Arista CloudVision®

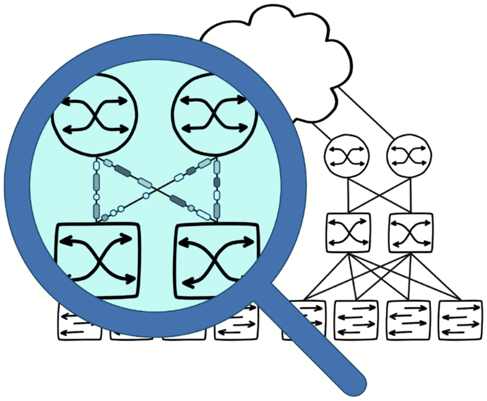
Cloud Automation for Everyone

CloudVision

Table of contents

Introduction

There is an old adage within IT management mindsets when problems arise – the network is guilty until proven innocent. As the interconnect between all IT infrastructure components including compute and storage, both physical and virtual, applications and their clients, the network is crucial to all IT operations. The network is expected to always be available. When an IT issue occurs, the network is usually the initial suspect.



Network operations teams must manage availability, security, agility, costs, and risks across multiple network domains including campus, data center, branch, WAN, and cloud environments. To do so, they require a system of tools and services that enable them to leverage efficient and repeatable workflows to manage day-0 through day-2 requirements of the network. The demand on and therefore capabilities of these tools must evolve as most IT environments strive for the holy grail of a network-as-a-service delivery model.

Traditional approaches to monitoring and managing networks have failed to keep up with demands. Network operations teams face ongoing challenges including rapid planning and deployment of applications, site deployments and expansions, rapid problem troubleshooting and resolution, and risk management and compliance assurance. They must meet these demands all while maintaining an accurate accounting of network devices, their versions, configurations, connections, and status. All these actions must also be planned, approved, executed, verified, documented, and be repeatable. As human error remains a primary cause of network issues, software-driven approaches are needed to enable operations automation to improve both reliability and mean-time-to-innocence.

Cloud Principles for Enterprise Network Operations

Arista has long been delivering network solutions with a unique software-driven approach to building reliable networks designed around the principles of best practices, standardization, simplification, cost-savings, and automation. Arista coined the term "cloud networking" to characterize the evolving approach to address these principles, while working closely with and learning from the largest hyper-scale cloud operators on their journeys.

Cloud operators pioneered new approaches to network design and operational practices with a software-first thinking to overcome the vast operational and technical challenges they faced. These derived principles modernized networking for hyper-scale cloud service providers with simplified network designs using standards-based protocols, open scale-out IP fabric designs, and software-driven orchestration to help them scale their operations while minimizing resource consumption and maximizing infrastructure utilization and service delivery times.

Just as hyper-scale cloud operators pioneered the use of network operations automation to simplify time-consuming and error-prone operational tasks, and to mitigate the human-derived risk factors – such principles can be applied to enterprise network operations in much the same way and achieve the same benefits.

Enterprises wanting to incorporate such principles into their own IT operations models are faced with decisions including:

- **Buy vs Build -** While hyper-scale cloud operators developed most of their management systems in-house, most enterprises do not have the time, skill sets, or resources to build their own network automation systems. Therefore, many enterprises look for a modern, turnkey, comprehensive network operations platform providing the same benefits.
- **Modern vs Antiquated Toolsets -** Automated network operations cannot be built upon network management tools that are decades old, based on SNMP polling or screen-scraping. They require a system approach with real-time automation, offering open network state-streaming APIs for continuous real-time knowledge of network state and configuration, and advanced AI/ML analytics to provide instantaneous compliance audits, full network visibility including application layouts, and speedy troubleshooting capabilities.

- **Common vs Siloed device capabilities -** Traditional enterprise networks have often been deployed by selecting a different "box" for each "place-in-the-network". With each type of device often comes a different operating system, varying design limitations, mismatched feature sets and APIs, and siloed management applications. Choosing platforms with the greatest feature set commonality, across the widest aperture provides an alternative to the disparate "places-in-the-network" approach.

There are also different approaches to achieving a level of network ops automation depending on a customer's specific requirements and in-house skill sets. These approaches include:

- **Do-It-Yourself (DIY) -** typically deployed by hyper-scale cloud operators who are building massive public infrastructures. Automation is fundamental to their business model and a means to remain competitive. With many specialized in-house applications and services, they employ large software teams to automate their entire operation. Arista provides open tools including an EOS SDK, Openconfig / gRPC agents, streaming telemetry, and eAPI device programmability enabling these customers to fully integrate EOS-based switches into their broader software orchestration systems.
- **Continuous Integration/ Continuous Delivery (CI/CD) -** typically deployed by service providers and enterprises leveraging automation frameworks such as Hashicorp Terraform or Red Hat Ansible to automate the provisioning of the network infrastructure. These customers often have resources and skills to write their own custom scripts and are invested in DevOps automation approaches along with the required resources. Arista supports these customers by providing open software integration into DevOps frameworks like Terraform, Ansible, and others as well as supporting streaming receiver platforms like ELK stack, Prometheus, and others.
- **Turnkey Solution -** There are few tools that exist today to comprehensively deliver a turnkey network automation solution, and fewer still for customers that do not have the time, skills, or resources to modify a subpar solution to meet their needs. CloudVision provides a turnkey solution for all customers, enabling customers to provision, manage and observe their infrastructure while permitting extensibility and customization. CloudVision is designed to help customers of all sizes, in particular small, mid-sized, and large enterprises across every industry who are looking to reduce OpEx by applying the principles and lessons learned by cloud providers.

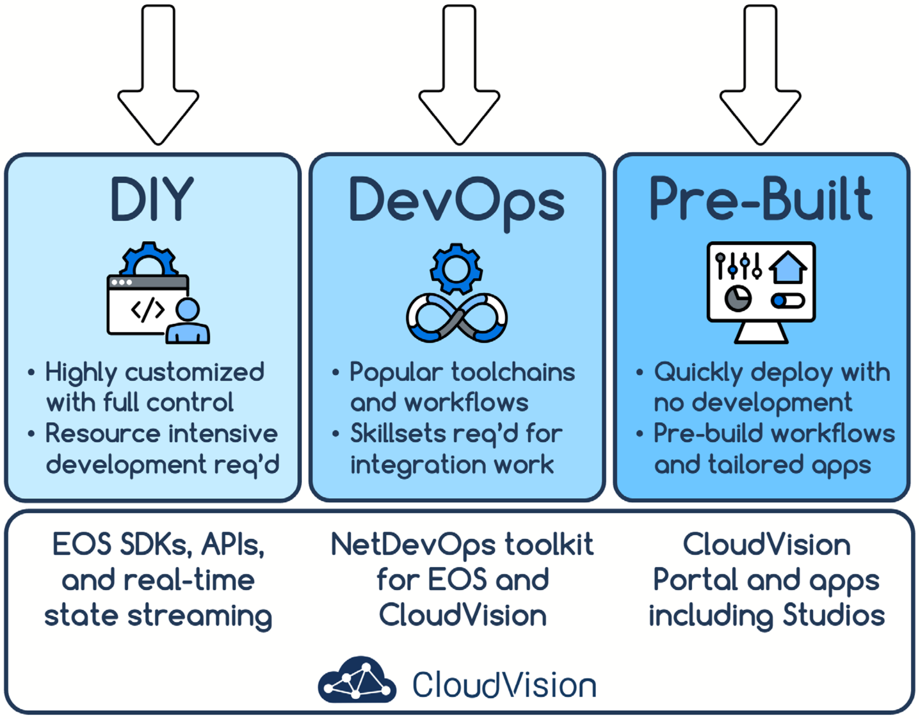

DIY
• Highly customized with full control
• Resource intensive development req'd
DevOps
• Popular toolchains and workflows
• Skillsets req'd for integration work
Pre-Built
• Quickly deploy with no development
• Pre-build workflows and tailored apps
EOS SDKs, APIs, and real-time state streaming
NetDevOps toolkit for EOS and CloudVision
CloudVision Portal and apps including Studios
CloudVision

Figure 2: Solutions from DIY to Pre-Built

CloudVision Overview

CloudVision is a modern, multi-domain network management platform built on cloud networking principles for telemetry, analytics and automation. It provides a single unified management plane across the enterprise, breaking down traditional management silos and bringing consistency to network operations across the entire enterprise network.

Arista's Extensible Operating System (EOS®) together with CloudVision® provide a platform based on a software-driven model for turnkey network automation across multiple network domains. A consistent approach for automated operations and real-time network visibility applies across the enterprise network including campus wired and wireless, data center, branch, the wide area network, and hybrid cloud.

Backing the platform is Arista's network data lake or NetDL. NetDL represents a comprehensive set of time-series state data streamed from each Arista EOS-based platform in the network and also includes select 3rd party data from Arista partners. Partner data includes such sources of truth as IP address management (IPAM) information along with information about connected workloads from partners such as VmWare. NetDL gathers EOS-based device state including device platform details, configurations, protocols, and services, and rolls this into a complete real-time picture of the entire network. Since the data is stored in a time-series, the operator can even go back in time to see a past picture of the network and its state to perform root cause analysis of any encountered problems. This vast wealth of knowledge is utilized by each feature within CloudVision to offer unparalleled visibility into a multi-domain enterprise network. NetDL not only includes gathered state data from Arista EOS-based devices but also incorporates data from 3rd party sources.

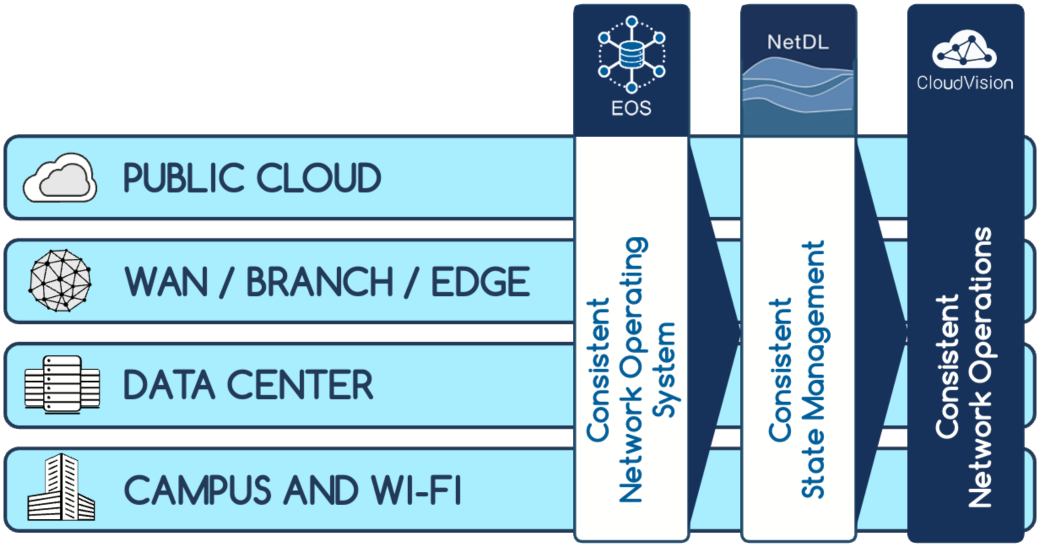

EOS
NetDL
CloudVision
PUBLIC CLOUD
WAN / BRANCH / EDGE
DATA CENTER
CAMPUS AND WI-FI
Consistent Network Operating System
Consistent State Management
Consistent Network Operations

Figure 3: Consistent Approach for Every Place in the Network

CloudVision provides a single network management platform for enterprises incorporating:

- multi-domain network operations and visibility consistency
- zero-touch automated provisioning
- cognitive analytics with machine learning
- suite of applications addressing security, compliance, provisioning, change controls, etc
- an ecosystem of partner value-added integrations

CloudVision as-a-Service or On-premises

CloudVision can be deployed in two models. For on-premises deployments, the software can be deployed as a virtual or physical appliance and must be deployed in production as a three node cluster for utmost availability. Arista offers a turnkey CloudVision hardware appliance which can be deployed in the required cluster topology thereby ensuring the hardware meets all requirements of the CloudVision software. With the on-premises deployment, hardware, software, network, storage, and compute management services are the responsibility of the appropriate in-house ops teams team with regards to the locally deployed CloudVision cluster nodes.

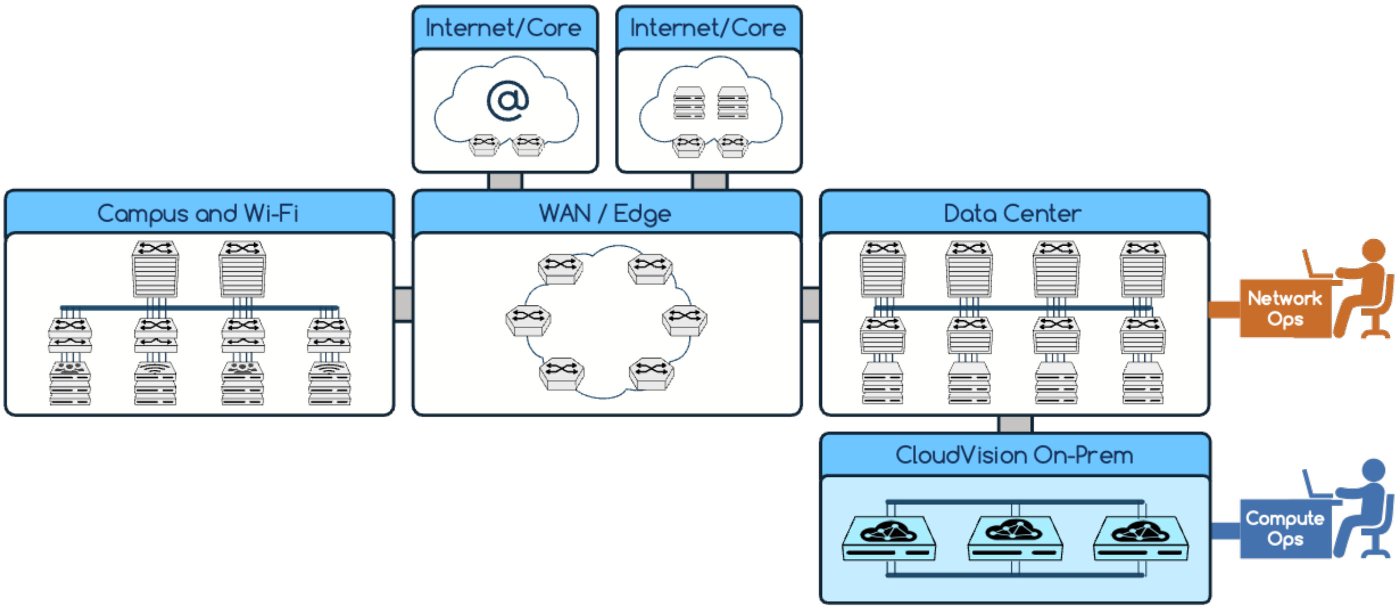


Figure 4: On-Premises CloudVision Deployment

To alleviate the additional on-premises ops requirements, CloudVision can also be deployed as a fully managed cloud-service offering - CloudVision-as-a-Service or CVaaS. CVaas leverages the same software stack as provided by the on-prem deployment model thereby giving the same user experience. However, CVaaS adds the capabilities of rapid bring-up and device onboarding, and access to an always up-to-date CloudVision application. The managed-service is operated, scaled and maintained by dedicated Arista site reliability engineers on a proven and secure tier-1 public cloud platform.

