Contents

Chapter 1: Introduction to CloudVision................................. 1

Chapter 2: CloudVision Portal (CVP) Overview.......................... 3
  2.1 CloudVision WiFi................................................. 3
     2.1.1 CVW HA Mode Operation................................. 4
     2.1.2 Key Features of CVW on CV............................... 4
     2.1.3 Capacity of CVW on CV.................................. 4
  2.2 CVP Cluster Mechanism........................................ 5
     2.2.1 CVP Cluster and Single Node Failure Tolerance .......... 5
  2.3 System Requirements........................................... 5
  2.4 Key CVP Terms.................................................. 6
  2.5 CVP Virtual Appliance........................................ 8
     2.5.1 CVX and CVP............................................... 8

Chapter 3: CloudVision Portal (CVP) Setup.............................. 11
  3.1 Deploying CVP OVA on ESX...................................... 11
     3.1.1 VMware vMotion and Snapshot Support.................... 11
  3.2 Deploying CVP on KVM......................................... 15
     3.2.1 Downloading and extracting the CVP KVM tarball (.tgz archive).... 16
     3.2.2 Creating Virtual Bridge and Network Interface Cards (NIC)..... 16
     3.2.3 Generating the XML file that defines the CVP VM............... 17
     3.2.4 Defining and Launching the CVP VM......................... 18
  3.3 Set Up CVW on CV............................................... 19
     3.3.1 Setup CVW on a Standalone CV............................ 19
     3.3.2 Set Up CVW on a CV Cluster.............................. 20
  3.4 Shell-based Configuration...................................... 22
     3.4.1 Configuring a Single-Node CVP Instance using CVP Shell....... 22
     3.4.2 Configuring Multi-node CVP Instances Using the CVP Shell.... 23
  3.5 Shell Reconfiguration of Single-node, Multi-node Systems........ 36
     3.5.1 Single-node Shell Reconfiguration........................ 36
     3.5.2 Multi-node Shell Reconfiguration........................ 37
  3.6 ISO-based Configuration...................................... 39
     3.6.1 Create a YAML Document.................................. 39
     3.6.2 Feed the YAML File into the geniso.py Tool............... 40
     3.6.3 Map ISO to the VM's CD-ROM Drive....................... 41
  3.7 Certificate-Based TerminAttr Authentication.................... 42
     3.7.1 Enabling Certificate-Based TerminAttr Authentication......... 42
     3.7.2 Switching the Authentication from Certificates to Shared Keys.. 43
     3.7.3 Switching the Authentication from Shared Keys to Certificates.. 43
     3.7.4 Reboarding Existing Devices............................. 43
     3.7.5 Re-ZTP On-Boarded Devices............................... 45

Chapter 4: CloudVision as-a-Service.................................. 47
  4.1 Prerequisites................................................... 47
     4.1.1 Software Requirements.................................... 47
     4.1.2 Connectivity Requirements............................... 47
     4.1.3 Authentication Requirements............................. 48
Chapter 8: Device Comparison Application

8.1 Comparison Dashboard
8.2 Running Configuration
8.3 Snapshots
8.4 ARP Table
8.5 Comparing NDP Table
8.6 MAC Address Table
8.7 VXLAN Table
8.8 Viewing Device IPv4 Routing Table
8.9 Viewing Device IPv6 Routing Table
8.10 Comparing IPv4 Multicast Table
Chapter 11: Configlet Management (CVP) .............................................. 233
  11.1 Creating Configlets ............................................................ 233
     11.1.1 About the Configlet Builder Feature ............................ 233
     11.1.2 Creating Configlets Using the Configlet Builder ............ 233
     11.1.3 Using the Provided Configlet Builder Examples .................. 243
     11.1.4 Python Execution Environment ....................................... 246
     11.1.5 Creating Configlets Manually ......................................... 247
  11.2 Configlet Information Page .................................................. 249
     11.2.1 Tabs in Configlet Information Page .................................. 249
  11.3 Editing Configlets ............................................................. 252
  11.4 Deleting Configlets ............................................................. 253
  11.5 Importing and Exporting Configlets ........................................ 253
     11.5.1 Protection from Overwriting Configlets or Configlet Builders .. 253
     11.5.2 Importing Configlets or Configlet Builders ....................... 253
     11.5.3 Exporting Configlets or Configlet Builders ....................... 254

Chapter 12: Image Management (CVP) .............................................. 257
  12.1 Image Management Page ...................................................... 257
  12.2 Validating Images ............................................................. 258
     12.2.1 Alerts Indicating Unsupported EOS Image Versions ............ 258
  12.3 Upgrading Extended Operating System (EOS) Images .................. 258
     12.3.1 Example of Image Association ......................................... 259
     12.3.2 Tip for Handling Multiple Image Association Tasks ............ 260
  12.4 Creating Image Bundles ....................................................... 261
     12.4.1 Creating a Bundle by Tagging Existing Image Bundles .......... 262
     12.4.2 Creating a Bundle by Uploading a New Image ..................... 263
     12.4.3 Adding EOS Extensions to Image Bundles ......................... 264
  12.5 The Bundle Information Page ................................................ 265
     12.5.1 Summary Tab ............................................................... 266
     12.5.2 Logs Tab ................................................................. 266
     12.5.3 Applied Containers Tab ............................................... 266
     12.5.4 Applied Devices Tab ................................................... 267
     12.5.5 Updating Bundles ....................................................... 267
     12.5.6 Deleting Bundles ....................................................... 268

Chapter 13: Change Control ............................................................ 271
  13.1 Basic Options for Handling Tasks ......................................... 271
     13.1.1 Creating Tasks ........................................................... 271
  13.2 Using the Tasks Module ........................................................ 272
Chapter 14: Authentication & Authorization (CVP).................................305
14.1 Access Requirements for Image Bundle Upgrades..............................305
14.2 Managing AAA Servers.................................................................306
  14.2.1 Adding AAA Servers.................................................................306
  14.2.2 Modifying AAA Servers...............................................................307
  14.2.3 Removing AAA Servers...............................................................310
14.3 About Users and Roles.................................................................311
  14.3.1 Default Roles........................................................................311
14.4 Managing User Accounts.................................................................312
  14.4.1 Adding New User Accounts.........................................................312
  14.4.2 Modifying User Accounts.............................................................313
  14.4.3 Removing User Accounts.............................................................314
14.5 Managing User Roles....................................................................315
  14.5.1 Adding New User Roles.................................................................315
  14.5.2 Modifying User Roles.................................................................316
  14.5.3 Removing User Roles.................................................................317
14.6 Service Accounts............................................................................318
  14.6.1 Adding Service Accounts..............................................................319
  14.6.2 Editing Service Accounts..............................................................320
  14.6.3 Adding Tokens to Service Accounts..............................................320
  14.6.4 Deleting Service Account Tokens................................................321
14.7 Viewing Activity Logs.....................................................................323
14.8 Advanced Login Options..................................................................323
14.9 Access to the Access Control Page..................................................324

Chapter 15: CloudVision Topology.......................................................327
15.1 Main Panel of the Topology Screen..................................................328
15.2 Topology Overview.........................................................................331
15.3 Topology Layout Pane.....................................................................332
15.4 Topology Options Pane...................................................................333
15.5 Container Details Pane...................................................................334
15.6 Device Details Pane.........................................................................335
15.7 Link Details Panel...........................................................................336
15.8 Flow Visibility................................................................................337

Chapter 16: Tap Aggregation (CVP).....................................................343
16.1 Integration with CloudVision..........................................................343
  16.1.1 Initial Setup for Multi-Switch Tap Aggregation...............................344
16.2 Accessing the Tap Aggregation Screen............................................348
### Chapter 17: Using Snapshots to Monitor Devices

- About Snapshots: 359
- Standard Information in Snapshots: 359
- How to Use Snapshots: 359
- Accessing Snapshots: 360
- Accessing Snapshot Configurations: 360
- Defining Custom Snapshot Templates: 361
- How to Use Snapshots: 359
- Editing Custom Snapshot Templates: 362
- Viewing Snapshots Differences: 363

### Chapter 18: Backup & Restore, Upgrades, DNS NTP Server Migration

- Backup and Restore: 367
- Requirements for Multi-node Installations: 367
- Using CVPI Commands to Backup and Restore CVW Data: 367
- Using CVPI Commands to Backup and Restore CVP Provisioning Data: 368
- Upgrading CloudVision Portal (CVP): 370
- CVP Upgrades: 371
- CVP Node RMA: 372
- CVP / EOS Dependencies: 377
- Upgrade CVW As Part of a CV Upgrade: 377
- DNS / NTP Server Migration: 378
- Migrating the DNS and NTP Server: 378

### Chapter 19: Supplementary Services

- HTTPS Certificates Setup: 381
- Generating and Installing Self-Signed Certificate: 382
- Installing Public Certificate: 383
- Creating a CSR: 384
- Renewing the Certificate Authority: 388
- Customizing TLS and SSH Ciphers: 389
- Configuring Custom TLS Ciphers: 389
- Configuring Custom SSH Cipher: 389
- DHCP Service for Zero Touch Provisioning (ZTP) Setup: 389
- RADIUS or TACACS Authentication Setup: 390
- Background Tasks: 391
- Scheduling and Viewing Cronjobs: 392
- Resetting cvpadmin Password: 392

### Chapter 20: Troubleshooting and Health Checks

- System Recovery: 393
- VM Redeployment: 393
- CVP Re-Install without VM Redeployment: 393
- Health Checks: 394
- Running Health Checks: 396
20.3 Resource Checks........................................................................................................ 397
  20.3.1 Running CVP node VM Resource Checks...................................................... 397
  20.3.2 Increasing Disk Size of VMs Upgraded to CVP Version 2017.2.0............... 398
  20.3.3 Increasing CVP Node VM Memory Allocation.......................................... 399

Chapter 21: CloudVision Studios.............................................................................. 405
  21.1 Getting Started with Studios............................................................................ 405
  21.2 Accessing Studios......................................................................................... 406
  21.3 Workflow Overview....................................................................................... 407
    21.3.1 Commissioning Devices for Use in Studios............................................. 408
    21.3.2 Creating a Workspace............................................................................. 408
    21.3.3 Configuring an Existing Studio............................................................... 409
    21.3.4 Creating a New Studio............................................................................ 411
    21.3.5 Submitting a Workspace....................................................................... 413
  21.4 Studio Elements and Functions....................................................................... 414
    21.4.1 Reviewing a Workspace.......................................................................... 414
    21.4.2 Tags......................................................................................................... 417
    21.4.3 Schema................................................................................................... 420
    21.4.4 Template................................................................................................ 421
    21.4.5 Importing and Exporting Studios............................................................ 422
  21.5 Built-In Studios............................................................................................... 422
    21.5.1 Inventory and Topology......................................................................... 423
    21.5.2 Connectivity Monitor.............................................................................. 424
    21.5.3 Date and Time......................................................................................... 426
    21.5.4 Interface Configuration.......................................................................... 428
    21.5.5 Streaming Telemetry Agent................................................................... 430
    21.5.6 Campus Fabric...................................................................................... 432
    21.5.7 Layer 3 Leaf-Spine............................................................................... 435
    21.5.8 EVPN Services...................................................................................... 439
    21.5.9 Segment Security.................................................................................. 445

Appendix A: VMware vMotion and Snapshot Support..................................... 447
Introduction to CloudVision

CloudVision is a turnkey solution for network-wide workload orchestration and work flow automation. It was specifically designed to complement SDN (virtualization) controller solutions that orchestrate virtual network overlays, by focusing on work flow visibility, automation tasks, and initial or ongoing network provisioning across the underlying physical network.

The CloudVision components are packaged as a virtual appliance and operate as a highly available cluster with role based privileges integrated into existing authentication tools (AAA, RADIUS, TACACS). For maximum operational flexibility, CloudVision can be managed with the interactive EOS CLI, the open eAPI for granular programmatic access, or a web-based portal interface.

The foundation of CloudVision is an infrastructure service, sharing, and aggregating working state of physical switches running EOS to provide network visibility and central coordination. State from each participating EOS node is registered to CloudVision using the same publish/subscribe architecture of the EOS system database (SysDB). By communicating to each participating switch instance using a high performance binary API, CloudVision will actively synchronize state relevant to network-wide operational tasks. As an example, CloudVision's VXLAN Control Service aggregates network-wide VXLAN state for integration and orchestration with SDN controllers such as Openstack, VMWare NSX, and others.

The CloudVision web-based portal combines the most common operational tasks into a dashboard view decoupled from the underlying hardware. Workflow automation in CloudVision permits operators to execute common deployment and configuration tasks from a single visual touch point. The portal includes a turnkey solution for Arista's Zero Touch Provisioning (ZTP) and extends that from automating initial device provisioning to also include automating ongoing change controls over the operational life cycle of the device.

Using CloudVision, operators can organize devices in logical hierarchies through the use of list or configuration (config) container views for rapid categorization of device by role, type, or other specification. Configurations can be broken down into more manageable configlets that are built and stored directly on CloudVision, ready for network-wide or group-specific provisioning. The CloudVision database also keeps historical data, including a history of network state, configuration and software versions. This state can be used for taking a network-wide snapshot for change control verification of the network, helping to simplify the change management process and reduce maintenance window times.

For more information, see:
- CloudVision Portal (CVP) Overview
- CloudVision Portal (CVP) Setup
- Getting Started (CVP)

For more information about CloudVision eXchange (CVX), refer the EOS User Guide.
CloudVision Portal (CVP) Overview

CloudVision Portal (CVP) is the web-based GUI for the CloudVision platform. The Portal provides a turnkey solution for automating network operations, including network device provisioning, compliance, change management, and network monitoring. It communicates southbound to Arista switches via eAPI and has open standard APIs northbound for integration with 3rd-party or in-house service management suites.

CloudVision Portal (CVP) overview shows CloudVision as the network control point between the physical infrastructure (network layer) and the layer of service management.

Figure 1: CloudVision Portal (CVP) overview

Sections in this chapter include:
- CVP Virtual Appliance
- CloudVision WiFi
- CVP Cluster Mechanism
- System Requirements
- Key CVP Terms

2.1 CloudVision WiFi

The CloudVision WiFi (CVW) service is available as a container on the Arista CloudVision platform. Once you activate the CVW service, you can configure, monitor, troubleshoot, and upgrade Arista WiFi access points using the cognitive CVW UI.

CVW Architecture provides a conceptual overview of the Arista CVW solution.
CVW is containerized within the CV whether it's CVA (CV on a CV appliance) or a standalone CV VM. The CVW service runs on both single-node CV and CV cluster. In case of a CV cluster, CVW operates as a single logical instance in High Availability mode (HA-mode).

- CVW HA Mode Operation
- Key Features of CVW on CV
- Capacity of CVW on CV

### 2.1.1 CVW HA Mode Operation

When setting up CVW for the first time, it must be enabled on all the nodes of a cluster. Once CVW is enabled, then at boot time, the CVW service on the primary node automatically becomes the Active instance, and the one on the secondary node becomes the Standby instance. The HA failover and recovery mechanisms work exactly as expected. That is, if the primary node goes down, the CVW instance on the secondary node becomes active. When the primary node rejoins the cluster, a split-brain recovery kicks in and re-elects the new active and standby containers.

### 2.1.2 Key Features of CVW on CV

Except for OS and kernel processes, the CVW service on CV runs all the application processes required to manage Arista WiFi and wireless intrusion prevention system (WIPS). Some key features of the CVW service are as follows:

- CVW uses ports 3851 and 161 (both UDP) for all CV communication with external entities. These ports need to be opened in your network.
- CVW consists of two key components:
  - `wifimanager`, the server that manages the WiFi network.
  - `aware`, the cognitive WiFi UI of the server.

### 2.1.3 Capacity of CVW on CV

The table below shows the number of access points (APs) that a CVW container supports for the given CPU, RAM, and hard disk settings. The CPU and RAM values displayed in this table are the default settings for a DCA-200 device; the actual capacity may vary based on deployment, environment, and load.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Up to 5000 APs</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>8 Core</td>
</tr>
</tbody>
</table>
2.2 CVP Cluster Mechanism

CVP consists of distributed components such as Zookeeper, Hadoop/HDFS and HBase. Zookeeper provides consensus and configuration tracking mechanism across a cluster. Hadoop/HDFS is a distributed and redundant data store while HBase is a distributed key/value store. Running these services in a reliable fashion on multiple nodes require a quorum mechanism which is subject to limitations imposed by that mechanism.

- **CVP Cluster and Single Node Failure Tolerance**

2.2.1 CVP Cluster and Single Node Failure Tolerance

In absence of a quorum or a quorum leader, each node assumes itself to be the cluster leader in a three-node cluster leading to chaos and even data corruption. This leads to the quorum constraint for CVP cluster where only single node failure can survive. For example, a single node is allowed to form a cluster in a three-node cluster. In such cases, if cluster nodes cannot communicate with each other, all three nodes assume itself to be the lone survivor and operate accordingly. This is called a split-brain scenario where the original three-node cluster has split into multiple parts.

In real scenarios, assume only two nodes are active after a reboot and they failed to connect with each other. As no quorum is required, each node elects itself as the cluster leader. Now two clusters are formed where each cluster captures different data. For example, devices can be deleted from one cluster but not from the other. Device status is in compliance in one cluster but not on the other, etc. Additionally, services that store zookeeper configuration now has two copies with different data. Consequently, there is no effective way to reconcile the data when these nodes re-establish communication.

Let’s consider HBase component in CVP. HBase is a distributed key-value store and splits its data across all cluster nodes. Let’s assume that one node splits off from other two. If a single node can form a cluster, this single node forms one cluster and the other two together forms another cluster. It means that there are 2 HBase masters. That is the process which keeps track of metadata for all key/value pairs in HBase. In other words, HBase creates two independent sets of metadata which can even frustrate manual reconciliation. In essence, distributed infrastructure pieces must meet mandatory quorum requirements and which in turn means we cannot survive more than a single node failure.

Another reason to not tolerate dual node failures in a three-node CVP cluster is that all nodes are not made the same and total capacity of the cluster is more than what a single node can handle. Some services might be configured to run only on two of the three nodes and will fail when attempted to run on another. The total configured capacity of CVP cluster is 2 times that of a single node. That means in a three-node cluster, two nodes will have the capacity to run everything but one node cannot. Hence in a cluster of three CVP nodes, the cluster can survive only one CVP node failure.

2.3 System Requirements

The CloudVision Portal is deployed as a virtual or physical appliance.

**Note:** As of 2020.3.0, production instances of CloudVision should be deployed in a 3-node cluster. Single-node clusters must be used only for lab deployments.
Table 2: Minimum System Requirements

<table>
<thead>
<tr>
<th>Required Hardware</th>
<th>Production Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lab Deployment (&lt; 25 devices)</strong></td>
<td>A 3-node cluster must be used for production deployment. Each node must be configured to meet the minimum system requirements. The recommended hardware required per node to deploy CVP in a production environment (3-node cluster) are:</td>
</tr>
<tr>
<td>Single node instances of CVP are supported only in lab environments. The <strong>minimum</strong> hardware requirements to use CVP in a lab environment are:</td>
<td>• CPUs: 28 cores &lt;br&gt; • RAM: Recommended 52 GB &lt;br&gt; • Disk: 1 TB &lt;br&gt; • Disk Throughput: 40 MB/s</td>
</tr>
<tr>
<td>• CPUs: 8 cores</td>
<td></td>
</tr>
<tr>
<td>• RAM: 22 GB</td>
<td></td>
</tr>
<tr>
<td>• Disk: 135 GB (use RPM installer)</td>
<td></td>
</tr>
<tr>
<td>• Disk Throughput: 20 MB/s</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** For production deployments, information about device scale is available in the release specific version of the product release notes. For more information on throughput, refer to Troubleshooting and Health Checks.

Table 3: Latency Requirements

<table>
<thead>
<tr>
<th>Latency Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The latency between two CVP nodes must be up to 10 ms (recommended 5 ms or less). &lt;br&gt; • The latency from a CVP node to an EOS device must be up to 500 ms.</td>
</tr>
</tbody>
</table>

Table 4: Required Software Versions

<table>
<thead>
<tr>
<th>Required Software Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>The software versions compatible with CVP are:</td>
</tr>
<tr>
<td>• EOS license: Z license &lt;br&gt; • CVP license: Full subscription license</td>
</tr>
</tbody>
</table>

**Note:** For updates on compatible EOS switches, supported browsers, and supported TerminAttr versions, refer to the release specific version of the product release notes available at https://www.arista.com/en/support/software-download.

**Note:** CVP 2020.1.0 and future releases support host-to-host vmotion where the storage is shared between ESXi hosts. Only one host can be in vMotion at a given time.

**Related topics:**
• Key CVP Terms
• CVP Virtual Appliance

2.4 Key CVP Terms

Make sure you are familiar with the following key CloudVision Portal (CVP) terms. These terms are used throughout this guide to describe the various CVP features, and the CVP user interface contains icons that represent each of the key terms.
<table>
<thead>
<tr>
<th>Icon</th>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Device Image" /></td>
<td>Device</td>
<td>Devices managed by the CloudVision Portal.</td>
</tr>
<tr>
<td><img src="image" alt="Container Image" /></td>
<td>Container</td>
<td>Containers are a logical entity used to group network devices, and define a hierarchy to which user configuration can be applied.</td>
</tr>
<tr>
<td><img src="image" alt="Device Image" /></td>
<td>Device</td>
<td>Devices define the subset of available devices.</td>
</tr>
<tr>
<td><img src="image" alt="Configlet Image" /></td>
<td>Configlet</td>
<td>Configlets define a subset of a device's configuration.</td>
</tr>
<tr>
<td><img src="image" alt="Image Image" /></td>
<td>Image</td>
<td>Images define the software running on a given device.</td>
</tr>
<tr>
<td><img src="image" alt="Label Image" /></td>
<td>Label</td>
<td>Labels are arbitrary tags defined by the user and applied to devices for identification and filtering purposes.</td>
</tr>
<tr>
<td><img src="image" alt="Notification Image" /></td>
<td>Notification</td>
<td>Notifications are system messages providing the list of on-going, completed and canceled activities that are not tracked by tasks.</td>
</tr>
<tr>
<td><img src="image" alt="Task Image" /></td>
<td>Task</td>
<td>Tasks are work orders for taking an action against a given device.</td>
</tr>
</tbody>
</table>

N/A | Export to CSV | Downloads the table in csv format to your local drive.  

---

**Note:**

- Replaces hyphen (-) with N/A where hyphen indicates empty data.
- Replaces cells using the (unknown) string with empty cells where (unknown) indicates data missing due to an error(s).

Related topics:
2.5 CVP Virtual Appliance

The CVP virtual appliance is a packaged ova file that consists of Base OS packages, Hadoop, HBase, Apache Tomcat, JAVA jdk and the CVP web application.

You can deploy the virtual appliance as either a single-node (standalone) cluster or a multi-node cluster (cluster of three nodes). A multi-node cluster provides more benefits over a single-node cluster as specified in the table below.

Table 5: Single-Node and Multi-Node Cluster Comparison

<table>
<thead>
<tr>
<th>Single-Node Cluster</th>
<th>Multi-Node Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Low Scale</strong></td>
<td><strong>High Scale</strong></td>
</tr>
<tr>
<td>• Supports 250 devices and 10k interfaces</td>
<td>• Scalability is 6x times higher than single-node clusters</td>
</tr>
<tr>
<td>• Increasing resources may not mandatorily help due to bottlenecks of components</td>
<td>• Supports multiple containers in components</td>
</tr>
<tr>
<td></td>
<td>• Loads the share across nodes</td>
</tr>
<tr>
<td></td>
<td>• Optimization, speed, and availability are higher than single-node clusters</td>
</tr>
<tr>
<td><strong>No Redundancy</strong> - Does not support telemetry provisioning and streaming when the node goes down</td>
<td><strong>Redundancy</strong></td>
</tr>
<tr>
<td></td>
<td>• Supports 2N+1 redundancy</td>
</tr>
<tr>
<td></td>
<td>✋ <strong>Note:</strong> If a node goes down, kubernetes schedules the lost node pods on the other two nodes.</td>
</tr>
<tr>
<td></td>
<td>• Provides uninterrupted telemetry provisioning and streaming</td>
</tr>
<tr>
<td></td>
<td>• Provides Return Merchandise Authorization (RMA) when a node fails</td>
</tr>
<tr>
<td></td>
<td>• Each state has three replicas</td>
</tr>
<tr>
<td><strong>Corruption Management</strong></td>
<td><strong>Corruption Management</strong></td>
</tr>
<tr>
<td>• No recovery is available for lost data</td>
<td>• Automatically fixes issues 99% of the time</td>
</tr>
<tr>
<td>• Need manual intervention to fix hbase issues</td>
<td>• The feature to share load across nodes provides a faster and smoother experience</td>
</tr>
<tr>
<td>• Must remotely copy backups to a server everyday for restoring the node when the disk gets corrupted</td>
<td></td>
</tr>
</tbody>
</table>

The different deployment options will be discussed later on in this section, but for production deployments it is recommended that the cluster option is chosen. The single VM instance is recommended for testing purposes as it provides a simpler setup and requires less resources.

2.5.1 CVX and CVP

Certain CVP features leverage CVX. For the 2017.1 features, CVP is not dependent on any functionality provided by CVX, so deploying CVX along with CVP is recommended but not required.

You can register CVX with CVP in one of two ways:
• By provisioning CVX and then manually registering it in CVP.
• By ZTP booting CVX with CVP.

**Note:** CVX does not boot into ZTP mode by default, since it is a Virtual Machine (VM). Setting it up and then registering it manually with CVP is the recommended option.

The CVP appliance is shipped as a single OVA file which can be run on any x86 hypervisor. The hypervisors listed below have been tested and confirmed to work with the CVP appliance.

<table>
<thead>
<tr>
<th>Hypervisor</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware ESX</td>
<td>5.5</td>
</tr>
<tr>
<td>Linux RHEL</td>
<td>6.5-7.0</td>
</tr>
</tbody>
</table>

**Related topics:**

• [System Requirements](#)
• [Key CVP Terms](#)
CloudVision Portal (CVP) Setup

CloudVision Portal (CVP) can be run on ESX or KVM hypervisors. Before you can begin using the CVP, you must complete the CVP setup process which, involves the following:

1. Deploying CVP
2. Configuring CVP

Sections in this chapter include:

• Deploying CVP OVA on ESX
• Deploying CVP on KVM
• Set Up CVW on CV
• Shell-based Configuration
• Shell Reconfiguration of Single-node, Multi-node Systems
• ISO-based Configuration
• Certificate-Based TerminAttr Authentication

There are two different deployment procedures. One for deploying CVP on ESX, and one for deploying CVP on KVM. After you complete the deployment procedures, you then configure CVP.

The deployment procedures are:

• Deploying CVP OVA on ESX
• Deploying CVP on KVM

There are two configuration methods for the CloudVision Portal (CVP): shell-based and ISO-based. Both of these methods eliminate the need to directly modify system and CVP configuration files. This simplifies the setup process and reduces the potential for issues.

The configuration methods enable you to configure CVP in both single-node systems and multi-node systems. The configuration methods are:

• Shell-based Configuration (recommended)
• ISO-based Configuration

Note: Reconfiguration is limited to certain parameters on a deployed CVP multi-node cluster.

3.1 Deploying CVP OVA on ESX

Deploying the CVP OVA file should be the first step in any setup. After the CVP OVA file is deployed, you can chose between the two configuration methods for CloudVision Portal (CVP).

Note: Arista does not support VMware Snapshots on CloudVision virtual machines. Refer to Appendix A for more information about recommended backup mechanisms.

Pre-requisites:

Use of the Deploy OVF Template requires the VMware Client Integration plugin, which is not supported by the Chrome browser after versions 42.
1. The OVA file can be deployed as a VM in a VMware environment by using the drop menu under the Actions heading and selecting **Deploy the OVA template**.

   **Note:** For multi-node setups, the following steps must be completed once for each VM, 3 times to launch 3 VMs.

   ![Figure 3: Deploy the OVA template](image)

2. Having selected the Deploy OVF Template option, VCenter will prompt for the location of the OVA file; this can be either on a local hard disk, network share, or Internet URL. The location of the OVA file should be entered or selected.

   ![Figure 4: Location of the OVA file](image)

3. Click **Next** to go to the next task.
4. Review the OVA template details.

5. Click **Next** to go to the next task.

6. Type the name for the OVA file in the **Name** field and select the folder for the OVA file.

7. Click **Next** to go to the next task.
8. Select the resource where you want the deployed template (OVA file) to be run.

![Select Resource](image1.png)

**Figure 7: Select the resource**

9. Click **Next** to go to the next task.

10. Select the location where you want the files for the deployed template to be stored.

![Select Storage Location](image2.png)

**Figure 8: Select the destination storage**

- **Note:**
  It is recommended to select **Thick provision lazy zeroed** under the **Select virtual disk format** dropdown menu.

11. Click **Next** to go to the next task.
12. Setup the networks that the deployed template should use.

Figure 9: Setup the networks

13. Click **Next**.

VCenter loads the OVA and displays the configuration settings.

Figure 10: Select the Finish button to accept these settings

14. Review the configuration settings, and click **Finish** to accept and save the configuration.

VCenter begins to deploy the virtual appliance. Once the appliance is deployed, you can configure the CVP application using either **Shell-based Configuration** or **ISO-based Configuration**.

### 3.2 Deploying CVP on KVM

In standard KVM environments, deploying a CVP VM involves the following tasks:

- **Downloading and extracting the CVP KVM tarball (.tgz archive)**
- **Creating Virtual Bridge and Network Interface Cards (NIC)**
• Generating the XML file that defines the CVP VM
• Defining and Launching the CVP VM

Once you complete these tasks, you can configure the CVP VM.

### 3.2.1 Downloading and extracting the CVP KVM tarball (.tgz archive)

The first task in the deployment process involves downloading and extracting the CVP KVM tarball. The tarball is a .tgz archive that contains:

- The CVP VM
- Disk images for the CVP application
- The files used to configure CVP VM.

You download the tarball to the host server that is configured for KVM. The files contained in the .tgz archive include:

<table>
<thead>
<tr>
<th>Filename</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disk1.qcow2</td>
<td>VM disk image for the CVP application.</td>
</tr>
<tr>
<td>disk2.qcow2</td>
<td>Data disk image for the CVP application.</td>
</tr>
<tr>
<td>cvpTemplate.xml</td>
<td>A template for creating the XML file for libvirt domain specification.</td>
</tr>
<tr>
<td>generateXmlForKvm.py</td>
<td>A script for generating the CVP VM definition XML based on the XML template.</td>
</tr>
<tr>
<td>createNwBridges.py</td>
<td>A script for creating the network interfaces for the CVP VM.</td>
</tr>
</tbody>
</table>

Complete the following steps to download and extract the CVP VM .tgz archive:

1. Go to the Arista software downloads webpage and download the CVP VM tarball (**cvp-<version>-kvm.tgz**) to the host server set up for KVM.
2. Extract the tarball (**cvp-<version>-kvm.tgz**).

The following example shows extracting the CVP KVM .tgz archive.

```
[arastra@kvm vms]# cd cvpTests
cvp-2018.2.2-kvm.tar
[arastra@kvm cvpTests]# ls
cvp-2018.2.2-kvm.tar
cvpTemplate.xml
disk1.qcow2
disk2.qcow2
generateXmlForKvm.py
```

### 3.2.2 Creating Virtual Bridge and Network Interface Cards (NIC)

The second task in deploying CVP for KVM involves creating the bridges and interfaces that provide network connectivity for the CVP VM. You use the `createNwBridges.py` script you extracted in the previous task to create the required bridges and interfaces.
CloudVision Portal (CVP) Setup

Note: If the required network interfaces for CVP already exist, you do not have to complete this task. Go directly to Generating the XML file that defines the CVP VM

You have the option of deploying CVP with either two bridge interfaces or a single bridge interface.

- Two interfaces (the cluster bridge interface and the device bridge interface).
- Single interface (the device bridge interface).

Complete the following steps to create the network interfaces for CVP KVM connectivity:

1. (Optional) Use the `.createNwBridges.py -help` command to view a list of all the parameters available in the script.
   
   Note: Install the net-tools library using the `yum -y install net-tools` command before running the script.

2. Use the `./createNwBridges.py` to create the device bridge (or bridges) and interfaces needed.

The figure below shows an example of creating a single device bridge for a single-node deployment.

![Figure 11: Creating a device bridge (single node deployment)](image)

3. (Optional) Use the `brctl show` command to verify that the bridges were successfully created.

4. (Optional) Use the `ip address show` command to verify that the IP addresses have been allocated. In this example the one IP address for the br1 bridge.

The following output is an example of verifying bridge creation and IP address allocation. In this example, a bridge br1 was created, and one IP address has been allocated for the bridge.

```
[arastra@kvm1 ~]# ip address show br1
6: br1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether d0:94:66:4f:56:48 brd ff:ff:ff:ff:ff:ff
    inet 172.31.6.78/16 brd 172.31.255.255 scope global br1
       valid_lft forever preferred_lft forever
    inet6 fe80::d294:66ff:fe4f:5648/64 scope link
       valid_lft forever preferred_lft forever

[arastra@kvm1 ~]# ip route show
default via 172.31.0.1 dev br1
172.31.0.0/16 dev br1 proto kernel scope link src 172.31.0.1
```

3.2.3 Generating the XML file that defines the CVP VM

The third task in deploying CVP for KVM involves generating the XML file that you use to define the CVP VM. You use generateXmlForKvm.py script and the cvpTemplate.xml file you extracted previously to generate the XML file you use to define the CVP VM.

The cvpTemplate.xml file is a template that defines wildcard values that are filled by the other parameters that are specified when you execute the script.

Complete the following steps to generate the XML file:
1. (Optional) Use the `python generateXmlForKvm.py -help` command to view a list of all the parameters available in the script.

2. Run the `python generateXmlForKvm.py` script using the XML template (`cvpTemplate.xml`) as one of the inputs.

**Generation of XML file used to define CVP VM** shows an example of an XML being generated that can be used to define a CVP VM named `cvpTest`. The generated XML file is named `qemuout.xml`.

![Screenshot of terminal output](image)

**Figure 12: Generation of XML file used to define CVP VM**

### 3.2.4 Defining and Launching the CVP VM

The last task in deploying CVP for KVM is to define and launch the CVP VM. You use the XML file you generated in the previous task to define the CVP VM.

Complete the following steps to define and launch the CVP VM:

1. Run the `virsh define` command to define the CVP VM (specify the generated XML file).
2. Run the `virsh start` command to launch the newly defined CVP VM.
3. Run the `virsh console` command to attach (connect) to the CVP VM console.

Defining and Launching the CVP VM shows an example of the use of the commands to define and launch a CVP VM named cvpTest. The XML file used to define the CVP VM is named qemuout.xml.

![Figure 13: Defining and Launching the CVP VM]

You can now login as cvpadmin and complete the configuration of the CVP application. See Configuring a Single-Node CVP Instance using CVP Shell for the steps used to complete the configuration.

Related topics:
- Shell-based Configuration
- ISO-based Configuration
- Deploying CVP OVA on ESX

### 3.3 Set Up CVW on CV

This section describes the process to:
- Setup CVW on a Standalone CV
- Set Up CVW on a CV Cluster

#### 3.3.1 Setup CVW on a Standalone CV

CVW is disabled by default.

To enable CVW, perform the following steps:

1. Log in to the CV admin shell via the cvpadmin user.
2. Enter e to edit the settings. The CV configuration wizard is launched.

   **Note:** If you are setting up CV for the first time, you need to enter the values for all the settings (DNS, IP addresses, etc.) in the configuration wizard. Refer to the Shell-based Configuration for information on these settings. If you have already set up or just upgraded CV, and you only want to enable CVW, go to Step 3.

3. Set the **CloudVision WiFi Enabled** option to **Yes**.

   ![Figure 14: Setup CVW on a Standalone CV](image)

   Once the cursor is at the bottom of the configuration wizard, enter a to apply the configuration changes.

3.3.2 Set Up CVW on a CV Cluster

A few important points about the CVW service in a cluster deployment:

- CVW is disabled by default.
- For a CV cluster, you first need to Figure 15: Enable CVW on Primary Node and then Set Up CVW on Secondary and Tertiary Nodes.

   **Note:** The CVW service runs only on the primary and secondary nodes, but you need to apply the configuration changes to all the nodes, including the tertiary node. The CVW service starts on both nodes only after the setup on all the nodes (including the tertiary node) of the cluster has been completed.

- The CV configuration wizard consists of two parts (Figure 15: Enable CVW on Primary Node):
  - **common configuration**: Settings common to all the nodes in the cluster (For example, DNS and services such as CVW).
  - **node configuration**: Settings specific to a node (For example, Hostname and IP settings).

3.3.2.1 Enable CVW on Primary Node

To enable CVW on the primary node, perform the following steps:

1. Log in to the CV admin shell via the cvpadmin user.
2. Enter e to edit the settings. The CV configuration wizard is launched.

   **Note:** If you are setting up CV for the first time, you need to enter the values for all the settings (those belonging to the common configuration as well as the node configuration). Refer to Shell-based Configuration and Shell Reconfiguration of Single-node, Multi-node
CloudVision Portal (CVP) Setup

Systems for information on these settings. If you have already set up or just upgraded CV, and you only want to enable CVW, go to Step 3.

3. You can optionally assign a **CloudVision WiFi HA Cluster IP**.

![Figure 15: Enable CVW on Primary Node](image)

---

**Note:** CloudVision WiFi in HA mode configures an optional IP address, known as HA cluster IP that is automatically assigned to the active node in a cluster. Ensure that the HA Cluster IP address is different from the IP addresses of the actual device and cluster interfaces; but belongs to the same subnet as the Device Interface IP addresses of primary and secondary nodes. If HA cluster IP is not configured, IP addresses of both primary and secondary nodes must be configured on access points.

4. Set the **CloudVision WiFi Enabled** option to **Yes**.

### 3.3.2.2 Set Up CVW on Secondary and Tertiary Nodes

To set up CVW on the secondary and tertiary nodes, perform the following steps on the respective nodes:

1. Log in to the CV admin shell via the **cvpadmin** user.
2. Enter `e` to edit the settings. The CV configuration wizard is launched.

---

**Note:** The **Shell-based Configuration** settings are not editable on the secondary and tertiary nodes. If you are setting up CV for the first time, you need to enter the values for all the **Shell Reconfiguration of Single-node, Multi-node Systems** settings. If you have already set up or just upgraded CV, and you only want to enable CVW, go to Step 3.

3. Press **Enter** until the cursor reaches the bottom of the configuration wizard, past all the settings.
4. Once the cursor is at the bottom of the configuration wizard, enter `a` to apply the configuration changes.

---

**Note:** Whether **CloudVision WiFi Enabled** is set to **Yes** or **No**, applying the configuration changes causes the secondary and tertiary nodes to update their settings based on the primary node. This will start the CVW service on the primary and secondary nodes.
3.4 Shell-based Configuration

The shell-based configuration can be used to set up either a single-node CVP instance or multi-node CVP instances. The steps you use vary depending on whether you are setting up a single-node instance or a multi-node instance.

Cluster and device interfaces

A cluster interface is the interface that is able to reach the other two nodes in a multi-node installation. A device interface is the interface used by managed devices to connect to CVP. The ZTP configuration file is served over this interface. These two parameters are optional and default to eth0. Configuring these two interfaces is useful in deployments where a private network is used between the managed devices and a public-facing network is used to reach the other two cluster nodes and the GUI.

- Configuring a Single-Node CVP Instance using CVP Shell
- Configuring Multi-node CVP Instances Using the CVP Shell

3.4.1 Configuring a Single-Node CVP Instance using CVP Shell

After initial bootup, CVP can be configured at the VM's console using the CVP config shell. At points during the configuration, you must start the network, NTPD, and CVP services. Starting these services may take some time to complete before moving on to the next step in the process.

Pre-requisites:

Before you begin the configuration process, make sure that you:

- Launch the VM (see Deploying CVP OVA on ESX, or Deploying CVP on KVM.)

To configure CVP using the CVP config shell:

1. Login at the VM console as cvpadmin.
2. Enter your configuration and apply it (see the following example).

In this example, the root password is not set (it is not set by default). In this example of a CVP shell, the bold text is entered by the cvpadmin user.

Note: To skip static routes, simply press enter when prompted for number of static routes.

```
localhost login: cvpadmin
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Enter a command [q]uit [p]rint [s]ingletone [m]ultinode [r]eplace [u]pgrade
>s
Enter the configuration for CloudVision Portal and apply it when done. Entries marked with '*' are required.

common configuration:
dns: 172.22.22.40
DNS domains: sjc.aristanetworks.com, ire.aristanetworks.com
ntp: ntp.aristanetworks.com
Telemetry Ingest Key: arista
CloudVision WiFi Enabled: yes
CloudVision WiFi HA cluster IP:
Cluster Interface name: eth0
Device Interface name: eth0
node configuration:
*hostname (fqdn): cvp80.sjc.aristanetworks.com
*default route: 172.31.0.1
```
CloudVision Portal (CVP) Setup

DNS domains: sjc.aristanetworks.com, ire.aristanetworks.com
Number of Static Routes: 1
Route for Static Route #1: 1.1.1.0
Netmask for Static Route #1: 255.255.255.0
Interface for Static Route #1: eth0
TACACS server ip address:
*IP address of eth0: 172.31.0.168
*Netmask of eth0: 255.255.0.0

> v
Valid config format.
Applying proposed config for network verification.
saved config to /cvpi/cvp-config.yaml
Running : cvpConfig.py tool...

Valid config.
Applying proposed config for network verification.
saved config to /cvpi/cvp-config.yaml

3.4.2 Configuring Multi-node CVP Instances Using the CVP Shell

Use this procedure to configure multi-node CVP instances using the CVP shell. This procedure includes the steps to set up a primary, secondary, and tertiary node, which is the number of nodes required for redundancy. It also includes the steps to verify and apply the configuration of each node.

The sequence of steps in this procedure follow the process described in the basic steps in the process

Pre-requisites:
Before you begin the configuration process, make sure that you:
• Launch the VM (see Deploying CVP OVA on ESX, or Deploying CVP on KVM.)
• Login to the VM console for each of the three (3) nodes (login as cvpadmin on each node).

Complete the following steps to configure multi-node CVP instances:

1. Login at the VM console for the primary node as cvpadmin.
2. At the cvp installation mode prompt, type m to select a multi-node configuration.
3. At the prompt to select a role for the node, type p to select primary node.

   Note: You must select primary first. You cannot configure one of the other nodes before you configure the primary node.

4. Follow the CloudVision Portal prompts to specify the configuration options for the primary node. (All options with an asterisk (*) are required.) The options include:
   • Root password (*)
   • Default route (*)
   • DNS (*)
   • NTP (*)
   • Telemetry Ingest Key
   • Cluster interface name (*)
   • Device interface name (*)
   • Hostname (*)
   • IP address (*)
   • Netmask (*)
   • Number of static routes
   • Route for each static route
   • Interface for static route
   • TACACS server ip address
   • TACACS server key/port
   • IP address of primary (*) for secondary/tertiary only

   Note: If there are separate cluster and device interfaces (the interfaces have different IP addresses), make sure that you enter the hostname of the cluster interface. If the cluster and device interface are the same (for example, they are eth0), make sure you enter the IP address of eth0 for the hostname.

5. At the following prompt, type v to verify the configuration.


If the configuration is valid, the system shows a Valid config status message.

6. Type a to apply the configuration for the primary node and wait for the line Waiting for other nodes to send their hostname and ip with spinning wheel.

   The system automatically saves the configuration as a YAML document and shows the configuration settings in pane 1 of the shell.

7. When Waiting for other nodes to send their hostname and ip line is printed by the primary node, go to the shell for the secondary node, and specify the configuration settings for the secondary node (All options with an asterisk (*) are required, including primary node IP address)

8. At the following prompt, type v to verify the configuration.


If the configuration is valid, the system shows a Valid config status message.

9. At the Primarys root password prompt, type (enter) the password for the primary node, and then press Enter.
10. Go to the shell for the tertiary node, and specify the configuration settings for the node. (All options with an asterisk (*) are required.)
11. At the following prompt, type v to verify the configuration.


If the configuration is valid, the system shows a Valid config status message.
12. At the Primary IP prompt, type the IP address of the primary node.
13. At the Primary's root password prompt, press Enter.

The system automatically completes the CVP installation for all nodes (this is done by the primary node). A message appears indicating that the other nodes are waiting for the primary node to complete the CVP installation.

When the CVP installation is successfully completed for a particular node, a message appears in the appropriate pane to indicate the installation was successful. (This message is repeated in each pane.)
14. Go to shell for the primary node, and type q to quit the installation.
15. At the cvp login prompt, login as root.
16. At the [root@cvplogin]# prompt, switch to the cvp user account by typing su cvp, and then press Enter.
17. Run the cvpi status all command, and press Enter.

The system automatically checks the status of the installation for each node and provides status information in each pane for CVP. The information shown includes some of the configuration settings for each node.

For more information about the process, see:
- Rules for the Number and Type of Nodes
- The Basic Steps in the Process
- The CVP Shell
- Examples

3.4.2.1 Rules for the Number and Type of Nodes
Three nodes are required for multi-node CVP instances, where a node is identified as either the primary, secondary, or tertiary. You define the node type (primary, secondary, or tertiary) for each node during the configuration.

3.4.2.2 The Basic Steps in the Process
All multi-node configurations follow the same basic process. The basic steps are:
1. Specify the settings for the nodes in the following sequence (you apply the configuration later in the process):
   - Primary node
   - Secondary node
   - Tertiary node
2. Verify and then apply the configuration for the primary node. (During this step, the system automatically saves the configuration for the primary node as a YAML document. In addition, the system shows the configuration settings.)

Once the system applies the configuration for the primary node, the other nodes need to send their hostname and IP address to the primary node.
3. Verify and then apply the configuration for the **secondary** node.

As part of this step, the system automatically pushes the hostname, IP address, and public key of the secondary node to the primary node. The primary node also sends a consolidated YAML to the secondary node, which is required to complete the configuration of the secondary node.

4. The previous step (verifying and applying the configuration) is repeated for the **tertiary** node. (The automated processing of data described for the secondary node is also repeated for the tertiary node.)

Once the configuration for all nodes has been applied (steps 1 through 4 above), the system automatically attempts to complete the CVP installation for all nodes (this is done by the primary node). A message appears indicating that the other nodes are waiting for the primary node to complete the CVP installation.

5. You quit the installation, then login as root and check the status of CVP.

The system automatically checks the status and provides status information in each pane for the CVP service.

### 3.4.2.3 The CVP Shell

For multi-node configurations, you need to open 3 CVP consoles (one for each node). Each console is shown in its own pane. You use each console to configure one of the nodes (primary, secondary, or tertiary).

The system also provides status messages and all of the options required to complete the multi-node configuration. The status messages and options are presented in the panes of the shell that correspond to the node type.

**Figure 16: CVP Console Shells for Multi-node Configurations** shows three CVP Console shells for multi-node configurations. Each shell corresponds to a CVP Console for each node being configured.

### 3.4.2.4 Examples

The following examples show the commands used to configure (set up) the primary, secondary, and tertiary nodes, and apply the configurations to the nodes. Examples are also included of the system output shown as CVP completes the installation for each of the nodes.

- **Primary Node Configuration**
3.4.2.4.1 Primary Node Configuration

This example shows the commands used to configure (set up) the primary node.

```bash
localhost login: cvpadmin
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Enter a command
>m
Choose a role for the node, roles should be mutually exclusive
[p]rimary [s]econdary [t]ertiary
>p
Enter the configuration for CloudVision Portal and apply it when done.
Entries marked with '*' are required.

common configuration:
dns: 172.22.22.40, 172.22.22.10
DNS domains: sjc.aristanetworks.com, ire.aristanetworks.com
ntp: ntp.aristanetworks.com
Telemetry Ingest Key: arista
CloudVision WiFi Enabled: no
CloudVision WiFi HA cluster IP:
Cluster Interface name: eth0
Device Interface name: eth0
node configuration:
*hostname (fqdn): cvp57.sjc.aristanetworks.com
*default route: 172.31.0.1
Number of Static Routes:
TACACS server ip address:
*IP address of eth0: 172.31.0.186
*Netmask of eth0: 255.255.0.0
```

3.4.2.4.2 Secondary Node Configuration

This example shows the commands used to configure (set up) the secondary node.

```bash
localhost login: cvpadmin
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Secondary Node Configuration
- Secondary Node Configuration
- Tertiary Node Configuration
- Verifying the Primary Node Configuration and Applying it to the Node
- Verifying the Tertiary Node Configurations and Applying them to the Nodes
- Waiting for the Primary Node Installation to Finish
- Waiting for the Secondary and Tertiary Node Installation to Finish
Enter a command
>m
Choose a role for the node, roles should be mutually exclusive
[p]rimary [s]econdary [t]ertiary
>s

Enter the configuration for CloudVision Portal and apply it when done.
Entries marked with '*' are required.

common configuration:
  dns: 172.22.22.40, 172.22.22.10
  DNS domains: sjc.aristanetworks.com, ire.aristanetworks.com
  ntp: ntp.aristanetworks.com
  Telemetry Ingest Key: arista
  CloudVision WiFi Enabled: no
  CloudVision WiFi HA cluster IP:
  Cluster Interface name: eth0
  Device Interface name: eth0
  *IP address of primary: 172.31.0.186

node configuration:
  *hostname (fqdn): cvp65.sjc.aristanetworks.com
  *default route: 172.31.0.1
  Number of Static Routes:
  TACACS server ip address:
  *IP address of eth0: 172.31.0.153
  *Netmask of eth0: 255.255.0.0

3.4.2.4.3 Tertiary Node Configuration

This example shows the commands used to configure (set up) the tertiary node.

Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Enter a command
>t
Choose a role for the node, roles should be mutually exclusive
[p]rimary [s]econdary [t]ertiary
>t

Enter the configuration for CloudVision Portal and apply it when done.
Entries marked with '*' are required.

common configuration:
  dns: 172.22.22.40, 172.22.22.10
  DNS domains: sjc.aristanetworks.com, ire.aristanetworks.com
  ntp: ntp.aristanetworks.com
  Telemetry Ingest Key: arista
  Cluster Interface name: eth0
  Device Interface name: eth0
  *IP address of primary: 172.31.0.186

node configuration:
  hostname (fqdn): cvp84.sjc.aristanetworks.com
**CloudVision Portal (CVP) Setup**

*default route: 172.31.0.1
Number of Static Routes:
TACACS server ip address:
*IP address of eth0: 172.31.0.213
*Netmask of eth0: 255.255.0.0

3.4.2.4 Verifying the Primary Node Configuration and Applying it to the Node

This example shows the commands used to verify the configuration of the primary node and apply the configuration to the node.

```
> v
Valid config format.
Applying proposed config for network verification.
saved config to /cvpi/cvp-config.yaml
Running: cvpConfig.py tool...
[ 8608.509056] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9 vectors allocated
[ 8608.520693] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[ 8622.807169] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9 vectors allocated
[ 8622.810214] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
Stopping: network
Running: /bin/sudo /sbin/service network stop
Running: /bin/sudo /bin/systemctl is-active network
Starting: network
Running: /bin/sudo /bin/systemctl start network.service
[ 8624.027029] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9 vectors allocated
[ 8624.030254] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[ 8624.032643] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[ 8624.238995] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[ 8638.294690] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9 vectors allocated
[ 8638.297973] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[ 8638.300454] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
[ 8638.489266] warning: `/bin/ping' has both setuid-root and effective capabilities. Therefore not raising all capabilities.
Warning: External interfaces, ['eth1'], are discovered under /etc/sysconfig/network-scripts
These interfaces are not managed by CVP.
Please ensure that the configurations for these interfaces are correct.
Otherwise, actions from the CVP shell may fail.
```

Valid config.
3.4.2.4.5 Verifying the Tertiary Node Configurations and Applying them to the Nodes

This example shows the commands used to verify the configurations of the tertiary nodes and apply the configurations to the nodes.

```
> v
Valid config format.
Applying proposed config for network verification.
saved config to /cvpi/cvp-config.yaml
Running: cvpConfig.py tool...
[ 9195.362192] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9 vectors allocated
[ 9195.365069] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[ 9195.367043] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[ 9195.652382] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[ 9209.588173] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9 vectors allocated
[ 9209.590896] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[ 9209.592887] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
[ 9209.594222] IPv6: ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
Stopping: network
Running: /bin/sudo /sbin/service network stop
Running: /bin/sudo /bin/systemctl is-active network
Starting: network
Running: /bin/sudo /bin/systemctl start network.service
[ 9210.561940] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9 vectors allocated
[ 9210.564602] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[ 9224.805267] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9 vectors allocated
[ 9224.808891] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[ 9224.811150] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
[ 9224.812899] IPv6: ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
Warning: External interfaces, ['eth1'], are discovered under /etc/sysconfig/network-scripts
These interfaces are not managed by CVP.
Please ensure that the configurations for these interfaces are correct.
Otherwise, actions from the CVP shell may fail.
Valid config.
> q
```

3.4.2.4.6 Waiting for the Primary Node Installation to Finish

These examples show the system output shown as CVP completes the installation for the primary node.

- Waiting for primary node installation to pause until other nodes send files

```bash
[>]u[>]it [>]p[>]rint [>]e[>]dit [>]v[>]erify [>]s[>]ave [>]a[>]pply [>]h[>]elp ve[>]rbose

>a
Valid config format.
saved config to /cvpi/cvp-config.yaml
Applying proposed config for network verification.
saved config to /cvpi/cvp-config.yaml
Running : cvpConfig.py tool...
[15266.575899] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9
  vectors allocated
[15266.588500] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[15266.591751] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[15266.672644] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[15280.937599] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9
  vectors allocated
[15280.941764] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[15280.944883] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
[15280.947038] IPv6: ADDRCONF(NETDEV_CHANGE): eth1: link becomes ready
Stopping: network
Running : /bin/sudo /sbin/service network stop
Running : /bin/sudo /bin/systemctl is-active network
Starting: network
Running : /bin/sudo /bin/systemctl is-active network
[15282.581713] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9
  vectors allocated
[15282.585367] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[15282.588072] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[15282.948613] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[15296.871658] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9
  vectors allocated
[15296.875871] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[15296.879003] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
Warning: External interfaces, ['eth1'], are discovered under /etc/ sysconfig/network-scripts
These interfaces are not managed by CVP.
Please ensure that the configurations for these interfaces are correct. Otherwise, actions from the CVP shell may fail.

Valid config.
Running : cvpConfig.py tool...
[15324.884887] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9
  vectors allocated
[15324.889169] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[15324.893217] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[15324.981682] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[15339.240237] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9
  vectors allocated
[15339.243999] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[15339.247119] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
Stopping: network
Running : /bin/sudo /sbin/service network stop
Running : /bin/sudo /bin/systemctl is-active network
Starting: network
Running : /bin/sudo /bin/systemctl start network.service
```
Waiting for other nodes to send their hostname and ip

- Waiting for the primary node installation to finish

Waiting for other nodes to send their hostname and ip

Running : cvpConfig.py tool...

Stopping: ntpd
Running : /bin/sudo /sbin/service ntpd stop
Starting: ntpd
Running : /bin/sudo /bin/systemctl is-active ntpd
Starting: ntpd.service

Starting: systemd services
Starting: cvpi-check
Running : /bin/sudo /bin/systemctl start cvpi-check.service
Starting: zookeeper
Running : /bin/sudo /bin/systemctl start zookeeper.service
Starting: cvpi-config
Running : /bin/sudo /bin/systemctl start cvpi-config.service
Starting: cvpi
Running : /bin/sudo /bin/systemctl start cvpi.service
Running : /bin/sudo /bin/systemctl enable zookeeper
Running : /bin/sudo /bin/systemctl start cvpi-watchdog.timer
Running : /bin/sudo /bin/systemctl enable docker
Running : /bin/sudo /bin/systemctl start docker
Running : /bin/sudo /bin/systemctl enable kube-cluster.path
Running : /bin/sudo /bin/systemctl start kube-cluster.path
Waiting for all components to start. This may take few minutes.
Still waiting for aaa aeridiakmonitor alertmanager-multinode-service
ambassador apiserver apiserver-www apiserver-www apiserver-www apiserver-www audit
aware ... (total 271)
Still waiting for aaa aerisdisknonitor alertmanager-multinode-service
ambassador apiserver apiserver-www apiserver-www apiserver-www apiserver-www audit
bapmaintmode ... (total 235)
Still waiting for asa aerisdiskmonitor alertmanager-multinode-service ambassador apiserver apiserver-www spiserver-www apiserver-www audit bgpmaintmode ... (total 236)
Still waiting for aaa aerisdiskmonitor alertmanager-multinode-service ambassador apiserver apiserver-www apiserver-www apiserver-www audit bgpmaintmode ... (total 235)
Still waiting for aaa aerisdiskmonitor alertmanager-multinode-service ambassador apiserver apiserver-www apiserver-www apiserver-www audit bgpmaintmode ... (total 235)
Still waiting for aaa aerisdiskmonitor alertmanager-multinode-service ambassador apiserver apiserver-www apiserver-www apiserver-www audit bgpmaintmode ... (total 236)
Still waiting for aaa aerisdiskmonitor alertmanager-multinode-service ambassador apiserver apiserver-www apiserver-www apiserver-www audit bgpmaintmode ... (total 235)
Still waiting for eae aerisdiskmonitor alertmanager-multinode-service ambassador apiserver apiserver-www aps server-www audit bgpmaintmode ... (total 229)
Still waiting for eae aerisdiskmonitor alertmanager-multinode-service ambassador apiserver aps server-www aps server-www audit bgpmaintmode ... (total 228)
Still waiting for eae aerisdiskmonitor alertmanager-multinode-service ambassador apiserver aps server-www aps server-www audit bgpmaintmode ... (total 213)
3.4.2.4.7 Waiting for the Secondary and Tertiary Node Installation to Finish

This example shows the system output displayed as CVP completes the installation for the secondary and tertiary nodes.

