ACG RESEARCH

Delivering Management as Agile as the Cloud: Enabling New Architectures with CA Technologies' Virtual Network Assurance Solution

Introduction

Service providers and IT departments of every type are seeking ways to be more agile in meeting their application delivery needs. Their overriding goal is to accelerate their time to results, efficiency and ability to innovate in achieving their goals.

In doing so, operators have strongly embraced the principles of virtualization and cloud computing initially pioneered in data center and web-scale service provider environments and now being incorporated across the network landscape by software-defined networking (SDN) and network functions virtualization (NFV). SDN is opening up, streamlining and making more programmable the previously more tightly coupled and proprietary models used in delivering prior generations of switching and routing in data center and wide-area networks. And NFV is bringing a new paradigm into play for running value-adding network functions such as firewalling, load balancing and deep packet inspection. Using NFV, value-adding functions are deployed dynamically as software modules running in virtual machines on general purpose x86 servers versus in the proprietary, tightly-coupled appliance implementations, which have been their dominant mode of deployment in the past.

KEY FINDINGS

- Service providers and IT departments are seeking ways to increase agility, efficiency and innovation.
- Evolving to the virtualized and more software-driven environments of SDN and NFV is one way they are choosing to pursue this goal.
- SDN and NFV, however, reshape conventional network designs and introduce the need for new management and service assurance tools to handle implementation.
- CA Technologies' Virtual Network Assurance fills an important market need by aligning gracefully with the new virtual designs and also bridging efficiently with existing management systems, allowing new virtual systems to move forward in parallel with what's already deployed.

New Service Assurance Models Required

By using these models, SDN and NFV are enabling the agility, efficiency and innovation that operators and IT teams are looking for. Simultaneously though they are also creating the need for a new approach to monitoring and assuring the operation of the virtualized, automated environments they employ. The new stacks of SDN and NFV are more open, elastic and dynamically configurable than the comparatively static models of prior system implementations. A new framework is needed to understand the configuration, operation and performance of the new virtual environments in parallel with the operation of pre-existing systems.

> "As network services are becoming more cloud-like, so too it will be necessary for network management to follow the same paradigm. CA's Virtual Network Assurance provides the bridge for traditional network management to reach the new network."
>
> - Tim Diep, Director, Product Management, CA Technologies

CA Technologies understands this evolution and has created Virtual Network Assurance (VNA), a solution for supporting service assurance in the virtualized environments of SDN and NFV, while continuing its support for service assurance for the pre-existing systems that continue to function while new systems and applications come into play. This note highlights the innovative approach CA has taken in developing the VNA solution, as well as the benefits it provides to operators and IT teams embracing SDN and NFV.

The new stacks employed in SDN and NFV are illustrated in Figure 1. In it we see the use of virtual machines logically connected to each other by the use of network tunneling and forwarding functions supported in the virtual switches and routers of the infrastructure of the virtual system. The virtual machines are running network functions such as firewalling and load balancing that are logically chained to each other in support of a given application or user group. And the relationship of this new virtual stack to its underlying physical infrastructure of compute servers, storage and physical networking platforms is indicated by the operation of this new stack in the installation's physical hosts at the bottom of the diagram.

Since this software-driven, cloud-style model of deployment involves a new approach to the operation of important value-adding functions in the network, as well as the overall network itself, it underscores the point that monitoring and assurance functions related to the model need to embrace the new design framework as well. For example, network monitoring and measurement systems now need to be aware of the relationship of individual functions such as firewalling to the service chains to which they belong; the status of network tunneling and forwarding operations related to virtual machines (VM) and the virtual network functions (VNFs) they are supporting needs to be made visible.

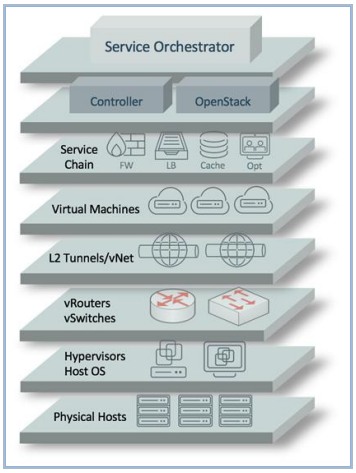

Figure 1. CA's New Stack Model for SDN and NFV

NFV's Management and Orchestration Reference Architecture (MANO)

The general structure for achieving this was created in the NFV Reference Architecture defined by operators and vendors in the European Telecommunications Standards Institute (ETSI) for NFV. As shown in Figure 2, it contains a number of APIs for components to communicate with each other, as in communication between a Virtualized Infrastructure Manager (such as OpenStack) to the VMs and virtual network it supports or communication of a VNF Manager with its VNFs. However, despite defining these, the model comes up short of articulating how these functions would actually realize a holistic view of the status, performance or service level agreement-related behavior of the deployment. That functionality is left open to interpretation by implementers. In general, it leaves open the question, how do I obtain an integrated, holistic, vendor-agnostic view of the status, performance and operation of my (very efficient, elastic and open) SDN and NFV solution?

