausr Credentials

You can collect the logs from the CBAC solution. The log file can be then attached to the ticket raised towards the Radisys Technical Assistance Center (TAC) for further analysis. TAC can be reached using the following contact information. E-mail: bba_tac@radisys.com

Perform the following steps to collect the logs.

1. Log in to the CBAC EMS CLI through SSH using the IP address assigned to the POD.
2. Execute the following command to retrieve the IP address of the POD.

```
demo@demo1:~$ sudo kubectl get pods -o wide
sdponemscli-76b59765bf-8x5kc 1/1 Running 0 28d
10.233.77.179 demo1 <none> <none>
```

3. After successful login, execute the following command to change the working directory to conf.

```
cd ./ems-cli/conf
```

4. Populate the *log_conf.yaml* file as per the Kubernetes infrastructure along with the OLT details.

   Execute the following command to collect the logs from various directories.

```
sdpon-cli>>> sdpon get-logs -f=log_conf.yaml
```

   Note: The `sdpon get-log` log collection method is intended as a backup for the new log collection method, which uses the managed element `me-id`. It must only be used if the new log collection fails, and not as the default option. This method deprecates in the future releases.

5. After the log collection operation is completed, you can retrieve the details of the directory where the files are stored in the console.

   Example:

```
sdpon-cli>>> sdpon get-logs -f=log_conf.yaml
Aug 11 2020 09:41:58 : Creating ansible inventory
Aug 11 2020 09:41:58 : COLLECTING SDPON-LOGS
[WARNING]: Ansible is in a world writable directory (/etc/logdump/inventory),
ignoring it as an ansible.cfg source.
PLAY
*********************************************************************
TASK [setup]
*********************************************************************
ok: [master]
TASK [Copying playbook master to collect OLT logs] ****************************
changed: [master]
TASK [Copying inventory.cfg to master node]
**********************************
changed: [master]
PLAY
*********************************************************************
TASK [Copying configuration file on all nodes]
*******************************
changed: [master]
TASK [Collecting all the required logs]
***************************************
changed: [master]
TASK [debug]
*********************************************************************
ok: [master] => {
"msg": [
"",
"Aug 11 2020 09:42:04 : Collecting OLT logs if present",
"Aug 11 2020 09:42:23 : Collecting all k8s pods' logs",
"/home/demo/.ansible/tmp/ansible-tmp-1597138924.21-
179396727457111/log_collecter.sh: line 338: /tmp/SDPON-SYSTEM-LOGS:11-08-2020-
09:41:58/demo1/KubernetesStats/pod_logs/k8s_etcd.txt: No such file or
directory",
"Aug 11 2020 09:42:23 : Collecting the gluster statistics",
"Aug 11 2020 09:42:24 : Collecting latest Alarms, Events and KPIs",
"Aug 11 2020 09:42:24 : Collecting the captured Auditlogs",
"Aug 11 2020 09:42:24 : Collecting the data present in ETCD",
"Aug 11 2020 09:42:24 : Collecting the VOLTHA logs",
```

```
"Aug 11 2020 09:42:24 : Collecting the ONOS logs",
"Aug 11 2020 09:42:24 : Collecting the Consul data",
"Aug 11 2020 09:42:24 : Copying the SystemInfo logs",
"Warning: Permanently added '192.168.122.14' (ECDSA) to the list of
known hosts.",
"",
"Aug 11 2020 09:42:26 : Collected all the required logs",
"Aug 11 2020 09:42:26 : Collected logs are stored in tar format"
]
}
PLAY RECAP
*********************************************************************
master : ok=6 changed=4 unreachable=0 failed=0
Aug 11 2020 09:42:26 : LOGS collected, Available at "/tmp/SDPON-SYSTEMLOGS:
11-08-2020-09:41:58"
```

6. The collected log is compressed and stored at the */mnt/onl/sdpon/logdumps/* file.

```
sdpon-cli>>> sdpon get-logs -f=log_conf.yaml
Oct 12 2021 12:03:24 : INFO glusterfs node count is not configured
[WARNING]: Ansible is in a world writable directory (/home/sdpon/ems-cli/conf),
ignoring it as an ansible.cfg source.
Oct 12 2021 12:03:25 : Creating ansible inventory
Oct 12 2021 12:03:25 : COLLECTING SDPON-LOGS
[WARNING]: Ansible is in a world writable directory (/etc/logdump/inventory),
ignoring it as an ansible.cfg source.
PLAY
***************************************************************************
TASK [setup]
*******************************************************************
ok: [setup-255]
TASK [Copying playbook master to collect OLT logs] ****************************
changed: [setup-255]
TASK [Copying polt BAL object dump script]
***********************************
changed: [setup-255]
TASK [Copying inventory.cfg to master node]
*********************************
changed: [setup-255]
TASK [Copying certs to the host machine]
************************************
changed: [setup-255] => (item=/etc/ssl/certs/server.crt)
changed: [setup-255] => (item=/etc/ssl/certs/client.crt)
changed: [setup-255] => (item=/etc/ssl/certs/client.key)
PLAY
***************************************************************************
TASK [setup]
*******************************************************************
ok: [setup-255]
TASK [Copying configuration file on all nodes]
*******************************
ok: [setup-255]
TASK [set_fact]
*****************************************************************
ok: [setup-255]
TASK [Collecting all the required logs]
************************************
changed: [setup-255]
```

```
TASK [debug]
*********************************************************************
ok: [setup-255] => {
"msg": [
"",
"Oct 12 2021 12:03:33 : Collecting dump of devices and flows",
"Oct 12 2021 12:03:36 : Collecting pOLT logs if present",
"",
"PLAY [OLT_IP]
*********************************************************************",
"",
"TASK [Executing OLT BAL object dump script]
***********************************",
"fatal: [setup-255]: UNREACHABLE! => {\"changed\": false, \"msg\":
\"Invalid/incorrect password: Warning: Permanently added '10.250.250.5' (ECDSA)
to the list of known hosts.\\r\\nPermission denied, please try again.\",
\"unreachable\": true}",
"\tto retry, use: --limit @/tmp/collect_olt_logs.retry",
"",
"PLAY RECAP
*********************************************************************",
"setup-255 : ok=0 changed=0 unreachable=1
failed=0 ",
"",
"Oct 12 2021 12:05:26 : Collecting all k8s pods' logs",
"",
"",
"Decoding OMCI messages from Kafka topic \"OMCI\" : ? ",
"Decoding OMCI messages from Kafka topic \"OMCI\" : ? ",
.
.
"Decoding OMCI messages from Kafka topic \"OMCI\" : ? Refer to `pcaps`
dir for the OMCI pcap/s",
"real\t0m 50.91s",
"user\t0m 5.59s",
"sys\t0m 0.83s",
"tar: removing leading '/' from member names",
"Oct 12 2021 12:07:25 : Collecting latest Alarms, Events and KPIs",
"Oct 12 2021 12:09:29 : Collecting the captured Auditlogs",
"Oct 12 2021 12:09:29 : Collecting the data present in ETCD",
"Oct 12 2021 12:09:31 : Copying the SystemInfo logs",
"Oct 12 2021 12:09:31 : Collected all the required logs",
"Oct 12 2021 12:09:46 : Copying the SDPON-SYSTEM-LOGS-12-10-2021-12-
03-24.tar to Remote Server 30.30.30.1",
"Oct 12 2021 12:09:47 : Collected logs are stored in tar format"
]
}
TASK [Deleting the previously copied files]
***********************************
ok: [setup-255]
PLAY
*****************************************************************************
TASK [setup]
*********************************************************************
ok: [setup-255]
TASK [Deleting the previously copied files on the master node] *****************
changed: [setup-255] => (item=/tmp/collect_olt_logs.yml)
changed: [setup-255] => (item=/tmp/get_olt_dumps.sh)
changed: [setup-255] => (item=/tmp/inventory.cfg)
```

```
changed: [setup-255] => (item=/etc/ssl/certs/server.crt)
changed: [setup-255] => (item=/etc/ssl/certs/client.key)
changed: [setup-255] => (item=/etc/ssl/certs/client.crt)
PLAY
*********************************************************************
TASK [setup]
*********************************************************************
ok: [setup-255]
TASK [Ansible delete file glob]
*********************************************
ok: [setup-255]
TASK [Ansible remove file glob]
*********************************************
PLAY RECAP
*********************************************************************
setup-255 : ok=15 changed=6 unreachable=0 failed=0
Oct 12 2021 12:09:53 : LOGS collected, Available at
"/mnt/onl/sdpon/logdumps/SDPON-SYSTEM-LOGS-12-10-2021-12-03-24.tar"
Log collection has taken 6 minutes
+---------+--------------+-----------+---------------+
| STATUS | ERROR MESSAGE | ERROR CODE | RESPONSE DATA |
+---------+--------------+-----------+---------------+
| success | | | |
+---------+--------------+-----------+---------------+
```

Collecting CBAC Log Without Using oltausr Credentials

1. Execute the following command to start the log collection.

```
managed-element log-collection -ME_ID*=olt1 -f=logcollection.json(Action : START)
```

2. Execute the following command to stop the log collection.

```
managed-element log-collection -ME_ID*=olt1 -f=logcollection.json(Action : STOP)
```

3. Execute the following command to check the status of the log collection.

```
managed-element get-log-collection-status -MEID*=olt1
```

4. After the log collection operation is completed, you can view the log collection notification in the *notification-listen* section.
5. The user can trigger the old log collection API to collect the logs using the oltauser credential.
6. The collected tar logs are stored in the */mnt/onl/sdpon/logdump* file.
7. The new log collection API is supported for all users, including third-party users in any role.

Recovering from Input/Output Error

Problem Description. If there are any corrupt files in the system, the following type of Input/Output (I/O) errors are seen on the console during a major ONL upgrade, ONL installation through ONIE, or during the ONL boot.

The system keeps rebooting, or a few of the applications may fail to come up due to I/O errors once the ONL is booted.

Solution. It is recommended to uninstall the ONL through ONIE and re-install the ONL from the ONIE rescue mode.

