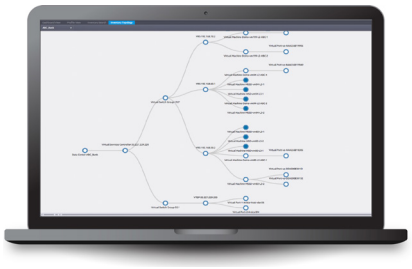
nuagenetworks
From Nokia

Virtualized Services Assurance Platform

Highlights

- Correlates and manages SDN-based overlay services and IP underlay networks to deliver proactive service assurance
- Delivers real-time analytics that simplify SDN service management, reduce problem escalations and accelerate service-problem resolutions
- Detects abnormal IP underlay infrastructure control plane behavior and configuration problems before they affect SDN-based overlay services
- Enables real-time graphical visualization of control planes for both overlay services and multivendor IP underlay networks



The Nuage Networks Virtualized Services Assurance Platform (VSAP) addresses the need for visibility and correlation between the networking requirements of virtual applications and workloads (the "overlay") and the physical connectivity provided by the IP network infrastructure ("the underlay"). The IP infrastructure route and path analytics generated by the VSAP simplify the management of SDN overlay services.

The VSAP provides proactive and real-time visualization, troubleshooting and analysis of underlay IP control plane protocol changes and their impact on SDN overlay service paths. With this information, network operators can limit the number of problem escalations while accelerating resolutions to service affecting problems.

The VSAP is tightly integrated with the Nuage Networks Virtualized Services Platform (VSP). As a result, SDN-based overlay services can be provided with an assured network path based on the latest analytics information derived from the underlying IP network infrastructure.

The VSAP interrogates the IP underlay network via standards-based protocol interactions to provide real-time visibility and management of the condition of the underlay so that the SDN-based overlay services can utilize the best path across the network.

Should underlying network conditions change, the VSAP provides proactive information to the Nuage Networks VSP so that the optimal overlay path selection is maintained at all times.

Enriched virtual services management

The VSAP adds underlay monitoring and analytics for SDN services that are managed with the Nuage Networks Virtualized Services Platform. Key benefits of the Nuage Networks VSP include:

- Provides SDN-enabled virtualization with support of L2-L4 services
- Optimizes and scales datacenter connectivity and is deployable on heterogeneous networks
- Uses programmable business logic and policies to fully automate network service creation
- Removes network constraints to deliver unrestricted placement of VM workloads to maximize efficiency of server resources
- Integrates public, private and hybrid cloud application into managed VPNs
- Includes extensive data analytics and performance monitoring capabilities
- Supports end-to-end cloud networking from the datacenter to the branch

Features

Network monitoring and troubleshooting

The VSAP makes it easy for SDN network operators to manage, assure and troubleshoot underlying IP networks by providing proactive and real-time visibility into internal routing issues. Network operators can quickly find the path to the SDN control plane for any virtual machine (VM) or virtual switch (vSwitch) in the network. Via the graphical topology overview the operator can highlight the path and assign IP path monitors. By tracking fault and alarm data, the operator can monitor historical changes on a path between the physical (IP router) and a virtual component.

The Interior Gateway Protocol (IGP) topology features provide the operator with a graphical representation through which they can monitor the underlying IP network infrastructure. Topology maps display real-time network topology information for a designated IGP administrative domain. With an intuitive color-coded interface the operator can see a visual representation of routers, paths and virtual objects within the specified IGP administrative domain. The topology view provides quick navigation to operational tools including configuration forms, network element telnet sessions, and feature configuration from within the IGP administrative domain.

Map highlighting can be used to highlight L2/L3 services, composite services, service tunnels, SPF and CSPF routes, and OAM diagnostics results on IGP maps.

For datacenter networks, map highlighting is most useful for mapping paths from a VM or vSwitch to either an associated SDN controller or a WAN gateway router. By performing a SPF highlight from a virtual object to a gateway router, the operator can create a highlighted mapping between the virtual objects to the physical network underlay.