This is where CA's VNA solution comes in and delivers its well-positioned value.

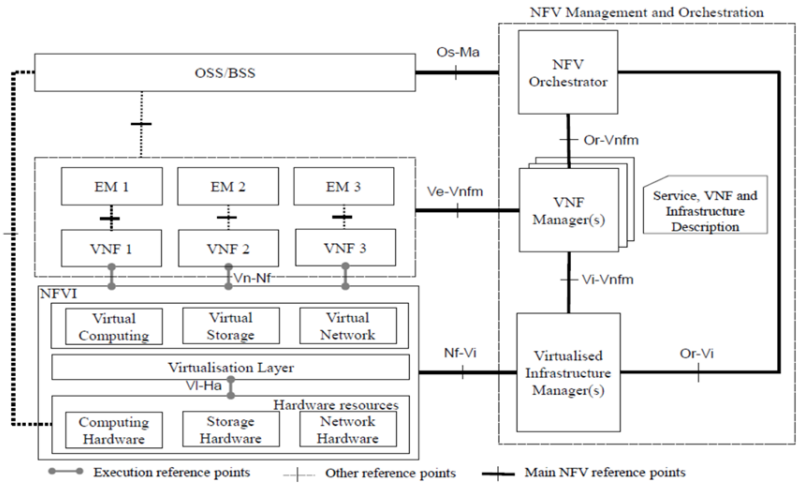

Figure 2. ETSI's NFV Reference Architecture

CA's Virtual Network Assurance

As shown in Figure 3, VNA is designed as a modular, extensible and dynamic solution that integrates with the logical elements of the NFV deployment on the left to understand their configuration, state and performance. At the same time, VNA communicates with monitoring and assurance applications running in support of pre-existing, non-SDN and non-NFV infrastructures that continue to work in the same IT or provider environment while new SDN and NFV solutions are being deployed (Figure 3). In this way VNA efficiently supports an integration of what's new with what's already running' in a way operations managers will clearly appreciate.

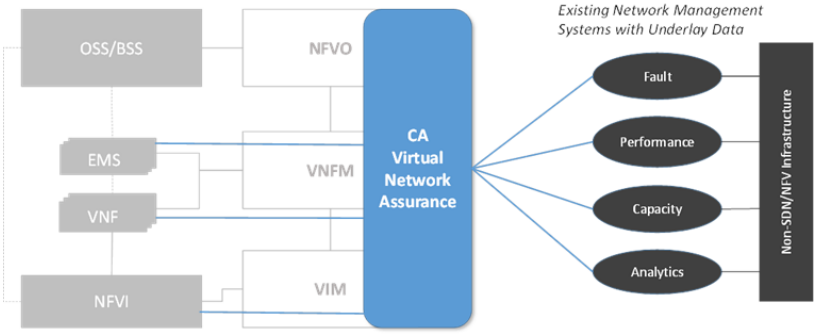

Figure 3. VNA's Logical Architecture

An important element of VNA that enables this intelligent integration is its use of a flexible data model along with extensible APIs for the way it communicates with both virtual infrastructure components such as VNFs and VIMs, as well as CA's own and other suppliers' network management systems supporting the non-SDN and non-NFV environments. A key element of SDN and NFV environments is their use of data modeling and open APIs as a tenet of how they achieve their modularity, flexibility and scale. VNA's embrace of this key approach is a strong indicator of its prospective value.

A less abstract view of how VNA's model is applied to use cases critically important to service providers and IT teams achieving their goals is shown in Figure 4. In it, VNA is shown communicating to its left with the OpenStack virtual infrastructure management system managing the virtual infrastructure for this NFV deployment: with a virtual firewall supplied by Checkpoint; and with NFV orchestration applications supplied by Oracle and Juniper. In parallel it is communicating with CA's Spectrum and Performance Management systems to create a unified perspective of the deployment between its virtual and physical domains. This combination of functions is high on the list of early stage deployment scenarios that service providers and data center operators can consider deploying for secure VPNs and secure tenant data center domains.

