ServiceNow® Event Management

The IT challenge

Business today is increasingly digital, and services are software-based. IT provides the mission-critical services to engage customers, automate processes, create innovative technology, and unlock business insights.

With digital businesses it is a competitive necessity for IT to know the business impact of a service outage in real time, which infrastructure components deliver a specific service, and how these components are connected.

IT provides the foundation for business services, maintaining all resources such as cloud instances, serverless infrastructure, network infrastructure, storage, and more. Unfortunately, the multiple disconnected monitoring tools that monitor the health of the resources supporting the services, often increase the challenge IT faces. Each tool generates its own siloed stream of data, and multiple tools often report the same issue. It is left to manually correlate this information to understand what is actually happening and then struggles to assess the business impact. Yet even when staff manage to do this, there is still a huge amount of noise— a single issue can create thousands of events that may have no business impact at all.

The ServiceNow solution

ServiceNow® ITOM Health with Event Management reduces event noise generated by monitoring tools using Artificial Intelligence for IT Operations (AIOps). AIOps applies machine learning and analytics to IT Operations functions which dramatically reduces the time and effort of manually correlating events by automatically adapting to evolving IT environments. Legacy event management systems that do not provide this level of artificial intelligence leave IT organizations to struggle with huge volumes of poorly correlated events.

Event Management brings events captured by existing infrastructure monitoring tools into ServiceNow for consolidation, analysis, and action. Events are then processed through filters that normalize and de-duplicate the incoming event stream to generate alerts, reducing event noise by up to 99%. The user is also presented with the service impact— which business services are affected and how badly they are affected.

Benefits

Improve service availability with AIOps
Lessen service outages by using AIOps which applies a range of advanced machine-learning techniques to reduce noise, identify service issues and provide related incident, problem, change, and knowledge information to speed resolution.

Increase value from existing tools
Consolidate events captured by multiple infrastructure monitoring tools by integrating them through out-of-the-box connectors, 3rd-party connectors, REST API, or SNMP traps.

Understand root cause of service issues
Transform infrastructure events into actionable alerts and incidents that point to the root cause of service issues. All of this data is consolidated in the Alert Intelligence workspace for quick action to reduce MTTR.

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.

View business services impacted by a single alert
Integration with external monitoring tools

Event Management has out-of-the-box connectors to monitoring tools and can integrate to other event sources via a REST API, SNMP traps, email or JavaScript-based custom connectors. In addition, 3rd-party connectors are available from the ServiceNow Store.

Event Management collects raw events and processes them to generate more qualified alerts for the affected configuration items (CIs). Event Management deduplicates events from monitoring tools into a single normalized alert that can be automatically correlated with a CI in the ServiceNow® Configuration Management Database (CMDB). With an alert bound to a CI, Event Management is able to automatically relate configuration item, incident, problem and change history providing IT with a comprehensive insight to prior and existing issues. If you don’t have a CMDB yet, the Tag-based Alert Clustering technique helps correlate alerts based on the tags.

Use service maps for fast impact and root cause analysis

When ServiceNow® Service Mapping is used in conjunction with Event Management, IT gets a view of impacted services to help identify root causes and prioritize alerts appropriately. Through an interactive service map, IT can easily see configuration items experiencing issues impacting the service and their upstream and downstream dependencies. Automated root cause analysis provides a view of configuration items with confidence scores indicating the most probable cause of a service issue, dramatically reducing resolution time.

Alert Intelligence

Alert Intelligence can significantly shorten the mean time to repair (MTTR) and simplify the operator experience by aggregating all the critical information necessary to address an alert in one console. Opening an alert reveals details such as the description, affected CI, calculated priority, severity, activity, impacted services and a timeline displaying secondary related alerts. Alert Insights leverages machine learning to provide related information aggregated from current repeated alerts, similar past alerts, past incidents in addition to knowledge base articles to aid root cause analysis. Potential remediation actions that include past actions that were taken for similar alerts can be performed from Alert Intelligence, giving operators an accelerated route from events to alert to incident to resolution.