White Paper

Arista CloudVision®: Cloud Automation for Everyone

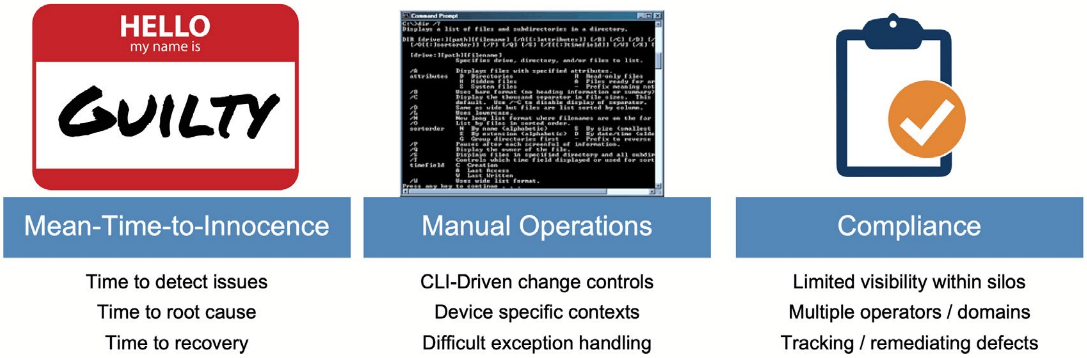
Table of contents

Table of contents

Introduction

In network operations circles, there is an old adage that the network is always guilty, until "proven innocent". By touching all infrastructure components - compute, storage, virtualization, apps, users, WAN, LAN, etc. - it is clear that the network plays a fundamental role in all IT operations. With such a broad scope, the network is the service that is expected to always work, and when an IT issue happens, the network is almost always suspected to be at fault.

Network operations teams are counted upon to manage availability, security, agility, costs, and risks. To do so, they need processes and tools that enable them to employ efficient and repeatable workflows with continuous visibility and observability. The approach that they take to do their daily jobs has to allow them to control and monitor their networks, make changes without disruption, and deploy new sites quickly and reliably.



```
C:\>dir /?
Displays a list of files and subdirectories in a directory.

DIR [drive:][path][filename] [/A[[:]attributes]] [/B] [/C] [/D] [/
  [/O[[:]sortorder]] [/P] [/Q] [/S] [/T[[:]timefield]] [/W] [/X] [

  [drive:][path][filename]
              Specifies drive, directory, and/or files to list.

  /A          Displays files with specified attributes.
  attributes   D  Directories                R  Read-only files
               H  Hidden files               A  Files ready for ar
               S  System files               -  Prefix meaning not
  /B          Uses bare format (no heading information or summary)
  /C          Display the thousand separator in file sizes.  This
              default.  Use /-C to disable display of separator.
  /D          Same as wide but files are list sorted by column.
  /L          Uses lowercase.
  /N          New long list format where filenames are on the far
  /O          List by files in sorted order.
  sortorder    N  By name (alphabetic)       S  By size (smallest
               E  By extension (alphabetic)  D  By date/time (olde
               G  Group directories first    -  Prefix to reverse
  /P          Pauses after each screenful of information.
  /Q          Display the owner of the file.
  /S          Displays files in specified directory and all subdir
  /T          Controls which time field displayed or used for sort
  timefield   C  Creation
              A  Last Access
              W  Last Written
  /W          Uses wide list format.
Press any key to continue . . .
```

Figure 1: Challenges for Network Operations

However, the traditional approaches to monitoring and managing networks have failed to keep up with today's cloud networking era. Today's network operations and engineering teams are challenged across a wide number of areas, including planning, site deployment and upgrades, day-to-day operations, troubleshooting, and compliance management. As human error remains a primary cause of observed network issues, new software-driven approaches are needed to enable automation in network operations and improve both reliability and mean-time-to-innocence.

Cloud Principles for Enterprise Network Operations

Over the past decade, Arista has been delivering cloud networking solutions with a unique software-driven approach to building reliable networks designed around the principles of standardization, simplification, cost-savings, and automation. We coined the term "cloud networking" to characterize the evolved approach and architecture which addresses these principles, while we worked closely with the largest hyper-scale cloud operators on their journeys.

Cloud operators pioneered new principles for scale-out designs and software-first thinking because the scale of operational and technical challenges that they faced in all aspects of their businesses could not be surmounted the old way. These cloud principles modernized networking for hyper-scale networks with simplified designs using standards-based protocols, open scale-out IP fabric designs, and software-driven orchestration to help them scale operations with minimal resources.

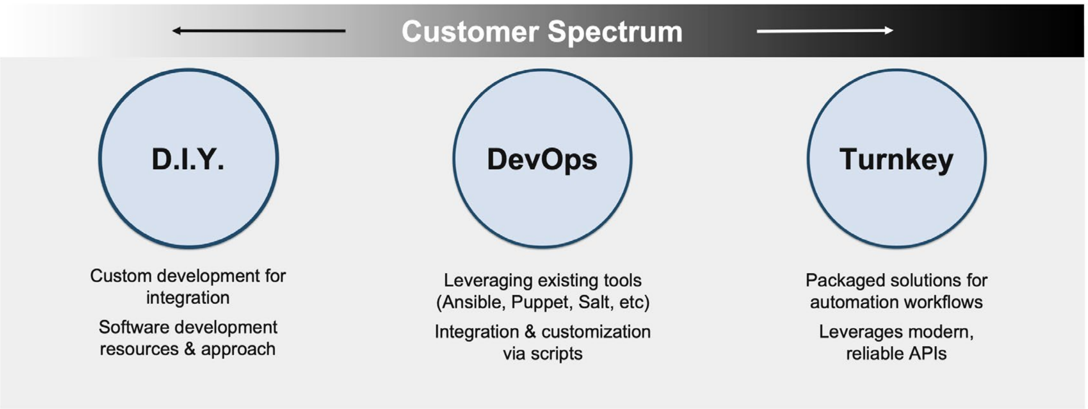
Just as hyper-scale cloud operators set an example with network automation to simplify time-consuming and error-prone tasks, and to separate the human factor that made continuous hyper-scale operations risky – these principles can now help enterprise customers with exceptional improvements in reliability, efficiency, and cost savings.

Enterprises that want to embark on this journey to cloud networking are often challenged with breaking away from the traditional network operation models, and will follow some common decision points and success factors to plan their path:

1. **Build vs. buying.** While hyper-scale cloud operators drove much of the new technologies and systems that they used to build their infrastructure, most enterprises do not have the time, skillset, or resources to build out their own homegrown cloud automation platform. However, these innovations can drastically improve network operations for everyone. Therefore, enterprises are looking for a modern, consistent NetOps platform that is also turnkey and provides the same benefits.
2. **Choosing a modern architecture.** Cloud network operations cannot be built on network management tools that are decades old (e.g. SNMP polling, screen-scraping, manual cut-and-paste configuration). Modern network architectures require a system approach with real-time automation, using open state-streaming APIs for continuous real-time synchronization of network state and configuration, and providing advanced AI/ML analytics to provide instantaneous compliance, visibility, and troubleshooting.
3. **Breaking down silos.** Traditional enterprise networks have often been deployed by selecting a different 'box' for each "place-in-the-network" (PIN). With each box comes a different operating system, with different design limitations and features, different APIs, and different management apps. The selection of platforms with the greatest commonality, across the widest aperture, provides an alternative to disparate places-in-the-network thinking, as does the selection of standard approaches to management plane communications.

Different Approaches for Different Enterprises

As decisions about how to approach network modernization with a software automation model are considered, each customer will have different options to consider. Various approaches exist and are not mutually exclusive. Fundamentally, there are several common approaches to network modernization for the enterprise customer, with the primary approaches summarized as follows:



Customer Spectrum
D.I.Y.
DevOps
Turnkey
Custom development for integration
Software development resources & approach
Leveraging existing tools (Ansible, Puppet, Salt, etc)
Integration & customization via scripts
Packaged solutions for automation workflows
Leverages modern, reliable APIs

Figure 2: Arista supports a variety of approaches to network automation

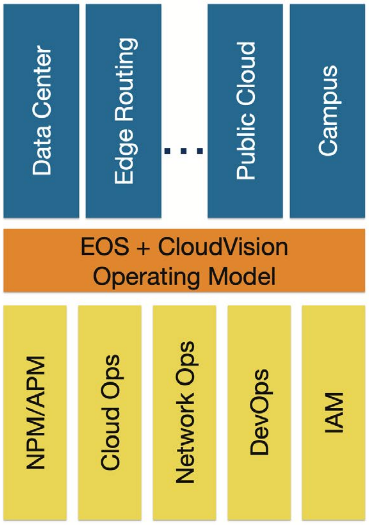
- **Do-It-Yourself (D.I.Y.) Automation.** DIY solutions are typically deployed by hyper-scale cloud operators, such as Microsoft or Facebook, who are building massive public infrastructures at scale exceeding 100's-1,000's of times those of the typical large enterprise. For them, automation is fundamental to their business model as a means to remain competitive. With many specialized in-house applications and services designed to account for infrastructure failure, they employ large software teams to automate their entire estate. Arista helps such customers by providing open tools like EOS SDK, Openconfig / gRPC agents, streaming telemetry, and eAPI device programmability. With unrestricted programmability of the EOS Linux software infrastructure, these customers are able to fully integrate EOS-based switches into their broader software orchestration systems.

- **DevOps CI/CD Model.** This model is typically deployed by relatively large service providers or enterprises, as they embark on an automation journey. Their approach includes using automation frameworks – typically also being used by the DevOps compute and platform operations teams – such as Hashicorp Terraform or Red Hat Ansible to automate the provisioning of the network infrastructure and to drive down OpEx costs. These customers have the resources and skills to write their own custom scripts and are invested in DevOps automation approaches with committed resources. Arista supports these customers by providing open software integration into DevOps frameworks like Terraform, Ansible, Puppet, and Chef, as well as supporting streaming receiver platforms like ELK stack, Prometheus, and others.
- **Turnkey solution.** There are few tools that exist today to guide customers down a path to successful network automation, and fewer still for customers that do not have the time, skills, or resources to build a custom approach. CloudVision provides a turnkey solution for all customers, allowing customers to provision, manage and observe their infrastructure while still 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 the cloud providers.

A Single Platform with Universal Applicability

Arista's Extensible Operating System (EOS®) and CloudVision® are designed with universality and applicability in mind. Designed around cloud principles, these systems provide a platform based on a software-driven model for turnkey network automation across multiple network domains, which normalizes disparate places in the network with a uniform software operating model.

With CloudVision, this software approach is not just for the data center or for hyper-scale operators. A common approach for automated provisioning and real-time visibility can now apply to the campus, the hybrid cloud, and the routed interconnect, as well.



Operations teams can implement a single operating model and runbook for:

- Upgrade procedures
- Certification efforts
- Lifecycle management
- Vulnerability management
- Network designs
- Troubleshooting approaches
- Automation techniques
- Feature discrepancies
- Management platforms
- Ecosystem integration
- And more…

Figure 3: Benefits of a Consistent Operations Model

With Arista EOS and CloudVision, operators don't need to re-invent different approaches for each network domain. In fact, there is a significant benefit to consolidating network operations using a single uniform approach for every place-in-the-cloud (PIC) vs. legacy approaches that only address one place-in-the-network (PIN).

Legacy PIN approaches create network silos with different architectures, operating systems, limitations, and management tools thus ultimately increasing the cost and complexity of managing the entire enterprise network. What's more, centrally securing and automating the operation of disparate PINs becomes virtually impossible. In contrast, Arista's modern and consistent PIC approach provides operational consistency in multi-domain enterprise networks.

CloudVision Overview

CloudVision is a modern, multi-domain network management platform built on cloud networking principles for telemetry, analytics, and automation. Designed for use in data centers, wired and wireless workspaces, multi-cloud, and WAN routing use-cases, CloudVision provides a consistent operational model across domains, helping enterprises to simplify network operations by breaking down traditional network management silos. It provides a single unified management plane with open APIs for extensibility.

It provides a single management platform for enterprise networks with:

- multi-domain consistency
- zero-touch automation
- cognitive analytics with machine learning, and
- an ecosystem of partner value-added integrations

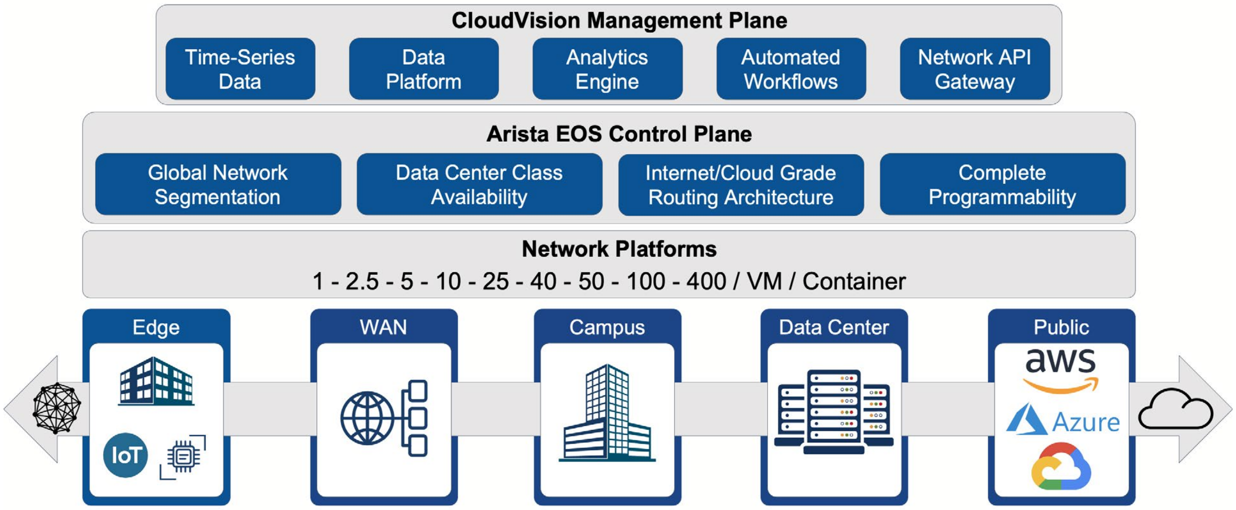


Figure 4: Consistent Approach for Every Place-in-the-Cloud

Unlike niche management products designed for a narrow use-case; CloudVision is a scalable multi-domain platform providing rich functionality that is useful across the entire enterprise, and yet provides leadership domain-specific features.

