2024.3.1 Release Notes

16 December 2024 (version: 1.2)

Table of Contents

1. Release Highlights

Base OS Upgrade to EL9

The base operating system is upgraded from EL7 to EL9. As part of this upgrade the base operating system is replaced and any customizations not described by the cvpi shell will be lost and need to be reapplied.

Software Management Studio

Use the Software Management Studio to provision devices with EOS images and extensions. You'll use the studio's Software Repository to upload EOS images, Streaming Agents, and extensions and then assign software from the Software Repository to devices.

Campus Features

CloudVision is introducing a number of new Campus features. Use the Access Interface Configuration quick action to assign configuration profiles to devices. The Interface Diagnostics quick action provides you with a fast and efficient way to troubleshoot interfaces in your campus. The new Campus Dashboard provides an overview of your network state. The dashboard includes all devices that have been configured in the Campus Fabric (L2/L3/EVPN) Studio, which have the Campus tag.

Campus Fabric Studio (L2/L3/EVPN)

The Campus Fabric studio allows you to set up and configure a complete campus network using Arista's validated designs. By leveraging zero touch provisioning (ZTP), you can seamlessly onboard EOS devices, define their roles and connections within the fabric, and configure L2 and L3 services across the fabric.

Access Interface Configuration Studio

This studio enables you to quickly configure access interfaces towards endpoint devices in your campus network. This configuration relates to the devices in Access Pods deployed using the Campus Fabric Studio.

Authentication Studio

Use the Authentication Studio to configure RADIUS servers for user authentication and 802.1X authentication and accounting.

Management Connectivity Studio

The Management Connectivity Studio is used to configure out-of-band (OOB) management interfaces for a single device or multiple devices. You'll create a profile of configured attributes for management interfaces, which can be assigned to multiple devices at once using tags.

CloudVision Profiles

You can now associate user profiles with roles. Users assigned a role with a profile will have their landing page updated to the one associated with the profile. If users inherit multiple profiles based on their role assignments, they can choose their preferred profile by clicking on their username in the top-right corner of the page.

Export Audit Logs via TCP

Export audit logs to external server endpoints using TCP over TLS.

Event Notification Output Templates

Configure an output template to customize the event notifications that CloudVision sends to receivers. Templates are available for configuring single- and multiple-alert notifications for a broad range of messaging platforms in plain text, json and html.

Custom HTTP Headers for Event Notifications

Create custom HTTP headers in order to integrate with unsupported third-party services or your own internal services. HTTP headers contain metadata in key-value pairs that are transmitted with HTTP requests and responses. Add headers that apply globally to all configured platforms or headers that apply only for specific receivers.

PTP Counters

View a device's PTP counters as a table in CloudVision in order to identify the types of messages that are being sent and received. Use this to troubleshoot issues with your network PTP configuration and connectivity.

Multi-Domain Segmentation Service

CloudVision provides support for microperimeter segmentation and enforcement as part of Arista's Multi-Domain Segmentation Service (MSS) for Zero Trust Networking (ZTN). With new features like MSS Policy Manager, Policy Monitor, Policy Builder, and the MSS Studio, you'll have the tools to both statically map endpoints to groups or leverage integration with external asset- and endpoint-management databases to dynamically learn endpoints and how they map to groups. You'll then be able to create and manage security policies and push them to EOS devices for segmentation enforcement.

For details refer to the Help Center.

2. Supported Scale

2.1 Cluster Scale

This release of the CloudVision Portal supports provisioning and monitoring of up to the following scale when deployed with the default recommended VM resources shown in the table below. Note that the number of active interfaces is defined as the number of physical (Ethernet) and virtual (Port-Channel, Vlan, etc) interfaces that are actively seeing traffic. A high performance NAS similarly means network attached storage that performs similarly from a read/write bandwidth perspective to locally attached SSDs. It is meant to exclude locally attached spinning-disks or equivalent systems. A 1TB data disk is sufficient for up to 1000 devices and 40,000 active interfaces. At larger scales a 2TB data disk is required.

Cluster Deployment	Per-Node Resources	Number of Devices	Number of Active Interfaces	Flow Tracking	WIFI Supported
Multinode	28 CPUs, 52G RAM, 1TB data disk (DCA-200-CV default)	1000	40000	5K flow updates/sec	Yes
Multinode	28 CPUs, 52G RAM, 2TB data disk (DCA-200-CV w/ extended disk)	1000	70000	5K flow updates/sec	Yes
Multinode	28 CPUs, 52G RAM, 2TB SSDs or high performance NAS (DCA-250-CV w/ extended disks, DCA-300-CV)	1000	100000	5K flow updates/sec	Yes
Multinode	70 CPUs, 116G RAM, 6TB SSDs or high performance NAS (DCA-350-CV)	2000	200000	5K flow updates/sec	Yes

2.2 Scale Breakdowns

The actual maximum number of devices supported on a given cluster depends on the average number of active interfaces per device, which can vary based on the deployment type. For example:

Supported Scale	Datacenter (Average 80 Active Interfaces/Device)	Campus PoE (Average 50 Active Interfaces/Devices)	CloudEOS (Average 8 Active Interfaces/Device
1000 Devices and 40K Active Interfaces	500	800	1000
1000 Devices and 70K Active Interfaces	875	1000	1000
1000 Devices and 100K Active Interfaces	1000	1000	1000
2000 Devices and 200K Active Interfaces	2000	2000	2000

2.3 Provisioning action scale limits

The total number of devices supported for provisioning is independent of the number of concurrent operations. The following table shows the concurrency limits for common provisioning operations.

Action	Maximum Actions
Concurrent Running Tasks	500
Simultaneous Device Moves from the Undefined Container to Another Container	500
Simultaneous Device Moves from One Container to Another	500

3. Important Functionality Changes

Single-node VM Resource Requirements

The resource requirements to run a single-node CloudVision VM instance have increased. The minimum resources are 16 CPUs and 32GB of RAM. See https://www.arista.com/en/cg-cv/cv-system-requirements for more details. Note: A single node CloudVision cluster is not recommended for use in production environments. It may be used for testing or in lab environments.

eAPI-over-TerminAttr

eAPI over HTTPS is deprecated in this release. We plan to stop supporting this feature in future CloudVision releases and recommend switching to eAPI over TerminAttr by turning on "Advanced login options" toggle on the Settings page.

