ZERO TOUCH, ZERO TROUBLE STARTS WITH AIOPS-ENABLED SERVICE ASSURANCE

Innovations like virtualization, converged network services, and the telco cloud offer exciting possibilities for communication service providers (CSPs) and their customers—provided they can solve the accompanying operational challenges. The evolution to software-defined everything can let operators activate services in minutes, not days; scale resources more flexibly to improve service while optimizing cost; and push workloads to the network edge to support new use cases in a more mobile and connected world—the list goes on.

But to realize this vision for the future of their industry, CSPs will need to modernize and transform service assurance in tandem with their environment. Traditional silo-based practices and technologies simply won't be able to meet expectations for greater agility, prediction, and automation. As IT and network technologies converge and hybrid and public clouds reshape the infrastructure, CSPs will need to take a new approach to service assurance—one that uses a common, artificial intelligence for IT operations (AIOps)-powered platform. This will improve reliability, accelerate mean time to repair (MTTR), improve agility, and enable the shift to zero touch and zero trouble operations across the converged environment.

Virtualization leaves traditional service assurance behind

One of the main reasons network operators are adopting virtualization is to enable greater speed and agility. Customers are annoyed when a new service takes three days to be activated, and developers and operations teams want to be able to spin up new services that span multiple

technology domains as quickly as possible. CSPs also want the flexibility to move workloads from the data center to the edge to support low-latency use cases like autonomous vehicles and virtual reality. In a software-defined world, operators have the freedom to reinvent their business at digital speed.

But service assurance is already proving to be a critical brake on this transformation. Designed for the massive, static, hardware-based, and slow-moving networks of the past, traditional approaches can't keep pace with the dynamic and converged nature of modern environments. Siloed, duplicative, and overlapping assurance technologies for IT and network infrastructure make it more difficult to monitor services, fix faults, and manage resources for functions with dependencies in both domains, such as virtualized network functions delivered over hybrid cloud.

In the old days, when an issue affected the network, the network operations team could usually infer the cause by looking at a relatively small set of logs and monitors. In a converged environment, those investigations can span both network and IT technologies as well as a Google, Azure, or Amazon Web Services (AWS) Cloud, making root cause analysis a much more challenging prospect. Meanwhile, the use of shared cloud resources introduces new types of issues that traditional network monitoring tools can't easily pick up, like a "noisy neighbor" virtual machine (VM) or a container starving other functions of resources. Correlating issues across silos and determining root causes becomes an exercise in frustration, while manual, disconnected processes increase MTTR and cost.

The threat to service quality is exacerbated by the reactive nature of traditional service assurance solutions. Aside from routine preventative maintenance, most operational behavior has consisted of waiting for something to break before acting—an approach that makes it impossible to maintain the reliability and availability customers now expect. When you can't stop problems from affecting service, and it takes you longer to resolve them, customers end up with poor voice quality, jittery video, or stalled downloads that are more frequent and last longer. That's a critical business problem for CSPs in hotly competitive markets where switching incentives are common and customer loyalty is fleeting.

To keep their converged infrastructure healthy and their services running at their best—and keep their customers, CSPs need to unify and automate service assurance—and ultimately drive to zero touch, zero trouble.

Building AIOps into service assurance

Slow, siloed, and largely manual processes make it far too difficult for operations teams to manage their environments and solve problems, much less work proactively to prevent problems and plan for future needs. What they need now is a way to achieve unified observability across both hybrid cloud and network infrastructures, quickly correlate this data, interpret its meaning, and act quickly to assure service quality.

With a unified, cloud-native AIOps platform, IT operations (ITOps), and network operations (NetOps) teams can leverage built-in intelligence to automatically identify the underlying conditions contributing to a disruption. Noise suppression helps teams work more efficiently by removing distractions and false alarms. As generative AI technologies like ChatGPT reshape the way people interact with systems, AIOps can translate complex root causes into natural language summaries and next-step suggestions. By correlating data across multiple network and technology domains, these technologies can understand the actual customer impact and provide timely and accurate

notification—a key element of a satisfying customer experience.

Shifting from reactive to proactive, AIOps can help teams predict future issues and see packet loss earlier to improve network reliability. To enable automated remediation and self-healing, the platform can prompt a network orchestrator to take steps such as restarting a given device or changing a parameter on the configuration setting to resolve an issue before it impacts service level agreements (SLAs). A self-learning AIOps platform helps ITOps and NetOps teams improve agility by automating the configuration of monitoring and management rules for cloud-native and dynamic infrastructure services and applications. By analyzing trends, forecasting scenarios, and simulating demand, CSPs can plan accurately for the capacity needed to support new products effectively at a high level of quality.

Completing the vision for the modern CSP

While AIOps can help CSPs evolve toward a zero touch, zero trouble model, there will always be situations where human intervention is needed. In the previous blogs in this series, we talked about the requirements for a unified network service management platform to streamline that resolution flow, as well as the unified discovery needed to provide complete data and visibility across converged infrastructure. Together, these three capabilities form the foundation for a new era of autonomous networks delivered through dynamic, multi-domain, hybrid cloud environments.

To learn more, read the first two blogs in this series, Modern CSPs Need Unified Visibility Across Hybrid Cloud and Demanding Markets Drive CSPs to Transform Network Service Management.

Then visit https://www.bmc.com/blogs/bmc-helix-receives-catalyst-showcase-award/ to find out about how BMC recently won a TM Forum catalyst award.