Input/Output Error Message

```
Allocating 66868711 sectors for ONL-DATA-ACTIVE
+ partprobe /dev/sda
Formatting /dev/sda7 (ONL-DATA-ACTIVE) as ext4
+ mkfs.ext4 -v -O ^huge_file -L ONL-DATA-ACTIVE /dev/sda7
mke2fs 1.42.7 (21-Jan-2013)
ext2fs_check_if_mount: Can't check if filesystem is mounted due to missing mtab file
while determining whether /dev/sda7 is mounted.
fs_types for mke2fs.conf resolution: 'ext4'
Discarding device blocks: [ 363.846462] ata2.00: exception Emask 0x0 SAct 0x0 SErr 0x0
action 0x6 frozen
[ 363.853658] ata2.00: failed command: DATA SET MANAGEMENT
[ 363.859113] ata2.00: cmd 06/01:01:00:00:00/00:00:00:00:00/a0 tag 12 dma 512 out
[ 363.859113] res 40/00:00:00:00:00/00:00:00:00:00/00 Emask 0x4 (timeout)
[ 363.873941] ata2.00: status: { DRDY }
[ 373.913450] ata2: softreset failed (device not ready)
[ 383.953450] ata2: softreset failed (device not ready)
[ 394.513451] ata2: link is slow to respond, please be patient (ready=0)
[ 418.959446] ata2: softreset failed (device not ready)
[ 418.964637] ata2: limiting SATA link speed to 3.0 Gbps
[ 424.165449] ata2: softreset failed (device not ready)
[ 424.170639] ata2: reset failed, giving up
[ 424.174788] ata2.00: disabled
[ 424.178999] print_req_error: I/O error, dev sda, sector 526920
[ 424.184972] print_req_error: I/O error, dev sda, sector 364517312
[ 424.184974] Buffer I/O error on dev sda2, logical block 292, lost async page write
[ 424.198911] print_req_error: I/O error, dev sda, sector 335124480
[ 424.198912] print_req_error: I/O error, dev sda, sector 527000
[ 424.198915] Buffer I/O error on dev sda2, logical block 332, lost async page write
failed - Input/output error
```

Recovering Docker Registry from Unresponsive Docker-Registry:5000

Problem Description

The connection refused error is displayed when the operator pushes or pulls the docker-registry:5000. This is because the docker registry container is not running.

The following error appears upon restarting the docker registry container.

Error response from daemon.

```
Cannot restart container 606ce448ea8d: failed to initialize the logging driver: dial tcp
127.0.0.1:514: connect: connection refused.
```

Note: This error is seen only in non-hardened OS-based repositories.

Solution.

Perform the following steps to recover from unresponsive docker-registry.

1. Add the following to the `/etc/rsyslog.conf` file at the end.

```
$IncludeConfig /etc/rsyslog.d/*.conf
$ModLoad imtcp.so
$InputTCPServerRun 514
```

2. Restart the rsyslog service.
3. Restart the docker-registry container.

Formatting the USB Device using Rufus Tool

This chapter provides information about formatting the USB device using the Rufus tool.

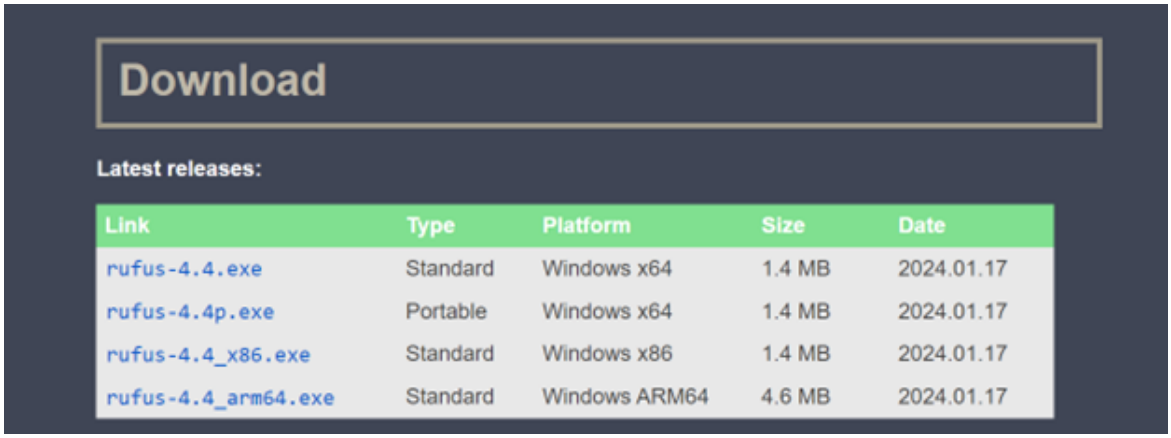
Note:

- To proceed with the formatting of the USB device using the Rufus tool, you must have admin privileges.
- Whenever formatting is performed, all the data on the USB is deleted. Therefore, make a backup of the data on a USB device if required.

Perform the following steps to format the USB using the Rufus tool.

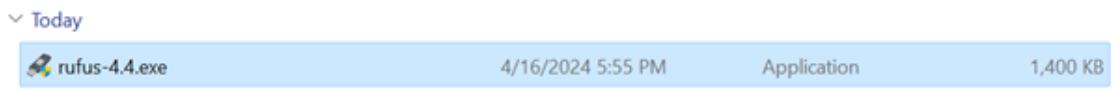
1. Download the Rufus tool from https://rufus.ie/en/.

Figure 433. Rufus Tool

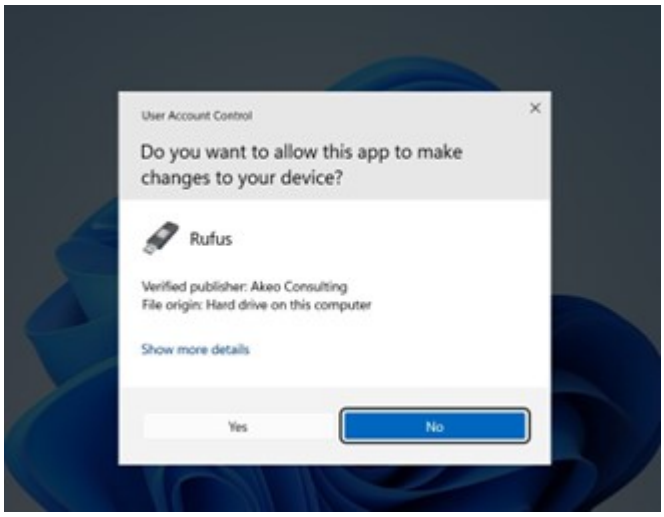


2. Select the Rufus version **Type** for standard and **Platform** for Windows x64.
3. Double-click on the downloaded file in the Downloads folder (`C:/Users/user name>/Downloads`) to proceed with USB device formatting.

Figure 434. Rufus File



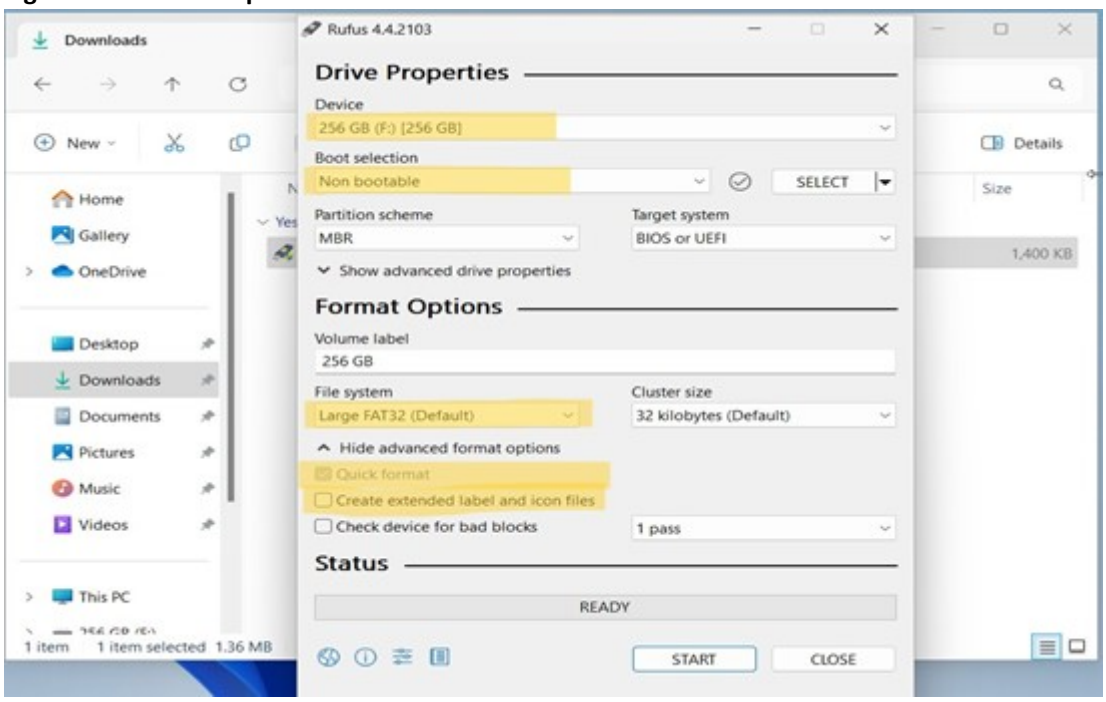
4. Once the user double-clicks on the file, the below pop-up window appears.



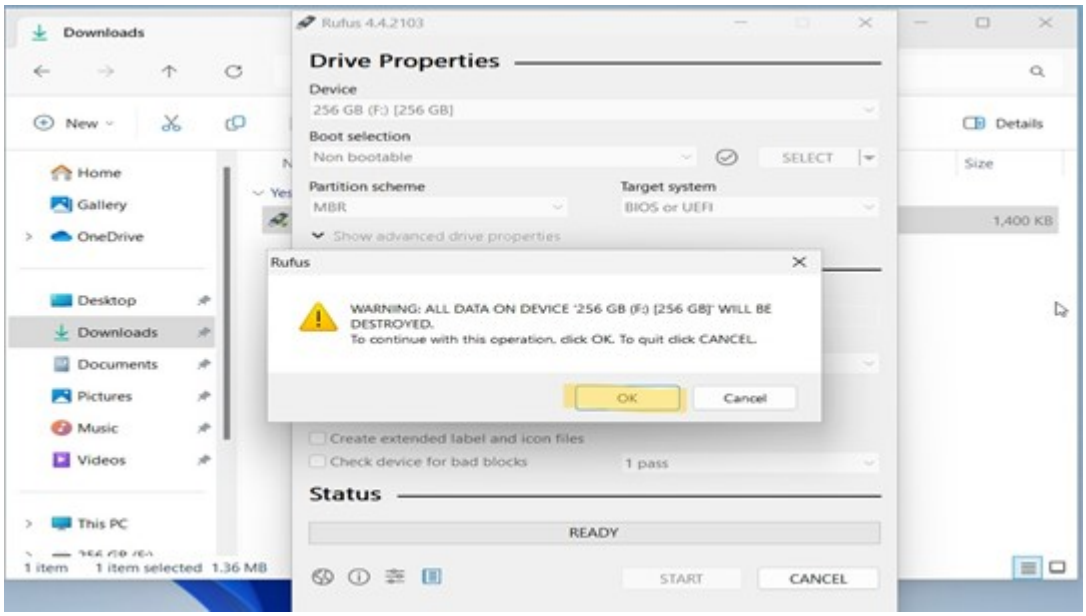
5. Select **Yes**.
6. The Rufus application starts, and the GUI appears. Select the below mentioned options.
   - In the "Device" option, select the **F:** drive containing the USB device.
   - In the "Boot selection", select **Not bootable**.
   - For “File system”, select **Large FAT32(Default)**.
   - Uncheck **Create extended label and icon files**.

