TECHNOLOGY WHITE PAPER

Correlating SDN overlays and the physical network with Nuage Networks Virtualized Services Assurance Platform

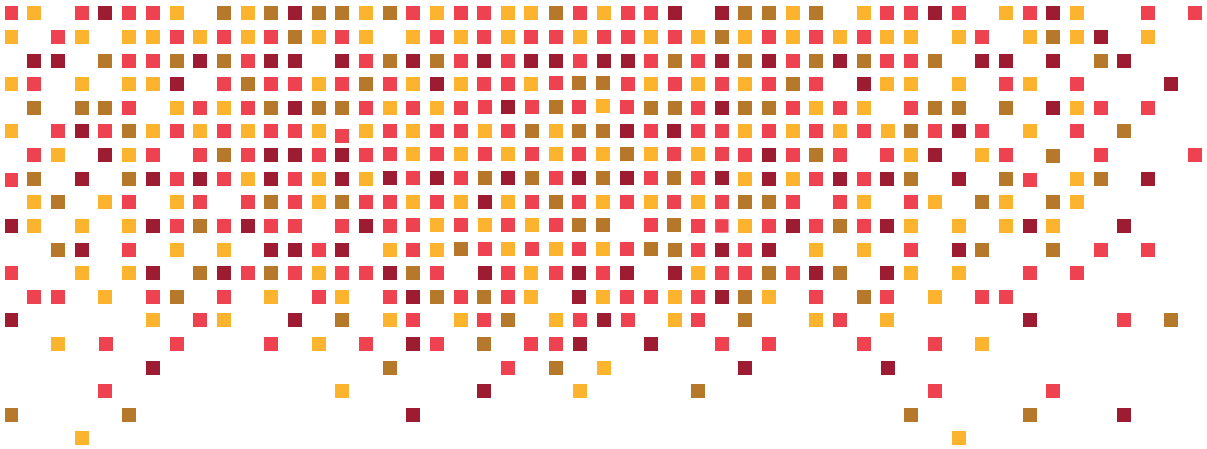
nuagenetworks
From Nokia

Abstract

Enterprises are expanding their private clouds and extending network virtualization within and across their datacenter and wide area environments. But their progress is impeded because they do not have clear and timely correlations between programmable Software Defined Network (SDN) overlays and the physical underlay.

Enterprise IT operations groups need tools that help them understand the IP network that supports the multitenant virtual workloads within and across their networks.

Nuage Networks™ Virtualized Services Assurance Platform (VSAP) gives enterprise IT operations groups the network visibility and troubleshooting tools needed to operate and manage virtual networks. Now, if a link goes down in the multivendor physical underlay network, IT operations staff know precisely which applications, services and virtual machines are affected so they can quickly take action.



CONTENTS

The management challenge in software defined networks

Historically, network connectivity has taken a relatively long time to plan and implement. And, once configured on the network, connectivity tends to stay in the same state for a long time because modifications also require long planning and deployment timelines.

However, Software Defined Network (SDN) connections are by nature dynamic. SDN service turn-up and modification times are measured in minutes, not in days or months. In an SDN overlay network:

- Connectivity provisioning is handled in the control plane rather than the management plane.
- Services are provisioned with little or no requirement to understand the underlying network infrastructure or topology.
- Service endpoints can move at a moment's notice, for example when a virtual machine (VM) compute resource needs to be upgraded to deliver more bandwidth or functionality.

This new agility means management applications need to provide feature-rich fault management so enterprise IT operations staff can quickly identify issues within the network domain. The challenge is for fault management functions to distinguish between faults that reside on the network infrastructure and those that occur on the compute side of the service deployment.

TABLE 1. SDNs bring management challenges

NETWORK MANAGEMENT CHALLENGE	NETWORK VISIBILITY NEEDED
Keep pace with rapidly changing services	Dynamic directory of current and historical virtual services
Proactively detect emerging service issues	Real-time monitoring and troubleshooting
Easily pinpoint issues to their root cause	Comprehensive SDN overlay and physical underlay network correlation
Prevent issue reoccurrence	Virtual service diagnostics and heuristics

Once a fault is detected, the management application must try to correlate that fault to other objects in the service path. It would be a fairly simple task for a management application that is monitoring a single domain — a pure SDN or pure traditional physical network — to provide this feature. The real challenge is when the management application must provide the correlation between virtual and physical domains.

With the dynamic nature of SDN services, the possibility of transitory faults increases. Because virtualized objects such as virtual machines can be turned up, turned off, or moved as service requirements change, faults may be there one moment and gone the next.

In traditional networks, transitory faults are easily dealt with by keeping a historical database that links the fault to a physical object. However, in the virtualized world, that object may no longer exist, or it may have moved. That means the management application must know the state of the dynamic virtual objects and correlate them to the physical world where they are used.

This white paper provides an overview of the key functions provided by the Nuage Networks™ Virtualized Services Assurance Platform (VSAP). And it explains how these functions help to simplify SDN operations and management by correlating virtualized overlay services with the operational state of the physical underlay network.

Addressing SDN management challenges with Nuage Networks VSAP

The Nuage Networks VSAP provides a comprehensive suite of tools to fault-find the physical and SDN networks so that the challenges described above are met.

