CUMULUS

The Future of **Network Visibility**

The Need for a High-performance Cloud Network

The explosion of cloud services and products is putting new demands on networks and infrastructure to scale and support high-availability applications. This also means that IT and networking staff are under unprecedented pressure to make sure their infrastructure is up to the task of delivering applications and services without failure.

One of the key potential bottlenecks of the high-performance cloud infrastructure is the network. In order to improve applications performance in the cloud, networks need to be optimized to adapt to changing application demands and cloud networking configurations.

The network for the new cloud infrastructure, whether it is built for private cloud, public cloud, or hybrid cloud, has new requirements to support the rise of cloud applications. These requirements include the following:

Cloud-native Architecture

Unlike legacy network systems that were large built on proprietary architectures for enterprise environments, the modern cloud network needs to be built on open standards and equipped for multi-vendor interoperability on open platforms.

High Visibility

In order to support application performance and the dynamic nature of the cloud, the modern cloud network must be equipped with sophisticated instrumentation and telemetry to deliver more automation and fault tolerance into the network.

Support for the NetDevOps Approach

The next cloud network must be built on a foundation of programmability, with networks supporting the cloud approach of DevOps and cloud-native technologies such as Linux, containers, and virtualization. This architecture, called NetDevOps, can enable flexible components for a real-time response to changing needs.

Technology is evolving to support these goals. As data centers have moved increasingly toward open standards, inter-operable, IT-based platforms, and open APIs, it has set up many opportunities to ingest data from telemetry, build analytics programs, and progress toward a more automated, fault-tolerant networking infrastructure.

1 Building Visibility with Data and Telemetry

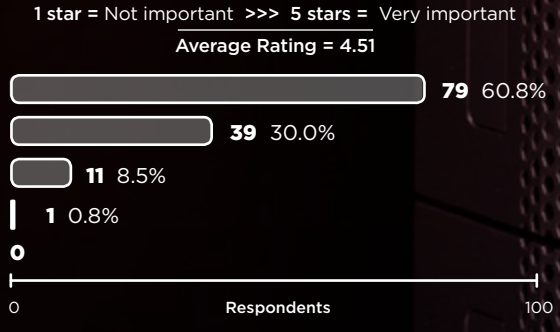
Visibility into the activity of the data center, including how networks and infrastructure are interacting with applications, has become key to building in fault tolerance and automation. Network architects using web-scale approaches want to build in the capability to monitor everything happening in the networking infrastructure to provide fault-tolerant features.

The first requirement to building a responsive cloud architecture is more data, gathered using many techniques. As they say, data is in the new oil. Or you can also think of it as the new gold – the rich resource required to build software innovation and automation.

The volume and diversity of data and dependencies in cloud- and webscale networks means ever-increasing complexity, making diagnosing faults more challenging. This is where the wealth of data and analytics technology can become the network managers friends. The more data and telemetry that can be collected, the better the opportunity for building in self-healing and automation functions.

A recent online survey of 130 webscale and communications network operators conducted by Futuriom revealed networking telemetry, monitoring, and analytics are considered essential for delivering network automation, according to 90% of those of those surveyed. Specifically, 61% rated those components "very important" and 30% rated them as "important" (30%) to network automation.

Please rate the importance and priority of using a combination of network telemetry, monitoring & analytics to drive network automation.



Why do the builders and managers of network environments have so much interest in telemetry, monitoring, and analytics? In order to build automation and fault-tolerant technologies, large amounts of data – both real-time and passive – are needed to fuel the analytics software that can facilitate network automation. The data provides the visibility into what's going on inside the cloud network. This data must be gathered from multiple vectors and domains. Without rich sources of real-time data and telemetry monitoring, it's impossible to build analytical models to drive automation.

Think of an airplane on auto-pilot. Autopilot systems are driven by telemetry and instrumentation. If the plane only has a couple of data points — say winds peed and altitude — this is not enough information on which to operate. Airplane autopilot systems require hundreds of real-time data inputs in order to change to adjusting conditions.

In order to drive automation in networking, the same principles of instrumentation must be applied. The more telemetry data that can be collected, the more sophisticated analytics and automation models can be built. Let's take a look at different approaches to building this automation into a cloud networking system.

Active vs. Passive Monitoring

Consider again the self-flying airplane, or a self-driving car. These systems require real-time data input, or active and passive monitoring.