   The following diagram shows the updated drive properties. Highlighted are the selected options for quick reference.

Figure 435. Drive Properties

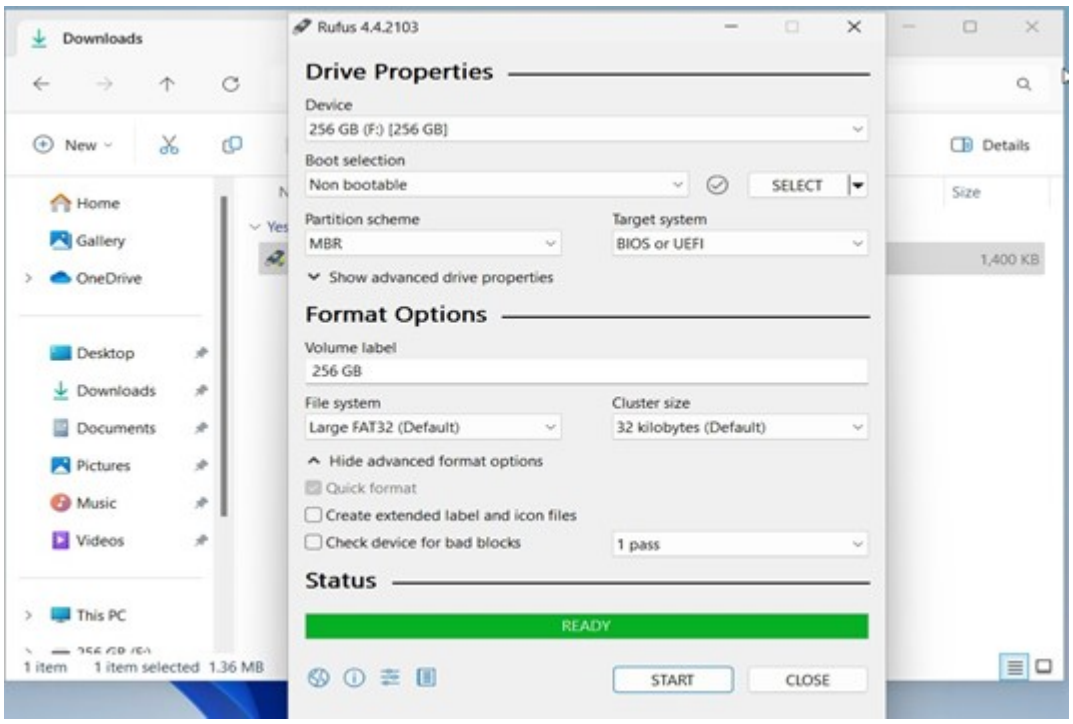


7. Click **Start** to format the USB device, a confirmation pop-up appears, and click **OK**.



8. Once the USB is formatted and ready, click **Close.**

   The following diagram shows the updated drive properties. The USB device is ready for copying the installation files.



voltctl and LWC CLI Commands

The voltctl is a CLI tool for managing and operating the VOLTHA components. This appendix describes some of the voltctl commands to manage the devices.

Accessing the VOLTHA CLI

On the deployment system, execute the following command to retrieve the status of all PODs.

```
$ sudo kubectl get po -o wide
```

Output:

```
NAME READY STATUS RESTARTS AGE IP NODE
etcd-etcd-0 1/1 Running 4 6d20h 10.233.121.88 localhost
etcd-etcd-defrag-27550380-qxlvs 0/1 Completed 0 64s 10.233.121.208 localhost
external-kafka-0 1/1 Running 8 6d20h 10.233.121.100 localhost
external-kafka-zookeeper-0 1/1 Running 4 6d20h 10.233.121.65 localhost
influxdb-86bd8b7cf9-9phn4 1/1 Running 4 6d20h 10.233.121.60 localhost
internal-kafka-0 1/1 Running 8 6d20h 10.233.121.93 localhost
internal-kafka-zookeeper-0 1/1 Running 4 6d20h 10.233.121.101 localhost
intersdpongateway-7d8bd9d5d4-rm889 1/1 Running 4 6d20h 10.233.121.48 localhost
log-manager-7d5465c87d-k59kt 1/1 Running 4 6d20h 10.233.121.91 localhost
logstash-c8cf54b6b-kkvx6 1/1 Running 5 6d20h 10.233.121.98 localhost
lwc-6dd5d9bf84-kz6wx 1/1 Running 4 6d20h 10.233.121.92 localhost
msm-85c9749b9-5xcl7 1/1 Running 4 6d20h 10.233.121.90 localhost
openolt-5dd9b869c5-c5bhs 1/1 Running 4 6d20h 10.233.121.84 localhost
openonu-764ddb99c-mmh46 1/1 Running 4 6d20h 10.233.121.94 localhost
redis-master-0 1/1 Running 4 6d20h 10.233.121.87 localhost
rwcore-5b877cc7d5-qb9gc 1/1 Running 5 6d20h 10.233.121.89 localhost
sdponaccessgateway-b6d98f5bc-hs4mg 1/1 Running 4 6d20h 10.233.121.44 localhost
sdpondevicemanager-75c4bd8f8c-8g8t6 1/1 Running 12 6d20h 10.233.121.99 localhost
sdponemscli-5c9c5d4c56-ftv46 1/1 Running 8 6d20h 10.233.121.104 localhost
sdponemsgateway-684b6b94cb-fqgz8 1/1 Running 5 6d20h 10.233.121.95 localhost
sdponmonmgr-78d55d48d9-hmtgt 1/1 Running 4 6d20h 10.233.121.58 localhost
sdponncm-66849c5dd9-mzx5x 1/1 Running 9 6d20h 10.233.121.103 localhost
sdponnda-545b7788c4-nm2st 1/1 Running 12 6d20h 10.233.121.102 localhost
sdponsecurity-b597654d9-bsmzq 1/1 Running 4 6d20h 10.233.121.97 localhost
sdponsubscribermanager-54bb88779b-cvmnv 1/1 Running 4 6d20h 10.233.121.96 localhost
sdpontelemetry-75977c544d-rpg9t 1/1 Running 4 6d20h 10.233.121.39 localhost
voltctl-5bc5ccdb8c-h7tsm 1/1 Running 4 6d20h 10.233.121.63 localhost
```

- Use the POD name from the row name mentioning **voltctl-*** and execute the following command.

  ```
  $ sudo kubectl exec -it <voltctl pod name> bash
  ```

  You are entered into the voltctl POD.
- Execute the following command to follow the path.

  ```
  cd /home/voltha
  ```

- Execute the following command to run the voltctl binary.

```
root@voltctl-68d8644686-rx497:/home/voltha# ls
voltctl
root@voltctl-68d8644686-rx497:/home/voltha# ./voltctl
Please specify one command of: adapter, completion, component, config, device,
devicegroup, event, log, logicaldevice, message or version
root@voltctl-68d8644686-rx497:/home/voltha# ./voltctl device
Please specify one command of: GetVoipLineStatusOnOnu,
configureIPHostInterfaceOnOnu, configureOnuIPv6HostIntf, create, delete,
disable, downloadImageToOlt, enable, enableVoiceProtocolOnOnuReq, flows,
inspect, list, port, reboot, transferOntImageToBAL, upgrade, upgradeStatus or
value
root@voltctl-68d8644686-rx497:/home/voltha# ./voltctl device list
ID TYPE ROOT PARENTID SERIALNUMBER CHANNELID ONUID MACADDRESS
ADMINSTATE OPERSTATUS CONNECTSTATUS REASON PARENTPORTNO ADDRESS
```

Useful Commands

The following are some of the useful commands.

- Execute the following command to retrieve the configuration.

```
./voltctl config
```

- Execute the following command to retrieve the list of adapters.

```
./voltctl adapter list
```

Device Related Commands

- Execute the following command to retrieve the list of active devices.

```
./voltctl device list
```

- Execute the following command to create a device.

```
./voltctl device create -t openolt -H <host ip>:9191
```

- Execute the following command to enable a device.

```
./voltctl device enable <device id>
```

- Execute the following command to disable a device.

```
./voltctl device disable <device id>
```

- Execute the following command to delete a device.

```
./voltctl device delete <device id>
```

- Execute the following command to retrieve the list of ports for a device.

```
./voltctl device port list <device id>
```

- Execute the following command to retrieve flow information for a device.

```
./voltctl device flows <device id>
```

- Execute the following command to reboot a device.

```
./voltctl device reboot <device id>
```

Accessing LWC

You can populate the data stored by the Light Weight Controller (LWC) in Redis.

- You can use the POD name mentioning **lwc-*** and execute the following command.

```
$ sudo kubectl exec -it <lwc pod name> bash
```

You are entered into the LWC CLI POD.

- Execute the LWC binary commands.

```
root@lwc-7d664ff7f8-bw7sv:/home/lwc# ./lwcctl
```

Command Output:

```
Environment variable KV_STORE_TIMEOUT undefined KV_STORE_TIMEOUT
Please specify one command of: cacheeline, cacheicmp, cachemvlan,
cachemvlanprofile, cacheport, cacheserviceprofile, cachevnetprofile,
cachevpvprofile, device, dhcpsession, flows, getflowhash, getgrouphash, group,
igmp, igmpchannel, igmpdevice, igmpgroup, igmpport, mcast, meter, mvlan,
ponports, port, service, setflowhash, setgrouphash, tasklist, vnet or vpvs
```

```
root@lwc-7d664ff7f8-bw7sv:/home/lwc# ./lwcctl flows
```

Command Output:

```
Environment variable KV_STORE_TIMEOUT undefined KV_STORE_TIMEOUT
Environment variable KV_STORE_TIMEOUT undefined KV_STORE_TIMEOUT
No flows found
```

Usage: *./lwcctl <command>*

The following commands are supported.

- flows: To check all the flows.
- igmp: List all IGMP configurations.
- port: To check port values.
- mvlan: To check MVLAN values.
- service: To check service information.

- vnet: To check VNET profile information.
- vpvs: To check VPVS values.

Use Cases

This section captures the various use cases of the COB solution.