CVaaS ensures enterprises that their CloudVision deployment is always current with the continuous delivery of tested feature updates and patches, including providing the earliest access to all of the latest feature improvements.

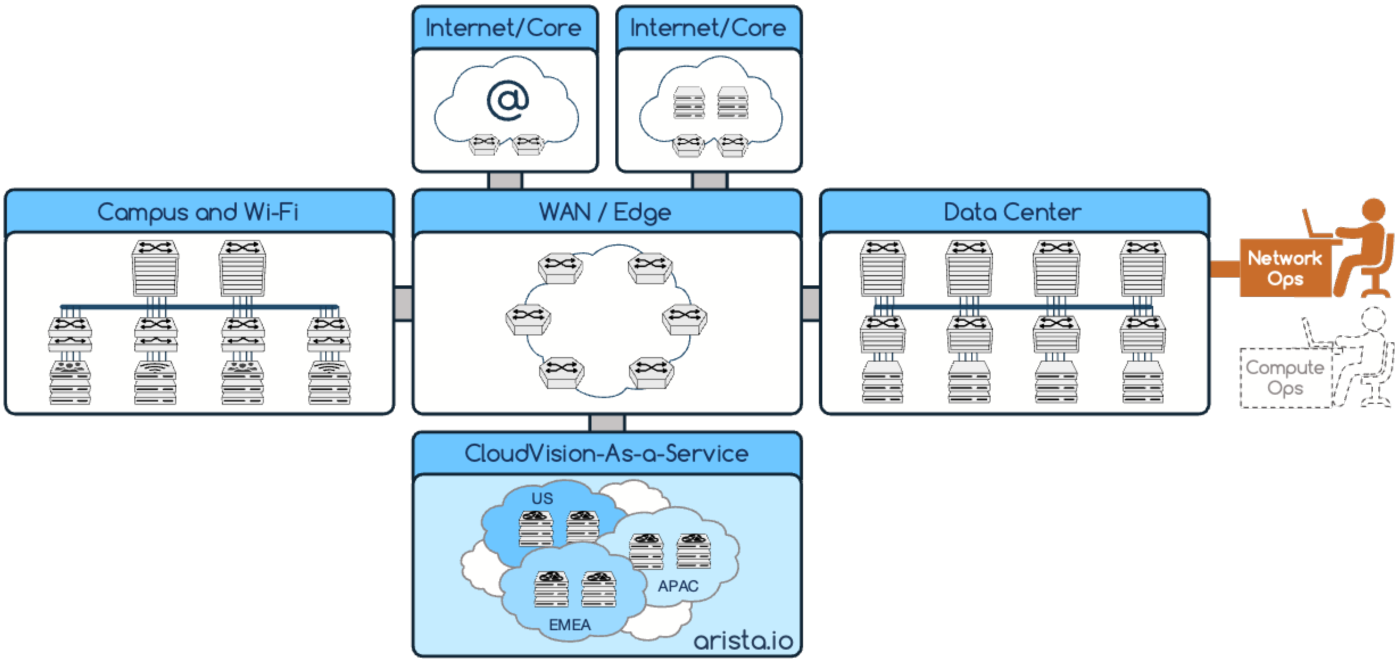


Figure 5: CloudVision-as-a-Service or CVaaS

Getting started with CVaaS is as simple as creating an onboarding token through the assigned CVaaS cluster and loading that into each on-prem EOS device to be onboarded. This can even be further simplified by leveraging Arista's Zero Touch Provisioning or ZTP and an already embedded token. This method is a way to onboard switches into CloudVision using a pre-generated token that is already embedded in Arista switches along with a couple options set within a DHCP server.   Following this method requires no user intervention on the switches themselves Once devices have been onboarded, the network ops team will immediately gain insights over network state, compliance, and visibility.

Access to new services, like proactive A-Care support analytics, connected advanced services support, and AI-ML based trending for rapid resolution of customer inquiries will be possible for customers of the managed-service in the future, as machine learning algorithms can provide aggregated insights and solutions based on the breadth of anonymized and processed data in the service.

While CVaaS has a number of unique advantages, the choice of on-prem or cloud-based deployment of CloudVision is left to the enterprise customer and provides fundamentally the same services and features.

CVaaS, like it's on-premises deployment, provides the same extensive set of capabilities including:

- Support for deployment of all Arista network products including EOS physical switches, virtualized CloudEOS public cloud and remote site based instances, containerized EOS routers running within Kubernetes clusters EOS images running on 'white boxes', and Arista Wi-Fi access points
- Error-free onboarding of new devices with Zero Touch Provisioning (ZTP) for faster onboarding and for rapid site or cloud upgrades or expansions
- Safe and secure with end-to-end data encryption for protection of data-at-rest and data-in-transit, rigorous operational controls, and security testing and hardening
- Multi-factor authentication and role assignment with a choice of identity services such as Microsoft Azure Active Directory, Google Identity Service, Okta, One Login, and others
- Supports the popular CloudVision and third-party integrations and applications, including ServiceNow, Ansible, Terraform, Multi-Domain Segmentation Services and others

CloudVision Architecture

CloudVision's overall architecture can be summarized into three main functionality blocks. The first block has the purpose of receiving all streamed network and device state from all Arista EOS-based devices under management in addition to providing a front-end access to CloudVision through a web UI or API. Extensive state data exists within each EOS device in a database known as SysDB. This data is updated in real-time by all functional processes within the device using a publish/subscribe architecture. SysDB maintains extensive state including from network protocols, hardware, and internal processes along with network flow information, various counters, and the configuration of the device itself. State from each participating EOS device is synchronized in a secure manner to CloudVision's database using the same publish/subscribe architecture of the EOS system database (SysDB). This combined state from all network devices is known as NetDB and represents a real-time view of the entire network. The value of having an aggregated real-time view of the network state cannot be overstated without the need to poll, screen-scrape, transform, filter and refresh. The receiver can also receive information from other relevant sources including partner applications. This larger view of the network consisting of not only network state received from SysDB but also from other relevant sources is known as Arista's Network Data Lake or NetDL. This comprehensive data set can provide a unifying abstraction point for integration with third-party IT operations, configuration management, deployment and orchestration tools like ServiceNow and Ansible.
The second functional block manages the storage of all the received data. Within CloudVision exists Arista's expansive data lake called NetDL. NetDL is a multi-modal storage facility that stores the vast amount of data that is streamed to CloudVision. This data is stored in the most appropriate and efficient mode of storage depending on the type of data. NetDL really represents the 'crown jewels' of CloudVision and is key to its industry leading position. Since this data is stored as a time-series, it can be retrieved by any of the CloudVision services for historical analysis, or the ability to go back in network state-time.

The third functional block consists of an analytics pipeline within CloudVision that analyzes the data and provides useful information to the various features and services within CloudVision. This is where the 'smarts' of CloudVision exist in that a wealth of visibility and control are afforded to the network operator, across a multi-domain network environment, in real time.

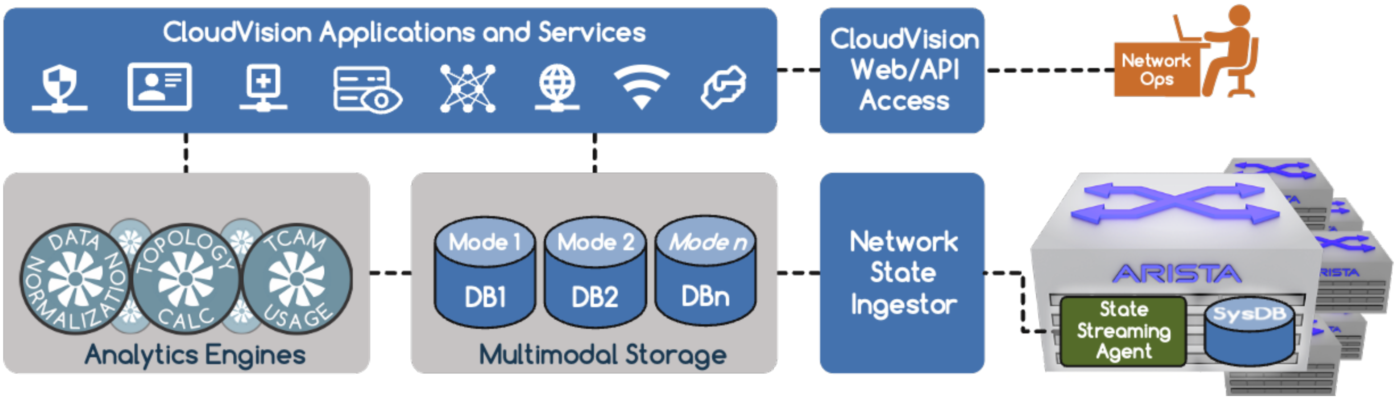


Figure 6: CloudVision High-Level Architecture

CloudVision is built on a modern scale-out architecture with multi-domain end-to-end telemetry and state-streaming, big-data distributed scale-out storage, and embedded stream processing capabilities. It is implemented as microservices orchestrated under Kubernetes and packaged as a turn-key solution whether deployed on-prem or within the cloud as CVaaS.

In a CVaaS deployment model, control plane and data plane traffic are always kept local to the on-premises network while the management plane lives in the cloud. Examples of control plane services include all routing protocols (such as BGP, OSPF, IS-IS, etc.), spanning tree, MLAG, and EVPN for VXLAN overlays. The data plane refers to the transport of user and application data. The management plane includes all functions used to provision, control, and monitor network devices and services. CVaaS leverages EOS device telemetry that is encapsulated, encrypted, and streamed from network devices to the cloud service.

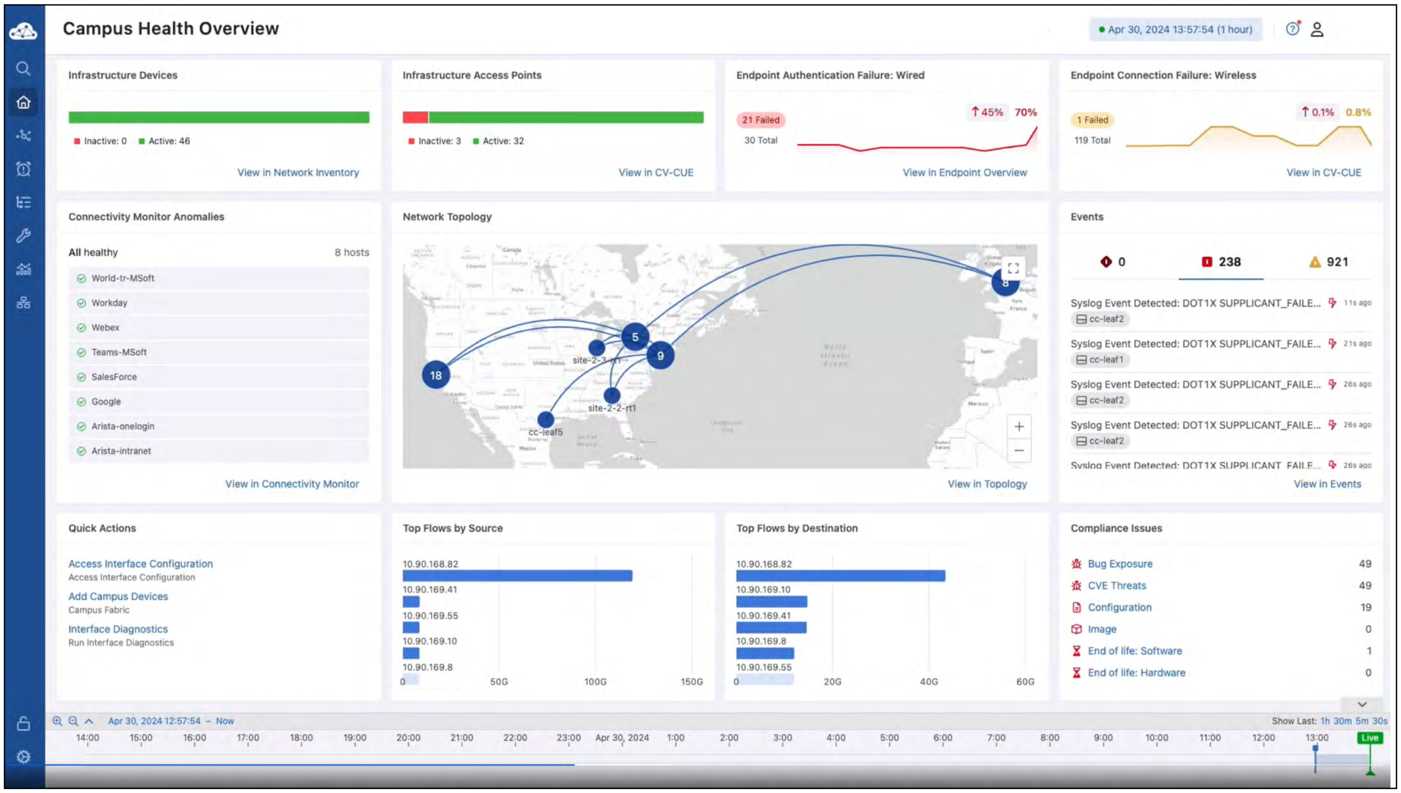
CloudVision is designed so that services on-premises continue to operate even when CloudVision is unavailable, such as during a network or cloud outage. Arista devices provide network access in the customer network using the last known configuration when they are disconnected from the cloud service, and devices can be accessed and managed locally at any time.

CloudVision Web Portal

The CloudVision portal combines the most common operational tasks in a web-based dashboard view, decoupled from the underlying hardware. Workflow automation in CloudVision permits operators to execute common deployment and configuration tasks from a single visual touchpoint.