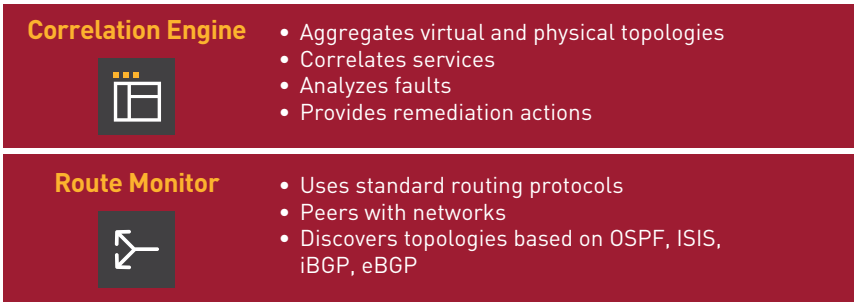
The Nuage Networks VSAP includes network monitoring and troubleshooting features that provide advanced visibility and fault management for the SDN datacenter and the wide area network. Now this next-generation fault management application, which is based on the JBoss Drools Business Rules Management System (BRMS) solution, also provides advanced root cause analysis for SDN objects.

Network operators can see the paths between virtualized objects, tracing routes across the underlay resources. And, with the application's ability to retain faults and correlated alarms, operators can easily pinpoint historical network issues and determine whether the fault is in the compute network or the network underlay.

Building on these key functions, the Nuage Networks VSAP provides integrated element, network, and service operations management for advanced network solutions. The main network management operations include:

- Element management with fault, configuration, accounting, performance, security (FCAPS) functionality.
- Network infrastructure management, service provisioning, scripting and service management.
- Network and service assurance, including topology views and operations and maintenance (OAM) diagnostic testing.
- RESTful application programming interface (API) integration to external applications.

FIGURE 1. The Nuage Networks VSAP offers key network management functions



Element management and correlation

In a datacenter and Software Defined Wide Area Network (SD-WAN) context, the Nuage Networks VSAP provides element management functionality for the:

- Nuage Networks 7850 Virtualized Services Gateway (VSG)
- Nuage Networks 7850 Virtualized Services Aggregator (VSA)
- Nuage Networks 7850 Network Services Gateway (NSG)
- Virtualized Services Controller (VSC) component in the Nuage Networks Virtualized Services Platform (VSP)

Each of these offerings can be discovered and managed by the Nuage Networks VSAP, as can network elements running the Nokia Service Router Operating System (SR OS).

The virtual components, such as virtual switches (vSwitches) and virtual ports (vPorts), can be configured with statistics collection and modeled within the same element management database. This enables correlation with element management functionality including:

- Network element backup and restore
- Equipment configuration and status monitoring
- Performance statistics collection
- Threshold-crossing alarms

Network infrastructure management

Network infrastructure management features in the Nuage Networks VSAP include support for service creation and management. Network infrastructure management is extended to provide support for virtualized service management, including:

- Manual and scripted service provisioning
- Policy-based services management

Network and service assurance

Network and service assurance features include support for:

- Topology maps
- Alarm management
- Service testing and troubleshooting
- Performance management

For SDN resources, these assurance features include topology maps for virtual network objects and virtualized services, as well as alarms that are unique to those objects. Network and service assurance functionality includes:

- Dynamic physical and virtual service topology maps
- Alarm filtering and correlation
- Statistics collection and plotting

Virtualized services creation and provisioning

The Virtualized Services Directory (VSD) component in the Nuage Networks VSP is a policy-based system that can be used to create virtualized services and provision them on the SDN elements.

The VSD communicates directly to the network elements for which the Nuage Networks VSAP discovers virtualized network and service objects. The Nuage Networks VSAP integrates these objects into the IP underlay network view for event correlation and other functionality. It uses the Simple Network Management Protocol (SNMP) to discover and monitor the SDN and physical components through the VSC component.

Route analytics and assurance

The Nuage Networks VSAP provides real-time Interior Gateway Protocol (IGP) and Border Gateway Protocol (BGP) topology capture, inspection, visualization and troubleshooting.