```

Valid config format.
saved config to /cvpi/cvp-config.yaml
Applying proposed config for network verification.
saved config to /cvpi/cvp-config.yaml
Running : cvpConfig.py tool...
[15492.903419] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9 vectors allocated
[15492.908473] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[15492.910297] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[15493.289569] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[15507.118778] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9 vectors allocated
[15507.121579] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[15507.123648] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
Stopping: network
Running : /bin/sudo /sbin/service network stop
Running : /bin/sudo /bin/systemctl is-active network
Starting: network
Running : /bin/sudo /bin/systemctl start network.service
[15508.105909] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9 vectors allocated
[15508.108752] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[15522.301114] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9 vectors allocated
[15522.303766] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[15522.305580] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready
Warning: External interfaces, ['eth1'], are discovered under /etc/sysconfig/network-scripts
These interfaces are not managed by CVP.
Please ensure that the configurations for these interfaces are correct.
Otherwise, actions from the CVP shell may fail.
Valid config.
Running : cvpConfig.py tool...
[15549.664989] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9 vectors allocated
[15549.667899] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[15549.669783] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
```
CloudVision Portal (CVP) Setup

IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready

Stopping: network
Running : /bin/sudo /sbin/service network stop
Running : /bin/sudo /bin/systemctl is-active network
Starting: network
Running : /bin/sudo /bin/systemctl start network.service

Stopping: ntpd
Running : /bin/sudo /sbin/service ntpd stop
Running : /bin/sudo /bin/systemctl is-active ntpd
Starting: ntpd
Running : /bin/sudo /bin/systemctl start ntpd.service

Pushing hostname, ip address and public key to the primary node
Primary's root password: 
Transferred files
Receiving public key of the primary node
Waiting for primary to send consolidated yaml
-
Received authorized keys and consolidated yaml files
Running : /bin/sudo /bin/systemctl start cvpi-watchdog.timer
Running : cvpConfig.py tool...
3.5 Shell Reconfiguration of Single-node, Multi-node Systems

The configuration of single-node systems and multi-node systems can be reconfigured using the CVP shell, even after the installation is complete. The reconfiguration process brings down the applications and CVPI for a brief period of time until reconfiguration is complete.

- Single-node Shell Reconfiguration
- Multi-node Shell Reconfiguration

3.5.1 Single-node Shell Reconfiguration

The process for reconfiguring a single-node system is based on the process used to complete the initial installation. You can change any of the configuration settings during the reconfiguration.
Note: The system must be in healthy state before reconfiguration is attempted.

To change an existing single-node configuration, do the following:

1. Follow the same steps you use for an initial single-node, shell-based install (see Configuring a Single-Node CVP Instance using CVP Shell).
2. When prompted with the message Are you sure you want to replace config and restart? yes/no: enter yes, and then press Enter. (Make sure there are no configuration errors.) This system automatically completes the configuration.

3.5.2 Multi-node Shell Reconfiguration

The process for reconfiguring a multi-node system is based on the process used to complete the initial installation. Just like initial installations, you can only edit the configuration of the node you are logged into.

- Configurable and Read-only Parameters
- Shifting Parameters
- Example of Primary Node Reconfiguration
- Procedure

3.5.2.1 Configurable and Read-only Parameters

You can change some, but not all of the configuration settings during the reconfiguration. The configuration parameters you cannot change are read-only after the initial configuration.

The configurable and read-only parameters are:

- Configurable parameters
  - default route (gateway)
  - dns
  - ntp
  - aeris ingest key
  - TACACS server IP address
  - TACACS server key/port

- Read-only parameters
  - Cluster interface name
  - Device interface name
  - hostname (fqdn)
  - ip address
  - netmask
  - Number of static routes
  - Route for each static route
  - Interface for static route
  - Primary IP address (use current primary ip address)

Note: The cluster must be in healthy state before reconfiguration is attempted. Also, do not edit cvp-config.yaml directly. Make sure you use the shell-based install to reconfigure it.

3.5.2.2 Shifting Parameters

You have the option of shifting common-level parameters (parameters that apply to the cluster), down to the node-level section, and from the node-level section up to the common-level. One example of a common-level parameters you can shift down is default gateway.
**Note:** If you shift parameters from one level to the other, you may encounter the “Incomplete config” warning during the verify section. If this happens, acknowledge the warning by typing “Y” at the prompt, and then continue with the install.

This example shows the “Incomplete config” warning:

```
> v
Incomplete config - Missing
secondary:
- default route
tertiary:
- default route

Override warnings? [Y/n] : Y
Valid config format
```

### 3.5.2.3 Example of Primary Node Reconfiguration

```
localhost login: cvpadmin
Changing password for user root.
New password:
 Retype new password:
passwd: all authentication tokens updated successfully.
Enter a command
>m
Choose a role for the node, roles should be mutually exclusive
[p]rimary [s]econdary [t]ertiary
>p
...
>e
CVP service is configured and may be running, reconfigure may be limited to certain parameters
common configuration:
  dns: 172.22.22.40
  ntp: ntp.aristanetworks.com
  Telemetry Ingest Key: modified_ingest_key_for_telemetry <-- modified key
  Cluster Interface name: eth0
  Device Interface name: eth0
node configuration:
  *hostname (fqdn): cvp57.sjc.aristanetworks.com
  *default route: 172.31.0.1
  Number of Static Routes:
  *TACACS server ip address:
  *IP address of eth0: 172.31.0.186
  *Netmask of eth0: 255.255.0.0
>v
Valid config format.
Using existing settings for new proposed network verification.
Warning: External interfaces, ['eth1'], are discovered under /etc/
sysconfig/network-scripts
These interfaces are not managed by CVP.
Please ensure that the configurations for these interfaces are correct.
Otherwise, actions from the CVP shell may fail.

Valid config.
>a
Valid config format.
saved config to /cvpi/cvp-config.yaml
```
Using existing settings for new proposed network verification. Warning: External interfaces, ['eth1'], are discovered under /etc/sysconfig/network-scripts. These interfaces are not managed by CVP. Please ensure that the configurations for these interfaces are correct. Otherwise, actions from the CVP shell may fail.

Valid config.
Are you sure you want to replace config and restart? yes/no: no

3.5.2.4 Procedure
To change an existing multi-node configuration, do the following:

1. Follow the same steps you use for an initial multi-node, shell-based install (see Configuring Multi-node CVP Instances Using the CVP Shell).
2. When prompted with the message Are you sure you want to replace config and restart? yes/no: enter yes, and then press Enter. (Make sure there are no configuration errors.)

   Note: You will also be prompted for primary node IP address and root passwords during reconfiguration.

Related concepts
Getting Started (CVP)
The login screen is displayed when you first connect to the application using a web browser.

3.6 ISO-based Configuration
The ISO-based configuration can be used to set up either a single-node or multi-node CVP instance(s). Before configuring and starting CVP, the following tasks must be completed.

Quick Start Steps:
- Launch the VM (see Deploying CVP OVA on ESX or Deploying CVP on KVM).
- Create a YAML Document
- Feed the YAML File into the geniso.py Tool
- Map ISO to the VM's CD-ROM Drive
- Verify the host name, reachability of the name server, and VM connectivity.

3.6.1 Create a YAML Document
Create a YAML document describing the node(s) (one or three) in your CVP deployment. When creating a YAML document, the following should be considered:

- The version field is required and must be 2.
- The "dns" and "ntp" entries are lists of values.
- The "dns", and "ntp" parameters are optional, but recommended to use.

   Note: The parameters, which are the same for all nodes, can be specified only once in the common section of the YAML. For example, "default_route" can be specified only once in the common section and not three times, once for each node.

   Example:

   The following example of a YAML document shows the use of separate (different) interfaces for cluster and device-facing networks. These parameters are explained in the previous section. For a
single-node deployment, remove the sections for "node2" and "node3" (assuming all nodes are on the same subnet and have the same default route).

```yaml
>cat multinode.yaml
version: 2
common:
  aeris_ingest_key: magickey
  cluster_interface: eth0
  default_route: 172.31.0.1
  device_interface: eth0
dns:
  - 172.22.22.40
ntp:
  - ntp.aristanetworks.com
node1:
  hostname: cvp6.sjc.aris.tanetworks.com
  interfaces:
    eth0:
      ip_address: 172.31.3.236
      netmask: 255.255.0.0
    vmname: cvp6
node2:
  vmname: cvp9
  hostname : cvp9.sjc.aristanetworks.com
  interfaces:
    eth0:
      ip_address: 172.31.3.239
      netmask: 255.255.0.0
    eth1:
      ip_address: 10.0.0.2
      netmask: 255.255.255.0
node3:
  vmname: cvp10
  hostname: cvp10.sjc.aristanetworks.com
  interfaces:
    eth0:
      ip_address: 172.31.3.240
      netmask: 255.255.0.0
    eth1:
      ip_address: 10.0.0.3
      netmask: 255.255.255.0
```

3.6.2 Feed the YAML File into the `geniso.py` Tool

Once you have created the YAML file, you are ready to feed it into the tool so that you can generate the ISO files for the CVP nodes. The root password can be provided at the command line or prompted from the user. If password is empty, no password will be set for root.

Note: The `geniso.py` tool is provided by `cvp-tools-1.0.1.tgz` which can be found at [https://www.arista.com/en/support/software-download](https://www.arista.com/en/support/software-download). The package also contains a README file with more details and requirements for `geniso.py`.

Complete the following steps:

1. Run the `yum install mkisofs` command.
2. Feed the YAML document into the `geniso.py` tool.

The system generates the ISO files for the nodes using the input of the YAML document.

**Example:**
- In this example, you are prompted for the root password.

  ```
  > mkdir tools
  > tar zxf cvp-tools-1.0.1.tgz -C tools
  > cd tools
  ...
  > ./geniso.py -y multinode.yaml
  $ Please enter a password for root user on cvp
  $ Password: [hidden]
  $ Please re-enter the password:
  $ Building ISO for node1 cvp1: cvp.iso.2015-11-04_00:16:23/node1-cvp1.iso
  $ Building ISO for node2 cvp2: cvp.iso.2015-11-04_00:16:23/node2-cvp2.iso
  $ Building ISO for node3 cvp3: cvp.iso.2015-11-04_00:16:23/node3-cvp3.iso
  ```

3. In case of using KVM as a hypervisor in a multi-node setup, copy the following ISO files to the corresponding nodes:

   - SCP node2's ISO to node 2

     ```
     [root@localhost cvp]# scp node2-cvp-appliance-2.iso root@172.28.161.44://data/cvp/
     root@172.28.161.44's password: [hidden]
     100% 360KB 57.5MB/s 00:00
     ```

   - SCP node3's ISO to node 3

     ```
     [root@localhost cvp]# scp node3-cvp-appliance-3.iso root@172.28.161.45://data/cvp/
     root@172.28.161.45's password: [hidden]
     100% 360KB 54.7MB/s 00:00
     ```

   **Note:** The script has to be run on one machine only. This generates three ISO images which contains the same ssh keys, thus allowing the nodes to send files without a password. If the script is run individually on each node, it result in images containing different ssh keys and the deployment process fails, until the user manually adds the ssh keys in `~/.ssh/authorized_keys`.

3.6.3 Map ISO to the VM's CD-ROM Drive

You can map the ISO to the VM's CD-ROM drive through either ESXi or KVM.

Refer to the chapter to start working on the CVP.

**Related concepts**

- [Getting Started (CVP)](#)

The login screen is displayed when you first connect to the application using a web browser.
3.7 Certificate-Based TerminAttr Authentication

Arista/EOS switches use TerminAttr for streaming network data to CVP in the following network configurations:

- Firewalls or dynamic NAT is deployed between CloudVision and EOS devices
- Multi-Factor Authentication (MFA) or One-Time-Passwords (OTPs) are used for authentication

**Note:** When terminattr authentication is enabled, CVP does not require EAPI-over-HTTPS connections. Any CVP authenticated user is also authenticated with the devices that CVP manages.

Each TerminAttr connection must be authenticated using either shared keys or certificate. The certificate-based TerminAttr authentication provides the following additional security features:

- Eliminates the shared key from the switch's configuration
- Uniquely authenticates each TerminAttr connection between the switch and CVP

**Note:** Third party devices can use only the shared key authentication. The minimum required version of TerminAttr to use this feature is v1.6.1.

The following sections describes configuring devices with certificate-based TerminAttr authentication:

- Enabling Certificate-Based TerminAttr Authentication
- Reboarding Existing Devices
- Re-ZTP On-Boarded Devices
- Switching the Authentication from Shared Keys to Certificates
- Switching the Authentication from Certificates to Shared Keys

3.7.1 Enabling Certificate-Based TerminAttr Authentication

When on-boarding a device through Zero Touch Provisioning (ZTP) or direct import, the certificate-based TerminAttr authentication uses a temporary token to enroll client certificates from CVP. The SYS_TelemetryBuilderV3 generates the TerminAttr configuration that uses certificate-based TerminAttr authentication.

**Note:** By default, CVP authenticates TerminAttr connections using shared keys.

Perform the following steps to enable certificate-based TerminAttr authentication:

1. In CloudVision portal, click the gear icon at the upper right corner of the page.
   The system displays the Settings screen.
2. Under the Cluster Management pane, enable **Device authentication via certificates** using the toggle button.

![Image of CloudVision Portal](image)

**Figure 17: Enable Device Authentication via Certificates**

### 3.7.2 Switching the Authentication from Certificates to Shared Keys

Perform the following steps for switching the authentication from certificates to shared keys:

1. Disable the **Device authentication via certificates** option on the settings page.
   
   See [Enabling Certificate-Based TerminAttr Authentication](#).

2. Regenerate the configlets for all devices using SYS_TelemetryV3 builder.
   
   The generated configlets start using shared key authentication.

3. Execute resulting tasks.

### 3.7.3 Switching the Authentication from Shared Keys to Certificates

Perform the following steps for switching the authentication from shared keys to certificates:

1. Enable the **Device authentication via certificates** option on the settings page.
   
   See [Enabling Certificate-Based TerminAttr Authentication](#).

2. Replace any configlet mapping using the SYS_TelemetryV2 configlet builder with the SYS_TelemetryV3 builder.

3. Regenerate device configlets.

4. Execute resulting tasks.

   Devices stop streaming as their certificates are not enrolled.

5. On-board all currently provisioned devices to restart streaming to CVP.
   
   See [Reboarding Existing Devices](#).

### 3.7.4 Reboarding Existing Devices

You must reboard a device when the certificate-based TerminAttr authentication fails due to missing or invalid client certificates.

Perform the following steps to reboard devices:
1. In CloudVision portal, click the **Devices** tab.

   The system displays the Inventory screen.

![Inventory Screen](image1.png)

**Figure 18: Inventory Screen**

2. Select **Onboard Devices** from the **Add Device** drop-down menu at the upper right corner of the **Inventory** screen.

   The system displays the Onboard Devices pop-up window.

3. Click the **Existing Device Registration** tab at the lower end of the **Onboard Devices** pop-up window.

![Existing Device Registration Tab](image2.png)

**Figure 19: Existing Device Registration Tab**

   **Note:** To view all devices, disable the **Show only inactive devices** option using the toggle button.

4. Select the required device.

5. Click **Register n Device(s)** where \( n \) is the count of selected devices.

   The system refreshes the selected device with new certificates, returns to the last provisioning state, and resumes streaming to CVP.
3.7.5 Re-ZTP On-Boarded Devices

Manual intervention is required to re-ZTP on-boarded devices after enabling the certificate-based TerminAttr authentication. This prevents unauthorized or malicious software from spoofing previously on-boarded devices.

Perform the following steps to re-ZTP devices:

1. In CloudVision portal, click the **Devices** tab.
   
The system displays the Inventory screen.

2. Select Re-ZTP Devices from the Add Device drop-down menu at the upper right corner of the Inventory screen.
   
The system displays the Re-ZTP Devices pop-up window.

   ![Figure 20: Re-ZTP Devices Pop-Up Window](image)

   **Note:** To view all devices, disable the Show only inactive devices option using the toggle button.

3. Select the required device.

4. (Optional) Click the time next to Global ZTP Deadline and configure the preferred time to re-ZTP selected devices.

5. Click **Grant ZTP Access to n Device(s)** where n is the count of selected devices.

   Devices must complete their re-ZTP before the enrollment window closes.
CloudVision as-a-Service

CloudVision as-a-Service is an Arista-managed, multi-tenant cloud service deployed in tier one public cloud providers. CloudVision as-a-Service features include secure state-streaming and analytics on top of an Arista managed multi-tenant scale-out architecture. Customers are assigned to a unique organization (tenant) in a specific region. All devices and users of that customer are part of this organization. Organizations are isolated from each other and a user in one organization cannot access any data from other organizations. Authentication is tied to the customer’s AAA provider. CloudVision as-a-Service provides device provisioning workflows and state streaming.

Sections in this chapter include:

- Prerequisites
- Onboarding Procedures
- AAA Providers

4.1 Prerequisites

Verify the following requirements before installing CloudVision as-a-Service.

- Software Requirements
- Connectivity Requirements
- Authentication Requirements

4.1.1 Software Requirements

Minimum software requirements are:

- EOS 4.20 or newer
- TerminAttr 1.11.1 or newer

4.1.2 Connectivity Requirements

EOS devices need to be able to connect to arista.io on port 443 (apiserver.arista.io:443).

*Note:* CloudVision as-a-Service only needs port 443 to be opened to initiate a secure connection to an EOS device.

To verify proper connectivity to apiserver.arista.io:443 use the following commands:

1. Verify proper DNS resolution.

   ```bash
   switch# bash nslookup apiserver.arista.io
   ``

   *Note:* If this is unsuccessful please check your DNS server configuration. If no DNS servers are available, add the `ip name-server` configuration as follows:

   ```bash
   switch(config)# ip name-server 8.8.8.8
   ``

2. Verify connectivity to CloudVision Service using the `curl` command:

   ```bash
   switch# bash
   ```
4.1.3 **Authentication Requirements**

CloudVision as-a-Service supports OAuth 2.0 for authorization. OAuth is one of the most common methods used to pass authorization from a single sign-on (SSO) service to another cloud application. While there are many OAuth providers in the market today, CloudVision as-a-Service supports Google OAuth, OneLogin, Okta & Microsoft Azure AD.

Note that CloudVision as-a-Service is transparent to 3rd party MFA (Multi-Factor Authentication) Providers. As long as the customer is using one of the above listed OAuth Providers for identity management, CloudVision Service should be able to authorize against that OAuth provider.

Authentication options:
- Using Google OAuth or Microsoft Azure AD
- Not using Google OAuth or Microsoft Azure AD
- AAA Providers

4.1.3.1 **Using Google OAuth or Microsoft Azure AD**

Only admin email addresses are required when using Google OAuth or Azure AD as a provider. Select the Sign in with Google or Sign in with Microsoft link at: https://www.arista.io/cv

4.1.3.2 **Not using Google OAuth or Microsoft Azure AD**

If you are using Okta, OneLogin, or another OAuth Provider, the following information is required to onboard CloudVision as-a-Service:
- OAuth Endpoint
- ClientID
- ClientSecret

Refer to the respective OAuth Provider documentation for information about obtaining this information.

Your OneLogin or Okta administrator will use this information to add CloudVision to their authorized applications and adjust user permissions to allow access to the service. If you experience any OAuth errors, open an Arista TAC support request for assistance. Provide a the full URL and a screen capture of the output,

**Note:** Email IDs are case sensitive when used for CloudVision Service login. If the case is First.Last@company.com, it will need to match exactly to the CloudVision Service login.

Once the CloudVision Service account is set up, an Invitation URL will be provided by Arista to login to the CloudVision Service.

For further onboarding procedures see Onboarding Authentication Providers.

4.2 **Onboarding Procedures**

This section contains:
- Onboarding Authentication Providers
• Onboarding Devices: Token-Based Authentication
• Subscribing to CloudVision as-a-Service updates

4.2.1 Onboarding Authentication Providers

Once the CloudVision as-a-Service instance is set up, use the following procedure to add a preferred authentication provider.

To add a preferred authentication provider:

1. Navigate to **Settings** using the gear icon. Verify under the **Features** section **OAuth Providers** is toggled on.

![Figure 21: OAuth Providers](image)

2. Navigate to **Access Control** and then **Providers**. To add a new authentication provider, click the 'Add Provider' button.

![Figure 22: Add Provider](image)
3. Select a provider that your organization uses.

![Add Provider](image)

**Figure 23: Shared Provider**

Note that currently Google and Microsoft are supported as a Shared Providers. Shared Providers use an Arista-provided set of credentials so no other information is required from the customer for the onboarding.

Other providers are currently supported as non-shared providers. Additional required form fields will appear upon selecting these providers. These fields will need to be filled out with credentials specific to your account with that provider.
4. Saving the provider will send a registration request to the CloudVision Service backend along with the related information.

5. Once the authentication provider is set up, make sure to add the admin email address and verify the login process before the Invitation URL expires. To add a user account navigate to Users and then the Add User screen.

Figure 24: Non-shared Provider

Figure 25: Add User
4.2.2 Onboarding Devices: Token-Based Authentication

To onboard the devices using token-based authentication.

1. To onboard the devices navigate to Devices and then Inventory and then Add Devices and then Onboard Devices.

![Onboarding Devices](image)

Figure 26: Onboarding Devices
2. Details on how to create a token, and using that token to onboard the devices are listed under the **Onboard Devices**. Please follow the directions to create a token and onboard your devices to CloudVision Service.

**Note:** You can use the same token to onboard multiple devices. CloudVision Service will use the device serial number to identify a device.

![Generate token and onboard devices](image)

**Figure 27: Onboarding Devices**
3. Once you successfully onboard the devices you should be able to see them under the **Devices** tab.

![Device Inventory Screen](image)

**Figure 28: Device Inventory Screen**
4. Click on the wrench icon (#) to provision the device. This will take you to the device-specific page. Select the Device Overview tab and then select Provision Device to provision the device in CloudVision Service.

![CloudVision as-a-Service](image)

**Figure 29: Device Overview**

**Note:** Prior to Provision Device make sure the user account exists in the EOS device. For example:

Assuming john.smith@company.com is the email address used for OAuth authentication you need to have john.smith as a user (for Arista Demo you will need to use

```plaintext
username@arista.com):
sw(config)#username john.smith privilege 15 <nopassword/secret>
```

If you have TACACS+ configured for authentication, in order for CloudVision as-a-Service to properly provision the device, the exact user account should already exist in the TACACS+ Server.

If you have a Radius server for EOS authentication, you need to add the `--disableaaa` argument into the TerminaAttr config.

For additional information on migrating an EOS device with a TACACS+/Radius authentication to the CloudVision Service, please refer to Authentication Prerequisites.

### 4.2.3 Subscribing to CloudVision as-a-Service updates
You can monitor CloudVision Service live status through https://status.arista.io. You can also subscribe to CloudVision Service notification via email/text using Subscribe to CloudVision.

Following are informational and disruption notification examples you would get after subscribing to CloudVision Service updates:

![CloudVision Informational Notification](image1.png)

**Figure 30: Informational Notification**

### 4.3 AAA Providers

Authentication And Authorization (AAA) Providers create and log in to CloudVision through any provider. The OAuth and SAML providers are pre-configured and require additional information to create the provider.

The following sections describe procedures to configure AAA providers:

1. **Requirements**
2. **Setting up an OAuth/SAML Provider in CloudVision**
3. **Setting up CloudVision with Identity Provider**
4. **Logging in with a Provider**
5. **Adding Launchpad as a Provider**

#### 4.3.1 Requirements

Pre-requisites:

- The device must have internet access.
- To create the OAuth or SAML provider, you must be registered with and have access to the Service Provider (SP) credentials.

Perform the following steps to create and edit SAML Providers:
1. Click on the gear icon.

2. On the General Settings page, under Features, enable SAML Providers (Beta) using the toggle button.

4.3.2 Setting up an OAuth and SAML Providers in CloudVision

You can setup an OAuth or SAML provider in CloudVision through the Providers screen. To open the Providers screen, click on the gear icon and navigate to Access Control > Providers. This screen lists current registered OAuth and SAML providers in corresponding tables and provides the following functionalities:

- Adding OAuth Providers
- Adding SAML Providers
- Removing OAuth Providers
- Removing SAML Providers

Note: The Shared Provider column lists the providers where Arista has a special account for CloudVision-as-a-Service (CVaaS).

4.3.2.1 Adding OAuth Providers

Pre-requisites:

- Shared providers does not require the additional information like endpoint, client ID, and client secret. This functionality is not supported on-prem or on the custom providers.
- The link at the bottom of the Add OAuth Providers window explains how the selected provider uses OAuth and where you can find the information required by the form.
- You can use the Custom OAuth option if your provider is not listed under the Provider drop-down menu.

Perform the following steps to add an OAuth provider:
1. Click the + Add OAuth Provider tab.
   The system opens the Add OAuth Provider screen.

   ![Add OAuth Provider Screen](image1)

   Figure 32: Add OAuth Provider Screen

2. Select the required OAuth provider from the Provider drop-down menu.

   ![Add OAuth Provider Screen to Configure a Provider](image2)

   Figure 33: Add OAuth Provider Screen to Configure a Provider

3. In the Endpoint field, type the provider URL where the Client ID and Client Secret are used to authorize the client.

4. In the Client ID field, type the unique public identifier the provider assigns to the client at the time of registration.

5. In the Client Secret field, type the unique private identifier the provider assigns to the client at the time of registration.

6. Click Add.
   The system registers the new OAuth provider and lists it in the OAuth providers table.

### 4.3.2.2 Adding SAML Providers

Pre-requisites:

- The link at the bottom of the Add SAML Providers window explains how the selected provider uses SAML and where you can find the information required by the form. The only provider that does not have this information is Launchpad.
• You can use the Custom SAML option if your provider is not listed under the Provider drop-down menu.

Perform the following steps to add an SAML provider:

1. Click the + Add SAML Provider tab.
   The system opens the Add SAML Provider window.

   ![Add SAML Provider Screen](image)

   **Figure 34: Add SAML Provider Screen**

2. Select the required SAML provider from the Provider drop-down menu.

   ![Add SAML Provider Screen to Configure a Provider](image)

   **Figure 35: Add SAML Provider Screen to Configure a Provider**

3. In the Identity Provider Issuer field, type the Issuer or Entity ID.
   
   **Note:** An Issuer or Entity ID is a URL that uniquely identifies a SAML identity provider.

4. In the Identity Provider Metadata URL field, type the URL to fetch identity provider metadata.
5. In the **Email Attribute Name** field, type the attribute name for the email ID in SAML.

6. In the **Authorization Request Binding** field, select the protocol binding used for the SAML authentication request to the identity provider.

7. Click **Add**.

   The system registers the new SAML provider and lists it in the SAML providers table.

### 4.3.2.3 Removing OAuth Providers

Perform the following steps to remove an OAuth provider:

1. On the **Providers** screen, under **OAuth Providers**, select the redundant provider from the OAuth provider table.

   ![Figure 36: Removing OAuth Provider(s)](image)

   *Figure 36: Removing OAuth Provider(s)*

2. Click the **Remove OAuth Provider** button.

   The system opens the **Confirm** screen.

   ![Figure 37: Remove OAuth Provider(s) Confirm Screen](image)

   *Figure 37: Remove OAuth Provider(s) Confirm Screen*
3. Click **Remove** to confirm the removal. The system permanently removes the OAuth provider.

4.3.2.4 **Removing SAML Providers**

Perform the following steps to remove an SAML provider:

1. On the **Providers** screen, under **SAML Providers**, select the redundant provider from the SAML provider table.

![Figure 38: Removing SAML Provider(s)](image-url)
2. Click the **Remove SAML Provider** button. The system opens the **Confirm** screen.

![Figure 39: Remove SAML Provider(s) Confirm Screen](image)

3. Click **Remove** to confirm the removal. The system permanently removes the SAML provider.

### 4.3.3 Setting up CloudVision with Identity Provider

You must setup CloudVision with your Identity Provider.


### 4.3.4 Logging in with a Provider

You can use your registered providers on the CloudVision login screen to log in to cloud and on-premise CloudVision deployments. Click on the provider that has been created to log in through that provider.

**Note:** The login screen of the CloudVision with Cloud Deployments displays all supported providers regardless of which ones were created. Whereas, the login screen of the CloudVision with Cloud Deployments only displays providers that have been created.

### 4.3.5 Adding Launchpad as a Provider

You can add a launchpad using one of the following methods as per your requirement:

- Adding a Launchpad for CVaaS Deployments
- Adding a Launchpad for On-Premise Deployments
- Adding a Launchpad for CVaaS and On-Premise Deployments

### 4.3.5.1 Adding a Launchpad for CVaaS Deployments

This section applies to non-CV-WIFI customers who want to use launchpad as an identity provider.
To add launchpad as a shared provider for CVaaS deployments, request the list of users to be created in launchpad by emailing to wifi-cloudops-tickets@.

Note:

- For cv-dev and cv-play, use the following information to configure Launchpad in Cloudvision:
  
  Provider: launchpad
  Identity Provider Issuer: https://mojoonedemo.airtightnw.com/idp/shibboleth
  Identity Provider Metadata URL: https://mojoonedemo.airtightnw.com/idp/shibboleth
  Email Attribute Name: User.email
  Authorization Request Binding: HTTP-Redirect SAML protocol binding

- For cv-staging and production, use the following information to configure Launchpad in Cloudvision:
  
  Provider: launchpad
  Identity Provider Issuer: https://login.mojonetworks.com/idp/shibboleth
  Identity Provider Metadata URL: https://login.wifi.arista.com/casui/idp-metadata.xml
  Email Attribute Name: User.email
  Authorization Request Binding: HTTP-Redirect SAML protocol binding

4.3.5.2 Adding a Launchpad for On-Premise Deployments

Perform the following steps to add a launchpad for on-premise deployments:

1. Log into the tenant/cluster and get the SAML metadata from the desired cluster by going to the `CLUSTER_URL/api/v1/saml_sp_metadata` URL.
   
   Note:
   
   Email the metadata obtained in Step 1 to wifi-cloudops-tickets@ requesting to create the first user account in Launchpad and to get Launchpad configured with the SAML metadata to trust this CloudVision cluster.
   
   Note: Other accounts for this customer/org can be created by the first account created for this org by the cloudops team.

2. Get the IdentityProvider Issuer URL, Identity Provider Metadata URL and the Email attribute name from Launchpad.

4.3.5.3 Adding a Launchpad for CVaaS and On-Premise Deployments

Perform the following steps to add a launchpad for CVaaS and on-premise deployments:

1. Log in to the CVP.
2. Click on the gear icon.
3. On the General Settings screen, under Features, enable SAML Providers (Beta).
4. Navigate to Access Control > Providers and click the + Add SAML Provider button.
5. Select **Launchpad (SAML)** from the **Provider** drop-down menu.

![Add SAML Provider Screen to Configure Launchpad](image)

**Figure 40: Add SAML Provider Screen to Configure Launchpad**

6. In the **Identity Provider Issuer** field, type the Issuer or Entity ID.

   **Note:** An Issuer or Entity ID is a URL that uniquely identifies a SAML identity provider.

7. In the **Identity Provider Metadata URL** field, type the URL to fetch identity provider metadata.
8. In the **Email Attribute Name** field, type the attribute name for the email ID in SAML.
9. In the **Authorization Request Binding** field, select the protocol binding used for the SAML authentication request to the identity provider.
10. Click **Add**.
11. Under **Access Control** in the left pane, click **Users**.

   The system opens the **Users** screen.

![Users Screen](image)

**Figure 41: Users Screen**

![Add User Screen](image)

**Figure 42: Add User Screen**

13. Provide the required information in corresponding fields.

### Note:

- CloudVision usernames and EOS switch usernames must match for CloudVision to manage configuration and images on the switches.
- Type the email address which you used to sign up with Launchpad in the Email Address field.

14. Click Add.

15. Logout from the CVP.

16. Login to your account via launchpad.
Chapter 5

Getting Started (CVP)

The login screen is displayed when you first connect to the application using a web browser. The CloudVision Portal (CVP) application is accessible after the CVP service has been started on the appliance. The login screen is displayed when you first connect to the application using a web browser. JavaScript must be enabled in the browser for the web application to work.

Sections in this chapter include:
- Accessing the CVP Login Page
- Accessing the Home Page
- Omnibox
- Customizing the Home Screen and Dashboard Logo
- Accessing CloudVision Wifi
- Key CVW Operations and Directories
- Wifimanager CLI Commands

5.1 Accessing the CVP Login Page

1. To access the login page, point your browser to the CloudVision Portal (http://HOSTNAME or https://HOSTNAME). The system opens the CVP login page.

![CVP Login Page](image)

Figure 43: CVP Login Page
2. Enter login credentials in the CVP login section.

![Login Section](image)

**Figure 44: Login Section**

*Note:* The username and passwords required will depend on the authentication method and accounts previously set up. Login using the username and password created when CVP was installed. If you chose the local authentication and authorization options, login initially using `cvpadmin` for the username and password.

3. Click **Login**. The system opens the CVP home page.

## 5.2 Accessing the Home Page

All features like Devices, Events, Provisioning, Metrics, CloudTracer, Topology, Inventory, and Compliance are displayed on the home panel. A service dashboard scroller also exists to the right of the screen.

*Note:* You must have required privileges to access a switch.

![Home Page](image)

**Figure 45: Home Page**

The home page provides the following selections.

- **Devices**: View all devices across multiple topologies.
- **Events**: View multiple events on multiple devices.
- **Provisioning**: Hierarchical tree structure of the network is maintained here. All the configuration and image assignment to the network switches are made via this module.
• **Metrics**: View multiple metrics across multiple devices. Select at least one metric and one device to begin.
• **CloudTracer**: CloudTracer metrics across multiple devices or hosts. Select at least one metric and one device or host to begin.
• **Topology**: View the location of devices in individual topologies.

### 5.3 Omnibox

The omnibox performs a search and displays results from all sections in CloudVision. You must select a result for navigating to the corresponding CloudVision section.

Click the search icon at the upper-right corner of the CVP screen to access the omnibox.

![Figure 46: Omnibox](image)

**Note:**
- You can refine search results by adding more keywords to the query.
- Omnibox hotkeys are `Command # + K` in Mac; and `Ctrl + K` in Windows.

The Omnibox provides a variety of results classifying them by the section it belongs to, an associated device or section name, and sometimes a description that explains what kind of result it is. The list of potential search result modules are:

- **Devices**
  - Matching devices
  - Sections of matching devices
- **Events**
  - Matching event types
  - If a keyword matches a device hostname, it provides an option to view all events on that device
  - Matching event configurations
- **Metrics**
  - Matching metrics
  - Matching metric dashboards
- **Topology** - Matching devices in topology
- **Provisioning** - Matching Provisioning sections
- **Settings** - Matching Settings sections

**Note:** Multiple results from the same section are grouped together.

CloudVision displays matching results from **Devices** and **Topology** sections when a search is performed using the `JPE` keyword.
Note:

- If you select *athens* from the **Devices** section, CloudVision displays the Device Overview screen of *athens*.
- If you select *athens* from the **Topology** section, CloudVision displays *athens* node in the Topology view.

If a search is performed with the *athens* keyword, CloudVision displays results from **Devices**, **Event**, **Metrics**, and **Topology** sections.

### 5.4 Customizing the Home Screen and Dashboard Logo

CloudVision enables you to customize the visible options and dashboard logo shown on the home page. You change the visible options and dashboard logo by customizing them from the Settings page.

By default, no dashboard logo is selected. The image you select for the logo appears in the dashboard next to the notifications icon.
Note: Note Any image you select for either the Home screen background or dashboard logo must not exceed 200 KB for each image. In addition, the images must JPG, PNG, or GIF.

Complete the following steps to customize the visible and dashboard logo:

1. Login to CVP.
2. Click the gear icon at the upper right corner of the page.
3. Click Settings in the left menu.
4. Select the required options provided under Basic Settings, Beta Features, Cluster Management, and Troubleshooting sections.

Figure 49: Default Settings for Home Page and Dashboard Logo

5. To customize the dashboard logo, perform the following steps:
   - Click the image box next to the logo field.
   - In the Upload logo dialog, Click Select file.
   - Navigate to the desired image, and click Open. (The imported image is displayed next the Select file box.)
   - Click Upload.

5.5 Accessing CloudVision Wifi

You can access the CloudVision Wifi (CVW) service via either the CLI Access or the UI Access.

CLI Access

To log in to the wifimanager container using CLI, run the /cvpi/apps/wifimanager/bin/wifimanager.sh cli 2>/dev/null command on the primary or the secondary node.
You can now run wifimanager commands. See the Wifimanager CLI Commands for a list of wifimanager CLI commands and their descriptions.

UI Access

The URL to access the wifimanager UI is \texttt{http(s)://<CVP-IP>/wifi/wifimanager} is where CVP-IP refers to the actual CloudVision Portal (CVP) IP/domain name.

The URL to access the cognitive Wifi UI is \texttt{http(s)://<CVP-IP>/wifi/aware} where \texttt{CVP-IP} refers to either the actual CVP IP or domain name.

For example, if the IP address of CVP is 10.12.3.4, then the URL to access the wifimanager UI is \texttt{https://10.12.3.4/wifi/wifimanager} and the cognitive Wifi UI is \texttt{https://10.12.3.4/wifi/aware}.

You can access CVW UI by clicking on the WiFi tab in the CVP UI, or you can access it directly using the URLs of either wifimanager UI or Wifi UI.
When you access the UI for the first time, you need to apply the CVW service license.

Note:
- For the license file, please write an email to support-wifi@arista.com
- Use the ifconfig command on the CV root shell to get the eth0 MAC addresses of the primary and secondary CV servers (you need not access the wifimanager CLI for this). You need to include both these MAC addresses when you email support to request a license. One license is generated for the two (primary and secondary) MAC addresses.

Once you apply the license, you must log in to the CVW UI using the following default credentials:
Username: admin
Password: admin
Figure 53: CVW Login Page

You can then change the password and add other users.

Note: You can now also connect Arista access points to the server.

5.6 Key CVW Operations and Directories

CVW is containerized as a service on CV. See the Wifimanager CLI Commands section for a list of wifimanager CLI commands and their descriptions.

For details on how to configure, monitor, and troubleshoot WiFi using CloudVision WiFi, see the CloudVision WiFi User Guide on the Arista WiFi Support Portal at https://www.arista.com/support/customer-portal. You can access the portal from the WiFi - Support Portal tile on your dashboard. For details and credentials to access the portal, contact support-wifi@arista.com.

CVPI Commands for CVW

The following table lists the operations you can perform on wifimanager and the corresponding CVPI commands used.

Table 6: CVPI Commands

<table>
<thead>
<tr>
<th>Operation</th>
<th>CVPI Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>start</td>
<td>cvpi start wifimanager</td>
</tr>
<tr>
<td>stop</td>
<td>cvpi stop wifimanager</td>
</tr>
<tr>
<td>status</td>
<td>cvpi status wifimanager</td>
</tr>
<tr>
<td>restart</td>
<td>cvpi restart wifimanager</td>
</tr>
<tr>
<td>reset</td>
<td>cvpi reset wifimanager</td>
</tr>
<tr>
<td>backup</td>
<td>cvpi backup wifimanager</td>
</tr>
<tr>
<td>restore</td>
<td>cvpi restore wifimanager &lt;/path/to/backup/file&gt;</td>
</tr>
<tr>
<td>debug</td>
<td>cvpi debug wifimanager</td>
</tr>
</tbody>
</table>

Note: The backup restore fails if the user running the restore command does not have access to the path where the backup file is stored.
The restart command restarts the wifimanager service, whereas the reset command resets wifimanager settings and data to factory default values. The debug command generates a debug bundle containing log files and configuration files that can be used to troubleshoot issues.

The following table lists the operations you can perform on aware and the corresponding CVPI commands used.

**Table 7: Aware CVPI Commands**

<table>
<thead>
<tr>
<th>Operation</th>
<th>CVPI Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>start</td>
<td>cvpi start aware</td>
</tr>
<tr>
<td>stop</td>
<td>cvpi stop aware</td>
</tr>
<tr>
<td>status</td>
<td>cvpi status aware</td>
</tr>
</tbody>
</table>

### 5.6.1 Wifimanager Directories

CVW stores its data in docker volumes that reside under the `/data/wifimanager` directory on the CV. The following table lists the important wifimanager directories and the information they contain.

**Table 8: Contents of wifimanager Directories**

<table>
<thead>
<tr>
<th>Directory on CV</th>
<th>Contains</th>
</tr>
</thead>
<tbody>
<tr>
<td>/data/wifimanager/log/glog</td>
<td>Application logs</td>
</tr>
<tr>
<td>/data/wifimanager/data/conf</td>
<td>Configuration files</td>
</tr>
<tr>
<td>/data/wifimanager/data/data</td>
<td>System data files/directories</td>
</tr>
<tr>
<td>/data/wifimanager/data/instances</td>
<td>Customer data files/directories</td>
</tr>
<tr>
<td>/data/wifimanager/data/pgsql_data</td>
<td>Postgres data</td>
</tr>
<tr>
<td>/data/wifimanager/log/slog</td>
<td>System logs</td>
</tr>
<tr>
<td>/data/wifimanager/backup</td>
<td>On-demand backups</td>
</tr>
</tbody>
</table>

### 5.7 Wifimanager CLI Commands

The following table provides the list of wifimanager CLI commands and their descriptions.

**Table 9: Wifimanager CLI Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>db backup</td>
<td>Backs up the database to the specified remote server.</td>
</tr>
<tr>
<td>db clean</td>
<td>Cleans up resources without disrupting services.</td>
</tr>
<tr>
<td>db restore</td>
<td>Restores the database from a previous backup on a remote server.</td>
</tr>
<tr>
<td>db reset</td>
<td>Resets the database to factory defaults but maintains network settings.</td>
</tr>
<tr>
<td>get cert</td>
<td>Generates a self-signed certificate.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>get openconfig mode</td>
<td>Displays current OpenConfig mode.</td>
</tr>
<tr>
<td>get cors</td>
<td>Displays the current status of CORS support.</td>
</tr>
<tr>
<td>get certreq</td>
<td>Generates a Certificate Signing Request.</td>
</tr>
<tr>
<td>get db backup info</td>
<td>Displays scheduled DB backup information.</td>
</tr>
<tr>
<td>get debug</td>
<td>Creates a debug information tarball file. This file can be used for debugging.</td>
</tr>
<tr>
<td>get debug verbose</td>
<td>Creates a basic debug information tarball.</td>
</tr>
<tr>
<td>get debug ondemand</td>
<td>Displays the debug information.</td>
</tr>
<tr>
<td>get device upgrade bundles</td>
<td>Displays information about device upgrade bundles available in the local repository.</td>
</tr>
<tr>
<td>get device repo config</td>
<td>Displays configuration (Mode and Hostnames) for repositories that store upgrade bundles and device capability information.</td>
</tr>
<tr>
<td>get idle timeout</td>
<td>Displays the current idle timeout value. A value of 0 indicates no timeout.</td>
</tr>
<tr>
<td>get integrity status</td>
<td>Checks the integrity of critical server components.</td>
</tr>
<tr>
<td>get ha</td>
<td>Displays High Availability (HA) Pair configuration and service status.</td>
</tr>
<tr>
<td>get lldp</td>
<td>Displays the LLDP configuration.</td>
</tr>
<tr>
<td>get remote logging</td>
<td>Displays the remote logging configuration.</td>
</tr>
<tr>
<td>get log config</td>
<td>Displays the logger configuration.</td>
</tr>
<tr>
<td>get log level gui</td>
<td>Displays log levels of GUI modules.</td>
</tr>
<tr>
<td>get log level aruba</td>
<td>Displays the log level of Aruba Mobility Controller Adapter module.</td>
</tr>
<tr>
<td>get log level wlc</td>
<td>Displays the log level of the Cisco WLC Adapter module.</td>
</tr>
<tr>
<td>get log level msmcontroller</td>
<td>Displays the log level of HP MSM Controller Integration.</td>
</tr>
<tr>
<td>get msmcontroller cert</td>
<td>Generates a self-signed certificate for HP Adapter.</td>
</tr>
<tr>
<td>get msmcontroller certreq</td>
<td>Generates a Certificate Signing Request for HP Adapter.</td>
</tr>
<tr>
<td>get access address</td>
<td>Shows access IP Address/Hostname of this server.</td>
</tr>
<tr>
<td>get server config</td>
<td>Displays complete server configuration.</td>
</tr>
<tr>
<td>get server cert</td>
<td>Uploads server certificate to a remote host.</td>
</tr>
<tr>
<td>get server check</td>
<td>Runs a server consistency check and displays results. If any fatal item fails, a failure result is recorded.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>get server tag</td>
<td>Displays the custom tag set by the user.</td>
</tr>
<tr>
<td>get serverid</td>
<td>Displays the server ID.</td>
</tr>
<tr>
<td>get sensor debug logs</td>
<td>Uploads AP debug logs to the specified upload URL.</td>
</tr>
<tr>
<td>get sensor list</td>
<td>Displays the list of APs.</td>
</tr>
<tr>
<td>get sensor reset button</td>
<td>Displays the state of the AP's pinhole reset button.</td>
</tr>
<tr>
<td>get status</td>
<td>Displays the status of server processes.</td>
</tr>
<tr>
<td>get ssh</td>
<td>Displays the SSH server status.</td>
</tr>
<tr>
<td>get version</td>
<td>Displays the version and build of all the server components.</td>
</tr>
<tr>
<td>get packet capture</td>
<td>Captures packets on Public and HA/Management network interface(s).</td>
</tr>
<tr>
<td>set scan config</td>
<td>Modify AP background scanning parameters.</td>
</tr>
<tr>
<td>set openconfig mode</td>
<td>Enable/disable OpenConfig mode.</td>
</tr>
<tr>
<td>set cert</td>
<td>Installs a signed SSL certificate.</td>
</tr>
<tr>
<td>set cors</td>
<td>Enables or disables CORS support.</td>
</tr>
<tr>
<td>set dbserver</td>
<td>Starts/stops database server.</td>
</tr>
<tr>
<td>set db backup info</td>
<td>Sets scheduled DB backup information.</td>
</tr>
<tr>
<td>set device capability</td>
<td>Updates the device capability information.</td>
</tr>
<tr>
<td>set device upgrade bundles</td>
<td>Upload/delete device upgrade bundles in the local repository.</td>
</tr>
<tr>
<td>set device repo config</td>
<td>Sets configuration (Mode and Hostnames) for repositories that store upgrade bundles and device capability information.</td>
</tr>
<tr>
<td>set erase</td>
<td>Configures the backspace key.</td>
</tr>
<tr>
<td>set ha dead time</td>
<td>Changes the Dead Time of High Availability (HA) service.</td>
</tr>
<tr>
<td>set ha link timeout</td>
<td>Sets the timeout in seconds to signal Data Sync Link failure.</td>
</tr>
<tr>
<td>set idle timeout &lt;timeout-in-minutes&gt;</td>
<td>Sets the idle timeout for the command shell. A value of 0 disables the idle timeout.</td>
</tr>
<tr>
<td>set lldp</td>
<td>Sets LLDP configuration.</td>
</tr>
<tr>
<td>set remote logging</td>
<td>Sets remote logging configuration.</td>
</tr>
<tr>
<td>set log config</td>
<td>Sets the configuration of the logger.</td>
</tr>
<tr>
<td>set log level gui</td>
<td>Sets log levels of GUI modules.</td>
</tr>
<tr>
<td>set log level aruba</td>
<td>Sets the log level of Aruba Mobility Controller Adapter Module.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>set log level wlc</td>
<td>Sets log level of Cisco WLC Adapter Module.</td>
</tr>
<tr>
<td>set log level msmcontroller</td>
<td>Sets log level of HP MSM Controller Integration.</td>
</tr>
<tr>
<td>set msmcontroller cert</td>
<td>Installs a signed SSL certificate for HP Adapter.</td>
</tr>
<tr>
<td>set loginid case sensitivity</td>
<td>Toggles login ID case sensitivity.</td>
</tr>
<tr>
<td>set server</td>
<td>Starts/stops application server.</td>
</tr>
<tr>
<td>set server discovery</td>
<td>Changes server discovery settings on given AP(s).</td>
</tr>
<tr>
<td>set server tag</td>
<td>Configure a custom tag for files generated by this server.</td>
</tr>
<tr>
<td>set access address</td>
<td>Sets access IP Address/Hostname of the server.</td>
</tr>
<tr>
<td>set serverid</td>
<td>Sets server ID.</td>
</tr>
<tr>
<td>set ssh</td>
<td>Starts/stops SSH access to the server.</td>
</tr>
<tr>
<td>set communication passphrase</td>
<td>Sets the communication passphrase used for AP-server authentication and to encrypt the communication between APs and the server.</td>
</tr>
<tr>
<td>set communication key</td>
<td>Sets the communication key used for AP-server authentication and to encrypt the communication between APs and the server.</td>
</tr>
<tr>
<td>set communication key default</td>
<td>Resets the communication key used for AP-server authentication and to encrypt the communication between APs and the server.</td>
</tr>
<tr>
<td>set sensor legacy authentication</td>
<td>This allows/disallows APs running on versions lower than 6.2 to connect to the server.</td>
</tr>
<tr>
<td>set sensor reset button</td>
<td>Sets the state of the AP's pinhole reset button (select AP models only).</td>
</tr>
<tr>
<td>set smart device oui</td>
<td>Add, remove MAC OUI's for specific smart device type IDs.</td>
</tr>
<tr>
<td>set webserver</td>
<td>Starts/stops web server.</td>
</tr>
<tr>
<td>set wlc mapper</td>
<td>Manage Cisco WLC Custom Mapper file.</td>
</tr>
<tr>
<td>exit</td>
<td>Exits the config shell session.</td>
</tr>
<tr>
<td>ping &lt;Hostname/IP Address&gt;</td>
<td>Ping a host.</td>
</tr>
<tr>
<td>reset locked gui</td>
<td>Unlocks Graphical User Interface (GUI) account for the &quot;admin&quot; user.</td>
</tr>
<tr>
<td>reset password gui</td>
<td>Sets Graphical User Interface (GUI) password for the &quot;admin&quot; user to factory default value.</td>
</tr>
<tr>
<td>upload db backup</td>
<td>Uploads successful DB backup(s) to an external server.</td>
</tr>
<tr>
<td>application signature update</td>
<td>Updates app visibility signature.</td>
</tr>
</tbody>
</table>
Chapter 6

General Customizations

CloudVision Portal (CVP) enables you to customize the grid columns of CVP graphical user interface (GUI) pages. You can customize the grid columns of all CVP GUI grids.

CVP also enables you to easily paginate (navigate) through the pages of the grids of the GUI. The pagination controls are available in all grids.

- Column Customization
- Pagination Controls

6.1 Column Customization

CloudVision Portal (CVP) enables you to customize the columns of the grids of CVP graphical user interface (GUI) pages. You can customize columns of any grid of the CVP GUI.

You use the Columns Settings dialog to customize the columns of the active grid. You can open the Columns Settings dialog by clicking the column customization icon, which is available of every page of the GUI.

Figure 54: Configlet Management page

Complete these steps to customize grid columns.

1. Go to a page that has the grid you want to customize.
2. Click the column customization icon.

3. Use the arrow icons to rearrange the columns of the grid as needed.

4. Once you are done rearranging the grid columns, click OK to save the changes.

6.2 Pagination Controls

The pagination controls you use to navigate through the pages of grids are available for each grid. The controls enable you to:

- Go to the previous page of the grid
- Go to the next page of the grid
- Go to the first page of the grid
- Go to the last page of the grid
- Go to directly to a specific page
Chapter 7

Device Management

CloudVision Portal (CVP) provides a powerful, event-driven, streaming analytics platform that enables you to monitor the state of all devices currently managed by CVP.

By configuring devices to stream device-state data to CVP, you can manage all of the devices in your current inventory of devices to gain valuable insights into the state of your devices, including real-time updates about changes in device state.

The device inventory is comprised of all devices that you have imported into CVP. After a device is imported into CVP, it can be configured and monitored using the various CVP modules.

- Requirements
- Limitations
- Features
- Telemetry Platform Components
- Supplementary Services: Splunk
- Architecture
- Accessing the Telemetry Browser Screen
- Viewing Devices
- Viewing Device Details
- Viewing Connected Endpoints
- Connectivity Monitor with CloudTracer
- Managing Tags
- Accessing Dashboards
- Topology View
- Accessing Events
- Events App (Beta)
- Troubleshooting

7.1 Requirements

Make sure you review the software and hardware requirements for deploying and using the Telemetry platform before you begin deploying the platform.

System Requirements

Note: If you upgraded from a previous version of CVP, you must verify that all of the CVP node VMs on which you want to enable Telemetry have the required resources to use Telemetry. See Resource Checks for details on how to check CVP node VM resources and perform any modifications needed to increase the current CVP node VM resources.

7.2 Limitations

The following table lists the current limitations of the Telemetry platform. Review the limitations to ensure you do not inadvertently attempt configurations that exceed the limitations.
Table 10: CVP Telemetry Platform Limitations

<table>
<thead>
<tr>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of devices</td>
</tr>
<tr>
<td>This represents the total number of devices currently configured to stream Telemetry data.</td>
</tr>
<tr>
<td>Device-state data</td>
</tr>
<tr>
<td>Streaming of LANZ data is not enabled by default. You must enable it on devices.</td>
</tr>
<tr>
<td>Secret configuration</td>
</tr>
<tr>
<td>If &quot;enable secret&quot; is configured, the secret must be the same as the Cloudvision user's password.</td>
</tr>
</tbody>
</table>

7.3 Features

The list the current supported and unsupported Telemetry platform features are provided in the following topics:

- Supported Features
- Unsupported Features

7.3.1 Supported Features

The CVP Telemetry Supported Features table lists the supported features. Review the supported features to ensure you are aware of the features available to you to monitor devices using Telemetry data.

Table 11: CVP Telemetry Supported Features

<table>
<thead>
<tr>
<th>Supported Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-time monitoring of devices</td>
</tr>
<tr>
<td>The Telemetry platform provides interfaces for viewing real-time updates about changes in device state as well as events. You can also view trends in device-state metrics and queries of historical device-state data.</td>
</tr>
<tr>
<td>Instant state change updates</td>
</tr>
<tr>
<td>Changes in the state of a device are instantly streamed to CVP.</td>
</tr>
<tr>
<td>Full state change data</td>
</tr>
<tr>
<td>All changes in device-state are captured and streamed to CVP for viewing. Types of device-state include:</td>
</tr>
<tr>
<td>• All SysDB state (except state under /Sysdb/cell/*).</td>
</tr>
<tr>
<td>• All SMASH tables.</td>
</tr>
<tr>
<td>• Process and kernel data (for example, CPU and memory usage).</td>
</tr>
<tr>
<td>• System log messages</td>
</tr>
<tr>
<td>Analytics engine</td>
</tr>
<tr>
<td>The Telemetry platform provides a robust analytics engine that aggregates the streamed device-state data across devices, monitors device state, and generates events to indicate issues. It also normalizes data so it is easier for other applications to use.</td>
</tr>
</tbody>
</table>
| **Telemetry events** | Device-state and system environment event types are streamed to CVP:
- Informational (updates about changes in device state).
- Warning (for example, unsupported EOS version on a device)
- Errors (data discards or input errors on interfaces, and more).
- Critical (system environment issues such as overheating). |
|----------------------|-------------------------------------------------|
| **High performance database** | The Telemetry platform utilizes a high performance Hbase database to store device-state data, including events. Data is stored in compressed format without a loss of resolution.
- The data storage capacity is approximately:
  - 43200 records worth of raw data per path
  - 5 days of 10 second aggregated data
  - 4 weeks of 60 second aggregated data
  - 3 months worth of 15 minute aggregated data |
| **Disk space protection** | To prevent telemetry data from consuming too much disk space in the CVP cluster, the Telemetry platform automatically blocks the ingest port for the entire cluster if disk usage exceeds 85% on any node of the cluster.
Once the ingest port is blocked, it remains blocked until disk usage drops below 80% on all nodes in the cluster. |
| **Data management** | To ensure that the most relevant data is given priority, the Telemetry platform provides automated data management, including:
- Maximum time limit on stored device-state data (1 month).
- Current and the most recent device-state updates are always stored (given priority over older state updates).
Periodic clean-up jobs are executed weekly (Saturday at 11:00 P.M.). Old device-state data is purged. |
| **Command support** | Several commands are provided for:
- Checking status of the Telemetry components.
- Enabling and disabling of Telemetry platform components.
- Starting and stopping Telemetry components.
- Viewing the debug log for Telemetry components.
- Troubleshooting the Telemetry components, including checking to see that logs are being created for the component.
- To display granular information on disk space usage of telemetry data and delete telemetry data selectively. |

### 7.3.2 Unsupported Features

The CVP Telemetry Unsupported Features table lists the unsupported features. Review the limitations to ensure you do not inadvertently attempt to configure or use unsupported Telemetry features.
Table 12: CVP Telemetry Unsupported Features

<table>
<thead>
<tr>
<th>Unsupported Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Streamed device-state data</td>
</tr>
</tbody>
</table>

7.4 Telemetry Platform Components

Arista’s streaming Telemetry platform consists of a set of components, all of which are essential to the proper operation of the platform.

The components of the Telemetry platform are:

- NetDB State Streaming Component
- CloudVision Analytics Engine Component
- REST and Websocket based APIs are available to programmatically get data from the CloudVision Analytics Engine. Contact your Arista Sales Engineer for more information.

7.4.1 NetDB State Streaming Component

The NetDB State Streaming component is an agent that runs on Arista switches. It is the Telemetry platform component that streams device-state data from devices to the CloudVision Analytics Engine, which is the back-end component of platform.

7.4.2 CloudVision Analytics Engine Component

The CloudVision Analytics Engine is the back-end component of the Telemetry platform. It is a set of processes that run on CVP. Collectively, the processes perform the following operations:

- Receives all of the device-state data streamed by the NetDB State Streaming component from devices that have been configured to stream device-state data.
- Runs automated data analysis on the device-state data received from the NetDB State Streaming component. The analytics processes aggregate the device-state data across devices, monitor device state, and generate events if something goes wrong. The processes also normalize data so it is easier for other applications to use.
- Stores all of the streamed device-state data received from the NetDB State Streaming component, and then makes the stored data available in CloudVision.
- Provides CloudVision Analytics Engine Viewer, which is referred to as the Aeris Browser. You use it to directly view device-state data received from devices that have been configured to stream device-state data. The Aeris Browser enables you to view raw device-state data.
- REST and Websocket based APIs are available to programmatically get data from the CloudVision Analytics Engine. Contact your Arista Sales Engineer for more information.

7.5 Supplementary Services: Splunk

For more information on the requirements for CVP to manage Splunk extensions on EOS devices, go to https://www.arista.com/en/support/software-download and download the PDF from Extensions > Splunk > AristaTelemetry.pdf.

Related topics:
- Requirement
- Installation
- Quick Start
7.5.1 Requirement

EOS 4.15.2 or later is required.

7.5.2 Installation

You can access the Splunk Telemetry App directly from CVP by completing the following steps. From your browser.

1. Copy the RPM to and install it on the switch.

   show extensions
   Name Version/Release Status RPMs

2. Install the Splunk Universal Forwarder RPM on EOS.

   copy <source>/splunkforwarder-6.1.4-233537.i386.rpm extension:
   extension splunkforwarder-6.1.4-233537.i386.rpm

3. Install the AristaAppForSplunk on EOS.

   copy <source>/AristaAppForSplunk-1.3.2.swix extension:
   extension AristaAppForSplunk-1.3.2.swix

   Note: Extensions must be installed on all supervisors.

   Restart the SuperServer agent.

   (config)# agent SuperServer shutdown
   (config-mgmt-api-http-cmds)# no agent SuperServer shutdown

4. Verify the extensions are loaded.

   show extensions
   Name Version/Release Status RPMs
   ------------------------------------------ -------------------------
   ------ ----
   AristaAppForSplunk-<version>.swix <version>/1.fc14 A, I 3
   splunkforwarder-6.1.4-233537.i386.rpm 6.1.4/233537 A, I 1
   EosSdk-1.7.0-4.15.2F.i686.rpm 1.7.0/2692966.gaevanseoss A, I 1
   A: available | NA: not available | I: installed | NI: not installed |
   F: f

7.5.3 Quick Start

1. Use the configuration to enable forwarding to the Splunk indexer. This assumes that a username/password and eAPI have been configured for the AristaAppForSplunk extension previously.

   daemon SplunkForwarder
   exec /usr/bin/SplunkAgent
   no shutdown

2. Configure and turn on the desired indexes for data collection. The credentials must match 'username <name> secret <passphrase>' configured on the switch.

   option eapi_username value <username>
   option eapi_password value 7 <encrypted-password>
   option eapi_protocol value https
3. Turn on desired indexes for data collection.