IP path monitoring

IP path monitors can be used to monitor the route between any two routers seen by the VSAP. When a network topology changes, such as a link metric or state change, the VSAP evaluates whether the routes of any registered path are affected. If they are, new routes are recorded and the IGP listening function of the VSAP is informed. If there is no route for a monitored path as a result of 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. This provides the operator with a graphical toolset to highlight current versus historical paths, including their respective network costs.

Service assurance and troubleshooting

The VSAP provides virtualized service management to improve awareness and assurance of the SDN overlay services and any service impacts generated by the underlying IP network infrastructure.

The move to compute and network virtualization has created a new level of complexity: operators must manage elements and objects that are not persistent. The VSAP provides an operation toolset that accommodates this new environment and the constant creation and deletion of service objects as VMs, vSwitches and dynamic paths move within the network. The event retrieval and correlation features in the VSAP reduce this complexity to provide assurance and troubleshooting for both SDN and IP service objects.

For instance, when troubleshooting, an operator can retrieve real-time information or a historical time interval log of network events such as Border Gateway Protocol (BGP) route changes pertaining to an SDN service under investigation. With this information, they can quickly deduce the reason for service interruptions.

Interior Gateway Protocol monitoring
The VSAP includes an IGP silent peering feature — the Route Monitor (RM). The RM is a virtual machine-based IGP listener. The RM acts as a silent router (listening only) that peers with the IGP to listen to any route advertisements and route changes within the network. As a listen-only peering function, the RM has no capability to advertise routes into the IGP.

The RM feature provides full visibility of the IP network and associated 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 network discovery to create a complete mapping of the network underlay to the service overlay. The VSAP automatically monitors virtual services as they relate to the VM and Virtual Port (vPort) state, with BGP reachability analysis to monitor the BGP state for VMs and network elements in the network.

Network object persistence
Virtual service objects, such as VM or vPort endpoints, are inherently mobile; they may be created/deleted or indeed moved on a frequent basis. The VSAP tracks these objects via their Universal Unique Identifier (UUID) and maintains state, reachability, alarm correlations, statistics and other data related to that object.

Virtual service objects move and are automatically deleted, which can make after-the-fact analyses challenging. To ensure historical service information is not lost, the VSAP logs persistent images of all service objects.

Event retrieval log and correlation
Network events are stored in an event log, which can be used for fault correlation. Operators can open the event log from the network service view or from the VM view. If the operator opens the log from the service view, the log events related to that service are provided. When opened from the VM view only events related to a specific VM are displayed. The operator can also specify a period of time to query the log for events.

The event log stores BGP events and network events for both root-cause analysis and impact analysis. BGP events include reachability alarms and flapping occurrences for the BGP prefix. The operator can retrieve information on a network service and troubleshoot historical events by correlating service events to BGP events.

For example, a "Prefix Down" BGP event means the virtual object was likely deleted and there will be a VM Down event for the related virtual object. In this case, an alarm would not be raised as long as the relation between events is evident. Flapping events on the VM can occur for legitimate reasons, which can be distinguished by the VSAP so that alarms regarding VM state changes can be suppressed and only generated when needed.

Learning correlation algorithm
The VSAP uses an algorithm to determine the window in which to find a correlated event, called a learning correlation algorithm. The algorithm dynamically learns the correlation interval and calculates the average and standard deviations. The algorithm takes into account variables such as time delays and VSAP system load. The learning correlation algorithm improves event and alarm correlation reliability over that of a basic correlation algorithm.

BGP event correlation
The VSAP correlates network events for impact and root-cause analysis. For the purposes of event correlation, the "IGP Upstream Connection Up" and "Down" events are similar to the "vSwitch Controller Up" and "Down" events. The IGP monitor is used to discover and log the upstream router events. An "IGP Upstream Redundancy Change" event is logged when a second path to a reachable upstream router is discovered.

VSAP fault correlation engine
The VSAP supports a unique fault management framework for datacenters. In addition to the fault management rules provided as part of the RM, the VSAP supports a set of correlation rules, which help operators monitor and troubleshoot virtual network and service objects. The VSAP correlation framework is extended to persistent images of virtual network and service objects to allow the operator to view the impact analysis for moved or deleted VMs, for example. This framework allows for more flexible correlation rules and allows correlation between specific alarms.