Updates to built-in studios when upgrading CloudVision

During the CloudVision upgrade process, built-in studios may introduce updates to their functionality. These updates are applied within a system generated workspace listed on the Workspaces page. In the case where the changes result in device configuration, the user must take steps to accept these changes. For more information, please refer to the Studios Upgrade Guide

Hypervisor support for x86-64-v2 CPU flags

The hypervisor must expose the x86-64-v2 CPU flags to the CloudVision virtual machine.

4. Upgrading to CloudVision 2024.3.1

Upgrade to the CloudVision Portal 2024.3 train is supported from existing systems running 2024.1.0 or above. Clusters running earlier release trains should first be upgraded to the highest supported release (currently 2024.1.2 or 2024.2.1) before upgrading to the 2024.3 train. The upgrade path follows the latest release in each major version of CloudVision, for more details please refer to the upgrade path tool on the Arista Support page.

The following steps can be taken at any point on an existing cluster as part of preparing for an upgrade to 2024.3.1.

Upgrade Checklist

1. Devices must have TerminAttr 1.19.5+ installed (1.28.7 recommended)
2. If not already upgraded to the 2024.3 release train then upgrade existing CloudVision clusters to at least the latest 2024.1.0 release (currently 2024.1.2 or 2024.2.1)
3. Upgrade all EOS devices under management to an EOS 4.23+ release train
4. Ensure that all devices are successfully streaming to the CloudVision cluster
5. Ensure that all devices are in image and config compliance
6. Take regular backups of cvp and take a final backup of cvp prior to upgrade
7. Ensure that all tasks are in a terminal state (Success, Failed, or Canceled)
8. Ensure that all Change Controls are in a terminal state

4.1 AlmaLinux EL9 Upgrade

The CloudVision 2024.3 release transitions to AlmaLinux EL9 as the underlying OS. The conversion will occur as part of the normal CloudVision upgrade process. The upgrade will occur during any CloudVision upgrades from a CloudVision version that precedes version 2024.3.0 to any subsequent version.

Before upgrading, please consider the following and complete any prerequisites:

- CloudVision DCA Appliances should be running CVA version 6.0.5 or later. To upgrade your CloudVision Appliance, view the DCA Appliance upgrade procedure
- There are no specific EOS requirements for the ALMALinux upgrade. Follow the Help Center guidance for upgrading CloudVision

- It is recommended that a console be connected to the primary CloudVision cluster node
- Allow a 3-hour network management maintenance window for the upgrade process
- Some customer-created Python scripts may not be compatible with EL9. If any imports fail, the upgrade process will halt, leaving the base OS unchanged. Contact TAC for assistance
- Other custom configurations to the base OS, such as cronjobs or firewall rules, will be lost. A backup or copy of any custom configs should be kept somewhere off of the CVP appliance

If hardening procedures are necessary, please contact TAC.

5. Deprecated and Backwards Incompatible API Changes

CloudVision APIs are marked as deprecated at least one major release train prior to removal, with instructions on the alternative API to use. The following APIs are marked as deprecated and will be removed in a future major release train. Please transition all existing uses of these APIs to the provided alternative.

Service: /cvpservice/event

Request: /event

- All /event APIs are marked as deprecated starting 2020.2.
- These APIs were only meant for internal use by various provisioning UIs

Service: /cvpservice/inventory

Request: POST /inventory/deleteDevices.do

- Marked as deprecated starting 2020.1
- Replaced by DELETE on /inventory/devices starting 2020.1.0
- Deleted in the 2020.3 train.

Service: /cvpservice/login

Request: GET /login/home.do

- Marked as deprecated starting 2020.2
- Internal API for the UI to validate the session. Can be replaced by a call to any other API, which will return a 401 if the session is not valid.
- Planned deletion after 2021.3 train.

Request: /cvpservice/login/logout.do

- Marked as deprecated starting 2024.3
- Replaced by the api/v1/oauth HTTP APIs
- Planned deletion in the 2025.1 train

Service: /cvpservice/provisioning (also available at /cvpservice/ztp)

Request: GET /provisioning/getconfigfortask.do GET /provisioning/v2/getconfigfortask

- Marked as deprecated starting 2020.2
- Replaced by /provisioning/v3/getconfigfortask, available starting 2018.2.3
- Planned deletion after the 2021.3 train

Request: /provisioning/runConfigSync.do

- Marked as deprecated starting 2020.2
- Replaced by /provisioning/checkCompliance.do, available starting 2018.2.3
- Deleted in the 2020.3 train

Request: POST /provisioning/validateAndCompareConfiglets.do

- Marked as deprecated starting 2020.2
- Replaced by /provisioning/v2/validateAndCompareConfiglets.do, available starting 2018.2.3
- Deleted in the 2020.3 train

Request: POST /provisioning/checkCompliance.do

- Marked as deprecated starting 2020.3
- Planned deletion after the 2021.3 train

Service: /cvpservice/task/

Request: GET /task/getLogsById.do

- Marked as deprecated starting 2020.1
- Replaced by /cvpservice/audit/getLogs.do
- Deleted in the 2020.3 train.

Request: GET /task/getLogById.do

- Marked as deprecated starting 2020.1
- Replaced by /cvpservice/audit/getLogs.do
- Deleted in the 2020.3 train.

Service: /provisioning/devices/

Request: POST /provisioning/devices/

- Marked as deprecated starting 2023.1

Service: api/v3/services HTTP APIs of AAA settings

Request: api/v3/services/arista.aaa_setting.v1.AAASettingConfigService

- Marked as deprecated starting 2024.2
- Replaced by the api/resources HTTP APIs
- Planned deletion in the 2024.3 train

Service: api/v3/services HTTP APIs of SSO Providers

Request: /api/v3/services/arista.identityprovider.v1.OAuthConfigService /api/v3/services/arista.identityprovider.v1.SAMLConfigService

- Marked as deprecated starting 2024.2
- Replaced by the api/resources HTTP APIs
- Planned deletion in the 2024.3 train

Service: api/v3/services HTTP APIs of Service accounts

Request: /api/v3/services/arista.serviceaccount.v1.AccountConfigService /api/v3/services/arista.serviceaccount.v1.AccountService /api/v3/services/arista.serviceaccount.v1.TokenConfigService /api/v3/services/arista.serviceaccount.v1.TokenService