```plaintext
option index-inventory value on
option index-interface-counters value on
option index-lanz value on
option index-topology value on
option index-syslog value on
option index-data value <index-name>
```


```plaintext
option splunk-server value <Server-IP:Port>
```

5. Start Splunk data forwarding.

```plaintext
option shutdown value off
```

7.6 Architecture

Telemetry Platform Architecture shows the architecture of the Telemetry platform, including all of the platform components and the data path of the streamed device-state data.

![Telemetry Platform Architecture](image)

Figure 57: Telemetry Platform Architecture

7.7 Accessing the Telemetry Browser Screen

You can access the CloudVision Telemetry Browser screen directly from CVP by completing the following steps. Open your browser.

1. Point your browser to the CVP IP address or hostname.
2. Login to CVP.
   The CVP Home screen appears.

   ![Figure 58: CVP Home Screen](image)

3. Click the gear icon at the upper right corner of the screen.

   ![Figure 59: Gear Icon](image)

4. Click Telemetry Browser in the left pane.
   The system opens the Telemetry Browser screen that allows exploring the raw data stored in CVP telemetry.

   ![Figure 60: CloudVision Telemetry Browser Screen](image)
7.8 Viewing Devices

You can quickly view information about devices that are currently configured to stream device-state data to CVP. Starting with 2018.2.0, the inventory management screen is available under Devices in the CVP user interface.

Related topics:
- Tiles View
- Tabular View

7.8.1 Tiles View

The tiles view allows search by device hostname, serial number, or EOS version. The screen updates to show all of the devices currently configured to stream device-state data to CVP. For each device, the name and the version of the EOS image are shown on the Devices screen.

![Figure 61: Viewing Devices (View Showing all Devices)](image)

7.8.2 Tabular View

The tabular view lists device status, model, software, TerminAttr agent, IP address, MAC address, and serial number. You can search for devices based on device hostname, serial number, or EOS version.

![Figure 62: Device Inventory](image)
7.9 Viewing Device Details

From the Inventory screen, you can quickly drill down to view details about a particular device by clicking the device icon. In tabular view, click the device name to view the corresponding device details.

The screen refreshes to show the device-state data streamed from the device to CVP.

Figure 63: Viewing Devices Details (Single Device)

Device details include the information on overview, system, compliance, environment, switching, routing, and interfaces.

Related topics:
- Device Overview
- System Information
- Compliance
- Environment Details
- Switching Information
- Routing Information
- Status of Interfaces
7.9.1 Device Overview

The Device Overview section provides an overview of system details, telemetry status, and interface counts. Click More to reach corresponding sections for detailed information.

Figure 64: Device Overview Section

The Historical Comparison sub-section provides the information on EOS version, 5-minute CPU load average, MLAG status, IPv4 attached routes, IPv4 learned routes, configured BGP, IPv6 attached routes, IPv6 learned routes, and MAC addresses learned.

The system displays only Device Overview and System information for third-party devices.
7.9.2 System Information

The System section provides an overview of device details, telemetry status, and PTP status.
Figure 66: System Section

Sub-sections provide information on processes, storage, log messages, hardware capacity, running config, and snapshots.

7.9.3 Compliance

The Compliance section provides information on vulnerability to known bugs.

Figure 67: Compliance Section

7.9.4 Environment Details

The Environment section provides statistics on temperature, fan speeds, and output power.
7.9.5  Switching Information

The Switching section provides the count of VLANs in which MAC address learning is enabled, count of total VLANs, count of configured VLANs, and detailed information on configured VLANs.

Sub-sections provide switching data like ARP table, NDP table, bridging capability, MAC address table, MLAG, and VXLAN.

7.9.6  Routing Information

The Routing section provides statistics on IPV4 route count by type, IPv6 route count by type, and routing statistics by VRF.
Sub-sections provide routing data like IPv4 and IPv6 routing tables, routing table changes, multicast data like sparse mode PIM and static, and BGP information.

### 7.9.7 802.1X Metrics

802.1X information shows which endpoints have authenticated, are undergoing authentication, or have failed to authenticate to the network. This information is available to view primarily from the 802.1X page in the Devices application.

### Accessing 802.1X Metrics

To access 802.1X Metrics From the Inventory screen in the Devices tab, select a device. In the scrolling menu on the left side of the page, select 801.X. The 801.X Metrics page is displayed.
The graphs display the total number of interfaces and the status of each. The table lists all of the endpoints with additional information. The columns show the following:

- **Identity**: the MAC address of the endpoint. The username, if provided, is displayed in parenthesis.
- **IP Address**: the IP address of the endpoint.
- **Interface**: which interface the endpoint is on. Selecting the interface will display a table showing all of the endpoints on that specific interface.
- **Host Mode**: the host mode of the endpoint (Single-Host, Multi-Host, Multi-Host Authenticated) with an optional Mac-Based VLAN Assignment. Place the cursor over Mac-Based VLAN Assignment to display the full name.
- **Auth Status**: the authentication status of the endpoint.
- **Auth Mode**: how the endpoint is authenticated.
- **VLAN**: the VLAN the endpoint is on.
- **VLAN Type**: the type of VLAN being used.

### 802.1X Dashboard View

802.1X metrics is also available from the Dashboard View. Refer to Dashboards for more information about creating a dashboard.

![802.1X Dashboard View](image)

**Figure 72: 802.1X Dashboard View**

### 7.9.8 Viewing Traffic Flows

CloudVision lets you analyze the network traffic routed through a single device or through all devices that have flow tracking configured.

**Note**: Traffic flows return tunneled flows when the inner packet headers matches the user's query.

You can drill down into the details of global and device specific network flow activities using bar charts, stacked time series graphs, and tables of usage statistics. See Accessing the Global Traffic Flows Screen and Accessing the Device Specific Traffic Flows Screen.

**Note**: You can drill down the details of device specific network flow activities using heatmaps also.
To view the data on traffic flows, you must enable traffic flow tracking in devices to get data. See Enabling Traffic Flow Tracking.

### 7.9.8.1 Enabling Traffic Flow Tracking

Enabling flow tracking on a device allows CloudVision to provide a detailed breakdown of the forwarded network traffic. Traffic flow tracking is enabled through either of the following methods:

- Enable sFlow Sampling on a Device
- Enable Hardware Based IPFIX Flow Tracking

#### Enable sFlow Sampling on a Device

Arista switches provide a single sFlow agent instance that samples ingress traffic from all Ethernet and port channel interfaces.

Run the following commands to enable sFlow sampling on a device:

```
switch(config)#sflow sample <sampling rate>
switch(config)#sflow polling-interval <polling interval>
switch(config)#sflow destination 127.0.0.1
switch(config)#sflow source-interface <source interface>
switch(config)#sflow run
```

sFlow monitors a random sample of packets at the configured sampling rate. Reported bandwidth and packet measurements are scaled up using the sampling rate to provide estimates of actual bandwidth usage and packet counts.

#### Enable Hardware Based IPFIX Flow Tracking

Arista switches also allow exporting flow information using the IPFIX format.

Run the following commands to enable hardware based IPFIX flow tracking:

```
switch(config)#flow tracking hardware
switch(config)#!
switch(config)#tracker <tracker name>
switch(config)#record export on inactive timeout <inactive timeout>
switch(config)#record export on interval <interval>
switch(config)#record format ipfix standard timestamps counters
switch(config)#!
switch(config)#exporter <exporter name>
switch(config)#collector <loopback interface ip>
switch(config)#local interface <loopback interface>
switch(config)#template interval <interval>
switch(config)#no shutdown
switch(config)#exit
switch(config)#interface <interface>
switch(config)#flow tracker hardware <tracker name>
switch(config)#no shutdown
```

### 7.9.8.2 Accessing the Global Traffic Flows Screen

To view the global traffic flows screen, navigate to Devices > Traffic Flows on the CloudVision portal. This screen displays information about traffic flows captured by all devices on the network with flow monitoring enabled. See the figure below.
Device Management

Figure 73: Global Traffic Flows Screen

**Note:** This screen may present multiple values reported by different devices for the same flow or flow category.

Use the following search filters for customised presentation of the traffic flows data:

- **Host filters**
  - **Source Hosts**
    - **Show** autocomplete field - Provide hostnames, IP addresses, or subnets in CIDR notation of the source host that needs to be displayed
    - **Hide** autocomplete field - Provide hostnames, IP addresses, or subnets in CIDR notation of the source host that needs to be concealed
  - **Destination Hosts**
    - **Show** autocomplete field - Provide hostnames, IP addresses, or subnets in CIDR notation of the destination host that needs to be displayed
    - **Hide** autocomplete field - Provide hostnames, IP addresses, or subnets in CIDR notation of the destination host that needs to be concealed
  - **Bidirectional** checkbox - Select the checkbox to view the traffic flows between specified hosts.
    - **Note:** When you select the **Bidirectional** checkbox, the **Source Hosts** and **Destination Hosts** fields change to **Hosts** and **To/From Hosts**.

- **Port filters**
  - **Source Ports** autocomplete field - Provide port numbers or service names of the source port
  - **Destination Ports** autocomplete field - Provide port numbers or service names of the destination port
  - **Show/Hide** dropdown - Select either **Show** or **Hide** to view or conceal the traffic flow data of specified source and destination ports respectively.
  - **Bidirectional** checkbox - Select the checkbox to view the traffic flows between specified ports.
    - **Note:** When you select the **Bidirectional** checkbox, the **Source Ports** and **Destination Ports** fields change to **Ports** and **To/From Ports**.

- **Protocol filter** - Provide IP protocols of the required traffic flow data in the autocomplete field.
  
  Select either **Show** or **Hide** to view or conceal the traffic flow data of specified protocols respectively.
• More filters
  • **Locality** - Select Public and Private checkboxes to view traffic flows of corresponding networks
  • **Fragmentation** checkbox - Selecting the checkbox displays only flows with fragmented packets
  • **Clear all filters** - Clears all specified filters
  • **Top** dropdown menu - As per your selection, the top n items are displayed for each break down.
  • **by** dropdown menu - Select the required method to measure traffic.

The global traffic flows dashboard provides the following display types for analyzing the flow data in different ways:

  • **Charts View**
  • **Summary Table View**
  • **Flow Records View**

**Note:**

- Click the **View in Topology** link to see the data from the perspective of the topology flows view.
- The refresh icon provides countdown in seconds for refreshing the traffic flow data. The data in live mode gets updated every 30 seconds.

**Charts View**

The **Charts** display option presents the summary of global traffic flows in charts. The traffic flow data is arranged based on the breakdown selected from the dropdown list. See the figure below.

![Figure 74: Global Traffic Flow Summary in Charts](image)

Bar charts represent the device specific traffic flows over the selected time period. The bar length represents the traffic flow of a device with highest usage.

**Note:**

- Click on a bar in the bar chart in the stacked graph to set the clicked-on item as a filter wherever it is possible. For example, hosts or ports of source and destination.
- Hover the cursor on the dot in a bar to find the observing device.

**Summary Table View**

The **Summary Table** display option presents the summary of global traffic flows in a tabular format. See the figure below.
Device Management

Figure 75: Global Traffic Flow Summary in Table

The traffic flow data is grouped based on the selected breakdowns. If multiple options are selected in the Group By field, the table displays a summary of usage statistics that is broken down according to the selected criteria. The summary can be sorted by bytes, packets, or flows in descending order.

Note: Click on a device name to view the traffic flows for the respective device.

Flow Records View

The Flow Records display option presents the record of all traffic flows in a tabular format. See the figure below.

Figure 76: Global Traffic Flow Record

Note: Click on a device name to view the traffic flows for the respective device.

7.9.8.3 Accessing the Device Specific Traffic Flows Screen

On the CloudVision portal, navigate to Devices > Inventory > Device_Name > Traffic Flows to view the Traffic Flows screen. See the figure below.
Inband Telemetry

This screen displays the summary of flows, bandwidth, packets, active hosts, and sampling rate. Provide the following details to view custom information of traffic flows:

- **Inband Telemetry Data**
  - Flow tracking (sFlow or IPFIX)
  - Inband telemetry
- **Host filters**
  - **Source Hosts**
    - Show autocomplete field - Provide hostnames, IP addresses, or subnets in CIDR notation of the source host that needs to be displayed
    - Hide autocomplete field - Provide hostnames, IP addresses, or subnets in CIDR notation of the source host that needs to be concealed
  - **Destination Hosts**
    - Show autocomplete field - Provide hostnames, IP addresses, or subnets in CIDR notation of the destination host that needs to be displayed
    - Hide autocomplete field - Provide hostnames, IP addresses, or subnets in CIDR notation of the destination host that needs to be concealed
- **Port filters**
  - **Source Ports** autocomplete field - Provide port numbers or service names of the source port
  - **Destination Ports** autocomplete field - Provide port numbers or service names of the destination port
  - **Show/Hide** dropdown - Select either Show or Hide to view or conceal the traffic flow data of specified source and destination ports respectively.
- **Protocol filter** - Provide IP protocols of the required traffic flow data in the autocomplete field.
  Select either **Show** or **Hide** to view or conceal the traffic flow data of specified protocols respectively
- **Interface filters**
  - **Show** autocomplete field - Select the interfaces of which the traffic flow needs to be displayed
  - **Hide** autocomplete field - Select the interfaces of which the traffic flow needs to be concealed
- **More filters**
  - **Locality** - Select Public and Private checkboxes to view traffic flows of corresponding networks
  - **Fragmentation** checkbox - Selecting the checkbox displays only flows with fragmented packets
  - **Clear all filters** - Clears all specified filters
- **Top** dropdown menu - As per your selection, the top n items are displayed for each break down.
- **by** dropdown menu - Select the required method to measure traffic.

The device specific traffic flows dashboard provides the following display types for analyzing the flow data in different ways:

- Figure 79: Device Specific Traffic Flow Summary in Charts
- Heatmap View
- Summary Table View
- Flow Records View

**Note:**

- Click the **View in Topology** link to see the data from the perspective of the topology flows view.
- The refresh icon provides countdown in seconds for refreshing the traffic flow data. The data in live mode gets updated every 30 seconds.

**Charts View**

The **Charts** display option presents the summary of device specific traffic flows in charts. The traffic flow data is arranged based on the breakdown selected from the dropdown list. See the figure below.

![Figure 78: Device Specific Traffic Flow Summary in Charts](image)

The following information is provided for each break down:

- Bar charts that display the total usage over the time period for items

  **Note:** Clicking on a bar in the bar chart or a time series in the stacked graph sets the clicked-on item as a filter wherever it is possible. For example, hosts or ports of source and destination.

- Stacked time series graphs that provide the following information:
  - The rate of usage vs. time

    **Note:** This information is provided only when the Sort By option is either Bandwidth (bytes) or Packets.
  - The number of flows active vs. time

    **Note:** This information is provided only when the Sort By option is Flow Count.
Charts View

The **Charts** display option presents the summary of device specific traffic flows in charts. The traffic flow data is arranged based on the breakdown selected from the dropdown list. See the figure below.

![Figure 79: Device Specific Traffic Flow Summary in Charts](image)

The following information is provided for each breakdown:

- Bar charts that display the total usage over the time period for items

  ![Note: Clicking on a bar in the bar chart or a time series in the stacked graph sets the clicked-on item as a filter wherever it is possible. For example, hosts or ports of source and destination.](image)

- Stacked time series graphs that provide the following information:
  - The rate of usage vs. time

  ![Note: This information is provided only when the Sort By option is either Bandwidth (bytes) or Packets.](image)
  - The number of flows active vs. time

  ![Note: This information is provided only when the Sort By option is Flow Count.](image)

Heatmap View

The **Heatmap** display option presents the summary of device specific traffic flows in a heatmap. See the figure below.
Device Management

Figure 80: Device Specific Traffic Flow Summary in Heatmap

The heatmap plots two breakdowns against each other. For example, the user selects top 20 source hosts vs. top 20 destination hosts. The system displays the top 20 destination hosts that communicated with any of those top 20 source hosts.

Each pairing of source host and destination host is shown as a cell in the grid. Cells are displayed in various shades of green based on their usage. The higher the usage, the darker the green shade.

Note: The system displays an empty cell if there is no usage.

Summary Table View

The Summary Table display option presents the summary of device specific traffic flows in a table. See the figure below.

Figure 81: Device Specific Traffic Flow Summary in Table

The traffic flow data is grouped based on the selected breakdowns. If multiple options are selected in the Group By field, the table displays a summary of usage statistics that is broken down according to the selected criteria. The summary can be sorted by bytes, packets, or flows in descending order.
Flow Records View

The Flow Records display option presents the record of device specific traffic flows in a tabular format. See the figure below.

When viewing individual flow records, the path of a flow, complete with ingress and egress interfaces, TTLs and latencies for each hop, can be inspected using the Hops column.

![Flow Records View](image)

**Figure 82: Flow Records View**

*Note:* Filters and fields related to packet fragmentation, tunnelling, and user identity are not available for inband telemetry data.

7.9.9 Address Search

Address Search supports searching MAC addresses, IP addresses of all formats, device IDs, and hostnames of inventory devices.

The Address Search page can be found in the primary Devices view on the sidebar. Navigating to it will open the Address Search page.

![Address Search Page](image)

**Figure 83: Address Search Page**

Enter the search information and press Enter to view the search results.
There are two tabs available in the search results view.

- Network Location is the default view. This view displays detailed information from the MAC, ARP, and LLDP Tables.
- Flow Visibility view displays the traffic that is being sent and received by all IP addresses associated with the search result.

### 7.9.10 Status of Interfaces

The Interfaces section provides status of Ethernet interfaces, VLAN interfaces, IP interfaces, and port channels.
Sub-sections provide detailed information on Ethernet interfaces, routed ports, port channels, traffic counters, LLDP neighbors, and Power Over Ethernet.

### 7.9.10.1 Power Over Ethernet

Power Over Ethernet (PoE) is a technology for delivering electrical power along with network data over physical Ethernet connections. Some benefits of PoE are provided below:

- Reduces the need of extension cables and additional outlets
- Provides a reliable power source on difficult terrain
- Prevents data transmission hiccups
- Substantial reductions in space usage, cost, and time

In CloudVision, the Power Over Ethernet screen provides a summary of all interfaces along with information on each interface.

![Power Over Ethernet Screen](image)

**Figure 86: Power Over Ethernet Screen**

The Power Over Ethernet screen displays the following information:

- **Summary of All Interfaces**
  - Total Approved Power - Sum of the approved maximum power amounts configured for each Ethernet port
  - Total Granted Power - Sum of the approved power amounts minus power loss to transmission over Ethernet cables
  - Total Output Power - Sum of actual power amounts delivered to each powered Ethernet device

- **Information on Individual Interfaces**
  - Interface - Interface name
  - Port Class - Maximum power in watts (W)
  - Port State - Operational status of a PoE device connected to the port
  - Approved Power - Configured maximum power output in watts (W) for the interface
  - Granted Power - Maximum power available to the device
  - Output Power - Power drawn by the device
  - Output Current - Current available on the PoE link in milliamps (mA)
  - Output Voltage - Voltage available over the PoE link in volts (V)
7.10 Viewing Connected Endpoints

Connected Endpoints are identified by DHCP collector. By default, the DHCP collector is enabled in TerminAttr. You must enable it on VLANs where you would like to identify connected endpoints. See Enabling DHCP Collector.

Once it is enabled, the Connected Endpoints summary screen provides information on all connected endpoints. See Accessing the Connected Endpoints Summary Screen.

Enabling DHCP Collector

As of TerminAttr v.1.6.0, the ECO DHCP Collector is enabled by default and listens on 127.0.0.1:67 for UDP traffic. Add 127.0.0.1 as an IP helper address on VLANs to capture device identification.

```
switch(config)# interface vlan100
switch(config-if-Vl100)# ip helper-address dhcp_server_address
switch(config-if-Vl100)# ip helper-address 127.0.0.1
switch(config-if-Vl100)# exit
switch(config)# ip dhcp snooping
switch(config)# ip dhcp snooping information option
switch(config)# ip dhcp snooping vlan 100
```

Accessing the Connected Endpoints Summary Screen

On the CloudVision portal, navigate to Devices > Connected Endpoints to view the Connected Endpoints Summary screen. This screen provides the classified summary of all endpoints along with the detailed information of each endpoint. See the figure below.

![Figure 87: Connected Endpoints Summary Screen](image)

**Note:** To reset to all endpoints, click the refresh icon (next to selected endpoint in breadcrumbs) that is displayed after selecting a particular endpoint.

This screen provides the following functionalities:
• Classification drop-down menu - Click and select the required classification.
• Endpoints Counts by Type pane - This pane provides a summary of the selected classification through the following groups:
  • Legend - Hover the cursor on Legend to view color classifications used for various categories.
  • Sunburst graph - Provides the summarized view of all endpoints in various categories, hierarchies, and counts.
  
  Note: Clicking on a category sets the appropriate category as the new active classification.
  • Classification - Displays selected classification in bread crumbs
  
  Note: Clicking a breadcrumb link sets the appropriate classification as the new active classification.
  • Sub-Types (Optional) - Displays the count of sub-types under classification
  
  Note: Clicking a sub-type link sets the appropriate sub-type as the new active classification
  • All selected classification Endpoints pane - This pane provides the specified information of each endpoint in selected classification under the following categories:
    • Device Type
    • Device Name
    • MAC Address
    • Last Seen

7.11 Connectivity Monitor with CloudTracer

The Connectivity Monitor includes Cloud Tracer to monitor metrics streamed from EOS devices. This section includes:

• Accessing the CloudTracer Screen
• CloudTracer Latency Anomaly Events
• Connectivity Monitor with VRF Support

7.11.1 Accessing the CloudTracer Screen

To view data metrics, open to the CloudTracer screen by clicking **CloudTracer** on the CloudVision Portal (CVP).

![CloudTracer Screen](image)

Figure 88: CloudTracer Screen

This screen is divided into the following two panels:
7.11.1.1  Left Panel of the CloudTracer Screen

This panel provides the following metric options:

- **Metric** pane - Click any of the following entities to view the corresponding current metric for \( n \) connections where \( n \) is the count of selected devices and hosts:
  - HTTP Response Time
  - Jitter
  - Latency
  - Packet Loss
- **Connections** pane
  - Device or host search string - Type the device or host name for a quick search
  - Configured devices - Select the required devices and hosts to view corresponding metrics
- **Clear All** - Click to clear all selections

7.11.1.2  Right Panel of the CloudTracer Screen

This panel displays metrics of selected options in the following ways:

- Current information of the selected metric type from selected devices and hosts

  **Note:** Metrics are streamed whenever data is gathered on EOS switches. The default interval to query metrics data is five seconds.

- Click on a metric to view detailed information.

**Figure 89: Detailed Metrics**

The upper panel of this screen provides graphical presentation of the metric. The lower panel of this screen displays the metric through following categories:

- **Metric History** tab - Displays the metric history ranging from the last hour to the last week.

  Click the required timeline to view corresponding metrics.

  **Note:** Click Zoom In and Zoom Out options to view metrics ranging from every 15 minutes to every minute.
• **Raw Data** tab - Displays indexes, timestamps, and values of raw data.

![Figure 90: Raw Data Tab](image1)

• **Data Paths** tab - Displays keys and data paths used to compute the data for this metric.

![Figure 91: Data Paths Tab](image2)

**Note:** Clicking required link navigates to the corresponding path in the telemetry browser.
• **Statistics** tab - Displays statistics of the selected device.

**Figure 92: Statistics Tab**

• Hover the cursor on metric to view metrics from all metric types.

**Figure 93: Metrics from All Metric Types**

**Figure 94: Metrics History of Selected Device**

### 7.11.2 CloudTracer Latency Anomaly Events

The cloudtracer latency anomaly event monitors the latency metric between devices and configured hosts. The events are designed to alert the user when the latency between a device and a configured host is outside of recent historical bounds.
Figure 95: Anomaly Event View is a sample event view for one of these events between the device with hostname `Oslo` and the cloudtracer host endpoint `www.bbc.co.uk`.

Figure 96: Anomaly Event View Overlay explains various stages of this event.

Prior to this event in Figure 96: Anomaly Event View Overlay, the latency metric (green line in upper graph) is stable with minimal deviations. The historical bounds (blue shaded region) that determine when the metric is in a normal state has a small range with both the upper and lower bounds near the historical mean (dark blue line). The historical bounds are computed by adding and subtracting a fixed multiple of the current latency standard deviation to the current mean.

The anomaly score starts to increase from zero when the latency value strays outside of the historical bounds. The latency values that are outside the bounds are highlighted in red. The anomaly score is the total number of standard deviations outside the historical bounds. The anomaly score is the positive cumulative sum of the number of standard deviations outside of the historical bounds. For example, if the bounds are set as 3 standard deviations outside of the mean and we get a value of the latency that is 5 times the standard deviation away from the mean, the anomaly score will increase by 2. If the next latency value was 1.5 times the standard deviation outside of the mean then we
would subtract 1.5 from the anomaly score. The anomaly score therefore keeps track of the cumulative deviation of the latency outside of the historical bounds. It is bounded below by zero.

**Figure 97: Anomaly Score Computation** provides a detailed explanation on computing the anomaly score.

The event is generated when the anomaly score exceeds a threshold for a set period of time.

**Note:** You can configure the threshold and time duration in the event configuration rules.

The anomaly score starts to decrease when the latency values are inside the historical bounds. The historical bounds have increased based on recent deviations in latency which makes the system less sensitive than prior to the event. The event ends when the anomaly score is below the threshold for a set period of time.
Figure 98: Decreasing of Anomaly Score provides a detailed explanation of the anomaly score decreasing when an event ends.

At the end of the time range, historical bounds are narrowing as the latency has now returned to a stable value with minimum deviations. The history needs approximately six hours to have negligible impact on the statistics and bounds.

This screen also provides the following additional metrics of this event (see Figure 99: CloudTracer Event Additional View):

- The other CloudTracer metrics are displayed for this device and host pair
- The latency metric between other devices and this host
- The latency metric between this device and other hosts

Figure 99: CloudTracer Event Additional View
7.11.3 Connectivity Monitor with VRF Support

Connectivity Monitor with VRF support allows you to configure multiple VRFs for each host and multiple source interfaces within each host on each device.

Enabling Connectivity Monitor with VRF Support

To enable Connectivity Monitor with VRF support, the feature must be enabled from the Settings page.

1. Select the Setting icon to open the General Settings page.
2. Select the toggle for Connectivity Monitor VRFs and Interfaces (Beta).

Viewing Connectivity Monitor with VRF Support

To view Connectivity Monitor with VRF Support, select Connectivity Monitor from the Devices tab.

Figure 100: Viewing VRF Results in Connectivity Monitor

You can select individual host/VRF/interface combinations to view latency/jitter etc. information for just the selection. Selection options include:

• Selecting the checkbox next to a VRF name will select all source interfaces on the VRF.
• Selecting the checkbox next to the name of the host will select all VRFs and all source interfaces within each VRF.
• Selecting the checkbox next to the device name will select every host configuration available on the device.

7.12 Managing Tags

On the CloudVision portal, navigate to Provisioning > Tags to view the Tags Management screen. See the figure below.

![Figure 101: Tags Management Screen](image)

This screen provides the following functionalities:

• **Search device or tags** field under the Devices column - Type either the required device name, tags category, or tag name for a quick search of devices and tags.
• **Search device, interface, or tags** field under the Interface column - Type either the required device name, tags category, tag name, or interface name for a quick search of device, interface, or tags.
• **Select All** checkbox - Select the checkbox to choose all devices simultaneously.
• **Edit tags** button - Click to delete unassigned tags. See Deleting Unassigned Tags.

7.12.1 Creating and Assigning Tags

Perform the following steps to create and assign a tag to a device:

1. On CVP, click Provisioning > Tags.
   The system displays the tags screen.
2. On the Device pane, select device(s) to which you want to create and assign a tag. The system opens the Assigned tags pane. See the figure below.

![Figure 102: Create and Assign](image)

**Note:**
- Optionally, use the search bar for searching required devices.
- To manage interface tags, click the Interface tab and perform required tasks.

3. Type the new tag in the search field under User Tags > Add or create tags > Type the label then the value separated by a colon.

**Note:**
- Tags should be of the form `<label>: <value>`. For example, owner: Bill.
- The System Tags pane displays tags that are automatically created and assigned by the system.

4. Click Create and Assign.

**Note:** If you had selected multiple devices, the new tag will be simultaneously assigned to all selected devices.

The new tag is displayed under Manage assigned tags.

7.12.2 Deleting Assigned Tags

Perform the following steps to delete an assigned tag:

1. On CVP, click Provisioning > Tags.

The system displays the tags screen.
2. On the **Device** pane, select the device(s) which is associated with the tag that needs to be removed.

The system displays all tags assigned to the selected device(s) under **Manage assigned tags**.

![Figure 103: Associated with Selected Devices](image)

**Note:**
- Optionally, use the search bar for searching required devices or tags.
- Hovering the cursor on the number next to the tag name, lists the devices to which the current tag is assigned.

3. Click the tag that needs to be removed.

The system displays plus and minus signs when the tag is clicked.

4. Click the minus sign to delete the selected tag.

5. Click **Save Edits**.

### 7.12.3 Adding Tags to Multiple Devices

Perform the following steps to add a tag to multiple devices simultaneously:

1. On the main pane of the tags screen, select the device to which the tag has already been assigned to; and new devices to which the tag needs to be assigned.

Under **Manage Assigned Tags** on the right pane, CVP lists tags that are assigned to selected devices.

**Note:** Hovering the cursor on the number next to the tag name, lists the devices to which the current tag is assigned. See the figure below.
Device Management

2. Click the desired tag.
   The system pops up plus and minus signs beneath the tag.
3. Click the plus sign to add this tag to all selected devices.
4. Click Save Edits.

7.12.4 Removing Tags from Multiple Devices

Perform the following steps to remove a tag from multiple device simultaneously:

1. On the main pane of the tags screen, select devices that are assigned with the tag that needs to be removed.

   Note: Alternatively, search the tag that needs to be removed. CVP lists all devices to which the tag is assigned to. To remove the tag from few devices, select only devices from which the tag needs to be removed. If you select all devices, the tag will be removed from all devices.

Under Manage Assigned Tags on the right pane, the system lists tags that are assigned to selected devices.

2. Click the tag that needs to be removed.
   The system pops up plus and minus signs beneath the tag. See the figure below.

Figure 104: Tag Assigned to Multiple Devices

Figure 105: Remove Tag from Multiple Devices
3. Click the minus sign to remove the tag from all selected devices.
4. Click Save edits.

7.12.5 Deleting Unassigned Tags

Perform the following steps to manage unassigned tags:

1. On CVP, click Provisioning > Tags.
   The system displays the tags screen.

2. On the main pane of the tags screen, click Edit tags.
   The system lists all unassigned tags.

3. Click the tag that needs to be removed.
The clicked tag turns to red.

Figure 106: Delete Unassigned Tags

4. Click Delete.
The system deletes the tag from CVP.

7.13 Accessing Dashboards

The Dashboards application allows you to create customizable dashboards consisting of multiple metrics across various datasets in different views. You can quickly resize and drag widgets on the grid to accommodate various custom layouts views. Data gathered from devices configured for streaming telemetry data to CVP.

- Dashboard Manager
- Editing and Creating Dashboards

7.13.1 Dashboard Manager

Dashboards Manager is where you are presented with the list of available dashboards. This screen can be viewed in either a grid or table format.
Each dashboard on the grid provides the dashboard name, description, and an approximate layout of the dashboard. To perform actions on any of the dashboards, select one or more dashboards by selecting the checkbox associated with each dashboard.

Figure 108: Dashboard Actions Menu

7.13.2 Editing and Creating Dashboards

Creating a Dashboard

Perform the following steps to create a dashboard.
1. Select **New Dashboard** from the Dashboard Manager page.
2. Select one or more widgets to display information.

![Figure 109: Dashboard Widgets](image)

3. Select the widget in the main screen to configure and label the widget.
4. Enter a title and description of the new dashboard.
5. Select **Save Changes** to save the new dashboard.

**Editing a Dashboard**

Perform the following steps to edit a dashboard. Dashboard widgets can be added, removed, or configured while in editing mode.

1. Select a dashboard to display from the Dashboard Manager page.
2. Select **Edit Dashboard** from the Dashboard Manager page.

![Figure 110: Editing a Dashboard](image)

3. Select a currently displayed widget in the main screen to edit or configure as needed.
4. To add a new widget, select from widgets tab.
5. To change the inputs, select the Inputs tab to configure as needed.
6. Select the pencil icons to edit the dashboard title and description.
7. Select **Save Changes** to save the changes.

### 7.14 Topology View

You can view the network hierarchy for the devices and subnetwork in real-time. The topology view is available for devices running on LLDP including Arista switches and connected neighbors.

**Related topics:**
- Setup
- Overlays
- Custom Topology Views
7.14.1 Setup

You can customize the topology by completing the following steps.

1. Click the **Topology** tab to view your network.
2. To enter layout hints, click on a device in the topology view and then click on the layout tab.

Following example shows the detail of a device.

![CVP Detail Layout](image)

Figure 111: CVP Detail Layout

7.14.2 Overlays

You can superimpose link-level metrics overlay onto the network topology. Use the Layers Panel to view these overlays and color-codes based on the severity of that metric. Following are the overlays supported in this release.

The following table lists the Overlays supported in this release.

<table>
<thead>
<tr>
<th>Overlay</th>
<th>Description</th>
</tr>
</thead>
</table>
### Bandwidth Utilization
Shows the bitrate as a percentage of the speed of the link. It uses the maximum bitrate in either direction on the link, averaged out over a one-minute window. Light green indicates a small percent of the link is being used, while darker greens indicate higher usage. Beyond 80% utilization, the links show up in yellow or red.

### Traffic Throughput
Shows the bitrate of a link as an absolute number. Darker blues indicate higher utilization.

### Error Rates
Show if either end of a link is registering input or output errors (for example, CRC Errors). It uses a one-minute window, and displays severity in increasingly dark reds.

### Discard Rates
Indicate that a link is dropping packets, likely due to congestion. Links discarding more packets in a one-minute window are shown in darker red.

### None
Turns off all colors.

## 7.14.3 Custom Topology Views

From the Topology tab, you can perform the following steps to customize a view:
1. To move a rack to a different pod use the Pod field. For example, the switch called cv-demo-sw3 is set to be in a pod 1.

Figure 112: User Layout Hints
2. To setup the pod or rack names, apply a layout hint for switch with alternate name or pod hint for the spine switch to rename the pod. Following example shows the top-of-rack switch cv-demo-sw3 default name change via the rack layout hint.

![Device Details in Layout](image)

**Figure 113: Device Details in Layout**

### 7.14.4 Changing the Node Type

The following table lists the node types supported by the Topology view.

**Table 14: Supported Node Type**

<table>
<thead>
<tr>
<th>Node Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge Device</td>
<td>The device is an edge device, for example, leading to the Internet or another network, or a similar function device.</td>
</tr>
<tr>
<td>Core Switch</td>
<td>The device is at the core level switch (above spines) or similar function device.</td>
</tr>
<tr>
<td>Spine Switch</td>
<td>The device is a pod level (spine or aggregation) switch or similar function device.</td>
</tr>
<tr>
<td>Leaf Switch</td>
<td>The device is a top of rack switch or similar function device.</td>
</tr>
</tbody>
</table>
### Endpoint Device

| The device is a server or similar endpoint device. |

Setting the **Node Type** layout hint gives the **Topology** view of the type of device selected. Selecting **skip auto-generating** forces the auto tagger to ignore the device and not assign or modify any of the hints.

![Figure 114: Changing Node Type](image)

### 7.14.5 Nodes and Features

Nodes are arranged in clusters. To expand a cluster, click on the representative **Cluster-node**. To collapse a cluster, click on the minus (−) icon.

You can select various overlays on the graph for color coding links.

To see details about a node and its neighbors, click on the **Node**. You can also see the immediate neighbors of the device and the metrics related to particular physical links between devices by clicking **Neighbors List**.

### 7.15 Accessing Events

You can access the following events screens:

- **Events Summary Screen**
- **Event Details Screen**

**Related topics:**

- **Events Summary Screen**
- **Event Details Screen**
- **Configuring Event Generations**
- **Managing Events**
  - **Disabling All Events of the Selected Type**
  - **Disabling All Events of the Selected Type with Exceptions**
- **Acknowledging Events**
- **Configuring Notifications**
  - **Configuring Status**
  - **Configuring Platforms**
  - **Configuring Receivers**
  - **Configuring Rules**

#### 7.15.1 Events Summary Screen

The events summary screen displays all events, and configures alerts and event generation. To view this screen, click **Events** on the CloudVision portal.

The **Events** screen provides the following information and functionalities:
• **Left Pane**
  - A search field for events, devices, and interfaces
  - Buttons to perform a search based on severity levels (info, warning, error, and critical)
  - A toggle button to add and remove acknowledged events from search results
  - The count of events from search results
  - A button that allows you to display new events and also provides their count A list of events (the most recent are shown at the top of the list)

• **Right Pane**
  - The count of all events and devices from search results
  - The time frame from which events are selected
  - Devices that have reported the most events and errors (shown in the **Most Active Devices** pane)
  - Most common events (shown in the **Most Common Events** pane)
  - Count of each error type from device errors (shown in the **Event Severities** pane)
  - A chronological history of all errors (shown at the bottom of the screen)

Click the **Events** tab to view all events.

![Figure 115: Events Summary Screen](image)

### 7.15.2 Event Details Screen

An event details screen displays appropriate event details, acknowledges the event, and configures event generation. To view this screen, click one of the events listed in the left pane from the **Events** screen.
Figure 116: Event Details Screen

This screen provides the following information and functionalities in the right pane:

- Left arrow to return to the events summary screen
- Warning of the event
- Time when event details were captured
- Hover the cursor on the event name. The system displays a popup window with event details.

Figure 117: Event Name Popup Window

The popup window provides the following options:

- Click View Events to view search results with the same event name.
Figure 118: Search Results with the Same Event Name

- Click **Compare Metrics** to navigate to the **Explorer** tab in Metrics app.
- Hover the cursor on the event name. The system displays a popup window with device details in that location.

Figure 119: Location Name Popup Window

The popup window provides the following options:

- Click **View Events** to view search results with the same location name.
Figure 120: Search Results with the Same Location Name

- Click **Compare Metrics** to navigate to the **Explorer** tab under **Metrics**.
- The **Acknowledge** button to acknowledge the appropriate event.
- The **Configure Event Generation** button to configure the generation of appropriate event.
- Metric details of the event
- A chronological history of all errors (shown at the bottom of the screen)

### 7.15.3 Configuring Event Generations

Configure rules and conditions to customize event generation.

Perform the following steps to configure the settings for generating events:

1. On the CloudVision portal, click the **Events** tab. The system displays the **Events** screen.
2. Click **Configure Event Generation** at the upper right corner of the **Events** section. The system displays the **Generation Configuration** screen with all configurable events listed in the left pane.

![Figure 121: Generation Configuration Screen](image)

**Note:** Alternatively, you can go to an event details screen and click **Configure Event Generation** to configure rules for generating events.

3. Click the required event in the left pane.
4. Click **Add Rule** in the lower end of right pane. A new **Condition** pane is displayed on the screen.

![Figure 122: Add Rule Pane in Generation Configuration](image)
5. In the **Condition** pane, click on the search field. The system displays the list of configured devices tags.

![Figure 123: List of Configured Device Tags](image)

**Note:** Alternatively, you can type the required device tag in the search field for a quick search.

6. Select preferred devices tags from the displayed list.

**Note:** After you have selected the device, the system displays the count of matched devices. The rule is applicable to all devices when you do not select any device tag.

7. Click on the **Interfaces** search field (available only for interface events).

The system displays the list of configured interface tags.

![Figure 124: List of Configured Interface Tags](image)

8. Select preferred interface tags from the displayed list.

**Note:** After you have selected an interface tag, the system displays the count of matching interfaces. The rule is applicable to all interfaces when you do not select any interface tag.
9. Provide the following criteria required to generate events:
   • **Severity** - Select the severity type from the drop-down menu. Options include **Info**, **Warning**, **Critical**, and **Error**.
   • **Threshold** (applicable only to threshold events) - Type the threshold value.
   • **Raise Time** - Type the preferred wait time (seconds) to create an event after reaching the threshold limit.
   • **Clear Time** - Type the precise time (seconds) to delete an event after the current value goes below the threshold limit.

   Note: Select the **Stop generating events** and checking rules checkbox if you do not want to apply further rules for selected tags. If no tags are selected, further rules are not applicable to any device.

10. Click **Move up** if you prefer to move this rule up in the priority list.

   Note: Rules are processed sequentially. The default rule is applied only when an event does not match any other rules. Click **Delete** rule to delete the corresponding rule. Click **Move down** in configured rules to move the corresponding rule down in the priority list.

11. Click **Save** in the left pane.

   Note: Click **View Configuration Differences** in the lower left pane to view differences in event configurations.

7.15.4 Custom Syslog Events

The **Custom Syslog Event** creates syslog message events based on rule conditions. To end all similar active events, you must update the configuration as per the recommended action provided in the EOS System Message Guide.


   Note: Rules are processed sequentially. Events that don't match user created rule conditions are processed by default rule(s).

Perform the following steps to create a rule for generating syslog events:

1. On the CloudVision portal, click the **Events** tab. The system displays the Events screen.
2. Click **Configure Event Generation** at the upper right corner of the **Events** section.

   Note: Alternatively, you can go to an event details screen and click **Configure Event Generation** to configure rules for generating events.

   The system displays the Generation Configuration screen with all configurable event types listed in the left pane.
3. Click **Custom Syslog Event**.

![Figure 125: Custom Syslog Event Screen](image)

4. **Click +Add Rule** in the right pane.
   
   A new condition pane is displayed on the screen.

![Figure 126: Conditions Pane for the Custom Syslog Event Rule](image)

5. **Provide the following information in specified fields:**
   - **Active devices** autocomplete field -
   - **Generate an event for these conditions** checkbox -

6. **Choose either Single Instance Events or Time Period Events** using the toggle button.
7. Based on your choice between single instance events and time period events, provide the following relevant conditions for generating a rule:

- Configuring Single Instance Events
- Configuring Time Period Events

Note: The corresponding fields appear after you choose the required event type.

8. Save Changes button - Click to save specified changes.

7.15.4.1 Configuring Single Instance Events

CVP creates a single instance event whenever either the specified syslog ID matches with the device syslog ID or the specified syslog message matches with the device syslog message. See Figure 126: Conditions Pane for the Custom Syslog Event Rule.

Provide the following information in specified fields to configure a single instance event:

- **Syslog ID** - Provide facility, severity, and mnemonic of a syslog with regular expressions in the following fields:
  - **Facility** field - Type the facility of syslog in either simple string or regular expression.
  - **All severities** field - Select the severity of the device.

  Note: If no severity is selected, CVP considers all available severities.

- **Mnemonic** field - CVP creates a single instance event when the log message specified in this field matches with a device syslog message.
- **Log Message** field - The log message to match against the device syslog message.

  Note: You must mandatorily configure either a syslog ID or a log message.

- **Mute Period** field - CVP does not create another similar event using this rule on a given device until the time period specified in this field expires for the ongoing event.

  Note: This prevents a large number of events generated for the same device within a short period of time due to a repetitive syslog message.

- **Event Title** field - Type the event title.
- **Severity From Syslog** checkbox - Select the checkbox if you prefer CVP to select the severity of the generated event to be derived from the syslog message severity.

  Note: CVP uses the following syslog message severities to event severities:
  - [0, 1, 2] - Critical event
  - [3] - Error event
  - [4] - Warning event
  - [5,6,7,...] - Info event

- **Severity** dropdown menu - Select the preferred severity of the generated event. Severity is configurable only when **Severity From Syslog** checkbox is not selected.
- **Event Description** field - Provide the event description.
- **Ignore subsequent rules for selected devices** checkbox - Select the checkbox to suppress generating events for a specific syslog or override upcoming configurations.
- **Move Up** / **Move Down** buttons - Use this button to manage the sequence of configured syslog event rules.
- **Delete** button - Click to delete the corresponding rule.

Note: Syslogs with high severities like 0 (Emergency), 1 (Alert), 2 (Critical), and 3 (Error) generate events by default unless they are ignored by user configured rules.

7.15.4.2 Configuring Time Period Events
Events can also be configured to be time period events that remain active between the syslog message that creates it and the syslog message that ends the event. See the figure below.

Figure 127: Configuring Time Period Event

Provide the following information in specified fields to configure a time period event:

- **Start Log Message** field - CVP starts a time period event when the start log message specified in this field matches with a device syslog message.
  
  Note: The start log message must be a string without special characters.

- **End Log Message** field - CVP ends a time period event when the end log message specified in this field matches with a device syslog message.
  
  Note: The end log message must be a string without special characters.

- **Parameter** field - Type the variable that must be configured in log messages specified in the **Start Log Message** and **End Log Message** fields.
  
  - **Value** field - Type a variable for the specified parameter in either a simple string or a regular expression.
  
  - **Add Value** - Click to add another variable for the specified parameter.

*Ethernet* is a parameter with values as *Ethernet1* and *Ethernet2*. See the figure below.

Figure 128: Example1 of Parameter Variables
In this case, the specified log messages matches with Ethernet1 and Ethernet2 values for either starting or ending an event.

*Ethernet* is a parameter with a value as *Ethernet.*. See the figure below.

![Figure 129: Example2 of Parameter Variables](image)

In this case, the specified log messages matches with all ethernet values like Ethernet1, Ethernet1/2, Ethernet1/3, and so on for either starting or ending an event.

- **Raise Time** field - After a start rule matches, the starting of an event is delayed for the duration specified in this field.

  Note: If the end event log message arrives before this delay elapses, the event is not generated. This option is useful in situations where you wish to generate an event only when a syslog condition has persisted for at least some set period of time.

- **Clear Time** field - After an end rule matches, the ending of the ongoing event is delayed for the duration specified in this field.

  Note: If the start event log message arrives before this delay elapses, the event is not ended and will continue as an active event. This option is useful in situations where you wish to generate a long single event which may encompass several start/end conditions being met during a set period of time.

- **Event Title** field - Type the event title.

- **Severity From Syslog** checkbox - Select the checkbox if you prefer CVP to select the severity of the generated event to be derived from the syslog message severity.

  Note: CVP uses the following syslog message severities to event severities:
  
  - [0, 1, 2] - Critical event
  - [3] - Error event
  - [4] - Warning event
  - [5,6,7,...] - Info event

- **Severity** dropdown menu - Select the preferred severity of the generated event. Severity is configurable only when **Severity From Syslog** checkbox is not selected.

- **Event Description** field - Provide the event description.

- **Ignore subsequent rules for selected devices** checkbox - Select the checkbox to suppress generating events for a specific syslog or override upcoming configurations.

- **Move Up / Move Down** buttons - Use this button to manage the sequence of configured syslog event rules.

- **Delete** button - Click to delete the corresponding rule.
Note: A configuration change in the current rule ends all ongoing events.

7.15.5 Managing Events
You can manage an event by customizing event rules differently. Refer to the following examples:
- Disabling All Events of the Selected Type
- Disabling All Events of the Selected Type with Exception

7.15.5.1 Disabling All Events of the Selected Type
Perform the following steps to disable all events of the selected type:

1. Navigate to the Generation Configuration screen.
2. Click the required event type in the left pane.
3. In the right pane, Click the + Add Rule button.
   Note: Retain only one rule with no values defined. To disable the event only for selected datasets, select appropriate devices tags in the Devices field.
4. Select the Stop generating events and checking rules checkbox.
   The system disables all events of the selected event type.

![Figure 130: Disable All Events of the Selected Type](image)

5. Click Save in the left pane.

7.15.5.2 Disabling All Events of the Selected Type with Exception
Perform the following steps to disable all events of the selected type with exceptions:

1. Navigate to the Generation Configuration screen.
2. Click the required event type in the left pane.
3. In the right pane, Click the + Add Rule button.
4. In the Conditions pane, provide the device tags that you still want to generate an event for. The system creates rule 1.
   Note: If you need devices with different conditions, add another rule by repeating steps 3 and 4
5. Click the + Add Rule button.
6. In the appropriate **Conditions** pane, select the Stop generating events and checking rules checkbox. The system creates rule 3.

**Note:** If you skip steps 5 and 6, the system applies default rules to all device tags except the ones that are defined in rules 1 and 2.

---

**Figure 131: Disable All Events of the Selected Type with Exception**

The system disables all events of the selected type except the ones that are defined in rules 1 and 2.

---

### 7.15.6 Acknowledging Events

Acknowledging an event confirms that you are aware of the corresponding event and its consequences. By default, acknowledged events are hidden and do not send alerts.

Perform the following steps to acknowledge an event:

1. Click the **Events** tab. The system displays the **Events** screen.
2. Select preferred event(s) in the side panel.
3. Click **Acknowledge** \( n \) in the upper right corner of the side panel.

**Note:** \( n \) represents the count of selected events.

The system displays the **Acknowledgment Event** window.

---

**Figure 132: Acknowledgment Event Pop-Up**

4. (Optional) Type a note for other users explaining the reason for the acknowledgment.
5. Click **Acknowledge n events** where \( n \) represents the count of selected events.

   **Note:** For acknowledged events, the system replaces the **Acknowledge** button with **Un-Acknowledge** button. To undo the acknowledgment activity, click **Un-Acknowledge** in the side panel of the acknowledged event.

### 7.15.7 Configuring Notifications

The event alerting system sends notifications for CVP events as they alert operating platforms that you have set up. Once you have customized the topology view for your network, provide the required information to configure the monitoring of notifications.

Perform the following steps to configure event alerts:

1. Click the **Events** tab.
2. Click **Configure Notifications** at the upper right corner of the Events section. The system displays the Notification Configuration screen.
3. Configure the following entities:
   - Configuring Status
   - Configuring Platforms
   - Configuring Receivers
   - Configuring Rules
4. Click **Save** in the left pane

#### 7.15.7.1 Configuring Status

The **Status** section configures monitoring the health of notification system.

Perform the following steps to configure the notification criteria:

1. Click **Status**. The system displays the **Status** screen.

   ![Status Screen of Notification Configuration](image)

   **Figure 133: Status Screen of Notification Configuration**

   2. On the **Test Alert Sender** pane, provide the required criterion in **Severity**, **Event type**, and **Device** drop-down menus.

   3. If required, click **Send Test Notification** to verify current configuration.

#### 7.15.7.2 Configuring Platforms

The **Platforms** section specifies what platforms will receive notifications.
Perform the following steps to configure preferred platforms:

1. Click **Platforms**. The system displays the **Platforms** screen.

![Platforms Screen of Notification Configuration](image)

**Figure 134: Platforms Screen of Notification Configuration**
2. Configure any of the following platforms through which you prefer to receive notifications from CVP:

- **Email**
  
  Provide the following information to receive email notifications:
  
  - Type your SMTP servers hostname and port number separated by a colon in the **SMTP Host** field.
  
    **Note:** Typically, the port numbers of SMTP and SMTP over TLS are 25 and 587.
  
  - Select the **Use TLS for SMTP** checkbox if you prefer to encrypt notifications received from and sent to the SMTP server.
  
  - Type the email address that you prefer to display as a sender in the **Email "From" Address** field.
  
    **Note:** We recommend an email address with the domain of your organization.
  
  - Type the username of your SMTP account in the **SMTP Username** field.
  
  - Type the password of your SMTP account in the **SMTP Password** field.

- **Slack**

  Create a custom integration through the Incoming WebHooks Slack application and type the Webhook URL in the **Slack Webhook URL** field.

- **VictorOps**

  In your VictorOps settings, add a new alert integration for Prometheus and type the Service API Key in the **VictorOps API Key** field.

  - If required, type a custom API URL in the **VictorOps API URL** field.

- **PagerDuty**

  If required, type a custom API URL in the **PagerDuty URL** field.

- **OpsGenie**

  - Create an API integration for your OpsGenie team and type the API key in the **OpsGenie API Key** field.

  - If required, type a custom API URL in the **OpsGenie API URL** field.

- **WeChat**

  - Type your WeChat credentials in the **WeChat API Secret** field.

  - Type your WeChat corporate ID in the **WeChat Corporate ID** field.

  - If required, type a custom API URL in the **WeChat API URL** field.

### 7.15.7.3 Configuring Receivers

The Receivers section configures a receiver for each preferred team to send notifications and link receivers to notification platforms.

Perform the following steps to add new receivers:
1. Click **Receivers**. The system displays the Receivers screen.

![Receivers Screen of Notification Configuration](image1)

**Figure 135: Receivers Screen of Notification Configuration**

2. Click **Add Receivers** at the end of the screen.

3. Type receiver's name in the **Receiver Name** field.

![Add Receiver Pane](image2)

**Figure 136: Add Receiver Pane**

4. Click the **Add Configuration** drop-down menu.

5. Select any of the options in following table and provide the required information to link alert receivers with alerting platforms.

<table>
<thead>
<tr>
<th>Configuration Options</th>
<th>Required Information</th>
</tr>
</thead>
</table>

**Table 15: Configuration Options**
### Add Email Configuration
- Type recipient's email address in the **Recipient Email** field.
- If required, select the **Send alert when events are resolved** checkbox.

### Add VictorOps Configuration
- Type a routing key in the **Routing Key** field.
- If required, select the **Send alert when events are resolved** checkbox.

### Add PagerDuty Configuration
- Type a routing key in the **Integration Key** field.
- If required, select the **Send alert when events are resolved** checkbox.

### Add OpsGenie Configuration
- Select the **Send alert when events are resolved** checkbox.

### Add Slack Configuration
- Type a channel in the **Channel** field.
- If required, select the **Send alert when events are resolved** checkbox.

### Add WeChat Configuration
- Select the **Send alert when events are resolved** checkbox.

### Add Pushover Configuration
- Type a recipient's user key in the **Recipient User Key** field.
- Type a pushover API token in the **Application API Token** field.
- If required, select the **Send alert when events are resolved** checkbox.

### Add Webhook Configuration
- Type the URL where you prefer to post event alerts in the **Target URL** field.
- If required, select the **Send alert when events are resolved** checkbox.

---

**Note:** Click the recycle bin icon at the right end of corresponding fields if you prefer to delete that configuration. Click **Delete Receiver** next to **Add Configuration** if you prefer to delete the corresponding receiver.

### 7.15.7.4 Configuring Rules
The Rules section customizes notifications that are sent to receivers.

Perform the following steps to add a new rule:
1. Click Rules. The system displays the Rules screen.

2. Click Add Rules. A new Rules Conditions pane is displayed on the screen.

3. Next to Add Conditions, click Severity, Event Type, Device, and Device Tags to provide the criteria that are used for monitoring the health of the alerting system.

   **Note:** Click Remove at the end of a field to delete that configuration.

4. Select the required receiver from the Receiver drop-down menu.

5. Select required checkboxes among Severity, Event Type, Device, and Interface to group similar events into a single alert.

6. Select the Continue checking lower rules checkbox to continue checking for alerts if this event matches subsequent rules.
7. Click **Move up** if you prefer to move this rule up in the priority list.

**Note:** Rules are processed sequentially. The default rule is applied only when an event does not match any other rules. Click **Delete rule** to delete the corresponding rule. Click **Move down** in configured rules to move the corresponding rule down in the priority list.

7.16 **Events App (Beta)**

For additional

The Events app (Beta) provides fast filtering results that are loaded 100 events at a time, improving loading times and responsiveness compared to the existing Events app. This new app also has improvements to the summary views and adds new filters.

**Accessing the Events App (Beta)**

To open the Events App (Beta):

1. Select the General Settings icon (top right # icon).
2. Select and enable the toggle for **New Events App (Beta)**.

![Figure 139: General Settings - New Events App (Beta)](chart)

**Note:** The **Beta events (Beta)** is a different feature. This section discusses **New Events App (Beta)**.

7.16.1 **Event Summary**

At the top of the app is the event summary. The summary has two tabs for the Event Chart and the Summary Tables. There is also a time range duration picker that selects the start of the time range for the summary results. The filters in the app sidebar also affect the summary views, allowing the request of specific summary queries.
Figure 140: New Events App (Beta)

Event Chart

The default summary view is the Events Chart. This chart displays the number of events that were created in a time range, broken down by severity. Hovering over a colored section of a bar shows how many events occurred with that given severity. A bar represents the events that were created within time range for that bar. The amount of time represented by a bar is dependent on the selected time range. Larger time ranges will group more events into a single bar.

Figure 141: Event Chart Summary

Summary Tables

The Summary Tables tab displays the events of the Events Chart in a table format. Results can be filtered by severity value, device, or event-type.
Summary Time Picker

In the top-right corner of the summary there is a time range picker. This affects the summaries only. The end-time of the summary window is determined by the Events Starting Before filter in the sidebar. The start-time is derived from the chosen time range. The range picker has a minimum duration of one hour and a maximum of one week.

Figure 143: Summary Time Picker

7.16.2 Events Table

Events matching the selected filters are displayed in the table below the summary.

Figure 144: Events Tables

The newest 100 events are initially loaded. Subsequent events are fetched via automatic pagination. The Ack (Acknowledgement) column only appears if the Show Acknowledged filter toggle is on. This allows other columns to expand when acknowledgment information is not required.
Events Table Functionality

- When scrolling down through the table of events, older events are automatically fetched.
- If there are no events matching the selected filters, the events table will display an empty data message.
- To update the display with events that may have occurred while viewing the Events Table, select the Show New Events button. The screen will be updated with the new data.
- To export the currently-loaded events, select the Export Table to CSV button.

7.16.3 Event Filters

Filter options are located in the sidebar. The selected filters affect the results in both the events summary and the events table. Multiple filters can be selected to refine the results shown in these sections. Filters are automatically applied as they are changed in the sidebar.

Events Starting Before

The Events Starting Before time selector defines the end cutoff time filter for events. Events that are created after the selected time will not be shown. By default, the filter is set to the current time.

Select this filter to open the date-time picker, allowing an older time to be selected. Select Apply to update with this new time filter. Select Use current time to show live events.

Severity

Selecting an event severity will display only the selected severity level.

Event Description

The Event Description filter allows events to be searched by arbitrary text in the event description field.

Event Type

When selected, the Event Types filter presents a list of all available event types. Selecting one or more options filters the results to events of the selected types.

Device

When Selected, the Device filter presents a list of all streaming devices. Selecting one or more devices will display events that occurred on the selected devices.

Show Acknowledged

Select Show Acknowledged to view events which have been previously acknowledged.

Active Events Only

Select Show Active Only to view events which are still active.

Resetting Filters

Select the Reset Filters button to place all Event filters to their default values.
7.17 Troubleshooting

A number of commands are provided with the Telemetry platform that you can use to troubleshoot the Telemetry platform components. The types of troubleshooting you can perform using the Telemetry platform commands are:

- General Troubleshooting
- Troubleshooting the NetDB State Streaming Agent
- Checking the Status of the Ingest Port

7.17.1 General Troubleshooting

Telemetry commands are provided that enable you to troubleshoot the Telemetry platform components. By default, debug log files are available for all of the Telemetry platform components, which you can view using Telemetry commands. You can also use standard CVP commands to check the status of Telemetry components and applications.

7.17.1.1 Viewing Debug Log Files

You can view debug log files for all platform components in a single log file, or for a particular platform component.

Note: To use the commands, you must login as cvp user. You must also login as cvp user to execute su cvp.

To view debug log files for all platform components in a single log file
Use the cvpi logs all command.

To view the location of debug log files for a particular platform component
Use the cvpi logs <component> command.

You must specify the component using the name of the component as it is specified in the component's yaml file definition.

To create a zip archive (.tgz) containing debugging information
Use the cvpi debug command.

This command creates a .tgz archive on each CVP node that contains debugging information. The archive is automatically saved to the /data/debug directory on each node. Files need to be collected manually.

7.17.1.2 Checking CVPI Status

You can use commands to check status of the Telemetry components and applications, and to check the status of the entire CVP environment.

To check the status of CVPI
Use the cvpi status all command.

This command checks the status of CVPI, including the Telemetry components and applications.

To check the status of CVP environment
Use the cvpi check all command.

This command runs a check to ensure that the CVP environment is setup correctly. In a multi-node setup, it checks to make sure that the nodes can communicate with to each other and have the same environments and configuration.
7.17.2  Troubleshooting the NetDB State Streaming Agent

The Telemetry platform component provides commands you can use to troubleshoot issues you may encounter with the installation or performance of the NetDB State Streaming Agent.

The commands enable you to:

- Inspect the agent's configuration
- Restart the agent
- View the agent's logs

7.17.2.1  Inspect the agent's configuration

Run the following commands to view the agent's configuration:

```
switch> enable
switch# config
switch (config)# daemon TerminAttr
switch (config-daemon-TerminAttr)# show active
daemon TerminAttr
eexec /usr/bin/TerminAttr -ingestgrpcurl=172.28.131.84:9910 -
ingestauth=key,ab27cf35f73543d2afe3b4c15c12e6a3 -taillogs
no shutdown
```

7.17.2.2  Restart the agent

Run the following commands to toggle the shutdown attribute:

```
switch (config-daemon-TerminAttr)# shutdown
switch (config-daemon-TerminAttr)# no shutdown
```

7.17.2.3  View the agent's logs

On the switch or using the CLI shortcut, run the following command:

```
bash cat /var/log/agents/TerminAttr-`pidof TerminAttr`
```

7.17.3  Checking the Status of the Ingest Port

The Telemetry platform automatically blocks the ingest port for the entire CVP cluster if the disk usage on any node of the cluster exceeds 90%. This feature prevents the potential for telemetry data to consume too much disk space in the CVP cluster.

You can easily check to see if the ingest port is blocked using the cvpi status ingest-port command.

**Example**

```
[cvp@cvp109 bin]$ cvpi status ingest-port
[ingest-port:status] Executing...
[ingest-port:status] FAILED
COMPONENT ACTION NODE STATUS ERROR
ingest-port status primary NOT RUNNING command: Error running '/
cvpi/bin/ingest-port.sh status'...
ingest-port status secondary NOT RUNNING command:
Error running '/cvpi/bin/ingest-port.sh status': exit status 1
```

152
ingest-port status tertiary NOT RUNNING command:
Error running '/cvpi/bin/ingest-port.sh status': exit status 1
[cvp@cvp109 bin]$
Device Comparison Application

To gain valuable insights into the state of your devices, such as state changes and comparison with another device, you can manage your inventory for real-time status updates.

The device comparison application gives information about the configuration running on the devices, the VXLAN table, MAC addresses of the devices, IPv4 and IPv6 routing tables, etc.

- Comparison Dashboard
- Running Configuration
- Snapshots
- ARP Table
- Comparing NDP Table
- MAC Address Table
- VXLAN table
- Viewing Device IPv4 Routing Table
- Viewing Device IPv6 Routing Table
- Comparing IPv4 Multicast Table

8.1 Comparison Dashboard

The Comparison Dashboard from the Device tab explores the difference between devices or changes that happened to devices over time. You can compare devices in the following categories:

- Two devices: Two devices at current time with live updates
- Two times: The state of a single device at two chosen times
- Advanced: Two devices at two chosen times

8.1.1 Accessing the Comparison Browser Screen

You can access the Cloud Vision Telemetry Browser screen directly from CVP by completing the following steps. Open your browser.

1. Point your browser to the CVP IP address or hostname.
2. Login to CVP. The CVP Home screen appears.
3. Click Devices.
4. Click **Comparison**.

**Figure 145: Start page for comparison of devices**

For a particular device with two chosen times, select the Two times option.

**Figure 146: Comparison of device at two chosen times**

Comparing two devices at two chosen times, select the Advanced option:

**Figure 147: Comparison of device advanced**
8.2 Running Configuration

To compare the data for the Running configuration for different devices, select **Running Config**. You have an option for current time comparison or chosen times comparison.

![CloudVision Portal](image)

**Figure 148: Comparison of Running configuration for two devices**

- **Supported Snapshots**

8.2.1 Supported Snapshots

All Snapshots give the list of snapshots, its capture time and its last executioner in the following figure.

![CloudVision Portal](image)

**Figure 149: All Snapshots options**

8.3 Snapshots

On the CloudVision portal, navigate to Devices > Comparison to **Snapshots** to view the snapshot for the device.
The screen provides the following functionalities:

- All Snapshots: Displays all current snapshots options
- Snapshots Filter: Select the required snapshot filter

### 8.4 ARP Table

On the Cloud Vision portal, navigate to **Devices > Comparison** to ARP Table to view the information about ARP. Arista’s device comparison platform for ARP table compares data between two devices at the same time and at different time settings.

You can compare the following:

- Device's IP Address
- Device's MAC Address
- Interface

### 8.5 Comparing NDP Table

On the Cloud Vision portal, navigate to **Devices > Comparison** to NDP Table to view the information about NDP. Arista’s device comparison platform for NDP table compares data between two devices at the same time and at different time settings.

The components of the comparison are as follows:
- Device's IP Address
- Device's MAC Address
- Interface
- Static entry

**Figure 152: Comparing NDP table**

You can compare the status at the current time against the following times:
- 30 minutes
- 1 hour
- 2 hours
- 12 hours and
- 24 hours ago.

**Figure 153: Comparing same device for NDP table for different times**

### 8.6 MAC Address Table

On the Cloud Vision portal, navigate to **Devices > Comparison** to MAC Address Table to view the information about MAC addresses for the devices. Arista's device comparison platform for MAC Address table compares data between two devices at the same time and at different time settings.

The components of the comparison are as follows:
- VLAN
- Device's MAC Address
- Type of the VLAN
- Port
- Number of moves on the Port
- Timing for last movement
You can compare the status at the current time against the following times:

- 30 minutes
- 1 hour
- 2 hours
- 12 hours and
- 24 hours ago.

Status is shown by added, removed and modified entries.
8.7 VXLAN Table

On the Cloud Vision portal, navigate to **Devices > Comparison** to VXLAN Table to view the information about MAC addresses for the devices.

The components of the comparison are as follows:

- VLAN VNIs
- VXLAN MAC Address

You can compare the status at the current time against the following times:

- 30 minutes
• 1 hour
• 2 hours
• 12 hours and
• 24 hours ago.

Status is shown by added, removed and modified entries.

Figure 160: Comparing same device for different times and status

To show all entries for the devices, Click ALL.

Figure 161: Showing all entries for the Devices for VXLAN table

8.8 Viewing Device IPv4 Routing Table

From the Comparison screen, you can quickly drill down to view details about IPv4 Routing from different devices. In tabular view, click the device names to compare the corresponding device details.
Figure 162: Comparing IPv4 routing table for different devices

The screen refreshes to show the status, IP address and functions it does for Nexthop. Status is generally shown by Static, Martian, Connected, Receive and Receive Broadcast.

Figure 163: Comparing IPv4 Routing table for different times for two devices

You can compare the status at the current time against the following times:

- 30 minutes
- 1 hour
- 2 hours
- 12 hours and
- 24 hours ago.

Status is shown by added, removed and modified entries.
8.9 Viewing Device IPv6 Routing Table

From the Comparison screen, you can quickly drill down to view details about IPv6 Routing from different devices. In tabular view, click the device names to compare the corresponding device details.

The screen refreshes to show the status, IP address and functions it does for Nexthop. Status is generally shown by Static, Martian, Connected, Receive and Receive Broadcast.

You can compare the status at the current time against the following times:

- 30 minutes
- 1 hour
- 2 hours
- 12 hours and
- 24 hours ago.

Status is shown by added, removed and modified entries.
8.10 Comparing IPv4 Multicast Table

On the Cloud Vision portal, navigate to Devices > Comparison to IPv4 Multicast Table to view the information about Multicast. Arista’s device comparison platform for IPv4 Multicast table compares data between two devices at the same time and at different time settings.

The components of the comparison are as follows:

- Sparse Mode PIM
- Static

You can compare the status at the current time against the following times:

- 30 minutes
- 1 hour
- 2 hours
- 12 hours and
- 24 hours ago.
Figure 169: Comparing same device for IPv4 Multicast table for different times
Network Compliance (CVP)

CloudVision continuously computes device configuration and image compliance; and updates compliance status automatically in response to changes in the network.

Configuration compliance is triggered in the following circumstances:

- A configlet is assigned to either a device or Container
- Configlet content changes affect all devices to which the configlet has been mapped
- EOS image version changes due to an image upgrade or downgrade
- A device restarts streaming after you make the changes mentioned above

Compliance statuses of image and switch configuration are computed when the following entities are edited:

- Running or designed configurations
- Extensions or EOS versions

**Note:** The compliance status of device and parent container icons update automatically.

Image compliance is triggered in the following circumstances:

- An image bundle is either applied or removed from either device or container
- Edited mage bundle content
- Edited either device, EOS version, or extensions

The Compliance Overview dashboard from the Devices tab presents the number of devices and their compliance status in the following categories:

- Bug Exposure
- Security Advisories
- Configuration Compliance
- Image Compliance

Sections in this chapter include:

- Device Compliance
- Notifications for Container-level Compliance Checks and Reconciles
- Compliance Dashboard
- Print Compliance Dashboard
- Setup for Automatic Sync of Compliance Bug Database

### 9.1 Device Compliance

In CloudVision Portal (CVP), devices have a compliance status which indicates whether the running configuration and image of a device is different from the designed (managed) configuration and image for the device.

The possible device compliance statuses are:

- **Compliant:** Devices in which the running configuration and image are identical to the designed configuration and image for the device.
• **Non-compliant**: Devices in which the running configuration or image are different from the designed configuration or image for the device

When you edit running and designed configurations of provisioned devices, CloudVision automatically computes the difference and updates the compliance status in response to changes in the network. CVP provides device compliance status indicators to easily identify non-compliant devices and the functionality required to bring non-compliant devices into compliance. One process used to resolve the difference in running and designed configuration is referred to as reconciling.

For more information, see:

• [Device Compliance Status Indicators](#)
• [Device Compliance Checks](#)

### 9.1.1 Device Compliance Status Indicators

CloudVision Portal (CVP) provides device compliance status information in both the **Network Provisioning** screen and the **Inventory** screen (list view).

#### 9.1.1.1 Network Provisioning Screen Compliance Status Indicators

The **Network Provisioning** screen (topology view) utilizes color coding to indicate the presence of compliance alerts on devices. A compliance alert on a device indicates that the running configuration or image is different from the designed configuration or image for the device. This feature enables you to easily see if a device has a compliance alert.

In addition to using color codes for device icons, CVP also uses color codes for container icons to indicate that a device within the container has a compliance alert. If a device within a container has an active alert, the container inherits the alert color of the device. For example, if a device within a container has a configuration mismatch, the container inherits the alert color used to indicate a configuration mismatch.

This feature enables you to easily see if a device within a container has an alert, even if the device is not visible. It also prevents you from having to open a container to see if a device within it has an alert.

**Note**: Containers only inherit the alert color of a device if the device is directly underneath the container in the hierarchy. If the device is not directly underneath the container in the hierarchy, the container does not show the alert notification color of the device.

For descriptions of the color codes used to indicate compliance status, see:

• [Device Icon Compliance Status Color Codes](#)
• [Container Icon Compliance Status Color Codes](#)

#### 9.1.1.2 Representation Under Show All Devices

The image below shows the representation of device compliance status information for devices that are only visible by accessing **Show all devices**. The statuses shown are the same as those shown using device icons in the topology view.

![Figure 170: Show All Devices display of device compliance status](#)...
9.1.1.3  Representation in List View

The image below shows the representation of device compliance status information when using the List View. The statuses shown are the same as those shown using device icons in the Topology view.

![List View display of device compliance status](image)

Figure 171: List View display of device compliance status

9.1.1.4  Removing Compliance Indicators

The Network Provisioning screen shows non-compliance whenever there is a mismatch between the running configuration or image and designed configuration or image of devices in the topology. To remove compliance indicators, reconcile the configuration of any devices that have a configuration mismatch.

Note: Compliance indicators are removed from the display only when there is no configuration mismatch.

9.1.1.5  Representation Under Show All Devices

The image below shows the representation of device compliance status information for devices that are only visible by accessing Show all devices. The statuses shown are the same as those shown using device icons in the topology view.

![Show All Devices display of device compliance status](image)

Figure 172: Show All Devices display of device compliance status

9.1.1.6  Device Icon Compliance Status Color Codes

The color of the device icon indicates the compliance status of the device. This table lists and describes the device icon color codes:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="gray.png" alt="Gray" /></td>
<td>The compliance status is normal (no compliance alert).</td>
</tr>
<tr>
<td><img src="orange.png" alt="Orange" /></td>
<td>The device has a configuration mismatch (the running configuration or image are different from the designed configuration or image for the device).</td>
</tr>
</tbody>
</table>
No task to resolve the mismatch is associated with the device.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No task to resolve the mismatch is associated with the device.</td>
</tr>
</tbody>
</table>

Orange (with task)
The device has a configuration mismatch (the running configuration or image are different from the designed configuration or image for the device). A task to resolve the mismatch is associated with the device.

See Representation Under Show All Devices for how this status is shown when using the Show All Devices option.

9.1.1.7 Container Icon Compliance Status Color Codes

The figure below shows a container that has a device within it that has an alert. In this example, the alert color is yellow, which indicates one of the following:

- A device within the container has a configuration mismatch.
- A device within the container has a configuration mismatch, and there is a task associated with the device to resolve the mismatch.

Figure 173: Container showing alert color

9.1.2 Device Compliance Checks

CloudVision Portal (CVP) enables you to see if devices are non-compliant by performing compliance checks at the device level and at the container level.

9.1.3 Device Access Alerts

The Network Provisioning screen shows device access alerts whenever a device is no longer reachable by CVP. This enables you to easily identify unreachable devices in the screen. Any device that is no longer reachable is represented on the screen using a color coded device icon.

This table lists and describes the color codes used for unreachable devices:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Like device compliance status alerts, CVP also uses color codes for container icons to indicate that a device within the container is unreachable. If a device within a container has an access alert, the container inherits the alert color of the device (red).

This feature enables you to easily see if a device within a container has an alert, even if the device is not visible. It also prevents you from having to open a container to see if a device within it has an alert.

**Note:** Containers only inherit the alert color of a device if the device is directly underneath the container in the hierarchy. If the device is not directly underneath the container in the hierarchy, the container does not show the alert notification color of the device.

### 9.2 Notifications for Container-level Compliance Checks and Reconciles

CloudVision Portal (CVP) provides notifications for container-level compliance checks and reconciles. When a container-level compliance check or reconcile is completed, CVP automatically generates a notification message, indicating that the action has occurred.

Because container-level compliance check or reconciles are not tracked by tasks, you track them using automated notifications. The notifications can be accessed directly from the Network Provisioning screen by clicking the **Notifications** icon. The presentation of the icon indicates whether there are unread notifications.

![Notification Icons]

**Figure 174: Read and Unread Notification Icons**

The notification list provides the following information:

- Current actions in progress, with a progress bar.
- Unread notifications (shaded in blue).
- Previously viewed notifications (no shading). These are shown at the bottom of the list.

The type of action (Check **Compliance** or **Reconcile**) is indicated for each notification.
Figure 175: List of notifications

Note: To view notifications for the previous CVP session, click the bell icon and choose View History.

For information on container-level compliance checks and reconciles, see:

- Device Compliance Checks

9.3 Compliance Dashboard

When you edit running and designed configurations of provisioned devices, CloudVision automatically computes the difference and updates the compliance status in response to changes in the network.

The Compliance dashboard displays the real-time summary view of image, configuration and security compliance for all managed devices. The assessment uses bug details published on https://www.arista.com and leverages the network wide database to compute the exposure based on hardware and software versions. The CVP 2020.2.0 release comes packaged with a file named AlertBase.json which contains information about software defects and security vulnerabilities. See the figure below.
The Compliance Dashboard screen displays graphical and tabular presentation of bugs alerts.

Note: You can filter bug alerts using All Alerts, Unacknowledged Alerts, and Acknowledged Alerts dropdown options available next to breadcrumbs.

The compliance dashboard table consists of Bug Alerts and Device Configuration tabs.

Bug Alerts

The Bug Alerts tab provides the following information:

- **Identifier**: Bug number for issues tracked.
  
  Note: The checkmark next to identifier ID signifies acknowledged bugs.

- **Type**: Identifies the type of bug. Security vulnerabilities are tracked by type CVE. Software defects are tracked by type Bug. This field can be used to filter on either of these types.

- **Summary**: Provides a description of the software defect/security vulnerability.

- **Severity**: Calls out the severity of the software defect.

- **Device Count**: Lists the number of devices impacted by the tracked issue.

  Note:
  
  - If a device is acknowledged in tracked issues, this count is decreased by one.
  - If the bug is acknowledged, CVP displays zero.
  - Unacknowledged actions undo these results.

- **Exposed Devices**: Lists the names of devices impacted by the software defect or security vulnerability.

  Note:
  
  - If a device is acknowledged in tracked issues, CVP does not list its name.
  - If a bug is acknowledged, CVP displays None.
  - Unacknowledged actions undo these results.
  - CVP generates events for CVE bugs that are exposed on device(s). These events last until the bug either is resolved on the device or is acknowledged.

Click the listed bug alert to view more details from the corresponding Bug Alert - Identifier ID pop-window. See the figure below.
You can fix listed bugs through one of the following ways:

- Upgrading your device to versions mentioned under **Version(s) Fixed**
- Installing the hotfix available at [https://www.arista.com/en/support/advisories-notices](https://www.arista.com/en/support/advisories-notices) as either a part of an image bundle or directly using the EOS CLI.

**Note:** You can search for hotfixes via identifier IDs.

Click the **Acknowledge Bug on n Device(s) and Close** button to hide the corresponding bug from bug info in selected devices.

**Note:**
- **n** presents the count of selected devices.
- (Optional) Provide reasons for acknowledgement in the text box.
- To undo the acknowledgement, reopen the bug to select acknowledged devices and click the **Unacknowledge Bug on n Device(s) and Close** button.

To acknowledge a bug for all current and future devices, select **Always acknowledge instances of this alert** checkbox and click **Save and Close** button.

**Note:**
- (Optional) Provide reasons for acknowledgement in the text box.
- To undo the acknowledgement, reopen the bug, unselect the checkbox, and click **Save and Close**.

The list of software defects and security vulnerabilities affecting a device are also available in the device view under the Compliance section.

**Note:** A checkmark is displayed next to an Identifier ID when either the bug is acknowledged or the current device is acknowledged for the corresponding bug.
Device Configuration

The **Device Configuration** tab displays the following information:

- **Device** - Lists the hostnames of devices.
  - **Note**: Clicking on a device name opens the Running Configuration screen.

- **Status** - Displays the device status on configuration compliance.
  - **Note**: CVP tracks out of sync status for configuration, image, and extensions.

- **Last Compliance Check** - Displays the timestamp of last compliance check.

**Figure 179: Device Configuration Tab**

### 9.4 Print Compliance Dashboard

Perform the following steps to print the Compliance dashboard:
1. Select **Print** from the browser menu. CVP displays the Print pop-up window. See the figure below.

Figure 180: Print Pop-Up Window

2. Select your printer from the **Destination** dropdown menu to print the screen.

   **Note**: To save a print-friendly version of the screen, select **Save as PDF** from the **Destination** dropdown menu. This PDF contains all rows of the compliance table.

3. Click **Save**.

### 9.5 Setup for Automatic Sync of Compliance Bug Database

In order to keep the bug database up to date and receive real-time assessments on exposure to software defects and security vulnerabilities, an automated sync can be configured between CVP and [https://www.arista.com](https://www.arista.com) using a token-based authentication and proxy URL.

Figure 181: Configuring Compliance Settings
The Compliance screen has a compliance section that accepts the following information:

- An authentication token generated by www.arista.com to enable CVP to keep its bug database up-to-date.
- Proxy URL to reach the update server at www.arista.com.

This token is generated per user and can be obtained from the user profile screen under the Portal Access section on www.arista.com.

![Authentication Token](image)

**Figure 182: Compliance Portal Access**

When this token is provided in the Compliance settings screen, it allows CVP to download the latest version of the https://www.arista.com/en/login file that is available on the Software downloads page.

**Note:** To leverage automatic updates of the compliance bug database, connectivity to www.arista.com should be ensured from the CVP VM.

The version and release date of the compliance bug database in use can be viewed in the Settings screen under **Telemetry Browser > analytics > BugAlerts > update**.

![Telemetry Browser Screen](image)

**Figure 183: Telemetry Browser Screen**
Network Provisioning (CVP)

The Network Provisioning Screen presents a hierarchical view of the network configuration.

It is not a network topology; it is a configuration tree view. The switches at the bottom of the tree inherit the configuration specified in the containers above them as well as the configuration that is specific to them. The containers and switches all have sub menus that are accessed by right mouse clicking on them. The main features of the screen are described below.

Note: Switches that have been added to the network from new will ZTP boot using generic details from CVP and appear in the Undefined container.

- Network Provisioning View
- Container Level Actions
- Device Bootstrap Process
- Device-level Actions
- Replacing Switches Using the ZTR Feature
- Managing Configurations
- Configuration Validation
- Using Hashed Passwords for Configuration Tasks
- Reconciling Configuration Differences
- Managing EOS Images Applied to Devices
- Rolling Back Images and Configurations
- Device Labels
- Viewing Containers and Devices
- Network Search
- Management IP

10.1 Network Provisioning View

The topology view of the Network Provisioning screen is a tree structure that consists of containers and devices. This view represents the current groupings of devices (devices grouped by container) as well individual devices.

By default, two types of containers are available in the topology view.

- Tenant: Top-most container.
- Undefined: Container for all devices that have registered themselves with the CloudVision Portal using Zero Touch Provisioning (ZTP) and are awaiting configuration. Undefined containers are shown in the view in a different color than defined containers.

The example shown below includes:

- One tenant container (there is always only one tenant container).
- Three containers under the tenant container (one of the three is an undefined container).
- Seven devices (one is under the undefined container, and 6 are grouped under the container named Vantage-DC (6)).
Figure 184: Network provisioning view showing tree structure

Note: Different color icons are used to indicate that devices have compliance alerts or access alerts.

For more information, see:
- Network Provisioning Screen Options
- Changing Between Network Provisioning View and List View

Related topics:
- Container Level Actions
- Device-level Actions
- Viewing Containers and Devices

10.1.1 Network Provisioning Screen Options

The following options are available from the Network Provisioning screen.

- **Device Management**  Lists all the switches that reside below the selected container level, these could belong to the selected container or reside in containers within the selected container.
- **Configlet Management** Lists the configlets associated with the selected container or if a switch is selected all of the configlets applied to it both directly and inherited.
- **Image Management** Lists the EOS or vEOS software image associated with a container or switch. Switches below the container selected will be loaded with this image.
- **Label Management** Lists the system or custom labels associated with the selected container or switch.
- **Refresh and Listview** Refresh the current screen to show any updates or changes to the switches or devices. Listview changes the display from Topology View and displays the switches in a list.
- **Containers** Containers are the basic logical construct of the topology view. They are used to used group devices and to apply configurations and deploy images to the device groups.
- **Container Right Click Options:**

  - **Show From Here** Changes the display to show only the containers and switches below the selected container.
  - **Expand / Collapse** toggles between shrinking or growing the tree topology below the selected container.
  - **Show All Devices** Lists the switches that are associated with that specific container. The container turns blue if it contains more than five switches and will only display 25 of the total number of switches in the topology structure.
  - **Container: Add / Delete** Create or remove a container that from the selected container.
• **Device: Add / Manage**  Add a device to the selected container or manage the switches already associated with the container. The manage option displays a list of switches which can be selected by enabling the tick box on the left-hand side. The selected switches can then be moved to another container, reset (returned to a ZTP boot state and associated with the undefined container), or removed from CVP completely.

• **Manage: Configlet / Image Bundle**  Allocate or remove a configlet or Image to or from a switch or container.

• **View Config**  View the configuration created from the combined configlets. At the container level this shows the combined configlet configuration associated with that container.

• **Check Compliance** - To initiate a compliance check on all devices under the container.

• **Reconcile** - To initiate configuration reconcile on all devices under the container.

Device Right Click Options:

• **Manage: Configlet / Image Bundle**  Allocate or remove a configlet or Image to or from a switch or container.

• **Labels**  Lists / assigns the user created labels associated with the selected switch.

• **View Config**  View the configuration created from the combined configlets. At the switch level the entire configuration that will be applied to the switch is shown.

• **Check Compliance**  Compares the current running configuration on the switch against the designed configuration in CVP. If they are out of sync the device change to an orange color.

• **Move**  Allows a user to move a switch from one container to another.

• **Factory Reset**  Erases the configuration on the switch then ZTP boots it. This will return it to the undefined container on the provisioning screen.

• **Remove**  Removes the switch from CVP. This stops CVP making changes to it and tracking its configuration. The switch is left running with its current configuration on it.

• **Replace** - To perform a Zero Touch Replacement (ZTR) of the selected device.

**Related topics:**

• **Changing Between Network Provisioning View and List View**

• **Container Level Actions**

• **Device-level Actions**

• **Viewing Containers and Devices**

**10.1.2 Changing Between Network Provisioning View and List View**

Click the icons to toggle between the topology view and the list view of the Network Provisioning screen.

**Changing to List View**

Click the List icon for a list view.
Figure 185: Changing to List View

Changing to Topology View
Click the **Topology** icon for a topology view.

Figure 186: Changing to Topology View

Related topics:
- Network Provisioning Screen Options
- Container Level Actions
- Device-level Actions
- Viewing Containers and Devices

### 10.2 Container Level Actions

Containers are a logical entity used to group network devices and to define a hierarchy to which configurations can be applied. When you apply a configlet to a container, the configlet is automatically applied to all of the devices in the container's hierarchy.

Simple container implementations:
• Create a container for every datacenter.
• Within each datacenter container, create a container for every POD (leaf-spine deployment).
• Add devices that belong to each POD to the POD container. Tenant: Top-most container.

For details on how to create, rename, and delete containers, see:

• Creating a Container
• Deleting a Container
• Renaming a Container

Related topics:

• Device-level Actions
• Viewing Containers and Devices

10.2.1 Creating a Container
To create a container:

1. Select a parent container (the container to which you want to add a new container).
2. Right-click the container and choose Add > Container. The New Container dialog appears:

   ![New Container Dialog](image)

   Figure 187: New Container Dialog

3. Enter the name of the new container and select OK to create the container.
4. Click Save to apply the changes.

   Related topics:

   • Device-level Actions
   • Viewing Containers and Devices

10.2.2 Deleting a Container

   Note: Only empty containers can be deleted.

1. Locate the container to be deleted.
2. Right-click the container and click Remove.

   Related topics:

   • Device-level Actions
   • Viewing Containers and Devices

10.2.3 Renaming a Container
To rename a container in a topology:

1. Double-click the name field of the container to open the name field editor.
2. Enter a new, unique name for the container and click **Enter** to rename the container.

Figure 188: Rename Container

Related topics:
- Device Bootstrap Process
- Device-level Actions
- Viewing Containers and Devices

10.3 Device Bootstrap Process

The device bootstrap process is a process that automatically makes un-provisioned devices available for configuration through CVP. Un-provisioned devices automatically boot up in Zero Touch Provisioning mode and register themselves with the CloudVision Portal (CVP). Once they are registered with CVP, devices become available for configuration in the Undefined Container.

1. Un-provisioned devices boot into Zero Touch Provisioning mode and send out a DHCP request.

2. The DHCP server then assigns the device an IP Address and returns a URL pointing to the CloudVision portal in the bootfile-name option. The URL with IP address will be like this `//ipaddress/ztp/bootstrap`.

3. The device executes this bootstrap script and registers itself with the CloudVision Portal. At this point, the device is available in the Undefined Container.

You can now add the device to the destination container of your choice and apply the correct image and configuration to the device.

Related topics:
- Device-level Actions
- Viewing Containers and Devices

10.4 Device-level Actions

CloudVision Portal (CVP) enables you to provision devices as needed based on your current networking requirements. Some examples of the types of actions you can perform include:

- Adding devices (use this action to add devices from the undefined container to defined containers)
- Moving devices (used this action to move devices from one defined container to another defined container)
- Removing devices (removing devices from the CVP topology)
- Reset devices
- Replace devices

For details on the steps you use to perform these device level actions, see:

- Adding Devices (from Undefined Container)
- Registering Devices
- Moving Devices from one Container to Another Container
- Removing a Device from a Container
- Device Factory Reset

When resetting a device:
The device will be removed from the parent container.
- The running configuration of the device will be flushed.
- Device will reboot with ZTP mode enabled.
- Device will be identified under undefined container.

There are three options you can use to move devices. They are:

- Option 1
- Option 2
- Option 3

**Option 1:**

1. Locate the device.
2. Right-click the device and choose **Factory Reset**.

   **Figure 189: Resetting the Device (option 1)**

**Option 2:**

1. Locate the parent container.
2. Right-click the container and choose **Show All Devices**. This will list all the devices under the container.

![Figure 190: Showing all devices during factory reset (option 2)](image)

3. Right-click the device and choose **Factory Reset**.

![Figure 191: Resetting the device (option 2)](image)

**Option 3:**

1. Locate the parent container.
2. Right-click the container and choose **Manage > Device**. This will load the inventory of all the child devices under the container.
3. Select the checkbox of the device to be reset, and click the reset icon.

On saving the session, a task will be spawned to reset the selected device.

10.4.1 Adding Devices (from Undefined Container)

Adding devices from the undefined container is the most common method for adding devices to a container in the CVP topology. This method involves adding devices that are not part of the hierarchy of devices to defined containers in the CVP topology. Containers that receive the added devices are called destination containers.

Complete the following steps to add a device from the undefined container to a destination container:

1. Locate the container to which you want to add a device.
2. Right-click the container and choose Add > Device. The current inventory of undefined devices for the selected container appears.
3. Select the device and click Add.
4. Save the session.
5. Execute the Device Add task using the Task Management module to add the device to destination container.
10.4.2 Deploying vEOS Routers

CVP deploys and provisions vEOS routers from cloud and datacenter to Amazon Web Services (AWS) and Microsoft Azure. Based on the requirement in vEOS deployment, configlets are assigned for push EOS configuration along with deployment parameters such as AWS Virtual Private Cloud (VPC), subnets, and security groups.

**Note:** When CVP is deployed behind NAT devices, the vEOS telemetry configuration needs to be updated. You can view telemetry data coming from the deployed device when you configure the public IP address of CVP.

**Related Topics:**
- Prerequisites
- Adding IPsec and vEOS Licenses
- Adding AWS to Public Cloud Accounts
- Deploying the vEOS Router to AWS
- Adding Microsoft Azure to Public Cloud Accounts
- Deploying a vEOS Router to Microsoft Azure

10.4.2.1 Prerequisites

The prerequisites to deploy vEOS routers within a cloud are:

- vEOS version 4.21.1.1F or later
- **CVP 2018.2.0**
- vEOS license
- Cloud (AWS/Microsoft Azure) credentials
- vEOS deployment parameters including VPC within which the vEOS has to be deployed, subnets and security groups associated with vEOS
- IP connectivity from deployed vEOS to CVP

10.4.2.2 Adding IPsec and vEOS Licenses

The addition of an IPsec license is optional based on the deployment.

Perform the following steps to add IPsec and vEOS licenses:

1. Click the gear icon at the upper right corner of the CVP. The system displays the **Settings** screen.
2. Click **EOS Feature Licenses** in the left pane. The system displays the **EOS Feature Licenses** screen.

![Figure 194: EOS Feature Licenses Screen](image-url)
3. Click **Add License** in the right pane. The system displays the **Add License** window.

![Figure 195: Add License Window](image1)

4. Click **Select license file**. The system displays the Windows Explorer.
5. Navigate to the required location and select the license.
6. Click **Open**.
7. Select the required option from the **License type** drop-down menu.
8. Click **Upload**. The system lists uploaded licenses in the **EOS Feature Licenses** screen.

![Figure 196: Licenses Listed in EOS Feature Licenses Screen](image2)

### 10.4.2.3 Adding AWS to Public Cloud Accounts

AWS Security Token Service (STS) is required when adding an AWS account to public cloud accounts.

AWS STS gives CVP temporary access to your AWS environment with proper permissions. This allows CVP to deploy the vEOS router and related resources in your AWS VPC.

CVP calls certain AWS APIs to query VPC information and creates a vEOS router Virtual Machine (VM) in VPC. It needs an AWS IAM (Identity and Access Management) role with permissions as listed in the code below:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeRegions",
                "ec2:DescribeVpcs",
                "ec2:DescribeImages",
```
"ec2:DescribeAddresses",
"ec2:DescribeKeyPairs",
"ec2:DescribeAvailabilityZones",
"ec2:DescribeSubnets",
"ec2:DescribeSecurityGroups",
"ec2:DescribeNetworkInterfaces",
"ec2:CreateNetworkInterface",
"ec2:ModifyNetworkInterfaceAttribute",
"ec2:DetachNetworkInterface",
"ec2:DeleteNetworkInterface",
"ec2:AllocateAddress",
"ec2:AssociateAddress",
"ec2:DisassociateAddress",
"ec2:ReleaseAddress",
"ec2:RunInstances",
"ec2:TerminateInstances"
],
"Resource": "*"
}
}

---

**Note:** You receive the STS token after the IAM role is created.

Perform the following steps to add a AWS account to public cloud accounts:

1. Click **Provisioning**. The system displays the **Network Provisioning** screen.
2. Click **Public Cloud Accounts** in the left pane. The system displays the **Public Cloud Accounts** screen.

![Public Cloud Accounts Screen](image)

3. Click **Add Credentials** in the upper right corner of the right pane. The system displays the **Add Credentials** window.
4. Select **Amazon Web Services** from the **Provider** drop-down menu.

![Figure 198: Add Credentials Window for AWS](image)

5. On the **Provider Details** pane, provide the access key, secret key, and token details in the corresponding fields.

6. Click **Save**. The system displays the configured AWS account in the **Public Cloud Accounts** screen.

![Figure 199: AWS Configured in Public Cloud Accounts](image)

### 10.4.2.4 Deploying the vEOS Router to AWS

Perform the following steps to deploy the vEOS router to AWS:

1. Click **Devices**. The system displays the Inventory screen.
2. Click the **Add Devices** drop-down menu at the upper right corner of the right pane.
3. Select **Deploy vEOS Router**. The system displays the **Deploy vEOS Router** window.

![Figure 200: Deploy vEOS Router Window](image)

4. Provide the following IPSec details in the appropriate fields:
   - **Shared Secret Key (optional)** - Pre-shared key for IPSec profile
   - **Tunnel Interface IP (optional)** - IP address under tunnel interface
   - **Tunnel#1 Destination IP (optional)** - Peer's (tunnel destination) IP address
5. Click the **Select Provider** drop-down menu and select **AWS**.

![Figure 201: VM Details for AWS](image)

6. Provide the following VM details in the appropriate fields:

   - **Name** - The name of the vEOS router instance
   - **Access Key** - The access key used in the public cloud account
   - **Region** - The region that the vEOS router will be deployed in
   - **Instance Type** - The type of vEOS router that the instance will run on
   - **Key Pair Name** - The Elastic Compute Cloud (EC2) keypair used to log in to the vEOS router
   - **Amazon Machine Identifier** - The vEOS AMIs on the AWS marketplace
   - **VPC ID** - The VPC that the vEOS router will be deployed to
   - **Security Group** - The security group that will be associated with the vEOS interface
   - **Availability Zone** - The availability zone that vEOS will be deployed in
   - **Subnet #1** - The first subnet that vEOS puts Ethernet1 in
   - **Assign Public IP Address to Subnet #1** - Select Yes if you need a public IP address assigned to the vEOS router; otherwise, select No
   - **Use Public IP Address as Local ID** - The public IP address of the vEOS router

   **Note:** The system displays the public IP address of the vEOS router after the VM is created.

   - **Subnet #2 (optional)** - The second subnet that vEOS puts Ethernet2 in
   - **Configlet (optional)** - The configlet to configure vEOS once it is active
7. Click Create VM with vEOS. The system displays the status of vEOS deployment under the Progress column on the Status pane.

![Figure 202: Status of vEOS Deployment to AWS](image)

You can also check the VM deployment process on your AWS Portal. Hover the mouse over the corresponding information icon to view detailed information about the vEOS router deployment. After the successful deployment of the vEOS router to AWS, you can use your AWS SSH Privacy Enhanced Mail (PEM) key to login to vEOS.

**Note:** To make CVP manage vEOS routers, register this device using the instructions in Registering Devices. Ensure that the AWS security group associated with vEOS router VM has an ingress rule of allowing TCP port 9910 from CVP’s IP address. You must configure AWS for the vEOS router to function as a VPC gateway using the instructions in Using vEOS Router on the AWS Platform.

### 10.4.2.5 Deploying a vEOS Router to Microsoft Azure

Perform the following steps to deploy a vEOS router to the Azure VNET:

1. Click Devices. The system displays the Inventory screen.
2. Click the Add Devices drop-down menu at the upper right corner of the right pane.
3. Select Deploy vEOS Router. The system displays the Deploy vEOS Router window.
4. Provide the following IPSec details in the appropriate fields:
   - **Shared Secret Key** (optional) - Pre-shared key for IPSec profile
   - **Tunnel Interface IP** (optional) - IP address under tunnel interface
   - **Tunnel#1 Destination IP** (optional) - Peer’s (tunnel destination) IP address
5. Select Azure from the Select Provider drop-down menu.

![Figure 203: VM Details for Microsoft Azure](image)
6. Provide the following VM details in the appropriate fields:
   - **Name** - The name of the vEOS router instance.
   - **Subscription ID** - The subscription that the vEOS router will be deployed to.
   - **Instance Size** - The size of vEOS router that the instance will run on.
   - **Resource Group** - The resource group that the vEOS router will be deployed to.
   - **Location** - The Azure region that contains the VNET.
   - **Security Group** - The network security group that will be associated with the vEOS interface.
   - **Virtual Network** - The VNET that vEOS will be deployed in.
   - **Subnet #1** - The first subnet that vEOS puts Ethernet1 in.
   - **Assign Public IP Address to Subnet #1** - Select Yes if you need a public IP address assigned to vEOS router, else select No.
   - **Use Public IP Address as Local ID** - The public IP address of vEOS Router.
     *Note:* The system displays the public IP address of vEOS router after the VM is created.
   - **Subnet #2** - The second subnet that vEOS puts Ethernet2 in.
   - **Configlet** - The configlet to configure vEOS once it is up.
   - **EOS Image** - The vEOS images on Azure marketplace.

7. Click **Create VM with vEOS**. The system displays the status of vEOS deployment under the Progress column in the Status pane.

![Figure 204: Status of vEOS Deployment to Microsoft Azure](image)

You can also check the VM deployment process on your Microsoft Azure Portal. Hover the mouse over the corresponding information icon to view detailed information about the vEOS router’s deployment. It contains the initial login credentials you can use to login to vEOS router, you can change the credentials after logging into the device.

*Note:* To make CVP manage vEOS routers, register this device using the instructions in **Registering Devices**. Ensure that the Azure network security group associated with vEOS router VM has an ingress rule of allowing TCP port 9910 from CVP’s IP address. You must configure Microsoft Azure for the vEOS router to function as VNET gateway using the instructions in **Using the vEOS Router on Microsoft Azure**.

### 10.4.2.6 Adding Microsoft Azure to Public Cloud Accounts

You need a subscription ID, a tenant ID, a client ID, and client server details in order to an azure account to public cloud accounts.

To get these details, you must create an application in the Azure active directory and assign proper permissions to CVP for authentication with Microsoft Azure environment to make API calls. CVP uses a few APIs to create a vEOS router. Therefore, you must add a contributor role to the resource group that has either Virtual Network Protocol (VNET) or the whole subscription.

Perform the following steps for adding the Microsoft Azure account to public cloud accounts:

1. Click **Provisioning**. The system displays the **Network Provisioning** screen.
2. Click **Public Cloud Accounts** in the left pane. The system displays the **Public Cloud Accounts** screen.
3. Click **Add Credentials** in the upper right corner of the right pane. The system displays the **Add Credentials** window.

![Add Credentials Window](image)

**Figure 205: Add Credentials Window for Microsoft Azure**

4. Select **Azure** from the **Provider** drop-down menu.

5. Under the **Provider Details** pane, provide the subscription ID, tenant ID, client ID, and client server details in the appropriate fields.

6. Click **Save**. The system displays the configured Microsoft Azure account in the **Public Cloud Accounts** screen.

![Public Cloud Accounts](image)

**Figure 206: Microsoft Azure Configured in Public Cloud Accounts**

### 10.4.3 Registering Devices

Registering is the method used for adding devices to CVP. As a part of registering devices, CloudVision automatically enables streaming of the registered devices' state to the cluster by installing and configuring the TerminAttr agent. Newly registered devices are always placed under an undefined container.

**Note:** Manual installation or configuration of streaming telemetry is not required prior to registration.

Complete the following steps to register devices with CVP:

1. Navigate to the **Inventory** screen.
2. Click the **Add Device** drop-down menu and select **Register Existing Device**. The **Device Registration** pop-up window appears.

Figure 207: Add Device for Registration
3. Enter the host name or IPv4 addresses of the device(s) to be registered; and click **Register**.

![Figure 208: Selecting Device for Registering](image)

The following figures show the device registration status through the registration process.

![Figure 209: Registration Status](image)

![Figure 210: Registration Successful](image)

The newly registered devices are now shown in the inventory.
The newly registered devices are shown in the undefined container in the Network Provisioning view.

10.4.4 Moving Devices from one Container to Another Container

Moving devices from one defined container to another is a method you can use to add devices to a container in the CVP topology. You use this method when you want to add devices to a container, and the device you want to add is currently under another container in the CVP topology. This method involves locating the device to be moved, and then moving it to the destination container. Containers that receive the imported devices are called destination containers.

There are three options you can use to move devices. They are:

- Option 1
- Option 2
- Option 3

10.4.4.1 Option 1

1. Locate the device.
2. Right-click the device and choose Move.

3. Select the destination container from the drop-down menu.
4. Save the session to move the device to the destination container.

10.4.4.2 Option 2

1. Locate the container that has the device you want to move.
2. Right-click the container and choose Show All Devices. This will load the inventory of all the devices under the container.
3. Locate the device to be moved.
4. Right-click the device and choose Move. After moving there will be a “T” icon to indicate the move has been tasked. (The task won't automatically be executed.)

Figure 214: Device with pending move task (option 2)

5. Go to Tasks and explicitly execute the move task. After the task has been executed, the “T” icon is removed.

10.4.4.3 Option 3
1. Locate the container that has the device you want to move.
2. Right-click the container and choose **Manage > Device**. This will load the inventory of all the devices under the container.
3. Select the device to be moved and click **<— >** to choose the destination container.
4. From the popup menu, select the destination container and click **OK**. This will provision a move for the device.

### 10.4.5 Removing a Device from a Container

A device can be removed from a container. Removing a device from the container will:

- Remove the device from parent container.
- Clear all information about the device in the CloudVision Portal.
- Stop any monitoring of the device.

There are three options you can use to remove devices. They are:

- **Option 1**
- **Option 2**
- **Option 3**

#### 10.4.5.1 Option 1

1. Locate the device.
2. Right-click the device and choose **Remove**.

![Figure 215: Removing a device (option 1)](image)

#### 10.4.5.2 Option 2

This option is available only for topology views.

1. Locate the parent container.
2. Right-click the container and choose **Show All Devices**. All the devices under the container are listed.

![Diagram showing how to select a device](image)

**Figure 216: Selecting the device to be removed (option 2)**

3. Select the device you want to remove.
4. Right-click the device and choose **Remove**. The device is removed from the Network Provisioning view.

![Figure 217: Removing the device (option 2)](image)

10.4.5.3 **Option 3**

This option is available only for the list view of the Network Provisioning screen.

1. Locate the parent container.
2. Right-click the container and choose **Manage > Device**. This will load the inventory of all the child devices under the container.

![Figure 218: Remove device from the container (option 3)](image)

3. Select the device you want to remove and then click **Remove**. On saving the session, a task will be spawned to reset the selected device.
10.4.6 Device Factory Reset

When resetting a device:

- The device will be removed from the parent container.
- The running configuration of the device will be flushed.
- Device will reboot with ZTP mode enabled.
- Device will be identified under undefined container.

There are three options you can use to move devices. They are:

- Option 1
- Option 2
- Option 3

10.4.6.1 Option 1

1. Locate the device.
2. Right-click the device and choose Factory Reset.

![Figure 219: Resetting the device (option 1)](image)

10.4.6.2 Option 2

1. Locate the parent container.
2. Right-click the container and choose **Show All Devices**. This will list all the devices under the container.

![Figure 220: Showing all devices during factory reset (option 2)](image)

3. Right-click the device and choose **Factory Reset**.

![Figure 221: Resetting the device (option 2)](image)

**10.4.6.3 Option 3**

1. Locate the parent container.
2. Right-click the container and choose **Manage > Device**. This will load the inventory of all the child devices under the container.
3. Select the checkbox of the device to be reset, and click the reset icon. On saving the session, a task will be spawned to reset the selected device.

![Figure 222: Selecting the device and resetting it (option 3)](image)

**10.5 Replacing Switches Using the ZTR Feature**

The Zero Touch Replacement (ZTR) feature enables you to replace switches without having to configure the new switch. When you replace a switch using this feature, the new switch assumes the identity (IP), image, and configuration of the old switch. You use the Network Provisioning screen to replace switches using the (ZTR) feature.

**Pre-requisites:** Before you can begin the process to replace a switch using ZTR, make you must complete the following steps:

1. Make sure that the old switch is physically powered down and is not physically connected to the network.
2. Physically connect the new switch to the network exactly as the old switch was connected.
3. Power on the new switch.
4. Make sure the new switch comes up using ZTP, and that it shows up in the undefined container as an available resource.

Complete these steps to replace a switch using ZTP:

1. Go to the **Network Provisioning** screen.
2. Right-click on the old switch, and select **Replace**. This initiates ZTR, and opens the **Undefined Device** screen.

![Figure 223: Selecting the switch to be replaced](image)
3. Select the new switch by checking the checkbox next to the Serial No. column, and then click Replace.

Figure 224: Selecting the new device and replacing the old device

4. In the Network Provisioning screen, click Save. A task icon T shows on the old switch, indicating that a task to replace it has been scheduled. Also, an R icon shows on the new switch, indicating that it is the replacement switch for a scheduled ZTR task.

Figure 225: Topology view showing device with pending replace task

5. Go to the Tasks screen.
6. Select the task and click the play icon to execute the task.

While the task is executing, you can open the logs for the task to view how ZTR manages the replacement. ZTR first pushes the old switch's image and configuration to the new replacement switch, and then initiates the reboot.

![Figure 226: Task log showing processing of device replacement](image)

### 10.6 Managing Configurations

CloudVision Portal (CVP) enables you to manage configurations by assigning configurations to containers and to devices. Configurations that you assign to containers are applied to all devices under the container's hierarchy. CVP also enables you to easily view the configuration currently assigned to containers and devices.

- Applying Configurations to Containers
- Viewing the Configuration Applied to Devices
- Applying Configurations to a Device

#### 10.6.1 Applying Configurations to Containers

Applying configurations to containers involves adding Configlets to containers or removing Configlets from containers.

**Adding Configlets**

1. Locate the container.
2. Right-click the container and choose Manage > Configlet. This will open the window display the inventory of configlets.
3. Select the configlet and click Update. This will provision configlet add for the container and all the devices under it.

**Removing Configlets**

To remove the configlet inventory from a container.

1. Locate the container.
2. Right-click the container and choose Manage > Configlet.
3. Remove the configlets.
4. Click Update.

![Figure 227: Remove the configlet and select Update](image)

### 10.6.2 Applying Configurations to a Device

Applying configurations to devices involves adding Configlets to devices.

**Note:** When you update a device configuration using configlets, CVP replaces the entire device configuration with the Designed Configuration for the device. For new devices with pre-existing configurations added into CVP, you must explicitly perform a one-time reconciliation to save the desired device-specific running configuration in CVP. If you do not, that configuration may be lost, or the configuration update task may fail (see Reconciling Device Configurations at the Device Level).

**Adding Configlets**

1. Select the device and choose **Manage > Configlets**.
   This loads the configlet inventory screen.
2. Select the configlets.
   You are required to validate the configuration.
3. To validate the configurations, select **Validate**.
   The validation screen will be loaded.
4. Select **Save** to propose a Config Assign action.
   When saving the session, this will spawn a Config Assign task.

### 10.6.3 Viewing the Configuration Applied to Devices

CloudVision Portal (CVP) enables you to use the Network Provisioning screen to view the configuration (Configlets) currently assigned to devices. When you view the Configlets, you can also see which Configlets are inherited from Containers, and which are applied directly to the device.

