Stop service outages in their tracks with ServiceNow® Predictive AIOps

The IT challenge

In today's digital world, businesses depend on digital services to engage customers, automate processes, drive innovation, and unlock business insights. IT is responsible for delivering these business-critical services and needs to ensure they are always available and responsive. 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, applications, networks, storage, and more. Instead of predicting and preventing service outages and degradations, IT is left drowning under a deluge of events and excessive noise. Teams struggle to keep up with the volumes or proactively detect the early symptoms of future service issues. And when IT finally gets to the bottom of an ongoing outage, they have to remediate it manually, causing further delays while the business continues to suffer.

The ServiceNow solution

ServiceNow® Predictive AIOps leverages the power of artificial intelligence to predict service issues, prevent impact to users, and automate remediation. It replaces a tidal wave of events with a trickle of actionable alerts, helping you identify and resolve service issues before customers and internal users are impacted. Predictive AIOps analyzes logs and metrics in a new way to detect application behavior issues that traditional monitoring techniques do not address since they mostly deal with grouping for preprogrammed failure scenarios. Predictive AIOps uses advanced machine learning and analytics techniques to proactively uncover and resolve complex, unforeseen service issues, including in evolving virtualized and cloud environments.

Predictive AIOps includes three intelligent capabilities that work seamlessly together to improve the health of your digital services:

- **Log Analysis and Anomaly Detection** identifies potential service issues before they cause service outages and degradations. It uses machine learning to identify normal operating patterns in logs, traces, and metrics—for example, specific log sequences or correlations between log field values over time. This includes correlating logs across different sources, such as a load balancer and its connected web servers. You can stream logs from Azure Monitor, Amazon S3, Amazon CloudWatch, Kafka, REST API and others. It then looks for antipatterns— disruptions in normal operational behavior—raising an alert against a corresponding CI when a significant antipattern is detected. This allows you to respond early and prevent service issues, rather than reacting once they occur. And because Log Analysis uses unsupervised learning, it automatically uncovers complex, distributed patterns without human intervention, including unanticipated patterns not foreseen by your IT operations team. In addition, there's an intuitive dashboard to visualize and track log alerts and anomalies.
- **Metric Analytics** collects raw metrics from the ServiceNow® Agent Client Collector and other monitoring tools, raising events against CIs when there is a performance anomaly. This allows you to identify service degradations that can lead to service outages. Predictive AIOps uses machine learning to automatically model normal metric behavior and set adaptive thresholds, eliminating the major effort needed to manually set thousands of thresholds—although these can be set manually if required. It also allows you to score anomalies based on how likely they are to lead to a service outage and provides heat maps and other tools that allow you to visualize and analyze metric data.

Predict and prevent service outages

Identify potential service issues before they cause service outages and degradations that impact your business.

Fix degraded services faster

Leverage machine learning and automation to reduce event noise, transform events into actionable alerts, pinpoint issues, diagnose likely root causes, identify potential fixes, and automate remediation.

Focus on what matters

Prioritize resolution of issues based on their service and business impact.

Reduce operational cost and increase productivity

Resolve service issues with an intuitive. intelligent single pane of glass that makes it easier to proactively identify, diagnose, and resolve service issues.

Scale for digitalization

Respond effectively to everincreasing business demands for high-value, reliable digital services.

Leverage your existing monitoring investment

Consolidate events from multiple monitoring tools using a wide range of out-of-the-box connectors and flexible, easyto-use custom integration framework.

- **Event Management** processes events, tags, and metrics to reduce noise. It also consolidates events from your existing monitoring tools, using AIOps techniques to turn a flood of these events into a small number of meaningful alerts. This reduces event volumes by up to 99%. If you don't have a CMDB yet, the Tag-based Alert Clustering technique helps correlate alerts based on the tags. When Event Management is used in conjunction with Service Mapping, you can see the service impact of these alerts, providing interactive service maps that make it easy to identify and prioritize service issues. It also carries out automated root cause analysis, showing you which CIs are the most probable cause of a service issue, along with associated confidence scores. This significantly reduces the time needed to diagnose service outages and degradations.

Instantly see and investigate service issues

Predictive AIOps comes with Operator Workspace that gives you a consolidated view of your business services. Prioritized service health issues are highlighted on an intuitive, colorcoded service health dashboard, making it easy to identify issues at a glance

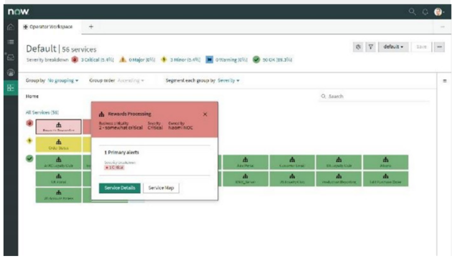
From here, you can drill into specific service health issues, showing related CIs and alerts on an interactive service map. You can also see associated incidents, change requests, and detected configuration changes on the same pane of glass, providing operational context that helps you to resolve issues more quickly—for example, determining whether an outage or degradation is related to a recent configuration change.