The portal includes a turnkey solution for Arista's Zero Touch Provisioning (ZTP) which includes automating initial device provisioning and automating ongoing change controls and device replacements over the operational life cycle of the network.

Using the CloudVision web portal, operators can organize devices into logical hierarchies or groupings through the use of list or configuration 'container views' – for rapid categorization of devices by role, type, or any other user-desired specification. Configurations can be broken down into more granular 'configlets' that are built and stored directly on CloudVision, ready for network-wide or group-specific provisioning. This flexible 'container views' model enhances operational efficiency while simplifying change management, thus reducing potential human error, providing a centralized source of configuration 'truth', and allowing both real-time and historic troubleshooting. In addition, ongoing risk and compliance management workflows can be automated to allow greater agility for the entire network operations lifecycle.



Syslog Event Detected: DOT1X SUPPLICANT_FAILE... 11s ago cc-leaf2
Syslog Event Detected: DOT1X SUPPLICANT_FAILE... 21s ago cc-leaf1
Syslog Event Detected: DOT1X SUPPLICANT_FAILE... 26s ago cc-leaf2
Syslog Event Detected: DOT1X SUPPLICANT_FAILE... 26s ago cc-leaf2
Syslog Event Detected: DOT1X SUPPLICANT_FAILE... 26s ago

Compliance Issues	
Bug Exposure	49
CVE Threats	49
Configuration	19
Image	0
End of life: Software	1
End of life: Hardware	0

Figure 7: CloudVision Web Portal

CloudVision's included web features can present real-time or historical data, including a history of network state, configuration and software versions and comparisons across different devices, metrics and time-windows. This centralized state visibility 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.

State Streaming

EOS-based device state, stored in SysDB within the device, is streamed from each device to the CloudVision database, through CloudVision's analytics pipeline, and then is represented within one of the many features within the web-based UI. There is no polling of any data anywhere within the system. A state streaming agent named TerminAttr exists within each EOS-based switch. The *TerminAttr* agent streams the time-stamped device-state data to the CloudVision.

The transport layer used between services throughout CloudVision is the gRPC remote procedure call. gRPC is a modern high-performance framework built on top of Google's open source Protocol Buffers mechanism and HTTP2, providing scale and performance to stream full network state from each EOS-based device into CloudVision.

The streaming telemetry agent in EOS and the device SDK are built upon gNMI (gRPC Network Management Interface), an open-source protocol specification created by the OpenConfig working group. gNMI is used to provide read, write, and subscribe semantics from network devices to the datastore, while OpenConfig provides the standard data models. These methods and data models are the obvious choice for modeling network state in CloudVision. These models have been supplemented where necessary by Arista to represent the complete state of an EOS-based device.

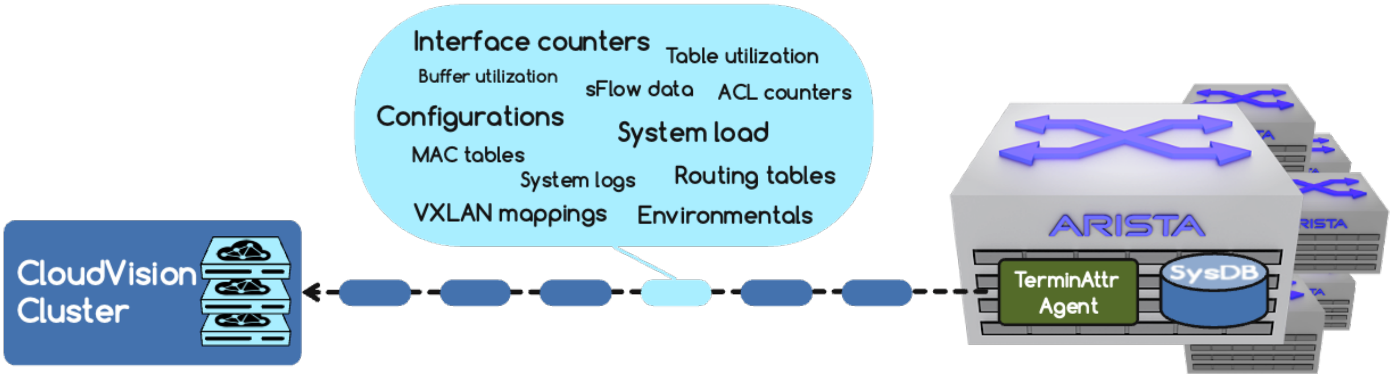


Figure 8: EOS State Streaming to CloudVision

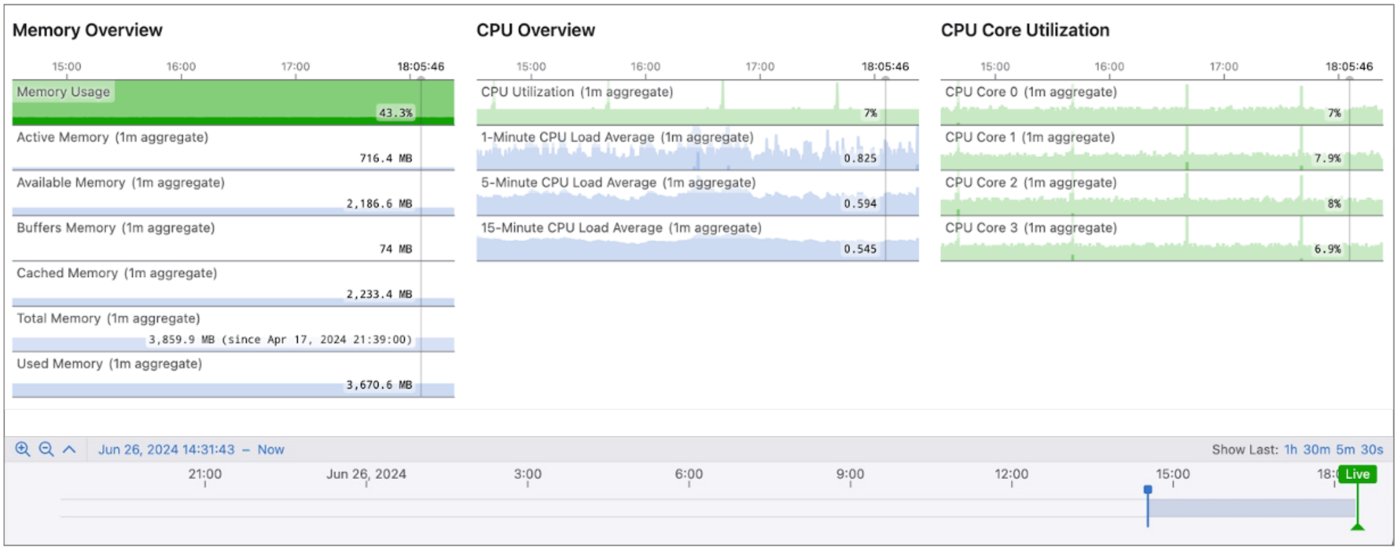
In order to provide a network-wide aggregate view, the CloudVision Analytics Engine serves as a backend repository to collect and process all streamed data, including historical time-stamped data as it is received. The Analytics Engine performs a variety of stream processing and data analysis including state correlation, event generation, trend monitoring, anomaly detection, and other analytics.

The Analytics Engine also offers an API server that enables customers and partners a single point of integration to third-party or internal tools using streaming and WebSocket-based APIs. CloudVision Telemetry Applications and third-party applications leverage access to the state repository via the API server, offering a seamless way to provide read/write access to the state repository.

The streaming telemetry and analytics then feed into the provisioning workflows in CloudVision, where the user can fully automate the rollout of network-wide changes, from initial deployment to ongoing change controls.

Real-time Telemetry

Telemetry streaming enables CloudVision to instantaneously identify network problems. It enables IT operations teams to quickly optimize network performance compared to legacy management systems relying on polling. When network conditions worsen due to configuration changes, intermittent faults, or demanding workloads, CloudVision presents instantaneous visibility of the condition. Intermittent problems occuring between polling intervals are no longer missed. Problem remediation can start within seconds.



Memory Overview

Memory Usage 43.3%

Active Memory (1m aggregate) 716.4 MB

Available Memory (1m aggregate) 2,186.6 MB

Buffers Memory (1m aggregate) 74 MB

Cached Memory (1m aggregate) 2,233.4 MB

Total Memory (1m aggregate) 3,859.9 MB (since Apr 17, 2024 21:39:00)

Used Memory (1m aggregate) 3,670.6 MB

CPU Overview

CPU Utilization (1m aggregate) 7%

1-Minute CPU Load Average (1m aggregate) 0.825

5-Minute CPU Load Average (1m aggregate) 0.594

15-Minute CPU Load Average (1m aggregate) 0.545

CPU Core Utilization

CPU Core 0 (1m aggregate) 7%

CPU Core 1 (1m aggregate) 7.9%

CPU Core 2 (1m aggregate) 8%

CPU Core 3 (1m aggregate) 6.9%

Jun 26, 2024 14:31:43 – Now

Show Last: 1h 30m 5m 30s

Figure 9: CloudVision's Timeline Slider Example

For historic troubleshooting situations, time-stamped records of the received state and telemetry data can be viewed within CloudVision applications on a time-series continuum with the use of a simple slider mechanism, showing granular details at every point in time. This capability enables events and data to be correlated with each other, and with any other observed anomalies that have been reported.

Analytics Platform AI/ML

AI/ML is the application of Artificial Intelligence (AI) techniques to predict outcomes of observed conditions and to take actions accordingly. By configuring devices to stream device-state and telemetry data to CloudVision, the Analytics Engines along with the CloudVision applications use Machine Learning (ML) algorithms to provide valuable insights into the entire state of the network, highlighting observed anomalies, and providing real-time insights, updates, and alerts.

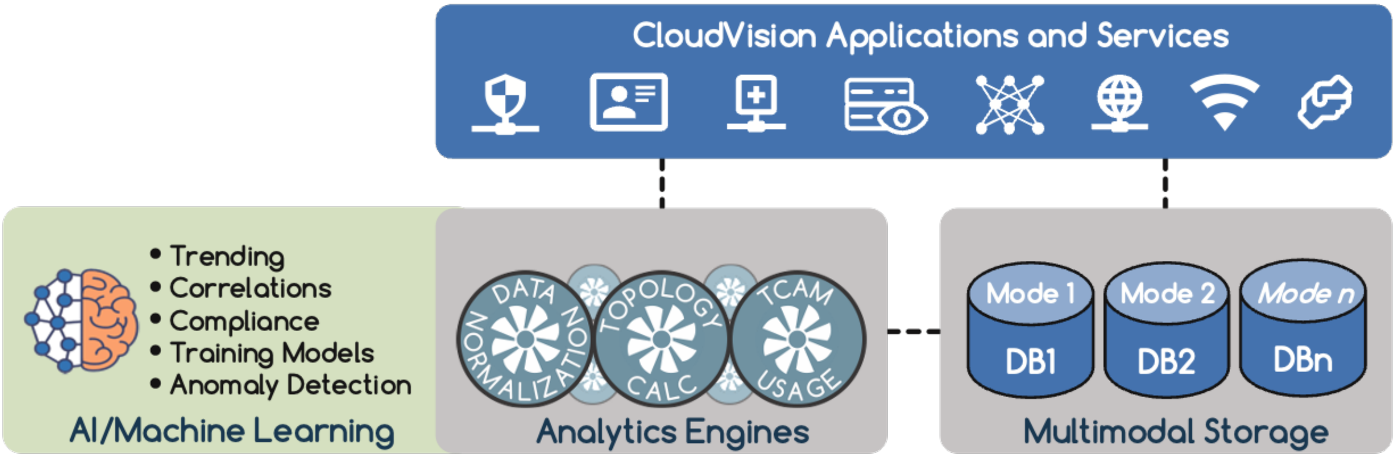


Figure 10: CloudVision Analytics Platform

CloudVision uses its analytics pipeline to improve network operations with AI/ML algorithms that are implemented in microservices called "Turbines". The value of the applied AI/ML technology in these scenarios depends on the quality and timeliness of data that is being analyzed, benefiting greatly from the real-time state and telemetry data that is streamed in real-time into the CloudVision platform from connected devices.

Some examples of where AI/ML technology is used in CloudVision include:

- **Reachability Anomalies.** Modeling time-series data to determine reachability and latency baselines derived from CloudTracer telemetry. Alerts are generated based on dynamically learned deviations from a reachability/latency baseline and compared over time.
- **Resource Utilization.** Monitoring resource utilization trends and associated telemetry to make predictive assessments and generate proactive notifications before functional hardware limits such as TCAM allocation are reached.
- **Device Observability.** Using correlation analysis of subtle device state changes such as optical power levels, hash selection, or buffer utilization to identify transient 'grey failures' and prevent these hard to pinpoint issues.
- **Quality of Experience.** Using decision tree models to quickly determine the root cause of issues faced by network clients connected to wireless and wired access points, Support Vector Machines (SVM) algorithms for analysis of application-specific quality of experience based on network parameters, and client experience baselines to detect client anomalies and alert network administrators to deviations in client experience compared with long term norms.

High Availability Clusters

CloudVision software can be deployed as a virtual or physical appliance. In an on-prem production deployment, a cluster of three redundant servers is used to achieve high levels of availability. In a CVaaS environment, larger clusters support multi-tenancy and can be expanded to as many nodes as required to meet service level objectives.

The Analytics engine uses the high-performance Hbase database to store device-state data, including events. Data is stored in a compressed format without a loss of resolution. Events and device state changes are time-stamped by the device as they occur and can be reviewed in a time slider in various application dashboards in CloudVision. Also, changes in device state and correlated events can be generated by the CloudVision platform to take predetermined actions, such as alerting an operator or executing a program or script.