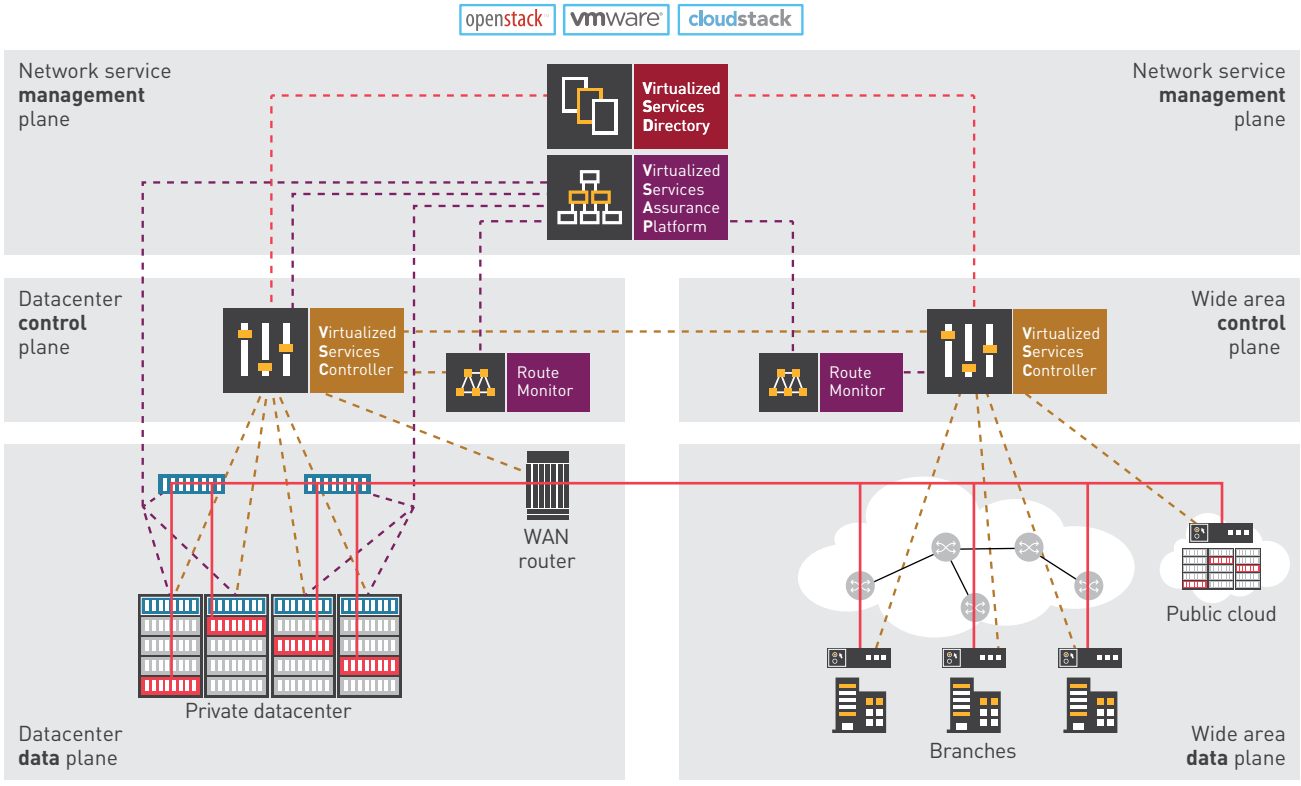
The solution retrieves routing data from its Route Monitor function and aggregates it for route analytics and assurance functionality. This functionality gives network operators visibility and mappings for virtualized services and their related components. It extends:

- Reachability event correlation functionality to virtual objects and enables historical impact and root cause analysis for associated faults.
- BGP reachability analysis to virtualized services and stores a log of reachability information.

The Route Monitor function is based on the Nokia 7701 virtualized Control Plane Assurance Appliance (vCPAA) product. The 7701 vCPAA provides analysis in a distributed computing platform and uses a passive version of the industry-tested and proven SR OS routing code. As a result, the Route Monitor provides a high degree of interoperability with customer networks, acting as a routing element that passively peers with the network. The main functions of the Route Monitor are to:

- Monitor routing data from the routing protocols that are running on it.
- Provide route calculation for routes passing through the routing areas for which it is responsible.
- Perform routing analysis and provide the results to the Nuage Networks VSAP so network-wide reports or alarms can be generated.

FIGURE 2. Nuage Networks VSAP connects to the SDN and the physical network



Network monitoring to improve visibility and fault management

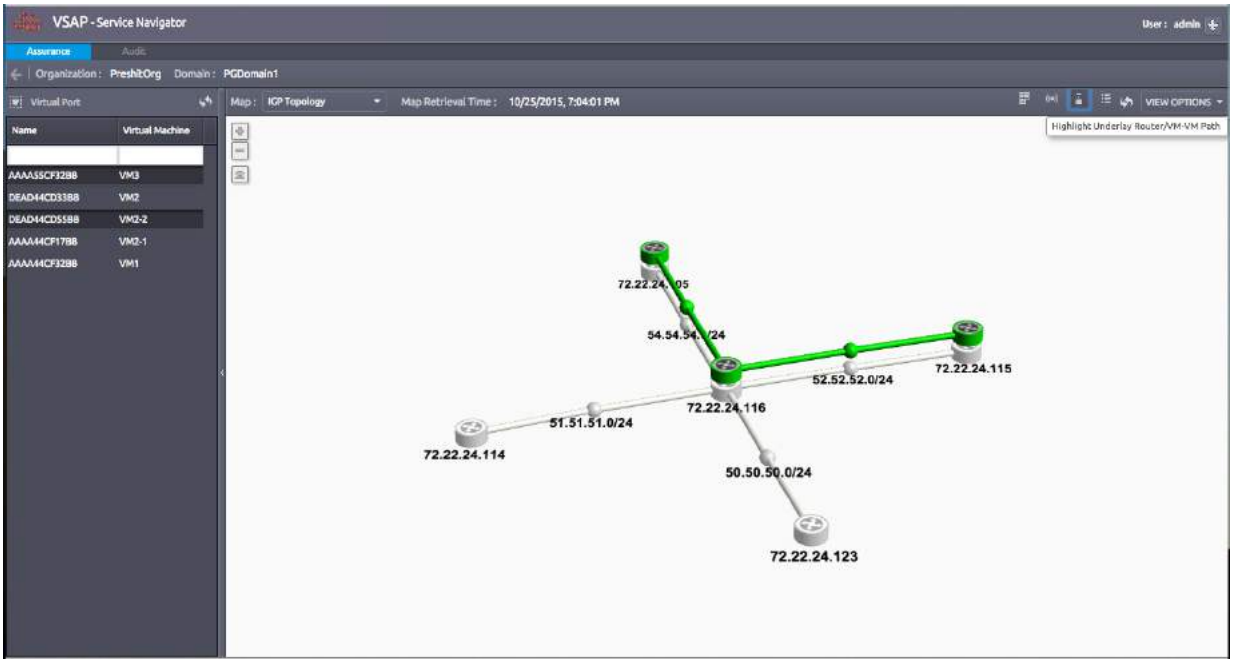
The infrastructure layer of Nuage Networks VSAP includes network monitoring and troubleshooting features that provide advanced visibility and fault management for the SDN. Operations staff can quickly find the path to the associated Virtualized Services Controller for any VM or vSwitch in the network. They can then graphically highlight the path and assign IP path monitors. Historical faults and alarms are retained so staff can monitor historical changes on a path between a physical router and a virtual component.