CloudVision as-a-Service or On-premises

CloudVision is now available as either 1) a software platform that is deployed on-premises as a virtual or physical appliance, or 2) as a fully managed cloud-service offering called *CloudVision as-a-Service*. CloudVision as-a-Service provides an equivalent user experience to the CloudVision on-premises offering, including the same user interfaces and applications, network database, APIs, and partner integrations - all with nothing to set up or manage on-premises.

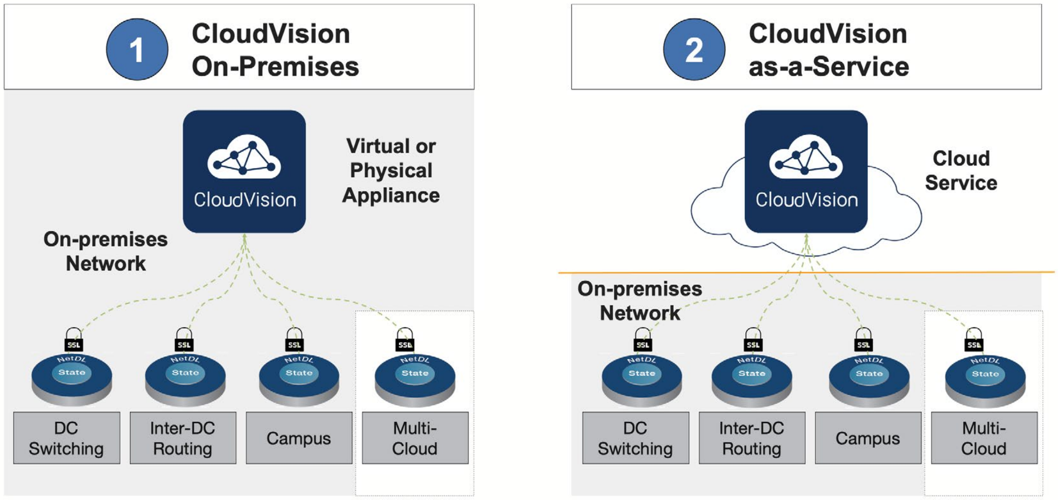


Figure 5: CloudVision Consumption Models

The managed as-a-Service option is operated, scaled and maintained by dedicated Arista site reliability engineers on a proven and secure tier-1 public cloud platform. It can eliminate the need for long hardware acquisition and approval cycles and offload compute/storage upgrades from the list of burdens faced by network operations teams.

CloudVision as-a-Service simplifies network upgrades, allowing IT teams to focus on the needs of their end-customers and not on managing their network-management tools. Advantages of the as-a-Service option include:

- Supports deployment of physical switches, virtualized EOS software instances running in the public cloud and remote sites, containerized EOS routers running in Kubernetes clusters, EOS images running on white boxes, and Arista WiFi access points.
- Provides error-free onboarding of new devices with Zero Touch Provisioning (ZTP) for faster time-to-value and for rapid site/cloud availability and upgrade.
- 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.
- Safe and secure with end-to-end data encryption for protection of data-at-rest and data-in-transit, rigorous operational controls, and security hardening and testing.
- Seamless with delegated multi-factor authentication and role assignment with a choice of customer-selected identity services such as Microsoft Azure Active Directory, Google Identity Service, Okta, One Login, and others.
- Supports the popular CloudVision third-party integrations and applications, including ServiceNow, Ansible, Terraform, Macro Segmentation Service and others.

Getting started with the managed-service is as simple as configuring the IP address of the service-tenant cluster in EOS devices and gaining immediate 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 CloudVision as-a-Service has a number of unique advantages, the choice of on-premises or cloud consumption is left to the user and will provide fundamentally the same capabilities.

Summary of CloudVision's Advantage

The CloudVision platform is a modern construct – 100% streaming-based, with no legacy SNMP polling or MIB limitations – for a more granular and complete centralized view. CloudVision uses the state-streaming design to focus on three key pillars of functionality:

- **Telemetry and Analytics.** Based on this native state-streaming for real-time and historical visibility into network state, incoming telemetry is constantly processed and evaluated with AI/ML capabilities to identify anomalies and provide extensive observability for the entire network.
- **Automated Provisioning and Change Control.** Provides seamless workflows for automated cloud-like network operations, dramatically reducing the possibility of errors and misconfigurations and making operations tasks significantly more efficient.
- **Orchestration.** Acting as a single point of integration for both 3rd party ecosystem partners and non-EOS devices, as well as providing a native API gateway for customer extensibility.

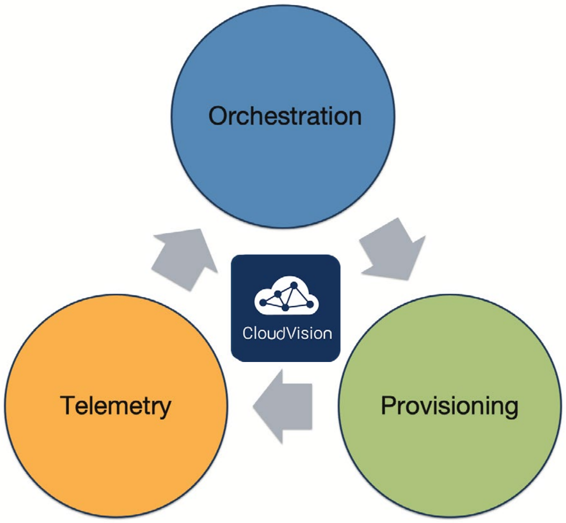


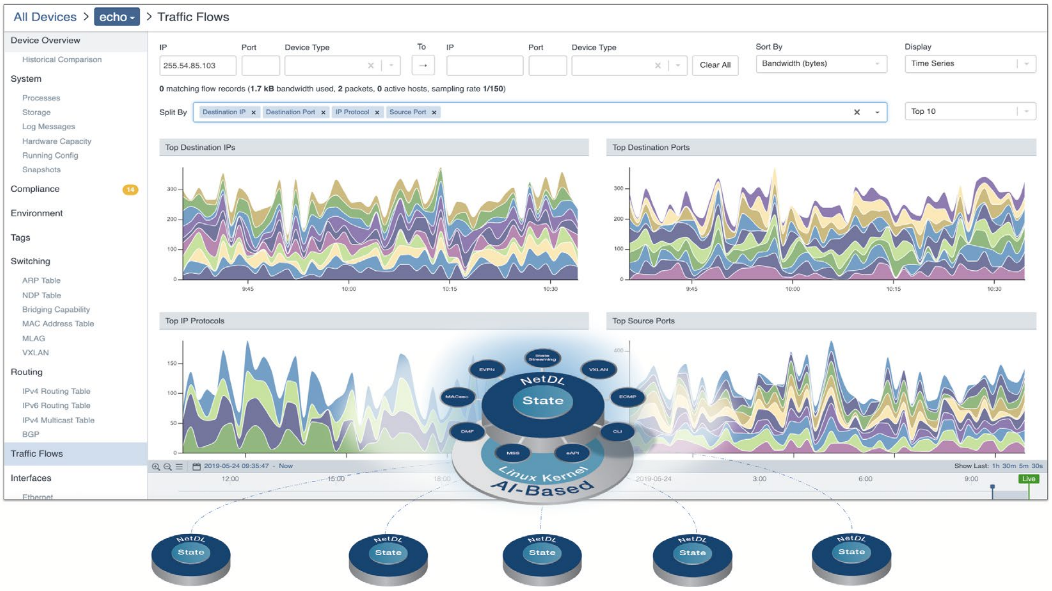
Figure 6: Three functional pillars in one platform

Arista's open software-driven cloud networking approach focuses on improving client and operator experience and improving economics for everyone. With a single operating system and streaming approach across all network platforms and use-cases, EOS and CloudVision dramatically simplify the complexity of the myriad of OS trains and management models that proliferate across a typical legacy network. Built from the ground up as a programmable software platform with exceptional reliability and unique state-streaming architecture, Arista EOS and CloudVision have established themselves as the preferred platform for cloud networking.

CloudVision Architecture

CloudVision was built with the architectural goal of streaming the state of all systems under management in real-time, through an analytics pipeline, and finally into a database for historical retrieval and analysis. The common challenge in traditional management systems when trying to build a given application is getting access to the right data in the first place. The CloudVision architecture and design allows a focus on building the most interesting applications on top of a complete dataset. This is incredibly important for any network analytics, where the insights can only be as deep as the underlying dataset allows.

To achieve this goal, CloudVision is built on a modern scale-out cloud-native architecture with 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 but delivered as a turn-key packaged solution or cloud service so that it is accessible to any customer.



IP: 255.54.85.103 · Port · Device Type · To · IP · Port · Device Type · Sort By: Bandwidth (bytes) · Display: Time Series

0 matching flow records (1.7 kB bandwidth used, 2 packets, 0 active hosts, sampling rate 1/150)

Split By: Destination IP, Destination Port, IP Protocol, Source Port · Top 10

2019-05-24 09:38:47 - Now · Show Last: 1h 30m 5m 30s

Figure 7: Powerful Analytics and Faster Insights with Rich Steaming Data

Arista has implemented what others would build for a modern telemetry system in the do-it-yourself model with integrations for customers that prefer to use additional advanced DevOps and workflow automation tools. While we recognize that many of our customers would like to build entirely bespoke infrastructure management tools for their unique environment, practicalities often make this buy vs. build decision difficult.

For example, below are some of the common open-source component choices for building a modern telemetry pipeline, along with the choices implemented in CloudVision:

Component	Distributed Key-value Database	Queuing System	Analytics Pipeline	Search Engine	Visualization	Container Management
Options	HBase, Cassandra, Kudu, Druid, etc	Kafka, ActiveMQ, ZeroMQ, RabbitMQ	Spark, Storm, Heron, etc	Elastic, Solr	Kibana, Grafana	Kubernetes, Docker Swarm, Apache Mesos
CloudVision Components	HBase	Kafka	CloudVision Turbines	Elasticsearch	CloudVision Telemetry UI	Kubernetes

Figure 8: Telemetry System Components

These components break down into functions as described below and as depicted in figure 8:

- A scale-out database built on top of HBase for storing all network state over time
- An indexing engine built with ElasticSearch for quickly searching through historical state
- A queuing system built with Kafka and gRPC to stream updates between components of the pipeline
- An API Server, providing a single point of access for all applications into the CloudVision database, exposing read, write, and subscribe semantics over a gRPC, WebSocket, and REST interface
- An analytics engine, called CloudVision Turbines, for stream processing applications
- The CloudVision UI for visualizing the underlying network-wide database and analytics insights for network operators

Network-wide Infrastructure Service

The foundation of CloudVision is an infrastructure service accessed via a web portal, sharing and aggregating the working state of network devices running Arista EOS® software to provide visibility and central coordination. The value of having an aggregated real-time view of the network state cannot be overstated. For the first time, the management plane can have a central view of all of the data that the network devices have across domains, without the need to poll, screen-scrape, transform, filter and refresh.

The CloudVision platform builds on the innovative EOS event-driven state database design model called SysDB, which holds the entire state for a particular device (e.g., running configuration, neighbor topology, protocol state, tables, monitoring counters, interface/link-state, processes, errors, and events). CloudVison leverages SysDB by extending it to a centralized CloudVision database (NetDB) through open state-streaming APIs, thus providing a platform for automation, orchestration and AI/ML-enabled analytics.

State from each participating EOS node is streamed and synchronized to CloudVision's database using the same publish/subscribe architecture of the EOS system database. By communicating to each participating switch instance using a high-performance streaming API, CloudVision actively synchronizes state relevant to network-wide operational tasks and can provide a unifying abstraction point for integration with third-party IT operations, configuration management, deployment and orchestration tools like ServiceNow and Ansible.

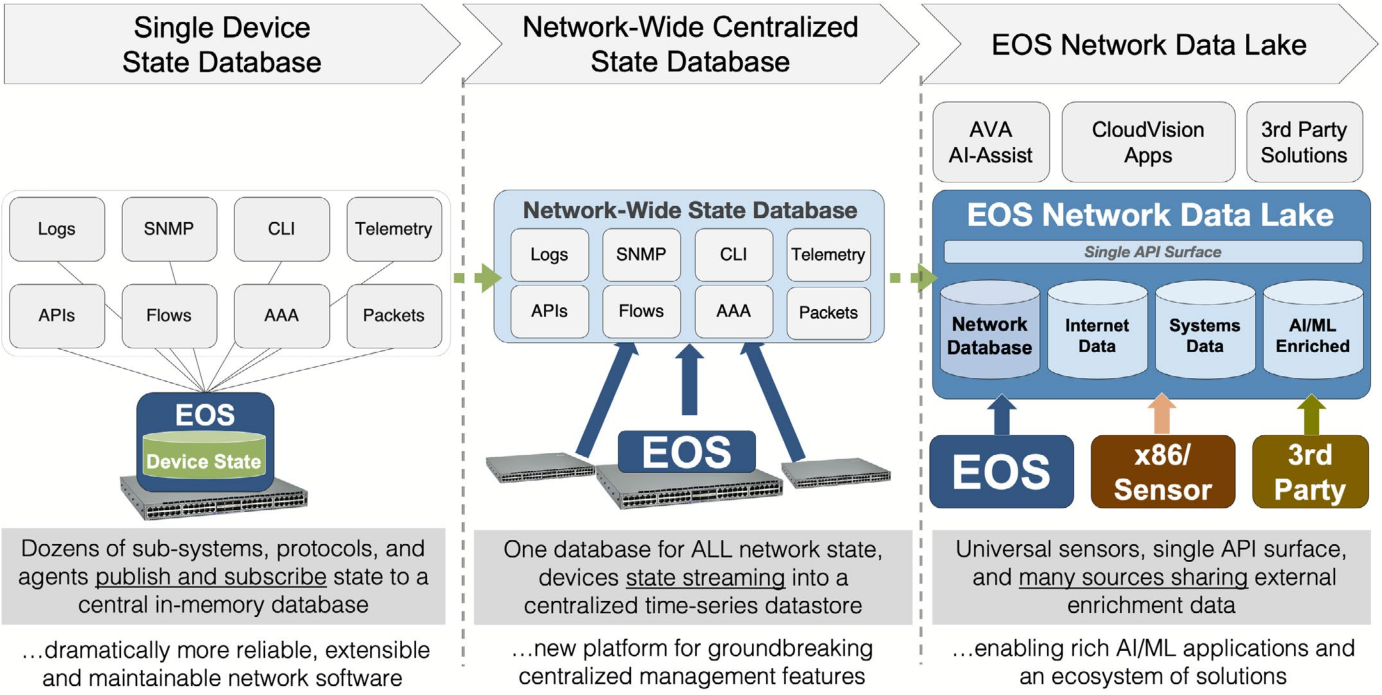

Single Device State Database
Network-Wide Centralized State Database
EOS Network Data Lake
Logs
SNMP
CLI
Telemetry
APIs
Flows
AAA
Packets
EOS
Device State
Network-Wide State Database
Logs
SNMP
CLI
Telemetry
APIs
Flows
AAA
Packets
EOS
AVA AI-Assist
CloudVision Apps
3rd Party Solutions
EOS Network Data Lake
Single API Surface
Network Database
Internet Data
Systems Data
AI/ML Enriched
EOS
x86/ Sensor
3rd Party
Dozens of sub-systems, protocols, and agents publish and subscribe state to a central in-memory database
…dramatically more reliable, extensible and maintainable network software
One database for ALL network state, devices state streaming into a centralized time-series datastore
…new platform for groundbreaking centralized management features
Universal sensors, single API surface, and many sources sharing external enrichment data
…enabling rich AI/ML applications and an ecosystem of solutions

Figure 9: Evolution of Network Data Store

The next step in integration of network data is the evolution of the network-wide NetDB data platform as a foundational technology to bind other Arista and third-party datasets into a multi-modal and multi-tenant Network Data Lake (NetDL™), using open state-streaming and data collection methodologies. NetDL will support multiple loosely coupled data modalities and will allow external data ingestion and enrichment to populate the pool of information available for AI training algorithms using guided and unsupervised learning.