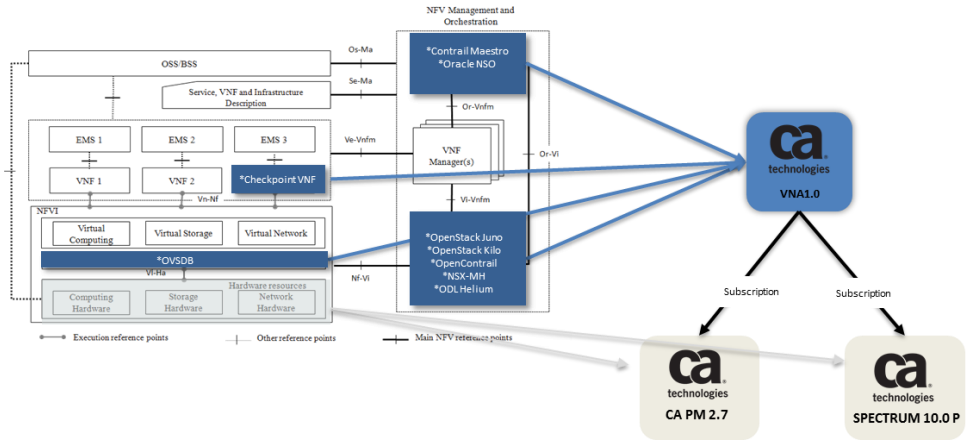

Figure 4. VNA and OpenStack Virtual Infrastructure Management System Use Case

A further illustration of VNA's value can be seen in the way it discovers, monitors and interprets the operation of service chains in NFV, shown in Figure 5. Taken from the VNA user interface, this diagram is showing a real-time understanding of a typical service provider's VNF use case for a broadband service offering in which security, content optimization and in-line traffic analysis are being performed to support an end customer's services. The VNF service chain, one of the most crucial innovations involved in NFV, is being monitored and managed in the process. Service chains are logical abstractions of the forwarding paths involved in connecting VNFs in sequence with each other to realize a service delivery goal. They are a logical overlay or abstraction above the switching and routing path the traffic is traversing to realize the goal. The ability of VNA to understand, monitor and manage NFV service chains is a critical element in its readiness to support the agile operations that service providers' customers want.

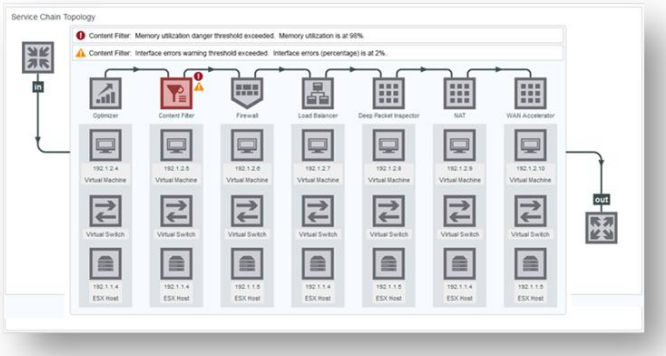

Figure 5. VNF Use Case for a Broadband Service

A final consideration in looking at the readiness of VNA to add value to SDN and NFV is that it also incorporates a policy enforcement function that allows it to communicate policy-based actions in real time to the virtual system infrastructure components with which it is working that support achieving operational goals automatically by inserting policy preferences into the operation of the virtual infrastructure it is supporting.

In this sense VNA is taking a positive step forward in the use of policies and analytics to enhance the behavior of SDN and NFV in parallel with the other software with which it is communicating (VIMs and MANO applications, for example).

Merging the Best of What's New with What's Already Up and Running

When we consider the goals operators and IT teams have for moving to SDN and NFV, we note that an important gap to be closed in realizing the promise of the new software-driven models is delivery of well-designed, vendor-neutral assurance solutions to help achieve the agility and efficiency goals for which SDN and NFV are designed. CA has taken an important step in advancing the state of the art in SDN and NFV by bringing the Virtual Network Assurance solution to market. Through its integration with SDN and NFV reference architectures using mechanisms and models preferred by participants in their ecosystems and its lateral integration with well-established assurance platforms supporting pre-existing environments, VNA is enabling operators and IT teams to pursue the best of what's new in parallel with what's already up and running with the confidence they need to get maximum value out of both. This is an important contribution to the market. It is taking concrete steps toward delivering management that is as agile as the cloud.