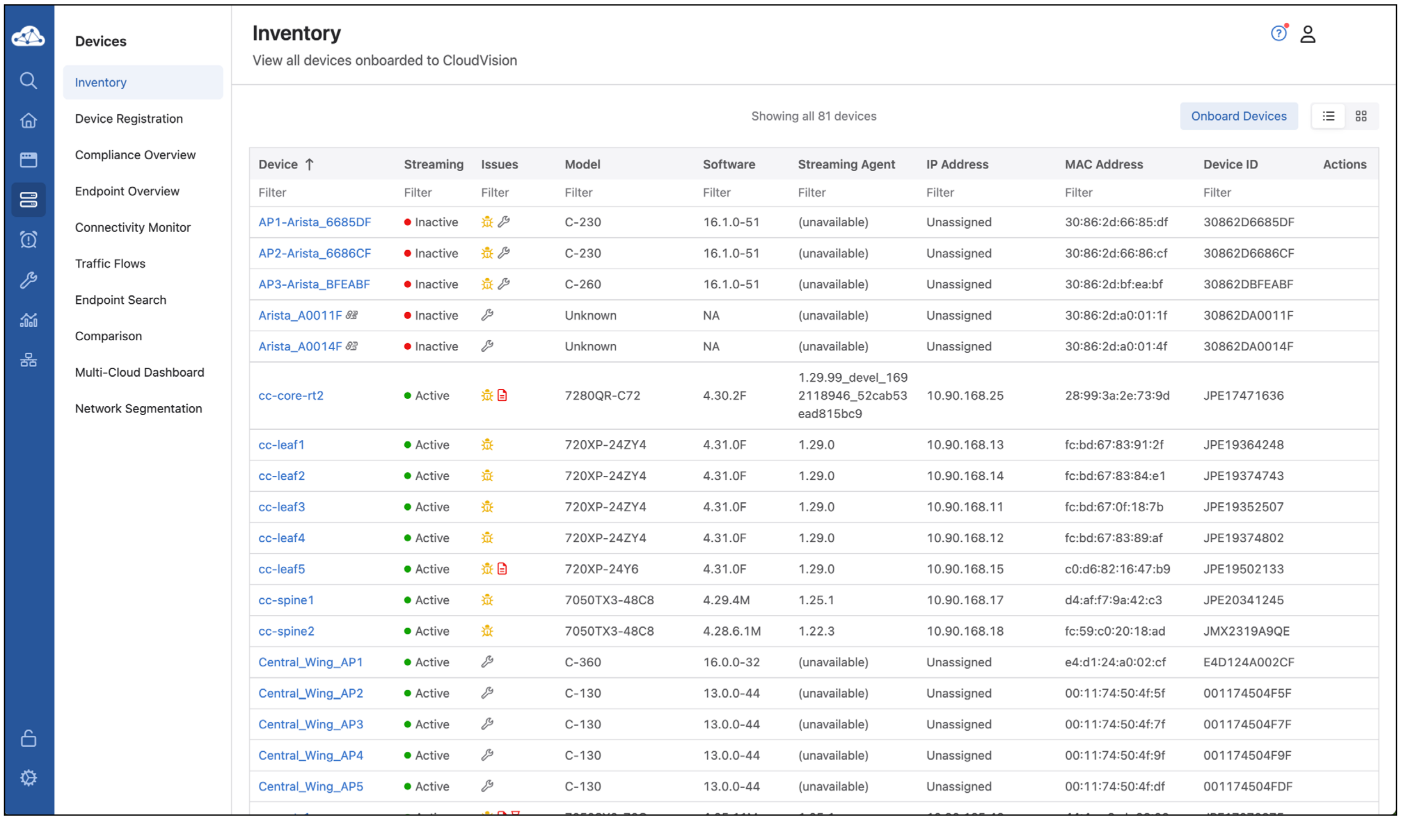
CloudVision Application Views

The CloudVision platform consists of the previously described core infrastructure and value-added applications shown as 'views' within the web GUI. The common views include Devices, Events, Provisioning, Dashboards, and Topology views. These views will be displayed in all instantiations of the CloudVision Portal. There are however additional views that are available depending on which additional features are enabled within CloudVision. Additional views may include the Overview, Network, and Application views.

Devices View

This view offers extensive detailed insights into device-level metrics that would be otherwise accessible using CLI commands. These include system details, environmentals, switching and routing statistics and related address tables, including VXLAN and much more. This view also includes sampled flow (sFlow or IPFIX) details collected by the EOS-based device if enabled within the device. Many areas of this view can be further expanded to show graphical representations of metrics over time or greater levels of detail.

The Devices view also provides access to an overall view of device compliance in regards to specific policies. These policies may relate to the requirement to run specific EOS versions, maintain certain configuration components or an ability to track potential bugs or Common Vulnerabilities and Exposures (CVE) threats that may exist within deployed devices. All this at a very simple glance.



Inventory

View all devices onboarded to CloudVision

Showing all 81 devices

Device ↑	Streaming	Issues	Model	Software	Streaming Agent	IP Address	MAC Address	Device ID	Actions
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	
AP1-Arista_6685DF	● Inactive	🐞 🔧	C-230	16.1.0-51	(unavailable)	Unassigned	30:86:2d:66:85:df	30862D6685DF	
AP2-Arista_6686CF	● Inactive	🐞 🔧	C-230	16.1.0-51	(unavailable)	Unassigned	30:86:2d:66:86:cf	30862D6686CF	
AP3-Arista_BFEABF	● Inactive	🐞 🔧	C-260	16.1.0-51	(unavailable)	Unassigned	30:86:2d:bf:ea:bf	30862DBFEABF	
Arista_A0011F	● Inactive	🔧	Unknown	NA	(unavailable)	Unassigned	30:86:2d:a0:01:1f	30862DA0011F	
Arista_A0014F	● Inactive	🔧	Unknown	NA	(unavailable)	Unassigned	30:86:2d:a0:01:4f	30862DA0014F	
cc-core-rt2	● Active	🐞 📄	7280QR-C72	4.30.2F	1.29.99_devel_1692118946_52cab53ead815bc9	10.90.168.25	28:99:3a:2e:73:9d	JPE17471636	
cc-leaf1	● Active	🐞	720XP-24ZY4	4.31.0F	1.29.0	10.90.168.13	fc:bd:67:83:91:2f	JPE19364248	
cc-leaf2	● Active	🐞	720XP-24ZY4	4.31.0F	1.29.0	10.90.168.14	fc:bd:67:83:84:e1	JPE19374743	
cc-leaf3	● Active	🐞	720XP-24ZY4	4.31.0F	1.29.0	10.90.168.11	fc:bd:67:0f:18:7b	JPE19352507	
cc-leaf4	● Active	🐞	720XP-24ZY4	4.31.0F	1.29.0	10.90.168.12	fc:bd:67:83:89:af	JPE19374802	
cc-leaf5	● Active	🐞 📄	720XP-24Y6	4.31.0F	1.29.0	10.90.168.15	c0:d6:82:16:47:b9	JPE19502133	
cc-spine1	● Active	🐞	7050TX3-48C8	4.29.4M	1.25.1	10.90.168.17	d4:af:f7:9a:42:c3	JPE20341245	
cc-spine2	● Active	🐞	7050TX3-48C8	4.28.6.1M	1.22.3	10.90.168.18	fc:59:c0:20:18:ad	JMX2319A9QE	
Central_Wing_AP1	● Active	🔧	C-360	16.0.0-32	(unavailable)	Unassigned	e4:d1:24:a0:02:cf	E4D124A002CF	
Central_Wing_AP2	● Active	🔧	C-130	13.0.0-44	(unavailable)	Unassigned	00:11:74:50:4f:5f	001174504F5F	
Central_Wing_AP3	● Active	🔧	C-130	13.0.0-44	(unavailable)	Unassigned	00:11:74:50:4f:7f	001174504F7F	
Central_Wing_AP4	● Active	🔧	C-130	13.0.0-44	(unavailable)	Unassigned	00:11:74:50:4f:9f	001174504F9F	
Central_Wing_AP5	● Active	🔧	C-130	13.0.0-44	(unavailable)	Unassigned	00:11:74:50:4f:df	001174504FDF	

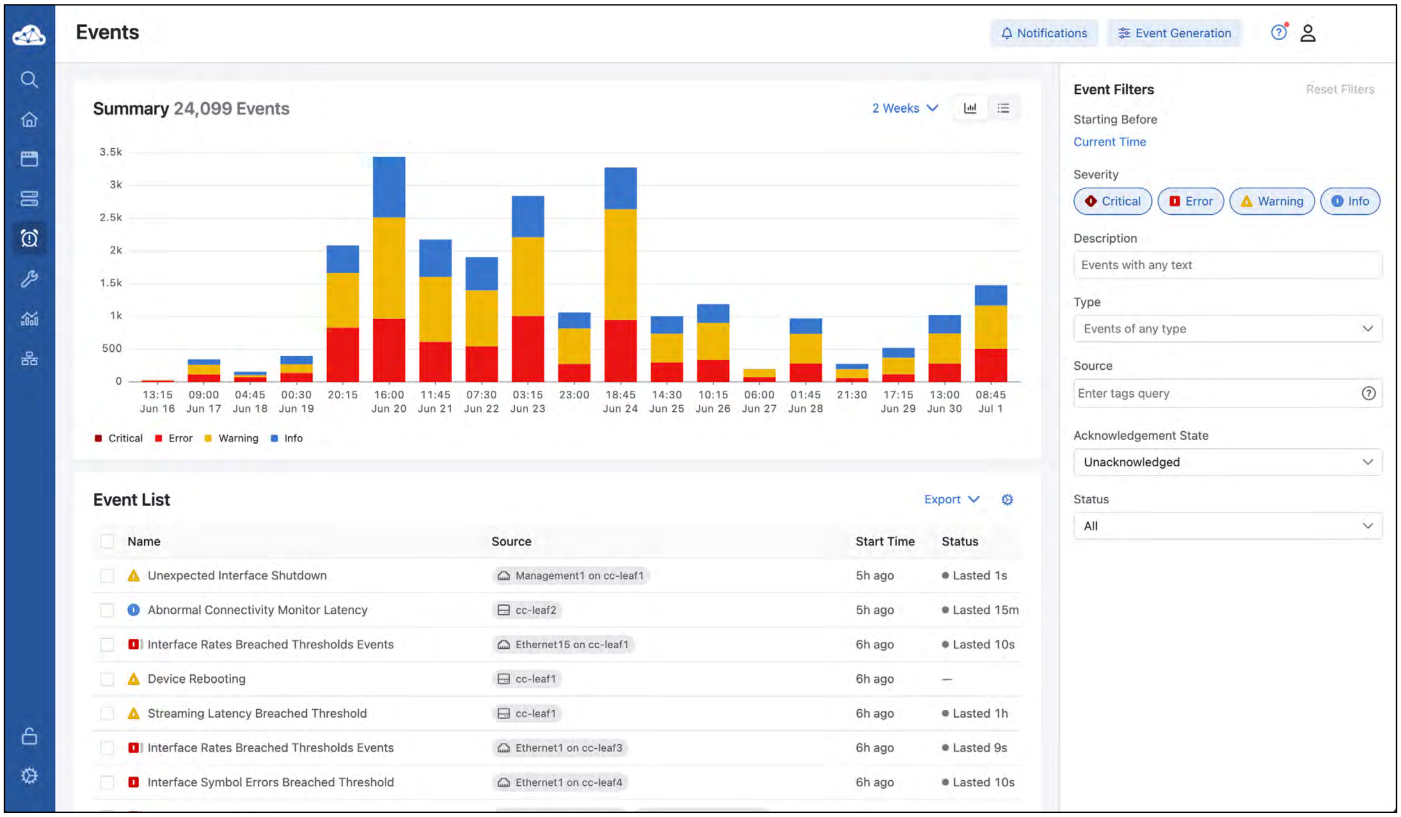
Figure 11: CloudVision Devices View

Finally the Devices view can also give insight to specific endpoints that are connected to the network. These end points are discovered through a variety of means and are all displayed within this Devices view.

Like other parts of the CloudVision portal UI, all device views include a selectable time window at the bottom of the screen enabling users to monitor these metrics in real-time or leverage the time-series state repository to view and compare state against historical points in time.

Events View

Events are created when one or more metrics in the state database reach certain criteria, as defined in the Analytics Engine. Events are categorized similarly to the Syslog model with varying levels of severity that can be used as a filter. The event store can also be searched by keyword. The unique aspect of the event view is the depth of correlated information that is offered, as compared to a typically 'thin' Syslog message. For example, a Syslog message for a drop counter only logs the event for a counter that has increased beyond a set threshold for an interface. This information is not sufficient to identify the root cause of the discards. Other metrics including traffic rate and buffer utilization are required to pinpoint the root cause. It is also key to acquire these metrics for the same time window during which the discards event occurred. The CloudVision event view presented for the interface discards event provides all pieces of the puzzle at the same point in time. This helps the operator identify whether, for example, the discards were a result of congestion. The correlated view is available for all such events generated for all monitored devices.



Summary 24,099 Events

Event List

	Name	Source	Start Time	Status
□	Unexpected Interface Shutdown	Management1 on cc-leaf1	5h ago	● Lasted 1s
□	Abnormal Connectivity Monitor Latency	cc-leaf2	5h ago	● Lasted 15m
□	Interface Rates Breached Thresholds Events	Ethernet15 on cc-leaf1	6h ago	● Lasted 10s
□	Device Rebooting	cc-leaf1	6h ago	—
□	Streaming Latency Breached Threshold	cc-leaf1	6h ago	● Lasted 1h
□	Interface Rates Breached Thresholds Events	Ethernet1 on cc-leaf3	6h ago	● Lasted 9s
□	Interface Symbol Errors Breached Threshold	Ethernet1 on cc-leaf4	6h ago	● Lasted 10s