Complete the following steps to view the Configlets applied to a device.

1. Go to the Network Provisioning screen.
2. Make sure you are using the topology view, not the list view.
3. Click on the device in the topology.
4. Click the Configlet icon.

The Configlets applied to the device are listed in a drop-down list.

- If a Configlet is inherited from a Container to which the device belongs, the Container icon appears in front of the Configlet name.
- If a Configlet is directly applied to the device, no Container icon is shown next to the Configlet name.

Figure 228: Viewing the Configlets applied to a device

10.6.4 Rolling Back Configurations Assigned to a Device

CloudVision's Network Rollbacks feature enables you to restore a previous configuration to devices. You can apply the rollback to all the devices in a container, or to single devices. When you rollback a container or device, you select the date and time for the rollback and whether you want to rollback the configuration or EOS image (or both).

See Rolling Back Images and Configurations for details.

10.7 Configuration Validation

The validation screen consists of three panes.

- Pane 1: Shows the proposed configuration.
- Pane 2: Shows the designed configuration. (This shows how a resulting running configuration will look like after successful configuration push.)
• Pane 3: Shows the current running configuration of a device.

Figure 229: Validating your configurations

10.8 Using Hashed Passwords for Configuration Tasks

Some EOS commands take a password or a secret key as a parameter. There are usually two ways of passing EOS command parameters:

• As plain text.
• As a hashed string.

Note: Because EOS always returns the hashed version of the command in its running configuration, using the plain text version of commands in Configlets results in the following issues:

• CVP shows that there are configuration differences that need reconciling, even if there are none.
• Compliance checks show devices to be out of compliance.

To avoid these issues, you should use the hashed version of EOS commands in Configlets (for example, use `ntp authentication-key 11 md5 7 <key>` instead of `ntp authentication-key 11 md5 0 <key>`). Using the hashed versions of commands also keeps the real password hidden.

10.9 Reconciling Configuration Differences

CloudVision enables you to reconcile differences between the designed (managed) configuration and running configuration on devices so that CVP is maintaining the full configuration of each device.

Related topics:

• Key Terms
• Reconciling Device Configurations at the Device Level
• Reconciling Device Configuration Differences at the Container Level
10.9.1 Key Terms

<table>
<thead>
<tr>
<th>Reconcilable differences</th>
<th>Configuration differences between the designed configuration and the running configuration, which do not conflict with the configuration in any configlets, other than the reconcile configlet.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconcile configlet</td>
<td>A specially marked device configlet that is system generated and used to store reconcilable differences in order for the designed configuration to match the running configuration.</td>
</tr>
</tbody>
</table>

Reconciling device configuration differences does not require a task, because there is no configuration to be pushed out to the device. Reconcilable differences are only adjusted in the reconcile configlet, to match the running configuration. Because of this, there is no task pushed to change the running configuration.

When you reconcile device configuration differences, you add the reconcilable differences found in the running configuration to the reconcile configlet of the designed configuration.

For details on reconciling device configuration differences, see:

- Reconciling Device Configurations at the Device Level
- Reconciling Device Configuration Differences at the Container Level

10.9.2 Reconciling Device Configurations Differences at the Container Level

CloudVision enables you to reconcile device configuration differences for all devices under the hierarchy of a selected container, instead of having to initiate this device by device.

 vrij Note: The designed configurations of devices in the container that do not have reconcilable differences are not changed.

For devices that have reconcilable differences, the lines or commands on the device that are not present in the designed configuration are pulled into the reconcile configlet for that device in one of two ways:

- Using the existing reconcile configlet that is specific to that device.
- Creating a new reconcile configlet that is specific to that device. This is done when there is no existing reconcile configlet specific for the device. The system automatically creates a unique name for the configlet.

A green checkmark beside the configlet indicates it as the reconcile configlet for the device.

Complete the following steps to reconcile device configuration differences for a container:

1. Go to the Network Provisioning screen.
2. Locate the container in the topology where you want to reconcile the configurations of all devices under that container hierarchy.
3. Right-click the container, hover the cursor on Reconcile, and click either **Reconcile All** or **Reconcile New**.

![Device configuration reconciliation at the container level](image)

The **Reconcile New** option reconciles only the configuration lines that exist on the device, but not in the designed configuration.

The **Reconcile All** option reconciles new lines and also lines that differ in designed and running configurations. This usually brings the device into compliance because the resulting designed configuration will be identical to running configuration. However, there can be cases where in spite of reconciling device configuration lines, the designed configuration may not end up identical to running configuration. In these cases, no changes are made to the reconcile configlet. Arista recommends to go through the device-level reconcile process (See Reconciling Device Configurations at the Device Level), and select the desired lines.

**Note:** The bell icon in the upper right corner turns yellow to indicate unread notifications.
4. (Optional) To view the notification for the reconciliation, click the bell icon. The notification list appears showing the container-level configuration reconciliation, and any other unread notifications.

![Figure 231: List of unread notifications](image)

10.9.3 Reconciling Device Configurations at the Device Level

CloudVision enables you to reconcile device configuration differences at the device level (specific, individual devices). Configuration differences at the device level occur when there are reconcilable differences in the running configuration of the device.

The Configuration Validation screen shows details of the configuration differences. When the system identifies a reconcilable difference, the Reconcile option becomes available, and the extra reconcilable configuration is listed in a text editor on the screen.

Reconcile Configlets

You use a type of configlet called a reconcile configlet to reconcile device configuration differences at the device level. A reconcile configlet is a configlet for a single specific device, and is explicitly marked as the reconcile configlet for that device. The reconcile configlet for a device contains the additional running configuration for that device.

Note: There is only one reconcile configlet for any device. It is the only configlet that contains the additional running configuration for the device.

Every time a device-level or a container-level reconcile is performed, the reconcile configlet for each device included in the reconcile action is modified to include the extra running configuration.

To reconcile device level configuration, perform the following steps:

1. If required, select additional lines from running configuration to reconcile.
2. Click the blue **Reconcile** button to add the reconcilable configuration in the running configuration to the reconcile configlet of the designed configuration.

![Figure 232: Configuration validation screen showing device-level configuration differences](image)

3. (Optional) Click **Edit** next to the configlet name to edit or rename the reconciled configlet.

4. (Optional) Click the reconcile disk icon next to the configlet name to save the reconciled configlet with the extra commands present in the running configuration.

![Figure 233: Reconcile Disk icon](image)

**Note:** CVP will not execute pushing a configuration that causes CVP to lose connectivity with the device if the management interface or IP is missing in the configuration. When the task is executed, it will fail.

5. Click **Save**.

**10.10 Managing EOS Images Applied to Devices**
CloudVision enables you to efficiently manage the EOS images of devices by assigning image bundles to containers or devices in the current CloudVision network topology. An image bundle assigned to containers are automatically applied to all devices under that container.

The image bundle you want to apply must already exist in the set of current EOS image bundles.

The following tasks are involved in managing the EOS image bundles assigned to devices:

- Applying an Image Bundle to a Container
- Viewing the Image Bundle Assigned to Devices
- Applying an Image Bundle to a Device
- Setting up an Image Bundle as the default for ZTP

10.10.1 Applying an Image Bundle to a Container

An image bundle can be added to, or removed from a container.

1. Select the container and choose Manage > Image Bundle. This will load image bundle inventory in topology.

   ![Image bundle inventory](image)

2. Select the bundle to be assigned to the container.
3. Click Update to provision the bundle add for the container. This action will cause a task to be created for each device in the container to upgrade it to the specified image bundle.

10.10.2 Viewing the Image Bundle Assigned to Devices

CloudVision Portal (CVP) enables you to use the Network Provisioning screen to view the image bundle currently assigned to a device. You can also see if the image bundle is inherited from a Container or assigned directly to the device.

Complete the following steps to view the image bundle applied to a device.

1. Go to the Network Provisioning screen.
2. Make sure you are using the topology view, not the list view.
3. Click on the device in the topology.
4. Click the image icon in the left pane.
   The image bundle assigned to the device is shown in a pop-up box.
   • If the image bundle is inherited from a Container to which the device belongs, the Container icon appears in front of the image bundle name.
   • If the image bundle is assigned directly to the device, there is no Container icon in front of the image bundle name.

![Figure 235: Viewing the Image Bundle assigned to a device](image)

10.10.3 Applying an Image Bundle to a Device

1. Right-click the device, then choose Manage > Image Bundle. This will open the window display the inventory of Image bundles.
   
   **Note:** Only one image bundle can be selected and assigned to a device at a time.

2. Select the bundle to be assigned to the device.
3. Click **Update** to provision the bundle add for the device.

   This action will cause a task to be created for that device to upgrade it to the specified image bundle.

10.10.4 Setting up an Image Bundle as the default for ZTP

Since all devices must run this image, you must apply the image at the tenant level.

1. Go to the **Network Provisioning** screen.
2. Right-click the **Tenant** container and choose **Manage > Image Bundle**.
3. Select the bundle you created and click **Update**.
4. Click **Preview** to verify the changes before saving the changes.
5. Click **Save** to apply the changes.

10.11 Rolling Back Images and Configurations

CloudVision Network Rollbacks feature enables you to restore a previous EOS image and configuration to containers and devices. You can apply the rollback to all the devices in a container,
or to single devices. When you rollback a container or device, you select the date and time for the rollback and whether you want to rollback the EOS image or configuration (or both).

CloudVision supports rollback to any previous point in time irrespective of captured snapshots. However, rollback is possible to a point that is far beyond the CloudVision Cluster update to 2018.2.0 only when your devices are upgraded to TerminAttr 1.4+ long before that.

**Note:** To help you select the desired rollback destination day and time, you can compare the image and running configuration differences between current and rollback times of all effected devices. The potential destination rollback date and time in the comparison is based on the destination rollback date and time you select.

### 10.11.1 Rolling Back Container Images and Configurations

Complete the following steps to apply a network rollback in containers:

1. Go to the **Network Provisioning** screen.
2. Right-click on the container you want to rollback, and then choose **Manage > Network Rollback**.

![Figure 236: Network Rollback Screen](image)

3. Using the Rollback Type: options near the top of the screen, select the type of rollback. The options are:
   - Configuration & Image Rollback (both the configuration and EOS image are rolled back)
   - Configuration Rollback (only the configuration is rolled back)
   - Image Rollback (only the EOS image is rolled back)
4. Either drag the vertical slider on the timeline to the desired date and select the time for rollback; or use the Rollback to menu for selecting rollback date and time (directly above the configuration pane on the left side).
5. Click the telemetry icon (directly above the configuration pane on the right side) for viewing the running configuration differences between current and rollback times.
6. If required, change the destination date and time for the rollback.
7. Click **Create CC** to create a Change Control (CC) record for the network rollback. CloudVision automatically creates a rollback task for each device in the rollback; and makes them part of CC.

**Note:** Rollback Change Controls are automatically assigned a unique name. You can rename the Change Control record by editing the Change Control record. Once the Change Control is created, it can be executed like any other Change Control.
10.11.2 Rolling Back Device Images and Configurations

Complete the following steps to apply a rollback in devices:

1. Go to the **Network Provisioning** screen.
2. Right-click on the device you want to rollback, and then choose **Manage > Rollback**.

   ![Figure 237: Device Rollback Screen](image)

3. Using the **Rollback Type** options near the top of the screen, select the type of rollback. The options are:
   - Configuration & Image Rollback (both the configuration and EOS image are rolled back)
   - Configuration Rollback (only the configuration is rolled back)
   - Image Rollback (only the EOS image is rolled back)

4. Either drag the vertical slider on the timeline to the desired date and select the time for rollback; or use the **Rollback to** menu for selecting rollback date and time (directly above the **configuration** pane on the left side).
5. Click the telemetry icon (directly above the configuration pane on the right side) for viewing the running configuration differences between current and rollback times.

Figure 238: Differences in Running Configuration

The Unified tab displays running configuration differences in a single window with differences highlighted. The Split tab displays running configurations in different windows with differences highlighted.

6. If required, change the destination date and time for the rollback.
7. Click Save to create a task for the device rollback.

10.11.3 Rolling Back Configurations Assigned to a Device

CloudVision's Network Rollbacks feature enables you to restore a previous configuration to devices. You can apply the rollback to all the devices in a container, or to single devices. When you rollback a container or device, you select the date and time for the rollback and whether you want to rollback the configuration or EOS image (or both).

See Rolling Back Images and Configurations for details.

10.12 Device Labels

A label is simply defined as Text Tags. There are two types of label:

- System labels: Assigned automatically by the system.
- Custom labels: Defined and assigned by the user.
  - Users can assign custom labels to devices from the Network Provisioning screen.
  - A device can be tagged with one or more custom labels.
  - Labels can be used to filter the devices in the Network Provisioning screen.

10.12.1 System Labels

System labels are defined by the system and are automatically applied to and removed from devices based on the following characteristics of that device:

- Software version
- Software bundle
Network Provisioning (CVP)

- Product model and family
- Assigned configlet name
- DANZ enabled
- MLAG enabled
- Parent container name

Note: System labels cannot be modified or removed by the user.

10.12.2 Custom Device Labels

You can create custom device labels and assign them to devices. The device labels you assign to a device show on the Network Provisioning screen next to the device.

10.12.2.1 Assigning an Existing Label to a Device

Complete these steps to assign an existing label to a device.

1. Select the device to be labeled.
2. Right-click the device and choose Labels.

![Choose Labels](image)

Figure 239: Choose Labels

The Assign Label pop-up menu appears, showing the available device labels.
3. Select the label to be applied and click **Save**.

![Figure 240: Assign Label](image)

The selected label will be applied to the device.

### 10.12.2.2 Creating a Custom Label for a Device

Complete these steps to create a new, custom label to a device.

1. Select the device for which you want to create a new, custom label.
2. Right-click the device and choose **Labels**.

![Figure 241: Choose Labels](image)

The Assign Label pop-up menu appears, showing the available device labels.

3. In the pop-up menu, click on **CREATE LABEL**.

![Figure 242: Create label Pop-up](image)

The Create Label dialog appears.
4. Type the new, custom label for the device, then click **Save**.

![Create Label](image)

**Figure 243: Create Label**

The new label is created and is assigned to the device.

10.12.3 **Left Pane Behavior in Network Provisioning View**

The left pane in the topology view is used to display information on the resources assigned to a given device or container.

![Left Pane View](image)

**Figure 244: Left pane view**

**Opening and Closing the Left Pane**

1. Double click the container or device to open the left pane.
2. Click the **X** button to close it.

10.13 **Viewing Containers and Devices**

The Network Provisioning screen provides you with various options that enable you to easily control the topology view so that you can view containers and devices based on your needs.

The options you use are:

- **Expand / Collapse** (see Expanding and Collapsing Containers).
• **Show From Here** (see [Show From Here](#)).
• **Show Full Topology** (see [Show Full Topology](#)).

CloudVision Portal uses color coded icons to indicate compliance or access issues with devices.

### 10.13.1 Expanding and Collapsing Containers

Containers can be expanded and collapsed within the Network Provisioning topology view so that you can change the view as needed based on your needs.

You use the **Show From Here** and **Show Full Topology** options to expand or collapse containers shown in the **Network Provisioning** screen.

The **Expand and Collapse** option is only available for the **Network Provisioning** view. It is not available for the List view.

The default view mode for containers is expanded. When you choose **Expand/Collapse** option for a container, one of the following occurs, depending on the current view mode:

- A container currently in expanded (normal) view is collapsed.
- A container currently in collapsed mode is returned to expanded view mode (the default).

Complete these steps to expand or collapse a container view from the **Network Provisioning** screen.

![Figure 245: Expanded and collapsed view of a container](image)

1. Select a container.
2. Right-click it and select the **Expand/Collapse** option.

### 10.13.2 Show From Here

The **Show From Here** option displays the topology with the selected container as the root. The hierarchy above the selected container will be hidden from the view allowing the user to only focus on the chosen container and the tree below it.

1. Select a container.
2. Right-click **Show From Here** to display the option. The hierarchy from the selected container will be displayed.

### 10.13.3 Show Full Topology

The **Show Full Topology** option allows the user to get back to the full topology view. This option will be enabled for a particular container once the user uses the show from here option on it.

1. Select a container.
2. Right-click **Show Full Topology** to view the option.
10.14 **Network Search**

In the **Network Provisioning** module, the user can use the search bar at the top of the module to find a given device or container.

10.14.1 **Search Behavior in Topology and List View**

This search is very different from rest of other search options available in topology. On user starts to type, the list of possible matches will be displayed below as an auto suggestion.

10.14.2 **Topology Search**

![Figure 246: Using search](image)

10.14.3 **List View Search**

The search behaves similar to the topology search.

For a single device search, the selected device will be listed in the grid.

![Figure 247: List view search](image)
10.14.4 Search in Other Grids

During a grid search, the user will not be provided with an auto suggest option. Only the records matching the specified data entered will be filtered and displayed in the grid.

![Figure 248: Grid searches](image)

10.14.5 Label Search

Use the search bar from the Network Provisioning screen to filter the devices based on labels. This is a contextual search.

To search a label:
1. Use the keyword Label: followed by the label name.

10.14.5.1 AND Operation

Lists all the devices which has both the labels present on it in the hierarchy.

Label: `<Label Name>` AND Label: `<Label Name>`

![Figure 249: Search AND operation](image)

10.14.5.2 OR Operation

Lists all the devices which has either one of the labels present on it in the hierarchy.

Label: `<Label Name>` OR Label: `<Label Name>`
10.14.5.3  NOT Operation

Lists all the devices which has first label one the labels present on it in the hierarchy.

Label: Label Name AND NOT Label: Label Name

10.14.6  Preview Option

All the actions performed in Network Provisioning module can be previewed before saving the changes.

To access the preview screen:

1. Select the “Preview” button.

Figure 250: Search OR operation

Figure 251: Search AND NOT operation

Figure 252: Preview option display
10.15 **Management IP**

The CloudVision Portal tracks the Management IP of each device to use in connecting to it. When this IP address changes, the device becomes unreachable by the portal. You can manually change the IP address used by the portal to communicate with a given device.

10.15.1 **Changing A Device's Management IP**

The management IP address of a device may change for one of the following reasons:

**Reason 1:**
When a device is provisioned using Zero Touch Provisioning, it may have been assigned a temporary IP address via DHCP. The CloudVision Portal will use this IP address to provision the device. Once the configuration is pushed and the device reboots, this IP address may change.

**Reason 2:**
1. If you change the device IP address directly via the switch console, CloudVision cannot record the change, and the device will become unreachable. **Current management IP** and **proposed management IP** can be used to mitigate this potential issue.

**Option 1:**
Current Management IP: The IP address used by CloudVision to communicate with a device.
1. Set the proposed IP address before pushing the configlet. This way CloudVision will try to reach the device with this IP address once configuration is pushed.

**Option 2:**
Proposed Management IP: The IP address that CloudVision uses after pushing the configlet.
1. In the Inventory Management screen and the topology, update the Management IP address. For any unreachable device, set the IP address to bring it back to the network.

10.15.2 **Setting Proposed Management IP**

You can set the Proposed Management IP while adding configlets to the device using the Proposed Management IP menu.
If you do not set the Proposed Management IP, you cannot save the configuration as not setting Proposed Management IP.

Figure 254: Setting the Proposed Management IP

1. Select the Proposed Management IP using the drop-down menu. 
   CloudVision lists the available Management IP, Loop back IP, VLAN IP, and Routed Ethernet IP.
2. Select the desired IP address.
3. Click Save.
   A task is spawned to assign the new Proposed Management IP.

10.15.3 Changing Current Management IP

1. Go to the Network Provisioning screen.
2. Select a device from topology/list view.
3. Right-click the device and choose **Manage > IP Address**

![Figure 255: Change Management IP](image)

4. A pop up will appear allowing you to manually add a new IP address.

![Figure 256: Change IP Address](image)
5. Verify the reachability of new IP address.

Figure 257: Verify IP Address
Chapter 11
Configlet Management (CVP)

Configlets are portion of configuration that CLOUDVISION user codes and maintains independently under Configlet Management inventory. These Configlets can be later applied to devices or containers in the topology.

Sections in this chapter include:
• Creating Configlets
• Configlet Information Page
• Editing Configlets
• Deleting Configlets
• Importing and Exporting Configlets

11.1 Creating Configlets

CloudVision Portal (CVP) enables you to create Configlets using two different methods. You can create Configlets using the CVP Configlet Builder feature, or you can create them manually. You should use the method that is best suited to your intended use of the Configlet.

Note: The Configlet Builder feature is designed to help you create Configlets dynamically based on variables.

For more information, see:
• About the Configlet Builder Feature
• Creating Configlets Using the Configlet Builder
• Using the Provided Configlet Builder Examples
• Python Execution Environment
• Creating Configlets Manually

11.1.1 About the Configlet Builder Feature

The Configlet Builder feature enables you to programatically create device configurations (Configlets) for devices that have relatively dynamic configuration requirements. This helps to prevent you from having to manually code Configlets.

The Configlet Builder feature is essentially a set of user interface (UI) widgets and a python script, that when used together, programatically generate Configlets for a device. The python script is embedded into a python interpreter, which is the component that generates Configlets. The UI widgets are essential if you want to use the feature to generate Configlets with user input.

Note: Using UI widgets associated with a Configlet Builder are optional. If the UI widgets are used, the generated Configlets require user input to be created.

The Configlet Builder can be used to create Configlets for both devices or containers, in the same way that static Configlets can be used with devices or containers. Configlets that are created using the Configlet Builder are executed (including the generation of Configlets) at the point when the Configlet Builder is applied to a device or container, or when a device is added to a container that contains a Configlet Builder.

11.1.2 Creating Configlets Using the Configlet Builder
The Configlet Builder enables you to create Configlets (device configurations). The example Configlet Builder shown being created configures the device’s management interface based on input you enter through the use of UI widgets.

Complete the following steps to create Configlets using the Configlet Builder:

1. Create a Configlet Builder from the Configlet page.

![Figure 258: Creating a Configlet Builder](image)

2. (Optional) Define the UI widgets to be associated with the Configlet Builder.

![Figure 259: Configlet UI Widgets](image)

The widget types are:

- **Text Box** – Use for single line text entries (for example, descriptions, host name).
- **Text Area** – Use for multiple lines of text (for example, MOTD, or login banner).
- **Drop Down** – Use to select a value from a menu as defined in the Value Field.
- **Tick Box** – Use to select a value from a tick list as defined in the Value Field.
- **Radio Button** – Use to select one option from a set of options as defined in Value Field.
- **IP Address** – Use to specify an IP address (this is a Dotted Decimal Address field).
- **Password** – Use to specify a single line of text (characters are hidden as they are entered).
3. Write a Python script that reads the inputs you entered in the previous step and then generates the Configlet.

**Note:** The figures listed in this table show examples of the steps involved in writing a script, including an example of use of standard Python syntax to build components of the Configlet.

<table>
<thead>
<tr>
<th>Figure</th>
<th>Example of</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example (Showing Import of CVP-Specific Internal Libraries)</td>
<td>Importing CVP-specific internal libraries into the script</td>
<td>The CVP-specific internal libraries are used by the script to access form fields and CVP variables.</td>
</tr>
<tr>
<td>Example (Showing Specification of Field IDs Defined in the Form Builder)</td>
<td>Specification of field IDs defined in the Form Builder</td>
<td>You must specify the IDs of fields you defined in the Form Builder in Step 2. The fields you specify are included in the Configlet content generated by the script.</td>
</tr>
<tr>
<td>Example (Showing Use Of Standard Python Script Syntax)</td>
<td>Use of standard Python syntax</td>
<td>The Configlet Builder supports the use of standard Python syntax to build parts of the Configlet. You can also make calls to external files and database.</td>
</tr>
<tr>
<td>Example (Showing Print Output)</td>
<td>Print output (Configlet content)</td>
<td>The script automatically produces print output from the CVP internal libraries you imported and the fields you have defined in the script.</td>
</tr>
</tbody>
</table>
print output is the content of the Configlet.

Figure 260: Example (Showing Import of CVP-Specific Internal Libraries)

```python
1 from cvplibrary import form
2 from cvplibrary import CVPGlobalVariables,
3 GlobalVariablesNames
4 hostNamesField = Form.getFieldID('switchNameField')
5 managementIPField = Form.getFieldID
6 ('ManagementIPField')
7 'ManagementMaskField' = Form.getFieldById
8 ('ManagementMaskField')
9 print "hostname" hostNameField.getValue()
10 print "interface management 1"
11 print "ip address" managementNetwork
12 print 'exit'
```

Figure 261: Example (Showing Specification of Field IDs Defined in the Form Builder)
Complete steps 4 and 5 to test the script to make sure it can generate Configlet content.

4. Fill in the Form Design fields.
5. Click **Generate**.

The Configlet content is generated and shows in the **Built Configlet** pane.

**Note:** If it is necessary to select a device to generate the Configlet, then select a device from the list of devices under Form Design.

![Figure 265: Selecting a Device from the List of Devices Under Form Design](image)

6. Validate the generated Configlet on the device by clicking the **Tick** icon at the upper-right of the page.

The Validate Device dialog appears.

![Figure 266: Example (Generating Configlet Content)](image)
7. In the Validate Device pop-up dialog, click Validate.

![Figure 267: Example Script (Validating Device)](image)

If the device cannot be validated, the error (or errors) are listed in the Validate Device dialog.

8. (If needed) Correct any errors and repeat step 7 to validate the device.

The Validate Device dialog shows a message to indicate a successful validation.

![Figure 268: Example Script (Re-Validating Device after Correction)](image)
9. To apply the new Configlet to the container, do the following:
   a. Go the Network Provisioning page.
   b. Right-click the container and choose Manage > Configlet.

Figure 269: Select the Container to Apply the New Configlet

The list of available Configlets appears on the Configlet page.

10. Select the Configlet to apply to the device by clicking the checkbox next to the name of the Configlet.

Figure 270: Select Configlet on Configlet Page
11. To add devices to the container, do the following:
   a. Go the **Network Provisioning** page.
   b. Right-click the container and choose **Device > Add**.

![Image](image1.png)

**Figure 271: Adding Devices to the Container**

12. Do one of the following:
   - Click **Yes** to apply the Configlet you selected to all of the devices in the hierarchy.
   - Click **No** if you do not want to apply the Configlet you selected to all of the devices in the hierarchy.

![Image](image2.png)

**Figure 272: Message Indicating Selection of Hierarchical Container**

The Configlet page appears showing the Configlet you selected to apply to the container.
13. To assign the Configlet Builder to the container you selected, select (click) the **Configlet Builder**.

**Figure 273: Selecting the Configlet to Assign to the Container**

The page loads a form.

**Figure 274: Form Loaded on Page after you Select the Configlet Builder**
14. Complete (fill in) the form and then click **Generate**. The Configlet Builder creates the new, device-specific Configlet, and the Configlet is shown in the **Built Configlet** pane.

![Figure 275: Configlet Page Showing New, Device-Specific Configlet](image)

**11.1.3 Using the Provided Configlet Builder Examples**

CloudVision Portal (CVP) provides some Configlet Builder examples to help you get started using this feature.

You can load the examples to your CVP instance using the following commands:

- Log into the primary node’s Linux shell as root user.
- Change directory to `/cvpi/tools` and import the example Configlets using the cvptool.

```shell
./cvptool.py --host <host> --user <user> --password <pass> --objects Configlets --action restore --tarFile examples.tar.
```

The provided examples include:

- **Example 1: Form-based management interface Configlet Builder**
- **Example 2: eAPI-based management interface Configlet Builder**
- **Example 3: SSH-based management interface Configlet Builder**
- **Example 4: MySQL-based management interface Configlet Builder**
- **Example 5: Device library based management interface Configlet Builder**

**11.1.3.1 Example 1: Form-based management interface Configlet Builder**

This example uses the form to input the management interface configuration, and generates a new Configlet to preserve the configuration.
11.1.3.2  Example 2: eAPI-based management interface Configlet Builder

This example uses eAPI to read the management interface configuration that the device received from the DHCP server during the ZTP boot, and generates a new Configlet to preserve the configuration.

Note: No UI widgets are associated with the Configlet Builder in this example.

11.1.3.3  Example 3: SSH-based management interface Configlet Builder

This example uses SSH to read the management interface configuration that the device received from the DHCP server during the ZTP boot, and generates a new Configlet to preserve the configuration.
11.1.3.4  **Example 4: MySQL-based management interface Configlet Builder**

In this example, the Configlet Builder uses the device’s MAC address to lookup up its Management IP address, netmask, default route, and host name, which are stored on external MySQL server, and generates a new Configlet to preserve the configuration.

**Note:** No UI widgets are associated with the Configlet Builder in this example.

11.1.3.5  **Example 5: Device library based management interface Configlet Builder**

This example uses Device library to read the management interface configuration that the device received from the DHCP server during the ZTP boot, and generates a new Configlet to preserve the configuration.
11.1.4 Python Execution Environment

The CloudVision Portal (CVP) python execution is supported by several CVP-specific libraries. These libraries provide access to the various CVP services and device state.

11.1.4.1 CVP Form

This library provides access to the user interface (UI) widgets that can be associated with a Configlet Builder (see the provided examples for usage details).

The supported methods are:

```python
from cvplibrary import Form
obj = Form.getFieldById( 'id' );
print obj.getValue()

obj.getFieldById( 'id' ); - Used to get the UI widget by id
obj.getValue() - To get the value
obj.getFieldID() - To get the unique id
obj.isMandatory() - Gets whether the field is mandatory or not
obj.getHelpText() - To get the help text
obj.getDependsOn() - To get the depends on
obj.getType() - To get the type (TextBox, Dropdown, etc)
obj.getDataValidation() - To get the Data validation
```

11.1.4.2 CVP Global Variables and Supported Methods

This library give access to the current execution context for Configlet Builders (see the provided examples for usage details).

The supplied global variables are:

```python
from cvplibrary import CVPGlobalVariables, GlobalVariableNames
CVPGlobalVariables.getValue(GlobalVariableNames.CVP_USERNAME)

Supported GlobalVariableNames:
  CVP_USERNAME - Username of the current user
  CVP_PASSWORD - Password of the current user
```
11.1.4.3 CVP Rest Client

This library allows a Configlet Builder to access any CVP API endpoint. The following is an example:

```python
from cvplibrary import RestClient
url='http://localhost/cvpservice/inventory/devices';
method='GET';
client=RestClient(url,method);
if client.connect():
    print client.getResponse()
```

If no certificates are installed on the server, then add the following lines to ignore ssl warnings:

```python
import ssl
ssl._create_default_https_context = ssl._create_unverified_context
```

11.1.5 Creating Configlets Manually

CloudVision Portal (CVP) enables you to create Configlet manually. This method should be used to create Configlets that are relatively static.

**Note:** If you need to create Configlets that require less user input, you may want to use the Configlet Builder feature.

Complete these steps to manually create Configlets:

1. Select the “+” icon in the grid.
2. The Create Configlet page appears.

![Create Configlet Page](image)

**Figure 281: Create Configlet Page**

3. Click **Save** to save the Configlet.
4. This will list the Configlet in the Configlet Management grid.

11.1.5.1 Validating a Configlet During Creation

CloudVision provides a facility to enter the Configlet code and validate it before saving the codes.

1. Enter the Configlet codes in the field provided.
2. On the right pane, there is a drop-down menu listing all the switches in CLOUDVISION.
3. Search for the device to be validated.

![Figure 282: Validate-Search Device]

4. Select the switch to validate.

![Figure 283: Select Device]

5. Select Validate.

On successful validation, the message Successfully Validated is displayed.

![Figure 284: Validate-Success]

When an error occurs, the message error will be displayed.

![Figure 285: Validation Error]

Related topics:
- Configlet Information Page
- Editing Configlets
- Deleting Configlets
- Importing and Exporting Configlets
11.2 Configlet Information Page

1. Select the name of the Configlet from the grid to access the Configlet information page.

![Figure 286: Configlet Information Page](image)

11.2.1 Tabs in Configlet Information Page

The Configlet Information page consists of:

- Summary Tab
- Logs Tab
- Change History Tab
- Applied Containers Tab
- Applied Devices Tab

11.2.1.1 Summary Tab

The Configlet “Summary” tab provides information about the Configlet. This tab is used to show static Configlets, and Configlet Builder Configlets.

![Figure 287: Summary Tab Page for Static Configlets](image)
11.2.1.2 Logs Tab

The "Logs" tab provides complete information on the Configlet assignment to devices and execution details.

11.2.1.3 Change History Tab

Any change in the Configlets will be recorded in the History tab.
1. Select the **View** option.

A popup window is opened comparing the last version of the Configlet with the edited version (Figure 290: Configlet History Page).

![Figure 290: Configlet History Page](image)

11.2.1.4 **Applied Containers Tab**

This tab gives the details on the containers to which the Configlet is assigned. This also shows the name of the user who made the assignment (Figure 291: Applied Container Page).

![Figure 291: Applied Container Page](image)

11.2.1.5 **Applied Devices Tab**

The **Applied Devices** tab displays the details on the devices to which the Configlet is associated in addition to other information such as **Parent container**, **Applied by**, and **Applied date**.

![Figure 292: Applied Devices Page](image)

When a Configlet is removed from any device through the Network Provisioning module, the device will be removed from the list.

**Related topics:**
- Editing Configlets
- Deleting Configlets
- Importing and Exporting Configlets
- Creating Configlets
11.3 Editing Configlets

You edit Configlets through the Configlet “Summary” page. When you save the edited Configlet, it will update the all the associated tasks and devices in CLOUDVISION.

- Configuration assign tasks which are waiting to be executed in task management that are using the edited Configlet are considered as associated tasks.
- Saving the edited Configlet affects all the associated tasks as follows:

| Pending tasks: | Tasks in pending state are auto updated. The spawned configuration points to the updated Configlet. |
| Failed tasks:  | Tasks in a failed state are auto canceled. A new configuration push task is spawned. |
| Save As:      | The edited Configlet can be saved as a new Configlet. Give the new Configlet a unique name. |

1. Select the **Edit** (pen) icon in the page.

![Figure 293: Configlet Summary Page](image)

2. Validate the Configlet with the **Validation** pane.

![Figure 294: Edit Configlet Summary](image)
3. Do one of the following:
   - Click **Save** to save the edited configlet.
   - Click **Save As** to save the edited configlet as a new Configlet (the name Configlet).

**Related topics:**
- Deleting Configlets
- Importing and Exporting Configlets
- Creating Configlets
- Configlet Information Page

### 11.4 Deleting Configlets

Only unused Configlets can be deleted. If a Configlet is assigned to a device or a container, it cannot be deleted from the inventory. To delete a specific Configlet, its association should be removed from the devices and container.

1. Select a Configlet in the grid. A “trash can” icon will appear.
2. Click the **Trash** icon to delete the Configlet.

**Related topics:**
- Importing and Exporting Configlets
- Creating Configlets
- Configlet Information Page
- Editing Configlets

### 11.5 Importing and Exporting Configlets

You can import and export Configlets using the CloudVision graphical user interface (GUI). This enables you to easily share Configlets with others and back up specific Configlets.

For Configlets shared with you by another system user, you import Configlets from your desktop. When you share Configlets with another system user, you export Configlets to your desktop. You use the Configlets page to import and export Configlets or Configlet Builders.

**Note:** Both Configlets and Configlet Builders can be imported and exported using the GUI.

For more information, see:
- Protection from Overwriting Configlets or Configlet Builders
- Importing Configlets or Configlet Builders
- Exporting Configlets or Configlet Builders

### 11.5.1 Protection from Overwriting Configlets or Configlet Builders

CloudVision provides protection from accidentally overwriting exiting Configlets or Configlet Builders when importing a Configlet or Configlet Builder.

If you import a file that contains one or more Configlets or Configlet Builders that are named the same as Configlets or Configlet Builders already in CVP, the system automatically adds a suffix to the names of the items you are importing. The suffix that is added is in the format of “<number>”.

### 11.5.2 Importing Configlets or Configlet Builders

You import Configlets or Configlet Builders into CVP when another system user has shared a Configlet or Configlet Builder with you. Once you import Configlets or Configlet Builders, the imported items
are available for use in CVP. You import Configlets or Configlet Builders from your desktop using the Configlets page.

Complete the following steps to import Configlets or Configlet Builders.

1. Open the Configlets page.
2. Click the Import icon, located in the upper right of the page.

A dialog appears that you use to select the file that contains the Configlets or Configlet Builders you want to import.

3. Select the file that contains the items you want to import.
4. Click Open.

The Configlets or Configlet Builders in the file you selected are imported into CVP.

11.5.3 Exporting Configlets or Configlet Builders

You export Configlets or Configlet Builders when you want to share them with another system user. Once you export Configlets or Configlet Builders, the exported items are available to be sent to and then imported by the other system user. You export Configlets or Configlet Builders to your desktop using the Configlets page.

Complete the following steps to export Configlets or Configlet Builders.

1. Open the Configlets page.
2. Select the checkbox of each Configlet and Configlet Builder you want to export.

3. Click the **Export** icon (located in the upper right of the page).

A single file (.zip archive) that contains all of the items you selected is automatically downloaded to your desktop.

4. (Optional) You can rename the downloaded file and make a copy of it before sharing it.

5. Share the file with one or more system users.

   **Note:** The items you share can be imported only on systems that support the import of Configlets and Configlet Builders (the Import icon on the Configlets page indicates support for this feature).

**Related topics:**

- Creating Configlets
- Configlet Information Page
- Editing Configlets
- Deleting Configlets
Chapter 12

Image Management (CVP)

The Extended Operating System (EOS) used by the switches are uploaded into CloudVision, and details about them are maintained in the Image Management Inventory.

The main purpose of the Image Management module is to enable you to manage the EOS operating system images across the devices in your current CloudVision environment. It provides you with the functionality required to:

- Validate images
- Upload EOS images to CloudVision
- Maintain the inventory of available EOS images
- Assign images to devices in your CloudVision environment

Sections in this chapter include:

- Image Management Page
- Validating Images
- Upgrading Extended Operating System (EOS) Images
- Creating Image Bundles
- The Bundle Information Page

12.1 Image Management Page

The Image Management page shows the current operating system images that are available for upload to CloudVision. Once uploaded, they can be assigned to devices.

You can navigate to the Image Management page through Provisioning > Image Management.

Figure 298: Image Management page

Related topics:
- Validating Images
- Upgrading Extended Operating System (EOS) Images
- Creating Image Bundles
- The Bundle Information Page
12.2 Validating Images

CloudVision Portal (CVP) provides automatic EOS image validation. This automated validation process helps to ensure that all devices in your CVP environment have EOS images that are supported by CVP.

The automatic validation of EOS images takes place whenever you:

- Upload images to CVP or add images to images bundles.
- Add devices to your CVP environment.

The automatic image validation ensures that images that are available to be included in image bundles and assigned to devices are supported by CVP.

**Note:** EOS images that are not supported cannot be added to an image bundle, or assigned to devices.

12.2.1 Alerts Indicating Unsupported EOS Image Versions

If you attempt to include an unsupported version of an EOS image when creating an image bundle, CVP alerts you with an error to let you know that the upload cannot be done, because the version of the EOS image you are trying to upload is not supported.

![Alerts Image](image)

**Figure 299: Alerts**

If you attempt to add a device to CVP that has an unsupported EOS image, the Status column of the Inventory page indicates that an upgrade is required.

The Network Provisioning page also indicate that the device is running an unsupported image (this alert shows only when placing your cursor over the device icon).

**Related topics:**
- Upgrading Extended Operating System (EOS) Images
- Creating Image Bundles
- The Bundle Information Page
- Image Management Page

12.3 Upgrading Extended Operating System (EOS) Images

CloudVision Portal (CVP) provides the functionality to upgrade the EOS image on a device. Typically, you upgrade the image on a device to change the version of the image from an unsupported image version to a supported image version.

You upgrade device images by associating an EOS image with a device or a container (the association is referred to as an image association). Image associations follow the same container inheritance rules as configlet associations. This means that the image you select to be associated is automatically inherited (assigned) to all devices under the level in the hierarchy at which you associate the image.
**Note:** When performing an image push, CloudVision checks if the target EOS image is already present on flash. If the `.swi` file is available, CloudVision uses the same file instead of downloading a new image from the network. This reduces network costs and time incurred during image upgrades.

For more information, see:
- Example of Image Association
- Tip for Handling Multiple Image Association Tasks

12.3.1 Example of Image Association

This example shows the behavior of image associations in a multi-level network hierarchy. The hierarchy in this example contains a tenant container named Demo-Lab. The Demo-Lab container has five child containers named CVX, Host-TOR1, Leaf, Spine, and TOR2.

![Figure 300: Same Task Scheduled for Every Device in CVX Container](image)

Based on the rules for image association inheritance, the Demo-Lab container could have selected the 4.18.8M device EOS image.

![Figure 301: Example of image Association (Example 1)](image)

The CVX container could override that image selection (4.18.8M image) for its devices by selecting the 4.20.7M image. As a result, all of the devices under CVX are assigned the 4.20.7M image, and the devices under Host-TOR1, Leaf, Spine and TOR2 inherit the 4.18.8M image from the Demo-Lab container.
If an image association is changed at any level, and the change is saved in the Network Provisioning page, the following occurs:

- The change impacts all devices under that level.
- A task is automatically created to upgrade the impacted devices.

For example, if the image selection was removed at the CVX level, the following would occur:

- All of the devices under the CVX level would inherit the Demo-Lab image.
- A task would be scheduled for every device in CVX to use the Demo-Lab image.

Related topics:

- Tip for Handling Multiple Image Association Tasks
- Creating Image Bundles
- The Bundle Information Page
- Image Management Page
- Validating Images

12.3.2 Tip for Handling Multiple Image Association Tasks

When several image association tasks are scheduled to be completed, use the following steps to execute the tasks. These steps help you to execute the tasks more efficiently.

1. Search on “Pending” in the Tasks page to find the tasks to be executed (status is “Pending”).
2. Select them all by clicking the checkbox next to the Task ID heading. If the search results returns multiple pages of tasks, then click the checkbox at the top of each page to select the tasks so they can be executed.

![Figure 303: Selecting Multiple Tasks to be Executed](image-url)

3. Click the **Play** icon to execute the selected tasks all at once.

**Related topics:**
- Creating Image Bundles
- The Bundle Information Page
- Image Management Page
- Validating Images
- Example of Image Association

### 12.4 Creating Image Bundles

Creating image bundles is a key image management task. You create image bundles so that you have supported image versions available to be assigned to devices in your CVP environment.

**Note:** An image bundle must have one `.swi` file. Extensions are optional (not required for image bundles), but you can add one or more extensions to an image bundle.

**Pre-requisite:** To ensure that you include valid (supported) EOS images in the bundles you create, make sure you validate the images you want to include in the bundle (see Validating Images).

Complete the following steps to create an image bundle:

1. Go to the **Image Management** page.
2. Click the “+” icon in the grid.

   This loads the **Create Image Bundle** page.
12.4.1 Creating a Bundle by Tagging Existing Image Bundles

CloudVision Portal (CVP) enables you to create a new image bundle by tagging existing image bundles. This prevents you from having to import the same image again to create another bundle.

1. Go to the Image Management page.
2. Click the “+” icon and then the Disk icon.
1. This opens the Images dialog, which lists all of the available images.

![Image Management (CVP)

Figure 305: Images dialog

3. Search for the desired image.
4. Select the image and click **Add** to add the image to the bundle.

The image will be displayed in the grid of the **Create Image Bundle** page.

![Image Management (CVP)

Figure 306: Added image shown in Create Image Bundle page

5. Click **Save** to create the new image bundle.

**Related topics:**
- Creating a Bundle by Uploading a New Image
- Adding EOS Extensions to Image Bundles

### 12.4.2 Creating a Bundle by Uploading a New Image

CloudVision Portal (CVP) enables you to create new image bundles by uploading new images to CVP.

1. Go to the **Create Image Bundle** page.
2. Click the upload from local icon available next to disk icon.

This opens a dialog to search and upload .swi files from system.
3. Navigate to the desired .swi file and upload it to CVP.  
The upload bar on the page shows the progress of the upload.

![Figure 307: Uploading .swi files to CVP (upload in progress)](image)

4. Click **Save** to create the new image bundle.

### 12.4.3 Adding EOS Extensions to Image Bundles

CloudVision Portal (CVP) enables you to add EOS extensions to image bundles along with .swi images. Extensions are either .rpm files or .swix files. You upload .rpm or .swix files using the Images page. Extensions are optional for image bundles.

**Note:** To verify that all the extensions you selected are installed and running on the device, run a compliance check on the device after you install the image bundle on the device.

Complete these steps to add EOS extensions to an image bundle:

1. Go to the **Create Image Bundle** page.
2. Click the upload from local icon.

   This opens a dialog to search and upload EOS extensions (.rpm or .swix files) from the system.
3. Navigate to the desired .rpm or .swix files and upload them.

The upload bar on the page shows the progress of the upload. The extensions you uploaded are shown in the Create Image Bundle page.

![Create Image Bundle page](image.png)

**Figure 308: Create Image Bundle showing uploaded extensions**

4. Select **Reboot Required** check-boxes for all extensions that require a reboot. (All uploaded extensions in this example require a reboot.)

5. Click **Save**. The extensions are added to the image bundle.

Once the image bundle is assigned to a device, a reboot task will be generated. The newly added extensions are installed on the device when the reboot task is executed. Any extensions that were previously installed but are not part of the current bundle are removed from the device.

### 12.5 The Bundle Information Page

The Image Management page provides high-level information about an image bundle (for example, the number of containers to which an image bundle is associated, and the number of devices to which an image bundle is assigned).

To view more detailed information about image bundles, use the Bundle Information page, which you can open from the Image Management page.

Complete these steps to open the **Bundle Information** page.

1. Go to the **Image Management** page.
2. Click the name of image bundle for which you want to view information.

![Bundle Information page](image.png)

**Figure 309: Opening the Bundle Information page**
The **Bundle Information** page appears, showing information for the selected image bundle. Use the following tabs to view specific information about the selected image bundle.

- Summary Tab
- Logs Tab
- Applied Containers Tab
- Applied Devices Tab

### 12.5.1 Summary Tab

The Summary tab provides basic information about the Image Bundle. It also provides options to go back to the **Image Management** page, to open the dialog used to update image bundles, and to delete corresponding image bundle and its extensions.

![Summary tab](image)

Figure 310: Summary tab

For details on the steps used to edit image bundles and delete image bundles, see:

- Updating Bundles
- Deleting Bundles

### 12.5.2Logs Tab

The Logs tab provides complete information on the image assignment to devices and execution details. It also provides the option to go back to the **Image Management** page.
12.5.3 Applied Containers Tab

The Applied Containers tab displays the details on the containers to which the bundle has been applied. It also displays the name of the user that applied the bundle and the date it was applied.

12.5.4 Applied Devices Tab

The Applied Devices tab displays the details on the devices to which the bundle is assigned, along with other information such as the parent container for the device, and the name of the user that applied the bundle and the date it was applied.

Related topics:
- Summary Tab
- Logs Tab
- Applied Containers Tab
12.5.5 Updating Bundles

Perform the following steps to update a bundle:

1. Go to the Image Management page.
2. Click the name of image bundle that you want to update.

The system displays the Summary tab.

Figure 314: Summary page showing bundle selected for edit

3. Click the edit icon at the upper right corner of the Summary section.
4. Edit the bundle as needed.
5. Click Save.

Related topics:
- Deleting Bundles

12.5.6 Deleting Bundles

Only unused bundles can be deleted. If a bundle is assigned to a device or a container, it cannot be deleted from the inventory.

Perform the following steps to delete a bundle:

1. Go to the Image Management page.
2. Click the name of image bundle that you want to delete.

The system displays the Summary tab.
3. Click the edit icon at the upper right corner of the **Summary** section.

![Figure 315: Summary page showing bundle selected for deletion](image)

4. Click the trash icon to delete the selected bundle from the inventory.

The system prompts to confirm the deletion.

5. Click **Yes** to confirm deletion.

6. Click **Save**.

   - **Note:** The association can be removed only if a new bundle is assigned to device or container.

   - **Note:** When an image bundle is assigned to a container, no task will be spawned to the subordinate devices.

**Related topics:**

- **Updating Bundles**
Change Control

Task Management is an inventory of all the tasks generated in CloudVision. You can create a Change Control or cancel a task in task management.

Sections in this chapter include:

- Basic Options for Handling Tasks
- Using the Tasks Module
- Using the Change Control Module

13.1 Basic Options for Handling Tasks

CloudVision provides two basic ways to handle tasks. You can handle tasks individually (task by task), or by groups of tasks.

To view and cancel tasks individually, use the Task Management module, which you can access by navigating to **Provisioning > Tasks** from the CloudVision Portal. For detailed information on the Tasks module, see Using the Tasks Module.

To execute grouped tasks (multiple tasks in the same group), use the Change Control module from either Tasks or Change Control screens. To access the Change Control screen, navigate to **Provisioning > Change Control** from the CloudVision Portal. For detailed information on the Change Control module, see Using the Change Control Module.

13.1.1 Creating Tasks

The following actions that affect the performance of devices are automatically generated as tasks:

- **Assigning Configuration** (assigning a configuration to a device or container)
- **Adding Devices** (adding a device from the undefined container to a defined container)
- **Managing Devices** (moving or removing devices from a container)

13.1.1.1 Assigning Configuration

1. Go to the Network Provisioning screen.
2. Select a device or container.
3. Assign configuration.
4. Save the topology to generate the task.

   ![Note: Editing a configlet also generates a task.]

13.1.1.2 Adding Devices

1. Go to the Network provisioning screen.
2. Select a container.
3. Add devices to the container.
4. Save the topology to generate the task.

   ![Note: If the hierarchy of the container has images or configlets, the created task will also include image push and configuration push tasks.]
13.1.1.3 Managing Devices

1. Go to the Network provisioning screen.
2. Select a container.
3. Move or remove devices from the container.
4. Save the topology to generate the task.

13.2 Using the Tasks Module

This module covers the following sections:

- Accessing the Tasks Summary Screen
- Creating Change Controls from the Change Controls Summary Screen
- Accessing the Tasks Details Screen
- Task Status

13.2.1 Accessing the Tasks Summary Screen

Use the Tasks Summary screen to create Change Controls, cancel tasks, view assignable and assigned tasks, navigate to the appropriate task details screen, and navigate to the device overview screen. See Task Screen below.

![Figure 316: Tasks Screen](image)

To access the Tasks Summary screen, go to the Provisioning screen and click Tasks in the left menu.

The Tasks Summary screen consists of the following entities:

- **+ Create Change Control button** - Click this button to create a Change Control
- **Cancel Task(s) button** - Click this button to cancel selected assignable tasks
• **Assignable Tasks Table** - Lists assignable tasks with the following information:
  - **Task ID** - Displays the task ID.
    
    Click the Task ID to go to the appropriate task details screen.
  - **Device** - Displays the device name on which this task is performed.
    
    Click the device name to open the appropriate **Device Overview** screen.
  - **Created By** - Displays who created the task.
  - **Type** - Displays the task type.
  - **Last Updated** - Displays when the task was last updated.
  - **Status** - Displays the task status.

• **Assigned Tasks Table** - Lists assigned tasks with the following information:
  - **Task ID** - Displays the task ID.
    
    Click the task ID to go to the appropriate task details screen.
  - **Device** - Displays the device name on which this task is performed.
    
    Click the device name to open the appropriate **Device Overview** screen.
  - **Created By** - Displays who created the task.
  - **Type** - Displays the task type.
  - **Last Updated** - Displays when the task was last updated.
  - **Status** - Displays the task status.
  - **Change Control** - Displays the Change Control name.
    
    Click the Change Control name to go to the appropriate **Change Control Details** screen.

### 13.2.2 Creating Change Controls from the Tasks Summary Screen

The Change Control module selects and executes a group of tasks that you want to process simultaneously. While creating a Change Control, you add tasks with pending or failed status to the Change Control.

Complete the following steps to create a Change Control from the tasks summary screen:

1. On the CloudVision Portal, click **Provisioning > Tasks**.

   The system displays the tasks summary screen.

2. Under the Assignable Tasks table, select tasks you want to include in the Change Control by selecting appropriate checkboxes.

   - **Note:** If you do not select any tasks, the system creates a Change Control without tasks.
3. Click + Create Change Control with \( n \) tasks where \( n \) is the count of selected tasks.

The system displays the appropriate Change Control details screen.

**13.2.3 Creating Change Controls from the Change Controls Summary Screen**

The first step involved in using the Change Control module to manage tasks is to create a Change Control. While creating a Change Control, you add tasks with pending or failed status to the Change Control. By default, all tasks in the same Change Control are added in parallel. If you want to change the execution order, you can drag and drop the action cards on the Change Control Details screen. You can execute grouped tasks after a Change Control is created, reviewed, and approved.

**Note:** If you do not add any tasks, the system creates a Change Control without tasks.

Complete the following steps to create a Change Control from the Change Control Summary screen:


The system displays the Change Control Summary screen.
2. Click + Create Change Control button at the upper right corner. The system displays the Assignable Tasks dialog box.

Figure 319: Assignable Tasks Dialog Box with No Tasks Selected

3. Select tasks you want to include in the Change Control by selecting appropriate checkboxes.

   Note: If you do not select any tasks, the system creates a Change Control without tasks.

4. Click + Create Change Control with n tasks where n is the count of selected tasks.

Figure 320: Assignable Tasks Dialog Box with Tasks Selected

The system displays the appropriate Change Control Details screen.
13.2.4 Accessing the Tasks Details Screen

The **Tasks details** screen provides detailed information for any given task. To access the Tasks details screen, click the task ID under the **Task ID** column in the **Tasks summary** screen.

![Task Details Screen](image)

**Figure 321: Task Details Screen**

The **Tasks Details** screen provides the specified information in following tabs:

- **Pending tasks** icon - Displays the count of pending tasks
- **Notifications** - Displays the count of unread notifications.
- **Logs** tab - Displays logs of the appropriate task.
  
  **Note:** This tab is displayed only for completed tasks.

- **View Image** tab - Provides detailed information on image changes.

![View Image Tab](image)

**Figure 322: View Image Tab**
• **View Config** tab - Displays provisioned, designed, and running configuration changes.

![Figure 323: View Config Tab](image)

### 13.2.5 Task Status

All CloudVision Portal (CVP) tasks are automatically assigned a specific status by the system. The system automatically updates tasks status to indicate the current status of a task.

The task statuses are:

- Pending
- In-Progress
- Completed
- Failed
- Canceled

#### 13.2.5.1 Pending

Any new task is generated with a 'Pending' status. This means that the task has been generated but not executed. You can execute a pending task at any time. Once the task is successfully executed (completed without failure), the status of the task changes to Completed.

#### 13.2.5.2 In-Progress

A task being executed moves to “In-progress” state.

- Config assign, pushes the configuration on the device.
- Image assign, copies the image from CLOUDVISION to the device.
- In-Progress tasks can be canceled.

Various statuses during the Change Control execution are:

- Execution In Progress
- Device Reboot In Progress
- Task Update In Progress
- Configlet Push In Progress
- Image Push In Progress
- Rollback Config Push In Progress
- Rollback Image Push In Progress
- Cancel In Progress
• ZTR Replacement In Progress

13.2.5.3 **Completed**
A task that has been completed. Upon completion, the status changes to Completed. Tasks with Completed status can't be executed or canceled.

13.2.5.4 **Failed**
A task moves to failed state due to multiple reasons such as:
• Device not reachable
• Wrong configuration
• Application problem

13.2.5.5 **Canceled**
A task that is removed from the queue of pending tasks. Tasks with the status of Completed or tasks that have already been canceled, cannot be canceled. Tasks with any status other than Canceled or Completed can be selected and canceled.

13.3 **Using the Change Control Module**
The Change Control module selects and executes a group of tasks that you want to process simultaneously. Selecting tasks and creating Change Controls function similarly in Change Control and Task Management modules.

Change Controls provides the following benefits:
• Sequencing tasks
• Adding unlimited snapshots to every device impacted by the Change Control execution
• Adding custom actions
• Pushing images via Multi-Chassis Link Aggregation (MLAG) In-Service Software Upgrade (ISSU) or Border Gateway Protocol (BGP) maintenance mode
• Reviewing the entire set of changes to approve Change Controls

☞ **Note:** Snapshots display the state of impacted devices before and after the execution.

For more information about Change Controls, see:
• Accessing the Change Control Summary Screen
• Creating Change Controls from the Tasks Summary Screen
• Accessing the Open Change Control Details Screen

13.3.1 **Accessing the Change Control Summary Screen**
The Change Control summary screen is used to manage Change Controls.
To access the Change Control screen, go to the Provisioning screen, and click Change Control in the left menu.

