

## ServiceNow Event Management

### Benefits

- **Automate the Creation of Alerts and Incidents from Events**

Transform IT infrastructure events into alerts automatically and trigger IT processes for faster remediation of service-impacting issues.

- **Understand Impact on Business Services**

Gain visibility into how infrastructure-enabled services are impacted by datacenter events through a consolidated overview dashboard and an interactive business service management map.

- **Leverage Existing Infrastructure Monitoring**

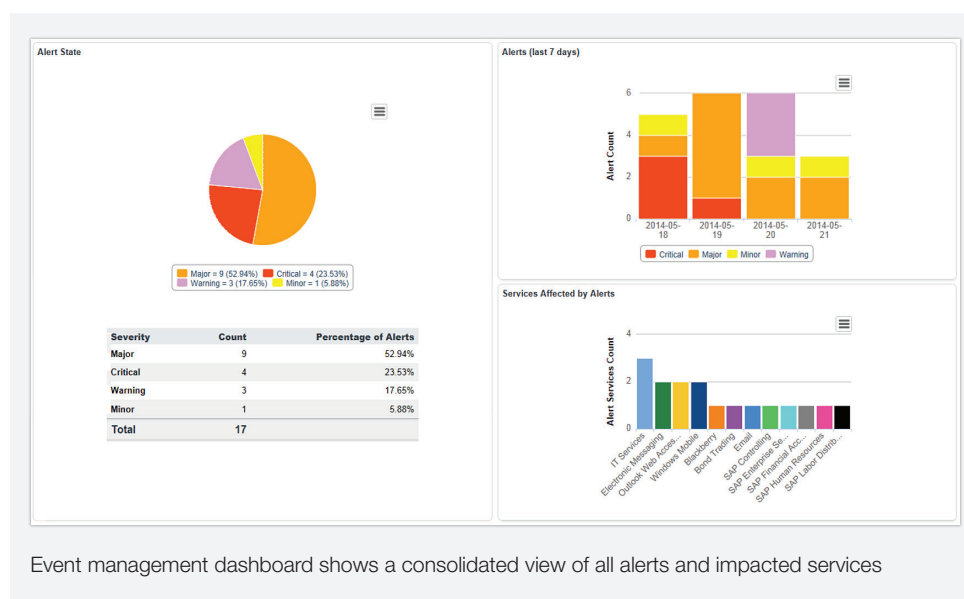
Connect existing monitoring tools easily to ServiceNow through a simple REST API.

### The IT Challenge

The enterprise relies on IT to maintain the compute, storage, and networking infrastructure that provides the foundation for business services. IT may use multiple tools to monitor this infrastructure, but often, the high volume of events from these different tools makes it difficult to understand the real issues and take corrective action. Furthermore, there is typically little visibility into the relationship between infrastructure events and business services, which makes it difficult to understand relative priority and which issues should be tackled first. Finally, there is no simple, automated way to connect service-impacting events to service management tools and processes for rapid remediation.

### The ServiceNow Solution

ServiceNow Event Management is an orchestration application that automatically creates actionable alerts from infrastructure events captured by 3rd party monitoring tools. An event management overview dashboard provides a consolidated view of all service-impacting events, including current active alerts, impacted services, and associated incidents. The application brings events captured by existing infrastructure monitoring tools into ServiceNow for consolidation and action. Events are processed through built-in and custom filters that normalize and de-duplicate the incoming event stream to generate qualified alerts. Alerts are then mapped to configuration items (CIs) and business services in the ServiceNow configuration management database (CMDB) to produce a service-impact view of infrastructure events. Rules may also be applied to alerts to trigger fast, contextually aware remedial action, such as automatically generating an incident and associating a knowledge base article. With ServiceNow Event Management, IT is better equipped to rapidly respond to business-impacting issues, allowing them to take appropriate, automated corrective action.