The VSAP fault management framework includes rules for correlating datacenter alarms across the following:

- Service status from virtualized service sites to virtual network components (vSwitch, vPort and VM, for example)
- Threshold crossing alarms from virtualized service sites to the vPort
- BGP prefix reachability alarms from IGP monitor to virtual network components
- BGP prefix reachability alarms from virtual network components to virtualized service sites

Wide area network services management

The VSAP provides an advanced toolset to assist in the operation and management of remote branch equipment connected via the Nuage Networks Virtualized Network Services (VNS) solution.

A Remote Health Agent (RHA) is built into the Nuage Networks 7850 Network Services Gateway (7850 NSG). The VSAP uses the RHA to provide a set of advanced monitoring and diagnosis tools that reduce the complexity of wide area network management.

The RHA is a lightweight agent that resides in the operating system of the 7850 NSG. It intelligently monitors system state, underlay and overlay network states and collects service statistics for central collection on the VSAP.

The VSAP collects and processes this information, and correlates this with other NSGs in the service construct to take actions such as raise alarms or perform automated OAM processes. These processes include further tests to diagnose problems such as overlay reachability checks, to track route-correlations for root-cause analysis, or to mirror traffic to the network operational center.

Statistics collection and plotting overview

The VSAP performs on-demand or scheduled statistics collection for managed network elements, services or virtual network objects. These statistics can be used to monitor or troubleshoot a datacenter's network, or to perform 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 form using the statistics plotter.

Statistics collection

The VSAP collects network performance statistics by polling network element MIB tables using SNMP. Performance statistics provide information about physical equipment, routing and other network element properties. MIB statistics collection policies define performance statistics collection at the network element level or the network object level. The VSAP supports the collection of some statistics counters from standard system, interface and routing MIBs on generic network elements.

The VSAP collects accounting statistics to gather throughput information for queues that are associated with virtual services and network ports. Accounting statistics policies can be defined for vPorts to monitor service or network accounting statistics.

VSAP system health

The VSAP collects server performance statistics to monitor internal system functions and processes. Server performance statistics are collected from internal VSAP data, such as memory usage and alarm counters.