The Change Control screen consists of the following entities:

- **Open Change Controls** and **Executed Change Controls** tables - Lists corresponding Change Controls with the following information:
  - **Name** - Displays the Change Control name
    - Click the Change Control name to go to the appropriate Change Control details screen.
  - **Devices** - Displays devices used in the Change Control
    - Click the device name to go to the appropriate Device Overview screen.
  - **Action** - Displays types of actions to be executed by the Change Control
  - **Last Updated** - Displays when the Change Control was last updated
  - **Status** - Displays the Change Control status

  **Note:**
  - Under the **Status** column of the **Open Change Controls** table, a pending Change Controls is represented with a doc-edit icon and an approved Change Controls is represented with a user-check icon.
  - Under the **Status** column of the **Open Change Controls** table, a failed Change Control is represented with a cross mark and a completed Change Control is represented with a tick mark.
  - Hover the cursor on the status icon in **Open Change Controls** table to view how long ago the current approval status was updated. When you hover the cursor on the status icon in **Executed Change Controls** table, it also displays the approver’s name.

- In the **Open Change Controls** table, click **Delete** to delete the appropriate Change Control.

  **Note:** After you delete an open Change Control, the system returns any tasks used by the deleted Change Control to the assignable tasks pool for reallocation.

- **Recent Activity** pane - Lists most recent activities like updated, executed, and deleted Change Controls.

  **Note:** Click on the Change Control name to go to the appropriate Change Control details screen.

- **Create Change Control** - Click this button to create a Change Control

- **Export to CSV** - Exports the summary data to a CSV file.
13.3.2 Creating Change Controls from the Change Controls Summary Screen

The first step involved in using the Change Control module to manage tasks is to create a Change Control. While creating a Change Control, you add tasks with pending or failed status to the Change Control. By default, all tasks in the same Change Control are added in parallel. If you want to change the execution order, you can drag and drop the action cards on the Change Control Details screen. You can execute grouped tasks after a Change Control is created, reviewed, and approved.

Note: If you do not add any tasks, the system creates a Change Control without tasks.

Complete the following steps to create a Change Control from the Change Control Summary screen:


The system displays the Change Control Summary screen.

![Figure 325: Change Control Summary Screen](image)
2. Click + Create Change Control button at the upper right corner.

   The system displays the Assignable Tasks dialog box.

   ![Assignable Tasks Dialog Box with No Tasks Selected](image)

   **Figure 326: Assignable Tasks Dialog Box with No Tasks Selected**

3. Select tasks you want to include in the Change Control by selecting appropriate checkboxes.

   **Note:** If you do not select any tasks, the system creates a Change Control without tasks.

4. Click + Create Change Control with n tasks where n is the count of selected tasks.

   ![Assignable Tasks Dialog Box with Tasks Selected](image)

   **Figure 327: Assignable Tasks Dialog Box with Tasks Selected**

   The system displays the appropriate Change Control Details screen.
13.3.3 Accessing the Open Change Control Details Screen

The open Change Control details screen performs the following functions:

- Displays Change Control information
- Adds actions to Change Control
- Adds, edits, and deletes child stages
- Reviews and approves Change Control

Perform the following steps to access the Change Control details screen:

1. On the CloudVision Portal, click **Provisioning > Change Control**.
   The system displays the Change Control summary screen.

2. Under the **Open Change Controls** table, click one of the listed Change Controls.
   The system displays the Change Control details screen.

![Change Control Details Screen](image)

**Figure 328: Change Control Details Screen**

The Change Control details screen consists of the following panels:

- **Header Panel**
- **Main Panel**
- **Edit Panel**

**Header Panel**

This primary panel provides the following basic information on the Change Control:

- Edit icon to update the Change Control name
- Change Control information -
  - The open Change Control details screen displays the status, last editor, and count of affected devices.

cka Note:

- Hover the mouse cursor over the clock icon to view last time of action.
• Hover the cursor on the count of affected devices to view their list. Clicking on an affected device opens the corresponding Device Overview screen.
• The executed Change Control details screen displays the status, approver, time of start, last editor, and count of affected devices.

Note:
• Click **Review** next to the status for details on review and approve process.
• **Review and Approve** - Click **Review and Approve** in open Change Controls for assessing Change Control updates. These updates include configuration differences, image bundle changes when appropriate, and commands that run as part of a CLI snapshot.

Figure 329: Review and Approve Pop-Up Window

Click **Approve** to accept Change Control updates.

Note: (Optional) Approver can leave comments in the **Notes**: field.
• On the approved Change Control details screen, click **Unapprove** to revert the approval status and **Execute Change Control** to run approved Change Controls.

Figure 330: Approved Change Control

Note: CVP executes Change Controls in the following ways:
• Runs approved Change Controls immediately if sufficient privileges are set for the **Change Control Management** permission.
• Stops the change automatically if an action fails.
• Runs actions in progress until complete.
• On the failed Change Control details screen, click **Rerun** to repeat the execution of a completed but failed Change Control. This creates a new Change Control that must be approved again.

![Figure 331: Rerun Change Control](Image)

**Note:** Click **Remove** when CVP prompts you with **Remove all actions for devices that have no failures?** for skipping the rerun of completed actions.

• Click **Rollback** in executed Change Controls to open the Rollback **Change Control** pop-up window. To create a rollback after evaluating the executed Change Control, select tasks to rollback from the table and click **Create Rollback Change Control**.

![Figure 332: Rollback Pop-Up Window](Image)

**Note:** CVP rolls back only completed configuration updates and image upgrade tasks.

### Main Panel

This main panel consists of the following entities:

- **Search bar** - Enter a string to perform a search in the Change Control tree.
- **Expand icon** - Click to expand all stages.
- **Collapse icon** - Click to collapse all stages.
- **Information icon** - Click to get help on Change Control.
Change Control tree - Change Controls are composed of actions and stages. Action types include tasks, CLI snapshots, health checks, custom scripts, enter BGP maintenance mode, and exit BGP maintenance mode.

Note: Different icons represent various task types like adding a new device, updating configuration on a device, and updating software image bundle on a device. Actions are represented with a bolt symbol.

Actions are grouped and nested within stages via drag and drop. Each stage executes its children in series (represented with a down arrow) or parallel (represented with an equal sign).

Note:
- Tasks being executed in parallel do not block subsequent actions in that branch.
- In a series execution, the Change Control execution starts from the first item and works its way from top to bottom. The next action starts only when the previous action completed successfully.
- You can toggle the option by clicking the stage type dropdown menu in the edit panel.

Edit Panel
This panel edits stages and actions.

- Edit a stage - Click the required stage in the main panel. The edit panel provides the following options:
  - Show details icon - Click to view associated configuration differences, image bundle changes, and action details.
  - Remove icon - Click to delete the stage.

  Note: Select multiple tasks to view details and delete multiple tasks simultaneously. Use command-click or Ctrl-click to select multiple items. To select a range of items, click the first item and then Shift-click the last item.
  - Group icon - Select multiple tasks to group them into sub-stages.
  - Edit icon - Click to edit the stage name.
  - Change Control stage type dropdown menu - Click to select the Change Control stage type.

  Note: By default, all tasks and actions execute in parallel.
  - Plus icon - Click to add a child stage.
  - Status - Displays telemetry of each device in the stage.

Note:
- Hover the cursor on \textbf{n metric group} to view selected metric groups.

Note: \( n \) represents the count of selected metric groups.
• Hover the cursor on *n device(s)* to view selected metric groups.
  
  **Note:** *n* represents the count of selected devices.

• Add actions - Adds actions to open Change Control. Select the required action and placement from corresponding dropdown menus; and click **Add to change control** to update selected changes.

![Figure 333: Add Actions to Change Control](image)

**Figure 333: Add Actions to Change Control**

• Logs - Displays logs of each update in the executed Change Control process.

![Figure 334: Change Control Logs](image)

**Figure 334: Change Control Logs**

  **Note:**
  
  • Use the search logs bar for filtering logs based on a string.
  • Click the download icon to download logs to your local drive.

13.3.3.1  **Change Control Drop-Down Menu**

Click the Change Control drop-down menu to select another Change Control.

13.3.3.2  **Change Control Edit Drawer**

The system provides collapsed and expanded views of the edit Change Control drawer.
Each icon in the collapsed view corresponds to the appropriate drawer section. The chevron button expands the drawer, displaying the most recently used section. Click any of the active icons in the collapsed view to expand the Change Control drawer with the selected section.

The Change Control edit drawer consists of the following entities:

- Edit Change Control name - Click the Change Control name to edit the name.  
  
  **Note:** Alternatively, click the edit icon next to Change Control name to edit the name.

- Info tab - Provides information of the current Change Control and displays the list of affected devices. Hover the mouse on any of the affected devices to view appropriate device details.

Click **View Events** to view events of the appropriate device. Click **Compare Metrics** to view metrics of the appropriate device. Click on any of the affected devices to view the appropriate device overview screen.
• **Add Actions** tab - Adds actions, assigns to a stage, and adds them to assigned stage.

![Figure 338: Add Actions Tab in Edit Change Control Pane](image)

• **Logs** tab - Displays logs only when the Change Control in either running or has been executed.

![Figure 339: Logs Tab in Edit Change Control Pane](image)

**Note:** This tab is available only for completed Change Controls.

13.3.3.3 **Change Control Stages**

These panes consists of the following entities:

- Change Control stage name - Click either the Change Control name or the corresponding edit icon to update the name.
- Add a stage icon - Click the plus icon at the upper right corner of the stage to add a stage.
- Delete a stage icon - Click the appropriate trash icon at the upper right corner of the stage to delete the corresponding stage.
- Edit actions icon - Click the thunder icon within a card to edit or view the appropriate leaf.
• For open Change Controls, the system displays the actions window to edit the appropriate leaf.

![Figure 340: Info Tab in Edit Actions](image)

**Note:** For completed Change Controls, the system displays the actions window to view the appropriate leaf.

This window consists of the following entities:

• **Info tab** - This tab lists the actions to be run, edits actions, and displays action details. Click the edit icon to reorder and edit actions.

![Figure 341: Reorder and Edit Actions Screen](image)

- Click the select action drop-down menu and select the required action.
  
  **Note:** The system displays selected actions beneath the select action drop-down menu.

- Click **Clear** at the end of a field to delete the appropriate action.
**Note:** This option is available only for a card with multiple actions. The main action in a card is not available to clear.

- Click the check-mark to save changes.

**Note:** Here, actions comprise of provisioning, Border Gateway Protocol (BGP) maintenance, health checks, and snapshots.

- **Configuration Changes** tab - For tasks, this tab displays any configuration or image differences that will be applied as part of the task.

![Configuration Changes Tab in Edit Actions](image1.png)

**Figure 342: Configuration Changes Tab in Edit Actions**

- **Logs** tab - This tab displays log information of completed Change Controls.

![Logs Tab in Edit Actions](image2.png)

**Figure 343: Logs Tab in Edit Actions**

- **Remove from Change Control** button - Click Remove from Change Control to remove this task from the stage.

**Note:** Click **Remove** on the **Confirm** pop-up dialog box to confirm the deletion.

- **Done** button - Click **Done** to save changes.
- **Trashbin icon** - Click the trashbin icon at the upper right corner of the pane to delete the stage.
13.3.3.4 **Review and Approve**

Click the **Review** and **Approve** button at the upper right corner of the Change Control screen to review and approve the Change Control. This button displays the **Review and Approve** dialog box for the selected Change Control.

![Review and Approve Dialog Box](image)

**Figure 344: Review and Approve Dialog Box**

This window consists of a device search field and a list of changes by Change Control stages.

Type the device name in the search field and if available, the system displays the list of changes for the specified device.

The expanded Change Control stage list displays details of the actions to be executed in each stage, grouped by a device.

If you are happy with configuration changes, click the **Approve** button at the lower right corner of the dialog box to approve the Change Control.

13.3.3.5 **Execute Change Control**

After approval, the **Review and Approve** button is replaced with the **Execute Change Control** button.

![Execute Change Control Button](image)

**Figure 345: Execute Change Control Button**
Click the **Execute Change Control** button to execute the Change Control.

**Note:** A Change Control is executed until all actions are either completed or there is a failure in one or more of the actions.

### 13.3.3.6 Stop Change Control

While the system is executing changes specified in Change Control, it replaces the **Execute Change Control** button with the **Stop Change Control** button.

![Stop Change Control Button](image)

Click the **Stop Change Control** button to stop the execution of Change Control.

**Note:** Clicking the **Stop Change Control** button returns failed and incomplete tasks to the assignable tasks pool for reallocation.

If a Change Control has revertible actions, the system replaces the Stop Change Control button with the **Rollback Change** button after the execution of all actions.

![Rollback Change Button](image)

Click the **Rollback Change** button to rollback the execution of Change Control.

### 13.4 Non-Author Change Control Review

The non-author change control review feature enforces change control reviews by someone other than the author. This ensures that two separate people have reviewed a change before it is approved and can be rolled out onto the network.

**Enabling Non-Author Change Control Review**
**Note:** This feature can only be enabled from the **Cluster Management** role.

From the **General Settings** menu, select the **Non-author Change Control review** toggle to enable the feature.

![Figure 348: Enabling Non-Author Change Control Review](image)

Pending and approved changes are displayed in the **Change Control screen** located in the Provisioning tab.

When the feature is enabled, the user making the change (author) will not be allowed to modify the approval status (approve/disapprove) of their own changes.

### 13.5 Change Control Template

Change Control Template allows you to build and structure common change control operations, and to repeat them without having to rebuild or re-specify the actions and sequences. The template is easily modified which enables you to execute evolving change control operations quickly and efficiently.

To configure a Change Control Template, use the Action Bundle and Stage Rule tools. Each Stage Rule depends on an Action Bundle for its content, so at least one Action Bundle must be created before you can start using Change Control Templates.

#### Stage Rules

A Template is defined by a list of Stage Rules. Stage Rules can be executed in Series or Parallel at the root of the change control. Each Stage Rule is linked to one Action Bundle, which supplies the content for that stage.

#### Action Bundles

An Action Bundle is a specific sequence of actions that contain up to one task action and a limitless number of non-task actions. Action Bundles are reusable across multiple Templates and allow you to construct a specific sequence of actions without defining the tasks or devices that they will be applied to.

#### Workflow

Creating and implementing a change control event with a Template, requires five basic steps:

1. Create or select one or more Action Bundles.
2. Assign each Action Bundle to a Stage Rule.
3. Configure the Stage Rules of the Template.
4. Save the Template.
5. Apply the Template in Change Control.

Once the Template has been saved, it will be available to apply repeatedly. For future change control operations with the same actions and sequence, you will only need to follow Step 5.

13.5.1 Action Bundles

Action Bundles are a determined sequence of actions that can include up to one task action and an unlimited number of non-task actions. The Action Bundles are assigned them to the Stage Rules of a Template, which means that you will want to create, edit, and delete Action Bundles.

13.5.1.1 Accessing Action Bundles

You can manage Action Bundles by selecting **Provisioning** in the navigation bar and then selecting **Action Bundles**.

![Figure 349: Action Bundles](image)

13.5.1.2 Creating a New Action Bundle

When creating a new Action Bundle, one task action and unlimited non-task actions can be added.

1. Click **+ Action Bundle**
2. In the side panel that opens, enter a bundle name and an optional description and then click the **Add Action** menu.
3. Select an action from the available list.

![Action Bundle: Bundle Name](image)

- **Note:** Every action except for Execute Task is a non-task action. You can only add one task action for each Action Bundle.

4. Depending on the action type selected, you may have some additional options for what devices you can assign the action to.

- **Note:** The task action will always have its device assigned in the Stage Rule of the Template that the Action Bundle is applied to. For more information on these options, see [Device Placeholders and Static Arguments](#).

5. Select the actions of this Action Bundle to be executed in series or parallel.

6. Review the list of actions, and click **Save**. The Action Bundle will now be available to be assigned in the Stages Rules of Templates.

### 13.5.1.3 Editing an Action Bundle

To edit an Action Bundle.

- **Note:** Upon saving the edits, any template that the Action Bundle is a component of will be updated.

---

**Figure 350: Select an Action**

- **Note:** Every action except for Execute Task is a non-task action. You can only add one task action for each Action Bundle.

4. Depending on the action type selected, you may have some additional options for what devices you can assign the action to.

- **Note:** The task action will always have its device assigned in the Stage Rule of the Template that the Action Bundle is applied to. For more information on these options, see [Device Placeholders and Static Arguments](#).

5. Select the actions of this Action Bundle to be executed in series or parallel.

6. Review the list of actions, and click **Save**. The Action Bundle will now be available to be assigned in the Stages Rules of Templates.

### 13.5.1.3 Editing an Action Bundle

To edit an Action Bundle.

- **Note:** Upon saving the edits, any template that the Action Bundle is a component of will be updated.
1. Click **Edit** on the Action Bundle to be modified.

![Figure 351: Editing an Action Bundle](image1.png)

2. From the side panel, add new actions, modify the order of existing actions, or delete existing actions.
3. Click **Save** to update the Action Bundle.

### 13.5.1.4 Deleting an Action Bundle

**Note:** The following procedure does not remove the Action Bundle from any assigned Template.

1. Select **Delete**.

![Figure 352: Deleting an Action Bundle](image2.png)

2. A modal that will ask you to cancel or remove. Click **Remove**.

### 13.5.1.5 Device Placeholders and Static Arguments

When creating or editing the actions of an Action Bundle, you can assign device placeholders instead of specific devices to the action. These placeholders are then defined when the Action Bundle is added to the Stage Rule of a Template. This gives you the flexibility to assign the same Action Bundle to multiple Templates.

The following is a complete list of device placeholders, along with a sample list of devices you can statically apply the action to:
The placeholders available to you vary based upon the combination of action types that you have already selected. Consequently, additional placeholders may become available for an action after you have added more actions to the Action Bundle. Specifically, ‘Match task device’ and ‘MLAG peer of selected task’ only appear when the Action Bundle contains a task.

Provide via Template

When this action is assigned as a placeholder, you will configure it when building the Template. You can use the Device Filter field in the Stage Rule that the Action Bundle is applied to.

Select one of the following options:

- **All Devices in Change Control**: This option matches all devices associated with the change control (defined by which tasks are linked to the change control)
- **Regular Expression**: This option allows you to select certain devices from Change Control by defining a regular expression to evaluate against the device hostname

Match Task Device

An Action Bundle can contain a maximum of one task action. The device of the task is assigned in the Template using the Device Filter field.

When configuring the Action Bundle, a non-task action with the placeholder Match Task Device can be assigned. This means that the device associated with the task will be applied to the non-task action.

MLAG Peer of Selected Task

This placeholder enables you to sequence MLAG upgrades. You can run non-task actions on the MLAG peer of the device that the task in the Action Bundle is assigned to.

By using this placeholder, the MLAG Health Check can be run against the MLAG peer before running the task.
The following figure is an example of how actions can be arranged so that the MLAG health of both the task device and the task device’s MLAG peer are checked before running the task. The last action checks the MLAG health of the task device after the task has been performed.

![Figure 355: MLAG Peer of Selected Task](image)

**Static Action Arguments**

Static arguments can be applied in an Action Bundle by assigning certain non-task actions with a specific device. This enables you to always have a particular action run against a specific device when the Action Bundle is applied to a Stage Rule in a template.

![Figure 356: Static Action Arguments](image)

**13.5.2 Templates**

Action Bundles will be assigned to a Template. With the Template you will bundle and sequence specific actions and group those action bundles into stages to define the upgrade sequence.
Note: Applying a Template to a change control is a single operation. The Template is not permanently linked to the change control; therefore, making changes to a Template after it has been applied to a change control will have no effect on the existing change control.

- A Template can be applied multiple times. Each time the existing structure will be completely overwritten, and only the tasks will remain as the sole input to the Template.
- This feature cannot be used to craft arbitrarily complex change controls, and advanced users may want to leverage the Change Control API to construct custom layouts.

Accessing Templates

Select Provisioning and select Templates. The following screen will be displayed.

Figure 357: Accessing Templates

13.5.2.1 Create a New Template

When creating a new Template, an unlimited number of Stages Rules can be added using at least one Action Bundle.

1. Select + Template from the Templates screen.
2. Each Stage Rule is associated with a single Action Bundle. Select an Action Bundle from the menu or create a new one.

Figure 358: Create a New Template

3. Once you have assigned an Action Bundle, complete any additional fields associated with the specific Action Bundle.

Note: If the Action Bundle contains device placeholders, a Device Filter will appear. This is used to define which devices will be applied to this Action Bundle.
4. A sub-stage will be created for every populated Action Bundle. Arrange the sub-stages in Series or Parallel.

![Figure 359: Stage Rule](image)

5. You can repeat Steps 2-4 to create a Stage Rule for each Action Bundle to be added to the Template, and then arrange the order of the Stage Rules.

![Figure 360: Order Stage Rules](image)

**Note:** The same Action Bundle can be applied to multiple stages, each with a unique Device Filter.
6. Set the Stage Rules to execute in Series or Parallel.

![Figure 361: Set Stage Rule](image)

7. When done, select **Save Template**.

### 13.5.2.2 Edit a Template

**Note:** Any changes made to a Template will not be updated for any change control operations it has been applied to. The Template will need to be reapplied.

1. Click **Edit** on the Template to modify. The Template screen will display its current Stage Rules and details, how they are ordered, and the manner in which they will be executed.

![Figure 362: Edit a Template](image)

2. Edit any of the details by amending the fields, using the up and down arrows, or deleting Stage Rules.

3. Click **Save Template** when done.

### 13.5.2.3 Delete a Template
1. Click **Delete** on the Template you wish to remove.

![Figure 363: Delete a Template](image)

**Note:** Deleting a template will not affect change controls that were previously generated using that template.

### 13.5.2.4 Creating a New Change Control with a Template

Follow these instructions to create a change control and apply a Template at the same time.

1. Select **Tasks** or **Change Control** under the Provisioning tab, and click **Create Change Control**.
2. In the screen that is displayed, enter a name for the change control and select the tasks that should be included in the change control.
3. To build the change control with a Template, click **Template**.

![Figure 364: Creating a New Change Control with a Template](image)

4. From the menu, select a Template and select **Create Change Control**.
5. The Change Control screen will be displayed. Revise to the change control format, review and approve the proposed changes as needed. When done execute the network changes.

### 13.5.2.5 Applying a Template to an Existing Change Control

If a change control has been created but not approved or executed, you can apply a Template to it.

1. Select **Change Control**, and select the desired change control from the Open Change Control list.
2. The Change Control edit screen of the selected change control is displayed. Click **Select a Template** to open up a menu of your Templates.
3. Select the Template that you want to apply to the change control and click **Apply Template**. The Template configuration will be added to the change control for review and approval.

**Note:** Applying a Template to a change control operation is a single operation. Any changes made to the Template will not be automatically applied to the change control.
Chapter 14

Authentication & Authorization (CVP)

Authentication determines if the provided user credentials (username/password) are correct. If authentication succeeds, the user is logged in.

Authorization determines what operations the user can perform after login. Authorization can be for no access, read access, or read and write access.

In the Access Control page, the type of Authentication and Authorization can be defined. AAA servers are defined in this page.

This module guides account management administrators to manage AAA servers, user accounts, and user roles. It provides the functionality required to manage all aspects of user accounts.

Note: Only account management administrators have the permissions to manage accounts.

Sections in this chapter include:

- Access Requirements for Image Bundle Upgrades
- Managing AAA Servers
- About Users and Roles
- Managing User Accounts
- Managing User Roles
- Service Accounts
- Viewing Activity Logs
- Advanced Login Options
- Access to the Access Control Page

14.1 Access Requirements for Image Bundle Upgrades

If AAA is configured (enabled) on the switch, you must have certain access rights before you can perform image bundle upgrades on the switch.

The specific access rights required to perform image bundle upgrades when AAA is configured are:

- Config session
- Bash

The access rights to execute bash commands is required because the following bash command must be executed to upgrade image bundles:

```
bash timeout 10 sudo rm -f /mnt/flash/boot-extensions && echo -e '' > /mnt/flash/boot-extensions
```

Note: If AAA is enabled and you attempt to perform image bundle upgrades without having these required access rights, the upgrade will fail and the following error occurs:

```
Jul 11 11:36:45 cd342 Aaa: %AAA-4-CMD_AUTHZ_FAILED: User cvpadmin failed authorization to execute command 'bash timeout 10 sudo rm -f /mnt/flash/boot-extensions && echo -e '' > /mnt/flash/boot-extensions
```

Related topics:
14.2  Managing AAA Servers

The system uses the following functionalities to manage AAA servers:

- Adding AAA Servers
- Modifying AAA Servers
- Removing AAA Servers

14.2.1  Adding AAA Servers

1. Navigate to the Access Control Page.
2. Click the Authentication source drop-down menu and select either RADIUS or TACACS.

   The Access Control page lists all current servers. See Access to the Access Control Page.
3. Click + New Server at the upper right corner of the Servers section.

   ![Figure 365: + New Server in Access Control Page](image)

   The system pops-up the New Server window.

   ![Figure 366: New Server Pop-Up Window](image)

4. Provide the required Information in corresponding fields.
5. If required, click Test for testing the new configuration. Else, skip to step 8.
6. Enter your credentials when the **Test Server** pop-up prompts for it.

![Test Server Pop-Up Window](image)

**Figure 367: Test Server Pop-Up Window**

7. Click **Run Test**.

The system displays test results. If required, modify the configuration based on the test result.

8. Click **Save**.

The server is added to the list of servers in the AAA grid.

**Related topics:**
- Access to the Access Control Page
- Modifying AAA Servers
- Removing AAA Servers

### 14.2.2 Modifying AAA Servers

1. Navigate to the **Access Control** Page.
2. Select desired modes from **Authentication source** and **Authorization source** drop-down menus

   The system lists all registered servers of the selected AAA server type. See Access to the Access Control Page.

3. Click the edit icon available next to IP address of the corresponding server.

   The system pops-up the **Edit Server window**.

![Edit Server Pop-Up Window](image)

**Figure 368: Edit Server Pop-Up Window**

4. Modify the required information.
5. If required, click **Test** to verify latest changes.
6. Click **Save**.

**Note:** To apply external authentication, there should be at least one enabled server listed in the page.

### 14.2.2.1 Adding Vendor Specific Codes to AAA Servers

You can add vendor specific codes to AAA servers for the following:

- RADIUS
- TACACS+
- CISCO ACS

#### 14.2.2.1.1 RADIUS

Arista Vendor Specific Code: add it to the RADIUS dictionary.

```plaintext
VENDOR Arista 30065
BEGIN-VENDOR Arista
ATTRIBUTE Arista-AVPair 1 string
END-VENDOR Arista
```

To specify role for a user

```
"bob"      Cleartext-Password := "Pa$sW04d"
            Arista-AVPair = "shell:cvp-roles=network-admin",
            Service-Type = NAS-Prompt-User
```

#### 14.2.2.1.2 TACACS+

For TACACS+ there is no vendor specific code, just different strings.

**Note:** CloudVision support for TACACS+ servers can be affected with the setting of the “service” parameter. Some TACACS servers may require "service = shell" instead of "service = exec" in the TACACS+ configuration (tacacs.conf).

This example configures user “bob” in the admin group and specifies certain attributes. It specifies a “cvp-roles” attribute for the CloudVision role name (it can also be a list of roles).

A. tacacs.conf

```plaintext
group = admingroup {
    default service = deny
    service = exec {
        default attribute = permit
        priv-lvl = 15
        cvp-roles = network-admin
    }
    enable = nopassword
}
user = bob {
    login = cleartext "secret"
    member = admingroup
}
```

B. CVP AAA settings
C. Switch AAA configlet
14.2.2.1.3 CISCO ACS

To ensure that authentication and authorization work properly, complete the following procedures.

- Creating Identity Groups and Users
- Creating a Shell Profile using ACS
- Creating and Modifying Access Policy

14.2.2.1.3.1 Creating Identity Groups and Users

1. Select Users and Identity Stores, and then select Identity Groups.
2. Make sure a group named <user-group> exists. If this group does not exist, add it.
3. Add new users under the group named <user-group>.

14.2.2.1.3.2 Creating a Shell Profile using ACS

1. Go to the Policy Elements page.
2. Select Device Administration > Shell Profiles.
3. Click the Create button to create a new shell profile.
4. Select the Custom Attributes tab, and then add a new mandatory attribute named “cvp-roles”.
5. Specify one or more of the following values to the new “cvp-roles” attribute:
   - network-admin
   - network-operator

   Note: If you have created custom role(s) under CVP Account Management, you can use them.
6. Check to make sure that under the “Common Tasks Attributes” table, “Assigned Privilege Level” and “Max Privilege Level” are added by default with and the specified value is 15. Also, verify that requirement is set “Mandatory.”

14.2.2.1.3.3 Creating and Modifying Access Policy

1. Go to the Access Policies section and select the Default Device Admin policy.
2. Make sure that “Allow PAP/ASCII” option in the Authorization section is enabled (selected).
3. In the Authorization section, create a new rule named “Rule-1”.
4. Make sure that the status of the new rule (“Rule-1”) is Enabled, and set the identity group as “<user-group>”.
5. Select the shell profile that outlines the cvp-roles for all users under the group named <user-group>.

   Note: Alternatively, you can set add shell profile in the “default rule” section.
6. Make sure that “Service Selection Rules” (under the “Access Policies” section), is using the policy named “Default Device Admin”. The policy should be listed in the “Results” column of “Service Selection Policy” table, and the “status” column should be green, indicating that the policy is enabled.

   The shell profile should be automatically applied to all users under the group named <user-group>.

14.2.2.1.4 Supported TACACS Types

CloudVision Portal (CVP) supports different types of TACACS. Table Supported TACACS Types lists the supported types of TACACS, including the following information for each TACACS type:

- Supported version
- Service shell (whether it is supported for each type)
- Service exec (only the following attributes are supported):
  - acl
  - default
  - double-quote-values
  - message
  - optional
  - protocol
  - return
  - script
  - set

Table 16: Supported TACACS Types

<table>
<thead>
<tr>
<th>TACACS Type</th>
<th>Supported Version</th>
<th>Service Shell</th>
<th>Service Exec</th>
</tr>
</thead>
<tbody>
<tr>
<td>tac_plus (Shruberry)</td>
<td>F4.0.4.26</td>
<td>Not Applicable</td>
<td>Supported</td>
</tr>
<tr>
<td>tac_plus (Probono)</td>
<td>201706241310 201503290942/DES</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>CISCO ACS</td>
<td>4.4.0.46 5.3.0.40</td>
<td>Supported</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

Related topics:
- Access to the Access Control Page
- Adding AAA Servers
- Removing AAA Servers

14.2.3 Removing AAA Servers

Complete these steps to remove AAA servers:

1. Navigate to the Access Control page.
2. Select required options from Authentication source and Authorization source drop-down menus.
   The systems lists all current servers.
3. Select required servers for removal.
4. Click Remove Server(s) at the upper right corner of the Servers section.
   The systems lists all current servers.

Figure 369: Remove AAA Servers
5. Click **Delete**.

The system deletes selected AAA servers.

**Related Topics:**
- Access to the Access Control Page
- Adding AAA Servers
- Modifying AAA Servers

### 14.3 About Users and Roles

Account management is based on users and roles. In the CloudVision Portal, users and roles have specific meaning.

| Users | A user is a person who uses the CVP application and is authenticated by the system through the use of account credentials (username and password), which is maintained by CVP or external enterprise servers. Only the users with account management module credentials (Account management administrator) can create and manage users.

The account management administrator specifies the authentication credentials, name and contact information, status, and CVP permissions when creating user accounts for new users.

Account management administrators control which CVP modules users are authorized to use by assigning roles to users (the role assignments can be changed as needed at any time).

**Note:** Activity of CVP users is logged and can be viewed in the Audit Logs page. |
| Roles | A role is a set of read and write module permissions that defines user authorization to modules in CloudVision Portal. The account management administrator specifies the read and write permissions of each module when they create roles. Only account management administrators can create and manage roles.

Roles enable account management administrators to efficiently manage user permissions by assigning roles to users, and by changing the role assigned to users.

CloudVision Portal provides two default roles, one for the system administrator (network-admin) and one for a basic operator (network-operator). |

### 14.3.1 Default Roles

CloudVision Portal provides two default roles. These default roles can be assigned to users as needed.
network-admin

A user with the default “network-admin” role has read and write permissions for all CVP modules. In addition, this role has both device-level write permissions and database-level write permissions.

network-operator

A user with the default “network-operator” role has only read permissions for all CVP modules. Users with this role cannot make changes to the CVP database.

Note: The read and write permissions cannot be changed for the default roles. But, custom roles can be created where read and write permissions can be modified.

For more information, see Managing User Accounts.

14.4 Managing User Accounts

The system uses the following functionalities to manage user accounts:

• Adding New User Accounts
• Modifying User Accounts
• Removing User Accounts

14.4.1 Adding New User Accounts

When you create a new user account, you specify the login information (authentication credentials) of a person that needs to use one or more CVP modules. Personal information for the new user account is optional and can be specified when you create the new user or at a later time.

By default, new user accounts are enabled. The new user is able to use the CVP modules they are permitted to use, based on the role assigned to them. If you do not want the new user to use CVP at this time, select the Disable option (a Status option). You can enable the user account at a later time.

Note: As an alternative to creating user accounts in CVP, you can point CVP to an external AAA server that automatically creates users and maps them to roles during first login.

Complete these steps to create a new user:

1. Navigate to the Access Control page.
2. Under Access Control in the left menu, click Users.

The Users page lists all current users.

Figure 370: Users Page
3. Click **New User** at the upper right corner of the Users page.

The system pops-up the **New User** window.

**Note:** The **New User** pop-up window creates users only with the 'Local' authentication type.

![Figure 371: New User Pop-Up Window](image)

4. Provide the required information in corresponding fields.
5. Click **Save**.

The new user account is created.

**Note:** If the specified role is unavailable in the local CVP, then the network-operator role is automatically assigned to either the RADIUS or TACACS user. Unless you set the account status to disabled, the new user is active using CVP modules based on the role assigned to the user. If user roles conflict when multiple roles are assigned to a user account, the user role with higher privileges is applied to the user account.

**Related topics:**
- Modifying User Accounts
- Removing User Accounts
- Viewing Activity Logs

### 14.4.2 Modifying User Accounts

Modifying user accounts enables you to change the following aspects of existing user accounts:

- Login information (password)
- Contact information (email address)
- Status (enabled or disabled)
- Role(s) (the CVP role(s) assigned to the user)
- Personal information (first and last names)

**Note:** Once changes are saved, they are implemented immediately.

Complete these steps to modify a user account.

1. Navigate to the Access Control page.
2. Under **Access Control**, click **Users**.
3. In the **Users** page, click the edit icon available next to the corresponding user name.

The system pops-up the **Edit User** window displaying all information related to the corresponding user.

![Figure 372: Edit User Pop-Up Window](image)

4. Modify the required information.
5. Click **Save**.

**Related Topics:**
- Adding New User Accounts
- Removing User Accounts
- Viewing Activity Logs

**14.4.3 Removing User Accounts**

Complete these steps to remove a user account:

1. Navigate to the **Access Control** page.
2. Under **Access Control** in the left, click **Users**.

The **Users** page appears displays all current user accounts.

3. Select the users for removal.
4. Click **Remove User/Remove Users** at the upper right corner of the Users page.

The system prompts to confirm deletion.

![Figure 373: Remove User Account](image)
5. Click **Delete**.

The system deletes selected user accounts.

**Related Topics:**
- Adding New User Accounts
- Modifying User Accounts
- Viewing Activity Logs

### 14.5 Managing User Roles

The system uses the following functionalities to manage user roles:

- Adding New User Roles
- Modifying User Roles
- Removing User Roles

#### 14.5.1 Adding New User Roles

CloudVision Portal enables you to create new roles as needed to ensure that you are able to efficiently manage CVP user permissions. When you create a new role, you specify the read and write permissions for each CVP module.

Once a role has been created, it is automatically added to the list of Available roles, and you can assign it to users that should have the permissions defined in the role. When you assign the role to a user, they inherit the read and write permissions defined in the role.

Complete the following steps to create new roles:

1. Navigate to the **Access Control** page.
2. Under **Access Control** in the left menu, click **Roles**.

The Roles page lists all current roles.

![Figure 374: Roles Page](image)

**Figure 374: Roles Page**
3. Click **New Role** at the upper right corner of the Roles page.

The system pops-up the New Role window.

![New Role Pop-Up Window](image)

**Figure 375: New Role Pop-Up Window**

4. Provide the required information in corresponding fields.
5. Click **Save**.

The new role is saved to the CVP database and is available to be assigned to users.

**Note:** The roles created can be assigned to locally created users or by the external AAA server to its known users.

**Related topics:**
- Adding New User Roles
- Modifying User Roles
- Viewing Activity Logs

### 14.5.2 Modifying User Roles

CloudVision Portal provides the functionality required to change the permissions of an existing role. This enables you to efficiently change the permissions of all users that are assigned the role. After you modify the role, all users assigned the role inherit the read and write permissions defined in the new version of the role.
Complete the following steps to modify an existing role:

1. Navigate to the Access Control page.
2. Under in the left menu, click Roles.
3. In the Roles page, click the edit icon available next to the corresponding role name.

   The system pops-up the Edit Role window displaying all information related to the corresponding role.

![Figure 376: Edit Role Pop-Up Window](image)

4. Modify the required information.
5. Click Save.

   The new version of the role is saved to the CVP database.

   **Note:** All users assigned the role inherit the read and write permissions defined in the new version of the role.

**Related topics:**
- Adding New User Roles
- Removing User Roles
- Viewing Activity Logs

### 14.5.3 Removing User Roles

Complete these steps to remove a user role:
1. Navigate to the **Access Control** page.
2. Under **Access Control** in the left menu, click **Roles**.
   
   The Roles page lists all current user roles.
3. Select the required user roles for removal.
4. Click **Remove Role/Remove Roles** at the upper right corner of the **Roles** page.
   
   The system prompts to confirm removal.

   ![Figure 377: Remove User Role](image)

5. **Click Delete.**

   The system deletes selected user roles.

   **Note:** A role assigned to user(s) cannot be deleted.

   Related topics:
   - Adding New User Roles
   - Modifying User Roles
   - Viewing Activity Logs

### 14.6 Service Accounts

The service accounts in CloudVision access APIs in a controlled manner. You must create authentication tokens for service accounts to validate APIs.

To access the Service Accounts screen, navigate to the Settings screen (Click the gear icon at the upper right corner of the screen) > **Access Control** > **Service Accounts**.

The Service Accounts screen provides brief information of all service accounts in a tabular format. See the figure below.
You can perform the following tasks from this screen:

- Adding Service Accounts
- Editing Service Accounts
- Adding Tokens to Service Accounts
- Deleting Service Account Tokens

### 14.6.1 Adding Service Accounts

Perform the following steps to add a service account:

1. On the Service Accounts screen, click **+ Add Service Account**. The system displays the Add Service Account screen.

2. Type the service account name and description in respective fields.

3. Select preferred roles (optional) and status from respective dropdown menus.

   **Note:**
   - Enabled service accounts must have one or more roles assigned to it.
   - Disabled service accounts may not have any roles assigned to it.
4. Click **Save**.

   **Note:** If the Service Accounts screen does not display the new service account, Click **Refresh**.

### 14.6.2 Editing Service Accounts

Perform the following steps to edit a service account:

1. On the Service Accounts screen, click the required service account listed in the table.

   CVP opens the **Edit Service Account: service_name** screen.

   ![Edit Service Account Screen](image)

   **Note:** Alternatively, select the checkbox of required service account and click **+ Add Token to Service Account**.

2. Update required changes in the **Description** field, **Roles** dropdown and **Status** dropdown.

   **Note:**
   - Enabled service accounts must have one or more roles assigned to it.
   - Disabled service accounts may not have any roles assigned to it.

3. Click **Save**.

### 14.6.3 Adding Tokens to Service Accounts

Perform the following steps to create a token for service accounts:

1. On the Service Accounts screen, click the required service account listed in the table.

   CVP opens the **Edit Service Account: service_name** screen.

   **Note:** Alternatively, select the checkbox of required service account and click **+ Add Token to Service Account**.
2. Under **Generate Service Account Token**, type brief summary in the **Description** field. See the figure below.

![Generate Service Account Token](image)

**Figure 381: Generate Service Account Token**

3. Click **Pick Time** and select the expiry date.
   
   **Note:** The maximum duration for validity is one year.

4. Click **Generate**.
   
   **Note:** If the table under **Current Service Account Tokens** does not display the new token, click **Refresh**. The new token gets access to APIs based on roles selected for the service account.

### 14.6.4 Deleting Service Account Tokens

Perform the following steps to delete a service account:

1. On the Service Accounts screen, click the required service account listed in the table.
   
   CVP opens the **Edit Service Account: service_name** screen. Tokens associated to this service accounts are listed in the table under **Current Service Account Tokens**.
   
   **Note:** Alternatively, select the checkbox of the required service account and click **+ Add Token to Service Account**.

2. Select token(s) to be deleted.
3. Click **Remove Token(s)**.
   See the figure below.

![Image](image1.png)

**Figure 382: Delete Service Account Tokens**

CVP prompts to confirm the initiated task.

4. Click **Remove** on the confirmation box.
   See the figure below.

![Image](image2.png)

**Figure 383: CVP Confirmation to Delete Tokens**

5. Click **Save**.

   **Note:**
   - If the table continues to display deleted token(s), click **Refresh**.
• To simultaneously delete all expired tokens across all service accounts, click **Remove all Expired tokens** \((n)\) on the Service Accounts screen where \(n\) stands for the number of expired tokens.

14.7 Viewing Activity Logs

The **Audit Logs** page displays activity logs of user accounts and user roles.

Complete these steps to view activity logs:

1. Click the gear icon at the upper right corner of the CVP page.
2. Click **Audit Logs** on the left menu.

The system displays the Audit Logs page.

3. Select desired options from **View logs for** drop-down menus.

The system displays corresponding logs.

![Figure 384: Audit Logs Page](image)

14.8 Advanced Login Options

Multi-Factor Authentication (MFA) and One-Time Passwords authenticate all CVP managed devices when you authenticate with CVP. CVP runs CLIs on managed devices by sending eAPI requests over the gRPC connection established by TerminAttr.

**Note:**

- Under **Cluster Management** on the settings screen, enable **Advanced login options for device provisioning** to use MFA and one-time passwords.
- CVP needs TACACS to perform command authorization and accounting as per EOS configuration.
- Use the new Device class to make eAPI requests for using this mechanism in Configlet Builder python scripts.

Pre-requisites to install this feature are:

- Devices must run CVP 2018.2.3 or later releases
- Managed devices must have TerminAttr version 1.5.0 or later versions

**Note:** TerminAttr is included with EOS, but may be a version earlier than v1.5.0. Newer versions are available as an extension (swix)

Refer to CVP and TerminAttr release notes available at [https://www.arista.com/en/support/software-download](https://www.arista.com/en/support/software-download) for detailed information on compatible TerminAttr versions with CVP and EOS.
• Ensure that the eAPI unix domain socket is enabled with `management api http-commands` and `protocol unix-socket` configurations in devices running EOS releases prior to 4.20

To enable MFA and One-Time Passwords authentication, enable Advanced login options for device provisioning using the toggle button under Cluster Management on the Settings page. See the figure below.

![Advanced Login Options for Device Provisioning Toggle Button](image)

**Figure 385: Advanced Login Options for Device Provisioning Toggle Button**

### 14.9 Access to the Access Control Page

To gain access to the Access Control Page, complete the following:

1. Click the gear icon on the home page.

![Gear Icon](image)

**Figure 386: Gear Icon**
2. Click **Access Control** in the left menu.

The system displays the Initial Access Control screen.

![Initial Access Control Page](image1.png)

**Figure 387: Initial Access Control Page**

The system displays the **Servers** section when either RADIUS or TACACS is selected as Authentication source.

![AAA Access Control Page](image2.png)

**Figure 388: AAA Access Control Page**

- If the authentication is local, the authorization must be done locally.
- If the authentication is done externally, the authorization can be done locally or externally.

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>Local</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Local</td>
</tr>
<tr>
<td></td>
<td>RADIUS</td>
</tr>
<tr>
<td>TACACS</td>
<td>Local</td>
</tr>
<tr>
<td></td>
<td>TACACS</td>
</tr>
</tbody>
</table>

**Note:** External servers supported by CloudVision are RADIUS and TACACS.

**Related topics:**
- Managing AAA Servers
- Managing User Accounts
- Managing User Roles
- Access Requirements for Image Bundle Upgrades
CloudVision Topology

The CloudVision Topology screen provides an explicit visual representation of the connectivity of your network, allowing you to understand your network's structure and performance more easily. It provides the following benefits:

- Easily understand parts of your network by collapsing or filtering out irrelevant parts
- Explore the historical state and performance of your network or watch it update live
- Support for both datacenter and campus style network connectivity

CloudVision topology provides Virtual Extensible LAN (VXLAN), Internet Protocol Security (IPsec), Distributed Path Selection (DPS), and Link Layer Discovery Protocol (LLDP) network links between endpoints.

Note:

- Information and Statistics for each member link is accessed from the side panel. See Topology Overview.
- If this screen does not display any devices, refer to the CVP release notes at https://www.arista.com/en/support/software-download for compatibility issues.

To view the Topology screen, click the **Topology** tab on the CloudVision Portal.

**Figure 389: Topology Screen**

This screen is divided into main and side panels. The main panel displays the main topology visualization. Devices are drawn with paths to connect them if they share at least one network connection. They are grouped into containers that can be expanded or collapsed to control which portions of the network are displayed in detail. See Main Panel of the Topology Screen.

The side panel provides the following panes to perform the specified functionalities:
• To customize the network view:
  • Topology Overview
  • Topology Layout Pane
  • Topology Options Pane
• To view the component information:
  • Container Details Pane
  • Device Details Pane
  • Link Details Panel
  • Flow Visibility

15.1 Main Panel of the Topology Screen

The main panel displays the network topology where devices are grouped into containers according to their connectivity or assigned role in the network.

The icons in the following table represents specified containers:

Table 18: Icons Used in Network Topology

<table>
<thead>
<tr>
<th>Cloud</th>
<th>Datacenter</th>
<th>Campus</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Cloud Icon" /></td>
<td><img src="image2.png" alt="Datacenter Icon" /></td>
<td><img src="image3.png" alt="Campus Icon" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Building</th>
<th>Floor</th>
<th>Pod</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image4.png" alt="Building Icon" /></td>
<td><img src="image5.png" alt="Floor Icon" /></td>
<td><img src="image6.png" alt="Pod Icon" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rack</th>
<th>Spine</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image7.png" alt="Rack Icon" /></td>
<td><img src="image8.png" alt="Spine Icon" /></td>
</tr>
</tbody>
</table>

The icons in the following table represents specified devices:
### Table 19: Device Icons

<table>
<thead>
<tr>
<th>Device</th>
<th>Icon</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch</td>
<td>![Switch Icon]</td>
<td>Blue WAP represents managed devices. Gray WAP represents unmanaged devices.</td>
</tr>
<tr>
<td>Wireless Access Point</td>
<td>![WAP Icon]</td>
<td></td>
</tr>
<tr>
<td>Management Device Badge</td>
<td>![Management Badge]</td>
<td>This badge next to a device icon represents a management device.</td>
</tr>
<tr>
<td>Computer</td>
<td>![Computer Icon]</td>
<td></td>
</tr>
<tr>
<td>Third Party Device</td>
<td>![Third Party Device Icon]</td>
<td></td>
</tr>
<tr>
<td>Telephone</td>
<td>![Telephone Icon]</td>
<td></td>
</tr>
</tbody>
</table>

This panel provides the following options for a detailed view:

- **Zoom to fit icon** - Click to fit the topology on the screen.
- **Expand containers icon** - Click to expand all containers in the topology.
- **Collapse containers icon** - Click to collapse all containers in the topology.
- Alternatively, right-click on the main panel to get **Expand Network**, **Expand All**, and **Collapse All** options.

![Figure 390: Right-Click on a Device](image)

**Note:** Right-click on a cluster to get cluster specific context menu options.
• Download icon - Click to open the Export Preview pop-up window. Click Export for downloading the current topology image to your local drive in either PNG or SVG formats with selected image resolution.

Note: We recommend to select higher resolutions for readable device labels in bigger topologies.

Figure 391: Export Preview Pop-Up Window

• Double-click on a container to expand it.

• To collapse a container, hover the cursor on a dotted rectangular box and click on the displayed hyphen symbol.

Figure 392: Collapse a Container

• Click container component(s) to view corresponding information on the left panel.

• Selected components are highlighted with dashed frame.

Note: Press and hold the shift key while selecting multiple devices. Press and hold the shift key while dragging to select a region.

• Hover the cursor on a topology component to view the count of corresponding events.

Note: You must enable the option to view events.
### 15.2 Topology Overview

The Topology Overview pane provides the following options:

- **Layout** - Click to view the *Topology Layout* pane. See Topology Layout Pane.
- **Options** - Click to view the *Topology Options* pane. See Topology Options Pane.
- **Network Filters** - Provides the following options to filter networks:
  - **Tags** - To view desired tags by name and value. The main Topology view will be updated and only devices with the chosen tags will be displayed.
  - **Management network** - Display or hide management networks using the toggle button.
  - **VLAN membership** - To view desired VLAN(s), type either a VLAN ID or a range of VLANs.

![Figure 393: VLANs in Topology](image)

**Note:** The right panel displays selected VLAN(s) distinguished with various colors.

- **Link Overlay** drop-down menu - Select an overlay to color each link based on selected metric type. Options include:
  - Active Events
  - Bandwidth Utilization
  - Discard Rate
  - Error Rate
  - Traffic Throughput
  - VLANs
  - None
- **Devices**
  - Search field - Type the device name, MAC address, or model to perform a quick search.
  - List of devices - Click on a device to view the detailed information of corresponding device. See Device Details Pane.
15.3 **Topology Layout Pane**

On the Topology Overview pane, click **Layout** and select a container component from the topology on the right panel to edit layout hints of multiple device(s) in the **Topology Layout** pane.

Topoogy automatically tries to guess a layout with specified containers and roles for your devices based on their connectivity and advertised LLDP capabilities. However, you might sometimes find that the automatic categorization is incorrect, or you simply want a custom layout different from what was originally envisioned. The **Layout** pane lets you override the automatic categorizations and control the layout more directly.

The layout works on the basis of hints that describe the role of a device, whether it exists within a datacenter or campus network, and where it should go in that network. Devices with similar roles and positions in the hierarchy are grouped together. Parallel hierarchies like network pods or racks are created if different names are used.

**Examples**

- A device named *athens* is a datacenter leaf switch, but it has no rack server connections yet and is miscategorized as an edge switch. You can click on athens and then select **Node type** as **leaf** to force it to take on a leaf role. It moves into the leaf position inside its datacenter hierarchy.

- To partition your network into New York and San Francisco datacenters, multi-select the devices or containers that must go in the New York datacenter, type **New York** in the **Datacenter** field, and confirm it. Repeat the same process for San Francisco. Now, your network is divided between these two datacenters, and you can expand or collapse New York and San Francisco datacenters independently to view only one datacenter at a time.

This pane provides the following selections:
• **Network type** drop-down menu - Select the network type that most closely matches your network arrangement. It provides the following options:

  • **Campus** - Devices are manually arranged in containers for different buildings and floors. It provides the following options:
    • **Node type** drop-down menu - Select the preferred device type or roles.
    • **Building** drop-down menu - Select the building name that the selected device preferred to be placed into.
    • **Floor** drop-down menu - Select the preferred floor number in the selected building.
    • **Devices** drop-down menu (Optional) - Set a name to be used to group devices in the selected floor.

  • **Datacenter** - Aspine-and-leaf type layout is used and devices are arranged into pods and racks. It provides the following options:
    • **Node Type** drop-down menu - Select the preferred device type or roles.
    • **Pod** drop-down menu - Select the pod name that the selected device preferred to be placed into.
      
      **Note:** Devices in different pods of the same datacenter appear in different pod containers that can be expanded and collapsed independently.
    • **Rack** drop-down menu - Select the name of a rack similar to pod.

  • **Show Advanced** - Click to view the **Skip Auto-Generated Classifications** drop-down menu.

    **Note:** Click **Hide Advanced** to hide the **Skip Auto-Generated Classifications** drop-down menu. If the **Skip Auto-Generated Classifications** option is enabled, CVP does not automatically identifies the device(s). Only manually-provided layout hints affect the layout of the selected device(s).

  • **Set all to Auto** - Use the automatic layout classification exclusively; all manually-specified layout hints are removed from selected devices.

  • **Save** button - Click to save latest changes.

### 15.4 Topology Options Pane

On the **Topology Overview** pane, click **Options** to edit display settings of topology.

![Topology Options Screen](image)

**Figure 395: Topology Options Screen**

This pane provides the following selections:

• **Show active events**: toggle button - If this option is enabled, active events are shown as badges on devices. These are the same events that are displayed on the Events page. If the same device has multiple events, the badge type of the highest severity event is displayed. Containers also show
badges if they contain any devices with active events. This allows you to quickly find active events anywhere in a large network.

**Note:** This option is enabled by default.

- **Use device images:** toggle button - Enable this option to view photorealistic device images for identified devices. If this option is disabled, icons are used instead. See Figure 396: Network Hierarchy Tree with Images.

![Figure 396: Network Hierarchy Tree with Images](image)

- **Auto-detect management devices:** - If this option is disabled, CVP will not attempt to automatically identify management devices. Devices are considered management devices if they are known to have a relatively high number of connections over a management interface.

- **Auto tagger hints pane** - Influences the way devices are arranged. If a device’s hostname matches the provided text string or regular expression, it will automatically be tagged with the given role. Options include:
  - **Spine Hint:** - Type a text string that is used to identify matching spine devices.
  - **Leaf Hint:** - Type a text string that is used to identify matching leaf devices.
  - **Save button** - Click to save latest changes.

### 15.5 Container Details Pane

To view more information about a device or the devices in a container, click the corresponding device or container on the right panel.
This screen provides the following functionalities:

- **Expand** - Expands the selected container.
- **Collapse** - Collapses the selected container.
- **Layout** - Edits layout hints of the selected container. See Topology Layout Pane.
- **Neighbors** - Displays the list of connected devices from neighboring container.

  **Note:** Click on any neighboring device name to view the corresponding device pane. See Device Details Pane.

- **Members** - Displays the list of container members. Each entry provides the following options:
  - **Device name** - Click to view the corresponding device pane. See Device Details Pane.
  - **View Connectivity** - Click to view the connectivity between selected device and neighboring device. See Link Details Panel.
- **Active Events** (Optional) - Displays events of the selected container. Click on an event link to view the corresponding event details screen.

  **Note:** This option is available only when the **Show active events** option is enabled in the Topology Options pane. See Topology Options Pane.

### 15.6 Device Details Pane

To get a device pane, click on a device (switch, wireless access point, server, or telephone) on the right panel. See Figure 398: Device Details Pane.
Figure 398: Device Details Pane

This screen provides the following functionalities:

- Additional information on the device.
- **Device Overview** - Click to view the Interface Overview screen. [Device Overview](#)
- **Events** - Click to view the Events summary screen. See [Events Summary Screen](#).
- **Layout** - Click to edit layout hints of the selected device. See [Topology Layout Pane](#).
- **Neighbors** - Displays the neighbors list of selected device. Each entry provides the following options:
  - **Device name** - Click to view the corresponding device pane.
  - **View Connectivity** - Click to view the connectivity between selected device and neighboring device. See [Link Details Panel](#).
- **Active Events** (Optional) - Displays events of the selected device. Click on an event link to view the corresponding [Event Details](#) screen.

**Note:** This option is available only when the **Show active events** option is enabled in the [Topology Options](#) pane. See [Topology Options Pane](#).

### 15.7 Link Details Panel

To view the links panel, click on a connectivity link between two components on the right panel.
Links represent connections between devices or clusters of devices. If two devices or clusters have at least one network connection, a link is drawn to connect them. If they have many network connections, they still have a single link in the topology view and information provided for the link is aggregated over those connections. Expanding and collapsing containers expand and collapse links; you may sometimes want to expand containers to see links in greater detail.

This screen provides the following information of the selected connectivity link:

- **Click on a device name to view the corresponding device panel.**
- **Metrics** - Displays statistics of traffic throughput, bandwidth utilization, discard rate, and error rate.
  
  **Note:** Hover the cursor on the metrics to view metrics at the corresponding time.
- **Member Links** - Displays the list of connected ports.
  
  **Note:** Click on any connected port link to view the corresponding Interface Overview screen.
- **Flows** - Displays traffic flows active on the selected connectivity link.
  
  **Note:** Clicking on a listed traffic flow link provides information on connected devices.
- **Events** - Displays events of the selected connectivity link. Click on an event link to view the corresponding Event Details screen.
  
  **Note:** This option is available only when the **Show active events** option is enabled in the Topology Options panel. See Topology Options Pane.