Specifically, NetDL is a vision and architectural direction for Arista that will enable an ecosystem of Arista strategic partners and Independent Software Vendors (ISVs) to deliver market and customer-specific intelligent insights and solutions in the areas of network operations, continuous integration, cyber-security, application/network performance, and other categories.

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) and extends that from automating initial device provisioning to also include 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 'container views' or tagging – 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. The operational model can be further optimized with provisioning workflows through CloudVision Studios, which is discussed in more detail in the Network Automation section. This flexible model enhances operational efficiency while simplifying change management, thus reducing potential human error, providing a centralized source of configuration truth, and allowing both realtime and historic troubleshooting. Further, ongoing risk and compliance management workflows can be automated to allow greater agility for the entire network operations lifecycle.

CloudVision's visual applications 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

Device state is streamed throughout the system end-to-end: from each device, into the CloudVision database, through CloudVision's analytics pipeline, and then to the web UI. There's no polling anywhere in the system. The CloudVision streaming telemetry agent runs on all Arista EOS-based switches. It streams the time-stamped device-state data to the CloudVision analytics engine, which is the back-end data processing component of the platform and location of storage and analysis of Arista machine data.

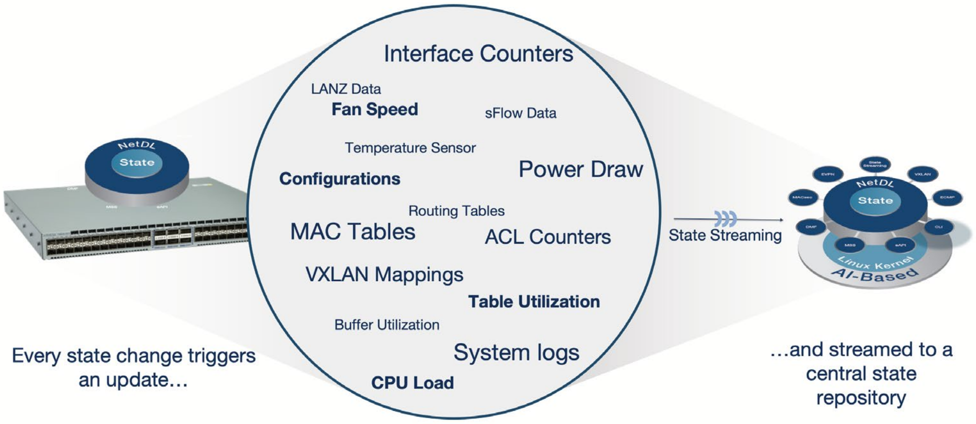


Figure 10: CloudVision's Analytics Pipeline

The transport layer between services throughout the system uses grpc remote procedure call framework (gRPC). gRPC is a modern high-performance framework built on top of Google protocol buffers (protobufs) and HTTP2, providing the scale and performance to stream the full network state from each device into the CloudVision analytics pipeline.

The streaming telemetry agent in EOS and the Device SDK are built on top of 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 choices for modeling network state in CloudVision and have been supplemented by Arista to represent the complete state of the EOS network where necessary.

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.

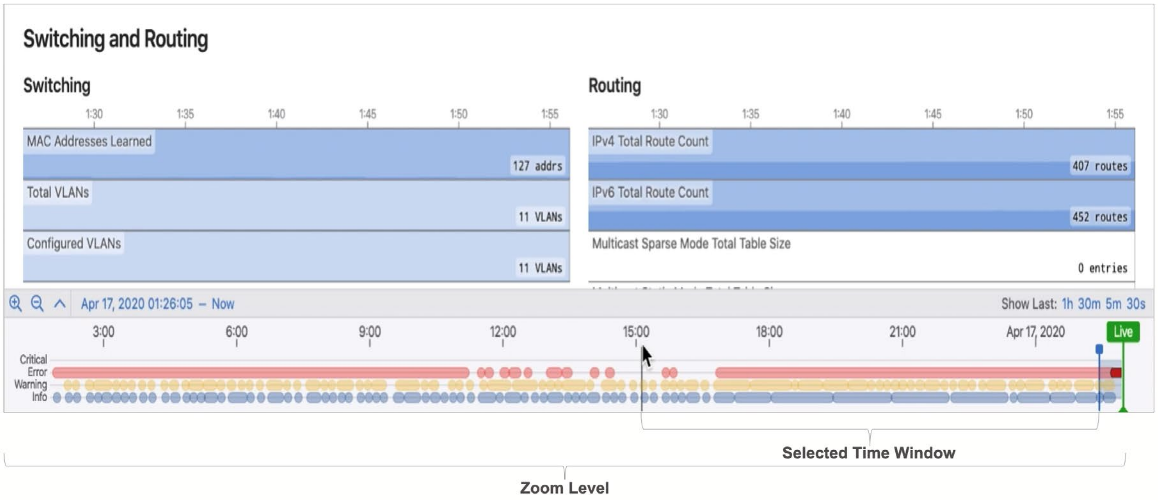
In addition to providing a historic state database network-wide, the analytics engine also offers an API server that allows customers and partners to leverage a single point of integration to third-party or internal tools using streaming and WebSocket-based APIs. CloudVision Telemetry Applications and 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

Along with providing real-time visibility into the state of the network and its attached devices, CloudVision streaming technology provides a modern approach to network telemetry. Unlike legacy management architectures that relied upon periodic SNMP polling, which gathered telemetry and configuration data from the network every few minutes at best, CloudVision streaming delivers a constant feed of real-time telemetry data to the CloudVision analytics engine, database, and CloudVision applications. All of the data that is collected is stored and can be viewed and further analyzed in any time window that the user selects.

Telemetry streaming allows CloudVision to identify network problems virtually instantaneously, and it allows IT operations teams to optimize network performance much more quickly than legacy management using polling ever could. When conditions worsen due to errant configuration changes, intermittent faults, or demanding workloads, there is instantaneous visibility throughout the system. Transient problems that might impact users between polling intervals are no longer hidden. Remediation can start within seconds.



Switching and Routing

Switching

MAC Addresses Learned 127 addrs
Total VLANs 11 VLANs
Configured VLANs 11 VLANs

Routing

IPv4 Total Route Count 407 routes
IPv6 Total Route Count 452 routes
Multicast Sparse Mode Total Table Size 0 entries

Apr 17, 2020 01:26:05 – Now

Show Last: 1h 30m 5m 30s

Selected Time Window

Zoom Level

Figure 11: CloudVision's Timeline Slider Example in Events Views

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

As the variety and volume of metrics that network devices can generate are increasing, and with an explosion of IoT devices and mobile users connecting to enterprise networks, it is imperative that a telemetry-based approach to management tools replace legacy monitoring. An enterprise-class telemetry architecture can address issues such as security, scaling, and polling gaps to provide full observability of all aspects of network operations.

The rest of this whitepaper will focus on the various CloudVision functions that can be deployed on-premises or via the cloud service for enterprise use-cases across data center, campus, and hybrid cloud.

Analytics Platform AI/ML

CloudVision contains a powerful, event-driven, streaming analytics engine that enables you to monitor the state of all managed devices, orchestrate various actions, and gain valuable insights along the way. Conceptually, 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 and CloudVision Apps 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.

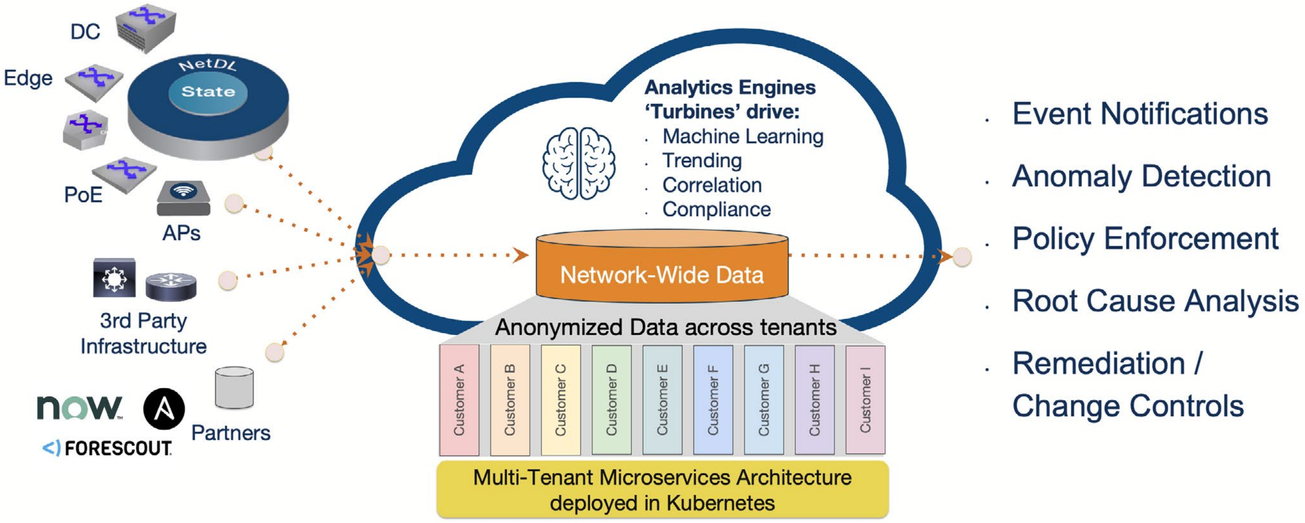


Figure 12: CloudVision Analytics Platform

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

In practical terms, CloudVision Analytics can dramatically improve operational efficiency, network uptime, and cost savings through better network observability, automated workflows, and orchestration of the network across services. The outcome is enhanced reliability, faster root cause analysis, and faster mean time to innocence.

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

- **Reachability Anomalies.** Modeling time-series data for reachability and latency baselines, derived from Cloud Tracer telemetry, where alerts are identified 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.

The CloudVision analytics platform provides a comprehensive and extensible resource for AI NetOps services, such as proactive TAC support and efficient network-wide capacity management. More information on these capabilities is included below in descriptions of CloudVision Apps. The use of AI/ML in CloudVision is increasing as more use cases are discovered.

High Availability Clusters

CloudVision software is deployed as a virtual or physical appliance, and in a production on-premises cluster uses three redundant servers to achieve high levels of availability. In the cloud service version of CloudVision, Arista hosts a multi-tenant cluster and can be expanded to as many nodes as required to meet service level objectives.

The CloudVision cluster consists of distributed components such as Zookeeper, Hadoop/HDFS, and HBase. Zookeeper provides consensus and configuration tracking mechanisms across a cluster of redundant systems. The cluster relies upon the underlying Hadoop/HDFS data store for high availability and HBase as a distributed key/value store. Running these services in a reliable fashion on multiple nodes is a proven and open approach used in many big data applications and provides reliability, performance, and scale with limited overhead.

The Analytics engine utilizes the high-performance Hbase database to store device-state data, including events and alerting. 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.

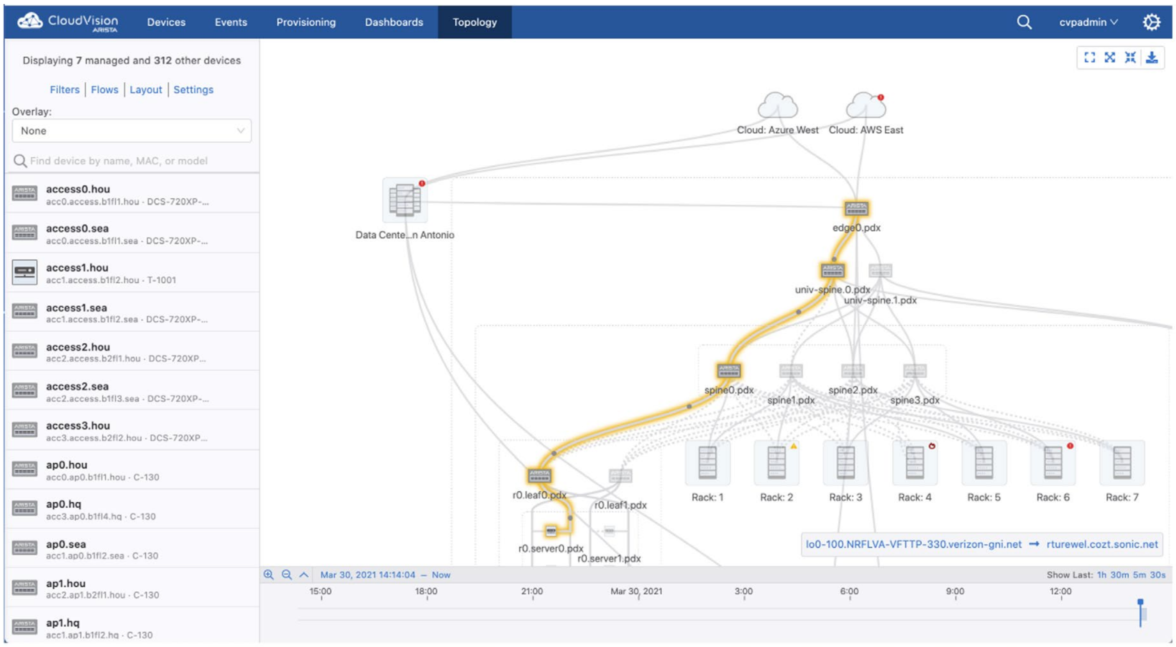
CloudVision Applications

The CloudVision platform consists of the previously described core infrastructure and several value-added applications shown as 'views' in the web GUI. These include Topology View, Events View, Device View, Dashboards Views and Cloud Tracer.