- Marked as deprecated starting 2024.2
- Replaced by the api/resources HTTP APIs
- Planned deletion in the 2024.3 train

Service: api/v3/services HTTP APIs of admin.Enrollment

Request: api/v3/services/admin.Enrollment

- Marked as deprecated starting 2024.2
- Replaced by the api/resources HTTP APIs
- Planned deletion in the 2024.3 train

Service: ccapi

Request: /api/v3/services/ccapi.ChangeControl

- Marked as deprecated starting 2023.1
- Replaced by the Change Control resource API
- Planned deletion in the 2023.3 train

Service: tag.v1

Request: /api/resources/tag/v1

- Marked as deprecated starting 2023.1
- Replaced by tag.v2
- Planned deletion in the 2023.3 train

6. Compatibility

6.1 Supported Browsers

Browser	Version
Google Chrome	115+
Mozilla FireFox	115+
Microsoft Edge	115+

6.2 Supported CloudVision Appliances

CloudVision Appliance Version	Supported CVA Version
1.1.x	Not Supported, Upgrade Required
1.2.x	Not Supported, Upgrade Required
2.0.x	Not Supported, Upgrade Required
2.1.x	Not Supported, Upgrade Required
3.0.x	Not Supported, Upgrade Required
4.0.x	Not Supported, Upgrade Required
5.0.x	Not Supported, Upgrade Required
6.0.0 - 6.0.4	Not Supported, Upgrade Required
6.0.5+	Supported CVA Version

6.3 Supported HyperVisors

Hypervisor	Supported Hypervisor Version
VMware ESXi (recommended) Hypervisor	6.7.0 and above
KVM	qemu-kvm 1.5.3+ and libvirt 4.5.0+

6.4 CentOS Version for RPM Installer

CloudVision Portal Version	Supported CentOS Version for RPM Installer
Supported Versions for RPM Installer 2020.2+	CentOS Minimal 7.7.1908
Supported Versions for RPM Installer 2021.2+	CentOS Minimal 7.9.2009
Supported Versions for RPM Installer 2024.3+	AlmaLinux release 9.4

6.5 Supported EOS Versions

CloudVision Portal Version	Compatible EOS Versions
2024.3.1	4.23 - 4.32.2

Though EOS versions 4.23 - 4.26 are supported by CloudVision, they are EOL. The recommendation is to upgrade.

6.6 Supported TerminAttr Versions

6.6.1 Supported Versions

CloudVision Portal Version	Bundled TerminAttr Version	Minimum TerminAttr Version	Recommended TerminAttr Version
2024.3.1	1.28.4	1.19.5	1.28.7

6.6.2 TerminAttr Version Bundled by EOS Version

EOS Version	Bundled TerminAttr Version	TerminAttr Extension Required
EOS 4.21 - 4.23	< 1.8.0	Yes, 1.19.5+ recommended
EOS 4.24.0F	1.8.0	Yes, 1.19.5+ recommended
EOS 4.24.1	1.9.0	Yes, 1.19.5+ recommended
EOS 4.24.2	1.10.0	Yes, 1.19.5+ recommended
EOS 4.25.0	1.11.0	Yes, 1.19.5+ recommended
EOS 4.25.1F	1.12.1	Yes, 1.19.5+ recommended
EOS 4.25.2F	1.13.1	Yes, 1.19.5+ recommended
EOS 4.25.5M	1.13.7	Yes, 1.19.5+ recommended
EOS 4.26.0	1.14.0	Yes, 1.19.5+ recommended
EOS 4.26.1	1.15.2	Yes, 1.19.5+ recommended
EOS 4.26.2	1.16.2	Yes, 1.19.5+ recommended
EOS 4.26.7M	1.19.5	No
EOS 4.27.0	1.17.0	No, but 1.19.5+ recommended
EOS 4.27.1	1.18.1	No, but 1.19.5+ recommended
EOS 4.27.2	1.19.0	No, but 1.19.5+ recommended
EOS 4.27.4.1M	1.19.4	No, but 1.19.5+ recommended
EOS 4.28.0F	1.20.0	No, but 1.22.1+ recommended
EOS 4.28.1F	1.21.0	No, but 1.22.1+ recommended
EOS 4.28.2F	1.22.1	No
EOS 4.29.0F	1.23.0	No, but 1.24.2 recommended
EOS 4.29.1F	1.24.2	No
EOS 4.29.2	1.25.0	No
EOS 4.29.3	1.25.1	No
EOS 4.30.0F	1.26.0	No, but 1.28.2+ recommended
EOS 4.30.1F	1.27.0	No, but 1.28.2+ recommended
EOS 4.30.2F	1.28.0	No, but 1.28.2+ recommended
EOS 4.30.3M	1.28.0	No, but 1.28.2+ recommended
EOS 4.31.0	1.29.0	No

6.7 Supported CloudVision Extensions

The following minimum versions are required for common applications that can be installed as CloudVision extensions. If you have previously installed one of these applications, you'll need to reinstall it following the AlmaLinux EL9 upgrade that occurs when upgrading from a CloudVision version that precedes version 2024.3.0.

Application	Minimum Supported Versions
CloudBuilder	v2.4.7
IPAM	v.1.3.2+
ServiceNow	v1.6.1
CVPRAC Python Library	v1.4.0+

6.8 Supported CloudVision-Wifi

Bundled CV-Wifi Version
wm-v18.0.0-176 CV-CUE - 2024.09.27.2

7. Resolved Caveats

Cluster Deployment and Management

Severity 1 / Severity 2

• Migration is needed for single tenant schema to multi tenant schema. The current migration only supports to the first version of multi tenant schema, which is released at 2024.2.0. In CVP version 2024.3.0, new columns are added so migration from 2024.1.0 to 2024.3.0 will fail because number of columns doesn't match for the source and target tables. The workaround is to upgrade to 2024.2.0 first then upgrade to the newest version. (1029537)

• Upgrade to CloudVision version 2024.3.0 will fail if aeris admin certs need their permission fixed. Ensuring that the certs have the expected permissions at script initialization time will allow the upgrade to proceed. (1025933)

• When upgrading to CloudVision Version 2024.3.0, upgrade will fail if the "cprov" and "service-action" components are down/disabled. Enabling and starting the components will allow the upgrade to proceed. (1030818)

• Upgrading CloudVision on AWS will bootloop on the dracut upgrade step. (1039643)

Severity 3

• Upgrading to CloudVision version 2024.3.X will fail when CloudVision is running in the 'wifi_analytics' deployment model. The upgrade will fail during the 'Retrieving Configlet Builder Scripts' portion of the upgrade script with a traceback message.