Event Filters
Reset Filters

Starting Before
Current Time

Severity
Critical Error Warning Info

Description
Events with any text

Type
Events of any type

Source
Enter tags query

Acknowledgement State
Unacknowledged

Status
All

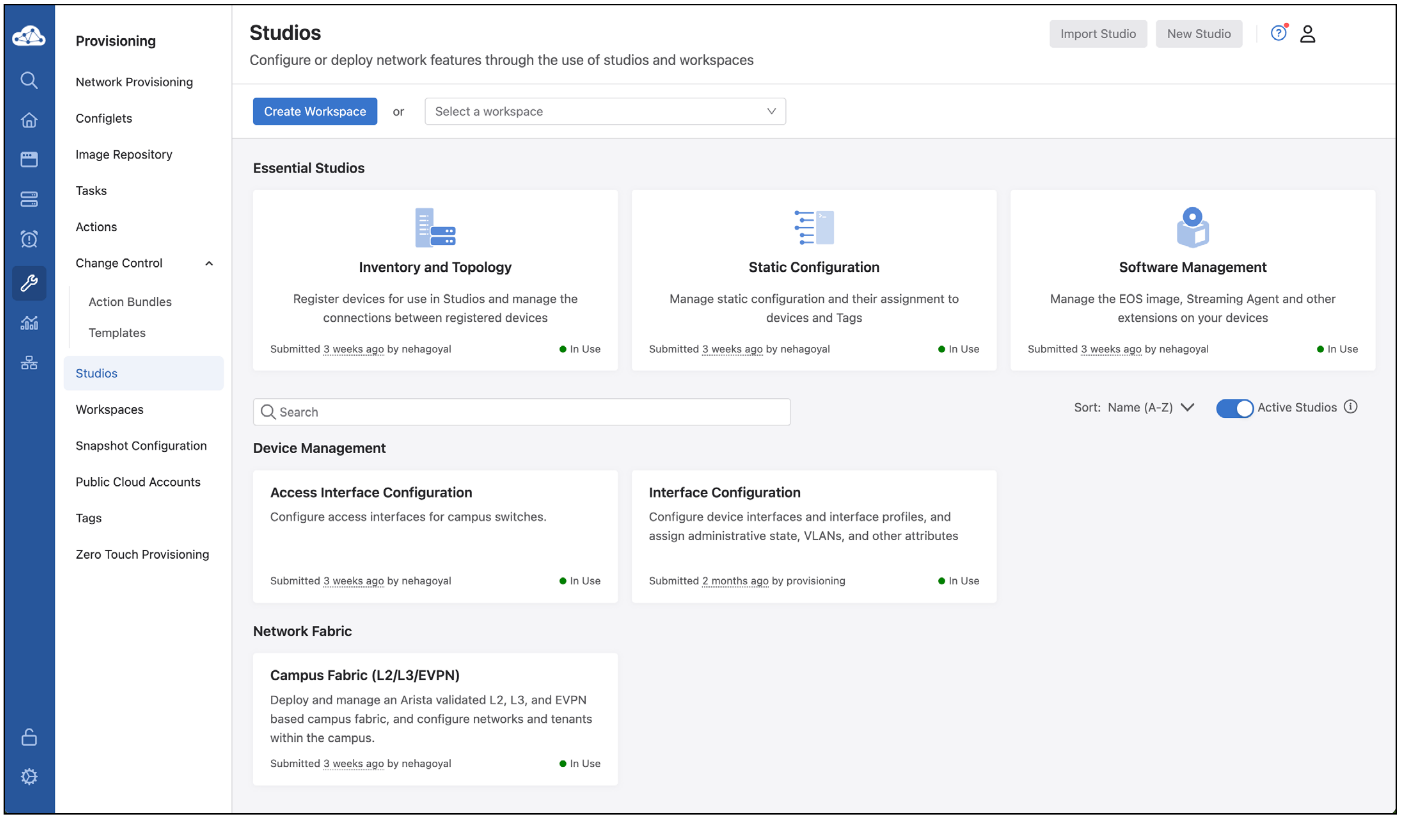
Figure 11: CloudVision Devices View

CloudVision supports the ability to configure and receive alerts for generated events. Operators can be alerted via email, chat-based services including Slack or Google Chat, and PagerDuty applications. Webhooks are available for custom alerting and monitoring requirements to integrate alerts into existing monitoring and incident management systems including centralized log servers, ServiceNow, or any web server-based application that can accept an HTTP POST notification. Webhooks also provide flexibility in performing actions in response to an event. For example, a CloudVision event can trigger a new incident ticket for a link down event, or close a tracked task for a software upgrade on the change of a device's EOS version.

Alert rules can be configured based on the event type, severity, and also per device to enable users to customize how they receive alerts from various devices. This capability helps raise visibility for specific events on critical devices.

Provisioning View

The Provisioning View houses all features and tools provided to perform comprehensive day-0, day-1, and day-2 tasks related to device and network-wide configuration. These tasks include everything from the pre-provisioning and bring-up of a complete network to performing configuration changes across a series of EOS-based devices.



Studios

Configure or deploy network features through the use of studios and workspaces

Essential Studios

Inventory and Topology

Register devices for use in Studios and manage the connections between registered devices

Submitted 3 weeks ago by nehagoyal ● In Use

Static Configuration

Manage static configuration and their assignment to devices and Tags

Submitted 3 weeks ago by nehagoyal ● In Use

Software Management

Manage the EOS image, Streaming Agent and other extensions on your devices

Submitted 3 weeks ago by nehagoyal ● In Use

Device Management

Access Interface Configuration

Configure access interfaces for campus switches.

Submitted 3 weeks ago by nehagoyal ● In Use

Interface Configuration

Configure device interfaces and interface profiles, and assign administrative state, VLANs, and other attributes

Submitted 2 months ago by provisioning ● In Use

Network Fabric

Campus Fabric (L2/L3/EVPN)

Deploy and manage an Arista validated L2, L3, and EVPN based campus fabric, and configure networks and tenants within the campus.

Submitted 3 weeks ago by nehagoyal ● In Use

Figure 13: CloudVision Provisioning View

At the heart of this view is the CloudVisions Studios feature set which provides an extensive ability to plan, design, and install various network configurations based on a set of preloaded highly flexible templates known as workflows without the need to write CLI code. By simply designating, or tagging devices based on their roles within a network, for example leaf or spine, configurations can be auto-generated from simple user-provided inputs within a configuration workflow.

CloudVision Studios provides many built-in workflows for many of the common configuration tasks including for initial data center or campus build-outs, adding incremental network capacity, and basic day-to-day required network changes. In addition, Studios can be created or customized for any feature set thereby avoiding the need to cut and paste CLI text into rigid templates or scripts.

Fancy writing specific CLI for one, some, or all the EOS-based devices within a network? This view also provides access to the Configlets facility. Configlets are snippets of CLI code that can be automatically installed in all or a subset of devices with a few simple clicks. Configlets enable the operator to create a standard set of CLI snippets for such services as AAA, NTP, and ACLs and then ensure they are consistently applied to each device within the network.

Another important feature that is accessible through this view is the Zero Touch Provisioning feature or ZTP. ZTP enables users to completely configure new devices added to the network without the need to connect a console to the device itself. One could actually build an entire network's worth of configuration even before the devices arrive on the loading dock and load this configuration into these new devices by simply cabling them and powering them up.

This view also provides access to the comprehensive change control services that are tied into all aspects of provisioning through CloudVision.

Dashboards View

This view highlights the power of a multi-domain, and multi-role capability of CloudVision. Users with different responsibilities can build customized or leverage built-in dashboards for monitoring a vast variety of metrics across specific groups of devices or interfaces. This enables the user to choose metrics and correlate them across the network for the same time window and quickly identify anomalies. Multiple dashboards can be created, each displaying a correlated set of metrics and devices tailored to monitor specific network happenings, perhaps even to keep a watchful eye on a past troublesome network event.

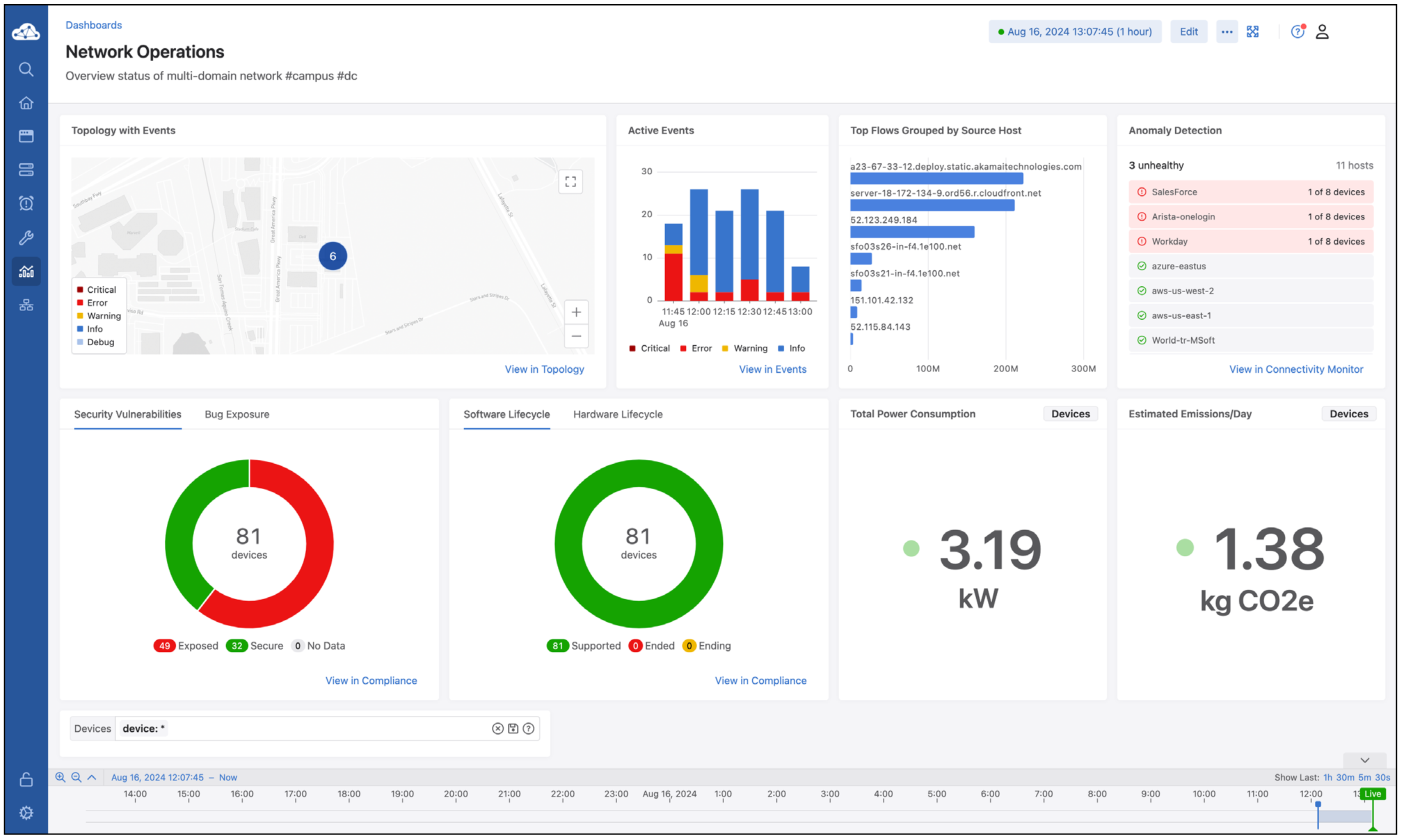


Figure 14: Sample CloudVision Dashboard

Leveraging Dashboard views, accessing the output of CLI commands across the network can be presented in one consolidated UI panel empowering the operator to identify anomalies quickly and decrease time to resolution. This view also aids with tracking compliance, flows, endpoints, top utilized interfaces, errors, and congestion across devices and interfaces in the network with just a few clicks.

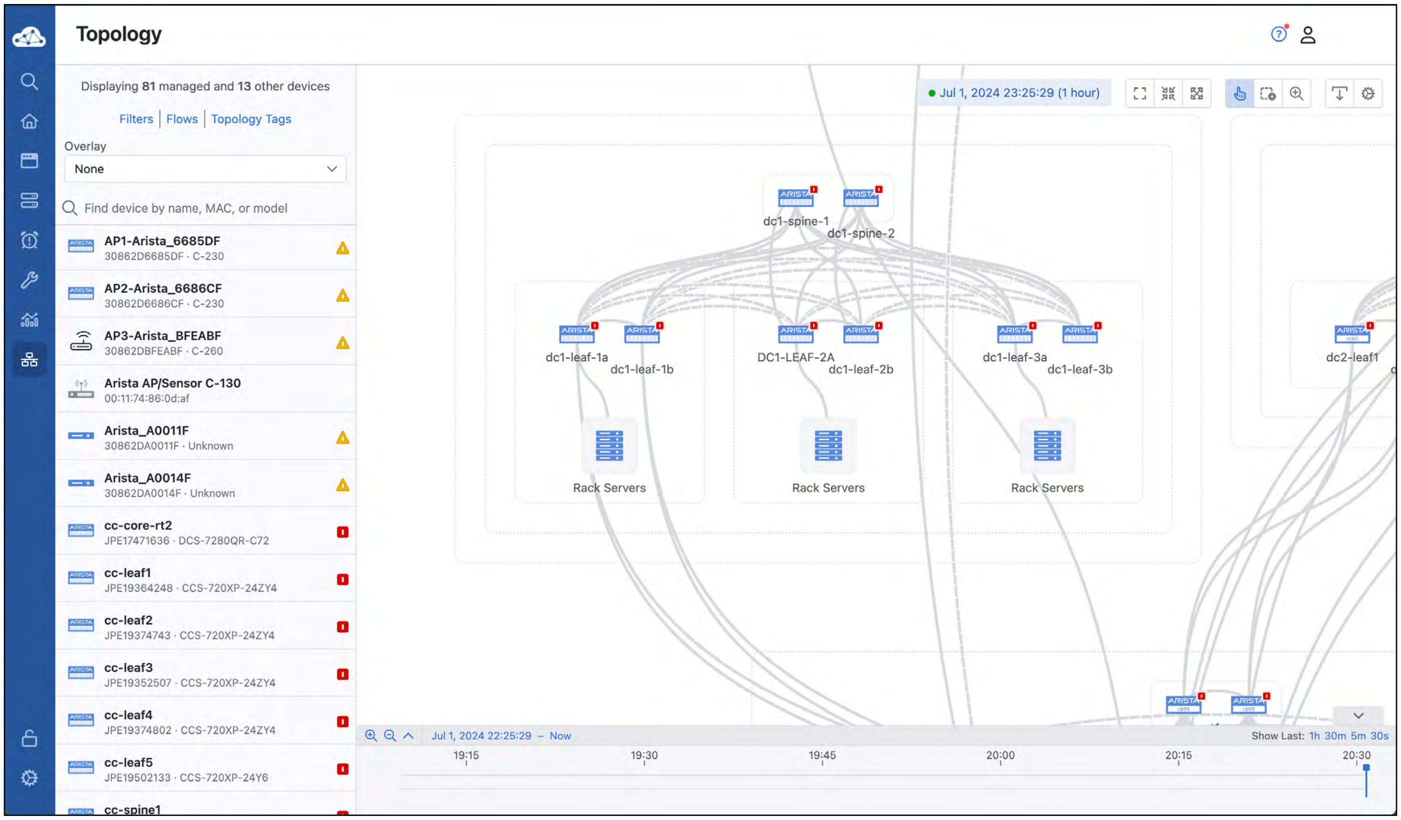
Another example of a customized dashboard is a dedicated AI Jobs dashboard that provides a unified view of network and AI job health metrics. It includes job completion times, congestion indicators (such as ECN-marked packets, PFC pause frames, and packet drops), buffer and link utilization, and real-time topology views of AI job flows—delivering actionable insights to maintain seamless, high-efficiency AI workload execution.

