SDxCentral

Special Report: Network Performance Management (NPM) in the Cloud Era

Table of Contents

What matters to them is a reliable digital experience.

Next-generation networks demand next-generation assurance.

CA Virtual Network Assurance

SDN/NFV performance and fault management.

Learn more at ca.com/vna

ca technologies

market summary

Intro: Network Performance Management (NPM) in the Cloud Era

The landscape for application performance management (APM) and network performance management (NPM) tools has changed enormously over the last few years, driven largely by changing infrastructure and application architectures.

The industry as a whole, including enterprises, service providers and vendors, is grappling with difficult performance management issues. How do you monitor, analyze and optimize the behavior of highly distributed, virtualized, cloud-based systems built of ever smaller components such as containers and micro-services?

SDxCentral recently examined the trends that are re-shaping the APM and NPM markets and driving the need for integrated APM/NPM solutions. This special report focuses on some of the findings specifically in the NPM area.

Trends Impacting NPM Solutions

A variety of trends are driving the NPM market to evolve and keep pace with modern technologies and the digital experience. Some of these trends include:

- Adoption of hybrid data center architectures and cloud-based services and applications is driving the need for cloud support in NPM tools, including end-to-end views of application transactions
- Strong uptake of SDN and NFV to automate provisioning is driving the need for performance management to follow
- Relentless growth in network traffic, fueled by video, Internet of Things and other applications is driving the need for scalable tools that can collect and analyze very high volumes of application and network traffic and performance data
- Rise of the “consumer user” is driving the need for transaction-oriented end-user experience metrics
- New software development approaches such as DevOps and containers is driving the need for closed-loop monitoring and visibility into application components and their interdependencies