Topology View

CloudVision breaks down legacy network silos by providing an end-to-end view across the data center, campus, and cloud with a single management plane. With enterprise applications increasingly becoming cloud-based and clients increasingly remote, only a consistent and unified management plane can provide visibility for any client to cloud use cases. CloudVision's Topology View is designed to visualize these broad network topologies into a common interface with live analytics and workflow task visibility.

The Topology View app helps network administrators visualize the network topology to understand how devices are interconnected and quickly identify hotspots in the network based on link level metrics such as bandwidth, errors and discards. CloudVision's Topology View provides an intuitive approach to mapping the network topology not just based on LLDP neighbors but also backend analytics that automatically calculate device type, neighbor relationships, and common layouts. Using heuristics, CloudVision determines if devices in a topology are Leaf, Spine, or an Endpoint device, and presents them in a network design view that relates to their logical interconnection. These layouts can be collapsed and expanded to reduce visual complexity and help network administrators visualize their network in a way that aligns with the network design.



Displaying 7 managed and 312 other devices

Overlay: None

access0.hou
acc0.access.b1fl1.hou · DCS-720XP-...

access0.sea
acc0.access.b1fl1.sea · DCS-720XP-...

access1.hou
acc1.access.b1fl2.hou · T-1001

access1.sea
acc1.access.b1fl2.sea · DCS-720XP-...

access2.hou
acc2.access.b2fl1.hou · DCS-720XP...

access2.sea
acc2.access.b1fl3.sea · DCS-720XP-...

access3.hou
acc3.access.b2fl2.hou · DCS-720XP...

ap0.hou
acc0.ap0.b1fl1.hou · C-130

ap0.hq
acc3.ap0.b1fl4.hq · C-130

ap0.sea
acc1.ap0.b1fl2.sea · C-130

ap1.hou
acc2.ap1.b2fl1.hou · C-130

ap1.hq
acc1.ap1.b1fl2.hq · C-130

lo0-100.NRFLVA-VFTTP-330.verizon-gni.net → rturewel.cozt.sonic.net

Mar 30, 2021 14:14:04 – Now

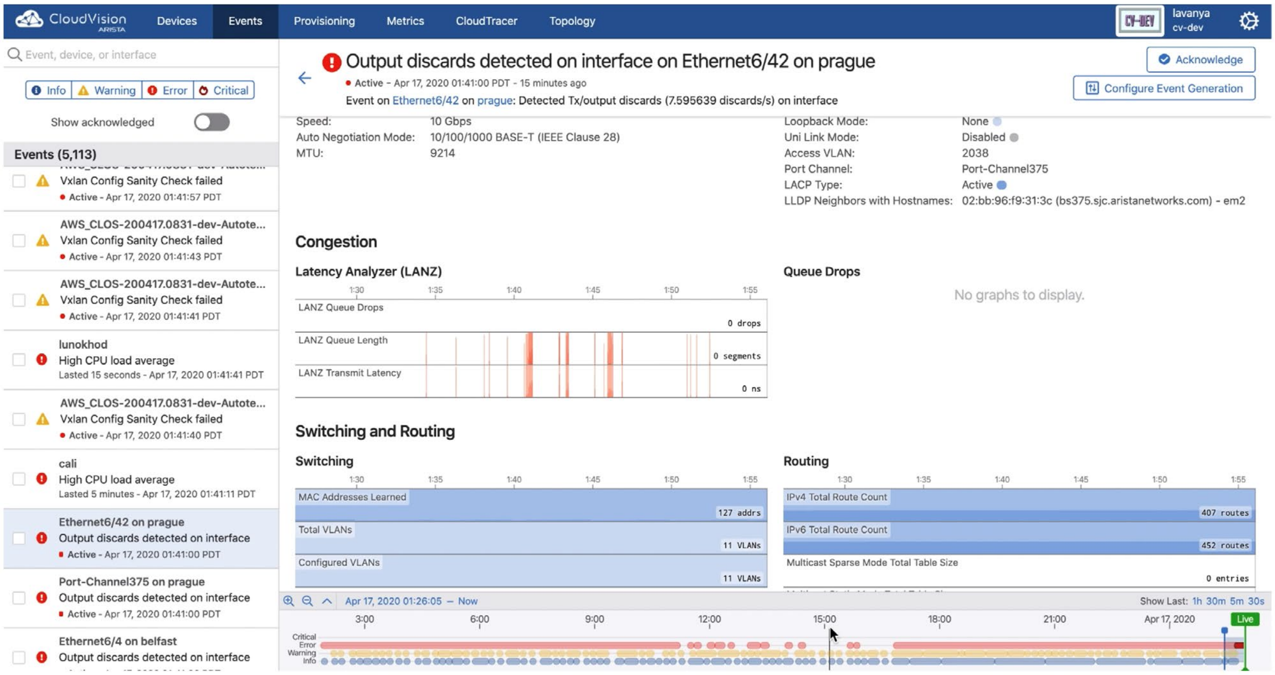
Show Last: 1h 30m 5m 30s

Figure 13: CloudVision Topology View

Topology View allows users to overlay metrics on the network topology view. This helps network administrators quickly identify problems such as network congestion and traffic imbalance from a network-wide perspective. Items such as 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 view allows users to start at a network-wide level and use the overlays to drill down to the problem area for troubleshooting. The timeline can be leveraged in Topology View to view the historical state for segmentation, flow, and link-level metrics.

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, and the event store can 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 that the counter has increased a set threshold for an interface. This information is not sufficient to identify the root cause of the discards. In operational practice, not only are other metrics such as traffic rate, buffer utilization required to pinpoint the root cause but also it's key to have these metrics for the same time window when the discards were incrementing. The CloudVision event view for interface discards provides all pieces of the puzzle and at the same point in time helps the operator identify if the discards were a result of congestion. The correlated view is available for all such events generated for all monitored devices.



Events (5,113)

- Vxlan Config Sanity Check failed
  Active - Apr 17, 2020 01:41:57 PDT
- AWS_CLOS-200417.0831-dev-Autote...
  Vxlan Config Sanity Check failed
  Active - Apr 17, 2020 01:41:43 PDT
- AWS_CLOS-200417.0831-dev-Autote...
  Vxlan Config Sanity Check failed
  Active - Apr 17, 2020 01:41:41 PDT
- lunokhod
  High CPU load average
  Lasted 15 seconds - Apr 17, 2020 01:41:41 PDT
- AWS_CLOS-200417.0831-dev-Autote...
  Vxlan Config Sanity Check failed
  Active - Apr 17, 2020 01:41:40 PDT
- cali
  High CPU load average
  Lasted 5 minutes - Apr 17, 2020 01:41:11 PDT
- Ethernet6/42 on prague
  Output discards detected on interface
  Active - Apr 17, 2020 01:41:00 PDT
- Port-Channel375 on prague
  Output discards detected on interface
  Active - Apr 17, 2020 01:41:00 PDT
- Ethernet6/4 on belfast
  Output discards detected on interface

Output discards detected on interface on Ethernet6/42 on prague

Active – Apr 17, 2020 01:41:00 PDT – 15 minutes ago

Event on Ethernet6/42 on prague: Detected Tx/output discards (7.595639 discards/s) on interface

Speed:	10 Gbps	Loopback Mode:	None
Auto Negotiation Mode:	10/100/1000 BASE-T (IEEE Clause 28)	Uni Link Mode:	Disabled
MTU:	9214	Access VLAN:	2038
		Port Channel:	Port-Channel375
		LACP Type:	Active
		LLDP Neighbors with Hostnames:	02:bb:96:f9:31:3c (bs375.sjc.aristanetworks.com) - em2

Figure 14: CloudVision Events View

As demand on a network increases with the onset of server virtualization, consolidation, IP storage, Hadoop, there will be times of congestion on the network. When there is congestion on the network, Arista switches have a feature called 'LANZ' (Latency "ANalyZer") which can proactively highlight when there is congestion and the impact of the latency. However, this is an interface-level command that must be collected box-by-box and not holistic for the network.

CloudVision helps the network operator to monitor health and congestion network-wide and identify hot spots that may be on a specific port or link. This allows the operator to quickly move workloads and workflows to less demanding resources on the network.

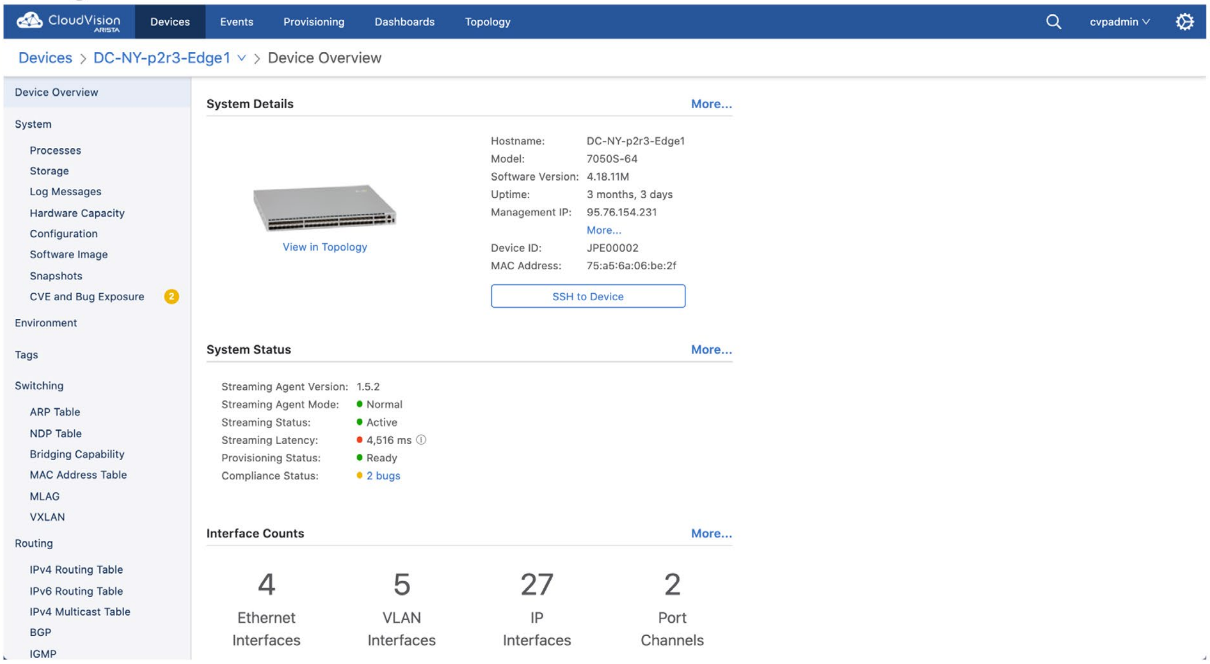
CloudVision supports the ability to configure and receive alerts for events generated. Users can get alerted via email, common chat-based services such as Slack or HipChat, and PagerDuty applications. Webhooks are available for custom alerting and monitoring needs that can help integrate the alerts into existing monitoring and incident management systems like centralized log servers, ServiceNow, or any web server-based application that can accept an HTTP POST notification. Webhooks also provide flexibility in taking actions in response to an event, for example, opening an incident ticket for a link down event from a specific device or closing an incident/task for a software upgrade on change of EOS version, triggering configurable actions based on certain event types from critical devices.

Further, alert rules can be configured based on the type of event, severity, and per device to allow users to customize how they receive alerts from various devices. This helps raise visibility for specific events on critical devices and prevents network operators from overlooking important events.

Device View

This view offers a detailed insight into relevant metrics at a device level that is accessible using CLI commands, such as environmentals, system details, interface statistics, MAC addresses, and routing tables. In addition to these metrics, it also includes platform-level details like digital optical monitoring (DOM), hardware route table, ACL table. PoE metric and buffer utilization for every device that SNMP-based legacy tools typically do not provide. The graphical user interface adds an abstraction layer by removing platform-level subtleties that are often dependent on chip architecture and are heavily reflected in CLI commands making the outputs hard to interpret for network operators.

Like other parts of the CloudVision portal user interface, all device views include a selectable time window at the bottom of the screen allowing users to either monitor these metrics in real-time or leverage the time-series state repository to view and compare the historical state across time, devices, and network segments – providing for much faster troubleshooting and issue remediation.



System Details

Hostname: DC-NY-p2r3-Edge1
Model: 7050S-64
Software Version: 4.18.11M
Uptime: 3 months, 3 days
Management IP: 95.76.154.231
More...
Device ID: JPE00002
MAC Address: 75:a5:6a:06:be:2f

System Status

Streaming Agent Version: 1.5.2
Streaming Agent Mode: ● Normal
Streaming Status: ● Active
Streaming Latency: ● 4,516 ms ⓘ
Provisioning Status: ● Ready
Compliance Status: ● 2 bugs

Interface Counts

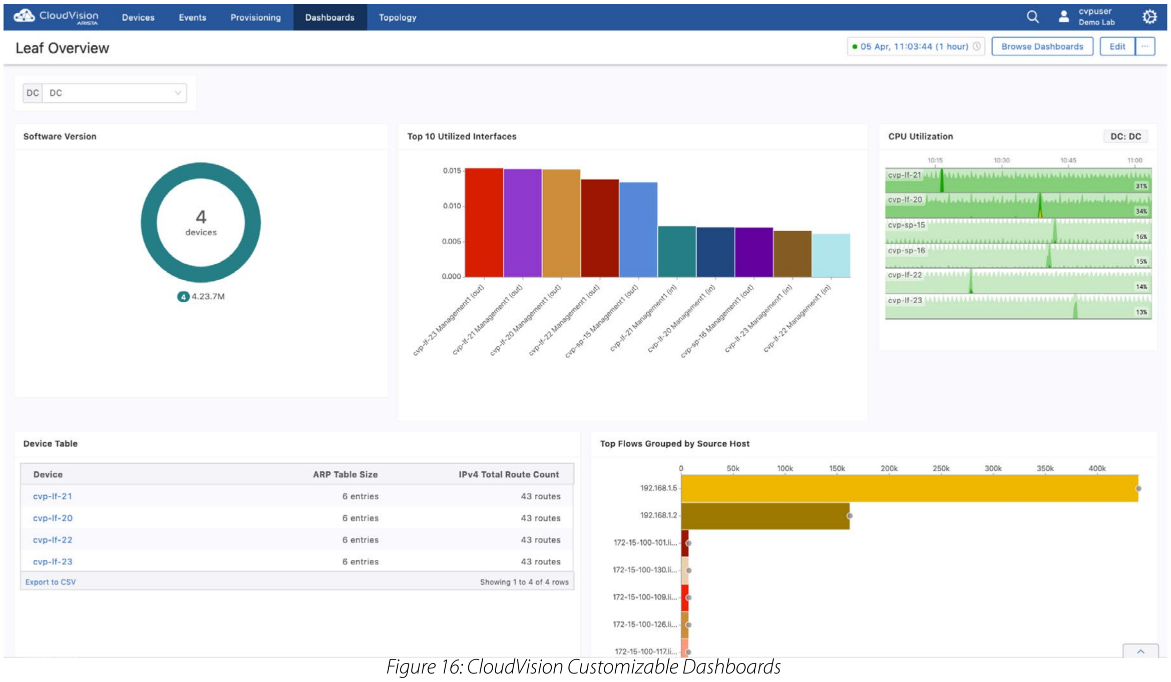
4 Ethernet Interfaces
5 VLAN Interfaces
27 IP Interfaces
2 Port Channels

Figure 15: CloudVision Device View

Dashboards Views

This view highlights the power of a network-wide perspective by allowing the user to choose metrics and correlate them across the network for the same time window. Users can build customized dashboards for monitoring groups of devices or interfaces using built-in and user-created tags. This allows network operators to quickly identify anomalies in device metrics or gauge the exposure of behavior in the network. For example, identifying a sudden surge in the number of routing table entries on one device may warrant a quick check on how many devices saw a surge in route table entries at the same time to see if devices in critical paths could be at risk. This would otherwise be a tedious approach to get the outputs from the CLI on a device-by-device basis.

