Nationwide CSP Improves Services, Slashes Network Complexity with Automated Assurance

The Problem: Staying Afloat in an Ocean of Network Alarms

One of the world’s leading Communications Service Providers (CSP) delivers a complete range of enterprise IT solutions—WAN connectivity, MPLS VPNs, Ethernet circuits, hosted voice-over-IP, managed cloud and security services, and more. But with customers consuming so many diverse services, the CSP was struggling to effectively monitor its services. One of its biggest issues was the management of its IP Backbone, Metro-Ethernet and transport networks, which was integral in providing the majority of its services. It lacked the ability to quickly diagnose and respond to issues across the sprawling MPLS and IP infrastructure. The size and complexity of the multi-vendor network made up of Cisco, Juniper, Ciena, and Nokia solutions - in addition to a number of other vendor’s routers and switches - made on-going operations and management a challenge.

The network team was overwhelmed by as many as 250,000 alarms every day, making it impossible to quickly zero in on the real, serious issues versus the symptoms. Worse, even when the true problem was identified, they couldn’t tell which customers were impacted without manually comparing the network topology with customer management databases. This made it difficult to immediately recognize which problems were likely to result in expensive service-level agreement (SLA) violations. Additionally, the CSP’s network management system (NMS) rules had to be updated each time the network topology changed or a new service was deployed - a huge manual effort that took thousands of hours annually.

The Solution: Automated Diagnosis, Correlation, and Prioritization

With VMware Smart Assurance, the CSP drastically simplified network operations—making life much easier for its network operations teams while improving the service experience of its customers. Smart Assurance automatically discovered the topology of the network via standard protocols, directly interfacing with thousands of physical and virtual devices from a multitude of vendors. It also was able to identify the label-switched paths (LSPs) and virtual routing functions

About The Client

Industry: Telecommunications

Product: VMware Smart Assurance

Challenge: Network Operations could not maintain Service Level Agreements and had to pay penalties due to prolonged outages. Outages could not be diagnosed quick enough due to lack of visibility and too many alarms.

Results:

Reduced 250,000 alarms per day to 110

Automated root cause analysis to quickly pinpoint problems

Prioritized response for critical customers and SLAs

Automated closed-loop actions via integration with customer databases and ticketing systems

Saved 1000s of hours by avoiding manual updates
(VRFs) and automatically relate the MPLS infrastructure to the configured VPNs, layer 2 services and the associated subscribers. Smart Assurance continuously maintains a view of the service providing objects, their inter-relationships, the configured services and consuming subscribers to automatically determine the root cause of issues. The benefits of this comprehensive view resulted in a reduction of network alarms from 10,000 to 1 for scenarios such as a simple fiber cut. Troubleshooting time was reduced from hours to minutes, and unnecessary truck rolls eliminated.

When issues arise, Smart Assurance ingests data directly from the devices and element management systems (EMS), automatically correlating all symptoms and status of devices. It then compares this information against signatures in the Codebook engine to identify the root cause of the problem. Now the operations teams can quickly see the real issues and respond, without having to sift through thousands of low-priority alerts. Smart Assurance can also trigger automated actions to remediate routine issues without requiring any human intervention. Together, these capabilities have reduced the CSP’s daily alarms from 250,000 to just 110 authentic issues.

Impact Analysis via API Integration with Customer Databases

Smart Assurance also integrates directly with the CSP’s customer databases via APIs to get tenant information, allowing the network team quickly see which customers are impacted by any issue. The solution leverages a scoring algorithm that calculates the value of impacted customers and services to assess the criticality of each problem. For example, if a card fails on a router, Smart Assurance will show which VPNs (and which internal and external customers using them) are affected, so the team can prioritize its response according to the business need. The system can also output information to external support systems and automatically issue trouble tickets.

Additionally, unlike the CSP’s previous NMS (and many others), Smart Assurance is not rules based. This means they don’t have to dedicate multiple full-time engineers to continuously update rules and scripts, freeing up thousands of personnel hours per year that can be devoted to more strategic and revenue-generating efforts.

99.9%

fewer network alarms

Thousands

of personnel hours freed from manually updating NMS rules.

Learn More

For additional information about VMware Smart Assurance:

1-877-VMWARE
(outside North America, dial +1-650-427-5000)
telco.vmware.com