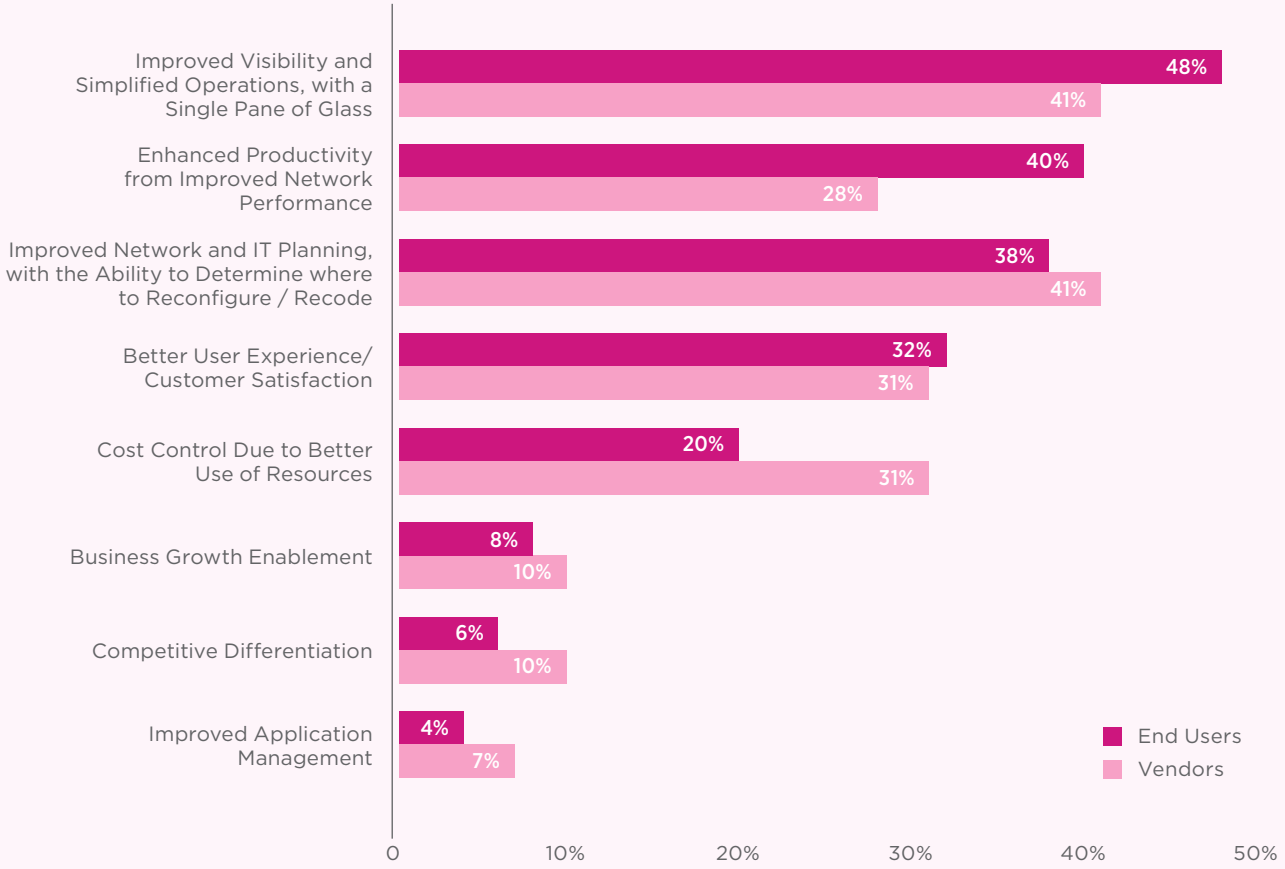
User Feedback on NPM Market

SDxCentral conducted a survey asking the community to weigh in on the NPM market. Of the 79 respondents to the survey, 37% were technology vendors; 24% telecommunications service providers; 19% enterprise end-users; 9% were cloud service providers; and 11% other. Figures in this report sort these results into two groups of respondents: technology vendors and end-users/customers (which includes enterprises, telecommunications service providers and cloud service providers).

When asked to rank the principle benefits of NPM technologies, respondents identified improved visibility and simplified operations as the biggest value (48%). They also cited enhanced productivity from improved network performance (40%).

market summary

PRINCIPLE BENEFITS OF NPM TECHNOLOGY



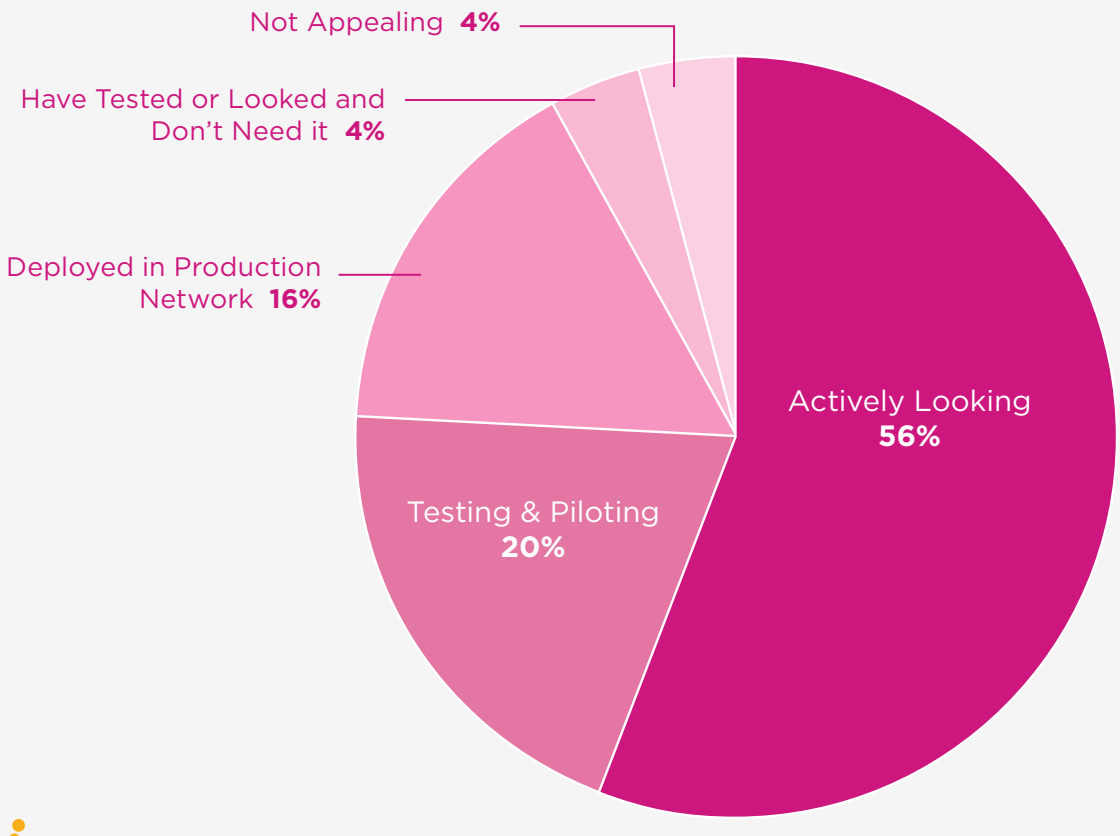
Respondents could choose their top two principle benefits.