With the Dashboards views, accessing the output of the CLI command across the network in one consolidated user panel empowers the operator to identify anomalies quickly and decreases 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 using a few clicks versus a manual approach.



Device Table

Device	ARP Table Size	IPv4 Total Route Count
cvp-lf-21	6 entries	43 routes
cvp-lf-20	6 entries	43 routes
cvp-lf-22	6 entries	43 routes
cvp-lf-23	6 entries	43 routes

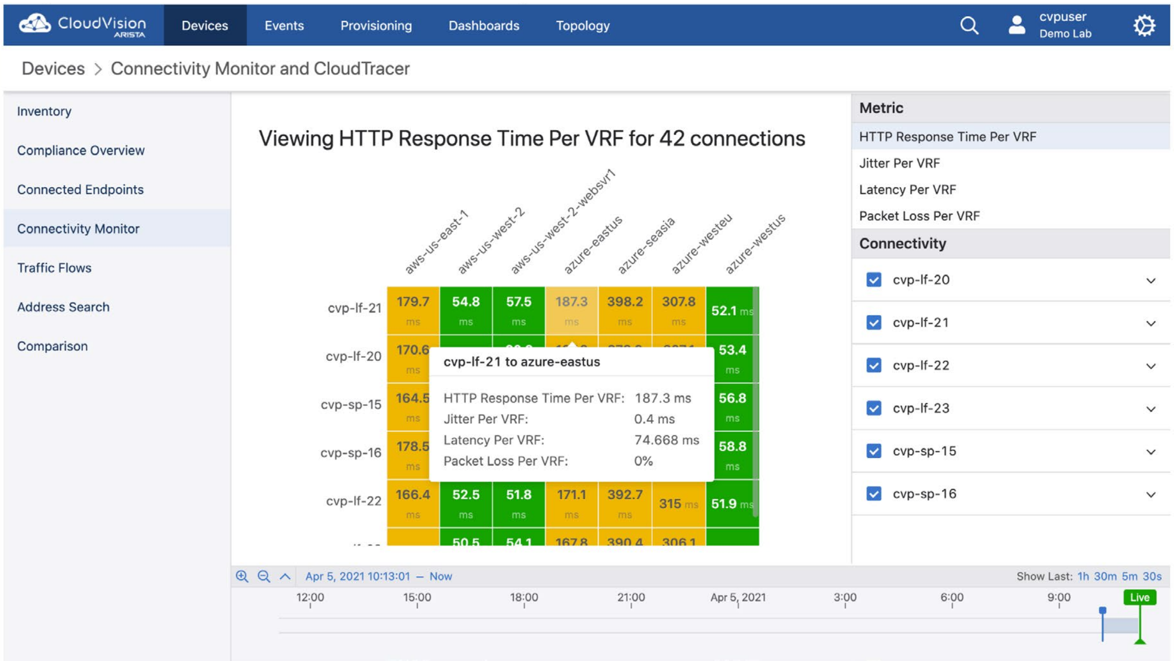
Export to CSV Showing 1 to 4 of 4 rows

Figure 16: CloudVision Customizable Dashboards

Cloud Tracer

While telemetry and visibility are important within the data center, it is even more important when operating in a diverse hybrid cloud environment to constantly monitor the entire client-to-cloud network experience. Compute workloads that span public and private clouds need to maintain consistent availability, as do clients accessing cloud-based and on-premises compute and storage resources. It is up to the network operator to be aware of any connectivity and reliability issues across the entire enterprise estate, even on the transit networks that they don't own.

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



Viewing HTTP Response Time Per VRF for 42 connections

	aws-us-east-1	aws-us-west-2	aws-us-west-2-websvr1	azure-eastus	azure-seasia	azure-westeu	azure-westus
cvp-lf-21	179.7 ms	54.8 ms	57.5 ms	187.3 ms	398.2 ms	307.8 ms	52.1 ms
cvp-lf-20	170.6 ms						53.4 ms
cvp-sp-15	164.5 ms						56.8 ms
cvp-sp-16	178.5 ms						58.8 ms
cvp-lf-22	166.4 ms	52.5 ms	51.8 ms	171.1 ms	392.7 ms	315 ms	51.9 ms
		50.5	54.1	167.8	390.4	306.1	

cvp-lf-21 to azure-eastus

HTTP Response Time Per VRF:	187.3 ms
Jitter Per VRF:	0.4 ms
Latency Per VRF:	74.668 ms
Packet Loss Per VRF:	0%

Figure 17: Cloud Tracer Connectivity Monitor

While initially designed for the hybrid cloud use-case, the Cloud Tracer 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 what caused any changes in connectivity and performance and how it affected applications and client experiences.

CloudVision Network Automation

Even today, most network device provisioning, software upgrades, and configuration changes are still being done manually. This not only takes significant amounts of time, but it also leads to complexity and often error-prone operational procedures.

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 network configurations, deployment, and ongoing operations.

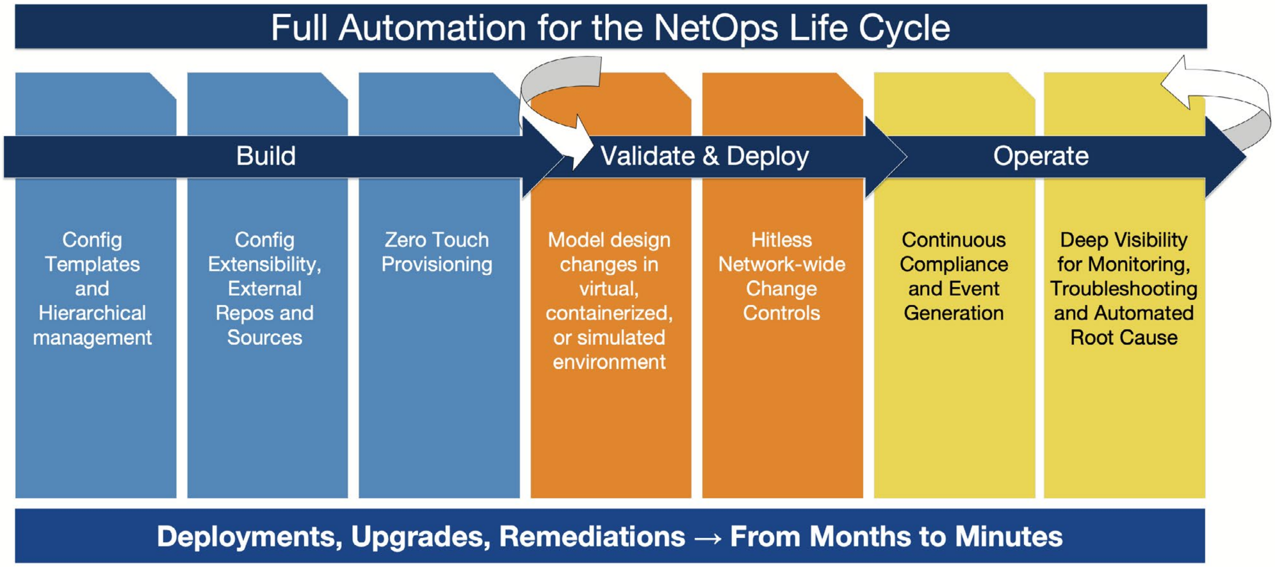

Full Automation for the NetOps Life Cycle
Build
Validate & Deploy
Operate
Config Templates and Hierarchical management
Config Extensibility, External Repos and Sources
Zero Touch Provisioning
Model design changes in virtual, containerized, or simulated environment
Hitless Network-wide Change Controls
Continuous Compliance and Event Generation
Deep Visibility for Monitoring, Troubleshooting and Automated Root Cause
Deployments, Upgrades, Remediations → From Months to Minutes

Figure 18: Full Automation for the NetOps Lifecycle

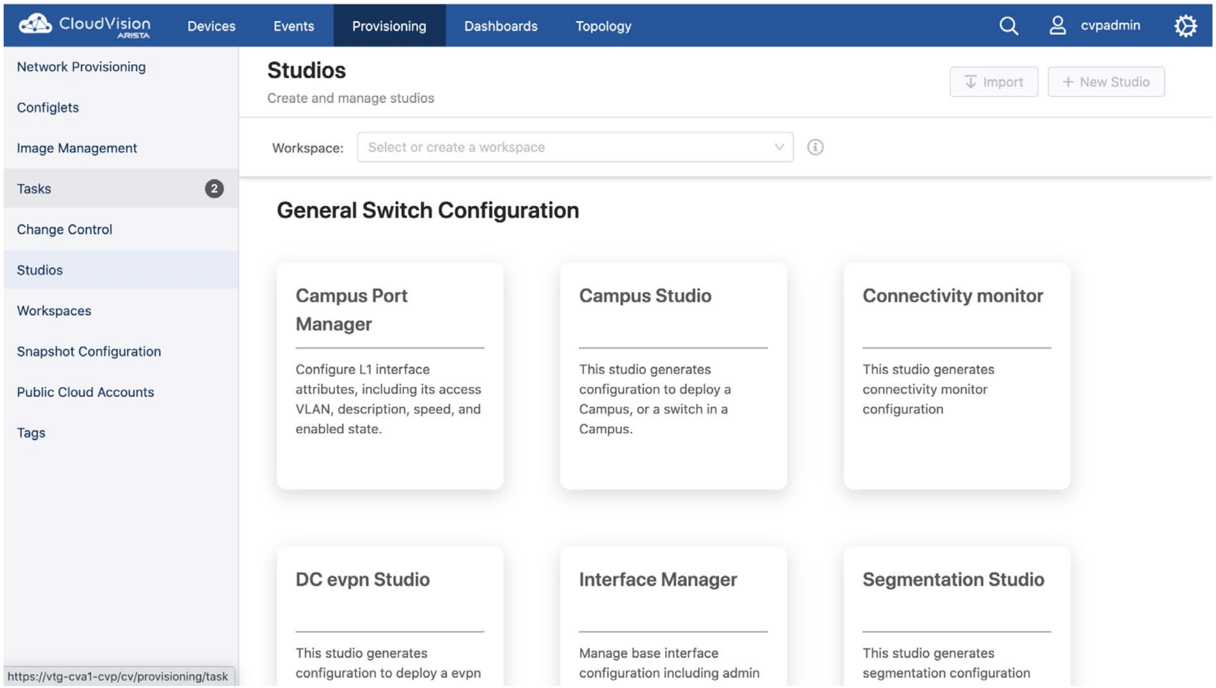
Building the Network

Arista was one of the first in the networking industry to deliver Zero Touch Provisioning (ZTP). ZTP allows the customer to make a switch out of the box, rack it, and automatically provision it with a machine-generated configuration, officially approved image, or script without any human intervention – similar to how an IP Phone configures itself, or how a wireless access point configures itself with no manual intervention.

However, there was no turnkey way to orchestrate the ZTP process using a network-wide view. When network switches are managed, typically a configuration, image, and script are used to provision and manage change controls for that switch. The Provisioning app allows a customer to perform all three actions at the same time in a network-wide view.

To take ZTP a step further, CloudVision allows administrators to not only deploy brand new switches in remote locations without requiring an engineer to manually configure the switch but for replacements as well. Zero Touch Replacement (ZTR) allows a switch that has failed to be reprovisioned, or decommissioned to inherit the configuration and settings of an existing switch without requiring to apply all settings from scratch. Once again, with the flexibility of the EOS single binary image, it makes moving switch settings from one switch to another with ease.

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 simple campus networks for the enterprise, through to complex EVPN deployments in the data center. This prevents administrators from having to manually create each configuration for every switch. Using abstracted network data models, CloudVision Studios translates network design 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 low-code approach for easy customizations to these workflows and the ability to create new workflows with Studios for the advanced network administrators.



Studios

Create and manage studios

General Switch Configuration

Campus Port Manager — Configure L1 interface attributes, including its access VLAN, description, speed, and enabled state.

Campus Studio — This studio generates configuration to deploy a Campus, or a switch in a Campus.