Keep pace with Intelligent, adaptive alert correlation

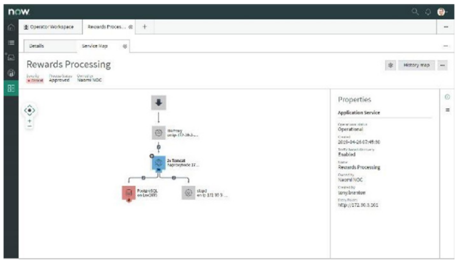
In the same way that Log Analysis identifies patterns in your log data, Event Management uses machine learning to identify temporal and topological patterns in your historical alert data. It then uses these patterns to correlate alerts in real time, identifying groups of alerts that are caused by the same issue. Instead of just seeing individual symptoms, you now know how these symptoms are related. You can also provide feedback on the usefulness of these alert groups, and even add or delete alerts. Event management uses this feedback to automatically adjust the way it groups alerts in future.

Correlate alerts without needing a CMDB

Tag-based alert correlation capability lets you group alerts based on similar alerts without needing a CMDB. The tags are derived from alert information coming from monitoring tools, also reducing event noise further. This feature provides rapid time to value since it's helpful even if you haven't discovered your IT infrastructure yet.



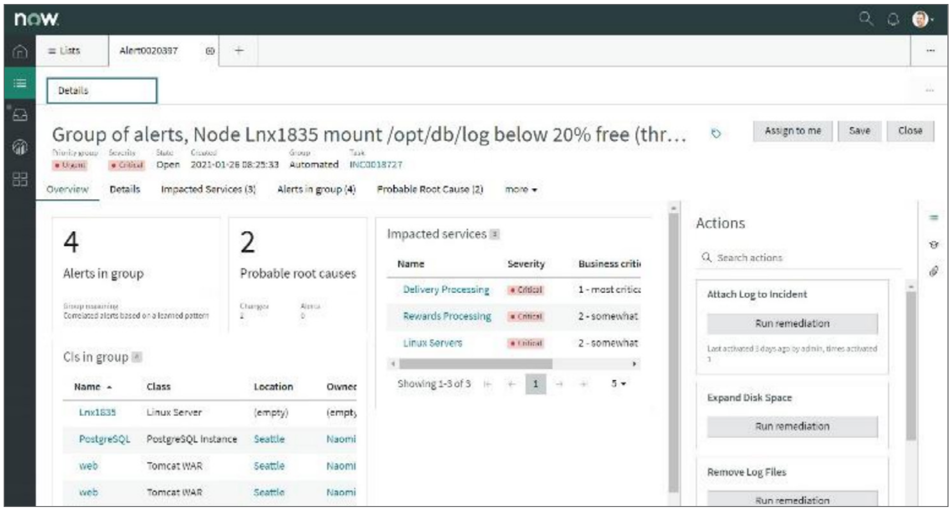
Operator Workspace



Operator Workspace

Accelerate resolution with Alert Intelligence

Alert Intelligence simplifies alert resolution by giving you a single pane of glass where you can see all of the critical information you need to address an alert, such as the alert description, affected CI, severity, impacted services, and secondary related alerts. It also provides Alert Insights, using machine learning to identify repeated alerts, similar past alerts and incidents, and relevant knowledgebase articles, as well as potential remedial actions based on previous resolutions.



Group of alerts, Node Lnx1835 mount /opt/db/log below 20% free (thr…

Priority group	Severity	State	Created	Group	Task
Urgent	Critical	Open	2021-01-26 08:25:33	Automated	INC0018727

4
Alerts in group
Group reasoning
Correlated alerts based on a learned pattern

2
Probable root causes
Changes 2
Alerts 0

Cls in group

Name ▲	Class	Location	Owner
Lnx1835	Linux Server	(empty)	(empty)
PostgreSQL	PostgreSQL Instance	Seattle	Naomi
web	Tomcat WAR	Seattle	Naomi
web	Tomcat WAR	Seattle	Naomi

Impacted services

Name	Severity	Business criti
Delivery Processing	Critical	1 - most critic
Rewards Processing	Critical	2 - somewhat
Linux Servers	Critical	2 - somewhat

Showing 1-3 of 3

Actions

Attach Log to Incident
Last activated 3 days ago by admin, times activated 1

Expand Disk Space

Remove Log Files

Alert Intelligence

Resolve service issues faster with automatic remediation

You can configure Predictive AIOps to respond automatically to alerts, helping you to resolve service issues faster. For example, you can use Flow Designer and IntegrationHub to create sets of remediation actions, such as retrieving log files, freeing up disk space, restarting a service, or attaching a knowledgebase article to the alert. These actions are triggered when an alert meets specific criteria that you define, or you can manually initiate these actions simply by right-clicking on the corresponding CI. You can also trigger tasks such as auto-closing an alert or creating incidents, change requests, security incidents, field service work orders, and customer service cases.

Leverage your existing monitoring tools

Predictive AIOps includes out-of-the-box connectors to a wide range of log collection tools, and you can integrate it with additional event sources via custom REST, SNMP, JavaScript, and email connectors. Connectors developed by 3rd parties are also available in the ServiceNow Store.

DS-PredictiveAIOps-050422