IGP topology features let operations staff map and monitor datacenter network infrastructure. Topology maps display real-time network topology information for a designated IGP administrative domain. They provide a color-coded interface that shows a visual representation of routers, paths and virtual objects within the specified IGP administrative domain. Map highlighting can be used to view:

- Layer 2 and Layer 3 services
- Composite services
- Service tunnels
- Shortest Path First (SPF) and Constrained Shortest Path First (CSPF) routes
- OAM diagnostics results on IGP maps

In an SDN, map highlighting is most useful for mapping paths from a VM or vSwitch to an associated SDN controller or a Provider Edge (PE) router. As shown in the example below, highlighting the SPF from a virtual object to a PE router reveals the mapping between the virtual object and the network underlay.

FIGURE 3. Visual traces between SDN elements map virtual objects with the network underlay



IP path monitors can be used to monitor the route between routers. When there is a network topology change, such as a link metric or a state change, the system evaluates whether the routes of registered paths are affected:

- If routes are affected, new routes are recorded by the Route Monitor.
- If there is no route for a monitored path after a topology change, a record is logged.
- If there is a change in the SPF calculation based on a topology change, the change is recorded.

Highlighting shows current versus historical paths, including their respective costs.

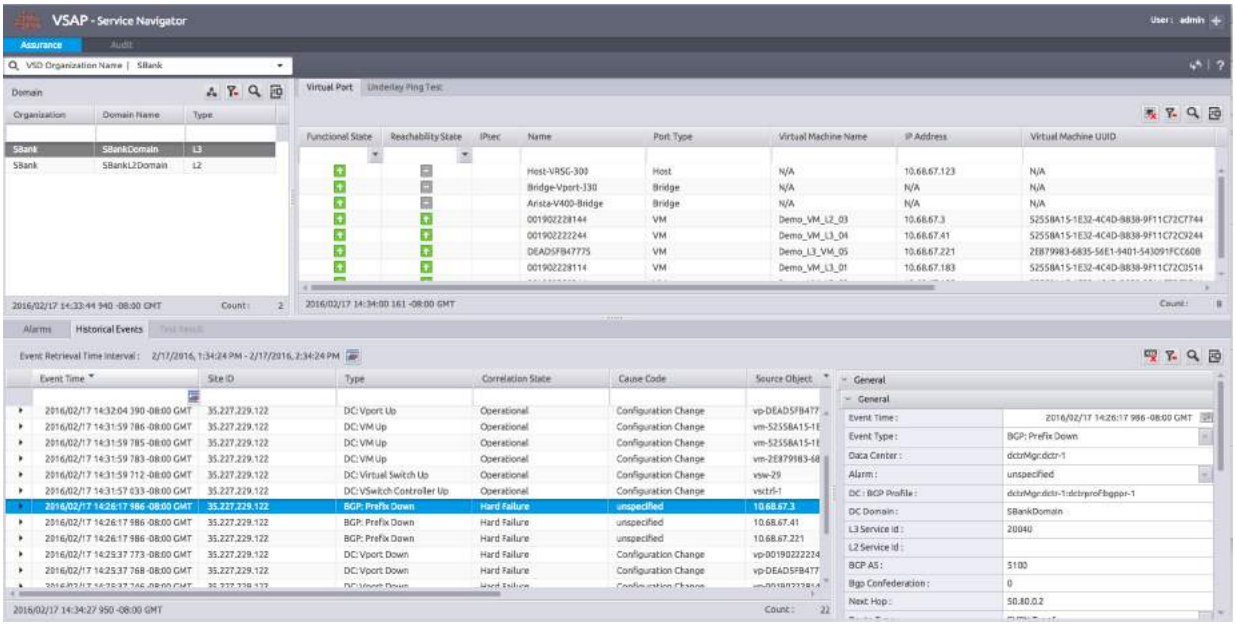
Lightweight Services to improve service assurance and awareness

The Nuage Networks VSAP provides SDN services, called Lightweight Services, to improve awareness and assurance in virtualized services management. These Lightweight Services offer opportunities for service object persistence to accommodate the constant deletion and creation of service objects as VMs move within the network. As a result:

- Event retrieval and correlation features are extended to persisted service objects and datacenter-specific events.
- BGP virtual private network (VPN) route analytics are extended to virtualized services. This provides assurance and troubleshooting for distributed Virtual Routing and Switching (VRS) and Ethernet VPN (EVPN) service objects.

The example below shows the user interface that lets operators view historical BGP events pertaining to a particular service context for a specified period. Operators can assess these events to quickly determine the reason for historical service interruptions or failures.

