Drive down service outages with AIOps

The IT challenge

In today’s digital world, businesses depend on software-based services to engage customers, automate processes, drive innovation, and unlock business insights. IT is responsible for delivering these mission-critical services and needs 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 IT organizations 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 IT 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. IT 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 IT costs, and mounting financial and competitive damage.

The ServiceNow solution

ServiceNow® ITOM Health uses the power of AIOps 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, ITOM Health applies machine learning and advanced analytics to correlate events, adapting automatically to rapidly evolving virtualized and cloud environments.

ITOM Health 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.

In addition, ITOM Health identifies anomalous behavior in your IT environment such as performance issues that can potentially cause service issues but are not automatically identified when capturing events. It does this by using AIOps 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 AIOps

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.

Leverage the combined power of ITOM and ITSM

Accelerate issue resolution with relevant, contextual change, problem, and incident data.

Increase productivity

Free up IT 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
ServiceNow® ITOM Health can ingest events, logs and metrics to deliver a comprehensive AIOps solution with AI/ML-based correlation, anomaly detection and predictive intelligence. It includes out-of-the-box connectors 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.

The Agent Client Collector is ServiceNow’s own monitoring agent to generate events and collect metrics on your Windows and Linux servers. Its centralized agent administration and packaged modules to collect data from the OS, application servers, middleware and databases help reduce the cost of ownership. You can extend the agent to rapidly meet your additional monitoring needs and still benefit from the AIOps capabilities of ITOM Health.

Finally, ITOM Health can ingest logs to understand normal behavior patterns and raise an alert when anomalous behavior is detected and even before the full issue occurs, thus adding predictive intelligence to ITOM’s AIOps capabilities.

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. Event Management then uses this information to automatically modify its future alert grouping behavior.

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 the results on Operator Workspace. Operator Workspace dashboard represents each service as a color-coded, resizable tile. This makes it easy to visually prioritize service issues based on issue criticality and service importance. Selecting a tile displays a view of primary alerts and the top priority alert affecting that service—allowing you to instantly focus on the probable cause of a service issue.

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 repeated alerts, similar past alerts and incidents, and relevant knowledgebase articles to help with root cause analysis.

Detect anomalous CI behavior
ITOM Health 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.

Automatically remediate service issues
You can configure ITOM Health 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 automatically trigger tasks such as creating incidents, change requests, security incidents, field service work orders, or even customer service cases.