Telecommunications Network Performance Management

The challenge

In today's digital world, Communications Service Providers (CSPs) depend on software-based services to engage customers, automate processes, drive innovation, and unlock business insights. CSPs are responsible for delivering these mission-critical services and need to ensure that they are always available and responsive. Otherwise, the financial and reputational impact can be devastating.

However, this is an enormous challenge. Many CSPs continue to operate in silos, using multiple tools to monitor the health of individual domains, such as cloud and serverless infrastructure, networks, storage, and more. This leaves networks drowning in disconnected, redundant data, with a single issue often creating thousands of events. And, many events are just noise and none of them have any business or service context.

Network staff must manually filter and correlate this deluge of event data—and, when they do finally get to the bottom of a service issue, there's no easy, automated way to remediate it. The result? Lengthy service outages, escalating costs, and mounting financial and competitive damage.

The ServiceNow solution

ServiceNow® Telecommunications Network Performance Management (TNPM) uses the power of Artificial Intelligence (AI) and Machine Learning (ML) to turn this tidal wave of events into a trickle of actionable alerts—cutting through the noise, pinpointing service issues, and helping you to rapidly identify and remediate the root cause. Unlike legacy event management systems which are static and rule based, Network Performance Management applies machine learning and advanced analytics to correlate events, adapting automatically to rapidly evolving virtualized and cloud environments.

Network Performance Management consolidates data from your monitoring tools, intelligently normalizing, deduplicating, filtering, and correlating events to generate meaningful alerts attached to corresponding CIs in the ServiceNow CMDB. This reduces event noise by up to 99%. Event management then shows you the service impact of these alerts—which services are affected and how badly—and it also lets you automate remedial actions.

Network Performance Management can connect to other network monitoring tools via TMF642 API, a standardized interface from TM Forum. TMF642 API is a REST API for alarm management that supports end-to-end connectivity, interoperability and portability across complex OSS eco-system. The interface simplifies the process for creating, tracking and managing alarms, enabling rapid, repeatable, and flexible integration among operations support systems.

In addition, Network Performance Management identifies anomalous behavior in your network environment such as performance issues that can potentially cause service issues but are not automatically identified when capturing events. It does this by using AI and ML to automatically model normal behavior for performance metrics and detect anomalies for new metrics that fall outside predicted thresholds.

Together, these features help you detect, diagnose, and remediate service issues far more quickly and accurately, dramatically reducing MTTR and increasing service quality.

BENEFITS

Improve service availability and reduce MTTR with AI/ML

Leverage machine learning and automation to reduce event noise, transform events into actionable alerts, pinpoint service issues, identify likely root causes, and automate remediation. Measure service performance and identify anomalies that could lead to service outages or degradations.

Break down infrastructure silos

Consolidate events from multiple monitoring tools using a wide range of out-of-the-box connectors, custom REST, JavaScript, SNMP, or email, and leverage connectors built by third parties.

Increase productivity

Free up staff from time-consuming and error-prone tasks, including manually correlating events, creating and maintaining event rules, and setting and managing metric thresholds.

Deliver an intuitive user experience

See and prioritize service issues at-a-glance, seamlessly drill down to the underlying root cause, instantly identify CIs with similar issues, and resolve alerts using a single, integrated pane of glass.

Events, logs and metrics ingestion

Network Performance Management can ingest events, logs and metrics to deliver a comprehensive solution with AI/ML-based correlation, anomaly detection and predictive intelligence. It includes out-of-the-box connectors and standardized interfaces specified by TM Forum to a wide range of monitoring tools, and you can integrate other event sources via custom REST, SNMP, JavaScript or email. Connectors developed by third parties are also available in the ServiceNow Store.

Intelligent, adaptive correlation

Event Management uses machine learning to identify temporal and statistical patterns in your historical alert data. It then uses these patterns to correlate new alerts in real time, identifying groups of alerts that are caused by the same underlying issue. Instead of just seeing individual symptoms, you now know how these symptoms are related. You can provide feedback on the usefulness of these groups by adding or deleting alerts from a group. Instantly see service impact

Event Management works seamlessly with ServiceNow ITOM Visibility's Service Mapping feature, correlating alerts to identify impacted services. It then assesses the combined impact of these alerts on the service, displaying

Interactive service maps

Accelerate resolution with Alert Intelligence

Alert Intelligence simplifies alert resolution by giving you a single pane of glass where you can see all the critical information you need to address an alert, such as the alert description, affected CI, severity, impacted services, secondary alerts, and probable root causes. It also provides Alert Insights, using machine learning to identify re-peated alerts, similar past alerts and incidents, and relevant knowledge articles to help with root cause analysis

Alert Intelligence

Detect anomalous CI behavior

Network Performance Management uses machine learning to analyze raw operational metrics, automatically determining thresholds for normal behavior. It then detects and scores anomalies relative to these thresholds, with high scores indicating that a CI may be at risk of causing a service outage. Qualified anomalies result in alerts, which appear alongside other alerts in Operator Workspace and Alert Intelligence. This allows you to detect performance issues that may not be captured by events and avoids the need to continually adjust thousands of thresholds in your monitoring tools.

Anomaly Detection

Automatically remediate service issues

You can configure Network Performance Management to respond automatically to alerts, helping you to resolve service issues faster. For example, you can use Flow Designer to create sets of remediation actions, such as retrieving log files, freeing disk space, or restarting a service. These actions are triggered when an alert meets specific criteria that you define. You can also automatic-ally trigger tasks such as creating incidents, change requests, security incidents, field service work orders, or even customer service cases.

servicenow.

servicenow.com