Triple Play Services

Prerequisites

The following prerequisites must be fulfilled to enable the triple play services.

To enable the triple play services, the following are the requirements.

- A server or PC with at least two Ethernet/NIC interfaces for the Internet gateway and downlink to BNG router/switch/OLT.
- A system runs Ubuntu over a VirtualBox.
- Applications: Asterisk SIP server (open source), VLC player, packet, and speed test.

Perform the following steps.

1. On the BNG server, download VirtualBox from http://www.virtualbox.org for Linux hosts.
2. Download Ubuntu from http://www.ubuntu.com/download/desktop.
3. Install VirtualBox on the system and follow the installation steps.
4. Create a new VM.
5. Select **Linux > Ubuntu (32 or 64 bit)**.
6. Assign RAM and disk space as required and retain the default values for other fields.
7. Right-click on the created VM, assign the file storage to **Controller IDE > Empty**, and locate the Ubuntu file downloaded in step http://www.ubuntu.com/download/desktop.
8. Start the system, install Ubuntu, and log in to the VM.
9. In the terminal, execute the following commands.

```
$ sudo apt-get update
$ sudo apt-get upgrade
```

10. Your server is updated and ready to be used as a data, voice, and video server.
11. Install and configure the DHCP server. Execute the following commands to install and start the DHCP server.

```
$ sudo apt-get install isc-dhcp-server
$ sudo service isc-dhcp-server start
```

Note: For more information on configuring the DHCP server, refer to the https://www.computernetworkingnotes.com/linux-tutorials/how-to-configure-dhcp-server-in-linux.html

12. Configure a sub-interface on server ports with the required S-tag and C-tag for a double tag scenario. Configure another sub-interface with another S-tag for multicast VLAN for the VLC multicast server.

    Example,

```
sudo vconfig add enp0s8 359
sudo ifconfig enp0s8.359 up
sudo vconfig add enp0s8.359 259
sudo ifconfig enp0s8.359.259 192.168.59.100 up
sudo vconfig add enp0s8 4059
sudo ifconfig enp0s8.4059 up
sudo ifconfig enp0s8.4059 192.168.59.250/24 up
sudo ifconfig enp0s8.4059
sudo route -n add -net 224.0.0.0 netmask 255.0.0.0 dev enp0s8.4059
```

VoIP Call with SIP Server

This section covers the procedures for configuring the VoIP call with the SIP server.

1. Execute the following commands to set up voice, install, and run the asterisk software.

```
sudo apt-get install asterisk
sudo asterisk -r
```

2. Create a backup of the *sip.conf* file.

```
sudo mv /etc/asteris/sip.conf /etc/asterisk/sip.conf.bkp
```

3. Create a new *sip.conf* file and configure it.

```
sudo vi/etc/asterisk/sip.conf
```

4. Perform the following steps to configure the *sip.conf* file.
   a. Access your Asterisk SIP server, log in through a shell. Example: SSH or a console.
   b. As a root user, change directories to your Asterisk configuration file directory.

      Example:

```
asteriskhost:~/# cd /etc/asterisk
```

   c. Edit the SIP configuration file *sip.conf*.

```
sudo vi/etc/asterisk/sip.conf
```

      The following is an example of a typical Asterisk VIP device *sip.conf* configuration.

      Sample user1 : 9993 and sample user2: 9994 (the number 9993 must be changed to fit your dial code structure).

      Configure the bind address local net as per the test network.

```
[general]
Context=internal
allowguest=no
allowoverlap=no
bindport=5060
bindaddr=0.0.0.0
srvlookup=no
disallow=all
allow=ulaw
alwaysauthreject=yes
canreinvite=no
nat=yes
session-timers=refuse
localnet=192.168.1.0/255.255.255.0

[9993]
type=friend
secret=password
nat=yes
host=dynamic
canreinvite=yes
username=9993
rfc2833compensate=yes

[9994]
type=friend
secret=password
nat=yes
host=dynamic
canreinvite=yes
username=9994
rfc2833compensate=yes

A simple version to configure is
[9993]
type=friend
host=dynamic
secret=123
context=internal

[9994]
type=friend
host=dynamic
secret=456
```

d. Edit the SIP extension configuration file: *extensions.conf*.

```
sudo mv /etc/asterisk/extensions.conf /etc/asterisk/extensions.conf.bkp
vi /etc/asterisk/extensions.conf
```

Following is an example of a typical Asterisk VIP device *extensions.conf* configuration.

The number 9993 must be changed to fit your dial code structure.

```
[internal]
exten => 9993,1,Answer()
```

```
exten => 9993,2,Dial(SIP/9993,60)
exten => 9993,3,Playback(vm-nobodyavail)
exten => 9993,4,VoiceMail(9993@main)
exten => 9993,5,Hangup()

exten => 9994,1,Answer()
exten => 9994,2,Dial(SIP/9994,60)
exten => 9994,3,Playback(vm-nobodyavail)
exten => 9994,4,VoiceMail(9994@main)
exten => 9994,5,Hangup()

exten => 8993,1,VoicemailMain(9993@main)
exten => 8993,2,Hangup()

exten => 8994,1,VoicemailMain(9994@main)
exten => 8994,2,Hangup()

 Example is for Extension 9993 and 9994 and  can also be configure like so
 exten => 9993,1,Dial,sip/9993|30|to
```

5. Execute the following commands to enable the voice mail feature.

```
sudo mv /etc/asterisk/voicemail.conf /etc/asterisk/voicemail.conf.bkp
sudo vi /etc/asterisk/voicemail.conf
```

6. Execute the following command to restart the Asterisk software.

```
sudo asterisk -r
```

Configuring SIP Clients

This section covers the procedures for configuring the Session Initiation Protocol (SIP) clients.

1. Download SIP clients in the two Windows/Linux laptops that are used as clients of the ONTs. An example application is X-lite. Download http://www.counterpath.com/x-lite-download/ or any other soft phone like 3cx.
2. Configure the laptops to receive an IP address by DHCP or the DHCP client and have IP addresses assigned by the DHCP server on the BNG in the same network of the SIP server if it is a bridged network. If using a traditional POTS-based phone, configure the two SIP clients in the RG ONT router. Ensure that the WAN port is in the same network of the SIP server.
3. Configure account name/phone number as 9993.

   User ID: **9993**

   Password: ***<Password>***

   Domain/Sipserver as SIP server IP address.

   SIP server port 5060

   RTP port 20000

4. Click register to connect the phone and register it.

5. Repeat on the other laptop client with the other number 9994.
6. Once both phones are registered with the SIP server, phone calls can be made between them.

Configuring IPTV

This section covers the procedures for configuring the IPTV.

1. Execute the following commands on the BNG server.

```
sudo apt update
sudo apt install vlc
```

2. Ensure that good quality .mp4 video files are available on the BNG server.
3. Execute the following command to start VLC player and stream a multicast stream on group address 239.1.1.1.

```
vlc -vvv Radisys.mp4 --sout
'#duplicate{dst=rtp{mux=ts,dst=239.1.1.1,sdp=sap,name="TestStream"}}' --ttl
32 -L
similarly another stream can be started by
vlc -vvv test2.mp4 --sout
'#duplicate{dst=rtp{mux=ts,dst=238.1.1.1,sdp=sap,name="TestStream"}}' --ttl
32 -L
```

4. Ensure that a VLC player runs on the network interface, which is connected as a downlink to the OLT NNI side.
5. Perform the following steps on the ONT side client laptops (Linux/Windows).
   a. Install VLC player.
   b. Start the VLC player.
   c. Select **Media > Open Network stream**
   d. Select **UDP** (udp://@239.1.1.1:1234) or **RTP** (rtp://@239.1.1.2:5004)
   e. Click play and your multicast join starts getting the video steam playing.

Replacing SFTP Server

This section explains the procedure to replace a node as part of a Ceph cluster or keepalived VRRP cluster when there is a failure in the SFTP cluster.

You can replace the SFTP server in the following scenarios.

- Failure of Ceph admin node.
- Failure of Ceph non-admin node
- Failure of the node running the active SFTP server
- Failure of the node running the standby SFTP server

The types of SFTP server failures are as follows.

- **Hardware or VM failure.** The failed Ceph node VM or Hardware must be replaced or repaired
- **OS failure.** The OS must be repaired or reinstalled
- **Data corruption failure.** The Ceph OSD must be repaired for data corruption or the OSD drive must be reformatted
- **Temporary application failure.** This refers to failure(s) of internal SFTP services. For example, Ceph OSD, Ceph Monitor (Mon), Ceph Meta Data Server (MDS), SSH, and so on. You can resolve the temporary failures by an application start/restart or node reboot

Replacing SFTP Server

Prerequisites

Verify the following before replacing the SFTP server.

- Ensure that the date and time is synchronized across all the Ceph nodes. For more information, see the Configuring NTP Client and Server Parameters *(on page 238)* section.
- Execute the following commands to check the clock skew warnings across Ceph nodes.

```
ceph status
ceph health detail
```

Perform the following to replace a SFTP server.

1. Take the backup of the failed node data to avoid data loss. You can use methods such as sftp, scp, or rsync to take the backup of the data.
2. Remove the failed or faulty Ceph node. See Removing Ceph Node *(on page 278)* section.
3. Prepare a new Ceph node or repair the faulty Ceph node. See Repairing Failed Node/ Creating a New Node *(on page 280)* section.
4. Add the new or repaired Ceph node to the Ceph cluster. For more information, see the Setting Up Ceph Cluster *(on page 63)* section.
5. If the failed node is an active or standby SFTP server, set up the SFTP server on the new node. Otherwise, skip to step 6 *(on page 278)*. For more information, see the Setting Up Ceph Cluster *(on page 63)* section.
6. Verify the SFTP cluster. For more information, see Verifying SFTP Cluster *(on page 290)* section.

Removing Ceph Node

Perform the following steps to remove the failed or faulty Ceph node.

