Visualize Your Networks with Automated Assurance

Gain Insights into Telecom Services and Networks with Multi-Layer Assurance

Service Assurance At a Glance

The automated service assurance capabilities from VMware by Broadcom monitors and analyzes multi-vendor physical and virtual environments in a single platform.

Key Capabilities and Benefits

- Simplify NOC and SOC operations with a centralized, cross-domain view.
- Gain rapid insights with integrated fault and performance management, service management, root-cause analysis, and impact assessment.
- Reduce costs and complexity through automation and optimization for assurance across layers and domains.
- Use closed-loop automation and rapid remediation to reduce OpEx and optimize resources and workloads to meet surges in demand.
- Increase operational efficiency by using artificial intelligence and machine learning (AI/ML) for rapid problem isolation, automatic suppression of extraneous alarms, and automated rule updates.

As communications service providers (CSPs) strive to deliver mission-critical telecommunications services, end-to-end service assurance is essential. New services must be operationalized in real time and managed proactively to meet quality expectations and service-level agreements (SLAs). Downtime is not an option.

To deliver differentiated services with agility and scalability, CSPs are adopting a cloud-native approach. Meanwhile, with the advent of 5G services, intelligence and data are moving to the edge.

Such changes require a new approach to service assurance. Many existing tools are inadequate for monitoring a distributed multi-layer, multi-vendor, virtualized and containerized environment. Cloud-native deployments with thousands of components and network functions make it extremely difficult to get clear visibility of diverse infrastructure and to obtain the deep insights needed for root-cause analysis.

Traditional manual fault identification and remediation processes are incapable of rapidly handling this complexity or the large volumes of telecommunications network data, events, and alarms. Since traditional processes do not associate identified problems with impacted services and customers, real-time SLA commitments that require high reliability and availability are jeopardized.

Meeting SLA and service quality expectations in real time requires automated remediation across layers for physical and virtual infrastructure, management, network functions, and services.

Operational intelligence and end-to-end automated assurance

The automated service assurance capabilities from VMware by Broadcom let you monitor physical and virtual components from the core of your networks to the edge, including the radio access network (RAN). From a centralized location, you gain integrated operational intelligence for your network infrastructure and components across multi-vendor domains, including physical, virtualized and containerized environments.

The telco-focused service assurance solution combines in a single platform capabilities such as fault management, performance management, service management, root cause analysis, and service impact analysis. With actionable insights in near real time and end-to-end visibility of physical, virtual, and service

Packaged with Other VMware Telco Solutions

Service assurance capabilities are tightly coupled with the advanced package of VMware Telco Cloud Platform and with VMware Service Management and Orchestration, providing end-to-end multi-layer assurance from the transport to service layers across the core of your networks to the edge, including the RAN.

VMware Smart Assurance is now a part of the service assurance capabilities, creating a comprehensive assurance solution that enables you to automatically import and aggregate metrics, alarms, and topologies from multiple components of the network.

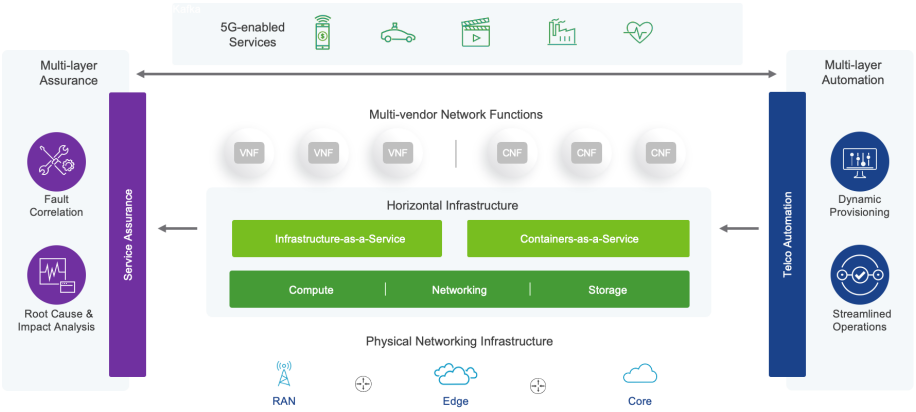

Figure 1: The multi-layer, cross-domain capabilities of the service assurance solution from VMware.

layers, network operations centers (NOCs) and service operations centers (SOCs) can manage many networks as one to rapidly resolve network issues.

