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. The financial and reputation impact to a business from service outages can be devastating in a time where services are expected to be always-on and always-available.

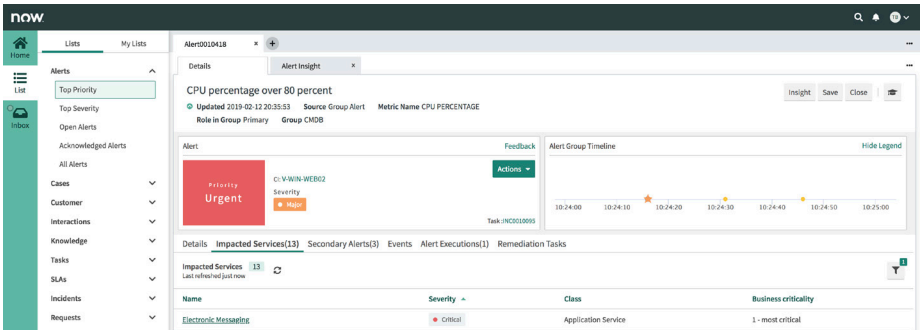
With digital businesses it is a competitive necessity for IT to know the business impact of a service outage in real time and to know which infrastructure components deliver a specific service and how these components are connected.

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 by eliminating redundant data and quickly assessing 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. In addition, there is no simple automated way to remediate impacted services. The result is lengthy service outages, poor Mean Time to Repair (MTTR) and a business that will soon be overrun by competitors offering more reliable services.

The ServiceNow solution

ServiceNow® Event Management reduces event noise generated by monitoring tools, using AIOps or Artificial Intelligence for IT Operations. AIOps applies machine learning and analytics to IT Operations functions and this dramatically reduces the time and the effort of correlating events because it automatically adapts to evolving IT environments. Unlike legacy event management systems that do not provide this level of artificial intelligence leaving IT organizations to struggle with huge volumes of poorly correlated events.

The application 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.



View business services impacted by a single alert

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 the service issues. All of this data is collected in the Alert Intelligence workspace for quick action to reduce MTTR.

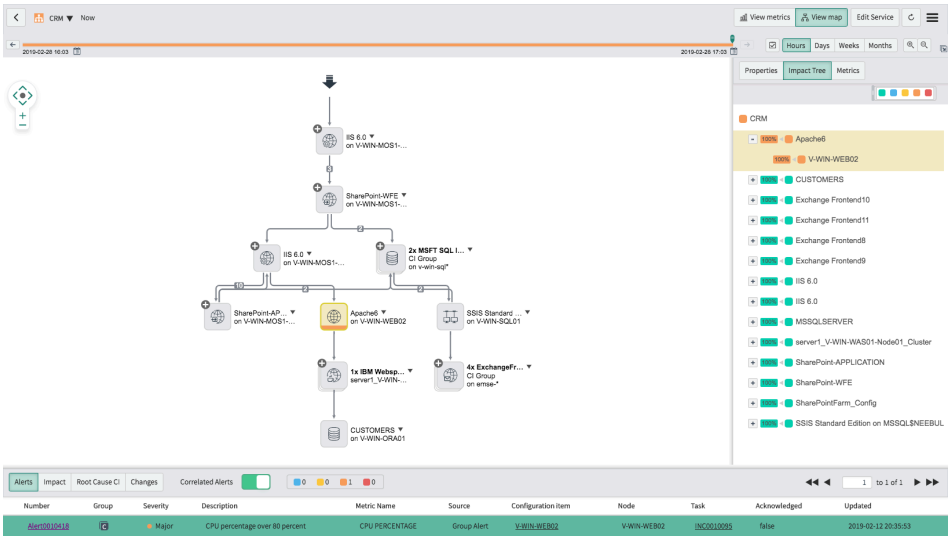
Integration with external monitoring tools

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 de-duplicates events from monitoring tools into a single normalized alert that can be automatically correlated with a configuration item 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.

Use service maps for fast impact and root cause analysis

Event Management uses ServiceNow® Service Mapping to correlate alerts with services providing IT with 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.



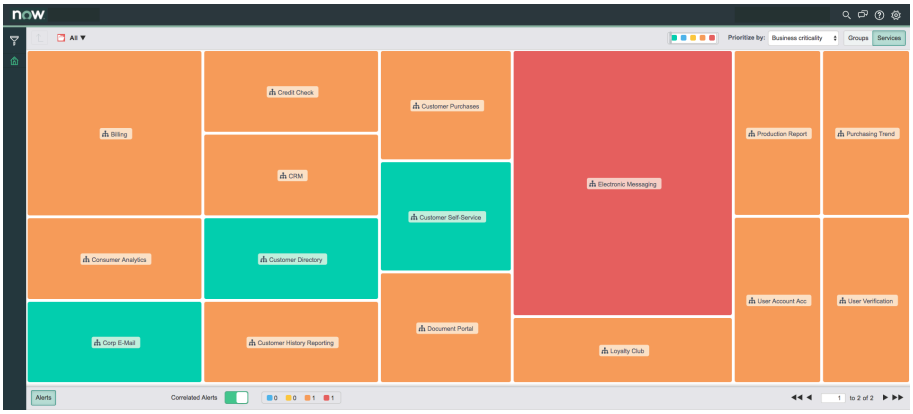
Use service maps for fast impact and root cause analysis

Identify and prevent service outages

IT can detect root cause issues and prevent service outages by using out-of-the-box, machine-learning techniques. By adding ServiceNow Operational Intelligence to Event Management, IT can also use operational metrics collected from monitoring tools via out-of-the-box connectors to investigate performance issues that may be precursors to service outages.