A powerful capability within Dashboards is the ability to add a specific active topology view into the dashboard. The topology view can even display real-time overlays including link utilization. The topology view can be configured to even display a subset of devices or those associated with a specific tag or role or pod within the network.

Topology View

CloudVision's Topology View is designed to visualize connected multi-domain network topologies into a common interface with live analytics and workflow task visibility.

The Topology View enables operators to visualize the network topology to understand how devices are interconnected and quickly identify hotspots in the network. CloudVision's Topology View provides an intuitive approach to mapping the network topology not just based on LLDP neighbors but also on analytics that automatically calculate device type such as leaf, spine, or endpoint, neighbor relationships, and common layouts. These layouts can be collapsed and expanded to reduce visual complexity and enable operators to visualize their network in a way that aligns with the network design.


Topology

Displaying 81 managed and 13 other devices

Overlay: None

Find device by name, MAC, or model

AP1-Arista_6685DF
30862D6685DF · C-230

AP2-Arista_6686CF
30862D6686CF · C-230

AP3-Arista_BFEABF
30862DBFEABF · C-260

Arista AP/Sensor C-130
00:11:74:86:0d:af

Arista_A0011F
30862DA0011F · Unknown

Arista_A0014F
30862DA0014F · Unknown

cc-core-rt2
JPE17471636 · DCS-7280QR-C72

cc-leaf1
JPE19364248 · CCS-720XP-24ZY4

cc-leaf2
JPE19374743 · CCS-720XP-24ZY4

cc-leaf3
JPE19352507 · CCS-720XP-24ZY4

cc-leaf4
JPE19374802 · CCS-720XP-24ZY4

cc-leaf5
JPE19502133 · CCS-720XP-24Y6

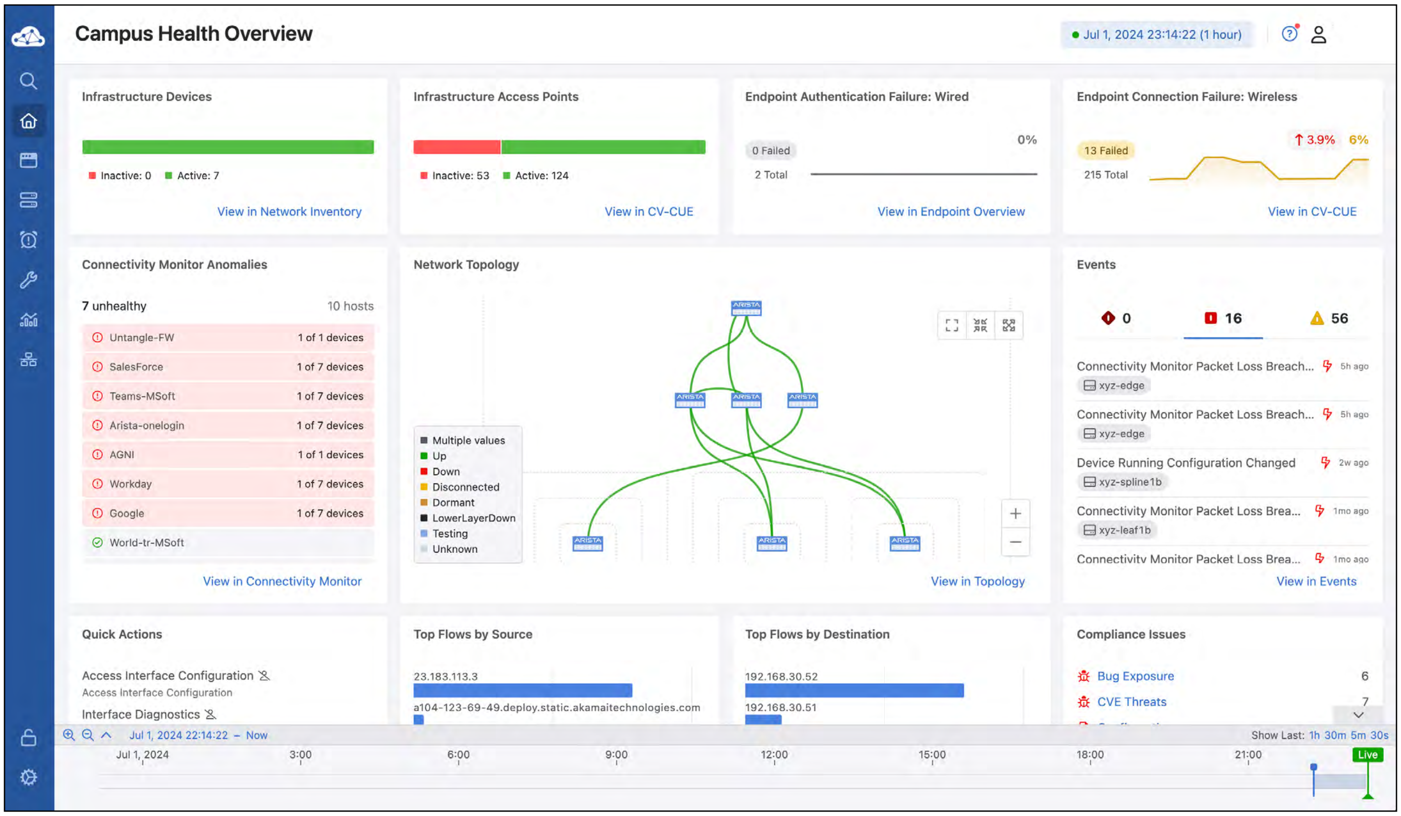
cc-spine1

Figure 15: CloudVision Topology View

The Topology View also enables users to overlay metrics on the presented network topology view. This enables operators to quickly identify problems such as network congestion and traffic imbalance from a network-wide perspective. Details including events, bandwidth, error/discard rates, network segments (VLAN and VXLAN), and network paths for traffic flows are displayed as optional layers on the topology. The timeline can be leveraged in Topology View to view the historical state for segmentation, flow, and link-level metrics.

Profile-Based Landing View

The view labeled Overview is a conditional view that is available when certain CloudVision features are enabled through a user's profile assignment. This view presents dashboards that are specialized to provide tools for specific feature sets. One such feature set is for Campus LAN management. When this feature set is enabled, the Overview View provides a tailored dashboard consisting of wired and wireless information such as device counts, events, compliance issues and even traffic flows.



Campus Health Overview

● Jul 1, 2024 23:14:22 (1 hour)

Infrastructure Devices

🟥 Inactive: 0 🟩 Active: 7

View in Network Inventory

Infrastructure Access Points

🟥 Inactive: 53 🟩 Active: 124

View in CV-CUE

Endpoint Authentication Failure: Wired

0 Failed
2 Total
0%

View in Endpoint Overview

Endpoint Connection Failure: Wireless

13 Failed
215 Total
↑ 3.9% 6%

View in CV-CUE

Connectivity Monitor Anomalies

7 unhealthy	10 hosts
Untangle-FW	1 of 1 devices
SalesForce	1 of 7 devices
Teams-MSoft	1 of 7 devices
Arista-onelogin	1 of 7 devices
AGNI	1 of 1 devices
Workday	1 of 7 devices
Google	1 of 7 devices
World-tr-MSoft	

View in Connectivity Monitor

Network Topology

View in Topology

Events

0 16 56

Connectivity Monitor Packet Loss Breach... 5h ago
xyz-edge

Connectivity Monitor Packet Loss Breach... 5h ago
xyz-edge

Device Running Configuration Changed 2w ago
xyz-spline1b

Connectivity Monitor Packet Loss Brea... 1mo ago
xyz-leaf1b

Connectivity Monitor Packet Loss Brea... 1mo ago

View in Events

Quick Actions

Access Interface Configuration
Access Interface Configuration
Interface Diagnostics

Top Flows by Source

23.183.113.3
a104-123-69-49.deploy.static.akamaitechnologies.com

Top Flows by Destination

192.168.30.52
192.168.30.51

Compliance Issues

Bug Exposure	6
CVE Threats	7

Jul 1, 2024 22:14:22 – Now

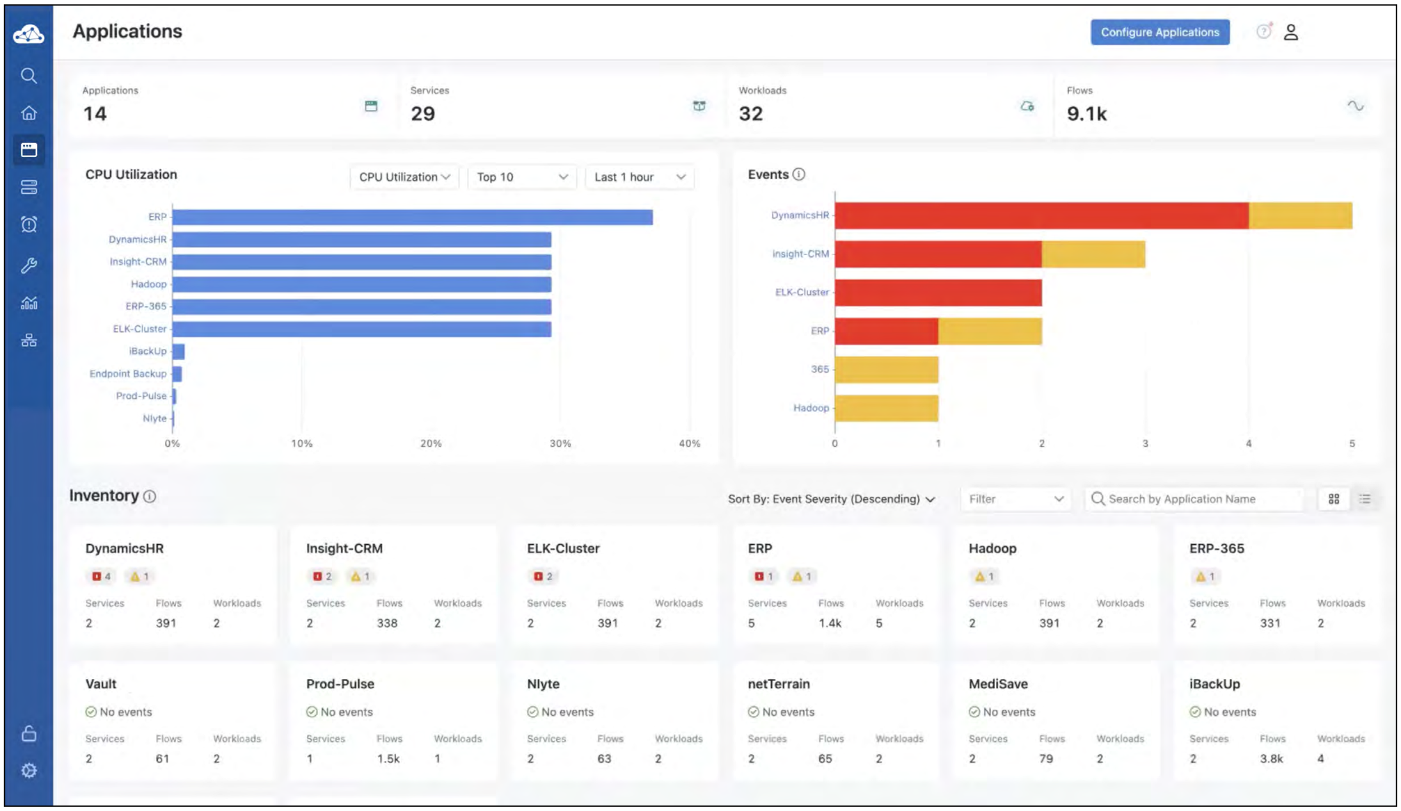
Show Last: 1h 30m 5m 30s

Figure 16: CloudVision Campus Overview View

Another use for the Overview View is when Arista's WAN Pathfinder feature set is enabled. In this scenario, the Overview View will display a tailored dashboard containing information related to the WAN Pathfinder service running with CloudVision.

Applications View

The Applications View within CloudVision is provided as part of CloudVision UNO or Unified Network Observability. CloudVision UNO is a network observability software offering that brings together network infrastructure performance and data from both network and compute resources to provide application and workload performance insights for data centers, campuses and wide-area networks. With UNO, CloudVision can now learn about compute resources attached to the network, including virtualized compute resources, and treat them as any other network node. Flows to and from these compute end points can be tracked and analyzed network-wide in addition to being viewable within the CloudVision topology.



Applications	Services	Workloads	Flows
14	29	32	9.1k

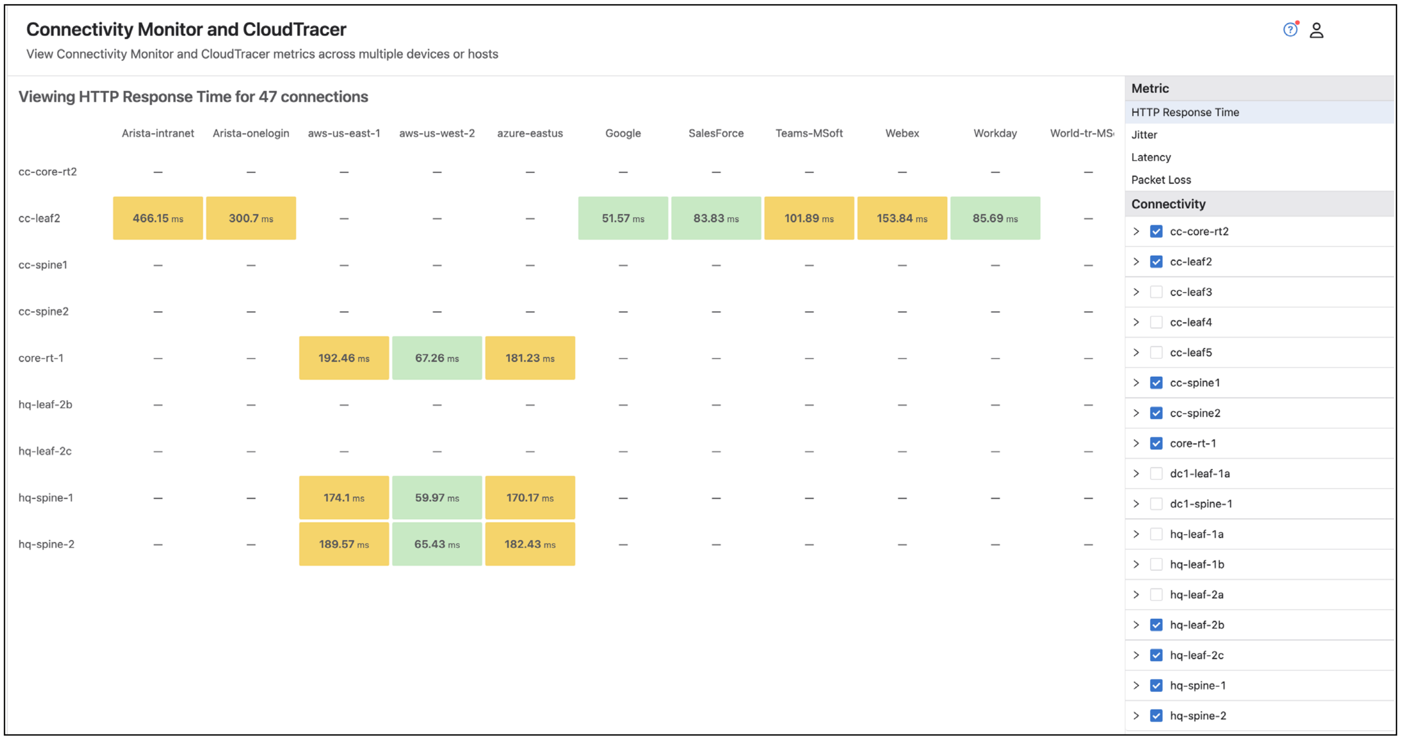
Application	Events	Services	Flows	Workloads
DynamicsHR	🟥 4 ⚠ 1	2	391	2
Insight-CRM	🟥 2 ⚠ 1	2	338	2
ELK-Cluster	🟥 2	2	391	2
ERP	🟥 1 ⚠ 1	5	1.4k	5
Hadoop	⚠ 1	2	391	2
ERP-365	⚠ 1	2	331	2
Vault	✓ No events	2	61	2
Prod-Pulse	✓ No events	1	1.5k	1
Nlyte	✓ No events	2	63	2
netTerrain	✓ No events	2	65	2
MediSave	✓ No events	2	79	2
iBackUp	✓ No events	2	3.8k	4