Enabling the 'cprov' component in CloudVision with the command 'cvpi enable cprov && cvpi start cprov', then re-trying the upgrade will work around this issue. 'cprov' can be disabled after the upgrade is complete with 'cvpi disable cprov && cvpi stop cprov'. (1025307)

• NTP AUTH breaks when upgrading to 2024.3 because of the difference in keyfile formats between ntp and chrony. (1033571)

Network Provisioning

Severity 1 / Severity 2

• If a device has no config changes but has image and topology updates in a workspace, submitting the workspace would unintentionally delete configlets from mainline config sources. This leads to the removal of configuration from the device in subsequent workspaces. (995083)

• Device image management using the Network Provisioning workflow can become unresponsive after restoring an on-premises cluster from a backup. (1026313)

• Software downloads in the Software Repository do not respect the proxy if configured on the Settings page causing EOS image and extension downloads to fail. (1024441)

• Logs in custom python actions are not visible in the Change Control log panel. Changing python script logging to use ctx.alog(<message>, customKey=ctx.action.ccId) will cause future runs of the action to have the logs appear (1029624)

• Containers in the Static Configuration Studio were incorrectly displayed as removed in the View Modification Details screen (1028496)

• Device may not get provisioned due to an older attempt to provision underway. (782617)

Severity 3

• When viewing software available for download from the Cloud in the Software Repository tab of the Software Management Studio, images not applicable to devices will be listed under CloudVision/CloudVision Applications. (1001480)

• Device shows as out of compliance in studios when Peer Supervisor is disabled, still booting or in not inserted state when using the software management studio. (1031891)

• User tags can sometimes become system tags upon workspace submission if the TagConfig and TagAssignmentConfig APIs are not used consistently. (704545)

• A tag may become unmodifiable if network elements are tagged with it before it has been created. (826749)

• When performing a change control, if the device does not have enough free space, an error message is displayed communicating available vs required space. However if the bytes are too close to each other, available will equal required, due to rounding. (1005884)

• Removing a device in Network Provisioning when it is also used in Studios removes all configuration generated by Studios. (1035621)

• Campus Fabric (L2/L3/EVPN) Studio does not generate "redistribute dot1x" under MAC VRF when 802.1x is enabled. (988205)

Telemetry

Severity 1 / Severity 2

• In Topology, filtering Inband Telemetry paths using the checkboxes in the Flows sidebar does not function. (1023751)

Severity 3

• In the Software Management Studio and the Software Assignment section, the Streaming Agent dropdown does not order values accurately for the 64 bit embedded TerminAttr version with suffixes in the name. It does not hide the unsupported versions correctly, but the build results after `Review Workspace` will highlight this. (1017016)

• The IP address for Connectivity Monitor hosts may not show up on the CloudVision dashboard. (984269)

• Datapoints on various time aggregated metrics might linger even after the data source has been removed/deleted, possibly resulting in stale dashboards. The potentially affected metrics are: fan speed, XCVR DOM metrics, device temperature, power supply readings and inlet temperatures. (1013571)

• The "deviceHostname" label is not populated in webhook bodies for interface components (with simple_output = true) (1022231)

• Paths with wildcards that are excluded from streaming by CloudVision may not be properly handled by TerminAttr causing extra data to be streamed to CloudVision. (1005914)

Limitations and Restrictions

• The Event Notification Microsoft Teams sender platform uses an old template format that is nearing deprecation on the Microsoft Teams side. (992699)

Multi-domain Segmentation Services

Severity 3

• In MSS studio, If user applies the same policy with monitor rule to multiple VRFs, rule recommendation won't be able to identify and apply the recommended rule/policy to the right VRF. We shouldn't allow applying the same policy with monitor rule to multiple VRFs (1014130)

8. Known Software Caveats

Cluster Deployment and Management

Severity 1 / Severity 2

• In rare cases the User application may become unresponsive resulting in issues displaying the legacy Provisioning, Configlet or Image Repository pages. Workaround this issue by running the following CLI commands on the cluster: `cvpi stop user` followed by `cvpi start all` (948416)

• Topology Flow overlays may not display values for all links in a flow, even if the overlay values are shown in the sidebar for those links. (998328)

Severity 3

• If logout.do API is invoked using the service account token, that token will be no longer valid. It will, however, still appear in the service accounts section of CloudVision. A new service account token must be generated after logout. (574191)

• The role-based access control is broken for some of the UI pages like Comparison, Network segmentation, Topology etc, although the user doesn't have required access they will see certain unauthorised sections in UI. (626944)

• The CloudVision roles that we create from cv > settings > aaa-roles page have two unique ids, one is role-id and other is role-name. Starting from CloudVision 2024.3, updating a role-name from cv > settings > aaa-roles page is disallowed. This is in accordance with the effort of removing role-ids from CloudVision because role-ids are not human readable and less intuitive to use them in role CRUD APIs. (936428)

• In certain scenarios the heap size allocated for HBase's regionserver might be too low to complete NetDB path migration during CloudVision upgrade.
Work around this issue by raising the heap size for regionserver, complete the upgrade, and reduce it back to its original value.
To increase the heapsize do the following:
Log in to the terminal of one of the CloudVision nodes.
Run the command:
  kubectl edit configmaps hbase-conf
This will open the default text editor, typically vi.
Find the section:
 hbase-env-regionserver.sh: |
You will see the current size set to the HEAPSIZE variable, for example:
  HEAPSIZE=5698

Find the end of the hbase-env-regionserver.sh section, it should have three if/fi blocks. After the final "fi" insert a new line:

```
export HBASE_HEAPSIZE=<new heap size value>
```

Try tripling the original value set for HEAPSIZE. For example:

```
...
if (( MEM < 16384 )); then
  export HBASE_HEAPSIZE=$((HEAPSIZE>1024 ? 1024 : HEAPSIZE))
fi
export HBASE_HEAPSIZE=15000 # Temporary increase in regionserver heap size
```

Note, the line must match the indentation of the "fi" above, 4-spaces.
Save and close the file ("Esc" then ":wq" in vi).
Then restart the regionserver pods with the following:

```
kubectl delete pod -lapp=regionserver
```

Let the NetDB path migration complete.
To restore the previous config do the same process as above to edit the config and delete the added "export HBASE_HEAPSIZE ..." line. Then restart the regionservers the same as before. Alternatively, 'cvpi stop hbase-conf && cvpi start all' will also restore the config to default. (957897)

Network Provisioning

Severity 1 / Severity 2

• Releases that support FIPS mode with OpenSSL 3.x will fail to upgrade EOS releases older than 4.32.0. Temporarily disabling FIPS mode on the nginx server and upgrading the EOS devices seems to be the only possible workaround.