sdxcentral.com

market summary

Recognizing the benefits of network performance management, respondents overall express a high level of interest in NPM solutions and tools. More than half are actively looking at NPM solutions, and roughly a third are in the testing and deployment phases of adoption. Another 20% are currently piloting NPM solutions, while 16% have already deployed them in a production network.

NPM INTEREST-LEVEL



Results from 50 End Users.

sdxcentral.com

Market Challenges Impacting NPM

NPM markets are changing rapidly, as influenced by the above trends. Many of these factors are having a specific impact on NPM. Below are some of the key trends.

Adoption of Cloud Architectures

Cloud architectures are increasingly popular for the data center, especially hybrid clouds that combine on-premises resources with public cloud-based services. A recent survey conducted by IDG Research Services found that 83% of respondents currently use or plan to use a hybrid cloud **environment**.[1]

On the plus side, hybrid clouds let enterprises instantly expand resources or spin up a new application, often at considerable savings compared to in-house deployments. However, use of public cloud services makes end-to-end performance management a challenge since network operations often have little to no visibility into traffic in the cloud, nor can they control it. The lack of end-to-end visibility across public cloud and on-premises infrastructure is one of the key challenges to deploying hybrid clouds.

Another challenge is that clouds, by their nature, are highly dynamic. Cloud management software can provision entire application systems automatically, while deployment tools like Puppet can update thousands of virtual machines simultaneously. Monitoring this dynamic resource usage and tracking the various network paths present in hybrid environments is difficult, making it hard to diagnose application and infrastructure performance issues.

Uptake of SDN and NFV

Adoption of software-defined networking (SDN) and network functions virtualization (NFV) technologies are contributing to the need for advanced performance management solutions. Many enterprises and service providers are already using SDN in their data centers to automate provisioning, benefiting from lower operational overhead and the ability to respond dynamically to business and application demands. Similarly, by separating network functions into discrete elements that can be activated and managed in software, NFV makes the IT infrastructure more flexible and scalable.

However, making resources and services immediately available presents performance management challenges. For example, traditional network management tools only run discovery operations periodically, creating significant visibility gaps in SDN and NFV deployments. Automating changes or instantiating user-demanded services without knowing whether the network can fulfill these requests is risky, as they could be provisioned over paths that are near the saturation point. Likewise, changes to one component in an SDN or NFV environment can affect many other components; performance management tools need to provide visibility into these interdependencies.

Impact of Network Traffic Trends

Changes in the volume, type and duration of network traffic are also having an impact on the type of performance management tools needed. Traffic volumes continue to climb. Video traffic, in particular, is escalating, both for consumer and business use (Netflix and YouTube now account for over half of all broadband traffic during peak hours). Uptake of VoIP, graphics-heavy social media sites and applications such as Snapchat and Instagram, as well as peer-to-peer file sharing are also contributing to rising traffic volumes.