Figure 17: CloudVision Applications View (UNO)

Building the Network

CloudVision CloudTracer™ provides a view of reachability information to endpoints throughout an organization’s multi-domain network. Using active probe-based techniques, each EOS device is able to track connectivity and performance information to multiple target endpoints, including detecting actual packet loss, latency, jitter, and HTTP response time using the embedded EOS connectivity-monitor resource. With CloudTracer, the gathered connectivity and performance information is state information that is streamed to CloudVision’s central database for further analysis. The CloudTracer dashboard displays the EOS reachability information, based on both real-time as well as historical data.

While initially designed for the hybrid cloud use-case, the CloudTracer connectivity monitor can provide real-time reachability information across any network type and any network endpoint. This data is extremely valuable when combined with other time-series data to determine the cause of any changes in connectivity and performance and how applications and client experiences may have been affected.



Connectivity Monitor and CloudTracer

View Connectivity Monitor and CloudTracer metrics across multiple devices or hosts

Viewing HTTP Response Time for 47 connections

	Arista-intranet	Arista-onelogin	aws-us-east-1	aws-us-west-2	azure-eastus	Google	SalesForce	Teams-MSoft	Webex	Workday	World-tr-MS
cc-core-rt2	—	—	—	—	—	—	—	—	—	—	—
cc-leaf2	466.15 ms	300.7 ms	—	—	—	51.57 ms	83.83 ms	101.89 ms	153.84 ms	85.69 ms	—
cc-spine1	—	—	—	—	—	—	—	—	—	—	—
cc-spine2	—	—	—	—	—	—	—	—	—	—	—
core-rt-1	—	—	192.46 ms	67.26 ms	181.23 ms	—	—	—	—	—	—
hq-leaf-2b	—	—	—	—	—	—	—	—	—	—	—
hq-leaf-2c	—	—	—	—	—	—	—	—	—	—	—
hq-spine-1	—	—	174.1 ms	59.97 ms	170.17 ms	—	—	—	—	—	—
hq-spine-2	—	—	189.57 ms	65.43 ms	182.43 ms	—	—	—	—	—	—

Metric

HTTP Response Time

Jitter

Latency

Packet Loss

Connectivity

- > ☑ cc-core-rt2
- > ☑ cc-leaf2
- > □ cc-leaf3
- > □ cc-leaf4
- > □ cc-leaf5
- > ☑ cc-spine1
- > ☑ cc-spine2
- > ☑ core-rt-1
- > □ dc1-leaf-1a
- > □ dc1-spine-1
- > □ hq-leaf-1a
- > □ hq-leaf-1b
- > □ hq-leaf-2a
- > ☑ hq-leaf-2b
- > ☑ hq-leaf-2c
- > ☑ hq-spine-1
- > ☑ hq-spine-2

Figure 18: CloudTracer Connectivity Monitor

Network Automation

Building on the strength of the telemetry architecture, CloudVision is also a powerful platform for network provisioning. CloudVision Studios provides the tools needed for a fully automated network operations lifecycle, including building the initial network configurations, deployment, and ongoing operations.

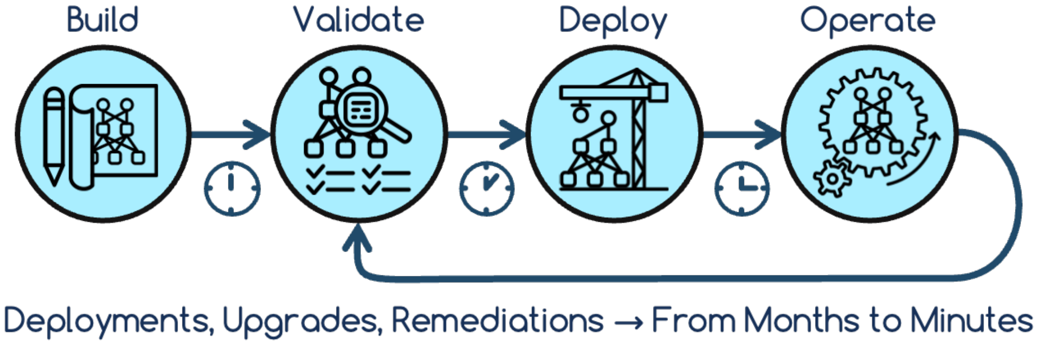

Build
Validate
Deploy
Operate
Deployments, Upgrades, Remediations → From Months to Minutes

Figure 19: Full Automation for the NetOps Lifecycle

Building the Network

Arista was one of the first in the networking industry to deliver Zero Touch Provisioning (ZTP). ZTP enables the operator to automatically provision a brand new EOS-based device with a machine-generated configuration and approved image without any human intervention. CloudVision enables administrators to not only deploy new switches in remote locations without requiring the device to be manually configured, but the installation of replacement devices can be handled the same way. Zero Touch Replacement (ZTR) enables a device that has failed to be decommissioned to inherit its configuration and settings and reprovisioned within the replacement device.

CloudVision Studios brings operational ease to provisioning with built-in point and click workflows that simplify the provisioning of Arista validated network designs ranging from complex EVPN setups to Pod deployments for the enterprise campus and data center. Using abstracted network data models, CloudVision Studios translates network designs to deployment by automating the creation and validation of configuration from day-0 provisioning to ongoing day-1 and day-2 tasks associated with network maintenance. CloudVision Studios also supports a no-code approach for easy customizations to these workflows and the ability to create new workflows with Studios for the advanced network administrators.

Validating and Deploying the Network

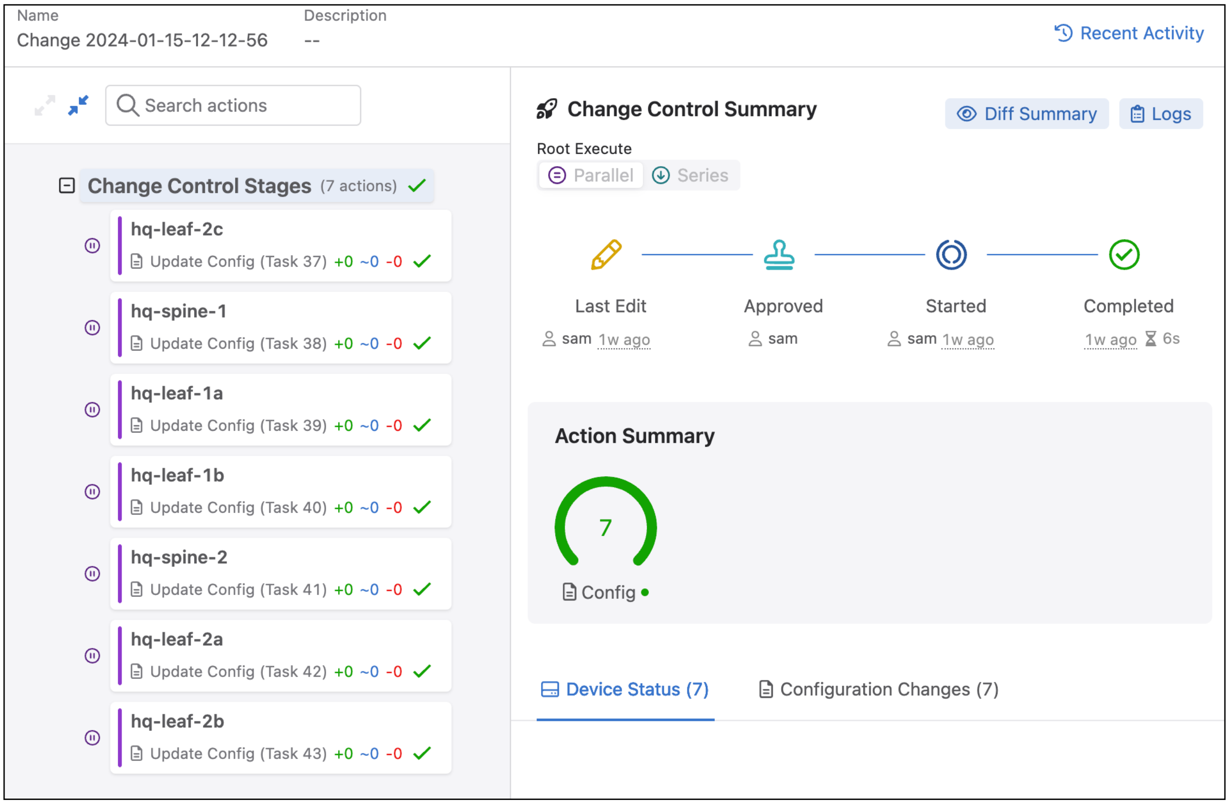
After device configurations are built, CloudVision Studios can validate the configurations and deploy the required changes to the production network. Customers can also integrate CloudVision Studios with 3rd party validation tools that can simulate the effect of configuration changes on the network using software modeling. Software modeling can be useful when networks are too large to efficiently simulate, or as an initial test before moving on to a fully simulated environment. These integrations can be made part of the configuration change control in CloudVision to ensure the proposed changes meet all the predefined tests before executing the change.

Once the configurations are validated and approved, CloudVision can then roll out the configurations through integrated network-wide change control workflows.

Using Change Controls

The change control capabilities of CloudVision bring a controlled and coordinated approach to changes made to the network, while maintaining a documented audit trail. To ensure minimum service disruption, changes made to the network are planned at length and heavily scrutinized in the change control process, often requiring prior lengthy approvals and testing cycles. An average enterprise network change control process can take many hours across several weekends. A series of manual, device-by-device processes are employed and tend to be complicated and error-prone. Automated change control reduces this time dramatically resulting in significant operational savings.

CloudVision's Change Control workflow provides a facility for an operator to orchestrate these otherwise manual steps into an automated workflow. Individual device tasks are grouped into a change control that allows for scheduling, stage-based sequencing, redundancy modal awareness, pre-snapshot and post-snapshots, and notification processing.



Name: Change 2024-01-15-12-12-56
Description: --

Change Control Stages (7 actions) ✓

- hq-leaf-2c — Update Config (Task 37) +0 ~0 -0 ✓
- hq-spine-1 — Update Config (Task 38) +0 ~0 -0 ✓
- hq-leaf-1a — Update Config (Task 39) +0 ~0 -0 ✓
- hq-leaf-1b — Update Config (Task 40) +0 ~0 -0 ✓
- hq-spine-2 — Update Config (Task 41) +0 ~0 -0 ✓
- hq-leaf-2a — Update Config (Task 42) +0 ~0 -0 ✓
- hq-leaf-2b — Update Config (Task 43) +0 ~0 -0 ✓

Change Control Summary

Root Execute: Parallel | Series

Last Edit	Approved	Started	Completed
sam 1w ago	sam	sam 1w ago	1w ago 6s

Action Summary

7 Config ●

Device Status (7) | Configuration Changes (7)

Figure 20: CloudVision Change Control

The modal awareness includes procedures for upgrades to MLAG switch pairs as well as a mode to upgrade spine switches by bringing them gracefully out and back into service through BGP maintenance mode.