The workaround is:
1. ssh into a CVP node and disable FIPS mode in nginx with: kubectl set env daemonset/nginx-app ARISTA_ENABLE_FIPS=0
2. verify with: kubectl exec -it $(kubectl get po -l="app=nginx-app" -o name | head -n 1) -c nginx -- openssl version (should display the openssl version only and not "FIPS mode is enabled")
3. go to the UI and run the EOS upgrades
4. after the upgrades have completed, ssh into a CVP node and reenable FIPS mode in nginx with: kubectl set env daemonset/nginx-app ARISTA_ENABLE_FIPS=1
5. verify with: kubectl exec -it $(kubectl get po -l="app=nginx-app" -o name | head -n 1) -c nginx -- openssl version (should display "FIPS mode is enabled" and the openssl version)

This workaround is meant to be temporary and only enabling EOS upgrades for releases older than 4.32.0. The kubernetes config changes won't persist across cvpi commands (cvpi stop, cvpi start, cvpi config, etc.). (1034941)

• When the total number interfaces across all devices that are accepted in the Inventory and Topology Studio is very high (tens of thousands), workspace builds may fail with error "context deadline exceeded".
The workaround is to reduce the number of devices/interfaces in the Inventory and Topology Studio. (703338)

• ZeroTouch agent may keep restarting continuously during Zero Touch Provisioning (ZTP) if the DHCP option 67 (boot file name) is a hostname that needs to be resolved as opposed to an IPv4 or IPv6 address. This will result in ZTP getting stuck. The workaround is to use an IPv4 or IPv6 address in the boot file URL. (718251)

• In rare situations, when there are multiple devices being onboarded, the image diff for some of them may fail to load. The workaround is to restart the image app. (963687)

• Removing devices from a container can sometimes cause other devices to not have the Container system tag anymore (808068)

• Set Config action for a device in ZeroTouch mode may fail when bringing device out of ZeroTouch mode (949086)

• While running change control actions (Set Image, Set Configuration, etc) if there is an error reaching the device using 'show version', 'show redundancy status' eAPI commands, the actions will be retrying for 24 hours, instead of the user configured action timeout. Users can stop the change control for these stuck actions. (969812)

• A tag may continue to match devices or interfaces that are no longer in inventory. (1000192)

• Streaming status of a device can be inconsistent for some duration before eventually becoming consistent (971874)

Severity 3

• When reconciling managed lines at the device level in Network Provisioning, the checkbox corresponding to the line is ticked by default when it should not be. (636908)

• The change control review page computes reboot information based on only the image and extensions that will be added. It does not include the extensions that will be deleted and have reboot required flag checked. (640473)

• When viewing the table layout of Network Provisioning, the table columns can appear squashed. The workaround is to either resize the columns manually or view the screen in hierarchy mode. (662452)

• If a user has configured per-studio permission for a given studio and if that studio is deleted on mainline, then any eventual RBAC set from the roles page will fail with an error displaying all deleted/non-mainline/invalid studios in the request.
Workaround is to manually delete the RBAC rules of deleted studios in the roles page. (703900)

• From within the validate and compare page, running config is displayed twice sometimes for some device types. Workaround is to reload the page. (733327)

• Removing a device selection input in a studio does not automatically unassign the corresponding tag.
The workaround is to navigate into that input, remove the device from the "Assigned Devices" dropdown, and the remove the input. (777613)

• Clicking Rebuild on the Review Workspace page does not start a new build if a build is already in progress. (802582)

• When a user is assigned a role with no access to the device section, there might still be ways for the user to get access to device information. One of the way is by selecting a device from topology and clicking on the device overview. Another way is to search for the device in the search bar. In both these cases they are shown a permission denied error but they can still see the device information. (807037)

• Change Control Rollback can mistakenly include Tasks that were in the process of being created by another user who was working at the same time from the Network Provisioning view. To remedy, delete the extraneous task from the Rollback Change Control so that it is available to assign to another Change Control. (868588)

• The query for device Id in the interface page of the Inventory & Topology Studio may look editable, but this field is read-only (911174)

• The software management repository has a download/export feature which does not work when there are table filters applied. The download functionality exports the whole table in the repository irrespective of filters. (949593)

• In the Software Management Studio, the software assignment tab might take longer load times when there are large number of rows (480+) in the assignment table. (960647)

• The information displayed when hovering over an entry in the "Existing Assignments" column in the Software Repository table and the "Devices" column in the Software Assignment table of the Software Management Studio may be incorrect for devices that have once been assigned but were later decommissioned. (965353)

• Assigning vEOS-lab images to CloudEOS devices is not allowed. CloudVision doesn't guard against this behavior during the Software Validation stage. (975084)

• When viewing a single change control, the search input will show all actions and stages when no matches are found. The expected behavior is to show no actions and a message indicating that filtering is active. (982615)

• Large scale change controls that execute all actions in parallel might cause a browser out of memory crash. The browser crash has no impact on the backend execution of the change control. A page refresh will rectify the issue. (955162)

• At the moment 32 Set Image actions are executed in parallel. In case a change control has large number of Set Image actions, and the Set Image action timeout is at the default 1 hour limit, this timeout might not be sufficient. Increasing the timeout to a larger value will help in executing all actions within the change control. (955184)

• Change Control action count in the Action Summary section may show inaccurate percentage due to rounding errors. Review the actual counts for precise information. (961140)

• There are additional calls being made before executing change control action(s), this adds some delay in seeing the actions on the UI after clicking on Start CC. (961292)

• SetImage using default 24hr timeout instead of using user configured timeout causing this issue. (968334)

• The Change Control "Action Summary" gauges do not indicate red failed stages until the change control is complete. While the change control is in progress, failed stages or actions will be rendered as blue. (969185)