Internet of Things (IoT) devices as diverse as store kiosks and smart watches are also adding to network traffic loads. It's estimated that the number of IoT devices could reach as high as 50 billion nodes in 2020, driven by both commercial and consumer use cases.

[1]Source: http://apmdigest.com/application-performance-hybrid-cloud-1

End User Expectations

In the era of the "consumer user," employees, end customers and other users have come to expect anywhere, anytime access to content and applications with performance equivalent to a wired connection (or, put another way, "I want it now!). Research shows that just a one-second increase in page response time can decrease page views by 11%, cut customer satisfaction by 16%, and decrease revenue by 7%.[2]

Applications Trends

In contrast to yesterday's monolithic applications, today's apps are built with reusable components and are highly distributed, often with components spread across on-premises data centers and public clouds.

Development approaches such as DevOps allow IT to build, test and deploy applications much faster than in the past, so the pace of application development and deployment is accelerating. Container software systems such as Docker are being used to create large platforms for distributed apps, as well as to develop microservices, which execute in containers. Some containers address each other's workloads through API calls, while other container systems rely on network functionality to connect their distributed parts.

Many organizations are now managing application ecosystems composed of hundreds or thousands of foundational elements, with transactions executing across heterogeneous software platforms, networks, databases, and legacy technologies. As enterprise applications become more componentized and networked, an understanding of the relationships and dependencies between infrastructure and application elements has become critical to performance management.

Requirements for Products in the New NPM Market

Given the critical role applications play in business success, a key goal for enterprises and service providers is to ensure the best possible network performance. Poor performance can originate in the network, servers, application logic, database or other areas. Trying to pinpoint the cause is increasingly difficult since applications change rapidly and now run on a highly dynamic, automated and increasingly virtualized infrastructure that's often distributed across on-premises and public cloud infrastructure.

In today's world, applications and network performance have become more intertwined than ever. It's no longer sufficient simply to monitor discrete network elements, such as CPU/memory utilization, device pooling, packet loss and jitter, and to infer application performance from resource utilization. In addition, the dynamic nature of today's virtualized infrastructure means IT can no longer count on a static topology as a source of monitoring data.