Closed-loop remediation cuts across infrastructure, network functions, and service layers to manage real-time SLA and service quality conformance. The automatic association of issues enables you to determine the root cause and automate the remediation of issues by priority to deliver a consistent level of service quality. The result of automated closed-loop remediation reduces costs, improves operational efficiency, boosts customer satisfaction, and improves network reliability.

Service management by associating operations with customers

Telecommunications services require reliable and consistent service quality, which makes it essential to visualize and manage the network from a service and customer perspective. That requires making the connection between a network fault or performance degradation with the services and SLAs impacted.

VMware, through its service assurance solution, bridges the gap between operations and customer care by automatically associating infrastructure failures with service impacts affecting customers or tenants. The solution identifies the technology and business objects affected by each problem to connect the business context with the infrastructure issue.

To prioritize support efforts, the solution generates a service health impact analysis presented on a dashboard with an impact value associated with each problem. The analysis includes the following:

- See at a glance the problems that require priority remediation.
- Correlate all the active, inactive and unknown alarms together with the network topology to rapidly identify the problem's root cause instead of presenting the user with thousands of separate symptom alarms and alerts from a plethora of tools.

The solution identifies the technology and business objects affected by each

Holistic Assurance to Associate Problems with Customer Impacts

With the service assurance solution from VMware, you can holistically monitor and gain deeper insights into complex virtual and physical telecommunications infrastructure and services end to end, from the core of your network to the edge.

One Place, Many Devices

From a single pane of glass, the service assurance solution provides multi-layer automated assurance in a multi-vendor and multi-domain environment. More than 4,000 physical and virtual devices are supported.

- Use operational intelligence to reduce complexity
- Perform rapid root-cause analysis
- See how problems impact services and customers

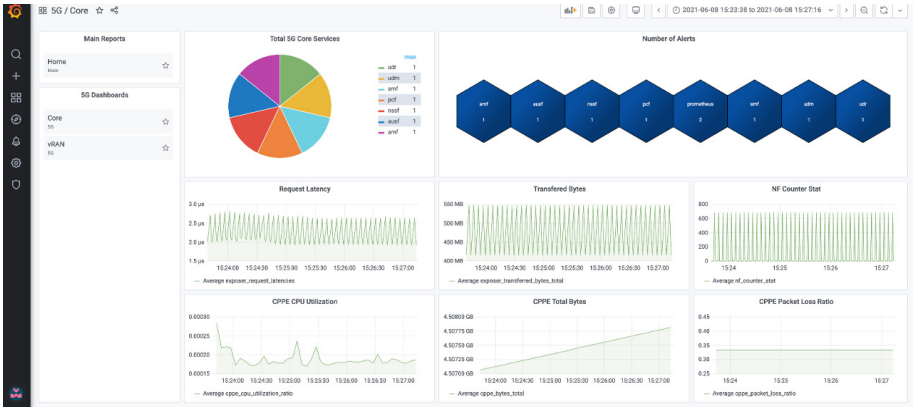

Figure 2: Service management.

problem and then analyzes the failure's impact on the service and customer. It also issues notifications and triggers actions.

By putting infrastructure problems in a business context, you can prioritize responses in real time and focus on tenants with priority services and SLAs.

Automated root cause and service impact analysis

The solution's root cause and service impact analysis capabilities rapidly resolve problems by correlating symptoms from the following layers of the infrastructure stack and pinpointing the problem's root cause:

- Physical and virtual
- Containers as a service (CaaS) and Kubernetes clusters
- CNFs and VNFs
- Services and applications
- Transport network

The results of a business impact analysis then drive closed-loop remediation through integration with the resource, service and lifecycle management orchestrators from VMware that are based on SOL API standards.

The combined solutions' remediation policy framework automates the processes and procedures for common faults that can be handled without human involvement.

- Define policies to allow automated remediation actions when infrastructure faults occur that affect service.
- Take different automated remediation actions based on a problem's duration.
- Manage remediation with alerts.
- Drive automated closed-loop actions for infrastructure lifecycle management by making recommendations to orchestrators based on root cause issues, such as a need to allocate more vCPUs on a node to handle increasing traffic.

Unified Data Collector SDK

The service assurance solution's data collection framework collects data and alarms from different layers and sources, including third-party monitoring tools by using the data collector software development kit.

The SDK is built on a programmable Python-based framework that collects data for fault and performance monitoring from such sources as Kafka, REST, and SNMP.