• The "Onboard Devices" menu under the "Add Device" button does not support device registration using IPv6 addresses (952619)

• Compliance check computation might fail with context deadline exceeded error when the action times out. Workaround is to increase the action timeout using the tunables. (965907)

• The latest successful device onboarding attempt overrides the previous failed ones. In this case, the user cannot see the failed attempts. (992647)

• With large device batches, the Software Management Studio is showing delayed completion of workspace reviews for a small subset of the devices. (975090)

Telemetry

Severity 1 / Severity 2

• When an input panel is deleted from the dashboard, there is no warning if it is being used in another panel. (810001)

• Auto device decommissioning feature may inadvertently decommission a device if the decommission duration is set to a small value and auto decommissioning is enabled. It is recommended that the feature be turned off if devices are expected to be inactive for an extended duration. (955845)

• For a freshly configured Wifi Connector, the "View in CV-CUE" button is not displayed in the Infrastructure Access Points and Wireless Endpoints sections in the "Campus Health Overview" dashboard. This can be fixed by running the following commands. Knowledge of Wifi customer ID is required to execute these steps. SSH into any of the CloudVision nodes as the root user and run the following commands.
1. /cvpi/apps/aeris/bin/aeris-cli create dataset --storage hbase --storageoption table=aeris_v2 --storageoption zkquorum=localhost:2181 --type device --org Default --name "WIFI_CONTROLLER/<wifi-customer-ID>"
For a multinode setup, replace the zkquorum storage option value with "${PRIMARY_HOSTNAME}:2181,${SECONDARY_HOSTNAME}:2181,${TERTIARY_HOSTNAME}:2181"
2. /cvpi/apps/aeris/bin/aeris-cli --storageoption zkquorum=127.0.0.1:2181 --storageoption table=aeris_v2 permission --org "Default" --srcName "WIFI_CONTROLLER/<wifi-custmore-id>" --srcType "device" --targetName "AllDevices" --targetType "group" --perm "inherit" --inherit true
zkquorum needs to be replaced here as well for a multinode setup.
3. cvpi stop apiserver && cvpi start all
The UI needs to be refreshed after all the commands are run successfully, the "View in CV-CUE" button should be available. (1023792)

Severity 3

• It is possible to configure custom syslog event rules in the UI with certain invalid regular expressions which the CloudVision events backend will not allow. In particular, regular expressions with negative look-aheads will be accepted as a valid rule configuration in the UI but cannot be used to generate events on the CloudVision backend. No errors will be logged in this case and the failure will not be apparent to the user when saving the rule configuration. (635378)

• Long-running browser instances may see an error toast, "Error: Connection to data source lost. Reconnecting...", that does not disappear when the connection is re-established. (700304)

• If subinterface counters feature (experimental) is enabled, a subinterface counter data will remain in telemetry after it's deleted on the device. (707721)

• Interface tag searches and filters do not support subinterfaces or third party device interfaces. (716765)

• Removing all matches under a tag key/label will not necessarily prevent that key/label from appearing under tag label suggestions when querying for tags. (717999)

• CloudVision telemetry reports LANZ queue length as measured in segments within LANZ Queue length graphs. However the units are dependent on the chip type of the switch. In most cases, segment is correct; however certain SKUs (such as 7150) are measured in bytes. This may lead to misleading or inaccurate displays on the UI (775514)

• Clicking "Unacknowledge" on an inactive CloudVision event that was previously acknowledged may lead to a new event alert being sent for that event even if the event has previously been alerted on. (790962)

• When users with edit permissions keep a dashboard in edit mode, log out, and then log in with read-only permissions, they still see the UI for editing the dashboard. However, their changes won't be saved to the backend. (847871)

• In some cases a red line may appear at the top of the latency horizon graphs, even when the measured latency is not excessive. Clicking on the horizon graph and viewing the values in the modal view gives full information on the recorded values. (889934)

• The Routing Table Utilization Breached Threshold event view may fail to load the Hardware Table Capacity graph with a "No hardware capacity to display" error message (916223)

• Supplicants that had authenticated through MBA on an interface in the past, but are not longer present, may show up in the table reporting 802.1X supplicants on a device with (unknown) values. (930719)

• Tag queries will show results for devices and interfaces that are no longer commissioned if their tags failed to get cleaned up on decommissioning. (964728)

• XCVR interfaces set up to use media channels may not have their DOM metadata correctly represented on the UI. (973702)

• ChangeControl services in CloudVision generate app audit logs for various actions. Some of these logs are not really audit logs but are Change Control execution logs which show up on the UI. These are also being exported as syslogs along with other audit logs. These logs will not exported from 2024.4.0 release. (924782)

• When Elasticsearch nodes lose connectivity with each other within the Elasticsearch cluster -- either the master node loses connections to the data node or vice versa -- Elasticsearch can decide to bring itself down, in order to help reestablish connectivity between the two upon subsequent restart. The connectivity issue can be legitimate (eg. CloudVision nodes lose connectivity with each other) or transient (eg. a slower than expected network throughout disrupts time-sensitive communications internal to Elasticsearch).

As a result, Kubernetes reports restarts of "elasticsearch-server" pods. This is expected that Kubernetes will bring the Elasticsearch cluster back in working condition after restart of the

pods.

During the restart of the pods, Elasticsearch service may become partially or completely unavailable. (977001)

• In the software management studio, the embedded Streaming Agent is not searchable in the software assignment page. (986985)

• The Traffic Counters page for a device may show excessive precision for large numbers, not enough precision for small numbers, or numbers that are too large to fit into the heatmap cell. (999412)

WiFi Server

Severity 3

• "log level clouddbmgr" CLI command executed from within wifimanager container shell would not take effect for its first execution. (1017398)

9. Limitations and Restrictions

Cluster Deployment and Management

Limitations and Restrictions

- Upgrade to 2024.3.0 will lose any customization, including any RPMs installed for 3rd applications, and for extra functionality on the host OS. (936485)

Network Provisioning

Limitations and Restrictions

- CloudVision does not support managing EOS devices over interfaces configured via DHCP. (246747)

- Applying an image bundle with Streaming Agent (TerminAttr) extension (swix) to a device that has an embedded Streaming Agent with the same version will lead to the device being out of extension compliance. Workaround is to remove the extension from the bundle, which will bring the device back in extension compliance. (736173)