Connectivity monitor — This studio generates connectivity monitor configuration

DC evpn Studio — This studio generates configuration to deploy a evpn

Interface Manager — Manage base interface configuration including admin

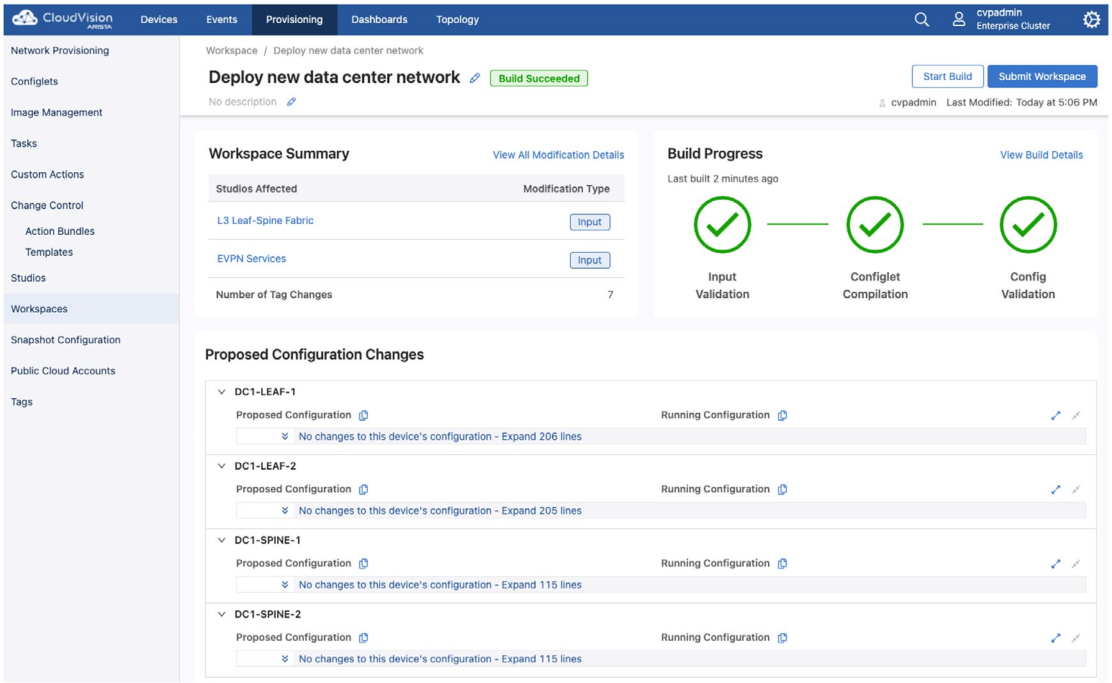
Segmentation Studio — This studio generates segmentation configuration

Figure 19: Built-in Workflows with CloudVision Studios

ZTP solutions were first born out of the need for automating the initial deployment of a switch in the infrastructure i.e. a 'day zero' process. To obtain OpEx cost reductions of managing the asset during the life cycle of its deployment in the data center, CloudVision is expanding the scope of 'Zero Touch' to a broader perspective to help automate ongoing changes over the lifecycle of the network devices. Customers are enabled to use a turnkey portal-based ZTP and ZTR solution to provision the device initially and throughout its lifecycle.

Validating and Deploying the Network

After the device configurations are built, CloudVision Studios can help validate those configurations and deploy the changes to production.



Workspace / Deploy new data center network

Deploy new data center network — Build Succeeded

No description

cvpadmin Last Modified: Today at 5:06 PM

Workspace Summary

Studios Affected	Modification Type
L3 Leaf-Spine Fabric	Input
EVPN Services	Input
Number of Tag Changes	7

Build Progress

Last built 2 minutes ago

Input Validation ✓ — Configlet Compilation ✓ — Config Validation ✓

Proposed Configuration Changes

DC1-LEAF-1
Proposed Configuration | Running Configuration
No changes to this device's configuration - Expand 206 lines

DC1-LEAF-2
Proposed Configuration | Running Configuration
No changes to this device's configuration - Expand 205 lines

DC1-SPINE-1
Proposed Configuration | Running Configuration
No changes to this device's configuration - Expand 115 lines

DC1-SPINE-2
Proposed Configuration | Running Configuration
No changes to this device's configuration - Expand 115 lines

Figure 20: Config Validation with CloudVision Studios

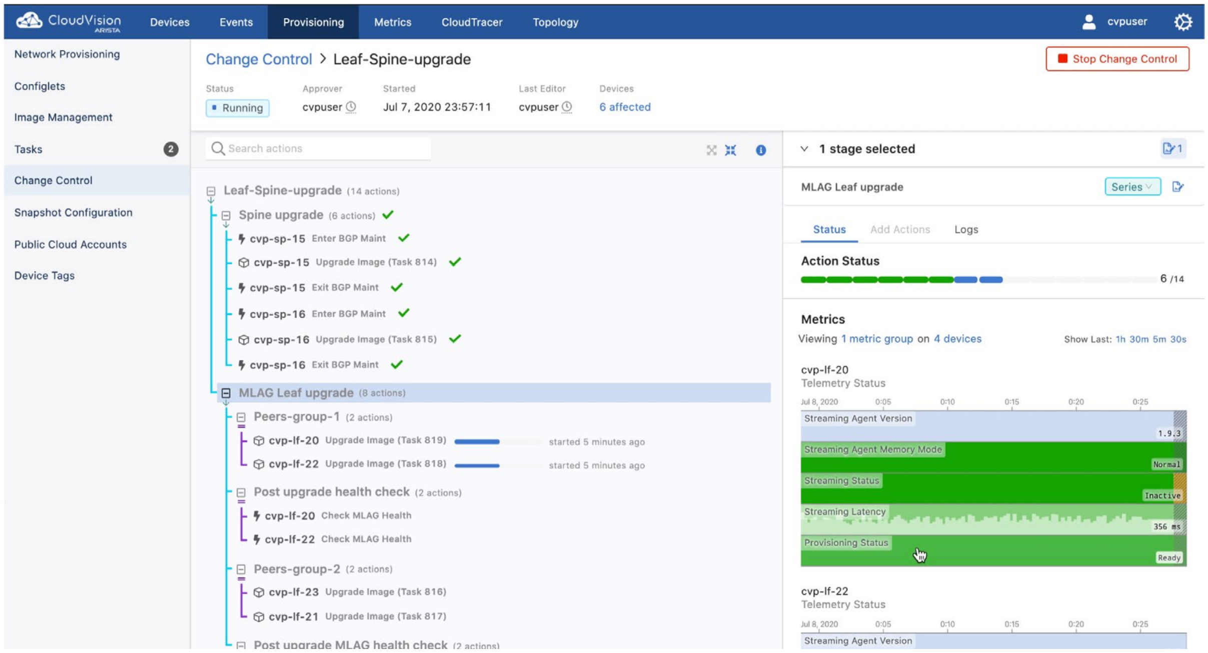
Many customers will build a virtual network environment using virtual machines or containers to simulate a network environment and validate the effects of configuration changes. vEOS-lab and cEOS-lab are software tools that run the exact same EOS software as an Arista switch but in a VM or container format. As such, they provide the same control and management plane experience as an actual physical switch running EOS. These software options are commonly used to build virtual environments for pre-production validation. Similarly, CloudVision can manage these VM or container-based EOS instances to build the virtual environment and to practice change controls on the virtual estate. CloudVision's ability to build and operate this virtual environment provides a useful simulation of actual production network changes.

Customers can also integrate CloudVision Studios with 3rd party validation tools, such as Batfish, 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 that the proposed changes meet all the predefined tests before executing the change. Once the configuration is validated and approved, CloudVision can help to roll out the network configuration through integrated network-wide change control workflows.

Using Change Controls

In the context of network maintenance, the change control process brings a controlled and coordinated approach to changes made in the network, while maintaining a documented audit trail and ensuring minimal disruption to network uptime. To ensure minimum service disruption, changes made to the network (configuration change, software upgrade, etc.) are planned at length and heavily scrutinized in the change control process, often requiring lengthy approvals and testing cycles before execution. The change control process in CloudVision comprises the following major steps, diagrammed below. An average change control in enterprise IT can take many hours across several weekends since a series of manual, box-by-box steps are employed and tend to be complicated and error-prone. Automating the change control process could reduce 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. Common change control workflows can be templatized and re-used for multiple provisioning or upgrade change management tasks. These templates include the ability to group tasks together to achieve a certain ordering of task execution, initiate custom snapshots of the environment that can be fed into the change management documentation process, and orchestrate actions that enable capabilities such as a seamless network-wide upgrades or execute some custom action that should be executed at a point during the change control.



Change Control > Leaf-Spine-upgrade

Status	Approver	Started	Last Editor	Devices
Running	cvpuser	Jul 7, 2020 23:57:11	cvpuser	6 affected

Leaf-Spine-upgrade (14 actions)
- Spine upgrade (6 actions) ✓
  - cvp-sp-15 Enter BGP Maint ✓
  - cvp-sp-15 Upgrade Image (Task 814) ✓
  - cvp-sp-15 Exit BGP Maint ✓
  - cvp-sp-16 Enter BGP Maint ✓
  - cvp-sp-16 Upgrade Image (Task 815) ✓
  - cvp-sp-16 Exit BGP Maint ✓
- MLAG Leaf upgrade (8 actions)
  - Peers-group-1 (2 actions)
    - cvp-lf-20 Upgrade Image (Task 819) started 5 minutes ago
    - cvp-lf-22 Upgrade Image (Task 818) started 5 minutes ago
  - Post upgrade health check (2 actions)
    - cvp-lf-20 Check MLAG Health
    - cvp-lf-22 Check MLAG Health
  - Peers-group-2 (2 actions)
    - cvp-lf-23 Upgrade Image (Task 816)
    - cvp-lf-21 Upgrade Image (Task 817)
  - Post upgrade MLAG health check (2 actions)

1 stage selected 1

MLAG Leaf upgrade Series

Action Status 6 /14

Metrics

Viewing 1 metric group on 4 devices Show Last: 1h 30m 5m 30s

cvp-lf-20
Telemetry Status

Streaming Agent Version	Streaming Agent Memory Mode	Streaming Status	Streaming Latency	Provisioning Status
1.9.3	Normal	Inactive	356 ms	Ready

cvp-lf-22
Telemetry Status

Figure 21: Change Control Orchestration

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

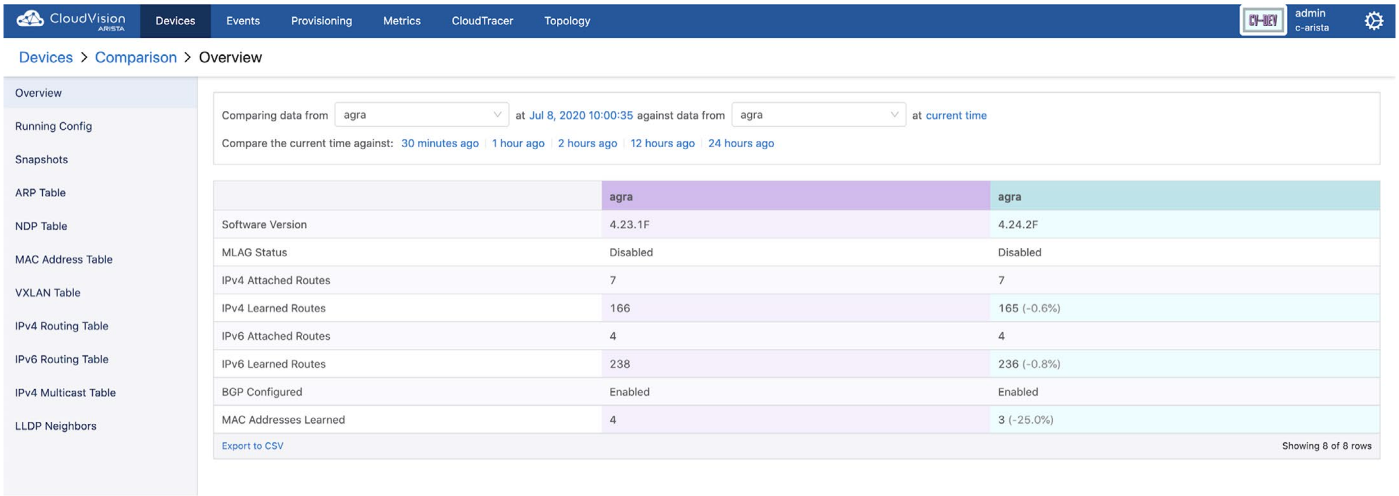
Once the change control is built, the operator must go through both a review and approval step before the change control can be executed. In addition, each of these steps is tied into CloudVision's Roles Based Access Control (RBAC) system so that different authority levels can be applied to each step. A strict non-author review model can also be enforced for change control approvals.

All of these capabilities work together to ensure that the network change control proceeds without impacting the network operation. With this workflow, operators have a tool that can make changes across the entire network without concern for slow manual procedures and typical human errors.

Viewing Device Comparisons

Typically, enterprise customers perform change controls outside production hours and request a change control window. When the change control window starts, the engineer performing the change will perform pre-change control procedures e.g. capturing switch interface status, VLAN status, IP routing status, multicast status, ACLs, QoS configuration, etc. using a number of 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 engineer will most probably run exactly the same scripts again. The reason these scripts are run is to ensure that the delta performed during the change is as expected. The only way to ensure this delta is accurate is if the engineer were to manually compare the pre-change & post-change status. If the change impacts a large number of devices, it is not manually possible to ensure 100% accuracy and there is a reliance on the sample-based confirmation, which substantially increases the risk of the change. Typically depending on the device or the complexity of the change, verifying the change manually can take an hour per device.

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 leveraged to track changes in key device metrics or review state before and after configuration changes and to facilitate network-wide rollback. 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.



Devices > Comparison > Overview

Comparing data from agra at Jul 8, 2020 10:00:35 against data from agra at current time

Compare the current time against: 30 minutes ago | 1 hour ago | 2 hours ago | 12 hours ago | 24 hours ago

	agra	agra
Software Version	4.23.1F	4.24.2F
MLAG Status	Disabled	Disabled
IPv4 Attached Routes	7	7
IPv4 Learned Routes	166	165 (-0.6%)
IPv6 Attached Routes	4	4
IPv6 Learned Routes	238	236 (-0.8%)
BGP Configured	Enabled	Enabled
MAC Addresses Learned	4	3 (-25.0%)

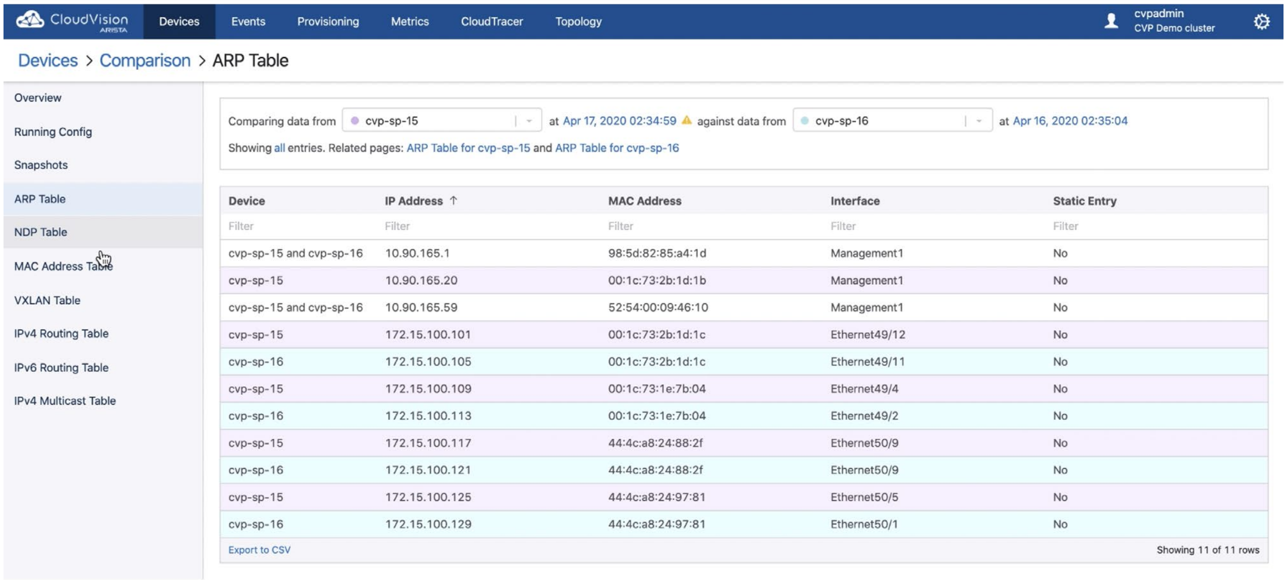
Export to CSV

Showing 8 of 8 rows

Figure 22: Using Snapshots for Device Comparison Views

This functionality can be viewed on a per device basis as 'Historical Comparison'. Historical comparison tracks deviations from an established baseline for key metrics that network operators typically track per device such as CPU utilization, peering status for BGP, MLAG, and entry count for MAC, ARP, and routing tables. In addition to these device states, users can also capture outputs of CLI commands periodically and review the differences between outputs in a user-friendly rendering that highlights the differences. Continuous snapshots leverage the state repository to automatically track and compare changes in device state which provides a starting point for the network operators trying to identify what's changed in their network.