The collector SDK includes pre-packaged tools for development and validation.

Automated discovery and topology mapping

Proactive service management carries several requirements:

- Automated discovery of network functions and their relationships to services
- Automated root-cause analysis
- Proactive remediation
- Service impact analysis.

The mix of physical, virtual, and containerized network functions can obscure their interrelationships, dependencies, and relationships to a tenant or telecommunications service.

To overcome this complexity, the service assurance solution automatically discovers on-premises and cloud network resources in real time by using standard APIs.

It then provides an end-to-end topology map that shows the physical and logical connectivity and relationships between the underlying network infrastructure and the software components that compose the telecommunications service.

AI/ML-driven fault and performance management

Using artificial intelligence and machine learning, the service assurance solution automatically establishes dynamic performance baselines and calculates real-time performance metrics. It identifies anomalies or performance degradations, and alerts you when anomalous behavior is detected.

Operational efficiency is increased with automatic suppression of thousands of extraneous alarms and elimination of costly manual upkeep of static rules. Resources and workloads are optimized dynamically to meet ebbs and surges of service requirements.

The results of the end-to-end fault and performance monitoring across physical and virtual layers are visualized graphically. Because the service assurance solution from VMware includes a contextual topological view of both the underlay and overlay networks, you can accurately triage situations and take proactive steps to prevent serious impacts to application performance for your telecommunications services.

Advanced Alerting and Insights

The size and complexity of traditional telecommunications networks makes it difficult to manage a multitude of alerts with intricate logic involving various parameters. To overcome such difficulties, the advanced alerting and insights capabilities of the solution let you create customized alerting rules with complex threshold logic using multiple conditions and parameters for alarms and triggers. Furthermore, alarm definitions for different issues and anomalies can be tailored with customizable tags, which are automatically populated with data from multiple collectors to generate actionable notifications.

SD-WAN Assurance

VMware extends its service assurance capabilities to VeloCloud SD-WAN, allowing you to obtain end-to-end visibility and control over the entire telecommunications network, from core to RAN to WAN, ensuring optimal performance, reliability, and security.

Use cases

The use cases for the service assurance solution include the following:

USE CASE	DESCRIPTION OF SOLUTION
5G RAN and core	Both CNFs and VNFs are automatically discovered and shown graphically in the network topology map, including how they are physically connected, by using latitude and longitude. When CNFs or VNFs are impacted by failures or exhibit performance degradation, you are notified with actionable insights for the immediate remediation of the root cause.
IP and transport network	The solution monitors complex L2 and L3 networks and automatically determines causality of the physical and virtual network infrastructure and the end-to-end connectivity. Remediation is achieved by invoking the Element Management System (EMS), by using the SDN controllers, or by running predefined scripts.
Cloud infrastructure	The solution integrates with VMware Aria Operations to monitor virtual infrastructure. With the combined solutions, detailed insights on compute, networking, and storage are collected and correlated against the data from the network functions and transport layers to perform end-to-end root cause analysis.
Pipeline reporting	The solution monitors and validates the accuracy of the configuration at each stage of network infrastructure deployments to mitigate the failures caused by an incorrect deployment. Pipeline reporting lets you see the stages of deployment and configuration in one place while enabling you to take immediate action to troubleshoot issues so deployments continue without interruption.
SD-WAN assurance	The solution integrates with VMware VeloCloud SD-WAN to provide end-to-end visibility and control over the entire telecommunications network, from core to RAN to WAN, ensuring optimal performance, reliability, and security.

Comprehensive service assurance

The service assurance solution from VMware delivers end-to-end visibility across multi-vendor vertical tiers of physical, virtual, and cloud-native infrastructure as well as the horizontal domains of fixed line, transport, core, RAN, and edge.

- Discovery and topology mapping
- Business impact analysis
- Automatic suppression of extraneous alarms
- Automated root-cause analysis
- Automated closed-loop remediation
- Performance and fault management driven by AI/ML

The result improves efficiency, reduces operating costs, maintains the quality and reliability of telecommunications services, and ultimately boosts customer satisfaction.

Learn MORE

For more information about telco assurance from VMware, call 1-877-VMWARE (outside North America, dial +1-650-427-5000) or visit https://telco.vmware.com/

vmware® by Broadcom

Item No: bc-vmw-telco-cloud-service-assurance-so 9/24