1. Execute the following command in the Ceph cluster to retrieve the Ceph cluster status.

```
ceph status
```

Figure 436. Ceph Cluster Status

```
root@ceph-node-3:/home/ubuntu# ceph status
  cluster:
    id:     a675b843-7024-4cd9-a1c3-fd4929434722
    health: HEALTH_WARN
            mons are allowing insecure global_id reclaim
            clock skew detected on mon.ceph-node-4
            1/3 mons down, quorum ceph-node-3,ceph-node-4
            1 osds down
            1 host (1 osds) down
            Degraded data redundancy: 27/81 objects degraded (33.333%), 11 pgs degraded

  services:
    mon: 3 daemons, quorum ceph-node-3,ceph-node-4 (age 40s), out of quorum: ceph-node-2
    mgr: ceph-node-3(active, since 7s), standbys: ceph-node-4, ceph-node-1
    mds: 1/1 daemons up, 2 standby
    osd: 3 osds: 2 up (since 40s), 3 in (since 12h)

  data:
    volumes: 1/1 healthy
    pools:   3 pools, 41 pgs
    objects: 27 objects, 1.8 MiB
    usage:   19 MiB used, 20 GiB / 20 GiB avail
    pgs:     27/81 objects degraded (33.333%)
             30 active+undersized
             11 active+undersized+degraded
```

2. Execute the following command in the Ceph cluster to retrieve the list of Ceph OSD nodes.

```
ceph osd tree
```

Figure 437. Ceph OSD Nodes

```
root@ceph-node-3:/home/ubuntu# ceph osd tree
ID  CLASS  WEIGHT   TYPE NAME             STATUS  REWEIGHT  PRI-AFF
-1         0.02939  root default                                   
-5         0.00980      host ceph-node-2                           
 1    hdd  0.00980          osd.1           down   1.00000  1.00000
-7         0.00980      host ceph-node-3                           
 2    hdd  0.00980          osd.2             up   1.00000  1.00000
-3         0.00980      host ceph-node-4                           
 0    hdd  0.00980          osd.0             up   1.00000  1.00000
```

3. Execute the following commands to disable and stop Ceph daemons running on the faulty or failed node.

```
sudo systemctl stop ceph.target
sudo systemctl disable ceph.target
```

4. Execute the following command to set the weight of the faulty or failed Ceph node to zero.

```
sudo ceph osd reweight {osd-name} 0
```

5. Execute the following commands to remove the OSD from the Ceph Cluster.

```
sudo ceph osd out {osd-name}
sudo ceph osd purge {osd-name} --yes-i-really-mean-it
sudo ceph osd crush remove {osd-hostname}
sudo ceph osd rm {osd-id}
```

Note: Note the various OSD tree field values such as osd-hostname, osd-id, osd-name as shown in Figure 414. Ignore the field values if the output of step 5 *(on page 279)* is <*OSD*> does not exist.

6. Execute the following command to remove Ceph monitor.

```
sudo ceph mon remove {osd-hostname}
```

7. Execute the following command (on each of the running Ceph nodes) to open the hosts file. Then manually remove the hostname of the failed node.

```
sudo vim /etc/hosts
```

8. Execute the following command (on each of the running Ceph nodes) of the hostnames and IP addresses of the failed node from the `/etc/ceph/ceph.conf` file in all the remaining Ceph nodes.

```
sudo vim /etc/ceph/ceph.conf
```

9. Execute the following commands and verify that the failed Ceph node (OSD, Mgr, MDS, Mon) is removed from the Ceph cluster.

```
sudo ceph status
sudo ceph osd tree
```

Repairing Failed Node/ Creating a New Node

You can clean up the failed node VM or machine and reuse it as the new Ceph node or set up a different node VM or machine and use it as the new Ceph node.

Adding a New Ceph Node to Ceph Cluster

Perform the following steps to add a new Ceph node to the Ceph cluster.

Prerequisites

The following prerequisites must be fulfilled before adding a new Ceph node.

- Ensure that the date and time on the new or repaired node is synchronized with the other Ceph nodes. For more information, see the Configuring NTP Client and Server Parameters *(on page 238)* section.
- Execute the following command to set the hostname for the new or repaired node.

```
hostnamectl set-hostname <new node hostname>
```

- Ensure that a disk is mounted on the new or repaired node to store the Ceph data. For more information, refer to the *Adding Raw Disk for Ceph to VM in KVM and ESXi* section in the *Multinode RMS Installation and Upgrade Guide*.

- Ensure that the disk mounted (*/dev/<disk>*) is clean. Otherwise, erase all the data before adding a new node.
- Execute the following command and ensure that the new node is clean, and Ceph is not installed on the new node.

  ```
  ceph --version
  ```

  The output of this command must be an error: Command not found.

- Ensure that there is Internet connectivity on the new or replaced node.
- Ensure that the name servers are configured accurately in the `/etc/netplan` or `/etc/resolv.conf` files.

Perform the following to add a new Ceph node.

1. Execute the following command in all the Ceph nodes to check whether the failed node is the Ceph admin node or a node other than the Ceph admin node.

   ```
   ceph-deploy --version
   ```

   If the command returns an error (Command not found) on all the nodes, the node that went down was the Ceph admin node. Otherwise, the node on which the command executes successfully is the Ceph admin node, which is running.

   Note: The Ceph admin node is the node from which the Ceph cluster is deployed. The Ceph admin node includes ceph-deploy package and all the required keys (SSH and Ceph cluster keyrings) to setup the cluster.

2. If the failed node is the Ceph admin node, prepare the Ceph admin node. Otherwise, skip to step 3 *(on page 284)*.

   Perform the following steps to prepare the Ceph admin node.

   Reconfigure the SSH keys, install Ceph on the admin node, and gather the Ceph cluster keys on the admin node.

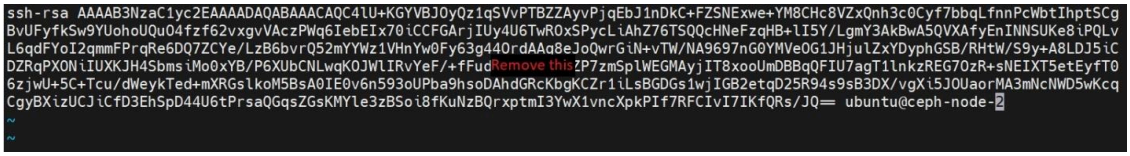
   a. Choose any one of the existing Ceph nodes as Ceph admin and SSH into it as a VM user (VM username).

      Note: The “VM username” is same as the *ansible_ssh_user* configured during the SFTP server installation.

   b. Execute the following command and remove entries from the *~/.ssh/authorized_keys* file in all the nodes.

      ```
      vim ~/.ssh/authorized_keys
      ```

Figure 438. Remove Authorized Keys



c. Execute the following command to generate an SSH key pair in the *~/.ssh* directory.

```
ssh-keygen -t rsa -b 4096 -f ~/.ssh/id_rsa_ceph
```

Note: Do not provide any passphrase.

d. Execute the following command to copy the SSH public key to the `~/.ssh/authorized_keys` file in all the nodes.

```
ssh-copy-id -i ~/.ssh/id_rsa_ceph.pub <VM user name>@<CEPH node IP>
```

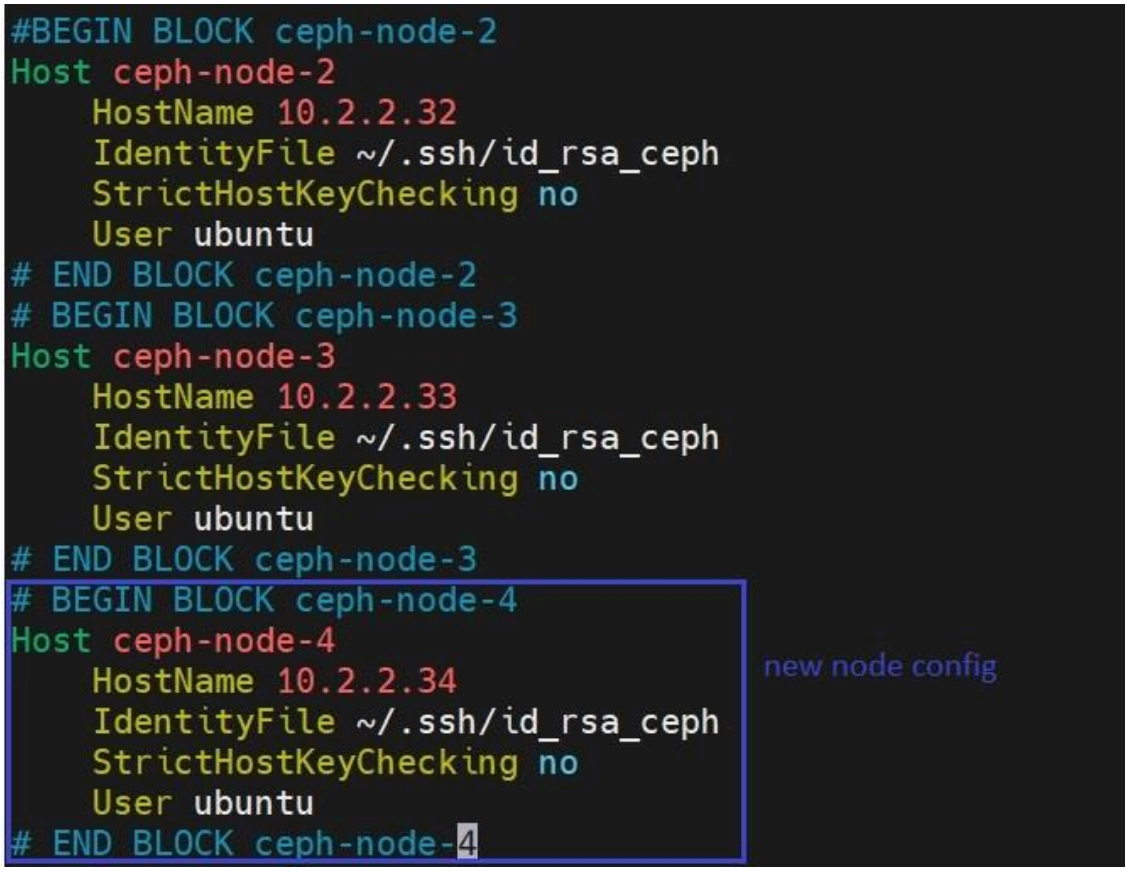
Note: You are prompted to provide a password of the remote host.

e. Add the following block to the `~/.ssh/config` file in the Ceph admin node to connect to other Ceph nodes.

```
#BEGIN BLOCK <ceph node-1 hostname>
Host <ceph node-1 hostname>
HostName <ceph node-1 IP Addr>
IdentityFile ~/.ssh/id_rsa_ceph
StrictHostKeyChecking no
User <ceph node-1 VM username>
# END BLOCK <ceph node-1 hostname>
# BEGIN BLOCK <ceph node-2 hostname>
Host <ceph node-2 hostname>
HostName <ceph node-2 IP Addr>
IdentityFile ~/.ssh/id_rsa_ceph
StrictHostKeyChecking no
User <ceph node-2 VM username>
# END BLOCK <ceph node-2 hostname>
# BEGIN BLOCK <ceph node-3 hostname>
Host <ceph node-3 hostname>
HostName <ceph node-3 IP Addr>
IdentityFile ~/.ssh/id_rsa_ceph
StrictHostKeyChecking no
User <ceph node-3 VM username>
# END BLOCK <ceph node-3 hostname>
```

Note: Add the new node configuration also to the `~/.ssh/config` file as shown in the following figure.