This 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. This is also often the task that consumes the most time when done using a device-by-device approach. 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 and summarizes the metrics for layer-2 and layer-3 tables such as ARP, MAC, IPv4 Routing, and IPv6 Routing tables. The views offer a user-friendly way to identify exactly what entries were removed and added between the two points in time making it easy for network operators to focus on the changes rather than spending time parsing data trying to identify what has changed over time.



Comparing data from cvp-sp-15 at Apr 17, 2020 02:34:59 against data from cvp-sp-16 at Apr 16, 2020 02:35:04

Showing all entries. Related pages: ARP Table for cvp-sp-15 and ARP Table for cvp-sp-16

Device	IP Address ↑	MAC Address	Interface	Static Entry
Filter	Filter	Filter	Filter	Filter
cvp-sp-15 and cvp-sp-16	10.90.165.1	98:5d:82:85:a4:1d	Management1	No
cvp-sp-15	10.90.165.20	00:1c:73:2b:1d:1b	Management1	No
cvp-sp-15 and cvp-sp-16	10.90.165.59	52:54:00:09:46:10	Management1	No
cvp-sp-15	172.15.100.101	00:1c:73:2b:1d:1c	Ethernet49/12	No
cvp-sp-16	172.15.100.105	00:1c:73:2b:1d:1c	Ethernet49/11	No
cvp-sp-15	172.15.100.109	00:1c:73:1e:7b:04	Ethernet49/4	No
cvp-sp-16	172.15.100.113	00:1c:73:1e:7b:04	Ethernet49/2	No
cvp-sp-15	172.15.100.117	44:4c:a8:24:88:2f	Ethernet50/9	No
cvp-sp-16	172.15.100.121	44:4c:a8:24:88:2f	Ethernet50/9	No
cvp-sp-15	172.15.100.125	44:4c:a8:24:97:81	Ethernet50/5	No
cvp-sp-16	172.15.100.129	44:4c:a8:24:97:81	Ethernet50/1	No

Figure 23: CloudVision 'Diff Views' Example

Using Network Rollback

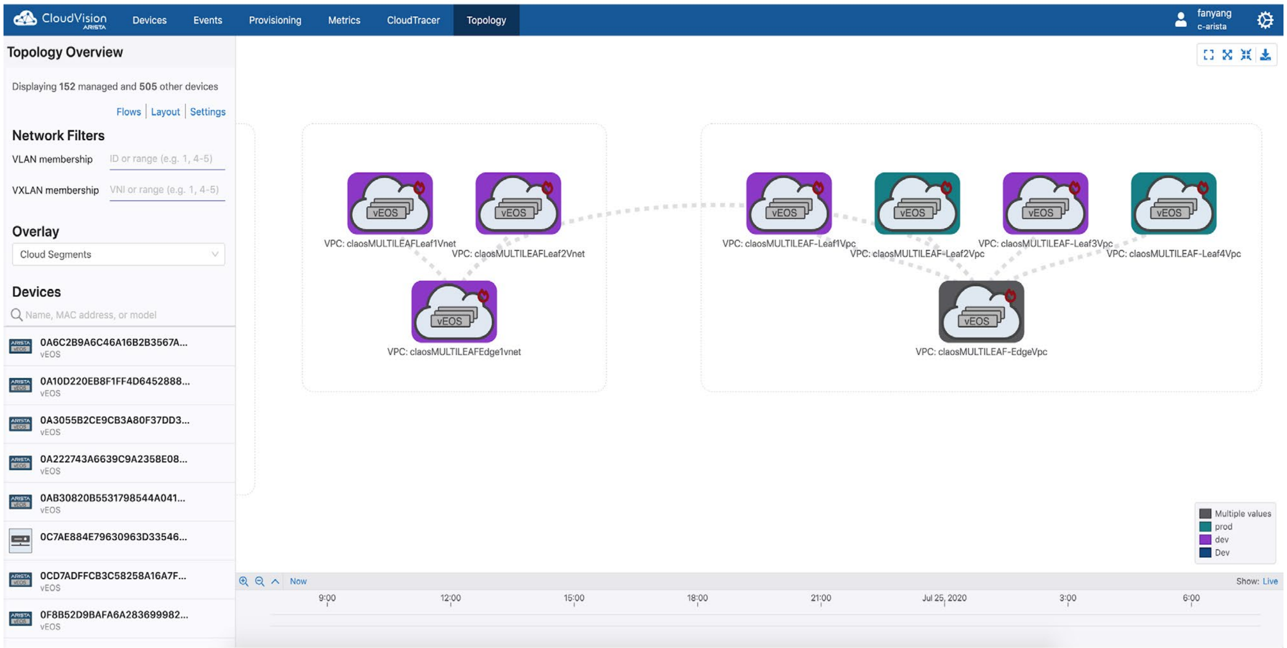
Building on top of the Snapshots, network-wide rollback brings this concept to our maintenance windows for a before and after comparison before the change takes place. All enterprise networks have maintenance windows in order to make changes to adjust to business needs. However, any time a maintenance window or change happens, there may be a need to roll back to a previous configuration for unforeseen reasons. Similar to how with virtualization we have the ability to take a snapshot and rollback to previous dates, Cloudvision now brings this concept to the networking world.

One issue with traditional network operating systems is the inability to easily move between different versions of code, or configuration. Network engineers in the past have used notepad files or spreadsheets in order to accomplish their maintenance windows. CloudVision now allows for an easier approach; leveraging CloudVision's state database allows for quick change between two different states on one, some, or all switches in your network.

Deploying CloudEOS

CloudEOS is Arista's multi-cloud and cloud-native networking solution supporting autonomic operation, delivering an enterprise-class, highly secure and reliable networking experience for the cloud. CloudEOS is the same Arista EOS software image packaged as a virtual machine or a containerized package, and is usually deployed in public cloud and Kubernetes environments to interconnect virtual private cloud (VPC), virtual private network (VNET), and Kubernetes networks.

By integrating Hashicorp Terraform with CloudVision, CloudEOS will be declaratively provisioned and configured in public cloud environments to build out a secure, high performance, and segmented enterprise backbone network in minutes to accelerate enterprise customer's cloud adoption. Once the network is built, CloudVision's multi-cloud dashboard allows customers to monitor their cloud network, including VPCs, VNETs, as well as network performance (latency, jitter, packet loss, and bandwidth) between and across multiple cloud providers. In CloudVision's topology view, customers can visualize the cloud deployments to understand how VPCs, VNETs are interconnected, and what segment those resources belong to for compliance reasons.


CloudVision ARISTA
Devices
Events
Provisioning
Metrics
CloudTracer
Topology
fanyang
c-arista
vEOS
VPC: claosMULTILEAFLeaf1Vnet
VPC: claosMULTILEAFLeaf2Vnet
VPC: claosMULTILEAFEdge1vnet
VPC: claosMULTILEAF-Leaf1Vpc
VPC: claosMULTILEAF-Leaf2Vpc
VPC: claosMULTILEAF-Leaf3Vpc
VPC: claosMULTILEAF-Leaf4Vpc
VPC: claosMULTILEAF-EdgeVpc
Multiple values
prod
dev
Dev
Now
Show: Live
9:00
12:00
15:00
18:00
21:00
Jul 25, 2020
3:00
6:00

Topology Overview

Displaying **152** managed and **505** other devices

Flows | Layout | Settings

Network Filters

VLAN membership: ID or range (e.g. 1, 4-5)

VXLAN membership: VNI or range (e.g. 1, 4-5)

Overlay

Cloud Segments

Devices

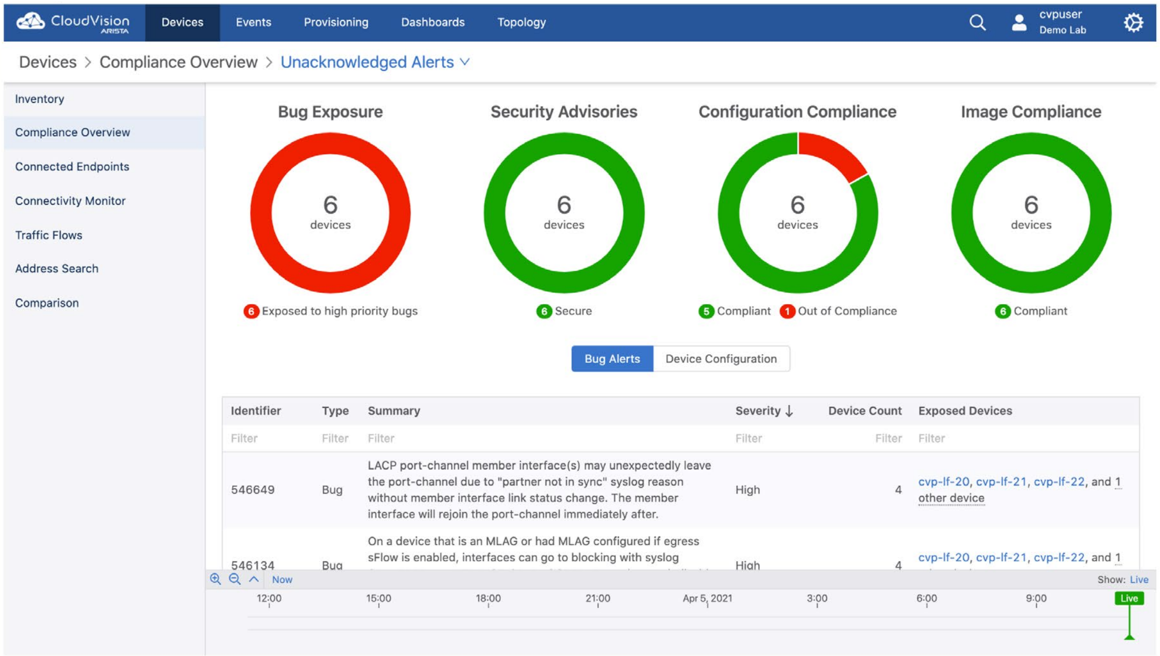
Name, MAC address, or model

0A6C2B9A6C46A16B2B3567A... vEOS
0A10D220EB8F1FF4D6452888... vEOS
0A3055B2CE9CB3A80F37DD3... vEOS
0A222743A6639C9A2358E08... vEOS
0AB30820B5531798544A041... vEOS
0C7AE884E79630963D33546...
0CD7ADFFCB3C58258A16A7F... vEOS
0F8B52D9BAFA6A283699982... vEOS

Figure 24: Topology View Example with CloudEOS Tunnels

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 system is updated in real-time as new vulnerabilities are released allowing a clear measurement of environmental risk and the rapid implementation of compensating controls and patches through the CloudVision upgrade workflow. This enables the enterprise to rapidly remediate these exposures while orchestrating the deployment of the non-disruptive patch or software release in a manner that minimizes or altogether eliminates any outage.



Identifier	Type	Summary	Severity ↓	Device Count	Exposed Devices
Filter	Filter	Filter	Filter	Filter	Filter
546649	Bug	LACP port-channel member interface(s) may unexpectedly leave the port-channel due to "partner not in sync" syslog reason without member interface link status change. The member interface will rejoin the port-channel immediately after.	High	4	cvp-lf-20, cvp-lf-21, cvp-lf-22, and 1 other device
546134	Bug	On a device that is an MLAG or had MLAG configured if egress sFlow is enabled, interfaces can go to blocking with syslog	High	4	cvp-lf-20, cvp-lf-21, cvp-lf-22, and 1

Figure 25: CloudVision's Compliance Dashboard

Compliance dashboard provides a real-time summary view of image, configuration, and security compliance for all managed devices. Compliance tracking for security vulnerabilities provides the user information about potential vulnerabilities and software releases that carry the fix for the same. 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 get the latest information on known software defects through updates from arista.com hence allowing customers 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 can further integrate CloudVision into their existing infrastructure and their own internally sourced management platforms. While customized development is not required to take advantage of the CloudVision platform in most cases, it can be called upon whenever needed.

For Arista partners, CloudVision is a preferred point of network integration for many best-in-class solutions including network virtualization controllers like OpenStack and VMware NSX®, public cloud infrastructures like Amazon AWS®, Google Cloud Platform® and Microsoft Azure®, workflow platforms like ServiceNow®, network security platforms like Palo Alto Networks® and Fortinet® next-generation firewalls, security monitoring tools like Forescout® Zero Trust Segmentation, and many others.

For Arista customers, CloudVision can be customized using the APIs to integrate with customer-developed scripts and programs using python, go, or other languages, and with DevOps workflows using the available Arista-provided CloudVision extensions for open-source automation tools like Ansible and Terraform.

CloudVision APIs

CloudVision's architecture uses standardized OpenConfig data models, where available, as the basis for exposing CloudVision's aggregated NetDB state and telemetry data. CloudVision APIs provide a programmatic method to access CloudVision 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. The CloudVision API Gateway provides access to the Infrastructure Service for all customers, third-party extensions, and Arista-provided applications.