The quality of the automation will always be a product of the quality and frequency of the data gathering. To create high-quality telemetry data for analytics models, it's important that cloud networking systems move to build both active monitoring and passive monitoring system.

Passive monitoring is common in both IT and networking departments and consists of using specific tools to gather performance and load data from both applications and networking devices such as routers, switches, or servers. In the networking domain, they can be used to tap into network flows using either hardware or software techniques and common protocols such as Simple Network Management protocol (SNMP) or NetFlow.

Passive monitoring is useful to gather large amounts of data from devices about user activity. However, it can often be limited by domain (networking hardware, with the exclusion of applications, for example) and is based on actual networking activity at the time. Think of it as a series of snapshots in time to gain insight into activity on the network or in the cloud.

Active monitoring uses scripts or emulation approaches to generate data about scenarios that can be manufactured. This is often referred to as "synthetic data" that can be injected into a cloud network and system to record the impact that specific environments might have on the infrastructure. An active monitoring approach can be used to build proactive analytics models to predict potential problems. By using an active approach, managers can test scenarios and build infrastructure to support a variety of real-world activity.

Building an intelligent cloud network to drive automation through network visibility requires both active and passive approaches. It's important to gather real-time user, network, and system data with a passive monitoring approach. And it's also important to use active monitoring to test application and user scenarios to build more robust systems. If one adheres to the approach of collecting as much data as possible to feed into systems, it's important to collect data using both active and passive approaches.

Polling vs. Streaming Telemetry

Another way to segment telemetry data is to consider polling or streaming approaches.

For example, of the most common uses of polling data is SNMP which might collect a variety of data fields such as availability, utilization, delay, throughput, and errors on network devices and servers. The data is stored in a Management Information Base (MIB) as a standardized data set. Devices are set up to "poll" or pull data from devices into this MIB.

The primary concern about the polling approach is that it collects data at specific intervals. This means that there may be certain gaps into the visibility of activity. For example, what if a major event occurs between intervals? These create data "blind spots" that can miss significant events.

Polling systems may also introduce scaling or security issues. In a large cloud network, for example, an analytics or visibility system must support polling data being collected large numbers of devices. This data must be quickly gathered and processed to keep up with fast-paced environment of the cloud. On the security front, network traffic data is always a key target of security incursions, which might be gaining access to MIBs and devices in the cloud to find important network data, such as the location of devices and their IP addresses.

Unlike polling telemetry, streaming data telemetry pushes the data out in real time from the source rather than waiting to pull it at intervals. The chief advantage of streaming telemetry is that it can be configured to push performance data in real-time to gain a more accurate view of activity in the cloud network. This telemetry can be fed into analytics programs using standard data models such as YANG or JSON.

Although both polling and streaming data is useful, streaming data is becoming far more important in webscale networks that need to assess network activity on a real-time basis so that it can drive automated provisioning and orchestration systems that can react to changes on-the-fly.

Proprietary vs. Open architectures

One of the key benefits of modern cloud infrastructure is the evolution toward more open systems that can gather data across a variety of platforms including networking devices, operating systems (OSes), and virtualized resources such as virtual machines and containers.

One of the key components of cloud systems, including both servers and networking devices, are OSes. In legacy systems, server and networking OSes are often proprietary in nature, built to work in a single-vendor system. In a proprietary architecture, it might be more challenging to gather data from systems that are not compatible.

Modern cloud infrastructure needs to be built on open and modular software components which provide flexibility configuring and operating the networks that connect applications.

This movement has many customers to look at the opportunities to adopt open networking platforms, often based on Linux OS systems that are familiar in the IT world, so that networking and cloud systems can be more deploy integrated. A key reason for this is that the Linux ecosystem is dependent on a wide variety of open tools and APIs.

Proprietary architectures and closed systems are becoming a thing of the past in the IT world, because they limit the ability to share data and connectivity using open APIs. Open systems that can more easily share information and data are the to building a network and cloud with deep visibility.

Dynamic Data Collection

When you combine the visions of a more diverse set of telemetry, open APIs, and the emergence of open IT systems, it creates more possibilities for telemetry and data collection.

A cloud-response networks needs to gather telemetry from a variety of techniques, including active and passive, as well as multiple domains (compute, storage, network, applications). Ideally, the network is collecting data from all these sources on a variety of metrics that might range from device CPU, bandwidth speed, to packet activity.