Figure 439. New Ceph Node Configuration



f. Execute the following command to edit the `/etc/sudoers.d/<VM username>` file.

```
sudo vim /etc/sudoers.d/<VM username>
```

Add the following line to the `/etc/sudoers.d/<VMusername>` file in all the nodes, including the new node, to enable password-less sudo access to all the nodes.

```
<VM username> ALL=NOPASSWD: ALL
```

Note: If the configuration is already present, skip to step 3 *(on page 284)*.

g. Add the hostname of the new node to the `/etc/hosts` file in the Ceph admin node.

h. Execute the following command to check if SSH access to the new node is allowed without the prompt for a password.

```
ssh <VM username>@<new node hostname>
```

Example:

```
ssh ubuntu@ceph-node-4
```

i. Execute the following commands to install the “ceph-deploy” on the Ceph admin node.

```
sudo apt install python3-pip -y
sudo pip3 install ceph-deploy
```

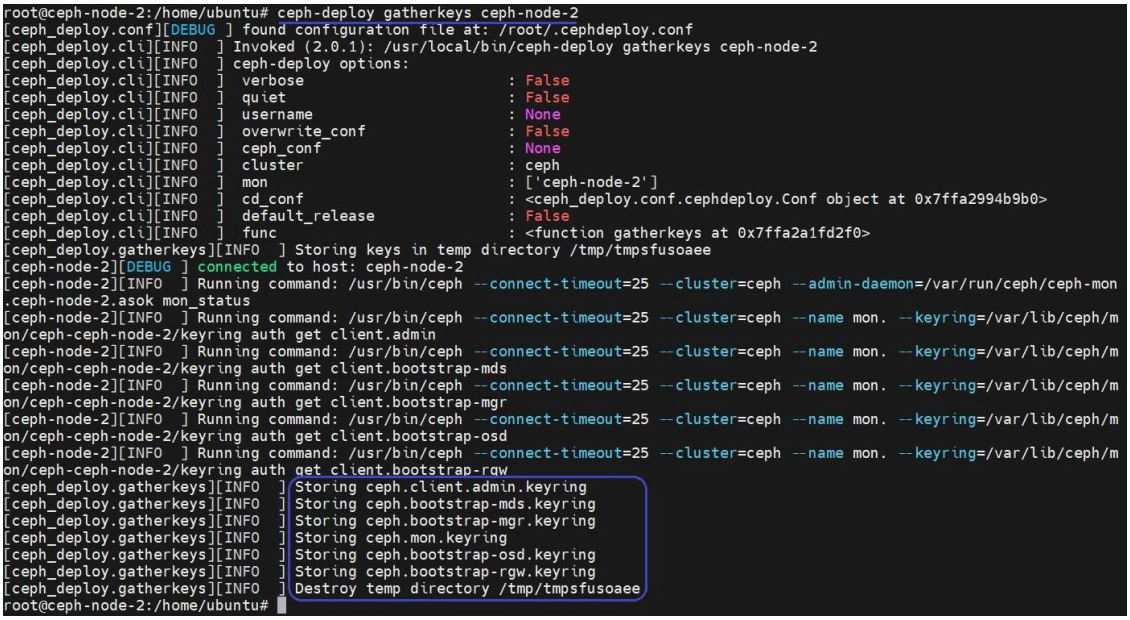
j. Execute the following command to check if the ceph-deploy is installed on the Ceph admin node.

```
ceph-deploy --version
```

k. Execute the following command in the home directory of “VM username” (`/home/<VM username>/`) to gather the Ceph cluster keys on the Ceph admin node.

```
ceph-deploy gatherkeys <admin hostname>
```

Figure 440. Ceph Cluster Keys



3. If the failed node is not the Ceph admin node, perform the following steps to enable password-less SSH access to the new node.

a. Execute the following command to copy the SSH public key from the Ceph admin node to the `~/.ssh/authorized_keys` file in the new node.

```
sudo ssh-copy-id -i ~/.ssh/id_rsa_ceph.pub <VM username>@<new CEPH node IP>
```

Note: You are prompted to provide a password of the remote host.

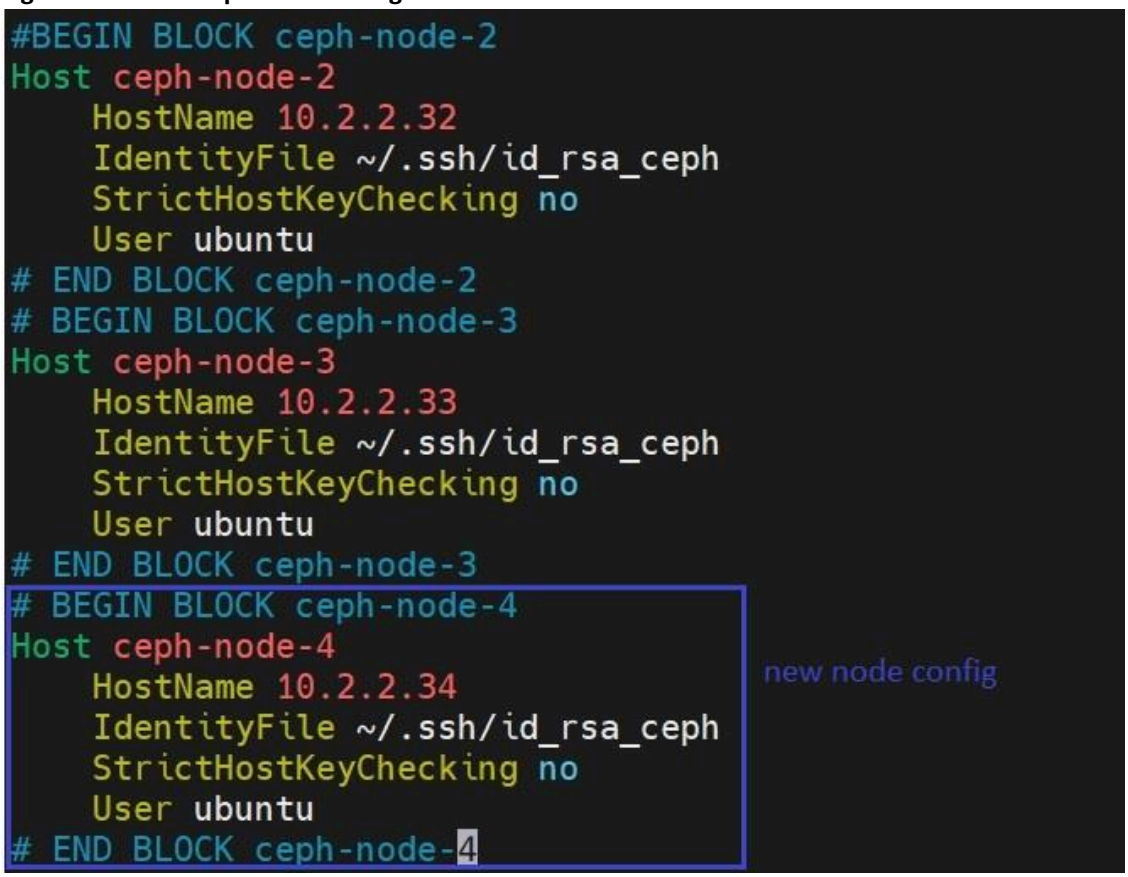
b. Remove the failed node block from the `~/.ssh/config` file in the Ceph admin node.

c. Add the following block to the `~/.ssh/config` file in the Ceph admin node to connect to the new Ceph node.

```
# BEGIN BLOCK <ceph new-node hostname>
Host <ceph new-node hostname>
HostName <ceph new-node IP Addr>
IdentityFile ~/.ssh/id_rsa_ceph
StrictHostKeyChecking no
```

```
User <ceph new-node VM username>
# END BLOCK <ceph new-node hostname>
```

Figure 441. New Ceph Node Configuration



d. Execute the following command to edit the `/etc/sudoers.d/<VM username>` file.

```
sudo vim /etc/sudoers.d/<VM username>
```

Add the following line to the `/etc/sudoers.d/<VM username>` file in the new node to enable the password-less sudo access to the new node.

```
<VM username> ALL=NOPASSWD: ALL
```

e. Add the hostname of the new node to the `/etc/hosts` file in the Ceph admin node.

f. Execute the following command to check if SSH access to the new node is allowed without the prompt for a password.

```
ssh <VM username>@<new node hostname>
```

Example:

```
ssh ubuntu@ceph-node-4
```

4. Install Ceph on the new node.

a. Add the hostname of the new node to the `/etc/hosts` file in the other nodes.

Note: Add the host file entries for all the nodes on the new node.

b. Set up apt repo on the new node.

Execute the following command to add the apt key.

```
sudo wget -q -O- 'https://download.ceph.com/keys/release.asc' | sudo apt-key add -
```

Create the ceph.list file in the `/etc/apt/sources.list.d/` directory and execute the following command to edit the `/etc/apt/sources.list.d/ceph.list` file.

```
sudo vim /etc/apt/sources.list.d/ceph.list
```

Add the following entry to the `/etc/apt/sources.list.d/ceph.list` file.

```
deb https://download.ceph.com/debian-pacific/ bionic main
```

c. Execute the following command on the Ceph admin node to install Ceph on the new node.

```
ceph-deploy install --release pacific <new node hostname>
```

5. Set up the Ceph cluster.

a. Execute the following command to edit the `/etc/ceph/ceph.conf` file.

```
sudo vim /etc/ceph/ceph.conf
```

Execute the following command to add the public_network configuration to the `/etc/ceph/ceph.conf` file in all the nodes except the new node.

```
public_network = <subnet to which the CEPH nodes belong>
```

Example:

```
public_network = 10.2.2.1/24
```

Note: If the public_network is already configured, skip to step 5.b *(on page 286)*.

b. Update the *mon_initial_members* and *mon_host* configuration in the `/etc/ceph/ceph.conf` file for all the nodes with the entry for the new node.

Figure 442. Public Network, Mon Host, and Mon Initial Members Configuration

c. Execute the following command to copy the `/etc/ceph/ceph.conf` file to the current directory (home directory of <*VM username*>) of the Ceph admin node.

```
cp /etc/ceph/ceph.conf ./
```

Note: The “ceph-deploy” script is executed from this path to deploy Ceph on the other nodes.