Consolidated Overview Dashboard

A consolidated view of infrastructure and service health is provided by the event management overview dashboard. Charts and tables in the dashboard provide an at-a-glance view of all alerts, associated incidents, and affected services. Current alerts, alerts over the last day, and alerts over the last seven days are shown by severity. A chart showing top CIs with the most alerts can help isolate a particular machine or CI that is generating events of various types through different monitoring tools. An overview of incidents associated with alerts is also listed by severity. Business services are associated with alerts to show services affected by alerts and an overall view of service health. Like all ServiceNow dashboards, the visualizations are interactive and can be easily drilled into to get additional details around CIs, alerts, services, incidents, and more. In addition, the event management overview dashboard can be enriched with powerful insight provided by ServiceNow Performance Analytics.

REST API for Integration to Monitoring Tools

ServiceNow Event Management can receive events from IT infrastructure monitoring tools such as Icinga and Nagios through a simple REST API. This approach means there are no agents to deploy and no monitoring rules or thresholds to write and manage. The REST API collects events from multiple monitoring tools, including standalone tools for network, server, and storage management, into ServiceNow for aggregation, filtering, and processing.

Built-In and Custom Event Filters

Raw events brought into ServiceNow are processed to generate more qualified alerts. Built-in filters automatically evaluate various criteria to reject, normalize, and/or de-duplicate events so the alert signal can be isolated from the event noise. Event

descriptions from multiple monitoring tools are de-duplicated into a single, normalized description. Monitored nodes are correlated with CMDB CIs so all future events that come in on a node can be related to a CI. CIs in maintenance mode are recognized, allowing any incoming events associated with those CIs to be suppressed. In addition, custom filters may be created, for example, to filter out events from a demo source, and filtering properties may be customized.

Service Impact View

ServiceNow Event Management leverages ServiceNow Configuration Management to correlate alerts with services, providing a service impact view to identify problems and prioritize them appropriately. Once an alert is determined from events, the alert is mapped to CIs, including business services. Impacted CIs and their upstream and downstream dependencies can be easily visualized through an interactive business service management map to readily understand service impact.

Automatically Actionable Alerts

Rules may be applied to alerts to facilitate faster remediation of service-impacting issues by automatically triggering various actions in ServiceNow Incident Management, knowledge base, and more. An alert rule may be used to auto-generate an appropriately prioritized incident from an alert according to criteria such as severity. Another alert rule may be used to associate a knowledge base article with the incident in order to facilitate rapid remediation of the underlying issue. Alert rules integrate ServiceNow Event Management with ServiceNow process automation capabilities in order to restore service in a highly automated and consistent manner.

	Number	Severity	State	Source	Node
<input type="checkbox"/>	Alert0010322	Critical	Open	Icinga	backup33158.yyz2
<input type="checkbox"/>	Alert0010331	Critical	Open	Icinga	maint-MTNNADCOFSW5
<input type="checkbox"/>	Alert0010318	Critical	Open	SolarWinds	anz012-34 demo
<input type="checkbox"/>	Alert0010334	Critical	Open	SolarWinds	AA_COLUMBIA_SC_36.213_24_T845
<input type="checkbox"/>	Alert0010330	Major	Open	Icinga	LIR_FAIRFIELD_NJ_36.245_12_U254

Events are filtered to produce actionable alerts

	Name	Active
<input type="checkbox"/>	Create incidents for Critical alerts	true
<input type="checkbox"/>	Incidents for major interface alerts	true
<input type="checkbox"/>	Link to KB article for SAP CIs	true
<input type="checkbox"/>	Rewrite demo alert severity	true
<input type="checkbox"/>	Rewrite demo alert description	true

Actions on selected rows:

Rules may be applied to alerts to trigger faster, contextually aware remedial action



www.servicenow.com

©2014 ServiceNow and the ServiceNow logo are trademarks of ServiceNow, Inc. ServiceNow believes information in this publication is accurate as of its publication date. This publication could include technical inaccuracies or typographical errors. The information is subject to change without notice. Changes are periodically added to the information herein; these changes will be incorporated in new additions of the publication. ServiceNow may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time. Reproduction of this publication without prior written permission is forbidden. The information in this publication is provided "as is". ServiceNow makes no representations or warranties of any kind, with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. ServiceNow is a trademark of ServiceNow, Inc. All other brands, products, service names, trademarks or registered trademarks are used to identify the products or services of their respective owners.