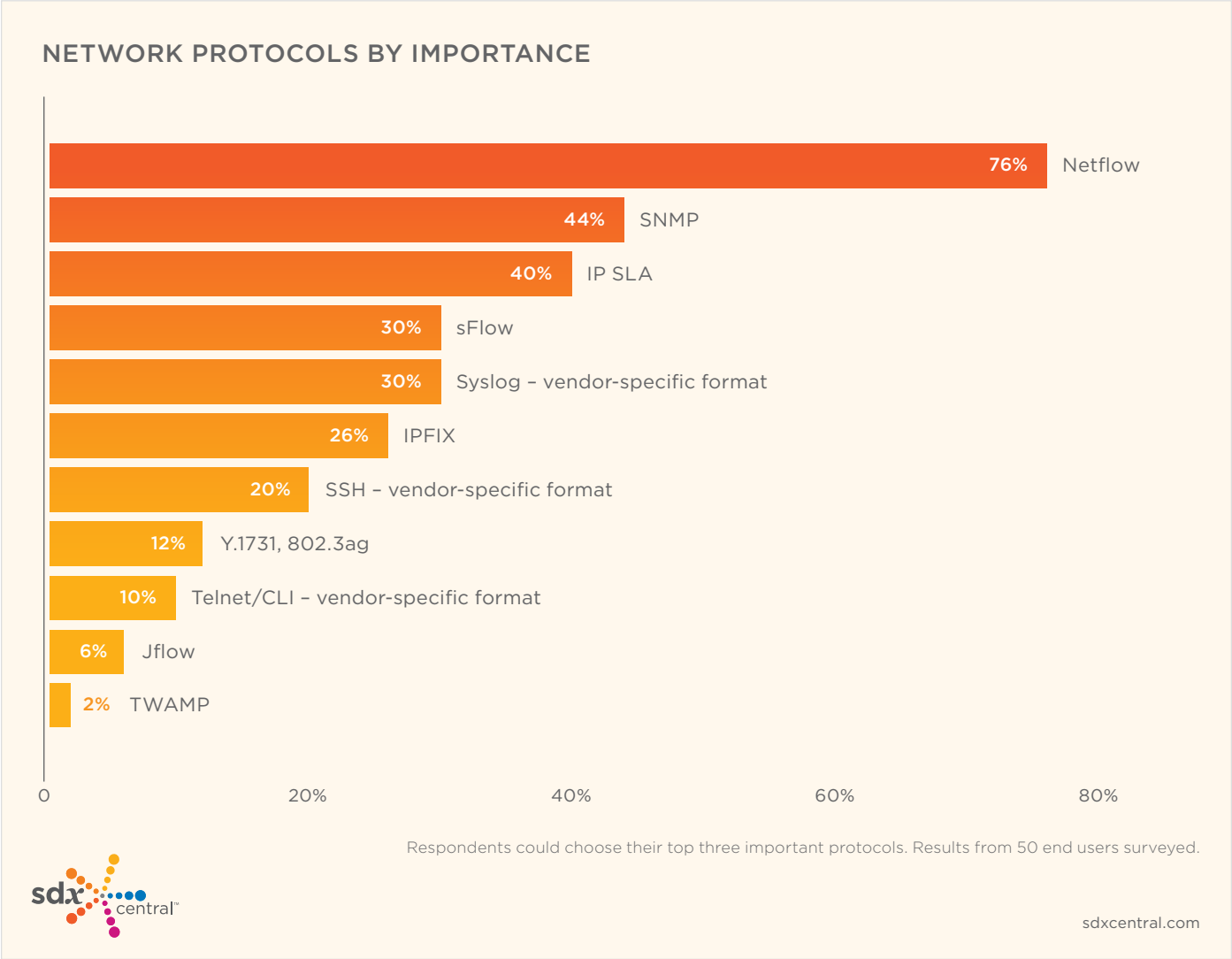
Below we highlight some of the key requirements for modern performance management solutions.

[2]Source: Riverbed - The Aberdeen Group.

The Type of Monitoring Data Collected

Wire data is created by reassembling network data into full streams and providing payload analysis and full context in real time. That's why wire data is an especially good source of accurate information about behavior events across the entire IT infrastructure and application portfolio. In fact, because packet header information in wire data can provide direct observations of end-user experience, analysts believe that wire data[3] will play a primary role in availability and performance analysis.

Wire data is also used to understand inter-tier transaction performance. The graph below illustrates the protocols that SDxCentral survey respondents consider most important to monitor.



[3]Source: http://www.packetdesign.com/blog/we-dont-have-the-luxury-of-end-to-end-complacency

How—and How Frequently—Data is Collected: Scalability Challenges

Collecting performance data at scale with the necessary frequency and volume is driving the need for very high-performance monitoring solutions. On the network side, for example, technologies such as packet sniffers, flow analyzers, deep-packet inspection, and network probes must evolve to keep pace with multi-gigabit network speeds. Some vendors have responded by introducing monitoring fabrics.

Monitoring must be done much more frequently than before, with data collection occurring in the 5 to 15 second range to avoid missing important events in the dynamic infrastructure. Increasing the frequency of monitoring also increases the volume of data collected and in need of analysis.

In addition, many industry players see a need for agents, collectors, and other entities that forward monitoring data to use "phone home" techniques to communicate to the back-end management system. Part of the problem is that traditional polling methods can't support the sheer volume of data that needs to be collected; the polling traffic itself could cause bottlenecks.