- TerminAttr 1.32.1 or higher versions will miss SupportedEosVersions data if they were uploaded to Software Repository in 2024.2.0. Upgrading to 2024.3.0 and re-uploading these versions will add this data and provide additional validations. (982327)

Telemetry

Limitations and Restrictions

- Incoming telemetry data timestamps can be misaligned with the real time. This may happen when the device clock is not synchronised or there is a very high load on the CloudVision nodes, which cause the backend component to perform joins of data sources that are aligned with real time rather than the device's time. (678740)

- Depending on the rate of increase in memory usage, the CloudVision Device Memory Usage Approaching Threshold event may occur too late for the user to take preventative action. (695327)

- For the Device Memory Usage Approaching Threshold event (and other prediction type events), the prediction point shows a small indicator on the graph and hovering on this for more information can be challenging. (695329)

• In some cases, event search on description will not return matches that users may expect. For example, "High hardware usage detected" text exists in some events and a search of "usage detected", "usage detect", or "usage" will return events matching the provided text; however search involving the middle of a word eg. "age" will not return any matches. This is a limitation with the way searches are executed in the underlying search engine. (793383)

• When Event Rollup is enabled, if several group events are rolled up the count displayed on the expandable row is incorrect. The count only includes the number of inner events of the group, and does not include the number of rolled-up events. (879782)

• Event Groups inherit the event severity from the inner events which form the event group and this set of inner events can be appended to over the lifetime of an event group. However the event group severity is set at creation time and cannot be modified. (887863)

• When attempting to set a custom event notification template which is not valid, CV can can display a error messages which does not contain sufficient information needed to debug the error in the template, in some cases there is also too much unnecessary information and it is hard to parse. (952461)

• The historical data retention for the MAC Address count metric may be limited if there is a high churn in the MAC table. (959450)

• XCVR DOM anomaly events may not be shown on the Topology page as part of the active events topology overlay, even when there are active events. (982430)

• Event counts in all histograms only include events that started during a particular time window and do not reflect the number of active events in that window. (1000361)

10. Appendix

Relevant EOS Limitations and Software Caveats

- Within a config session, configuring VLANs that are currently in use as internal VLANs may fail. The error message will state that internal VLANs cannot be created even if a VLAN would no longer be used as an internal VLAN once the config session is applied. (132550) Introduced in 4.14.0. Fixed in 4.21.9,
  4.22.4,
  4.23.0,
  delhi-maint,
  eos-trunk,
  florence-maint

- Modifying an existing daemon through config session or config replace fails to restart the daemon.

  The workaround is to manually shutdown and no shutdown the daemon. (154022) Introduced in 4.14.0. Fixed in 4.18.5,
  4.19.2,
  4.20.1

- Starting a daemon that has run previously may cause the system to fail to start any new agents, daemons, and CLI sessions. (190407) Introduced in 4.18.1. Fixed in 4.18.4,
  4.19.1,
  4.20.1

• BGP peer-group configuration may not be correctly applied if configuration changes are made within a configure session or with a configure replace command. (212396) Introduced in 4.20.5.

- The ConfigAgent process will grow in memory size for every eAPI request. The only workaround is to periodically restart ConfigAgent. Doing so will terminate all CLI connections. (235573) Introduced in 4.20.1. Fixed in 4.20.2

- During Zero Touch Provisioning, the device might fail to download the config script from the file server. (242292) Introduced in 4.20.2. Fixed in 4.20.3

- When using one of the following CLI commands; "reload", "install source", or "boot system" for an EOS-2GB.swi on a system with 2Gb flash memory and an SSD and/or external clock, the command fails with an error message saying the software image is not compatible with the hardware.

  The workaround for that bug is to download the image to flash memory, edit the boot-config and use the "reload force" CLI command instead of "reload". (242578) Introduced in 4.19.6. Fixed in 4.20.4

- "mpls ldp password" will show the same encoded password every time "show running-config" is run from the CLI. (242633) Introduced in 4.15.4. Fixed in 4.20.6

- After running "rollback clean-config" in a config session, interface range commands include inactive interfaces. (243338) Introduced in 4.14.0. Fixed in 4.18.8,
  4.19.6,
  4.20.3

- The Launcher agent will restart repeatedly if a user daemon is configured with a string containing a "%" character. (247398) Introduced in 1.0.0. Fixed in 4.18.7,
  4.19.7,
  4.20.5,
  eos-trunk

- When "channel-group" command is applied through eAPI on an Ethernet interface, its switchport configuration may override the switchport configuration of the port-channel that the Ethernet interface is configured in.

  Workaround is to add the required switchport configuration on all member interfaces of the port-channel. (412920) Introduced in 1.0.0. Fixed in 4.21.9,
  4.22.3,
  4.23.1,

delhi-maint,
eos-trunk,
florence-maint

•
Configuring a monitor session with many source interfaces may cause the CLI prompt to be become unresponsive. The command is expected to complete but just take longer. A separate CLI session can be used to enter other configuration commands. (520357) Introduced in 4.21.3. Fixed in 4.25.2,
eos-trunk

•
Configuring VLAN to VNI mapping within a config session may fail with a message that the VLAN conflicts with an internal VLAN, even if conflict is resolve when the config session is applied. (532496) Introduced in 1.0.0. Fixed in 4.22.9,
4.23.7,
4.24.4,
4.25.2,
eos-trunk,
florence-maint,
istanbul-maint,
lima-maint

•
Using comments inside the route map mode may result in the config being rejected with an internal error.
Remove the comments to work around this. (536882) Introduced in 4.25.1. Fixed in 4.25.3,
4.26.1,
eos-trunk,
oslo-maint

• The Routing Control Function CLI may show as out of compliance when the RCF configuration is edited locally. (553342) Introduced in 4.24.2.

•
When CloudVision verifies configlets, unsupported commands may not be rejected. (560938) Introduced in 4.20.1. Fixed in 4.22.11,
4.23.8,
4.24.6,
4.25.4,
4.26.1,

eos-trunk,
florence-maint,
istanbul-maint,
lima-maint,
oslo-maint

• The 'logging level all' CLI expands to individual commands in the configuration, preventing dynamic updates of the logging list as part of EOS upgrades. (579047) Introduced in 1.0.0.

• Any change to inband telemetry profile in profile mode gets applied only when inband telemetry mode is exited. (606599) Introduced in 4.26.1.