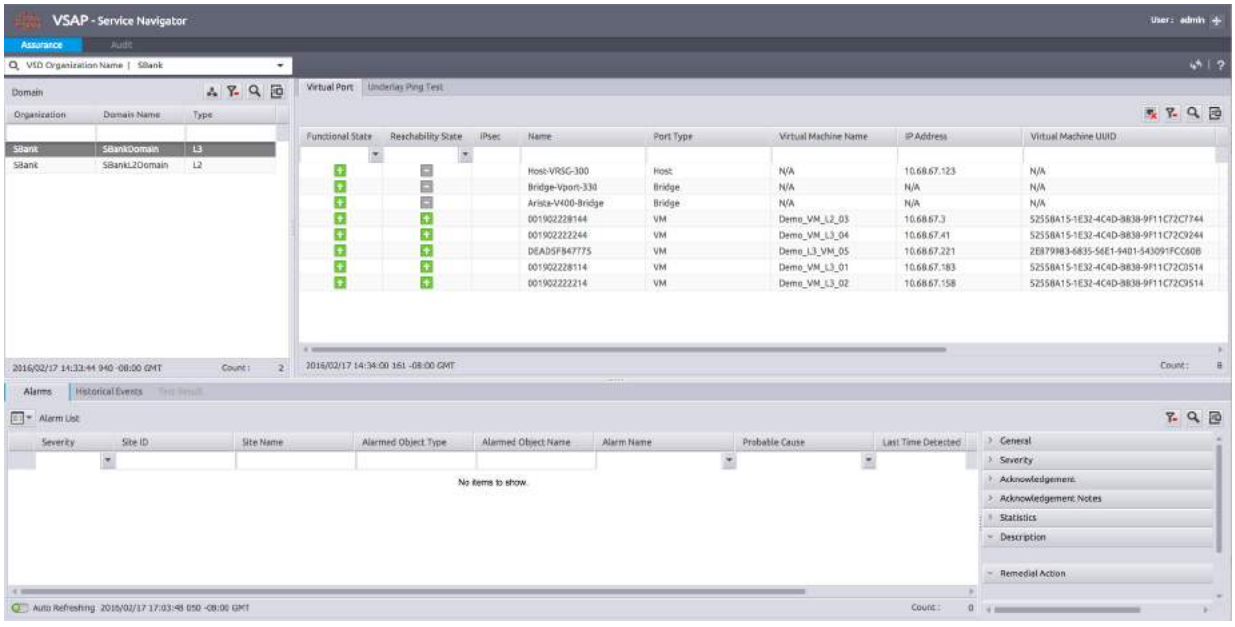
FIGURE 4. Historical event retrieval for VMs helps operators troubleshoot service interruptions



The Route Monitor BGP functionality provides a full view of the SDN and associated WAN routing. It supports multivendor topology views through dynamic discovery of IGP and BGP routing contexts. These views are combined with the vSwitch and VM mappings derived from virtual node (vNode) discovery to create a complete mapping of the network underlay to the network overlay. The Route Monitor also automatically monitors virtual services as they relate to the VM and vPort state. BGP reachability analysis allows operators to monitor the BGP state for VMs and network elements in the SDN.

The Service Navigator user interface, shown below, allows network operators to list virtual services. Selecting a service from the list provides operators with visibility into the functional state of the VMs associated with the service and VM reachability within the service context. Other BGP VPN features, such as map highlighting, can be used to associate and map virtual objects to the network underlay.

FIGURE 5. The SDN Service Navigator Dashboard increases visibility into VM state and reachability



Network object persistence

Virtual service objects, such as VMs and vPort endpoints, are inherently mobile and may be created, deleted or moved on a frequent basis. The Nuage Networks VSAP tracks these objects using the object's Universal Unique Identifier (UUID), maintaining state, reachability, alarm correlations, statistics, and other data related to the object.

As virtual service objects move or are automatically deleted, the Nuage Networks VSAP maintains a log of persisted service objects so that historical routing information is not lost.

Event retrieval log and correlation

Network events are stored in a history log that can be used for fault correlation. Operators can view a log of events related to a particular service or to a specific VM. They can filter the event list based on a specific time period or rewind from the current time.

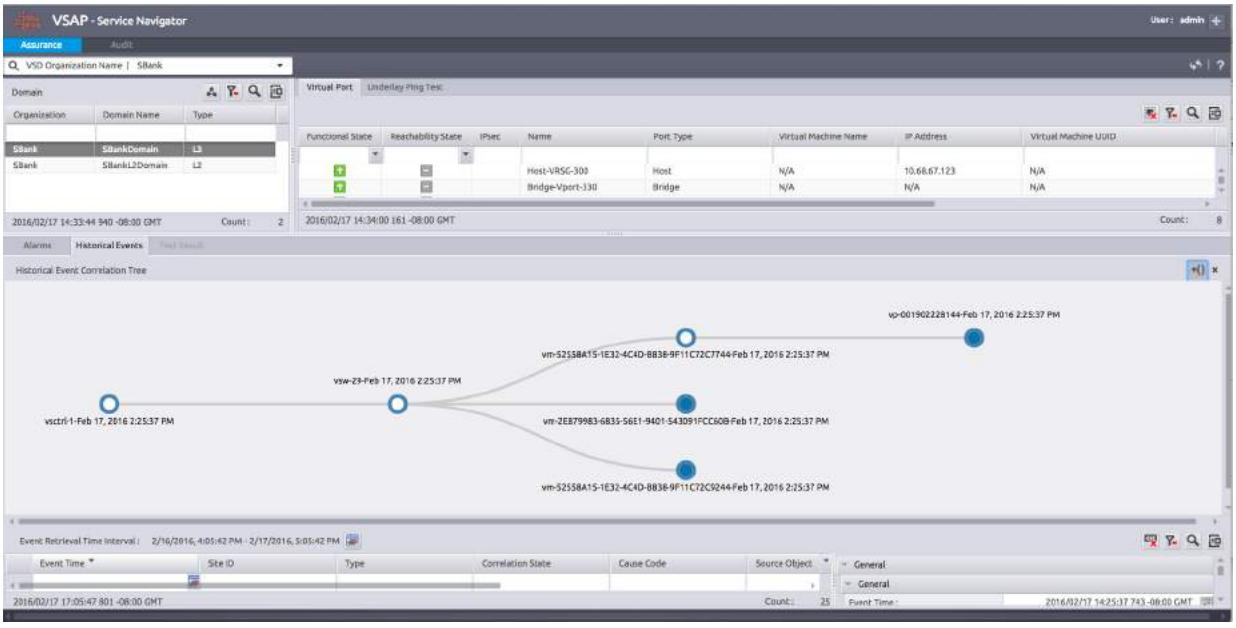
The event log stores BGP-based network events. These events include reachability alarms and flapping occurrences for the BGP prefix. When operators retrieve events for a service, they can troubleshoot historical events by correlating SDN element events to BGP events gathered from the physical underlay network.