The key drivers of this movement will include the following developments:

1. The growth of standardized and open platforms by the cloud providers, communications service providers (CSPs), and SAAS to build consistency of IT tools and services, increasing interoperability and applications portability (e.g. hybrid cloud).
2. The spread of Linux tools and DevOps culture from the core of the cloud into all areas of IT and networking, including CSPs and enterprise to create a NetDevOps culture. The proliferation of Linux and open-source tools speeds up development and interoperability of systems.
3. Wide adoption of telemetry and data APIs supplies a plethora of data that can be used by analytics software that can employ machine learning and artificial intelligence (AI) to drive automation.
4. The emergence of fault resolution approaches such closed-loop monitoring than can predict and resolve potential issues, providing automated fault resolution.

2 Key Benefits of Cloud Visibility

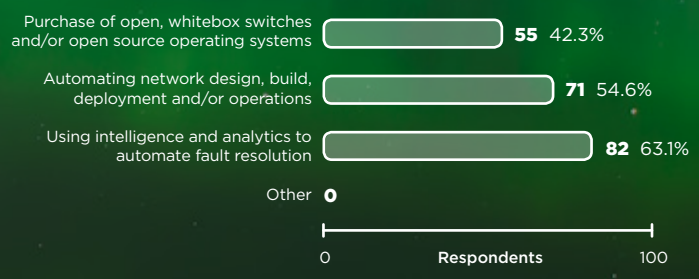
As networks adopt these key trends of increased telemetry and monitoring capabilities, wide implementations of open systems and APIs, and more interoperable systems is creating many opportunities to deliver automation.

Customers in the cloud world see the next wave of network automation support the growth of more resilient, fault tolerate infrastructure.

Automation drives productivity. It can also deliver services in a more cost-effective manner by reducing the number of resources and people needed to manage a cloud infrastructure. This enables enterprises and CSPs to focus on more important business goals, such as designing and launching new services and driving revenue.

A recent Network Automation Survey of 130 CSPs and cloud providers by Futuriom found that the top goals of automation were faster service delivery and increased revenue (79%), improved network security (75%), and improved ability to support dynamic/on-demand services. Secondary goals were reducing both operational costs (41.5%) and capital spending (37.7%).

Where would you like to implement network cost savings over the next 6 to 24 months?
(Choose all that apply)



It's clear that CSPs and enterprise cloud providers would like to reduce the costs associated with managing their network infrastructure, but they are even more interested in finding ways to speed up the velocity of their business by delivering services, increase revenues and secure their infrastructure.

Let's take a look at each of these benefits individually.

White-box and Capex Savings Drives Standardization

Although it's not top of the list of priorities for cloud architects, one key benefit of moving to open, standardized commercial off-the-shelf (COTS) hardware is that it lowers the overall capital expenditure (capex) of the network. Research shows that this is an added benefit of moving to open networking hardware with disaggregated OS and hardware components.

As cloud infrastructure architects look to lower costs, it benefits the industry overall. Standardized hardware means that chip and server companies can develop technologies at scale, lowering the cost for everyone. But the real benefit from this trend is that it drives the industry to using standardized components, setting the table for interoperability and add-on effects such as visibility and programmability.

Opex Savings by Fault Resolution

Research shows that as much of 80% of networking outages are caused by human error. Therefore, automation and fault resolution have the potential to massively reduce Opex costs.

As you can see above using analytics and network intelligence to automate fault resolution is a goal of 63% of the CSPs (cloud and communications service providers) surveyed. The key for building automated fault resolution are network visibility.

On order to drive automated fault resolution, network architects are building layers of software on top of their network architecture to gather and process network telemetry in analytics engines. This will be a key development going forward that is of great interest to end users looking to drive down the Opex of their networks.

Creation of a NetDevOps Culture

A combination of the many cloud trends is driving convergence between the previous isolated domains of networking, IT, and security. Functions in the cloud are being abstracted into software, so they can be supported by a wide range of powerful, open hardware.