Some vendors as well as the Principal Architect and Manager of Google's Network Architecture **team**[4] have expressed the need for telemetry in network devices that can "push" status information to management systems rather than the management system periodically polling those devices. Currently, the SNMP agent on a device will only push messages, or traps, to the management system when a threshold, such as CPU or bandwidth utilization, is crossed.

Storing and Analyzing All that Data: More Scalability Challenges

A converged performance management solution will need to be supported by an underlying data architecture that can cope with the arrival rate and quantity of management data collected. Having a common data store is key to enabling data sharing by different performance management tools, whether these are from a single vendor or best-of-breed solutions from different vendors.

Once collected, the data needs to be analyzed and presented. Again, scalability is an issue as the amount of data that needs to be analyzed is quite large. The industry is looking to self-learning analytics and other methods to handle combing through these volumes of data and performing functions such as statistical analysis, machine-learning-assisted pattern discovery, anomaly detection, causal analysis and data visualization.

The Capability to Leverage SDN/NFV

Both SDN and NFV environments need real-time monitoring and analytics so the network software itself can factor performance into the provisioning process. For example, if a given link is performing poorly, an SDN network with performance intelligence can route around it. Likewise, changes to one component in an SDN or NFV environment can affect many other components, so operators need visibility into these interdependencies. In the NFV market, the trend is toward the creation of microservices, which will be connected to one another via network virtualization, creating even more interdependencies.

In SDN and NFV environments, performance management tools need to provide granular visibility into changes occurring in these environments as well as highly scalable relationship analytics to support the many interdependencies.

[4]Source: http://www.packetdesign.com/blog/we-dont-have-the-luxury-of-end-to-end-complacency

Flexible Deployment Options

Customers want business-oriented performance metrics that can be used by multiple stakeholder groups. They also want less complex management interfaces with more sophisticated visualization and drill-down capabilities. Customers are also looking for a flexible delivery model that lets them choose to deploy NPM tools in any combination of on-premises, SaaS, or hybrid implementations, based on their existing platform and business model.

Tackling Performance Management in SDN and NFV Environments

The industry has made progress in addressing the performance management challenges that SDN and NFV present, including key standards work, which is imperative given the roles of these technologies in today's IT infrastructure.

For example, close work between the International Multimedia Telecommunications Consortium (IMTC) and Open Networking Foundation (ONF) has spurred the development of an open source implementation focused on automating unified communications and collaboration (UC&C) quality of experience (QoE). This solution is designed to combine network element information with UC&C session metrics in real-time to provide visibility into an automated problem resolution for voice, video and desktop-sharing sessions in-flight or any period thereafter.

While this is just one use case, it demonstrates how SDN can be used to automatically program dynamic QoS policies across the network on a per session basis. It's also significant because the focus is on the end point, enabling an end user, real-time media application to communicate the bandwidth and traffic treatment it needs, which the network then automatically provisions. At the same time, this solution provides visibility needed for root cause analysis of UC&C quality issues, and automates problem resolution without requiring dedicated probes, synthetics, etc.

The NFV camp has also been busy. For example, the Management and Orchestration (MANO) Working Group of the European Telecommunications Standards Institute (ETSI) has defined an architecture for the management and orchestration of all resources in the cloud data center, including computing, networking, storage, and virtual machine resources. One of the key components of the NFV management and orchestration (NFV MANO) architecture is the virtual infrastructure manager (VIM).

The VIM coordinates the physical resources necessary to deliver network services, which includes: managing compute, storage, network and other hardware resources as well as software resources such as hypervisors; discovery of their capabilities and features; maintaining an inventory of the allocation of virtual resources to physical resources; and orchestrating and optimizing the allocation, upgrade, release, and reclamation of NFV resources.

Many vendors offer VIMs. In addition, OpenStack is often deployed as a VIM: It controls pools of compute, storage, and networking resources that can be managed through OpenStack API. Many vendors have created OpenStack implementations of their own, including Red Hat, Mirantis, Oracle and VMware. Other vendors supply VIM solutions as well as add-ons to OpenStack.