### 15.8 Flow Visibility

On the Topology Overview pane, click **Flows** to open the Topology Flows panel. This screen displays traffic flows detected by EOS devices on the network.
Figure 400: Topology Flow Search

**Note:**
- CVP displays traffic flows only when SFLOW or IPFIX are configured on EOS devices.
- For complete flow visibility, flow collectors are required on all devices along the traffic flow path.

The **Topology Flows** panel provides search filters.

Search for traffic flows the following filters:
- Data source (Flow Tracking (sFlow or IPFIX) or Inband telemetry
- IP address
- Host
- Port
- Protocol
- VRF
- Latency
- Locality

Use the **Color links with total bytes in flows** toggle button to view aggregated bytes or packets of a traffic flow on a single link.

**Note:**
- The color of the link depends on the corresponding flow metric as displayed on the color chart.
- Hover the cursor on a topology flow to view the flow metric of the corresponding link.

You can limit the count of displayed flows via the options available in the **Top** menu. Traffic flows sorted by the selected metric (**Bytes**, **Packets**, **Mean Latency**, **Max Latency**, and **Min Latency**) from the **results sorted by** menu are displayed on the top of the list.

The listed traffic flows in the side panel displays the five-tuple information. The arrow indicates the direction of traffic flow.
In this example, TCP protocol is used in the traffic flowing from p4-proxy101.sjc.aristanetworks.com via 1666 port to bs332.sjc.aristanetworks.com via 37150 port. 36.6GB of data is flown over the given time window.

Flows are displayed based on the timeline selected at the bottom of the Window. To search previous flows, select an earlier time by either using the timeline's time selector, or by dragging the displayed time window to a different position.

**Note:** Live view updates the data every 60 seconds.

**Flow Highlight**
Clicking on a listed traffic flow result highlights the nodes and edges in the graph where the flow has been seen. Animated dots indicate the direction of the traffic flow.

**Note:**
- In environments that capture flow data through sFlow, devices may not capture short-lived or small flows, especially if the selected time window is small.
- This highlight does not guarantee to capture the exact path; it just displays all the devices and links where that flow was seen in the given time window.

The **Devices Reporting Matching Flows** section displays the five-tuple information and lists devices that reported the flow. Each device entry includes the ingress and egress port-channels, ingress and egress interface, packets, bytes and the timestamp when this flow was seen given the time window.

Click on the following entities to view the corresponding specified information:
- Eye icon to magnify the device on the main panel
- *Device hostname* to view the Device Overview page
• **Interface** to view the Interface Overview page
• **Explore** button to view this flow on the Traffic Flows section

**Flow Animation**

To view traffic flow animation, click **Settings** on the **Topology Overview** panel and enable it using the **Enable traffic flows animation** toggle button.

![Figure 403: Enabling Traffic Flow Animation in Settings](image)

**Note:** Few browsers consume high amounts of CPU to render traffic flow animations.

If traffic flow animation is disabled, animated dots are replaced with static arrows indicating the direction of flow.

![Figure 404: Topology with Disabled Traffic Flow Animation](image)

**Links Panel**

The Links panel is accessible via clicking the **Links** tab and displays the topology connections where the top traffic flows have been seen.
Figure 405: Links Panel
Chapter 16

Tap Aggregation (CVP)

Arista EOS provides unprecedented visibility for rapidly identifying and troubleshooting application and performance problems with tracers such as VM Tracer and MapReduce Tracer. EOS integrates with Apache Hadoop systems to track big data workloads, aggregates and monitors business critical applications across thousands of devices, and provides deep visibility and integration with virtualization platforms such as VMware vSphere.

Arista EOS also simplifies tap aggregation with the Arista Data Analyzer (DANZ) feature set. For organizations with compliance requirements to aggregate and capture traffic, Arista EOS enables traffic collection at high data volumes with minimal infrastructure investment and without impacting network performance.

The Arista EOS CloudVision platform further enhances network visibility through a network-wide database approach. By consolidating the network state to a central database, the network operator can visualize the environment.

Sections in this chapter include:

• Integration with CloudVision
• Accessing the Tap Aggregation Screen
• Enabling Multi-Switch Tap Aggregation
• Configuring Tap Aggregation Devices

16.1 Integration with CloudVision

In CloudVision's multi-switch tap aggregation, a datacenter network feeds taps into a layer of switches. These switches forward their traffic to an aggregation layer which subsequently sends traffic to tool ports. Thereby in CloudVision Portal (CVP), you can monitor and manage clusters of switches working in concert.
CloudVision assigns a unique VLAN ID to each external tap port. It tags the traffic arriving on each external tap port with the appropriate VLAN ID and forwards it to each tool-facing device. The traffic arrived on the tool-facing switch passes through a large policy map that matches the VLAN ID of the packet and then sent to the default groups configured on the original tap port. Tool ports that are configured as members of that group receives the packet and forwards it to the external tool device.

You can access the tap aggregation screen for each switch. The CVP multi-switch tap aggregation provides the following functionalities:

- Configures an interface's switchport mode as either tap port or tool port.
- Configures default groups on an external tap port
- Configures the group membership on an external tool port
- Automatically manages policy-maps to correctly steer packets from external tap ports to external tool ports
- Provides built-in verification and reconciliation tools to ensure consistent and valid configuration in devices
- Instinctively monitors details of traffic throughput, interface status, and tap aggregation
- Integrates with CloudVision's other telemetry features including events, notifications, device and interface detail views, and metric comparisons.

16.1.1 Initial Setup for Multi-Switch Tap Aggregation

Initial setup for multi-switch tap aggregation includes the following tasks:
1. **Prerequisites**

2. **Creating a Tap Aggregation Cluster**

3. **Setting Up Tap and Tool Devices**

4. **Configuring Internal Fabric**

### 16.1.1.1 Prerequisites

The prerequisites to create a multi-switch tap aggregation cluster are provided below:

- CVP version 2019.1.0 and above
- Ensure that devices are:
  - In tap aggregation mode
  - Streaming via TerminAttr agent to a CVP node or cluster
  - Provisioned
  - Physically connected
  - Have Port-Channels configured (if they are being used)
- **Advanced login options for device provisioning and Multi-switch tap aggregation** options are enabled in CVP. See [Enabling Multi-Switch Tap Aggregation](#).

**Note:** When prerequisite conditions are met, CVP displays the list the configured tap aggregation devices on the Tap Aggregation screen. See [Configuring Tap Aggregation Devices](#).

### 16.1.1.2 Creating a Tap Aggregation Cluster

Perform the following steps to create a tap aggregation cluster:

1. On CVP, click **Provisioning > Tags**.

   The system displays the Device Tags screen.

   ![Figure 407: Device Tags Screen](image)

   **Note:** To assign tags to interfaces, click the **Interface** tab.
2. On the main panel, select device(s) of your tap aggregation cluster that you want to create a tag for. The system displays the **Assigned tags** panel.

   **Note:**
   - In general, tags should be of the form `<label>: <value>`.
   - (Optional) Use the search bar for searching required devices.

3. Under **User Tags > Add or create tags**, type `tapAggCluster: <clusterName>` in the text box.

   **Note:**
   - To create and assign tap and tool tags, add tags of `tapAggType: tap` or `tapAggType: tool` to appropriate devices.
   - The **System Tags** panel displays tags automatically created by CVP.

4. Click **Create and Assign**.
   The new tag is displayed under **Manage assigned tags**.

   ![Figure 408: Create and Assign](image)

   **Note:** To delete a tag, click on the inessential tag > the minus sign > **Save edits**.

### 16.1.1.3 Setting Up Tap and Tool Devices

Devices are classified as either tap devices or tool devices by using tags with the `tapAggType` type. Perform the following steps to classify devices with ports:

1. On the CloudVision Portal, click **Provisioning > Tags**.
2. Click **Interface** to open the interface tags panel.
3. Select desired tap interfaces. 
The system displays the **Assigned tags** panel.

![Assigned Tags Panel](image)

4. Under **User Tags** > **Add or create tags**, type tapAggType: tap in the text box.
5. Click **Create and Assign**.
6. Select desired tool interfaces. 
The system displays the **Assigned tags** panel.
7. Under **User Tags** > **Add or create tags**, type tapAggType: tool in the text box.
8. Click **Create and Assign**.

### 16.1.1.4 Configuring Internal Fabric

We must manually specify all connections between the devices in our tap aggregation cluster’s internal fabric so that CVP can determine the cluster's topology, which will later be used for generating the cluster policy.

Perform the following steps to configure internal fabric:

1. On the CloudVision Portal, click **TapAgg**. 
The system displays the tap aggregation screen.

   **Note:** If you are configuring internal fabric for the first time, CVP displays the ‘You do not have exactly one connection between each of your cluster devices. Update internal connections warning.

2. Select the desired cluster from the **Cluster** drop-down menu at the upper left corner.
3. Select Internal Fabric from the Table drop-down menu. The system displays the internal fabric screen.

![Internal Fabric Screen](image1.png)

**Figure 410: Internal Fabric Screen**

4. Provide the following information in corresponding fields to add a connection:
   - Source Device
   - Source Interface
   - Destination Device
   - Destination Interface

5. Click **Add Connection**. The system automatically configures the source and destination interface as tool and tap ports respectively.

16.2 **Accessing the Tap Aggregation Screen**

The tap aggregation screen configures internal fabric and provides a summary of all ports and groups configured in tap aggregation clusters.

![Tap Aggregation Screen](image2.png)

**Figure 411: Tap Aggregation Screen**

This screen provides the following information:

- **Cluster** drop-down menu - Select the desired cluster to switch among various tap aggregation clusters.
- **Table** menu - Select the desired table. Available options are:
  - External Ports - Manages external ports. See **External Ports Table Type**.
  - Group Table - Displays an overview of all groups created in the tap aggregation cluster.

![Figure 412: Groups Overview](image)

- Internal Fabric - Configures internal fabric. See **Configuring Internal Fabric**
- **Tap Interfaces** column - Lists all configured tap ports.
  - **Note:** Clicking on the interface link displays the Interface Overview screen. Clicking on the device link displays the Device Overview screen.
- **Bitrate In** column - The bitrate of incoming packets.
- **Aggregation Groups** column - Lists all aggregation groups.
- **Tool Interfaces** column - Lists all configured tap ports.
  - **Note:** Clicking on the interface link displays the Interface Overview screen. Clicking on the device link displays the Device Overview screen.
- **Bitrate Out** column - The bitrate of outgoing packets.
- **Export to CSV** - Click to download the appropriate table contents to your local drive.

### 16.2.1 External Ports Table Type

Select External Ports from the **Table** drop-down menu to access the following functionalities:

- **Cluster Management**
- **ACLs and Tap Ports Management**
- **Tool Ports Management**

### 16.2.2 Cluster Management

Cluster management includes the following functionalities:

- **Adding and Removing Devices**
- **Managing Tap and Tool Ports**
- **Saving Running-Configuration**
- **Verifying Running-Configuration**

**Adding and Removing Devices**

Click the Manage Devices button to open the Device Tags screen where you can add or remove devices from a cluster. See Assigning devices to a Tap Aggregation Cluster.

**Managing Tap and Tool Ports**

Click the Manage Ports button to open the Manage Ports pop-up window.
Figure 413: Manage Ports Pop-Up Window

This screen provides the following functionalities:

- View all current tap and tool ports
- Add or remove multiple tap and tool ports

Note: Click **Apply Changes** to save configuration changes.

**Saving Running-Configuration**

Click the **Save Running Configs** button to save the running-configuration of all devices in the cluster as startup configuration.

The system displays the Save Running Configs pop-up window.

**Verifying Running-Configuration**

Click the **Configuration Status** button to verify that all devices in the cluster are configured correctly.

The system displays the Verify Running Configs screen which lists verification results of each rule that the application checks for. Click **Verify Configuration** to verify all current configurations.
In case of an error, click **Fix Configuration** to resolve the configuration error(s).

The system computes all commands required to fix the current configuration and applies the correct configuration on devices in the Tap Aggregation cluster.

**Note:** Click **Export to CSV** to download the table in csv format to your local drive.

### 16.2.3 ACLs and Tap Ports Management

Perform the following steps to manage ACLs and Tap Ports:
1. Select a tap port by clicking on a row in the Tap Interfaces table.
   The system displays the appropriate tap port’s configuration and metrics in the right panel.

![Tap Port’s Configuration and Metrics Panel](image)

Figure 417: Tap Port’s Configuration and Metrics Panel

2. On the right panel, perform the following steps to execute specified functionalities:
   - Creating an ACL
   - Modifying an ACL
   - Modifying Traffic Steering
   - Modifying Group Membership

Creating an ACL

1. Click the + Add Match Statement button.
   The system displays a Match Statement Card #1 pane.
2. Select Create ACL from the Match ACL drop-down menu.
   The system displays the Create ACL pop-up window.

![Create ACL Pop-Up Window](image)

Figure 418: Create ACL Pop-Up Window

3. Provide the required information in the corresponding entities:
   - Name
   - Description
   - ACL Type
4. Click Create ACL.
   The system confirms when configuration changes are applied successfully.
Modifying an ACL

1. Click the **Add Match Statement** button.
   The system displays a **Match Statement Card #1** pane.
2. Select the edit icon next to the required ACL from the **Match ACL** drop-down menu.
   The system displays the Manage ACL pop-up window.

![Figure 419: Manage ACL Pop-Up Window](image)

3. Update required changes.
4. Click **Apply Changes** to confirm updated changes.

**Note:** Click **Delete ACL** to delete the appropriate ACL.

Modifying Traffic Steering

1. Click the **Add Match Statement** button.
   The system displays a **Match Statement Card #1** pane.
2. Select the required options from **Match ACL and Set Groups** drop-down menu.
3. Click **Apply Changes**.

Modifying Default Groups

Select required group(s) from the multi-purpose **Default Groups** widget.

16.2.3.1 Tool Ports Management

Perform the following steps to add or remove groups from the tool port:
1. Select a tool port by clicking on a row in the **Tool Interfaces** table. The system displays the appropriate tool port's configuration and metrics in the right panel.

2. Select required group(s) from the multi-select **Group Membership** drop-down menu.

3. Click **Apply Changes**.

### 16.2.3.2 Groups Management

Select the required port from either Tap Interfaces or Tool Interfaces pane to initiate modifying group membership in the right panel.

**Modifying Group Membership**

Perform the following steps to modify group membership:

1. Select the required group from the Aggregation Groups pane. The system displays the appropriate group’s configuration and metrics in the right panel.
2. Click the Modify Membership button.
   The system displays the Manage Group Membership pop-up window.

3. Choose required ports.
4. Click Apply Changes.

   Note: The system configures selected ports and deconfigures unselected ports that were previously selected.

16.3 Enabling Multi-Switch Tap Aggregation

Perform the following steps if you do not find the TapAgg tab on the CVP screen:

1. Click the gear icon at the upper right corner of the screen.
   The browser displays the Settings screen.
2. Under the Beta Features pane, enable **Multi-switch tap aggregation** using the toggle button. See Enabling Multi-Switch Tap Aggregation

![Enable Multi-Switch Tap Aggregation](Figure 422: Enable Multi-Switch Tap Aggregation)

**Note:** We recommend to enable **Advanced login options for device provisioning** under the **Cluster Management** pane. This performs configuration changes over the connection between CVP and the device’s TerminAttr agent.

### 16.4 Configuring Tap Aggregation Devices

CVP enables you to select and configure devices for tap aggregation. When you configure a device, you specify the tap aggregation interfaces, aggregation groups, and tool interfaces. You can also view the running configuration on the device and the differences between the designed configuration and running configuration.

You use the tap aggregation screen to select the device for configuration, and the **Tap Aggregation Manager** to configure the device.

Complete these steps to configure a device:
1. Go to the tap aggregation screen.

2. Click the pop-out icon of device you want to configure.

   **Note:** In case of a huge list, search for the device using the Filter search box.

   The Tap Aggregation Manager appears for the device you selected.

3. Specify the tap aggregation interfaces, aggregation groups, and tool interfaces as needed.

4. (Optional) To view the running configuration for the device, click the Running Config button.

5. Click Save to save the configuration for the device.
Chapter 17

Using Snapshots to Monitor Devices

CloudVision enables you to monitor changes in the state of the devices in your network over time through the use of snapshots.

Note: Starting from 2018.2.0 release, snapshots UI is available as part of the Device View in Telemetry.

Sections in this chapter include:

• About Snapshots
• Standard Information in Snapshots
• How to Use Snapshots
• Accessing Snapshots
• Accessing Snapshot Configurations
• Defining Custom Snapshot Templates
• Editing Custom Snapshot Templates
• Viewing Snapshots Differences

17.1 About Snapshots

In CloudVision, the snapshot service runs as a scheduler to capture device snapshots periodically.

The information recorded in snapshots provides you with insights on the configuration, EOS image, and other aspects of the device. Snapshots are captured for individual devices (single switches) only.

17.2 Standard Information in Snapshots

The information recorded in the snapshot reflects the state of the device at the time snapshot was captured. A snapshot only contains outputs of custom commands that are part of a snapshot template. (You must select a snapshot template when you capture a snapshot.) See Defining Custom Snapshot Templates and Editing Custom Snapshot Templates for information on using snapshot templates.

When upgrading to the 2018.2 train, only snapshot templates are migrated but not previous snapshots. CloudVision stores migrated templates without any device list associated with them. Hence, they are marked as unscheduled. However, these templates can be used to capture snapshots before and after change controls.

17.3 How to Use Snapshots

In CloudVision, snapshot service schedules and periodically captures the outputs of commands that are specified in the template. The frequency of capturing command outputs is based on the scheduling frequency mentioned in the snapshot template. The information recorded in snapshots can provide you with insights on the configuration, EOS image, and other aspects of the device. Snapshots are captured for individual devices (single switches) only.

The main uses of snapshots are:

• Viewing snapshots to understand the state of a device at a given time, or over time.
• Comparing snapshots to see the change in state of a device between two points in time.
• Comparing snapshots to see the state of a device before and after a change control.

17.4 Accessing Snapshots

Snapshots are stored under the CVP dataset, which you can access any time for detailed analysis. The Snapshots page displays all valid snapshots created over time. Each valid snapshot provides the following additional information:

• **Name** - The name of the template (you assign the name when you create the template).
• **Capture Time** - The date and time when the snapshot was last captured.
• **Last Executed By** - The user that captured the snapshot.

It also allows navigating to snapshots of the corresponding snapshot template.

![Snapshots Page](image)

**Figure 425: Snapshots Page**

You can navigate to the Snapshots page through one of the following paths:

• **Inventory > Device_ID > Snapshots**
• **Network Provisioning > Right-click on the required device > Snapshot.**

17.5 Accessing Snapshot Configurations

The Snapshot Configuration page displays all snapshot templates created over time. It further allows you to edit current snapshot configuration, navigate to the Snapshots page, view the status of each snapshot configuration, and create a new custom snapshot configuration.
Using Snapshots to Monitor Devices

17.6 Defining Custom Snapshot Templates

To ensure that snapshots contain the information you need for effectively monitoring changes in the state of devices over a certain period of time, CloudVision allows you to define custom snapshot templates.

A snapshot template defines commands, outputs of which need to be captured as part of the snapshot using that template. When you create a snapshot template, associate a list of devices, and set an execution frequency with it, the snapshot service starts capturing and storing snapshots for that template based on the scheduled frequency.

Complete the following steps to define a new custom snapshot template:

1. Navigate to **Inventory > Device_ID > Snapshots > Snapshot Configuration**.
   The Snapshot Configuration page displays currently available snapshot templates.
2. Click the (or create a new configuration) hyperlink at the lower right side of the page. The Snapshot Configuration page displays the Add Snapshot Configuration section.

![Figure 427: Add Snapshot Configuration Section](image)

3. In the Name field, type the name of the custom snapshot template.
4. In the Commands field, enter the EOS CLI commands to be executed by the snapshot.
5. If necessary, click the Devices drop-down and select required devices.
6. Under Interval, Specify the frequency for capturing snapshots in either minutes, hours, or days.
7. Click Save.

The Snapshot Configuration page immediately displays the latest configuration along with the list of current configurations.

**Note:** A snapshot configuration that is created without a device is saved and marked as unscheduled. Snapshot templates with bash commands are marked as invalid. However, these unscheduled and invalid templates can still be selected while creating a Change Control to capture pre and post change control snapshots.

### 17.7 Editing Custom Snapshot Templates

Complete the following steps to go to defined templates:

1. Navigate to **Inventory > Device_ID > Snapshots > Snapshot Configuration**.

The Snapshot Configuration page displays currently available snapshot templates.
2. Click the snapshot name for editing the corresponding snapshot template.

3. Modify the required information in corresponding fields.

4. Click **Save**.

### 17.8 Viewing Snapshots Differences

You can take snapshots of single devices only. The exact set of information and presentation of the information in the snapshot is determined by the snapshot template you choose when capturing the snapshot.

Complete the following steps to view snapshots of a device:

1. Go to the **Network Provisioning** page.
2. Locate the device for which you want to view snapshots.
3. Right-click on the device icon, then click **Snapshot**.

![Figure 429: Initiate Viewing Snapshot](image)

The **All Snapshots** page displays all valid snapshots.

**Note:**

You can also navigate to the **All Snapshots** page through **Telemetry > Devices > Device_ID > Snapshots**.

4. Click on the snapshot template name for viewing the corresponding snapshot.

![Figure 430: All Snapshots Page](image)
5. Click the date and time breadcrumb for viewing all snapshots of the corresponding template.

![Figure 431: View All Snapshots](image)

6. Click the required snapshot to view the corresponding output.

![Figure 432: Select Snapshot](image)

7. Click Compare against a previous time for viewing corresponding snapshot differences.
8. The page displays corresponding snapshot differences.

Figure 433: Compare Snapshots

Note: Snapshot differences are displayed in color codes to quickly identify significant changes in the state of the device over time. Click the Split tab for viewing snapshot differences in different windows.
Chapter 18

Backup & Restore, Upgrades, DNS NTP Server Migration

This document provides details on how to perform backup and restore operations and upgrading CloudVision Portal (CVP).

- Backup and Restore
- Upgrading CloudVision Portal (CVP)
- DNS / NTP Server Migration

18.1 Backup and Restore

CloudVision Portal (CVP) enables you to backup and restore the complete CVP provisioning dataset, including containers, devices, configlets, images, and configlet / image assignments. You can use commands to backup and restore CVP data.

Arista provides a simple script at /cvpi/tools/backup.py which is scheduled by default to run daily to backup CVP data, and retain the last 5 backups in /data/cvpbackup/. Backing up and restoring data saves information about the CVP instance to a tgz file, and then restores the information from the tgz file to a new CVP instance. The CVP commands provide all of the functionality required to complete backup and restore operations.

**Note:** It is a good practice to regularly create and export backups to ensure that you have an adequate supply of backup files available to you that you can use to restore CVP data.

**Note:** There is no backup or restore of the Telemetry analytics dataset.

The current CVP release does not support restoring backups taken from previous CVP releases. If you would like to restore a backup from a previous CVP release, install the previous release, restore the backup, and then upgrade to the current release. After you have successfully upgraded to the current release, take another backup so that you can directly restore that into current main release in the future.

For more information, see:

- Requirements for Multi-node Installations
- Using CVPI Commands to Backup and Restore CVW Data
- Using CVPI Commands to Backup and Restore CVP Provisioning Data

18.1.1 Requirements for Multi-node Installations

The basic requirements for backup and restore operations are the same for single-node installations and multi-node installations.

18.1.2 Using CVPI Commands to Backup and Restore CVW Data

Arista recommends to back up wifimanager regularly and especially before performing any upgrades.

- Restore CVW Data
- RMA
18.1.2.1  Restore CVW Data

You can restore wifimanager from a backup using the `cvpi restore wifimanager <path/to/backup/file>` command.

![Figure 434: Restore CVW Data](image)

**Note:** For a CV cluster, you can run this command only on the primary node. If no backup was carried out before the upgrade, you can use a scheduled backup under the `/data/wifimanager/data/data/backup` directory to restore wifimanager.

18.1.2.2  RMA

For RMA or recovery issues, contact support-wifi@arista.com.

**Note:** Back up wifimanager on any node before submitting it for an RMA. When the node is re-deployed post-RMA, you can restore earlier wifimanager data from a backup that you have stored elsewhere.

18.1.3  Using CVPI Commands to Backup and Restore CVP Provisioning Data

Backup and restore are CVPI functionalities of CVPI components.

**Note:**
- The default directory to save and restore backup data files is `/data/cvpbackup`.
- The default directory for backup/restore log files is `/cvpi/logs/cvpbackup`.
- The default directory for temporary files during backup/restore is `/data/tmp/cvpbackup`.

The following commands are used to backup and then restore the containers, devices, configlets, images, and configlet or image assignments that are defined in CVP.

**Note:** When restoring devices, use the username and password that can access the devices being registered.

18.1.3.1  Backup CVP Provisioning Data

Use the `cvpi backup cvp` command for saving a copy of CVP data as backup.

```plaintext
cvpi backup cvp
```

**Note:** To check the progress of the backup, read the latest `backup_cvp.*.log` file in `/cvpi/logs/cvpbackup`. 
This command creates the backup files for the CVP component.

```
[cvp@cvp108 bin]$ cvpi backup cvp
```

18.1.3.2  Restore CVP Provisioning Data

Use the `cvpi restore` command to restore backup files for the CVP component.

```
cvpi restore cvp cvp.timestamp.tgz eosimages.timestamp.tgz
```

The `cvp.<timestamp>.tgz` parameter contains provisioning data from the DataBase (DB) of the CVP application. The `cvp.eosimages.<timestamp>.tgz` parameter contains EOS images and extensions stored in the DataBase (DB) of the CVP application.

**Note:** To check the progress of the restore, read the latest `restore_cvp.*.log` file in `/cvpi/logs/cvpbackup`.

This command restores the backup files of the CVP component.

```
[cvp@cvp108 bin]$ cvpi restore cvp cvp.2019.1.0.tgz cvp.eosimages.2019.1.0.tgz
```

**Note:** To check the progress of the backup, tail `-f /cvpi/logs/cvpbackup/backup_cvp.20190606020011.log`.

CVP backup creates two backup files in the `/data/cvpbackup` directory for restoration. The `eosimages.tgz` is generated only when it differs from the currently available copy of the `eosimages.tgz`, and is an optional parameter for restore if the CVP system already contains the same EOS image.

The `cvpi backup` command can be run anytime and does not disrupt the cvp application. However, the `cvpi restore` command will stop the cvp application and disrupt the service for the duration of the restore. If the restore is from a backup on a different CVP system to a new CVP system, it may also be required to on-board the EOS devices or restart the Terminattr daemons on the EOS devices after the restore.

18.1.3.2.1  Troubleshooting CVP Restore Failure of Provisioning Data

If the cvpbackup directory does not exist in `/data` when copying the restore files to a newly built VM, you must create it and assign the ownership to the cvp user and group in either of the following two ways:

- Login as cvp user and create the cvpbackup directory

  Use the `su cvp` command to login as cvp user and the `mkdir -p /data/cvpbackup` command to create the cvpbackup directory.

- Create the folder as root and change the ownership

  Use the `mkdir -p /data/cvpbackup` command to create the folder as root and the `chown -R cvp:cvp /data/cvpbackup/` command to change the ownership of cvpbackup directory and its files to cvp user and group.
Verifying the Ownership of cvpbackup Directory

Use one of the following commands to verify the ownership of cvpbackup directory:

- **ls**
  This example verifies the ownership of cvpbackup directory using the `ls` command.
  
  ```bash
  [root@cvp-2019 data]# ls -l /data/ | grep cvpbackup
drwxrwxr-x. 2 cvp cvp 236 Mar 16 02:01 cvpbackup
  ```

- **stat**
  This example verifies the ownership of cvpbackup directory using the `stat` command.
  
  ```bash
  [root@cvp-2019 data]# stat /data/cvpbackup/ | grep Access
  Access: (0775/drwxrwxr-x) Uid: (10010/ cvp) Gid: (10010/ cvp)
  ```

Verifying the Ownership of Files Inside the cvpbackup Directory

The following example verifies the ownership of files inside the cvpbackup directory using the `ls` command:

```bash
[root@cvp-2019 data]# ls -l /data/cvpbackup
total 18863972
-rw-rw-r-- 1 cvp cvp 6650171 Mar 14 02:01 cvp.20200314020004.tgz
-rw-rw-r-- 1 cvp cvp 9642441292 Mar 14 02:08 cvp.eosimages.20200314020004.tgz
```

Correcting the Ownership of cvpbackup Directory Files

Use the `chown` command to correct the ownership of cvpbackup directory files.

```bash
chown cvp:cvp cvp.<timestamp>.tgz cvp.eosimages.<timestamp>.tgz
```

The `cvp.<timestamp>.tgz` parameter contains provisioning data from the DataBase (DB) of the CVP application. The `cvp.eosimages.<timestamp>.tgz` parameter contains EOS images and extensions stored in the DataBase (DB) of the CVP application.

This example changes the ownership of all cvpbackup directory files.

```bash
[root@cvp-2019 data]# chown cvp:cvp cvp.20200319020002.tgz cvp.eosimages.20200314020004.tgz
```

18.2 Upgrading CloudVision Portal (CVP)

Similar to Arista EOS, CVP is packaged and released in trains.

⚠️ **Note:** While upgrading CVP, refer to the latest release notes available at Arista Software Download page; and upgrade procedures.

Devices under management must:

- be running supported EOS version
- have supported TerminAttr version installed
- have the TerminAttr agent enabled and successfully streaming telemetry to CVP.

The following steps can be taken at any point on an existing cluster as part of preparing for an upgrade to the current version:
1. Upgrade existing CVP clusters to the latest CVP release
2. Upgrade all EOS devices under management to the supported release train.
3. For devices running EOS releases prior to 4.20, ensure that the eAPI unix domain socket is enabled with the following configuration:
   
   ```
   management api http-commands
   protocol unix-socket
   ```
4. Install supported TerminAttr on all EOS devices under management.
5. Enable state streaming from all EOS devices under management by applying the `SYS_StreamingTelemetry` configlet and pushing the required configuration to all devices.
6. Ensure that all devices are successfully streaming to the CVP cluster.
7. Ensure that all devices are in image and config compliance.
9. Ensure that all tasks are in a terminal state (Success, Failed, or Canceled).
10. Ensure that all Change Controls are in a terminal state.

   **Note:** After the cluster is upgraded to the latest CVP release, systems running unsupported TerminAttr versions fail to connect to the CVP cluster. These devices will have to be first upgraded to a supported TerminAttr version by re-onboarding them from the CloudVision UI. You cannot rollback a device to a time before it was running the supported TerminAttr version.

   The upgrade from the previous CVP release to the current CVP release trains include data migrations that can take several hours on larger scale systems.
   
   - Upgrades
   - CVP Node RMA
   - CVP / EOS Dependencies
   - Upgrade CVW As Part of a CV Upgrade

### 18.2.1 Upgrades

Upgrades do not require that the VMs be redeployed, and do not result in the loss of logs.

The CVP cluster must be functional and running to successfully complete an upgrade. As a precaution against the loss of CVP data, it is recommended that you backup the CVP data before performing an upgrade. To upgrade CVP to the current release, you must first upgrade CVP to the supported release that supports an upgrade to the current release. For more information, refer the CVP release notes at Arista Software Download page.

   **Note:** We do not support centos updates (`yum update` commands) outside of CVP upgrades.
   
   - Verifying the health of CVP before performing upgrades
   - Upgrading from version 2018.1.2 (or later)

### 18.2.1.1 Verifying the Health of CVP before Performing Upgrades

Upgrades should only be performed on healthy and fully functional CVP systems. Before performing the upgrade, make sure that you verify that the CVP system is healthy.

Complete the following steps to verify the health of CVP.

1. Enter into the Linux shell of the primary node as `cvp user`.
2. Execute the `cvpi status all` command on your CVP:

   ```
   cvpi status all
   ```

   This shows the status of all CVP components.
3. Confirm that all CVP components are running.
4. Log into the CVP system to check functionality.
   Once you have verified the health of your CVP installation, you can begin the upgrade process.
   • Upgrading CloudVision Portal (CVP)

18.2.1.2 Upgrading from version 2018.1.2 (or later)

Use this procedure to complete the fast upgrade of CVP to the current version of CVP.

Pre-requisites:
Before you begin the upgrade procedure, make sure that you have:
• Verified the health of your CVP installation (see Verifying the health of CVP before performing upgrades.
• Verified that you are running version 2018.1.2 or later.

Complete the following steps to perform the upgrade.
1. SSH as root into the primary node.
2. Run these commands:
   a. cd /tmp/
   b. mkdir upgrade
   c. cd upgrade
   d. rm * -f (to remove data from old upgrades if already present)
   e. scp/wget cvp-upgrade-<version>.tgz to this directory.
3. Run the su cvpadmin command to trigger the shell.
4. Select the upgrade option from the shell.

Note: On a multi-node cluster, upgrade can be performed only on the primary node. Upgrading to the current version may take up to 30 minutes.

Note: If an issue occurs during an upgrade, you will be prompted to continue the upgrade once the issue is resolved.

Note: Upgrade to 2021.1.0 and newer requires the configuration of a kubernetes cluster network. You will be prompted during the upgrade to enter the private IP range for the kubernetes cluster network.

18.2.2 CVP Node RMA

Use this procedure to replace any node of a multi-node cluster. Replacing nodes of multi-node cluster involves removing the node you want to replace, waiting for the remaining cluster nodes to recover, powering on the replacement node, and applying the cluster configuration to the new node.

When you replace cluster nodes, you must replace only one node at a time. In case, you plan to replace more than one node of a cluster, you must complete the entire procedure for each node to be replaced.

Note: It is recommended that you save the cvp cluster configuration to a temporary file, or write down the configuration on a worksheet. The configuration can be found in /cvpi/cvp-config.yaml.

1. Power off the node you want to replace (primary, secondary, or tertiary).
2. Remove the node to be replaced.
3. Allow all components of the remaining nodes to recover.
   The remaining nodes need to be up and settled before continuing to step 4.
4. Use the cvpi status all command to ensure that remaining nodes are healthy.

[cvp@cvp73 root]$ cvpi status all
Executing command. This may take some time...
Completed 215/215 discovered actions
primary components total:112 running:104 disabled:8
secondary components total:122 running:114 disabled:8
tertiary components total:97 running:91 disabled:6

5. Power on the replacement node.
6. Log in as cvpadmin.
7. Enter the cvp cluster configuration.

CentOS Linux 7 (Core)
Kernel 3.10.0-957.1.3.el7.x86_64 on an x86_64

localhost login: cvpadmin
Last login: Fri Mar 15 12:24:45 on ttyS0
Changing password for user root.
New password:
Retype new password:
password: all authentication tokens updated successfully.
Enter a command
>r
Please enter minimum configuration to connect to the other peers
*Ethernet interface for the cluster network: eth0
*IP address of eth0: 172.31.0.216
*Netmask of eth0: 255.255.0.0
*Default route: 172.31.0.1
*IP address of one of the two active cluster nodes: 172.31.0.161
Root password of 172.31.0.161:
8. Wait for the RMA process to complete. No action is required.

Root password of 172.31.0.161:
External interfaces, ['eth1'], are discovered under /etc/sysconfig/network-scripts
These interfaces are not managed by CVP.
Please ensure that the configurations for these interfaces are correct.
Otherwise, actions from the CVP shell may fail.

Running : /bin/sudo /sbin/service network restart
[  334.001886] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9 vectors allocated
[  334.004577] vmxnet3 0000:0b:00.0 eth0: NIC Link is Up 10000 Mbps
[  334.006315] IPv6: ADDRCONF(NETDEV_UP): eth0: link is not ready
[  334.267535] IPv6: ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
[  348.252323] vmxnet3 0000:13:00.0 eth1: intr type 3, mode 0, 9 vectors allocated
[  348.254925] vmxnet3 0000:13:00.0 eth1: NIC Link is Up 10000 Mbps
[  348.256504] IPv6: ADDRCONF(NETDEV_UP): eth1: link is not ready

Fetching version information
Run cmd: sudo -u cvp -- ssh 172.31.0.156 cat /cvpi/property/version.txt
0.18
Fetching version information
Run cmd: sudo -u cvp -- ssh 172.31.0.216 cat /cvpi/property/version.txt
10.19
Fetching version information
Run cmd: sudo -u cvp -- ssh 172.31.0.161 cat /cvpi/property/version.txt
0.16
Running : cvpConfig.py tool...
[ 392.941983] vmxnet3 0000:0b:00.0 eth0: intr type 3, mode 0, 9 vectors allocated
9. Continue waiting for the RMA process to complete. No action is required.

Action Output
--------------
COMPONENT       ACTION  NODE       STATUS
ERROR
hadoop          cluster  tertiary  (E) DONE
hbase           cluster  tertiary  (E) DONE

Executing command. This may take some time...

(E) => Enabled
(D) => Disabled
(?) => Zookeeper Down

Action Output
--------------
COMPONENT       ACTION  NODE       STATUS
ERROR
aerisdiskmonitor config  primary  (E) DONE
aerisdiskmonitor config  secondary (E) DONE
aerisdiskmonitor config  tertiary  (E) DONE
<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>ACTION</th>
<th>NODE</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>apiserver</td>
<td>config</td>
<td>primary</td>
<td>(E) DONE</td>
</tr>
<tr>
<td>apiserver</td>
<td>config</td>
<td>secondary</td>
<td>(E) DONE</td>
</tr>
<tr>
<td>apiserver</td>
<td>config</td>
<td>tertiary</td>
<td>(E) DONE</td>
</tr>
<tr>
<td>cvp-backend</td>
<td>config</td>
<td>primary</td>
<td>(E) DONE</td>
</tr>
<tr>
<td>cvp-backend</td>
<td>config</td>
<td>secondary</td>
<td>(E) DONE</td>
</tr>
<tr>
<td>cvp-backend</td>
<td>config</td>
<td>tertiary</td>
<td>(E) DONE</td>
</tr>
<tr>
<td>cvp-frontend</td>
<td>config</td>
<td>primary</td>
<td>(E) DONE</td>
</tr>
<tr>
<td>cvp-frontend</td>
<td>config</td>
<td>secondary</td>
<td>(E) DONE</td>
</tr>
<tr>
<td>cvp-frontend</td>
<td>config</td>
<td>tertiary</td>
<td>(E) DONE</td>
</tr>
<tr>
<td>geiger</td>
<td>config</td>
<td>primary</td>
<td>(E) DONE</td>
</tr>
<tr>
<td>geiger</td>
<td>config</td>
<td>secondary</td>
<td>(E) DONE</td>
</tr>
<tr>
<td>geiger</td>
<td>config</td>
<td>tertiary</td>
<td>(E) DONE</td>
</tr>
<tr>
<td>hadoop</td>
<td>config</td>
<td>primary</td>
<td>(E) DONE</td>
</tr>
<tr>
<td>hadoop</td>
<td>config</td>
<td>secondary</td>
<td>(E) DONE</td>
</tr>
<tr>
<td>hadoop</td>
<td>config</td>
<td>tertiary</td>
<td>(E) DONE</td>
</tr>
<tr>
<td>hbase</td>
<td>config</td>
<td>primary</td>
<td>(E) DONE</td>
</tr>
<tr>
<td>hbase</td>
<td>config</td>
<td>secondary</td>
<td>(E) DONE</td>
</tr>
<tr>
<td>hbase</td>
<td>config</td>
<td>tertiary</td>
<td>(E) DONE</td>
</tr>
<tr>
<td>kafka</td>
<td>config</td>
<td>primary</td>
<td>(E) DONE</td>
</tr>
<tr>
<td>kafka</td>
<td>config</td>
<td>secondary</td>
<td>(E) DONE</td>
</tr>
<tr>
<td>kafka</td>
<td>config</td>
<td>tertiary</td>
<td>(E) DONE</td>
</tr>
<tr>
<td>zookeeper</td>
<td>config</td>
<td>primary</td>
<td>(E) DONE</td>
</tr>
<tr>
<td>zookeeper</td>
<td>config</td>
<td>secondary</td>
<td>(E) DONE</td>
</tr>
<tr>
<td>zookeeper</td>
<td>config</td>
<td>tertiary</td>
<td>(E) DONE</td>
</tr>
</tbody>
</table>

Executing command. This may take some time...

**ERROR**

Including: /cvpi/tls/certs/cvp.crt
Including: /cvpi/tls/certs/cvp.key
Including: /etc/cvpi/cvpi.key
Including: /cvpi/tls/certs/kube-cert.pem
Including: /data/journalnode/mycluster/current/VERSION
Including: /data/journalnode/mycluster/current/last-writer-epoch
Including: /data/journalnode/mycluster/current/last-promised-epoch
Including: /data/journalnode/mycluster/current/paxos
Including: /cvpi/tls/certs/ca.crt
Including: /cvpi/tls/certs/ca.key
Including: /cvpi/tls/certs/server.crt
Including: /cvpi/tls/certs/server.key
mkdir -p /cvpi/tls/certs
mkdir -p /data/journalnode/mycluster/current
mkdir -p /cvpi/tls/certs
mkdir -p /etc/cvpi
mkdir -p /data/journalnode/mycluster/current
mkdir -p /cvpi/tls/certs
mkdir -p /data/journalnode/mycluster/current
mkdir -p /cvpi/tls/certs
Copying: /etc/cvpi/cvpi.key from secondary
rsync -rtvp 172.31.0.161:/etc/cvpi/cvpi.key /etc/cvpi
Copying: /etc/cvpi/tls/certs/cvp.crt from secondary
rsync -rtvp 172.31.0.161:/etc/cvpi/tls/certs/cvp.crt /cvpi/tls/certs
Copying: /cvpi/tls/certs/server.key from secondary
rsync -rtvp 172.31.0.161:/cvpi/tls/certs/server.key /cvpi/tls/certs
Copying: /cvpi/tls/certs/ca.crt from secondary
rsync -rtvp 172.31.0.161:/cvpi/tls/certs/ca.crt /cvpi/tls/certs
Copying: /cvpi/tls/certs/cvp.key from secondary
rsync -rtvp 172.31.0.161:/cvpi/tls/certs/cvp.key /cvpi/tls/certs
Copying: /cvpi/tls/certs/ca.key from secondary
rsync -rtvp 172.31.0.161:/cvpi/tls/certs/ca.key /cvpi/tls/certs
Copying: /data/journalnode/mycluster/current/last-writer-epoch from secondary
rsync -rtvp 172.31.0.161:/data/journalnode/mycluster/current/last-writer-epoch /data/journalnode/mycluster/current
Copying: /cvpi/tls/certs/kube-cert.pem from secondary
rsync -rtvp 172.31.0.161:/cvpi/tls/certs/kube-cert.pem /cvpi/tls/certs
Copying: /data/journalnode/mycluster/current/VERSION from secondary
rsync -rtvp 172.31.0.161:/data/journalnode/mycluster/current/VERSION /data/journalnode/mycluster/current
Copying: /data/journalnode/mycluster/current/paxos from secondary
rsync -rtvp 172.31.0.161:/data/journalnode/mycluster/current/paxos /data/journalnode/mycluster/current
Copying: /data/journalnode/mycluster/current/last-promised-epoch from secondary
rsync -rtvp 172.31.0.161:/data/journalnode/mycluster/current/last-promised-epoch /data/journalnode/mycluster/current
rsync -rtvp 172.31.0.161:/cvpi/tls/certs/kube-cert.pem /cvpi/tls/certs
Starting: cvpi-config
Running: /bin/sudo /bin/systemctl start cvpi-config.service
Starting: cvpi
Running: /bin/sudo /bin/systemctl start cvpi.service
Running: /bin/sudo /bin/systemctl start cvpi-watchdog.timer
Running: /bin/sudo /bin/systemctl enable docker
Running: /bin/sudo /bin/systemctl start docker
Running: /bin/sudo /bin/systemctl enable kube-cluster.path

10. Enter "q" to quit the process after the **RMA process is complete!** message is displayed.
Run cmd: su - cvp -c '/cvpi/bin/cvpi status all --cluster' 2.59
Run cmd: su - cvp -c '/cvpi/bin/cvpi status all --cluster' 2.07
Run cmd: su - cvp -c '/cvpi/bin/cvpi status all --cluster' 2.70
Run cmd: su - cvp -c '/cvpi/bin/cvpi status all --cluster' 2.51
Run cmd: su - cvp -c '/cvpi/bin/cvpi status all --cluster' 2.57
Run cmd: su - cvp -c '/cvpi/bin/cvpi status all --cluster' 2.40
Run cmd: su - cvp -c '/cvpi/bin/cvpi status all --cluster' 2.24
Waiting for all components to start. This may take few minutes.
Run cmd: su - cvp -c '/cvpi/bin/cvpi status all --cluster' 9.68
RMA process is complete!
>q

11. Use the `cvpi status all` command to ensure that the cluster is healthy.

    [cvp@cvp87 ~]$ cvpi status all

    Executing command. This may take some time...
    Completed 215/215 discovered actions
    primary components total:112 running:104 disabled:8
    secondary components total:122 running:114 disabled:8
    tertiary components total:97 running:91 disabled:6

Related topics:

- CVP / EOS Dependencies
- Upgrades

18.2.3 CVP / EOS Dependencies

To ensure that CVP can provide a base level of management, all EOS devices must be running at least EOS versions 4.17.3F or later. To ensure device compatibility supported EOS version advice should be sought from the Arista account team.

CVP should not require any additional EOS upgrades to support the standard features and functions in later versions of the appliance. Newer features and enhancements to CVP may not be available for devices on older code versions.

Refer to the latest Release Notes for additional upgrade/downgrade guidance.

Related topics:

- Upgrades
- CVP Node RMA

18.2.4 Upgrade CVW As Part of a CV Upgrade

In case of a CV upgrade, services go through the following steps:

1. Services or service containers (such as CVW) are stopped.
2. Existing container images are deleted.
3. New component RPMs are installed.
4. The server is rebooted and all services are started again.

A service on CV is upgraded only if its version is different from the pre-upgrade version (CV stores its pre-upgrade state to decide this). The wifimanager component follows a similar process. When
CV boots up after an upgrade, wifimanager starts and upgrades only if the CV upgrade has resulted in a new wifimanager version. The following actions precede every wifimanager start operation:

a. load: Loads the wifimanager container image into docker when CV boots up for the first time after an upgrade.

b. init: Initializes wifimanager before the start. The wifimanager init is versioned init-8.8.0-01, for example. The init-<version> handler initiates a wifimanager upgrade if needed. Thus, if the wifimanager version has not changed after the CV upgrade, the wifimanager upgrade is not invoked. If the wifimanager version has changed, then a wifimanager upgrade is called before its start.

Note: Load and init are internal actions to the wifimanager start operation; they are not run separately. The CVW service might take longer to start than other CV services.

18.3 DNS / NTP Server Migration

You can migrate your DNS / NTP server after you have completed your initial deployment of CloudVision. Migrating the DNS / NTP server is typically done if you want to or need to change the DNS / NTP server that CloudVision currently uses.

For example, if the current CloudVision DNS / NTP server was intentionally isolated during the initial CloudVision installation, you need to migrate the server to make it accessible by external resources.

- Migrating the DNS and NTP Server

18.3.1 Migrating the DNS and NTP Server

The process for migrating the DNS / NTP server after the completion of the initial CloudVision installation involves updating the DNS and NTP server entries on each cluster node and modifying the /cvpi/cvp-config.yaml file (on each node) to reflect the updates to the server entries.

Pre-requisites

Before you begin the migration process, make sure that:

- The IP addresses and hostnames (fqdn) of the nodes must not change.
- For each node, make sure that:
  - At least one DNS server entry is present in the /cvpi/cvp-config.yaml file.
  - The DNS server that corresponds to the DNS server entry in the /cvpi/cvp-config.yaml file can be accessed by the cluster throughout the migration process. (The reason for this is that any changes made to resolv.conf take effect immediately upon saving the file.)
  - The time difference between the old NTP server and new NTP server should be negligible.
  - The old NTP server and new NTP server should be in same time zone.

Complete these steps to migrate the DNS / NTP server.

1. On each node, add the new server to /etc/resolv.conf, by adding a new nameserver line at the top of the file. For example, nameserver 172.22.22.40.

2. On each node, remove the old server from /etc/resolv.conf, by removing the old nameserver line.

3. On each node, do the following to update the NTP server:
   a. Run the ntpstat command to make note of the current NTP server.
   b. In /etc/ntp.conf, add the new NTP server entry and comment out the entry for the old NTP server.
   c. Run the service ntpd restart command.
   d. Run the ntpstat command to verify that the NTP server has been changed on all nodes.
4. On each node, edit the `/cvpi/cvp-config.yaml` file for reflecting changes to the DNS and NTP server entries you made in the previous steps.

5. To read the `/cvpi/cvp-config.yaml` file and restart the network service, run the `/cvpi/tools/cvpConfig.py -y /cvpi/cvp-config.yaml -n nodeX` command on each node where `X` is the respective node number.

**Related topics:**

- Backup and Restore
Chapter 19

Supplementary Services

This document provides configurations steps and examples for supplementary setup procedures for CloudVision Portal (CVP).

• HTTPS Certificates Setup
• Customizing TLS and SSH Ciphers
• DHCP Service for Zero Touch Provisioning (ZTP) Setup
• RADIUS or TACACS Authentication Setup
• Background Tasks
• Resetting cvpadmin Password System Recovery

19.1 HTTPS Certificates Setup

CVP uses nginx to front and terminate all HTTPS connections. To support HTTPS, the server must be configured with a certificate. A self-signed certificate is generated at first bootup.

The guidelines to import a certificate are:

• Correctly fill the Subject Alternate Name (SAN) IP and DNS fields in both signed and self-signed certificates:
  • The SAN IP field must contain the IP addresses of all CVP cluster nodes; and the IP address of any IP load balancer used in front of CVP.
  • The SAN DNS field must contain the Fully Qualified Domain Name (FQDN) of the following elements:
    • All CVP cluster nodes
    • Any Canonical Names (CNAMEs) and round-robin DNS names
    • Any IP load balancer used in front of CVP

  Note: Zerotouch Provisioning (ZTP) and REST API calls can fail if signed certificates are uploaded without appropriate data in SAN fields.

• When importing a CVP certificate signed by an internal Certificate Authority (CA), the uploaded file must sequentially contain the full trust chain of PEM-encoded certificates like a server certificate, all intermediate certificates (if available), and a root certificate.

• Leave an empty line between every two certificates when importing multiple certificates into a single file.

  Note: Do not leave an empty line at the end of the file.

• If the server certificate is self-signed then the server and root certificates are one-and-the-same, so only that single certificate is required.

• CVP does not support wildcard certificates.

To install an HTTPS certificate, navigate to the Settings page (Click on the gear icon) > Certificates (See the figure below).
Figure 435: Certificates Page

Install the certificate using one of the following methods:

- Generating and Installing Self-Signed Certificate
- Installing Public Certificate
- Creating a CSR

19.1.1 Generating and Installing Self-Signed Certificate

Perform the following steps to generate and install a self-signed certificate:
1. On the Certificates page, click + Add.
CVP opens the Add CVP Certificate pop-up window. See the figure below.

![Add CVP Certificate Pop-Up Window](image)

**Figure 436: Add CVP Certificate Pop-Up Window**

2. Select Self Signed Certificate from the Certificate Type drop-down menu.
3. Provide the required information.
4. Click Add.
CVP opens the Confirm pop-up window informing that the existing certificate will be replaced. See the figure below.

![Confirm Pop-Up Window](image)

**Figure 437: Confirm Pop-Up Window**

5. Click OK.
CVP replaces the certificate and restarts the nginx service.

**Note:** When CVP is restarted, add an exception in the browser for the new certificate.

19.1.2 Installing Public Certificate
Perform the following steps to install a public certificate:

1. On the Certificates page, click **Import**.
   
   CVP opens the **Import CVP Certificate** pop-up window. See the figure below.

   ![Import CVP Certificate Pop-Up Window](image)

   **Figure 438: Import CVP Certificate Pop-Up Window**

2. Select **Available Certificate** from the **Import type** drop-down menu.
3. Upload private key and public certificate.
4. (Optional) Provide passphrase.
5. Click **Import**.
   
   CVP replaces the certificate and restarts the nginx service.

   **Note:** When CVP is restarted, add an exception in the browser for the new certificate.

### 19.1.3 Creating a CSR

A server Certificate Signing Request (CSR) file can be created by either your internal CA (along with an associated server key) or via CVP.

Perform the following steps to create a CSR:

1. On the Certificates page, click **Add**.
   
   CVP opens the **Add CVP Certificate** pop-up window.
2. Select **Certificate Signing Request** from the **Certificate Type** drop-down menu. See the figure below.

![Add CVP Certificate Dialogbox for CSR](image)

**Figure 439: Add CVP Certificate Dialogbox for CSR**

3. Provide the required information in all fields.
4. Click **Add**.
CVP opens the **Add CVP Certificate** dialog box displaying the complete CSR information. See the figure below.

![Add CVP Certificate Dialog Box](image)

**Figure 440: Add CVP Certificate Dialog Box with CSR Details**

5. Click **Download** to download the CSR file.

**Note:** The CA provides the root key (For example, `myCA.key`) and root certificate (For example, `myCA.pem`).

6. Create a configuration file to define the SAN fields.

**Example:**

```
bash-4.2# cat cvp100.nh.aristanetworks.com.ext
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment,
dataEncipherment
subjectAltName = @alt_names

[alt_names]
DNS.1 = cvp100.nh.aristanetworks.com
DNS.2 = cvp100.nh
DNS.3 = cvp11.nh.aristanetworks.com
DNS.4 = cvp11.nh
DNS.5 = cvp12.nh.aristanetworks.com
DNS.6 = cvp12.nh
DNS.7 = cvp13.nh.aristanetworks.com
DNS.8 = cvp13.nh
IP.1 = 10.81.45.243
IP.2 = 10.81.45.247
IP.3 = 10.81.45.251
```
7. Run the following command to generate a signed certificate from the downloaded CSR file.

```bash
openssl x509 -req -in downloaded_file -CA root_certificate -CAkey root_key -CAcreateserial -out updated_certificate_filename -days validity_period_in_days -sha256 -extfile SAN_DNS_IP_ext_filename
```

Example:

```bash
openssl x509 -req -in CSR.csr -CA myCA.pem -CAkey myCA.key -CAcreateserial -out cvp100.nh.aristanetworks.com.gui2.crt -days 365 -sha256 -extfile cvp100.nh.aristanetworks.com.ext
```

8. Edit the new certificate file to add the root certificate at the end of the file.

Example:

```bash
bash-4.2# cat cvp100.nh.aristanetworks.com.gui2.crt
-----BEGIN CERTIFICATE-----
MIIEqz2N2cDEzLm5oLmFyaXN0YW5ldHdvcmtzLmNvbYIIY3ZwMTMubmiHBApRLfOH
[snip]
Ta7HF9MPgc5X0lVN2PRwEkEuPNlJFEmuj7xute41NuTBmngqAeuhdTbVpxuB3eoY=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIID6zCCAtOgAwIBAgIJANW5kelAXMzhMA0GCSqGSIb3DQEBCwUAMIGLMQswCQYD
[snip]
2QoyIITDLQor1I/2z+RDHWcX8wEiYrsYkzyZDm/7NeGqfygXjnVJwFJbtjpB8Y=
-----END CERTIFICATE-----
bash-4.2#
```

Note: In case of intermediate certificates, add them between the new certificate and the root certificate.

9. In the CVP, click on the gear icon > Certificates.
10. Click **Import**.
CVP opens the **Import CVP Certificate** dialog box.

![Image](image.png)

**Figure 441: Import CVP Certificate to Bind with CSR**

11. Select **Bind with CSR** in the **Import type** dropdown menu.
12. In the **Public Certificate** section, click **Select files**.
14. Click **Import**.

### 19.1.4 **Renewing the Certificate Authority**

**Note:** The device communication will be disrupted when these steps are executed.

The Certificate Authority (CA) in the on-premise CVP can be renewed with the following steps:

1. SSH into the primary.
2. Reset the Certificate Authority (CA) and stop apiserver and ingest with the following commands.

```bash
yes | cvpi reset ca-init-v1
cvpi stop ingest cvpi
stop apiserver
```

3. Renew CA and aeris admin certificates with the following commands.

```bash
cvpi init ca-init-v1
/cvpi/apps/aeris/bin/create-admin-cert.sh
```

4. Restart all stopped components.

```bash
cvpi start all
```

5. Re-onboard all devices from the Device Onboarding page.
19.2 Customizing TLS and SSH Ciphers

CVP uses nginx to front and terminate all HTTPS connections. To support HTTPS, the server must be configured with a certificate. A selfsigned certificate is generated at first bootup.

- Configuring Custom TLS Ciphers
- Configuring Custom SSH Ciphers

19.2.1 Configuring Custom TLS Ciphers

Complete these steps to configure custom TLS ciphers.