The event log provides access to two correlation features for BGP and SDN events:

- Root cause analysis
- Impact analysis

Operators can choose a historical event from a list and request root cause and impact analysis in the form of tree, as shown in the example below. The root of the tree represents the root cause event and the branches represent symptoms, or events, that occurred as a result of the root event.

FIGURE 6. The historical event correlation tree enables root cause and impact analysis



BGP event correlation

Correlating information from the SDN services layer and the physical network — provided by IGP protocols such as BGP — into a concise operational view improves visibility of the network and service impact as well as root cause analysis of the fault.

When correlating this information, the Nuage Networks VSAP processes BGP events, such as IGP Upstream Connection Up and Down events, similarly to vSwitch Controller Up and Down events in the SDN layer. The IGP monitor function, which is used to discover and log upstream router events, plays a key role in gathering the underlay information.

Where BGP prefix events affect the SDN-based services, the Nuage Networks VSAP correlates SDN-specific alarms based on the:

- Virtualized network events in the event log.
- Correlation for absent vPort or BGP prefix events.

In cases where a vPort or BGP prefix event is expected, but not present, the Nuage Networks VSAP raises an alarm.

With its comprehensive BGP support, the Nuage Networks VSAP provides the operational tools needed to troubleshoot BGP-related network issues.

The Route Monitor discovers and monitors BGP routing information, then consolidates data from the 7701 vCPAAs to provide an overview of the end-to-end network. Operations teams can, for example, monitor whether a change in the number of BGP routes could compromise network stability, or if key BGP routes are disappearing. For IP VPN routes, the Route Monitor flags a high rate of change for a set of virtual routing functions.

Overlay and underlay fault correlation

The Nuage Networks VSAP overlay- and underway-aware correlation functions lead the industry in providing a physical and virtual network fault management framework.

In addition to the fault management rules provided as part of the Route Monitor, the Nuage Networks VSAP provides correlation rules that help operators monitor and troubleshoot virtual network and service objects. They can, for example, view impact analysis for moved or deleted VMs. Operators also benefit from flexible correlation rules and the ability to correlate specific alarms.