6. Add an OSD to the new node.
   a. Execute the following command in the Ceph admin node to create an OSD on the new node.

```
ceph-deploy osd create --data <device> <new CEPH node hostname>
```

   Example:

```
ceph-deploy osd create --data /dev/sdb ceph-node-4
```

   b. Execute the following commands to retrieve the OSD status. Verify the recovery status and check if the new OSD is present.

```
sudo ceph osd tree
sudo ceph status
sudo ceph health detail
```

7. Deploy Ceph Mgr on the new node.
   a. Execute the following command in the Ceph admin node.

```
ceph-deploy mgr create <new CEPH node hostname>
```

   b. Execute the following commands to SSH into the new node and switch to root user.

```
ssh <new node VM username>@<new node IP>
sudo su
```

   c. Execute the following command in the new node to update the CEPH Mgr directory permissions.

```
chmod o+rx /var/lib/ceph/mgr/ceph-<new CEPH node hostname>/
```

   d. Execute the following command in the new node to update the CEPH Mgr file permissions.

```
chmod 644 /var/lib/ceph/mgr/ceph-<new CEPH node hostname>/*
```

8. Deploy CEPH MDS on the new node.
   a. Execute the following command in the Ceph admin node.

```
ceph-deploy mds create <new CEPH node hostname>
```

   b. Execute the following commands to SSH into the new node and switch to root user.

```
ssh <new node VM username>@<new node IP>
sudo su
```

   c. Execute the following command in the new node to update the CEPH MDS directory permissions.

```
chmod o+rx /var/lib/ceph/mds/ceph-<new CEPH node hostname>/
```

d. Execute the following command in the new node to update the CEPH MDS file permissions.

```
chmod 644 /var/lib/ceph/mds/ceph-<new CEPH node hostname>/*
```

e. Execute the following command to reload the MDS server.

```
systemctl reload ceph-mds@<new CEPH node hostname>
```

9. Execute the following command in the Ceph admin node to deploy the CEPH Mon on the new node.

```
ceph-deploy mon create <new CEPH node hostname>
```

Note: You can ignore the warning text.

10. Copy the Ceph keyrings from the Ceph admin node to the new node.

a. Execute the following command in the Ceph admin node.

```
sudo scp /etc/ceph/ceph.client.admin.keyring <new node vm username>@<new node
 hostname>:/tmp/
```

Example:

```
sudo scp /etc/ceph/ceph.client.ceph_user.keyring ubuntu@10.2.2.32:/tmp/
```

b. Execute the following commands in the new node.

```
sudo cp /tmp/ceph.client.admin.keyring /etc/ceph/
sudo cp /tmp/ceph.client.ceph_user.keyring /etc/ceph/
```

Verifying Ceph Status on New Node

Verify if all the Ceph services are running on the new node.

Execute the following command on the new node to verify the Ceph status.

```
ceph status
```

If the status of mgr, mds, or mon is down, execute the following commands (in the corresponding Ceph node) to reload daemon and restart the Ceph mgr, mds, or mon.

```
sudo systemctl daemon-reload
sudo systemctl restart ceph-mgr@<hostname> or ceph-mds@<hostname> or ceph-mon@<hostname>
```

Note: The <*hostname*> field specifies the hostname of the new node.

Setting Up Active or Standby SFTP Server

If either an active or standby SFTP server is not running on any of the Ceph nodes, perform the following steps to set up the active or standby SFTP server on the new Ceph node post adding a new Ceph node to the cluster.

1. Configure SFTP node. For more information, see the Setting Up SFTP Server *(on page 59)* section.
2. Prepare file system on the SFTP node.
   a. Execute the following commands to SSH into the new SFTP node and switch to root user.

   ```
   ssh <new node VM username>@<new node IP>
   sudo su
   ```

   b. Execute the following command to install ceph-fuse on the new SFTP node.

   ```
   apt-get install ceph-fuse
   ```

   c. Execute the following command in the new SFTP node to generate the client keyring.

   ```
   ceph fs authorize cephfs client.ceph_user / rw
    -o /etc/ceph/ceph.client.ceph_user.keyring
   ```

   d. Execute the following command to create the mount point directory in the new SFTP node.

   ```
   mkdir -m 755 /mnt/sftpstore
   ```

   e. Execute the following command to change the mount point directory ownership to SFTP user.

   ```
   chown sftpuser:sftp /mnt/sftpstore
   ```

   f. Add the following configuration to the `/etc/fstab` file.

   ```
   none /mnt/sftpstore fuse.ceph
    ceph.id=ceph_user,ceph.conf=/etc/ceph/ceph.conf,_netdev,defaults 0 0
   ```

   g. Execute the following command to mount all the file systems to the fstab.

   ```
   mount -a
   ```

   h. Execute the following command to verify the mount point.

   ```
   mountpoint -q /mnt/sftpstore
   ```

   Note: If nothing is returned in the output, it implies that the mount point is functioning properly.

3. Add the new SFTP server to the VRRP cluster. For more information, see the Replacing Keepalived Cluster Node *(on page 97)* section.

Verifying SFTP Cluster

Perform the following steps to verify if the SFTP cluster is running.

1. Execute the ceph status command and verify the following.
   - Verify that the cluster is healthy without errors. General health warnings are acceptable.
   - Verify that all the three OSDs are up and running.
   - Verify that the CEPH Mons are up with quorum of 3. The removed Ceph Mon node should not appear.
   - Verify that there are three Ceph Mgr nodes (one active and two standby).
   - Verify that there are three Ceph MDS nodes (one active and two standby).
2. Execute the ceph osd tree command and verify the following.
   - Verify that the old or failed OSD is not present and the new OSD is functioning.
   - Verify that the weight is equal across all the OSD nodes.
   - Verify that the affinity is equal across all the OSD nodes.
3. Verify that the `/mnt/sftpstore` file in both the SFTP nodes (active and standby) have the same data.
4. Connect an SFTP client to the SFTP server and verify the following.
   - Verify if you can connect to the SFTP server.
   - Verify if the read operations such as listing of files in the `/mnt/sftpstore` directory are working.
   - Verify if the write operations such as copying a file to SFTP server are working.

Replacing CBAC Repository Server

You can replace the failed or unhealthy node with a new node when the repository server (active or standby) fails.

You can replace the failed node in the following scenarios.

- VM or hardware failure
- OS failure
- Any failures that render the repository server unusable

The repository server can handle another failure after the failed node replacement.

Perform the following steps to replace the failed CBAC repository server.

1. Create a new node and set up the repository server on the new node or repair the failed node and set up the repository server on the repaired node. For more information, see the Setting Up Local Repository Server *(on page 56)* section.
2. Upload all the required packages to the new node. Ensure all the packages in the active repository server are copied to the new node.
3. Add a new node to the keepalived VRRP list. For more information, see the Replacing Keepalived Cluster Node *(on page 97)* section.

Auto Provisioning of CBAC

This appendix provides information about the Auto provisioning of CBAC.

Auto Provisioning of CBAC

Using VLAN tags, each operator runs many virtual networks on the same physical network infrastructure. Similarly, the management network is separated from the other networks using a management VLAN, which must be configured before commissioning so that the OLT can connect to the management network. Each operator may use a unique VLAN tag for management.

The Radisys OLT device is provisioned with one of the following methods, and the methods are followed on nodes that are already commissioned at the factory with CBAC-D.

- DHCP-based auto-discovery
- Static Configuration–Device Registration

Prerequisites

The following prerequisites must be fulfilled before you perform the auto provisioning of CBAC-D.

Device-Registrar Prerequisites

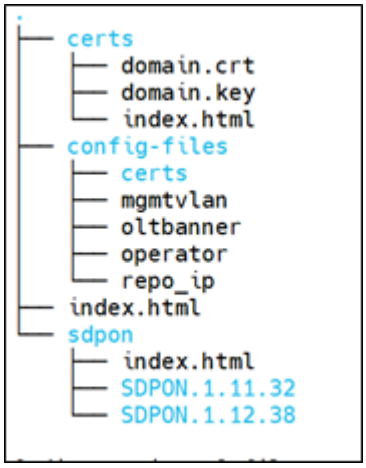
- The device-registrar functionality is hosted on RMS. The device-registrar is configured with the TLS vendor-certificate for the OLT "Register Device" procedure.
- A user must configure the Kafka port, REST port, log server details, and uncheck the **Enable OLT Blacklisting** option from the global settings of RMS. For more information on enabling OLT blacklisting, refer to the Field Descriptions table in the RMS User Guide.
- Radisys enables the bootstrapping script to set up the HTTP server hosted with the following.
  - Docker-registry
  - Helm artifacts
  - CBAC configuration artifacts
- The repository server is hosted with R4.1.0 release packages.

  For more information about setting up the repository server, see the Setting Up Local Repository Server *(on page 56)*.

Note: You can ignore the version in the snippet.

The following figure illustrates the repository server directory structure.

Figure 443. Repository Server Directory Structure



DHCP Server Prerequisites

The DHCP server is configured by mapping the client identifier (serial number) to the IP address required for the DHCP IP address assignment.

OLT Prerequisites

- The OLT is installed with ONL, OLT applications, and CBAC microservices.
- The management VLAN is configured on the OLT.
- The OLT is configured with the TLS vendor certificate required to connect to the device registrar for the *"Register Device"* procedure.

Configuring DHCP-Based Auto-Discovery

Upon commissioning and powering, each OLT uses the DHCP or static procedure to acquire the IPv4 or IPv6 management IP address. As a part of this procedure, the OLT also learns the initial configuration required to connect to the network.

Note: In the following sections, *Europa* refers to RLT-1600C or RLT-3200C OLT, and *Phoneix* refers to RLT-1600G, RLT-1600X, or RLT-3200G OLT.

DHCP Procedure

This section captures the DHCP options that must be used at the DHCP server and the DHCP server sample configurations for OLT auto-discovery and registration in RMS.