1. Create a file named `/etc/nginx/conf.d/locations/cvp-ciphers.https.conf` that contains all of the SSL ciphers you need. Any open ssl cipher string can be used.
2. Run the following command to make sure the configuration does not contain any errors:

   ```bash
   /usr/sbin/nginx -t -c /etc/nginx/conf.d/cvpi-server.conf
   ```
3. Run the following command to reload nginx with the updated configuration.

   ```bash
   systemctl reload nginx
   ```

19.2.2 Configuring Custom SSH Cipher

Complete these steps to configure custom SSH ciphers.

⚠️ **Note:** Upgrading CVP removes custom SSH ciphers. You must reconfigure SSH ciphers after the upgrade.

1. Edit the `/etc/cvpi/sshd_config` to include custom ciphers and MAC definitions.
2. Run the following command to make sure the configuration does not contain any errors:

   ```bash
   sshd -t -f /etc/cvpi/sshd_config
   ```
3. Run the following command to reload sshd with the updated configuration.

   ```bash
   systemctl reload sshd
   ```

19.3 DHCP Service for Zero Touch Provisioning (ZTP) Setup

The ZTP process relies on a DHCP server to get devices registered with CVP. The DHCP server can be on the CVP, but is more commonly an external DHCP server.

1. Ensure the DHCP server is installed (it is installed by default in CVP).

   ```bash
   rpm -qa | grep dhcp
dhcp-common-4.1.1-43.P1.el6.x86_64
dhcp-4.1.1-43.P1.el6.x86_64
   ```
2. Edit the `/etc/dhcp/dhcpd.conf` file to include the option `bootfile-name`, which provides the location of the script that starts the ZTP process between CVP and the device.

In this example, DHCP is serving the `172.31.0.0/16` subnet.

Note: The `172.31.5.60` is the IP address of a CVP node, and it is recommended to use the HTTPS URL to point to the bootstrap file. This ensures that the specified devices, after they ZTP, will show up under the undefined container of the specified CVP.

```
[root@cvp1-dhcp dhcp]# cat dhcpd.conf
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#   see 'man 5 dhcpd.conf'
#
subnet 172.31.0.0 netmask 255.255.0.0 {
    range 172.31.3.212 172.31.5.214;
    option domain-name "sjc.arista networks.com";
}
host esx21-vm20 {
    option dhcp-client-identifier 00:0c:29:f9:21:99;
    fixed-address 172.31.3.211;
    option bootfile-name "https://172.31.5.60/ztp/bootstrap";
}
host esx21-vm22 {
    option dhcp-client-identifier 00:0c:29:d1:64:e1;
    fixed-address 172.31.3.213;
    option bootfile-name "https://172.31.5.60/ztp/bootstrap";
}
```

3. Restart the DHCP service after any configuration changes with the `service dhcpd restart` command.

4. Configure `dhcppd` to start on system boot with the `chkconfig dhcppd on` command.

Related topics:
- RADIUS or TACACS Authentication Setup
- Background Tasks
- Resetting cvpadmin Password
- HTTPS Certificates Setup

19.4 RADIUS or TACACS Authentication Setup

1. Edit the client file `/etc/raddb/clients.conf` by adding the following:

```
# CVP
client 172.31.0.0/16 {
    secret = cvpsecret
}
```

2. To add more, enter the following:

```
# Arista Networks
client 172.17.0.0/16 {
    secret = cvpsecret
}
client 172.18.0.0/16 {
    secret = cvpsecret
}
client 172.20.0.0/16 {
    secret = cvpsecret
}
```
The default `clients.conf` file will have a section for local host. The user should either delete the whole section or comment it out. If CVP will be connecting to RADIUS on local host, you have to add a client entry for `127.0.0.0/16` (same as above).

1. Edit the `users` file `/etc/raddb/users` by adding the following:

   ```
   # CVP
cvpuser  Cleartext-Password := "cvpuser"
   Service-Type = NAS-Prompt-User

   start radiusd:  sudo service radiusd start
   enable radiusd on boot: sudo chkconfig radiusd on
   ```

2. If RADIUS is not working, run the server in debug mode.

   ```
   # service radiusd stop
   # /usr/sbin/radiusd -X -f
   ```

   RADIUS will now run on the terminal with verbose output. This will let you know if RADIUS is receiving auth requests and what failure is being hit for the request. After you are done debugging, Control-C the process and start radiusd as a service.

   **Note:** You may have to either disable iptables or firewall.serviced depending on the OS version. You could also configure it to allow traffic on ports 1812 and 1813 on the Radius server.

**Related topics:**
- Background Tasks
- Resetting cvpadmin Password
- HTTPS Certificates Setup
- DHCP Service for Zero Touch Provisioning (ZTP) Setup

### 19.5 Background Tasks

CloudVision provides command-line tools that can be executed from the linux shell or scheduled as cronjobs either on a CVP node or on an external server, for the following tasks:

- Compliance checks
- Snapshots
- Backups

The tools are available by default on the CVP nodes in the `/cvpi/tools/` directory. The tools can be used on an external linux server by downloading the `cvp-tools-<version> .tgz` from [https://www.arista.com](https://www.arista.com) to the external linux server.

Detailed help on the tool is available by using the `--h` option with the tool:

```
cvpi/tools/compliance.py --h
cvpi/tools/backup.py --h
```

**Related topics:**
- Resetting cvpadmin Password
- HTTPS Certificates Setup
- DHCP Service for Zero Touch Provisioning (ZTP) Setup
19.5.1 Scheduling and Viewing Cronjobs

To schedule cronjobs to perform periodic compliance checks or snapshots, insert commands into the crontab using the following command:

```
crontab -e
```

**Note:** When inserting commands to schedule cronjobs, you only need to do this on one node of the cluster.

**Example**

To schedule a periodic compliance check and snapshot to be performed hourly on the tenant container, and a backup to be performed daily at 2:00 am, insert the following lines into the crontab file on the primary node if not already present. In this example, the user is named “me” and the password is “pwd”.

```
0 * * * * /cvpi/tools/compliance.py --user me --password pwd --containers tenant
0 2 * * * /cvpi/tools/backup.py --limit 5
```

To see the active cronjobs, use the following command:

```
crontab -l
```

To view the console outputs of the cronjobs tail, view (open) the following log file:

```
tail -f /var/log/cron
```

**Related topics:**
- Resetting cvpadmin Password
- HTTPS Certificates Setup
- DHCP Service for Zero Touch Provisioning (ZTP) Setup
- RADIUS or TACACS Authentication Setup

19.6 Resetting cvpadmin Password

If the `cvpadmin` password is lost or forgotten, you can reset it from any of the CVP nodes using the following steps.

1. Log into a CVP node Linux shell as root user.
2. Navigate to `cd /cvpi/lib`
3. Execute the following command:

```
/cvpi/tools/update-mgmt-password -password <new password>
```

**Note:** Do not set the new password to the string "cvpadmin".

**Related topics:**
- HTTPS Certificates Setup
- DHCP Service for Zero Touch Provisioning (ZTP) Setup
- RADIUS or TACACS Authentication Setup
- Background Tasks
Troubleshooting and Health Checks

If you encounter an issue when using CloudVision appliance, check to see if there are troubleshooting steps for the issue.

- System Recovery
- Health Checks
- Resource Checks

20.1 System Recovery

System recovery should be used only when the CVP cluster has become unusable and other steps, such as performing `cvpi watchdog off`, `cvpi stop all`, and then, `cvpi start all`, `cvpi watchdog on` have failed. For example, situations in which, regardless of restarts, a `cvpi status all` continues to show some components as having a status of UNHEALTHY or NOT RUNNING.

There are two ways to completely recover a CVP cluster:

- VM Redeployment
- CVP Re-Install without VM Redeployment

⚠️ Note: A good backup is required to proceed with either of these system recoveries.

20.1.1 VM Redeployment

Complete the following steps:

1. Delete all the CVP VMs.
2. Redeploy the VMs using the procedures in.
3. Issue a `cvpi status all` command to ensure all components are running.
4. Login to the CVP GUI as `cvpadmin/cvpadmin` to set the cvpadmin password.
5. From the Backup & Restore tab on the Setting page, restore from the backup.

20.1.2 CVP Re-Install without VM Redeployment

Complete these steps:

1. Run `cvpReInstall` from the Linux shell of the primary node. This may take 15 minutes to complete.

   ```bash
   [root@cvp99 ~]# cvpReInstall
   0. Log directory is /tmp/cvpReinstall_17_02_23_01_59_48
   Existing /cvpi/cvp-config.yaml will be backed up here.
   ...
   ...
   Complete!
   
   CVP configuration not backed up, please use cvpShell to setup the cluster
   ```
CVP Re-install complete, you can now configure the cluster

2. Re-configure using the procedure in Shell-based Configuration. Log into the Linux shell of each node as cvpadmin or su cvpadmin.

3. Issue a cvp status all command to ensure all components are running.

4. Login to the CVP GUI as cvpadmin/cvpadmin to set the cvpadmin password.

5. From the Backup & Restore tab on the Setting page, restore from the backup.

Related topics:
- Health Checks
- Resource Checks

20.2 Health Checks

The following table lists the different types of CVP health checks you can run, including the steps to use to run each check and the expected result for each check.
<table>
<thead>
<tr>
<th>Component</th>
<th>Steps to Use</th>
<th>Expected Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network connectivity</td>
<td>ping -f across all nodes</td>
<td>No packet loss, network is healthy.</td>
</tr>
<tr>
<td>HBase</td>
<td>`echo list</td>
<td>/cvpi/hbase/bin/hbase shell</td>
</tr>
</tbody>
</table>
| All daemons running on all nodes, bypass `cvpi status all` | On all nodes: `su - cvp -c "/cvpi/jdk/bin/jps"` | On primary and secondary nodes, 9 processes including jps.  
  - 3149 HMaster  
  - 2931 NameNode  
  - 2797 QuorumPeerMain  
  - 12113 Bootstrap  
  - 3040 DFSZKFailoverController  
  - 2828 JournalNode  
  - 11840 HRegionServer  
  - 12332 Jps  
  - 2824 DataNode  
  On tertiary 6 processes:  
  - 2434 JournalNode  
  - 4256 HRegionServer  
  - 2396 QuorumPeerMain  
  - 2432 DataNode  
  - 4546 Jps  
  - 8243 Bootstrap |
| Check time is in sync between nodes    | On all nodes run `date +%s`                      | UTC time should be within a few seconds of each other (typically less than one second). Up to 10 seconds is allowable. |
| I/O slowness issues                    | The disk I/O throughput is at an unhealthy level (too low). | Use the `cvpi resources` command to find out whether the disk I/O throughput is at a healthy level or unhealthy level. The disk I/O throughput reported in the command output is measured by the Virtual Machine.  
See Running Health Checks for an example of the output of the `cvpi resources` command. |

- Running Health Checks
20.2.1 Running Health Checks

Run the `cvpi resources` command to execute a health check on disk bandwidth. The output of the command indicates whether the disk bandwidth is at a healthy level or unhealthy level. The threshold for healthy disk bandwidth is 20MBs.

The possible health statuses are:

- **Healthy** - Disk bandwidth above 20MBs
- **Unhealthy** - Disk bandwidth at or below 20MBs

The output is color coded to make it easy to interpret the output. Green indicates a healthy level, and red indicates an unhealthy level (see the example below).

This example shows output of the `cvpi resources` command. In this example, the disk bandwidth status is healthy (above the 20MBs threshold).

![Figure 444: Example output of cvpi resources command](image)

Related topics

- **Resource Checks**
20.3 Resource Checks

CloudVision Portal (CVP) enables you to run resource checks on CVP node VMs. You can run checks to determine the current data disk size of VMs that you have upgraded to CVP version 2017.2.0, and to determine the current memory allocation for each CVP node VM.

Performing these resource checks is important to ensure that the CVP node VMs in your deployment have the recommended data disk size and memory allocation for using the Telemetry feature. If the resource checks show that the CVP node VM data disk size or memory allocation (RAM) are below the recommended levels, you can increase the data disk size and memory allocation.

These procedures provide detailed instructions on how to perform the resource checks and if needed, how to increase the CVP node VM data disk size and CVP node VM memory allocation.

- Running CVP node VM Resource Checks
- Increasing Disk Size of VMs Upgraded to CVP Version 2017.2.0
- Increasing CVP Node VM Memory Allocation

20.3.1 Running CVP node VM Resource Checks

CloudVision Portal (CVP) enables you to quickly and easily check the current resources of the primary, secondary, and tertiary nodes of a cluster by running a single command. The command you use is the `cvpi resources` command.

Use this command to check the following CVP node VM resources:

- Memory allocation
- Data disk size (storage capacity)
- Disk throughput (in MB per second)
- Number of CPUs

Complete the following steps to run the CVP node VM resource check.

1. Login to one of the CVP nodes as root.
2. Execute the `cvpi resources` command.

The output shows the current resources for each CVP node VM

- If the total size of sdb1 (or vdb1) is approximately 120G or less, you can increase the disk size to 1TB (see Increasing Disk Size of VMs Upgraded to CVP Version 2017.2.0).
- If the memory allocation is the default of 16GB, you can increase the RAM memory allocation (see Increasing CVP Node VM Memory Allocation).

![Figure 445: Using the cvpi resource command to run CVP node VM resource checks](image-url)
20.3.2 Increasing Disk Size of VMs Upgraded to CVP Version 2017.2.0

If you already upgraded any CVP node VMs running an older version of CVP to version 2017.2.0, you may need to increase the size of the data disk of the VMs so that the data disks have the 1TB disk image that is used on current CVP node VMs.

CVP node VM data disks that you upgraded to version 2017.2.0 may still have the original disk image (120GB data image), because the standard upgrade procedure did not upgrade the data disk image. The standard upgrade procedure updated only the root disk, which contains the Centos image along with rpms for CVPI, CVP, and Telemetry.

Note: It is recommended that each CVP node have 1TB of disk space reserved for enabling CVP Telemetry. If the CVP nodes in your current environment do not have the recommended reserved disk space of 1TB, complete the procedure below for increasing the disk size of CVP node VMs.

Pre-requisites

Before you begin the procedure, make sure that you:

- Have upgraded to version 2017.2.0. You cannot increase the data disk size until you have completed the upgrade to version 2017.2.0 (see Migrating the DNS and NTP Server).
- Have performed the resource check to verify that the CVP node VMs have the data disk size image of previous CVP versions (approximately 120GB or less). See Running CVP node VM Resource Checks.

Procedure

Complete the following steps to increase the data disk size.

1. Turn off cvpi service by executing the systemctl stop cvpi command on all nodes in the cluster. (For a single-node installation, run this command on the node.)
2. Run the cvpi -v=3 stop all on the primary node.
3. Perform a graceful power-off of all VMs.

Note: You do not need to unregister and re-register VMs from vSphere Client or undefine and redefine VMs from kvm hypervisor.
4. Do the following to increase the size of the data disk to 1TB using the hypervisor:
   - **ESX:** Using vSphere client, do the following:
     a. Select the Virtual Hardware tab, and then select hard disk 2.
     b. Change the setting from 120GB to 1TB.
     c. Click OK.
   - **KVM:** Use the `qemu-img resize` command to resize the data disk from 120GB to 1TB. Be sure to select `disk2.qcow2`.

   ![Figure 446: Using vSphere to increase data disk size](image)

5. Power on all CVP node VMs, and wait for all services to start.
6. Use the `cvpi status all` command to verify that all the cvpi services are running.
7. Run the `/cvpi/tools/diskResize.py` command on the primary node. (Do not run this command on the secondary and tertiary nodes.)
8. Run the `df -h /data` command on all nodes to verify that the `/data` is increased to approximately 1TB.
9. Wait for all services to start.
10. Use the `cvpi -v=3 status all` command to verify the status of services.
11. Use the `systemctl status cvpi` to ensure that cvpi service is running.

### 20.3.3 Increasing CVP Node VM Memory Allocation

If the CVP Open Virtual Appliance (OVA) template currently specifies the default of 16GB of memory allocated for the CVP node VMs in the CVP cluster, you need to increase the RAM to ensure that the CVP node VMs have adequate memory allocated for using the Telemetry feature.

**Note:** It is recommended that CVP node VMs have 32GB of RAM allocated for deployments in which Telemetry is enabled.
You can perform a rolling modification to increase the RAM allocation of every node in the cluster. If you want to keep the service up and available while you are performing the rolling modification, make sure that you perform the procedure on only one CVP node VM at a time.

Once you have completed the procedure on a node, you repeat the procedure on another node in the cluster. You must complete the procedure once for every node in the cluster.

**Pre-requisites**

Before you begin the procedure, make sure that you:

- Have performed the resource check to verify that the CVP node VMs have the default RAM memory allocation of 16GB (see Running CVP node VM Resource Checks).
- Make sure that you perform a GUI-based backup of the CVP system and copy the backup to a safe location (a location off of the CVP node VMs). The CVP GUI enables you to create a backup you can use to restore CVP data.

**Procedure**

Complete the following steps to increase the RAM memory allocation of the CVP node VMs.

1. Login to a CVP node of the cluster as cvp user.
2. Using the `cvpi status cvp shell` command, make sure that all nodes in the cluster are operational.

   ![cvpi status cvp shell command](image)

   **Figure 447: cvpi status cvp shell command**
3. Using vSphere client, shutdown one CVP node VM by selecting the node in the left pane, and then click the **Power off the virtual machine** option.

![Power off the virtual machine](image1)

**Figure 448: Power off the virtual machine**

4. Click to confirm powering off the virtual machine.

![Powering off confirmation](image2)

**Figure 449: Powering off confirmation**
5. On the CVP node VM, increase the memory allocation to 32GB by right-clicking the node icon, and then choose **Edit Settings**.

![Figure 450: Edit Settings](image)

The **Edit Resource Settings** dialog appears.
6. Do the following to increase the memory allocation for the CVP node VM:
   - Using the **Memory** option, click the up arrow to increase the size to **32GB**.
   - Click the **OK** button.

   The memory allocation for the CVP node VM is changed to 32GB. The page refreshes, showing options to power on the VM or continue making edits to the VM properties.
7. Click the **Power on the virtual machine** option.

![Image of VMware vSphere Web Client](image)

**Figure 452: Power on the virtual machine**

8. Wait for the cluster to reform.

9. Once the cluster is reformed, repeat **step 1 through step 7** one node at a time on each of the remaining CVP node VMs in the cluster.

**Related topics:**

- System Recovery
- Health Checks
CloudVision Studios

CloudVision Studios is a powerful tool for managing the configuration of network features. The intuitive interface is fully customizable, meaning that you can create and edit your own network features for configuration. This gives you complete control over the configuration of your network.

Requirements
To use Studios, the following requirements must be installed:

• CloudVision minimum version: 2021.2.0

Features
The following features are available:

• Out-of-the-box support for common workflow configurations
• Unified Day-1 and Day-2 workflows
• Customizable Studios for bespoke workflow configuration
• In-depth and accessible change control
• Simultaneous configuration and management of separate network features
• First-class gRPC + REST APIs that easily integrate third-party resources

Known Limitations
The following is a list of known limitations in the beta-version of CloudVision Studios:

• Configuration-reconciliation: this is handled by the Network Provisioning UI
• CloudVision Studios cannot be applied to devices in an undefined container
• Studios rollback: once a Workspace and its configuration have been submitted, a user will need to undo those changes by creating and submitting a new Workspace
• Studio input actions: scripts that automatically complete Studio inputs on a user’s behalf (e.g. integrating with an IPAM) are not yet supported
• Per-Studio or per-device RBAC: Phase 1 will include per-user roles and permission management that let users read and write Studio data, but do not limit user roles to specific Studios
• Users should only have one Workspace open at a time. If users have two open Workspaces that contain conflicts with one another and submit one of those Workspaces, the other may not be able to build correctly. Consequently, that second Workspace may need to be abandoned or reconfigured
• Workspaces should not be created on CloudVision clusters that manage more than 100 devices

21.1 Getting Started with Studios

Before using Studios, it is important to understand the two main elements: the Studios and Workspaces. You will use the two of these together to make changes to the mainline configuration of your network.
Studio

A Studio is an input template for a particular aspect or feature of a network. It defines the attributes of any devices belonging to that feature. All your Studios are visible on the Studios home screen.

When you visit Studios for the first time, you will see that there are already several built-in Studios. These cover some common network features, and each is explained separately in the section Built-In Studios. You can create your own custom-built Studios so that you can determine a new network feature for configuration.

Workspace

A Workspace is what you use to create, configure, or edit a Studio’s inputs, and to tag the devices that a Studio affects. It can be used to configure one or more Studios, which means that you can implement configuration changes across multiple network features at the same time.

There are three states a Workspace can have:

- **Submitted**: A Workspace that has configured one or more Studios and been submitted for approval in Change Control
- **Open**: A Workspace that has been created but not yet submitted
- **Abandoned**: A Workspace that has been discarded before submission

**Note**: Give any Workspace or Studio you create a relevant name and description, describing how it relates to the configuration of your network.

21.2 Accessing Studios

Studios is currently in beta-version and needs to be enabled in the CloudVision settings before it can be used.

To enable Studios

1. Select the **Settings** icon in the top-right of CloudVision and browse the list of features for **Studios (Beta)**. Switch the toggle to the **ON** position.

![Figure 453: Enabling Studios](image)
2. Once you have enabled Studios, click on the **Provisioning** tab.

![Provisioning Tab](image)

**Figure 454: Provisioning Tab**

3. Select **Studios** on the sidebar.

![Selecting Studios from the sidebar](image)

**Figure 455: Selecting Studios from the sidebar**

4. The Studios home screen is displayed. This is where you will initiate all your configurations. You can view your Workspaces and see their statuses by selecting on **Workspaces** under **Studios**.

### 21.3 Workflow Overview

Whenever you use Studios, you will begin by either creating a new Workspace or selecting an open Workspace. You will use a Workspace to implement any changes you want to make to one or more Studios. Once you have configured the changes, you will submit the Workspace. It will then be available in Change Control for the relevant user to approve or reject.

If you are using Studios for the first time, create a Workspace and then select the Inventory and Topology Studio to commission devices for use in Studios.
21.3.1 Commissioning Devices for Use in Studios

To configure any devices in Studios and Workspaces, you will first need to commission them for use in Studios. This is the purpose of the Inventory and Topology Studio.

To commission devices, you will first create a Workspace and then select the Inventory and Topology Studio. There you will add devices and configure their interface connections. These devices can then be assigned to another Studio using tags.

Note: You will not be able to assign devices to any Studios until you have commissioned devices using the Inventory and Topology Studio.

21.3.2 Creating a Workspace
1. Click **Create Workspace**, which will bring up the Create New Workspace modal.

![Create Workspace](image1)

**Figure 457: Create a Workspace**

2. Give your new Workspace a name and a description, and then click **Create**.

![Create Workspace](image2)

**Figure 458: Name and Describe the Workspace**

The Workplace you have created can now be used to manage the configuration of one or more Studios. It will be available for use in the Workspace dropdown menu.

### 21.3.3 Configuring an Existing Studio

To begin the process of configuring a Studio, you will need to either create a Workspace or already have an open Workspace available for use.
1. Create a Workspace or click the Workspace dropdown menu and select the open Workspace that you want to configure the Studio inputs with.

![Figure 459: Selecting a Workspace](image)

**Figure 459: Selecting a Workspace**

2. Click on the existing Studio that you want to edit.

3. Manage the devices the Studio is assigned to by clicking **Tag Assignment** and selecting **Assign Tags**.

![Figure 460: Tag Assignment](image)

**Figure 460: Tag Assignment**

For more information on how to use Tags, see Tags.

- **Note:** If the devices you wish to use for the Studio are not available for selection, you will need to commission them for Studios with the Inventory and Topology Studio.

4. Navigate through the Studio interface and configure your new input values.

If you want to add or remove the input variables themselves, see Editing a Studio’s Schema.
5. Once all the changes have been made, you can click **Review Workspace**.

Figure 461: Review Workspace

You will now be brought to the Build Screen that forms part of the Workspace submission process.

**Note:** If you want to make changes to multiple Studios with the same Workspace, do not click **Review Workspace** at Step 4. Return to the Studios home screen and repeat Steps 1-3, selecting the same Workspace for each Studio you want to configure.

### 21.3.4 Creating a New Studio

A new Studio will add a custom network feature to your Studio Suite, which you can then configure by defining its inputs. When creating a new Studio, you select these inputs and build its interface with the use of Schema.

1. Click the **Workspace** menu and select the Workspace you want to use to create the new Studio.

Figure 462: Select Workspace
2. Click the **New Studio** button in the header.

![Figure 463: Create New Studio](image1.png)

3. The Edit screen is displayed. You must enter a name and description for the new Studio.

4. After providing the Studio a name and description, you can configure the data that the Studio will collect as inputs. First click **Schema** then click **Add Root Input**.

![Figure 464: Add Root Input](image2.png)
5. Select one of the inputs to configure a variable of the Studio from the section labelled Add New Input. For an explanation of schema inputs, see Input Types.

![Add New Input](image)

**Figure 465: Add New Input**

*Note:* You can configure the Schema input as a CLI configuration by using the Template function once you have created the new input with Schema.

6. Once all the changes have been made, click **Review Workspace** to begin the build process. Once that is completed, the Studio will appear in your Studio Suite.

## 21.3.5 Submitting a Workspace

1. Click the **Review Workspace** button in the header.

![Review Workspace](image)

**Figure 466: Review Workspace**

2. The Workspace will be automatically built for submission, which includes input validation, compiling the configuration, and the validation of the configuration. On the Build screen, you will be able to review the proposed configuration changes.

*Note:* The Workspace is automatically built only for the first time that you click **Review Workspace**. Any subsequent changes made after that will require that you re-build the Workspace by clicking **Build**.
3. Once satisfied, you can click **Submit Workspace**.

![Submit Workspace](image1)

**Figure 467: Submit Workspace**

4. You will be presented with a modal that will bring you to Change Control.

![Workspace Submitted](image2)

**Figure 468: Workspace Submitted**

The relevant user will then be able to approve the Workspace, and its configuration will then become part of the mainline configuration of your network.

21.4 **Studio Elements and Functions**

To make the most of Studios, you will need to know a little more about the tools you have control over. This section explains the full use of the different components that make up the Studios interface, which all either form a part of or enhance the workflows.

21.4.1 **Reviewing a Workspace**

The Workspace build screen appears after you have clicked **Review Workspace**. It provides you with important information on the Workspace’s configuration before submitting to Change Control for approval.

There are several elements in the screen.
The most important element for indicating if there are any problems with the Workspace configuration is the Build Progress section. It shows you if the Workspace configuration contains any conflicts and if device configlets have been compiled correctly. It is composed of three components:

- **Input Validation**: Checks whether the values of the inputs follow the schema rules.
- **Configlet Compilation**: Identifies any coding errors.
- **Config Validation**: Determines whether the affected devices can support the proposed configuration.

By clicking View Build Details, you can see each of these components for the individual devices that the configuration affects.

This shows you the build progress for each device, and it helps you identify the devices the build progress has failed on.

The Workspace Summary table provides a brief overview of the type of modifications that a Workspace will make.
On the left-hand side, you can see each of the Studios that the configuration affects. On the right is displayed the type of change that has been made with the Workspace. By clicking on the type of configuration change, you will be brought to the screen in which that change was implemented.

Click View All Modification Details, to view all the configuration changes displayed together in the manner of Schema inputs.

21.4.1.3 Proposed Configuration Changes

Review the Proposed Configuration Changes to compare the Workspace configuration changes with what currently exists in the network.

This is shown for each individual device, and clicking on the device name will show you its proposed configuration.

On the left are your proposed changes and on the right is the existing configuration. It is color-coded for easy reference:

- Green = additions
- Blue = modifications
- Red = deletion
21.4.2 Tags

A tag is a value-label pair that you apply to a device or an interface. User Tags allows you to group devices or interfaces that share a common characteristic under a tag. By way of example, you could have:

**Role**: Spine or **DC**: New York

With Studios, you can then use these User Tags to create a separate configuration for different groups of devices. For instance, if you wish to separately configure the spines and leafs of a data center fabric, you can do so by tagging the relevant devices as spines or leafs.

**Note**: User Tags are not just for Studios, they have already been implemented for use with Event Customization, Event Notification, and Dashboard Configuration.

21.4.2.1 User Tags and System Tags

Only User Tags are supported in Studios, which are tags created and defined by a user of CloudVision through the following process.

System Tags are created by CloudVision and based upon characteristics or attributes of devices. These tags cannot be created or edited by you or any other CloudVision user. System tags are not static and could affect the stability of any Workspace configurations you create. For this reason, only User Tags are available in Studios.

Any changes made to User Tags can impact the configuration of devices. For this reason, User Tags can only be deployed inside a Workspace. When you build the Workspace and review its changes, you will then see any impact the tags have on the Workspace proposed configuration and can rectify it accordingly.

21.4.2.2 Creating Tags

To tag devices with User Tags, you will need to leave the Studios environment:

1. Click on the **Provisioning** tab, if necessary.

   ![Provisioning Tab](Figure 474: Provisioning Tab)
2. Click on **Tags**.

![Figure 475: Tags](image)

3. Click **Create Workspace** or select an open Workspace from the dropdown menu.

![Figure 476: Create Workspace](image)

4. Select one or more devices or interfaces, and then enter a value under **Add or Create Tags**.

![Figure 477: Add or Create Tags](image)

5. Click **Create and Assign** to give the tag to the selected device or devices.

**21.4.2.3 Applying Tags in Studios**

You will use User Tags in two places in Studios: as the field data for a resolver input, and when assigning a Studio to devices.
Resolver Input

Resolver Input is a Container Type that allows you to apply the input variables associated with it to a selection of devices. The following is an example of a resolver input, which, in this case, allows you to select tagged devices that you will assign to an NTP server.

![Figure 478: Resolver Input](image)

Studio Tag Assignment

Within each Studio, with the exception of Inventory and Topology, there is a Tag Assignment option.

![Figure 479: Tag Assignment](image)

You will use Tag Assignment to specify the devices that any given Studio configuration affects. All of the tagged devices you select must already have been commissioned for use in Studios with the Inventory and Topology Studio. In order to assign devices, click Assign Tags and then enter a device tag query.

![Figure 480: Tag Assignment](image)

You can edit these tagged devices at any point with a Workspace by clicking the pencil icon to the right of the last tag.
You can use tags to apply an entire Studio to a selected group of devices. For example, you may want the configuration of a Studio to relate only to devices in a particular data center. All devices in that data center can be tagged under a label, and you can assign that Studio to that tag label.

21.4.3 Schema

Schema are the input variables of a Studio and are used to collect data from a CloudVision User. They are defined when either Creating a New Studio or editing an existing Studio. You do this by selecting an input type in the Studio Edit screen and then completing a form.

![Figure 481: Schema](image)

21.4.3.1 Editing a Studio Schema

Only custom Studios can be edited.

**Note:** Built-in Studio schemas cannot be edited.

To edit a custom Studio Schema, create a new Workspace or select an open Workspace and then click the **Edit** button within a Studio.

![Figure 482: Editing a Studio Schema](image)

At the Studio Edit screen, you can select Schema and the process will be the same as creating a new Studio.

**Note:** While you cannot edit built-in Studios, you can export and then import the Studio as a clone that you can edit.
21.4.3.2 Input Types

Schema inputs can be broadly classified into two categories: Base Types and Container Types.

Base Types are inputs that hold a real value and have a defined format. In general, these inputs can be validated to ensure that their value matches the defined format. You can also add constraints that restrict the values that can be entered in their fields.

Container Types are inputs that group one or more Base Types into a unit. They can be used to assign a set of inputs to a specific group of devices, allow a Studio to provide multiple values for a given input, or to group multiple Base Types and make them into an input unit.

Each input type is further divided into different data types:

Base Types consist of:
- String
- Integer
- Float
- Boolean

Container Types consist of:
- Resolver
- Collection
- Group

You can find a full description of each data type in Appendix 2: Schema Input Types.

21.4.4 Template

Once you have defined an the variables for an input under Schema, you can use Template to convert the input into a CLI configuration. You can click on the input you want to configure, and then click Template.

![Figure 483: Template](image)

21.4.4.1 Mark-Up Language

You have a choice of two languages when writing a Template, Mako or Jinja2. The default setting is Mako, but you can select Jinja2 or change back to Mako by using the below toggle:

Both Mako and Jinja2 have a lightweight syntax that allows you to leverage the underlying Python of Studios to create an effective Template.
You can find a primer on Mako syntax here and for Jinja2 here. There is also a short guide for using Mako for Template in Appendix 1: Mako Syntax.

21.4.5 Importing and Exporting Studios

Studios are saved and distributed as .yaml files. The file contains the entire schema definition, template, and input values. You can easily import and export Studios using CloudVision.

Importing

1. Click Create Workspace or select an open Workspace from the dropdown menu.
2. Click Import.

![Figure 484: Import](image)

3. On the Import Studio modal, select the Studio file and then click Import.

The imported Studio will now be part of your Studio Suite.

Exporting

1. From your Studio Suite, select the Studio you wish to export.
2. Within the Studio screen, click Export.

![Figure 485: Export](image)

3. A pop-up box will appear, which will ask you the details for downloading the file. Enter the details and click Download or Save.

21.5 Built-In Studios

There are currently seven built-in Studios in the beta-version, which each relate to a network feature. You can create your own custom-built Studios by following the Creating a New Studio instructions.

Any devices you wish to include in a Workspace configuration must already have been commissioned by using the Inventory and Topology Studio. Consequently, this is the first Studio that you should use and which enables the use of all other Studios.

When using any Studio, except for Inventory and Topology, it is important to remember that you need to assign User Tags to the Studio. These tags relate to devices commissioned with the Inventory and Topology Studio. Only devices tagged to a Studio will be affected by any proposed configuration.

When you open up any Studio, other than Inventory and Topology, you will see the tag assignment option. Click Assign Tags and enter the User Tags for the devices you want the Studio to affect.
21.5.1 Inventory and Topology

This will be the first Studio that you’ll use, because it is responsible for making devices and their interfaces available for configuration in Studios. It serves as a control point for separating or combining your wider network topology with the topology that Studios configures.

With the Inventory and Topology Studio, you can accept devices and interface changes in your wider network topology and incorporate those devices and changes into Studios configuration. You can also use it to manually add devices and configure their interfaces for use in Studios.

Note: The Updates tab is the easiest way to commission devices for Studios, and is what you should use most often. The Updates tab receives and displays device and interface changes in your wider network, which you can quickly accept or ignore for use in Studios.

21.5.1.1 Adding a Device and Configuring its Interfaces

When you click on Inventory and Topology, the Inventory and Topology page is displayed.

From the Inventory and Topology page you can add devices and then configure their interfaces. Any device added here will be made available for use in other Studios. Once the information for each device has been entered, click View. This will display the Devices page, which shows the interfaces on a selected device. From this page you can add device interfaces and configure their connections to other device interfaces.
21.5.1.2 Managing Updates to the Network Topology

Select the Updates tab, to view new devices and amendments to device connections in your network. You can quickly add any device or interface changes in your network by using Updates.

![Device Interfaces](image)

**Figure 488: Inventory and Topology - Device Interfaces**

*Note:* All connections are bidirectional. It is not possible to create unidirectional connections.

All updates and their type will be listed here, and you can choose to accept these updates or ignore them. Accepting adds devices and their interfaces for use in Studios and updates any configuration in Studios the device relates to. Ignoring the updates will omit them from being configured in any Studio.

*Note:* In the beta-version, clicking Ignore for Now will result in updates remaining in the Review Updates list.

21.5.2 Connectivity Monitor

The Connectivity Monitor Studio configures an EOS feature to send probes to a remote host. EOS will then report latency, jitter, round-trip times, and HTTP connectivity to those remote hosts. The corresponding telemetry for the monitored hosts can be found under Devices and Dashboards.

With Connectivity Monitor, you can set up or update the hosts and set which hosts should be monitored.
Select the Connectivity Monitor Studio to display the following screen.

Figure 490: Connectivity Monitor

From the Connectivity Monitor screen, the hosts that the probes will monitor can be defined. Enter a name for the device followed by the IP address and a description for the host. Enter an optional HTTP URL, which will configure the EOS to measure the HTTP response time for that URL.

Groups of devices can be defined for monitoring by an EOS probe using Host Monitoring. Use device tags to define the host groups.

Figure 491: Host Monitoring

After one or more device tags have been defined, click on the arrow to the right. This will allow you to add hosts to the tagged group for monitoring. These hosts must already have been defined in the previous Hosts section.

Figure 492: Host Monitoring - Monitored Hosts

After the Studio has been configured, review the Workspace and submit to Change Control. Once it has been approved, the results of the configured monitoring can be viewed by selecting the Connectivity Monitor under Devices.
21.5.3 Date and Time

The Date and Time Studio is used to set the device time zones and to assign devices to NTP servers.

21.5.3.1 Setting a Device Time Zone

You can assign time zones to a set of tagged devices, and set a default time zone that is applied to all assigned devices not specified with a device tag query.

To set a time zone, click Add Device Time Zone or Add Default Rule. If relevant, enter a device tag, and then select a time zone from the drop down menu.

Time zones are ordered alphabetically. If the desired time zone is not in the list, select Other and enter a name for that time zone in the Other Time Zone field.
Figure 494: Setting a Device Time Zone

Once you have assigned time zones to devices and optionally set the default time zone, review and submit the Workspace. Once it is approved and executed in Change Control, the new settings will come into effect on your network.

21.5.3.2 Configuring the NTP Settings

You can assign devices to an NTP server using device tags. Click Add NTP Setting and then enter a device tag to select devices with that tag. When done, click the arrow on the right.

Add NTP servers for these tagged devices by clicking Add NTP Server. Multiple servers can be added for the selected device tag, but only one server should be set as preferred. You can also enable iburst, which will send eight packets to the NTP server on start-up instead of a single packet. This will allow for faster synchronization.
When you have assigned NTP servers to all the device tags, review and submit the Workspace. Once it is approved and executed in Change Control, the NTP settings will come into effect on your network.

### 21.5.4 Interface Configuration

The Interface Configuration Studio is used to provision interfaces that have been defined elsewhere. With it, you can configure interface speed, switchport mode, access VLAN or tagged VLANs, and enable or disable the interface. You can set up profiles with configurations for these attributes, which can then be applied to multiple interfaces. The use of profiles means that you do not need to separately configure repeating attributes for each device.

Select **Interface Configuration** to display the following screen.

You can either configure an interface belonging to an individual device, or you can configure an interface profile.

#### 21.5.4.1 Configure a Device
All devices that have been commissioned for Studios using Inventory and Topology Studio will be listed under Device. Select the device to configure one or more interfaces for by clicking the arrow on the right.

![Figure 498: Configure a device](image)

The list of interfaces that can be configured on this device and the available options are displayed. Scroll to the right to see all of the available options.

There is also a profile option, which can be used to assign a profile to the device. If you assign a profile, you do not need to enter a value for any other inputs; any values that you do enter for other inputs will override the values of the profile.

**Note:** If a device you want to configure is not available for selection, add it using the Inventory and Topology Studio.

### 21.5.4.2 Configuring a Profile

Profiles are used to avoid having to configure each device interface separately. You can create profiles with different characteristics and then assign a single profile to a device interface, which will apply the configuration associated with that profile to the interface of the device.

On the homescreen of Interface Configuration, click **Add Profile**. Enter a profile name and click the arrow on the right. The following screen is displayed.
From the Profile screen, the speed, the switchport mode, the VLAN access, or tagged VLANs can be set. The mode selected for the interface may present you with more input options. When entering a description for the profile, enter “$1” which will pull the individual interface’s description into the description when applied to a device. For instance, you could give the profile description “Floor 3 phone ports: $1”; when you apply this profile to a device interface with the description “Office 1”, the full description of the interface will then be read elsewhere as: “Floor 3 Phone Ports: Office 1”.

When the profile has been configured, apply it to device interfaces by selecting a device to configure. The profile can be applied to multiple interfaces across multiple devices. If you enter any individual interface parameters with a profile selected, the individual parameters will override those of the profile.

21.5.5 Streaming Telemetry Agent

The Streaming Telemetry Agent Studio enables you to define the streaming telemetry agent (TerminAttr) configuration for EOS devices streaming to CloudVision. The streaming telemetry agent is integral to the communication of state between network devices and CloudVision.

When you open the Studio, the following screen will be displayed.
21.5.5.1 Authentication

The first input determines how device streaming should be authenticated. There are two ways for the CVP server to authenticate the device sending the telemetry information:

- Certificate
- Ingest key

If you select No, the ingest key will be used, which is a shared cleartext key. This key is defined as part of the CloudVision set up process.

By selecting Yes, certificates are used for streaming authentication. CloudVision generates a JSON Web Token (JWT) that is then saved to a temporary location (e.g. /tmp/token). This token is used by TerminAttr for the initial secure authentication, and once authentication is successful, TerminAttr generates a certificate signing request (CSR) and sends it to the CloudVision server, which then signs the CSR with its own CA certificate and provides the generated client certificate to TerminAttr and stores it in the certificate partition on EOS. After this, TerminAttr will switch to using the client certificate and key, and renames the token by appending .backup to the filename and will not use it anymore.

21.5.5.2 VRF Assignment

Once you have selected the mode for authenticating the data, the VRF assignment can be selected. Here you will select devices with a tag query and then assign them to a VRF.
21.5.5.3 Device AAA Settings

You can select devices using a tag query and disable elements of AAA for them.

When disabling AAA, you are disabling authorization and accounting for eAPI commands sent by CloudVision to TerminAttr only when the Advanced Login setting is used. This does not affect AAA for other transports, such as SSH or eAPI over HTTPS.

The Advanced Login setting has been the default login method since version 2021.2.0. It can use multi-factor authentication and one-time passcodes to authenticate all CloudVision managed devices when you authenticate with CloudVision. When you select Yes, all eAPI requests are sent over the gRPC session established by TerminAttr instead of eAPI over HTTPS.

Disabling AAA is required in situations when the Advanced login setting is enabled and users are authenticated with certain RADIUS servers, where the server does not support authorization requests that do not have a preceding authentication request.

21.5.6 Campus Fabric

The Campus Fabric Studio provides a single point of control over the configuration of a campus network. The Studio is designed to allow the user to deploy and manage campus devices within the network using design patterns consistent with Arista best practices.

The Studio supports two common campus fabric designs. These designs are illustrated below, with support in beta-version for the L2 MLAG fabric.
21.5.6.1 Deploying and Configuring a Campus

Select **Campus Fabric** to display the Campus Fabric screen.

![Campus Fabric Diagram](image)

**Figure 503: Campus Fabric**

To create a new campus, click **Add Campus** and enter a name for the campus network. When done, click the arrow on the right.

The main configuration screen for the campus will be displayed.

![Campus Fabric Configuration Screen](image)

**Figure 504: Campus Fabric**

To assign devices that belong to this campus, click **Assign Tags**. You can now add devices with a tag query to this campus network. If a desired device is not present, add it using the Inventory and Topology Studio or, if the tag is not present, create a new User Tag.

![Assign Tags](image)

**Figure 505: Tag Assignment**
Next, configure the parameters and aspects of the L2 MLAG fabric. These parameters are used throughout the campus network when an MLAG pair exists. Configure the VLANs that will be defined for the campus network. A special management network may be defined when in-band management of the switches is required. The SVI virtual address is used as the anycast gateway across the campus Spline switches, as well as an IP helper address for DHCP relay functionality.

Central to the configuration of a campus network is assigning the roles to the selected devices in its fabric. They can be either campus Spline devices or leaf devices within a pod.

![Figure 506: Assigning Roles](image)

A campus Spline device may be used for both connecting downstream campus leaf switches, as well as connecting hosts. The campus Spline device will often have links toward networks external to the campus fabric.

A pod is a collection of leaf devices that connect to a campus Spline pair of switches. Each pod consists of one or more switches and may be used to form an MLAG stack. Some examples of campus pods are shown below:

![Figure 507: Examples of Campus Pods](image)

The selection of devices available to assign either as campus Splines or as members of a pod are those that you defined earlier on this screen as belonging to the campus.

The connections between devices are configured in the Inventory and Topology Studio. If the devices are already wired-up in your network, they will be shown there. If not, the intended connections can be specified in that Studio, and configuration for those interfaces will be generated.
To build a campus network, you’ll need the following connections:

- Between campus Splines: all interfaces connecting to the two Splines will be configured as an MLAG peer-link port channel.
- Between Splines and campus pod primary and secondary: these connections are referred to as “uplinks” and “downlinks”. They should be arranged according to the L2 MLAG design shown above. Configure these connections as multi-chassis link aggregation (MLAG) port channels.
- Between the campus pod primary and secondary: all interfaces of the two leaf switches will be configured as an MLAG peer link port channel.
- Between pod primary and secondary and pod members: the connections between these devices are configured as multi-chassis link aggregation (MLAG) port channels

Once the configurations of your campus fabric have been set, submit the Workspace and your campus network will be available for review and approval in Change Control.

21.5.7 Layer 3 Leaf-Spine

You’ll use this Studio along with EVPN Services to build a layer 3 leaf-spine network. The L3 Leaf-Spine Studio configures Day 1 deployment of the network, and EVPN Services configures Day 2 operations.

Note: In its beta-version, the Studio only supports BGP EVPN-VXLAN fabrics. It does not currently support the configuration of super-spines, multiple parallel transit connections between the same leaf and spine switches, detect/set speed on interfaces, and doesn’t support recirc channels on platforms that require them for VXLAN routing.

The Studio has been designed to support the following Arista validated L3 leaf-spine design:

![Layer 3 Leaf-Spine Diagram](image)

Figure 508: Layer 3 Leaf-Spine

Note: In order to build this design, you’ll first need to use the Inventory and Topology Studio to either accept the LLDP derived topology connections or manually add devices and interface connections.

21.5.7.1 Layer 3 Leaf-Spine - Required Tags

The following device tags must be in place before configuring the inputs in this Studio. You can create these tags within the same Workspace by accessing Tags.
### Table 20: Leaf-Spine Required Tags

<table>
<thead>
<tr>
<th>Tag</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC</td>
<td>DC: DC1</td>
<td>DC defines the data center that is being configured.</td>
</tr>
<tr>
<td>DC-Pod</td>
<td>DC-Pod: DC1</td>
<td>Data center pod name.</td>
</tr>
<tr>
<td>Role</td>
<td>Role: Leaf</td>
<td>Device Role. Can either be a leaf or spine.</td>
</tr>
<tr>
<td></td>
<td>Role: Spine</td>
<td></td>
</tr>
<tr>
<td>Spine-Number</td>
<td>Spine-Number: 1</td>
<td>The number for a spine device. Each spine must have a unique number.</td>
</tr>
<tr>
<td>Leaf-Domain</td>
<td>Leaf-Domain: 1</td>
<td>Specifies the leafs within a common AS, which is usually an MLAG pair of leafs. The value must be an integer.</td>
</tr>
<tr>
<td>Leaf-Number</td>
<td>Leaf-Number: 1</td>
<td>The number for a leaf device. Each leaf must have a unique number. Leaf pairs are assumed to be numbered consecutively starting with an odd number (e.g. the device tagged Leaf-Number:9 and the device tagged Leaf-Number:10 are two devices in an MLAG pair of leafs). If a leaf is not part of an MLAG pair, just use one number of the odd-even pair and do not use the other number for another leaf (e.g. the device tagged Leaf-Number:1 will be configured as a standalone leaf if no other device is tagged Leaf-Number:2).</td>
</tr>
</tbody>
</table>

The tag placement is illustrated in the following diagram:
21.5.7.2 Configuring the Fabric

Once tags are in place, you can create a data center in the Studio using the Data Center (DC) tag.

After a data center is in place, then create and configure its pods. Each pod is a leaf-spine module inside the data center fabric. Use the DC-Pod tag to assign devices to a pod.
Next, you will be presented with pre-filled values for the fabric of this pod, along with sections that allow you to add leaf and spine devices. Change the fabric configuration for the pod as needed.

You can add spine and leaf devices by using the Role tag. When adding a leaf device, you can further specify an ASN that will override the ASN number set at the pod level. You'll also be able to see on this screen a summary of all the devices in this domain.
Figure 513: Configuring the Fabric - Summary

Once you have configured all the data centers, pods, and their devices, review and submit the Workspace. A change control containing the configuration updates associated with the changes from the Workspace will be created. Review, approve, and execute the change control for the fabric configuration defined in the Workspace to take effect in the network.

Note: You can then stretch VLANs and VRFs across the newly deployed pods by using the EVPN Services Studio.

21.5.8 EVPN Services

The EVPN Services Studio allows you to deploy L2 and L3 network services. These services are applied to tenants that you create. Each tenant shares a common Virtual Network Identifier (VNI) range for MAC-VRF assignment.

Note: EVPN Services Studio is designed to implement Day 2 operations on top of the Day 1 fabric created with the Layer 3 Leaf-Spine Studio.

21.5.8.1 EVPN Services - Required Tags

The following tags are required for this Studio. They will already be in place if you have deployed an L3 leaf-spine fabric with the Layer 3 Leaf-Spine Fabric Studio.

Table 21: Required Tags

<table>
<thead>
<tr>
<th>Tag</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>router_bgp.as</td>
<td>router_bgp.as:65050</td>
<td>Defines the BGP ASN that the switch will use when configuring overlay VRFs, VLANs, and VLAN aware bundles.</td>
</tr>
<tr>
<td>router_bgp.router_id</td>
<td>router_bgp.router_id:172.16.0.1</td>
<td>Defines the BGP Router ID used on the switch and makes up part of the route-distinguisher and route-target fields.</td>
</tr>
</tbody>
</table>
### Tag Description

<table>
<thead>
<tr>
<th>Tag</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mlag_configuration.peer_link</td>
<td>mlag_configuration.peer_link:Port-Channel2000</td>
<td>Specifies the MLAG peer link used on a switch that has an MLAG peer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: This tag is only necessary for MLAG peer relevant configuration.</td>
</tr>
<tr>
<td>Leaf-Domain</td>
<td>Leaf-Domain:1</td>
<td>Specifies the leaves within a common AS, which are usually an MLAG pair of Leafs. The value must be an integer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: This tag is only necessary for MLAG peer relevant configuration.</td>
</tr>
<tr>
<td>Leaf-Number</td>
<td>Leaf-Number:1</td>
<td>For a leaf device, its number. Each leaf must have a unique number. Leaf pairs are assumed to be numbered consecutively starting with an odd number (e.g. the device tagged Leaf-Number:9 and the device tagged Leaf-Number:10 are two devices in an MLAG pair of leafs). If a leaf is not part of an MLAG pair, just use one number of the odd-even pair and don’t use the other number for another leaf (e.g. the device tagged Leaf-Number:1 will be configured as a standalone leaf if no other device is tagged Leaf-Number:2).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: This tag is only necessary for MLAG peer relevant configuration.</td>
</tr>
</tbody>
</table>

**Note:** If you do not want to use the L3 Leaf-Spine Fabric Studio, then you will need to create these tags before configuring the EVPN Services Studio.

### 21.5.8.2 Configuring EVPN Services

When you open EVPN Services, the following screen will be displayed. From this screen, tenants are created and the default VRF and MAC-VRF attributes for all tenants are created.
When creating a tenant or selecting an existing tenant to configure, you can create VRFs and VLANs for use within this tenant. You will also determine the base number used to generate VNIs.
21.5.8.3 VRFs

When configuring a VRF, always specify a VNI. The remaining fields are all optional and their use depends upon how you are configuring your network.
The iBGP Detail fields are necessary when a VTEP is composed of a pair of leaf switches that have a host (or hosts) connected to only one switch in an MLAG pair. If incoming traffic arrives at the leaf switch in the pair that the host is not connected to, the leaf switch will drop that packet. By configuring a VLAN and SVI to establish an IBGP peering on for this VRF, both switches in an MLAG pair are aware of all host connections including those connected to only one switch.

NAT Source Details are used to configure a virtual source NAT address for the VRF. It is used mainly for troubleshooting, because all VTEPs share the same IP address and MAC address for each SVI. This means that pings to workloads behind remote VTEPs or local workloads (e.g. MLAG VTEPs) may not be successful because the reply cannot be returned. When the destination host responds to either an ARP request or ICMP echo request, the reply is processed by the first VTEP it arrives at, which is because all VTEPs have the same IP and MAC address. In order for each VTEP to successfully ping a workload, configuring a NAT source address enables a dedicated loopback interface that can be used as the source address for pings within a VRF.

The Override VRF Attributes section allows you to override the default VRF attributes associated with this VRF.

21.5.8.4 VLANs

A name must be provided for each VLAN that is created. Then select whether it is applied to a routed or bridged setting.
Figure 517: VLANs

By default, the toggle is set to routed. You can also provide details of a DHCP server and provide a
default gateway by entering a Switched Virtual Interface (SVI) virtual IP address, which are options
only available with a routed VLAN.

The last two options, Devices and Override Attributes, are shared with a bridged VLAN, where devices
can be assigned to this VLAN and override the default values generated for configuration elements
associated with this VLAN.

Note: When assigning devices to a VLAN, make sure to toggle the value for the Apply column
to Yes to configure that VLAN.

21.5.8.5  VLAN Aware Bundles

You can bundle VLANs that have already been created within a tenant into VLAN aware bundles. Each
bundle consists of a range of VLANs that share the same MAC-VRF attributes, which you can define
by overriding the default MAC-VRF attributes shared across tenants.
Segment Security

The Segment Security Studio enables you to separate your network into logical domains. Each domain contains a set of segments and policies that determine the forwarding behavior between segments. A segment describes a set of endpoints with identical security policies and network access privileges.

To create a segmentation domain, click Add Domain and enter a device tag query. A segmentation domain is identified by device tags, which gives you the ability to select a group of switches that form the domain. All devices in the same domain will be configured with identical segmentation policies.
Figure 520: Segment Security - Add Domain

Once you have created the domain, click the arrow on the right, and the Policies screen will be displayed.

Figure 521: Segment Security - Policies

Enter a segment a name and identify its members. The segment membership is based upon either IPv4 or IPv6 prefixes, or both.

Next, set the security policies between segments. These policies apply to a single VRF. Configure segment policies for the VRF by clicking View underneath the Policies heading. Determine the relationship between pairs of segments inside the domain and the forwarding behavior of traffic between them.
VMware vMotion and Snapshot Support

CloudVision includes the following infrastructure components that are used as the basis for the application services and database. This is not an exhaustive list, but the key components as it relates to this topic.

- Hadoop - open source framework from Apache that is used to store and process large datasets distributed across a cluster of servers
- Hbase - open source database from Apache that runs on Hadoop cluster
- Zookeeper - centralized service for maintaining configuration information, naming, providing distributed synchronization, and providing group services

The CloudVision database (hbase/hadoop) is deployed across the three nodes within the CloudVision cluster. The integrity of this database is critical to the correct functioning of CloudVision, and thus, there are specific requirements on the hypervisor and storage for these virtual machines forming these nodes.

VMware Snapshots

Within the CloudVision infrastructure, data is constantly being written to Apache hadoop by all nodes. Disk snapshots used by VMware have no hooks into the hbase quiesce states, meaning a snapshot of a disk state would almost always be inconsistent and lead to database corruption during a restore process. This results in a snapshot having no meaningful use as a restore point due to the nature of the database, which is typical for database application performance using VMware Snapshots (VMware reference).

VMware Snapshots are very I/O intensive, leaving almost no I/O for the virtual machines during the snapshot process. Impact on resources, such as disk, can lead to hbase and zookeeper failures. These symptoms are evident in multiple cases where the support team has identified snapshots that were in progress before failures.

VMware does not recommend using VM Snapshots as backups (https://kb.vmware.com/s/article/1025279), therefore other backup mechanisms are recommended by Arista as outlined below.

Note: For these reasons, Arista does not support VMware Snapshots on CloudVision virtual machines.

VMware vMotion

CloudVision supports VMware vMotion under specific configuration and operational criteria as follows:

- The virtual machine disks are shared between the source and target ESXi host
- Latency between ESXi hosts is less than 5ms
- Only one CloudVision node may be vMotioned at a time

Note: CVP 2020.1.0 and future releases support host-to-host vmotion where the storage is shared between ESXi hosts. Only one host can be in vMotion at a given time.

Backup Solutions for CloudVision

Daily backups of the CloudVision provisioning data are automatically scheduled to be taken at 2AM UTC. This backup file is stored locally on the CloudVision cluster. Common practice by customers is to schedule a copy of this backup file from the CloudVision cluster to some external data store.

There is an example script to help automate the copying of the backup file available on the Arista Github site (link to Github).
CloudVision telemetry data received from switches is replicated between the CloudVision clusters. In the event a single node becomes unavailable and a new node is added to the cluster, this telemetry data is replicated to the new node.

Arista EOS with the Streaming Telemetry agent (TerminAttr v1.7.1 and later) supports establishing connections to multiple CloudVision clusters. This enables the user to send the telemetry data to a backup CloudVision instance, to maintain an up-to-date redundant store.

There is a detailed explanation of this deployment model available on the Arista EOS Central site, which would assist with the design and deployment of this HA solution.