FIGURE 7. The alarm list lets operators show impacts for specific alarms

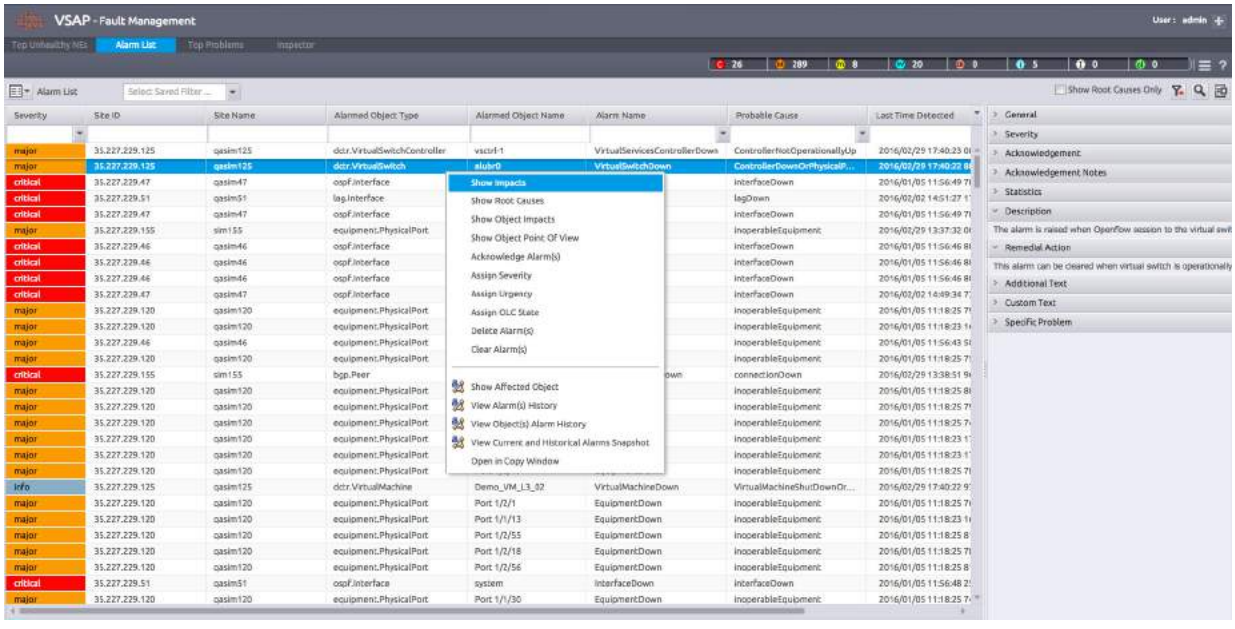
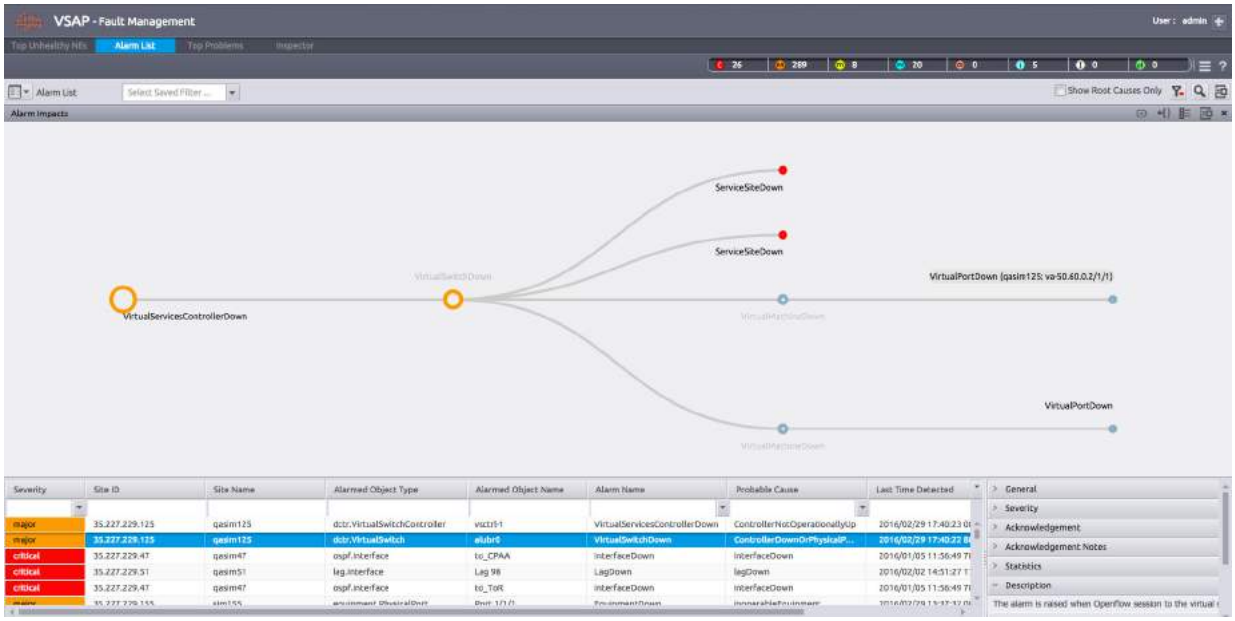


FIGURE 8. Alarm impacts are visually represented to simplify troubleshooting



The Nuage Networks VSAP fault management framework includes rules for correlating:

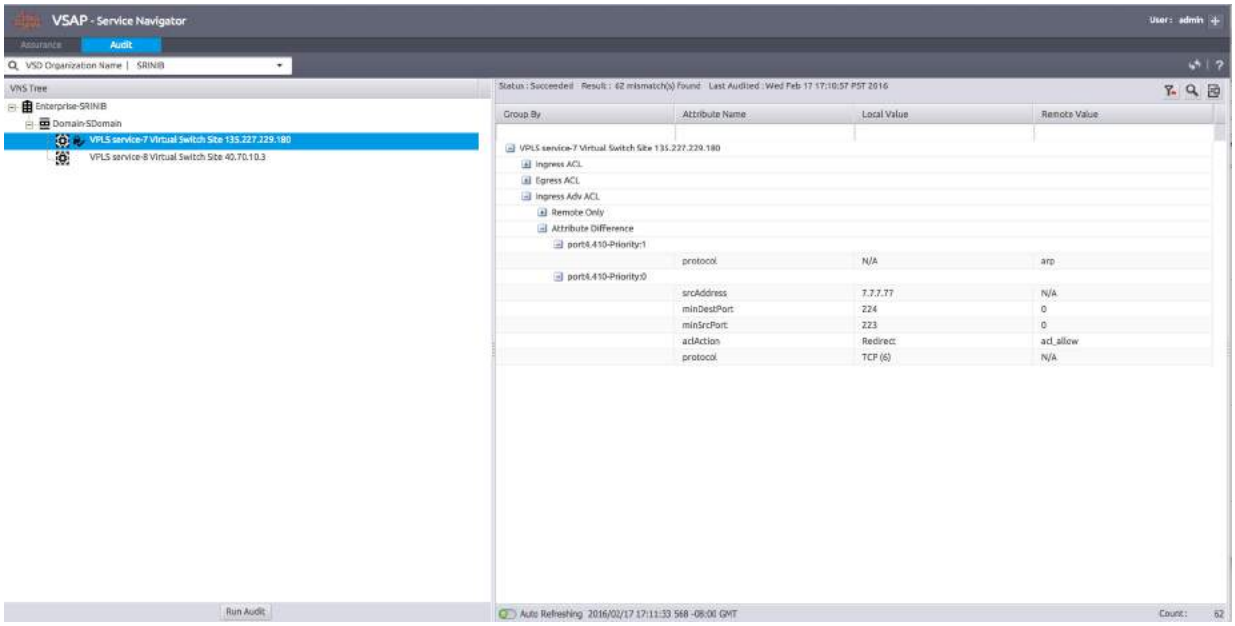
- Service status alarms from virtualized service sites to virtual network components such as vSwitches, vPorts and VMs.
- Threshold-crossing alarms from virtualized service sites to the vPort.
- BGP prefix reachability alarms from IGP monitors to virtual network components.
- BGP prefix reachability alarms from virtual network components to virtualized service sites.