In addition to these industry efforts, some vendors support SDN and NFV within their performance management tools. For example, CA Technologies supports many cloud and SDN/NFV architectures in its CA Virtual Network Assurance gateway, which provides monitoring visibility into the multi-layered cloud and SDN/NFV stack along with their physical network relationships with intuitive dashboards and service-level reporting; at all the scale and velocity that cloud and SDN/NFV architectures demand.

Conclusions: Requirements for NPM in the Virtual World

In today's cloud-based, virtualized IT infrastructure, applications and networks are deeply intertwined. These interdependencies are driving the need for a more holistic approach to performance management.

NPM will be key to delivering reliable, scalable networks for the cloud world. Consequently, vendor approaches to performance management are shifting, spawning new NPM functionality in order to provide an accurate picture.

Here are some of the new requirements:

- Supports cloud architectures
- Collects a variety of data types (log, API, wire, etc.) at very frequent intervals (5-15 seconds)
- Network monitoring able to scale to 40 or 100 Gbps and handle encrypted traffic at line rate
- Highly scalable, including efficient storage and handling of terabytes and petabytes of network traffic and performance data
- Provides visibility into and performance management of SDN and NFV environments
- Supports a variety of monitoring architectures to accommodate different business goals.
- Integrates with DevOps environments for closed-loop monitoring and provides visibility into container-based applications
- Ease of use based on automated, rather than manual, configuration and tagging
- Is programmable, allowing customer to extend the platform or tool's functionality

Featured Product Profile: CA Virtual Network Assurance

As a comprehensive big-data collection and analytics solution, CA Virtual Network Assurance uniquely scales to meet the demands of highly dynamic and complex hybrid-cloud and SDN/NFV networks. The solution extends operator visibility to allow operational and business support teams to proactively and efficiently ensure performance of their new digital networks; resulting in lowering the cost and complexity of service delivery, while accelerating mean time to repair and innovate.

The framework starts with existing fault and performance systems, such as CA Spectrum® and CA Performance Management, to monitor the old network as well as the underlay in the SDN/NFV networks. CA Virtual Network Assurance is then added to monitor the overlay stack. In this decoupled packaging, you can re-use not only existing infrastructure management investments, but also apply operational best practices to SDN/NFV. Examples of operational best practices are UI, reporting, tenant management, device management, etc. With inventory and performance data from the old and new networks managed in the same solution, you now have not only a single pane, but you also can correlate intersecting network relationships.

At the core of CA Virtual Network Assurance is the modeling of cloud and SDN/NFV as a multi-layer stack. By applying this model to the collection, normalization, presentation and analysis of performance data, the solution is able to adapt to the component level dynamic nature inherent in cloud and SDN/NFV networks. This tracking is accomplished through a component level relationship mapping scheme that can maintain an updated network stack, while the tiniest component expands, contracts, relocates, transforms, etc. This is a highly scalable way to track granular changes in dynamic SDN/NFV networks.

CA Virtual Network Assurance supports service chaining and represents collection data, inventories and performance in a service chain view. The key is that, while there are plenty of service chain views in the industry showing the logical (VNF) connections, Virtual Network Assurance visualizes the logical VNF connections as

well as the building blocks that support the service chain for improved operational knowledge and troubleshooting.

CA Virtual Network Assurance conforms to the ETSI model as an extension of the MANO components. The solution participates in NFVO, VNFM and VIM in order to collect the necessary data for service assurance. The data from MANO is not always the same based on system architecture and this is a reconstruction of the puzzle that CA Virtual Network Assurance does in order to produce a uniform data model to network operations.

CA uniquely monitors data flows across the most hybrid network architectures with rich open-API analytics and innovative and customizable visualizations of legacy networks as well as cloud and the SDN/NFV network stack and service chains to make it easy for both experienced and Level 1 operators to resolve problems faster than using siloed and limited tools.