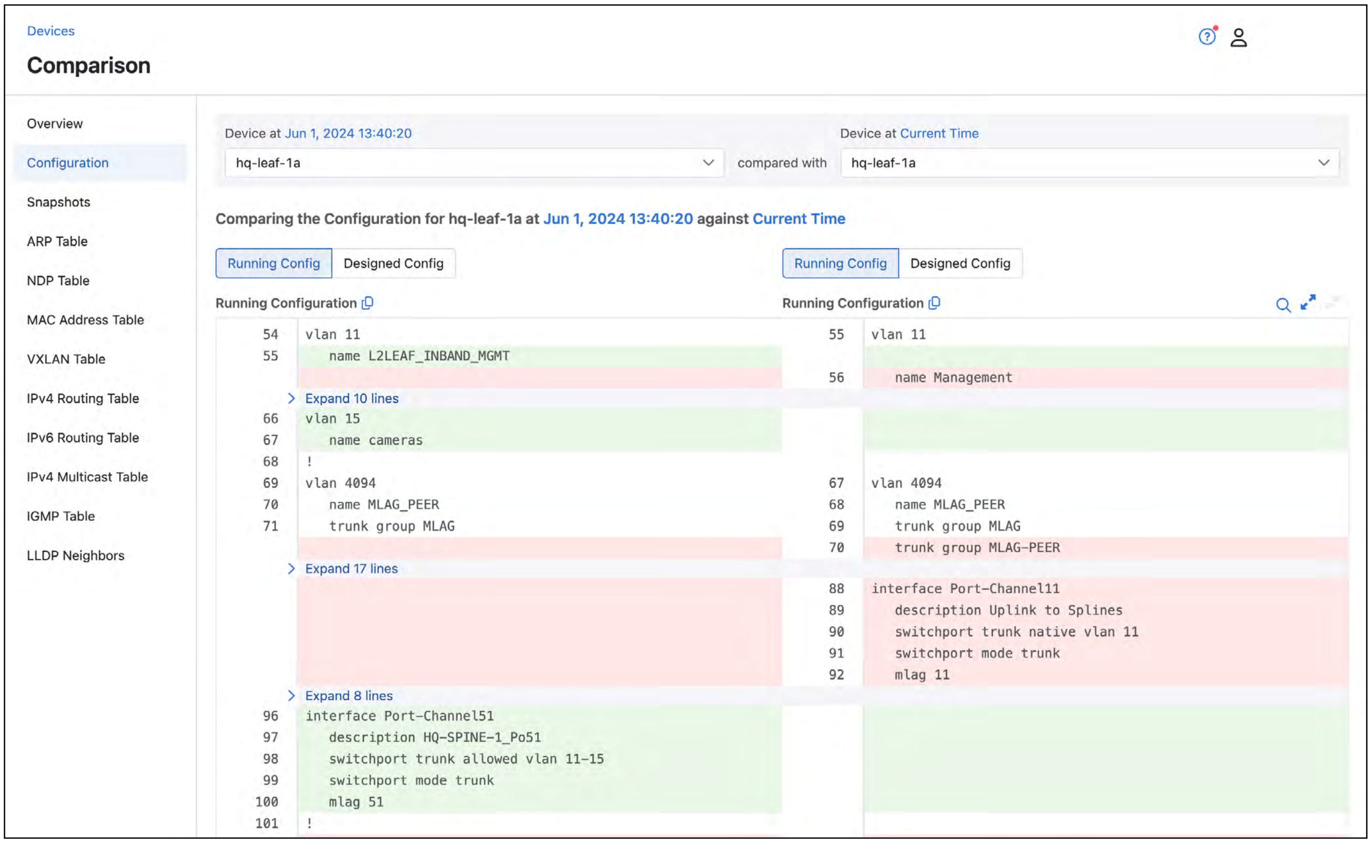
Once the change control is created, the operator must go through a review and approval step before the change can be executed. Each of these steps is tied into CloudVision's Roles Based Access Control (RBAC) system so that different authority levels can be applied to each step. A strict non-author review model can also be enforced for change control approvals. All of these capabilities work together to ensure that network changes proceed without impacting network operation.

Viewing Device Comparisons

Network operators typically request change control windows to perform changes to the network outside of production hours. At the start of the control window, the operator will perform pre-change control procedures including capturing various device state information using a number of CLI show commands. These scripts may be run on a single device on a larger set of devices depending on the size of the change. Once the change has been completed, the operator will likely re-run the same scripts to ensure the delta is as expected. The only way to ensure this delta is accurate is if the operator were to manually compare the pre-change & post-change information. Depending on the device or the complexity of the change, verifying the change manually can take a significant amount of time.

CloudVision's architecture of real-time state capture provides a better way to identify these state changes because it can identify the changes as they happen in real-time. When this data is captured over time, it can be used to track changes in key device metrics or review state before and after configuration changes and to facilitate network-wide rollback if necessary. Continuous snapshots and Diff Views are key features that leverage the historical state database to automatically track state changes and present comparison views that highlight the changes in device state.

The concept of comparing device outputs from different points in time has traditionally formed the basis for identifying changes in the network and is often the first step in network troubleshooting, at a significant time cost. CloudVision's historical state repository and analytics framework automatically tracks changes from a baseline and summarizes the changes based on key metrics indicative of normal operation. Diff views provide an easy-to-read view that clearly visualizes the differences between the data sets at the device level. The views offer a user-friendly way to identify exactly what entries were removed and added between the two points in time for a given metric or configuration making it easy for network operators to focus on the changes.



Device at Jun 1, 2024 13:40:20: hq-leaf-1a compared with Device at Current Time: hq-leaf-1a

Comparing the Configuration for hq-leaf-1a at Jun 1, 2024 13:40:20 against Current Time

Running Configuration

```
vlan 11
   name L2LEAF_INBAND_MGMT
vlan 15
   name cameras
!
vlan 4094
   name MLAG_PEER
   trunk group MLAG
interface Port-Channel51
   description HQ-SPINE-1_Po51
   switchport trunk allowed vlan 11-15
   switchport mode trunk
   mlag 51
!
```

Running Configuration

```
vlan 11
   name Management
vlan 4094
   name MLAG_PEER
   trunk group MLAG
   trunk group MLAG-PEER
interface Port-Channel11
   description Uplink to Splines
   switchport trunk native vlan 11
   switchport mode trunk
   mlag 11
```

Figure 21: CloudVision 'Diff Views' Example

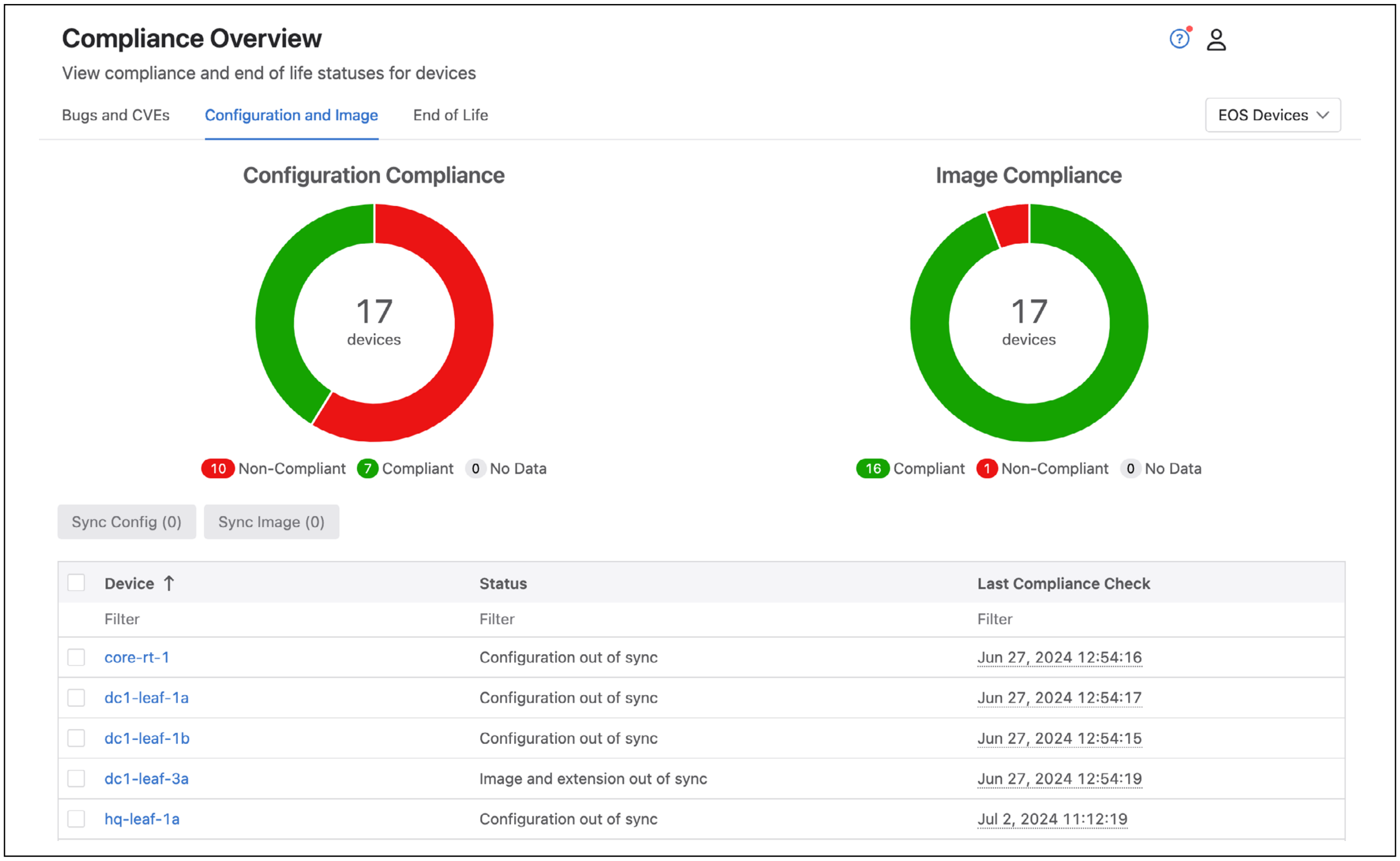
Network Rollback

All enterprise networks use maintenance windows to make changes to the network. However, when a maintenance window or change occurs, there may be a need to roll back to a previous configuration for unforeseen reasons. CloudVision offers this capability using network rollback.

One issue with traditional network operating systems is the inability to easily move between different versions of code, or configuration. Operators in the past have used text files or spreadsheets in order to conduct their maintenance windows. CloudVision now offers an easier approach; leveraging CloudVision's state database enables quick changes between two different states on one, some, or all devices in the network.

Risk Management with Compliance Checking

Arista's Compliance Dashboard provides a comprehensive view of the current state of the infrastructure as it relates to security advisories, NIST Common Vulnerabilities and Exposures, and enterprise-wide security and operational standards. This information is updated in real-time as new vulnerabilities are released. This enables a clear measurement of environmental risk and the ability to rapidly implement compensating controls and patches through the CloudVision upgrade workflow in a manner that minimizes or altogether eliminates any outage.



Compliance Overview

View compliance and end of life statuses for devices

	Device ↑	Status	Last Compliance Check
	Filter	Filter	Filter
□	core-rt-1	Configuration out of sync	Jun 27, 2024 12:54:16
□	dc1-leaf-1a	Configuration out of sync	Jun 27, 2024 12:54:17
□	dc1-leaf-1b	Configuration out of sync	Jun 27, 2024 12:54:15
□	dc1-leaf-3a	Image and extension out of sync	Jun 27, 2024 12:54:19
□	hq-leaf-1a	Configuration out of sync	Jul 2, 2024 11:12:19

Figure 22: CloudVision's Compliance Dashboard

The dashboard also shows a summary of known high severity software defects (software bugs) that affect managed devices. The assessment uses bug details published on www.arista.com and leverages the network-wide database to compute the exposure based not just on hardware and software versions but also on the real-time state of configuration and operating conditions. CloudVision has the ability to retrieve the latest information on known software defects through updates from arista.com hence enabling operators to leverage this information in making network-wide software upgrade and patch rollout decisions.

CloudVision Extensibility and Integrations

CloudVision is an open and extensible platform that can integrate with third-party systems and devices, both northbound and southbound. By leveraging well-defined REST APIs, customers and partners can further integrate CloudVision into their existing infrastructure and their own internally sourced management platforms.

CloudVision APIs

CloudVision's architecture uses standardized OpenConfig data models, where available, as the basis for exposing CloudVision's aggregated NetDL state and telemetry data. CloudVision APIs provide a programmatic method to access CloudVision's network-wide provisioning data models for custom automation, extensibility, and integrations.

Within the CloudVision platform, an API Gateway sits between a client and a collection of backend services, providing authentication, access control and request routing. It acts as a reverse proxy to accept all application programming interface (API) calls, securely access and aggregate the various services required to fulfill them, and return the appropriate results.

CloudVision APIs are state based, resource-oriented APIs modeled in Protobuf and accessed over gRPC using a standardized set of RPC verbs or via REST. Bi-directional information can also be exchanged with CloudVision through WebSockets, which is particularly useful for web-based application development. Functionality is defined in a data-oriented (rather than action-oriented) form.

The APIs are documented on an Arista Github page, here: https://aristanetworks.github.io/cloudvision-apis/

CloudVision Integrations

CloudVision can send notifications to a number of 3rd party notification receivers when events are triggered. This includes an option for webhooks to trigger notifications to generic applications. Supported notification endpoints include e-mail, VictorOps, PagerDuty, OpsGenie, Slack, Google Chat, Microsoft Teams Chat, and Webhooks.

CloudVision API Gateway and SDK also provide a platform for integration with IT Service Management (ITSM), and IT Operations Management (ITOM), and Artificial Intelligence for IT Operations (AIOps). They provide the ability to integrate with other orchestration and operations management workflows.

An example of this is how CloudVision integrates with ServiceNow to enable task and device-related information to flow freely between the two applications. With this integration, change requests are created in ServiceNow for every task created in CloudVision, and task execution takes place on approval of the change request in ServiceNow.

CloudVision can also play a significant role in DevOps automation. By interfacing with the CloudVision northbound API, DevOps modules like Ansible enable administrators to generate network configuration changes through CloudVision using their DevOps platform of choice. This enables standard DevOps workflows that manage compute and storage to manage networking, while still gaining all the additional benefits of CloudVision for monitoring, visibility, compliance, and change control.

In addition, CloudVision can be integrated with IPAM tools such as Bluecatt and Infoblox providing programmatic allocation of IP addresses in CloudVision Studios, pulling information from a single source of truth.

Multi-Domain Segmentation

CloudVision plays a role in Arista's broader Zero Trust Security architecture through the Macro-Segmentation Services (MSS) functionality. With MSS, CloudVision serves as an integration point to orchestrate Zero Trust Security policy, with support for strong network security enforcement techniques on a multi-domain basis. Please review this white paper for more information on Arista's Zero Trust Security.

Summary

Every CIO is driving a spending shift from traditional IT operations to innovations that meet business needs more quickly. The only way to obtain the substantial OpEx cost reductions required to remain competitive is to automate their network environments.

Traditionally, approaches have been shackled in working with closed or limited network operating systems. This seriously restricts the ability of an organization to be agile and flexible as the application requirements change quickly. This also provides an opportunity for network operations teams to manage a multi-domain network infrastructure without using any of the historic, error-prone methods (CLI, API, scripts).

Arista CloudVision is built on an innovative network-wide state database architecture and is for cloud-like operations. With a focus on simplified provisioning, configuration, image management, troubleshooting, visibility, security, and 3rd party integration, CloudVision provides the platform to allow any organization to reduce OpEx costs by running their network based on cloud principles.

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office
1390 Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A , 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062

Copyright © 2025 Arista Networks, Inc. All rights reserved. ARISTA, AGNI, AVA, CloudVision, EOS, Etherlink, MSS, and NetDL are among the registered and unregistered trademarks and Arista Networks is a trademark of Arista Networks, Inc. All other company names are trademarks of their respective holders. Information in this document is subject to change without notice. Certain features may not yet be available. Arista Networks, Inc. assumes no responsibility for any errors that may appear in this document.

March 12, 2025   02-0051-08