Software Defined Wide Area Network support

The Nuage Networks VSAP provides assurance and debugging support for datacenter and SD-WAN applications. One of its key features is the ability to audit the configuration and connectivity for Nuage Networks 7850 Network Services Gateway (NSG) branch equipment.

The 7850 NSG is centrally managed with no local access to device configuration for security reasons. This means configuration audits are not a trivial task. As shown in the figure below, the Nuage Networks VSAP compares configuration parameters on the Virtualized Services Controller (VSC) with the values configured on the 7850 NSG to simplify audits.

FIGURE 9. The Nuage Networks VSAP simplifies configuration audits on branch equipment



Statistics collection and plotting

The Nuage Networks VSAP performs on-demand or scheduled statistics collection for managed network elements, services and virtual network objects. These statistics can be used to monitor or troubleshoot a datacenter network, or to perform service level agreement (SLA) or billing functions. Statistics collection can be configured with policies that are distributed to specified network objects. Statistics are displayed in tabular or graphical format using the statistics plotter.

Statistics collection

Network performance statistics are collected using SNMP to poll the network element management information base (MIB) tables. It collects:

- Performance statistics to provide information about physical equipment, routing and other network element properties. SNMP MIB statistics collection policies define performance statistics collection at the network element level or at the network object level.
- Accounting statistics to provide throughput information for queues that are associated with Service Access Points (SAPs), network ports and subscriber profiles. Accounting statistics policies can be defined for vPorts to monitor service, network or subscriber accounting statistics.
- Server performance statistics to monitor system functions and processes. Server performance statistics are based on Nuage Networks VSAP internal data, such as memory usage and alarm counters.
- BGP statistics using functionality from the Route Monitor. MIB statistics policies can be applied to the 7701 vCPAA to define the collection of specified statistics counters. BGP statistics can be plotted and stored using the statistics plotter. The Route Monitor raises BGP-specific threshold crossing alarms when thresholds are reached.

Statistics plotting

All supported statistics types can be viewed in tabular or graphical format using historical or real-time data:

- Tables list specific values for historical data. Table data can be sorted, filtered and exported to files in different formats.
- Graphs can be used to identify trends and to display multiple statistics counters simultaneously. The statistics plotter graphs statistics from a specified time period or in real time.
- The statistics plotter can also plot ingress and egress statistics using calculated values. Plotted utilization statistics let operators view bandwidth usage on a specified port in tabular and graphical format.

Summary

Datacenter and wide area network topologies can be complex, mixing technologies, transport methods, equipment types and vendors. Provisioning overlay services across these networks introduces new challenges to provide effective monitoring and assurance.

Nuage Networks VSAP is based on robust technologies that have been deployed in some of the world's largest and most advanced networks for mobile, residential, enterprise and converged services for more than 10 years. As a result, the Nuage Networks VSAP is uniquely positioned to provide a single solution for service assurance across multitechnology, multilayer and multivendor networks.

The Nuage Networks VSAP addresses the challenges that network operators face when SDN services are deployed in the datacenter and when they are extended across the wide area network. The solution correlates SDN-based overlay services to the underlying physical network, giving network operators better visibility, monitoring and troubleshooting capabilities for SDN services.

Abbreviations

API	application programming interface
BGP	Border Gateway Protocol
BRMS	Business Rules Management System
CSPF	Constrained Shortest Path First
EVPN	Ethernet Virtual Private Network
FCAPS	fault configuration assurance performance security
IGP	Interior Gateway Protocol
IP	Internet Protocol
MIB	management information base
NSG	Network Services Gateway
OAM	operations and maintenance
PE	Provider Edge
SAP	Service Access Point
SDN	Software Defined Network
SD-WAN	Software Defined Wide Area Network
SLA	service level agreement
SNMP	Simple Network Management Protocol
SPF	Shortest Path First
SR OS	Service Router Operating System
UUID	Universal Unique Identifier
vCPAA	virtualized Control Plane Assurance Appliance
VM	virtual machine
vNode	virtual node
VPN	virtual private network
vPort	virtual port
VRS	Virtual Routing and Switching
VSA	Virtualized Services Aggregator
VSAP	Virtualized Services Assurance Platform
VSC	Virtualized Services Controller
VSD	Virtualized Services Directory
VSG	Virtualized Services Gateway
VSP	Virtualized Services Platform
vSwitch	virtual switch
WAN	wide area network

nuagenetworks
From Nokia