Table 11. List of DHCP Server Options

Options	DHCP IPv4 Option	IPv4 Comments	DHCP IPv6 Option	IPv6 Comments
NTP server	Option 42		Option 56	
TFTP server name	Option 66			
Bootfile name	Option 67		Option 59	Server name and URL of the file
DNS Server	Option 6			
Router	Option 3	Default Gateway		
Config-File	Option 209	Vendor specific option. Specifies the URL for downloading the configuration directory/files. **Note:** • The `config_files` path exists with the sshd-banner file by default in the *HttpServer (`/var/www/html`)* path. If not, the user must create the `config-files` directory in the *HttpServer (`/var/www/html`)* path, with the necessary sub-files as shown in Auto Provisioning of CBAC *(on page 292)*. • For PIM users, the operator file in the HTTP server path	Option 209	Vendor specific option. Specifies the URL for downloading the configuration directory/files. **Note:** • The *config_files* path exists with the *sshd-banner* file by default in the *HttpServer `/var/www/html`)* path. If not, the user must create a config-files directory in the HttpServer (`/var/www/html`) path, with the necessary

Table 11. List of DHCP Server Options (continued)

Options	DHCP IPv4 Option	IPv4 Comments	DHCP IPv6 Option	IPv6 Comments
		must be updated with the operator as <*operator_name*>.		sub-files as shown in Auto Provisioning of CBAC *(on page 292)*.
		Note: • For static commissioning, the user has to manually update `/mnt/onl/sdpon/deployment_ansible/inventory/group_vars/all` with the operator as <*operator_name*> in case of PIM user, and no update is required in case of default users (`admin/viewer/operator`). • The *sshd-banner* file contains the operator specific banner that must be used by the operator to update all the OLTs and hardened VMs.		**Note:** • For PIM users, the operator file in the HTTP server path must be updated with the operator as <*operator_name*>. • The *sshd-banner* file contains the operator specific banner that must be used by the operator to update all the OLTs and hardened VMs.

Sample DHCP Server Configuration

Following is the sample DHCP server configuration.

```
IPv6:
DHCPv6 config file: /etc/dhcp/dhcpd6.conf
default-lease-time 60;
max-lease-time 72;
# option definitions common to all supported networks...
option domain-name "example.org";
option domain-name-servers ns1.example.org, ns2.example.org;
option dhcp6.next-hop-rt-prefix code 243 = { ip6-address, unsigned integer 16,
unsigned integer 16, unsigned integer 32, unsigned integer 8, unsigned
integer 8, ip6-address };
option dhcp6.next-hop-rt-prefix 1063::254 243 22 9000 64 1 1063::;
option dhcp6.default-route code 242 = ip6-address;
option dhcp6.default-route 1063::254;
option dhcp6.default-nw code 244 = ip6-address;
option dhcp6.default-nw 1063::;
option dhcp6.server-mac code 250 = string;
option dhcp6.config-file code 209 = text;
option dhcp6.default-url code 114 = text;
option dhcp6.ntp-server code 56 = ip6-address;
option dhcp6.name-server code 23 = ip6-address;
option dhcp6.domain-search code 24 = text;
option config-file code 209 = text;
class "onl" {
match option dhcp6.client-id;
}
subclass "onl" "722033538827" {
option dhcp6.bootfile-param
"http://[1212::20c:29ff:fe2a:d385]/sdpon/SDPON.1.10.42/";
option dhcp6.default-route 1063::254;
option dhcp6.config-file "http://[1212::20c:29ff:fe2a:d385]/configfiles/";
option dhcp6.ntp-server 1212::5054:ff:fee1:174b;
option dhcp6.name-server 1154::1154;
option dhcp6.default-url = "https://sdpon/device-registrar/v1/register";
}
subnet6 1063::/64 {
range6 1063::86 1063::86;
}
IPV4:
DHCPv4 config file: /etc/dhcp/dhcpd.conf
ddns-update-style none;
default-lease-time 36000;
max-lease-time 72000;
option domain-name "devreg.com";
option domain-name-servers 154.154.154.154;
option config-file code 209 = text;
class "onl" {
match option dhcp-client-identifier;
}
subclass "onl" "722033538827" {
option bootfile-name "http://12.12.12.169/sdpon/SDPON.1.10.42/";
option ntp-servers 12.12.12.61;
option config-file "http://154.154.154.154/config-files/";
option default-url = "https://sdpon/device-registrar/v1/register";
}
# This is a very basic subnet declaration.
subnet 10.63.63.0 netmask 255.255.255.0 {
pool {
allow members of "onl";
range 10.63.63.28 10.63.63.29;
```

```
option routers 10.63.63.254;
}
```

Static Configuration–Device Registration

A user must perform the following OLT static configuration steps for the OLT device discovery and registration in RMS.

The following steps are for reconfiguring the R4.1.0 release.

1. Configure the IPv4 or IPv6 for management (in-band- eno1) interface in the `/etc/network/interfaces` file.
   Example:

```
# interfaces(5) file used by ifup(8) and ifdown(8)
# Include files from /etc/network/interfaces.d:
source-directory /etc/network/interfaces.d
auto lo
iface lo inet loopback
auto ma1
iface ma1 inet manual
auto ma1
iface ma1 inet static
        address 172.27.181.205
        netmask 255.255.252.0
        up ip route add 172.0.0.0/8 via 172.27.183.254
   auto eno1
        allow-hotplug eno1
iface eno1 inet6 static
        address 1063::86
        netmask 64
        gateway 1063::254
#     iface eno1 inet dhcp
       #     iface eno1 inet6 dhcp
```

2. You must configure the OLT and the OLT platform-related configurations from the OLT CLI. This prevents manual configuration errors, saves the OLT reboot, ensures the validation of data and values, makes easy configurations, and reduces time consumption.
3. Update the management VLAN and NNI in-band interface using the *oltconfig utility* provided by using the below commands if the user wants a different configuration than the factory default values as mentioned below.

   Note: The NNI port number in the following configuration is a physical port number.

   Example:

```
{
   "vlan":221,
   "nni":[3],
   "pon_device_mode":"gpon",
   "iwf_mode":"per_flow",
   "inband_storm_control_rate":100000,
```

```
   "version":"v.0.0.01"
}
```

Following are the steps to update the in-band vlan.

a. Run *oltconfig* utility in the OLT.

b. Execute the following command to set the vlan.

```
set inband vlan $vlan_value
```

Following are the steps to update the in-band NNI port.

a. Run the *oltconfig* utility in the OLT.

b. Execute the following command to set NNI ports. The **$nni_port_id** mentioned in the command must be -1 of the actual physical NNI port required to be configured as in-band port.

```
set inband nniports $nni_port_id
```

4. Update the *duid_type* in DHCPv6 requests by OLT in the `olt_config` file. By default, OLT uses a serial number in the **duid_type** field of the IPv6 DHCP process.

   Following are the steps to change a serial number to a MAC address in the configuration.

   a. Run the *oltconfig* utility in the OLT.

   b. Execute the following command to set the **duid_type**.

```
set duid_type mac
```

Note: Execute the following command in the *oltconfig* utility to revert the **duid_type** in the OLT configuration to the default configuration.

```
set duid_type serial_number
```

5. The **control_packet_in_rate** field in the `olt_config` file limits the rate of incoming control packets to the OLT. By default, it is set to 3000 Kbps and is not explicitly mentioned in the file. If a different rate limiting value is desired than the default one, the **control_packet_in_rate** field must be added with the new value using the *oltconfig* utility and rebooted the OLT for the new value to take effect. Perform the following to change the rate-limiting for the incoming control packets in the configuration.
   Following are the steps to change the rate limiting for the incoming control packets in the configuration.

   a. Run the *oltconfig* utility in the OLT.

   b. Execute the following command to set the **control_packet_in_rate**.

```
set control_packet_in_rate 3000
```

6. Update the repository server with the IP address in the `/etc/repo_ip` file.

7. Update the **repo_ip**, **logserver_ip**, **SDPON_version**, and **ntp_server_ip** parameters in the `/mnt/onl/sdpon/deployment_ansible/inventory/group_vars/all` file with the IP address.
8. Update the operator value in the `/mnt/onl/sdpon/deployment_ansible/inventory/group_vars/all` file.

   Note: The operator value can be empty for non-pim users. For other operators, enter the <*operator-name*>.

9. Update the OLT timezone. For more information, see the Updating OLT Time Zone *(on page 46)* section.
10. Execute the following command to reboot the OLT.

```
sudo reboot
```

11. Update the OLT security banner details. For more information, see the Updating OLT Security Banner *(on page 46)* section.
12. Configure the DNS server and domain name in the `/etc/resolv.conf` file.

    Example:

```
/etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
# DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 1154::1154
search devreg.com
Configure devreg.com fqdn cluster in DNS server with a DNS name sdpon.
```

    Note: If the name server is not available, follow step 11 *(on page 299)*.

13. Update the `/etc/hosts` file with the RMS IP address (<*rms-ip*> sdpon).

    Example:

```
127.0.0.1 localhost localhost.localdomain
1212::20c:29ff:fe2a:d385 docker-registry.com
1212::165 sdpon
::1 localhost6 localhost6.localdomain
```

    Note: This step is optional if CBAC resolves to RMS IP from the OLT.

14. Execute the following command in the OLT to verify the status of the CBAC redeployment.

```
admin@localhost:~$ sudo service sdpondeployment status
```

    Command Output:

```
sdpondeployment.service - SDPON deployment service on upgrade of OLT software
Loaded: loaded (/lib/systemd/system/sdpondeployment.service; enabled; vendor
Active: activating (start) since Tue 2021-09-28 09:56:42 UTC; 1min 11s ago
Main PID: 6542 (bash)
CGroup: /system.slice/sdpondeployment.service
+-6542 /bin/bash /usr/bin/sdpondeployment
+-8167 sudo -E bash -x /etc/dhcp/dhclient-exit-hooks.d/sdpon_ipv6
+-8168 bash -x /etc/dhcp/dhclient-exit-hooks.d/sdpon_ipv6
+-8210 sudo ansible-playbook -i inventory/hosts cleanup.yml -e ipvers
+-8211 /usr/bin/python3 /usr/local/bin/ansible-playbook -i inventory/
+-8570 /usr/bin/python3 /usr/local/bin/ansible-playbook -i inventory/
+-8571 /bin/sh -c /bin/sh -c '/usr/bin/python3 && sleep 0'
+-8572 /bin/sh -c /usr/bin/python3 && sleep 0
+-8573 /usr/bin/python3
+-8574 /bin/sh -c ansible-playbook -i inventory/inventory.cfg -u admi
+-8575 /usr/bin/python3 /usr/local/bin/ansible-playbook -i inventory/
+-9138 /usr/bin/python3 /usr/local/bin/ansible-playbook -i inventory/
```

15. After the activation, execute the following command to verify the PODs status.

```
sudo kubectl get pods
```

16. Configure the auto-discovery settings in the RMS GUI. Refer to the *RMS User Guide* for more information on the settings.
17. Execute the following command and enter the Device Registrar URL, NTP server IP, management IP, and Force register <*yes/No*>.

```
admin@localhost:~$ sudo static_ip_olt_reg
```

Command Output:

```
Enter Device Registrar URL
devRegUrl:https://sdpon/device-registrar/v1/register
Enter NTP server IP
ntp_ip:1212::5054:ff:fee1:174b
Enter management IP
mgmt_ip:1063::86
Force register <yes/No>:yes
```

Note: Use IPv4 addresses for IPv4 static provisioning scenarios and ensure that the IP address is changed from the factory provisioned IP address.