IGP statistics

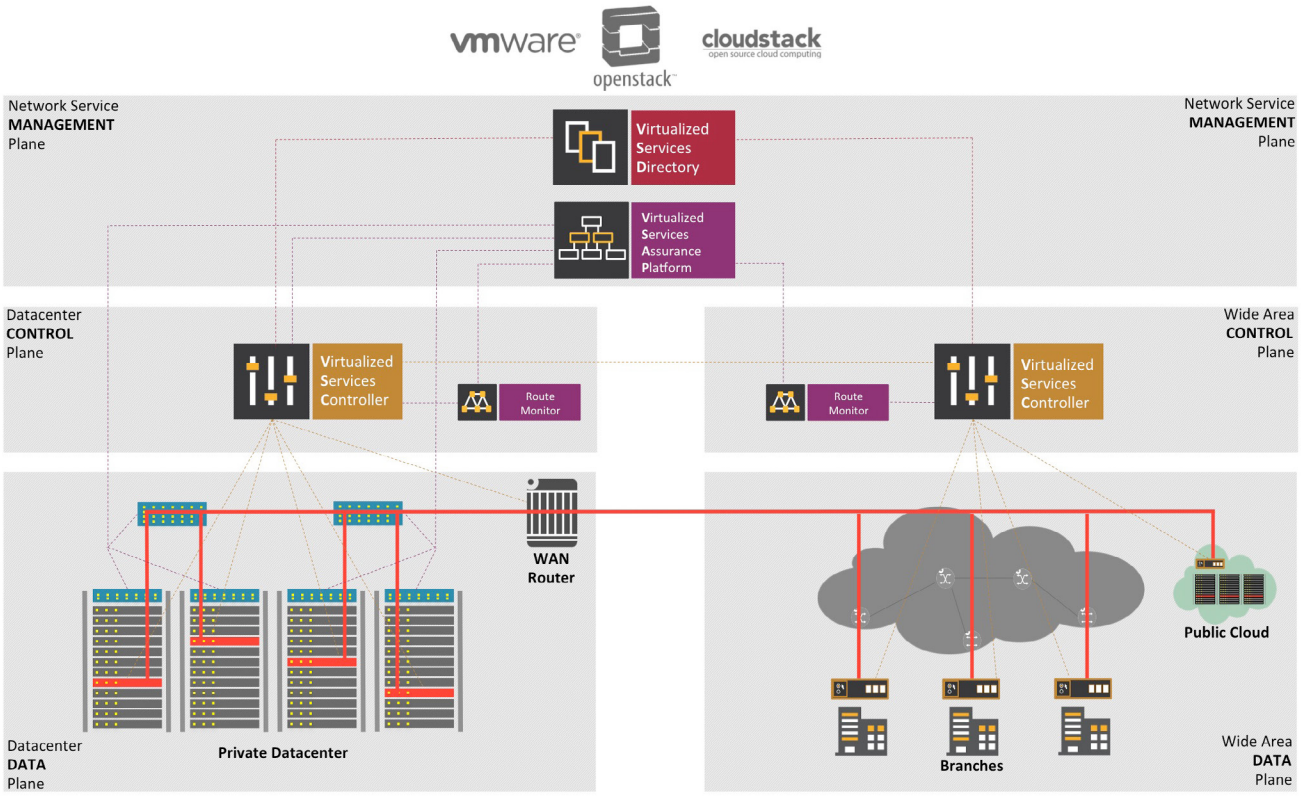
IGP statistics are collected by the RM and retrieved by the VSAP. MIB statistics policies can be applied to the RM to define the collection of specified statistics counters. IGP statistics can be plotted and stored using the statistics plotter. The VSAP has IGP-specific threshold crossing alarms, which are raised by the RM when specified thresholds are reached.

Statistics plotting

All supported statistics types can be viewed in tabular or graphical format using either historical or real-time data. Tables list specific values of historical data, and table data can be sorted, filtered and exported to files in different formats. Graphs can be used to identify trends and display multiple statistics counters simultaneously using the VSAP statistics plotter.

The statistics plotter graphs collected statistics from a specified time period, including real-time plotting. The statistics plotter can plot ingress and egress utilization statistics using calculated values. Plotted utilization statistics provide an accessible view of the bandwidth usage on a specified vPort in both tabular and graphical form.

Figure 1. The Nuage Networks Virtualized Services Assurance Platform within the network



Key benefits

FEATURE	BENEFIT
Overlay/underlay network correlation	■ Visibility in the SDN (overlay) and multi-vendor IP (underlay) network domains to improve root-cause and impact analysis troubleshooting. ■ When underlay failures affect a VM, the administrator can track the issue and diagnose the problem to the specific area of the IP fabric. For intermittent network connectivity the VSAP maintains a historical record of state changes in both the IP and SDN domains to provide audit capabilities to isolate the root cause.
Fault diagnosis and correlation	■ Analysis of underlay IP fabric faults matched to SDN overlay paths and IP hosts to provide advanced correlation and root-cause analysis of any service-affecting network outages. ■ Path visualization for connectivity between physical and virtual network endpoints provide end-to-end network visibility for both virtualized and non-virtualized (bare metal) endpoints.
Proactive assurance	■ Statistics collection and monitoring of the health of both virtual and physical network elements. ■ Threshold Cross Alarms (TCAs) proactively notify administration of any abnormal events.
IP fabric topology view	■ Graphical view of IP fabric with network baseline functionality to provide historic snapshots of IGP topology and physical network equipment with color-coded link status highlighting changes. ■ The topology map is based on the running network configuration discovered via routing peers and logical links.
Network inventory	■ Visual representation of the virtual components in use, including Virtual Tunnel End-Points(VTEPs), Nuage Networks Virtual Routing and Switching agents and third-party hardware VTEPs
IGP visibility	■ Monitoring of real-time state information of the IP fabric IGP (BGP, OSPF and IS-IS) via silent peering to provide running topology visibility to the network operations team.