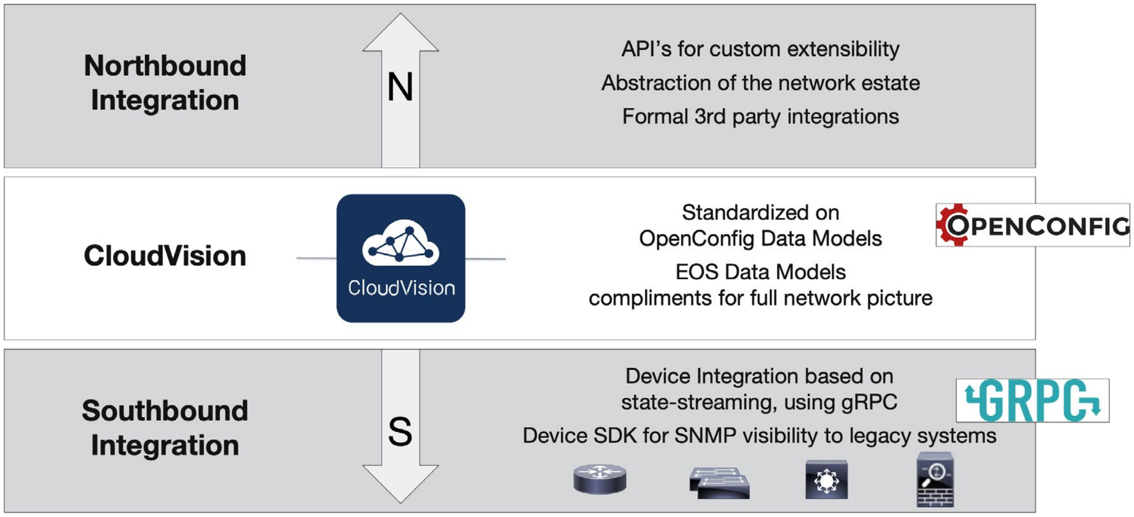

Northbound Integration
N
API's for custom extensibility
Abstraction of the network estate
Formal 3rd party integrations
CloudVision
CloudVision
Standardized on
OpenConfig Data Models
EOS Data Models
compliments for full network picture
OPENCONFIG
Southbound Integration
S
Device Integration based on
state-streaming, using gRPC
Device SDK for SNMP visibility to legacy systems
GRPC

Figure 26: CloudVision Network API Gateway

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. Designing the APIs to use state-synchronization confers some desirable traits:

- Model-driven extensibility - adding a new API simply requires creating a new data model from which the API is derived, making it trivial to adapt usage to new features/APIs. The API gateway provides strong versioning for consistency and backwards compatibility.
- Asynchronous publish-subscribe operations - any action, like a reboot request, is programmed by setting a request attribute. The client can then subscribe to a state attribute, like last-reboot time, to know that the request has been completed.
- State sharing - allows the various components involved in an action not to need to care about each other; they just need to synchronize their subscribed state when they start.
- Portability - by modelling APIs in protobuf and exposing gRPC, this data and management is accessible from nearly any environment in nearly any language. Clients are available in Go and Python, and an ecosystem of open-source tools can be utilized such as BloomRPC or Milkman GUIs, and gRPCurl.

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

Additionally, 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, WeChat, Pushover, and Webhook.

Using CloudVision APIs via the Network API Gateway customers can*:

- Access CloudVision's device inventory and attributes by device list, device attributes, or endpoint search on MAC/IP addresses
- Subscribe to CloudVision events including being able to retrieve event details and acknowledge events
- Access topology data including inventory, compliance dashboards, configurations/configlits, and image bundles
- Access change controls including user-defined CloudVision studios and user scripts
- Access in-app API explorer in the CloudVision Web Portal and built-in documentation

*Some API features may not be available in the current release.

ITSM, ITOM, and AIOps Integration

CloudVision API Gateway and SDK are an extensible platform with rich APIs that drive all of the CloudVision web portal GUI functionality and 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 with the workflow integration between CloudVision and ServiceNow. CloudVision integrates with ServiceNow to allow task and device-related information to flow freely between the two applications. Supported features include ServiceNow Change Request generation and ServiceNow Change Management Database (CMDB) Management. 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. Notes and logs for the change request are seamlessly ported between the applications to provide a complete audit trail. If ServiceNow is used for managing and tracking network devices in its CMDB, the CloudVision inventory feature supports automatic import and the population of switches managed by CloudVision into ServiceNow's CMDB.

DevOps Integration

When managing network configuration changes in a DevOps environment, a number of tools such as Ansible can be used to drive configuration changes through CloudVision. By interfacing with the CloudVision northbound API, DevOps modules like Ansible allow 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.

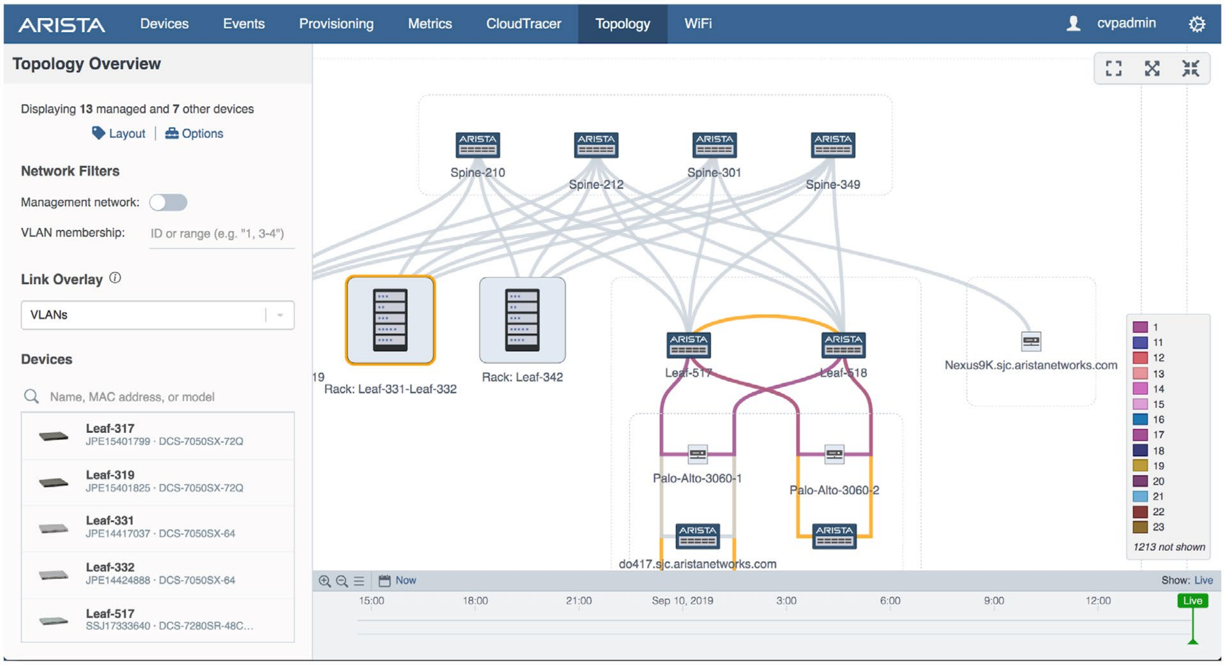
In addition, CloudVision integration with IPAM tools such as BlueCat and Infoblox provides programmatic allocation of IP addresses in CloudVision Configlet Builders, pulling information from a single source of truth.

Device SDK

CloudVision focuses on managing and monitoring Arista devices, leveraging the powerful EOS state streaming and eAPI capabilities. However, in brownfield deployments operators may have third-party devices, which can create monitoring blind spots.

To address these gaps, CloudVision's Device SDK provides support for monitoring third-party devices. Arista has standardized on gRPC and OpenConfig as the interface for all devices in CloudVision. This means that devices natively supporting OpenConfig and gRPC gNMI can integrate into CloudVision for visibility as well. The Device SDK also supports legacy devices that only accept SNMP, or other third-party device APIs, by translating into OpenConfig data models prior to streaming to CloudVision.

With the Device SDK, operators can now get end-to-end visibility of network utilization and device errors across a multi-vendor network.



Topology Overview

Displaying **13** managed and **7** other devices

Layout | Options

Network Filters

Management network:

VLAN membership: ID or range (e.g. "1, 3-4")

Link Overlay ⓘ

VLANs

Devices

Name, MAC address, or model

Leaf-317
JPE15401799 · DCS-7050SX-72Q

Leaf-319
JPE15401825 · DCS-7050SX-72Q

Leaf-331
JPE14417037 · DCS-7050SX-64

Leaf-332
JPE14424888 · DCS-7050SX-64

Leaf-517
SSJ17333640 · DCS-7280SR-48C…

Figure 27: Third-Party Device support visualization

Overlay Controller Integration

Most SDN controllers are focused on the overlay network itself and are not tightly coupled with the underlay network.

CloudVision provides that openness to serve as a central integration point to 3rd party controllers, such as VMware NSX or Openstack etc . CloudVision also provides a more scalable solution as it does not require the controller to talk to every single network device. Instead, the SDN controller simply talks to CloudVision's central integration point, which will then communicate the overlay information to the rest of the VTEP devices.

In addition to supporting OpenStack integration, CloudVision is fully open to supporting any customized controller that the customer may want to deploy. This provides the customer the choice of not being locked into any single overlay vendor.

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.

MSS-Group Service

As part of the MSS solution set, MSS-Group applies authorization policies to security segment groups rather than interfaces, subnets or physical ports. IP addresses and/or IP subnets are placed into administratively defined security segment groups. The ability to create security segments and to enforce policies between segments is built into the Arista switch's hardware.

CloudVision provides the orchestration mechanism for pushing consistent policy to all Arista switches performing MSS-Group enforcement. The security policy may be defined within CloudVision or through CloudVision integrations with a dynamic identity layer. By leveraging APIs available in CloudVision, partners such as Forescout can ensure that different devices are put into logical groups based on device fingerprints, behavior, 802.1X authentication and other mechanisms.

MSS Firewall Service

MSS Firewall is an MSS offering that enables an administrator to logically insert a Fortinet, Palo Alto Networks, or Check Point firewall dynamically into the data path for traffic inspection. With MSS Firewall, large data centers can centralize their firewalls in a service rack and insert them in the path between any workloads on-demand or based on a firewall policy. MSS Firewall uses standards-based forwarding to stitch service devices into the path of traffic, and it can fully function if the network is composed of devices from multiple vendors.

MSS Firewall can also be used to segment north-south traffic on the campus network. In campus use-cases, MSS Firewall is used to restrict traffic to secure applications and to guard against denial of service, DOS, attacks. Similarly, MSS Firewall can also be used to add additional inspection before a device is trusted or if the subject is deemed to be risky.

MSS Host Services

Arista and VMware have partnered to integrate VMware micro-segmentation technology with Arista MSS Host. The solution provides a single administrative domain to manage both VMs and physical workloads. Applying the security policy at the network edge for the physical workloads brings uniformity and consistency. In operation, Arista MSS Host will register with the VMware NSX controller and receive the policies. CloudVision will appropriately program the Arista switch or switch pairs to allow or deny conversation between the physical and virtual workloads. This allows for dynamic synchronization of security policies as new policies are created and existing policies are modified. The MSS Host and VMware NSX solution allows enterprises to secure all assets with uniform policy implementation at scale, mitigating the overall risk and delivering agile services.

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.

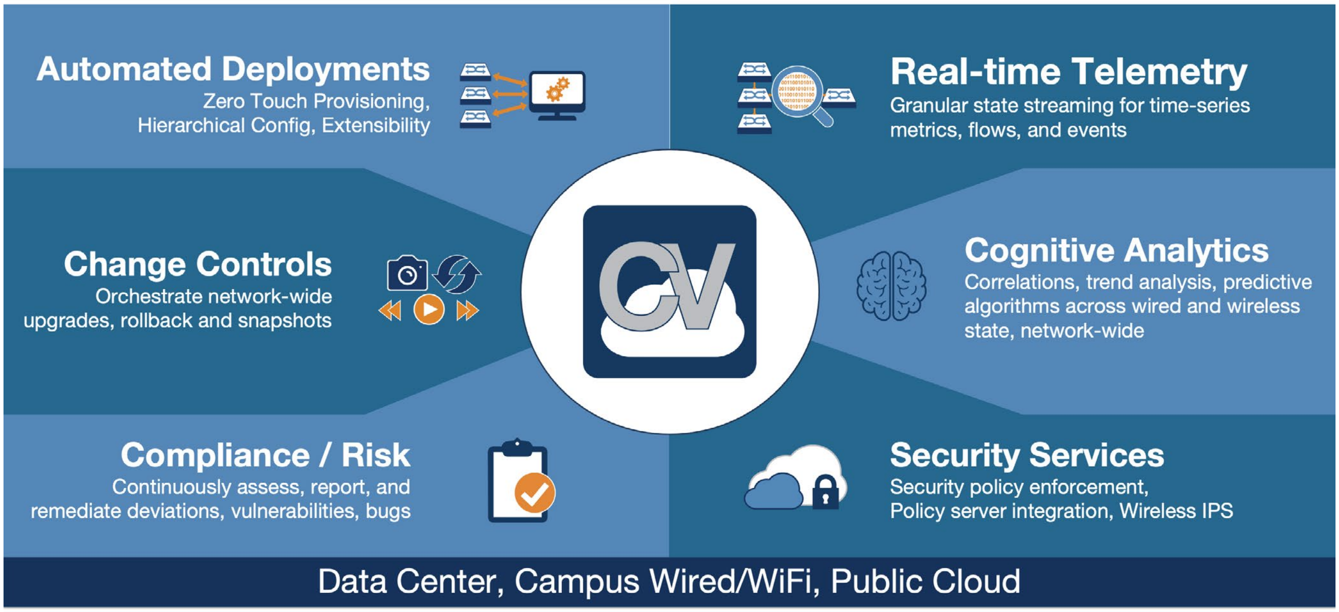

Automated Deployments
Zero Touch Provisioning, Hierarchical Config, Extensibility
Real-time Telemetry
Granular state streaming for time-series metrics, flows, and events
Change Controls
Orchestrate network-wide upgrades, rollback and snapshots
CV
Cognitive Analytics
Correlations, trend analysis, predictive algorithms across wired and wireless state, network-wide
Compliance / Risk
Continuously assess, report, and remediate deviations, vulnerabilities, bugs
Security Services
Security policy enforcement, Policy server integration, Wireless IPS
Data Center, Campus Wired/WiFi, Public Cloud

Figure 28: CloudVision, a multi-function network operations platform

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 be able to manage a network infrastructure network-wide 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 & B, 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