Event Management dashboard

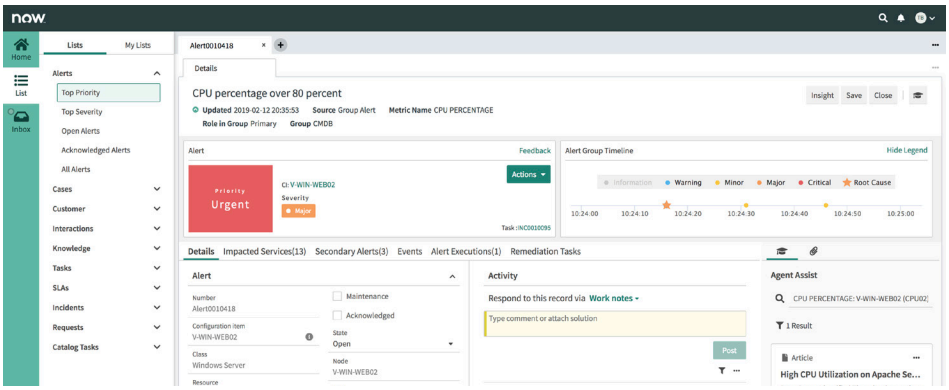
The Event Management dashboard provides a consolidated view of service health enabling IT to easily identify and assess the state of business services impacted by alerts. By selecting an alert IT can immediately see the related impacted business services, in addition to selecting a business service that shows only the related alerts. Tiles representing business services can be resized based on priority, severity and cost enabling quick prioritization. IT can drill into a business service from the dashboard to a service health map displaying the related configuration items (CIs), alerts, detected changes, incidents and change requests in a single pane of glass. The service health map allows IT to quickly determine the configuration item as the most probable cause and triage the issue. Triaging the issue by investigating configuration changes and viewing operational metrics can all be performed in a single view. Once a cause has been identified, remediation actions can be initiated with a simple right-click on a CI in the map, avoiding the need to switch between tools and dramatically improving operational efficiency and reducing MTTR.



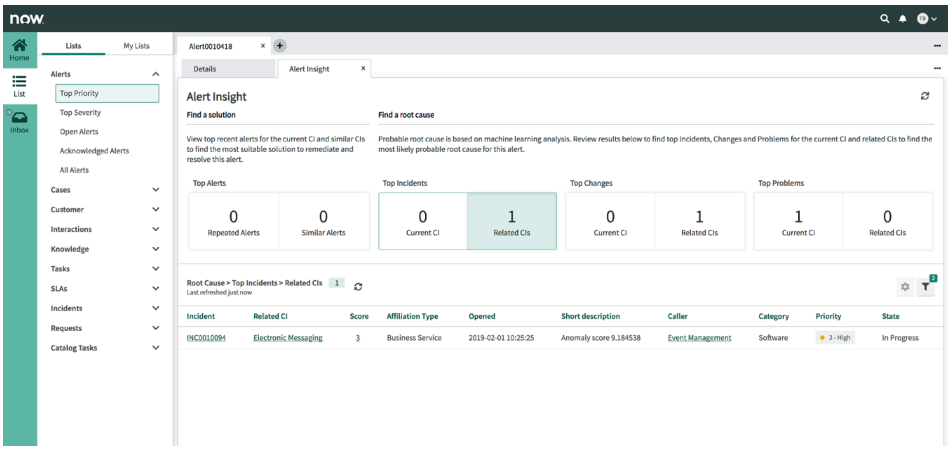
Service health dashboard makes it easier to identify issues and take action to reduce service outages.

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, past alerts similar to the current alert, past incidents in addition to knowledgebase 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.



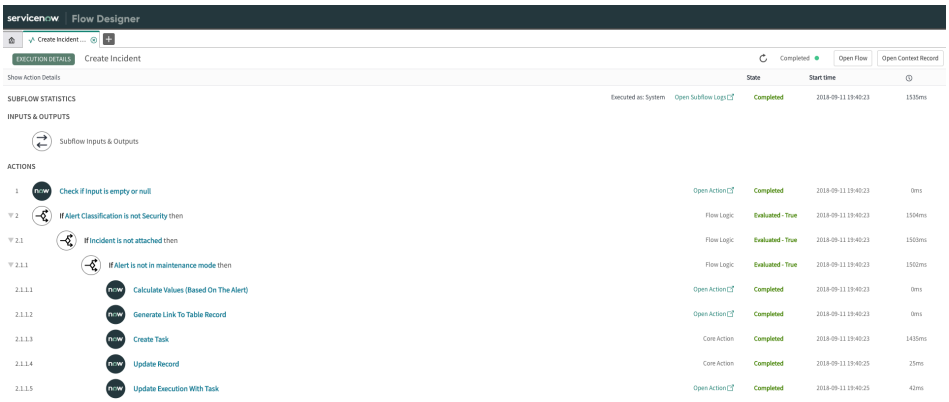
Viewing an alert's details in Alert Intelligence



Alert Insight aggregates related information to help identify a root cause and potential resolution

Automatic remediation

Event Management allows Alert Management Rules to be configured to automate responses to alerts meeting specific criteria, leading to faster resolution of service issues. Rules can be used to auto-close an alert or attach a knowledgebase article to an alert. Alert Management rules can also be used to automatically create tasks such as incidents, change requests, security incidents, field service work orders or even a customer service case. Using Flow Designer and Integration Hub, IT can create sets of remediation actions that can be automatically triggered or initiated from an alert, such as retrieving a log file, freeing space on a full disk, or restarting a service.



A flow for automatically creating an incident for an alert

SN-DataSheet-ServiceNowEventManagement-190217