The foundation of the cloud is a wide-variety of IT tools, many of them coming from the open-source community, based on Linux. Some of the tools include Telegraf and Prometheus, which are considered “Swiss Army Knives” for collecting data. Another key trend is building apps in containers, which leverage Linux operating systems by virtualizing the operating system. These trends mean that more emphasis in the future will be placed on building a standardized NetDevOps environment that is compatible with Linux-based IT approaches that are becoming the de factor standards of the cloud.

In the future, the networking, IT, and security departments of enterprises will increasingly look more like those of the webscale world: A single, collapsed team with diverse skills in DevOps, networking, and Linux-based technologies.

Improving Cloud Design and Operations

Cloud is a key driver of the IT industry. Overall, cloud computing is projected to increase from $67 billion in 2015 to $162 billion in 2020, with compound annual growth rate (CAGR) of 19%, according to a cross-section of industry research.

One of the key approaches to building cloudscale operations is that the infrastructure can be based on standardized and modular designs, it can be “scaled out” quickly to support growth.

The capability to scale out fast is convenient, but how does a business or organization plan and manage that? One of the key areas of interest in planning and design of infrastructure is intent-based networking (IBN), which uses software driven by data telemetry and analytics to predict business needs and facilitate the planning and design of networks and clouds to support operations and business goals.

3 The Open Network Ecosystem: Sample Case Studies

Cumulus Networks claims 34% of the Fortune 50 as customers. What is behind the high success rate? One of the reasons is the approach to facilitating network visibility by building an open ecosystem that can enable data telemetry, monitoring and automation to network cloudscale environments.

Cumulus has published dozens of case studies of its systems demonstrating successful adoption of its products. A review of these case studies reveals several themes: The customer like the consistency and interoperability with existing Linux toolsets, the potential for automation in configuration management, and the potential for increasing network visibility using NetQ. Below are a few select examples of how an open ecosystem can be used as a foundation for better network visibility.

Adobe. Features for automation and policy management

NTT. Wataru Ishida, an engineer with NTT, said that the open approach of Cumulus Networks has had an important impact on the network, enabling flexibility and low operational cost. Ishida points out that it's important to have a Linux-based OS in the network that can support cloud-based technologies such as Kubernetes, Calico, Docker, and GoBGP.

LogicMonitor. Andrew Martin, Network Engineer at LogicMonitor says that Cumulus Linux enables automated configurations and policy management with standard Linux tools such as Puppet and Ansible. This enables the team to leverage existing Linux toolsets rather than hiring hire people with specialized knowledge in proprietary networking gear.

SmartGames Technologies. Bernd Malmqvist, Tech Lead Systems Operations with SmartGames says it is using Cumulus NetQ for increased visibility using check commands to see what is happening on the network. "The benefits to us are early alerting and validating the entire state of the fabric. Monitoring is one thing, but with NetQ, the knowledge is instant," says Malmqvist. "NetQ is really unique; it's a tool that tells us exactly what is wrong in our environment, and the insight to know where an issue is stemming from."

LightSpeed. Joshua Holmes, CEO of Ethode, a LightSpeed hosting company, says that application integration and higher visibility was one of the key advantages to Cumulus, in addition to reliable support and attractive cost. "You can see stuff you never see with a proprietary vendor." He says they can monitor and detect more data and applications traffic using a Cumulus Linux-based system, including sophisticated UTM detection that is used for clients who have HIPPA and other compliance requirements.

Yahoo Japan. Kenya Murakoshi, general manager of network infrastructure for Yahoo Japan, the operator of a major web portal offering more than 100 web-based services, points that open, cloud-scale technologies are better equipped to handle the enormous growth of traffic driven by applications such as Hadoop and Internet video. Murakoshi says Yahoo Japan was interested in Cumulus because of its open approach the networking and the leaf-spine architecture that can be quickly plugged into the network in adaptable fashion.

Conclusion

Integrated networking telemetry, monitoring, and analytics will spawn a new era of networking innovation. Techniques for combining active and passive monitoring and data collection from multiple domains of the cloud infrastructure are the key to this innovation.

Networking visibility is providing the foundation for a layer of network intelligence that will enable it to be programmed to respond to fit the intent of applications, rather than being manually configured (which can result in it frequently breaking). This is key to development of new fields of network automation such as IBN and intent-based analytics.

The key result of the new network visibility will be to reduce the operational cost of running network infrastructure and optimized the planning and investment of networking infrastructure to adapt to cloud applications.

Learn about Cumulus network visibility solutions