• When inband telemetry is disabled, some flow information reported by CloudVision will be incorrect for a short time. (606609) Introduced in 4.26.1.

•
"default switchport mode routed" and "no switchport" config commands may need to be manually reconciled in CloudVision after ZTP. (665217) Introduced in 4.26.2. Fixed in 4.26.8,
4.27.6,
4.28.2,
eos-trunk,
rio-maint,
uppsala-maint

•
When using in-band management, Arista's best practice is to enable LACP fallback on the upstream LAG and/or MLAG links to prevent a temporary disruption when provisioning a downstream device. (676588) Introduced in 1.0.0. Fixed in 4.26.7,
4.27.7,
4.28.1,
rio-maint,
uppsala-maint

•
When performing a config-replace over eAPI, RCF compilation errors may be treated as warnings. (688732) Introduced in 1.0.0. Fixed in 4.30.0,
eos-trunk

• If 'dot1x...' and 'mac security...' CLIs appear sequentially in the same CloudVision configlet the designed configuration will fail to validate. This automatically occurs if both CLIs are reconciled into the reconcile configlet.

Separating the CLIs into different configlets will allow the designed configuration to validate. (798565) Introduced in 4.17.0.

- Switch may hold stale dynamic MSS-G configuration after an OpenConfig restart. After OC restart, deletes to previous configs will have no effect, however, new updates to the config will be correctly set. Due to this, customer may experience unexpected data drop/forward or unexpected resource usage due to the stale config. (814432) Introduced in 4.27.1. Fixed in 4.31.1

• Changing certain MLAG configuration parameters (MLAG domain ID, local MLAG interface, MLAG peer address, MLAG peer interface) will cause the MLAG session to temporarily go down while the connection is renegotiated. This can lead to transient L2 loops in the network until the MLAG session is re-established. If EVPN is also being used, this can lead to rapid MAC flaps between devices in the network, causing those MACs to become blacklisted by EVPN. To see if a particular MAC has been added to the EVPN blacklist, use the "show bgp evpn host-flap" command.

As a workaround, configuring EVPN host-flap recovery will allow the blacklisted MACs to age out after a configured time once the MLAG session has been re-established. Blacklisted MACs may also be cleared manually with the "clear bgp evpn host-flap" command. (891929) (1) Introduced in 4.20.5.

Relevant TerminAttr Limitations and Software Caveats

- Streaming Agent (TerminAttr) fails to stream the running config when there are 65533 or more lines that have changed since the last time the running config was streamed. Initialization is not affected, only subsequent running config changes. (375243) Introduced in TerminAttr-v0.1. Fixed in TerminAttr-v1.8.0

- Streaming Agent (TerminAttr) may restart unexpectedly when streaming a large collection under /Smash. (409785) Introduced in TerminAttr-v1.6.0. Fixed in TerminAttr-v1.7.0

- Token authentication may fail if one node in a multi-node CloudVision cluster is down when a retry on another node would succeed. (421336) Introduced in TerminAttr-v1.6.0. Fixed in TerminAttr-v1.7.2

- Streaming Agent (TerminAttr) low memory mode can cause increased load on the Sysdb process. (422612) Introduced in TerminAttr-v1.5.0. Fixed in TerminAttr-v1.7.3

- In low memory mode Streaming Agent (TerminAttr) does not stream to CloudVision. (423940) Introduced in TerminAttr-v1.7.1. Fixed in TerminAttr-v1.7.3

- Unable to identify devices from snooped DHCP packets with user-defined Circuit IDs. (426567) Introduced in TerminAttr-v1.6.0. Fixed in TerminAttr-v1.7.3

- Streaming Agent (TerminAttr) may restart unexpectedly if Flow Telemetry is enabled and encounters an sFlow packet with an empty AS Path. (443083) Introduced in TerminAttr-v1.6.0. Fixed in TerminAttr-v1.7.7

- On a dual-supervisor system, Streaming Agent (TerminAttr) may report incomplete information to CloudVision 2020.3.0 or later when verifying compliance. This may result in CloudVision reporting a system as being in compliance even when the standby supervisor is not configured with the expected boot settings. (512196) Introduced in TerminAttr-v0.1. Fixed in TerminAttr-v1.10.4,
  TerminAttr-v1.11.1,
  TerminAttr-v1.12.0,
  TerminAttr-v1.8.6,
  TerminAttr-v1.9.8

- Streaming Agent (TerminAttr) may restart unexpectedly when "Advanced login options" is enabled in CloudVision. (533996) Introduced in TerminAttr-v0.1. Fixed in TerminAttr-v1.10.6,
  TerminAttr-v1.12.2

- Streaming Agent (TerminAttr) may consume significant CPU resources on CloudVision when connecting with invalid credentials. (548733) Introduced in TerminAttr-v1.10.0. Fixed in TerminAttr-v1.10.7,
  TerminAttr-v1.12.3,
  TerminAttr-v1.13.2

•

On EOS 4.25.2 or later the route type information is shown as unavailable for the routing table. (558429) Introduced in TerminAttr-v1.13.3. Fixed in TerminAttr-v1.14.1

• The reported compliance status maybe incorrect sometimes after a config push task with large number of config lines is executed.
Workaround is to restart Streaming Agent (TerminAttr) on the device. (600308) Introduced in 4.30.1.

•

If Streaming Agent (TerminAttr) is enabled, 'management api gnmi' is configured, and TerminAttr is streaming to CloudVision 2022.3.0 or above, then Streaming Agent's CPU and memory usage may increase.
Workaround this issue by adding "-cvconfig=false" to the Streaming Agent configuration or disabling 'management api gnmi'. (772493) Introduced in TerminAttr-v1.19.0. Fixed in TerminAttr-v1.19.5

• Pushing changes to the Streaming Agent (TerminAttr) configuration via CloudVision may cause the config update to fail. The workaround is to push the Streaming Agent configuration separate from other configuration changes. (795985) Introduced in 1.0.0.

• Streaming Agent (TerminAttr) is calculating the interface metric rates, including interface errors. When the device is having connectivity problems to CloudVision, the rate notifications may be coalesced during periods where the device is unable to connect which causes a loss of intermediate state. (807166) Introduced in 1.0.0.

• Streaming Agent (TerminAttr) does not stream the devices running configuration when running in low memory mode. (946459) Introduced in TerminAttr-v0.1.