The CA Technologies profile was created through a collaborative effort between SDNCentral's Research Team and CA Technologies product experts. SDNCentral worked under the assumption the information provided by CA Technologies is factual, auditing the submission only to remove unverifiable claims and hyperbole.

CA TECHNOLOGIES

520 Madison Avenue
New York, NY 10022
Timothy.Diep@ca.com
(Director, Product Management)
1.800.225.5224
www.ca.com

PUBLIC

CA Virtual Network Assurance

(Click for Online Version)

www.ca.com/vna

Description of Company: CA's highly-experienced leadership team is committed to helping businesses invent the future with software one innovation at a time. CA continues to create leading-edge IT software and solutions for some of the most powerful companies in the world, including more than half of the Global Fortune 500, the 20 top global banks and the largest 25 federal agencies.

▸ CA Technologies in SDxCentral Company Directory

Description of Product(s):

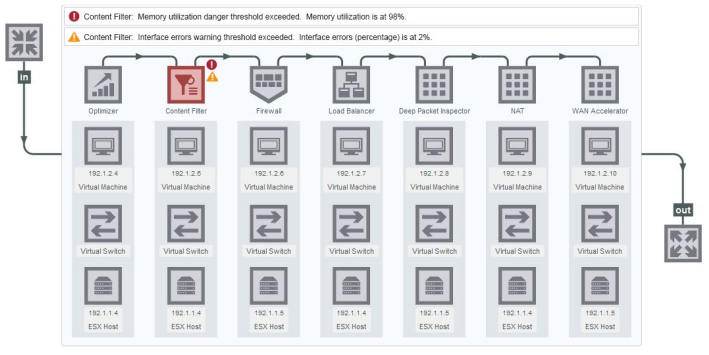
CA Virtual Network Assurance offers next-generation network performance and fault management capabilities to reduce the risk in SDN/NFV deployments. The solution extends network visibility of existing infrastructure management solutions with advanced collection, normalization and detection methods to remove management complexity of the highly dynamic and complex SDN/NFV networks and service chains.

▸ CA Virtual Network Assurance in SDxCentral Product Directory

Unique Value Proposition
CA Virtual Network Assurance aims to operationalize SDN and NFV by producing easy to understand visualization and targeting known vulnerable areas of the new and complex network stack and service chain.
Solution Demand
Financials, Government & Education, Retail, Telecom
Product Areas/Functions
Application performance monitoring; Cloud services monitoring across public, private, and hybrid clouds; Database diagnostics; Mobile device monitoring; Protocol-level analysis; Real-time application monitoring; Real time network monitoring; SDN analytics; SLA monitoring
Monitored Application Protocols
SNMP, HTTP, HTTPS, REST, TFTP, SOAP, TFTP, TCP, UDP
Monitoring Standards Supported
SNMP, Netflow, TWAMP, IPSLA, IPFIX, REST, IPDR via EMS
Maximum Scale
CA Virtual Network Assurance can discover, collect, inventory, store, and analyze up to 2 million entities in 5 minute granularity simultaneously.
Pricing Model
CA Virtual Network Assurance has a flexible pricing model based on physical and virtual devices.

SDN and NFV integration
CA Virtual Network Assurance interfaces through numerous protocols with SDN/NFV controllers, service orchestrators, cloud systems, and individual elements to rebuild the complex network stack into "easy to understand" visuals and dashboards so that operational teams can understand and confidently manage the new network.
Container Infrastructure Integration
CA Virtual Network Assurance can reside in containers as well as monitoring the processes of containers running NFV.
Cloud Integration (Private, Public, Hybrid)
CA Virtual Network Assurance has flexible probes to monitor private, public, and hybrid cloud systems bringing together a single pane for comprehensive analysis.

Service Chain Topology



SDNCentral, LLC
955 Benecia Avenue
Sunnyvale, CA 94085 USA
www.sdxcentral.com

The Trusted News and Resource Site for SDx, SDN, NFV, Cloud and Virtualization Infrastructure

Rev B