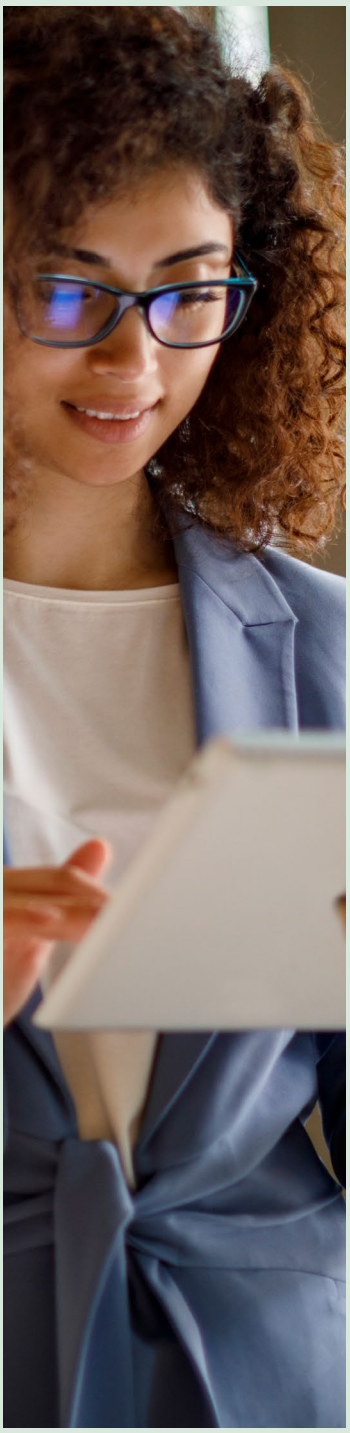
WHITE PAPER



ENHANCE SERVICE EFFICIENCY WITH SERVICENOW EVENT MANAGEMENT

Abstract

In dynamic-complex environments, one of the toughest challenges is to manage huge number of events that arise from different monitoring sources. When ingesting large volumes of data, it is critical to identify those events that have a substantial impact on application or business services. While it is vital to reduce the number of events that appear in an operator console, it is also important to highlight root-cause alerts that can cause an outage to the business service and create incidents in the service management system leveraged by the organization. This paper examines the importance of event correlation. It outlines the must have features and benefits of an effective event management solution.

Infosys®
Navigate your next

Introduction

IT managers across organizations want to cover their bases to avoid any downtime or service interruption for end users. Hence, they end up collecting data from different systems by deploying disparate monitoring tools like freeware or log monitoring techniques. Each tool generates 'havoc' events if any fault is found. However, not all of these events are relevant. Thus, to determine the real causes of the problems, one has to balance the desire for fast and inexpensive data collection with the need to make sense of each event.

Need for noise reduction

In today's world, every organization is rapidly growing its assets, whether these are on-premises data centers or cloud-hosted ones. Even as IT has become vital to business, technology is getting more complex. Hence, organizational silos comprising applications, networks, databases, servers, services, etc., are growing around each domain, resulting in silos within silos that reduce efficiency and increase costs. This leads to organizational concerns such as:

- Increase in costs arising from duplication of effort
- Increase in communication effort between teams for the same issues

To address the above concerns, it is necessary to have a single unified view of the IT environment. This can help identify the impacted services and applications from a single pane, which further enables drill-down and root cause analysis (RCA). With the help of event correlation, managers can view the affected service from top to bottom in a service/topology map.

Event correlation solution

Event correlation methods are designed to identify events, to group them to give more importance to certain events and to assign them to appropriate teams so that corrective action can be undertaken. When events gain complexity, it becomes very important for the correlation engine to detect root cause event and build its intelligence around it.

Various operations associated with event correlation are:

- De-duplicate multiple occurrences of the same event, remove redundancies and report them as a single event/alert
- Suppress events in time-based correlation whereby events are automatically closed if they appear in certain numbers at certain times
- Create groups based on certain parameters or based on CI relationships
- Enable group actions on grouped events like running workflows, triggering orchestration, enriching events, closing events, changing event states, and notifying people/teams.
- Provide upstream and downstream relationships to visualize and understand the impact on an application service and drill down to the root cause

ServiceNow Event Management

ServiceNow Event Management has out-of-the-box (OOTB) connectors that integrate with almost all leading monitoring tools available in the market. The alternative is to integrate other tools using REST API (PUSH), SNMP, email etc. This provides a view of all the events through a single management console. The module offers alert aggregation and RCA for discovered services, application services, technical services and alert groups. The main features of ServiceNow Event Management are:

- **Event level noise reduction**: Introduces event de-duplication through event rules. These mark similar events as duplicate events and map them with the first alert. This is done by analyzing the events and making the association based on content similarities.

- **Event rule threshold**: This threshold is based on the rate at which event management generates an alert. For example, if multiple events are generated for a single device within a short period, it might indicate a serious condition and an alert must be raised. However, if the events for a device are logged at longer intervals, the condition may not be serious. In this case, the user can suppress alert generation using the event rule threshold.

- **Alert correlation**: The purpose of event correlation is to reduce noise and narrow down problems by focusing on primary (root cause) alerts. ServiceNow supports the four types of grouping:
  - **Rule-based grouping**: New correlation rules allow users to manually classify alerts as primary or secondary, thereby establishing relationships between them
  - **Automated grouping**: Based on historical alerts, automated alert groups are formed using machine learning (ML) patterns
  - **Manual grouping**: Alerts are initially grouped based on manual input. Later, these patterns are studied by the Learner job that uses ML to group similar alerts automatically in the future.
  - **CMDB grouping**: CMDB alert grouping is based on topology. Alerts are correlated based on CI relationships in the CMDB.

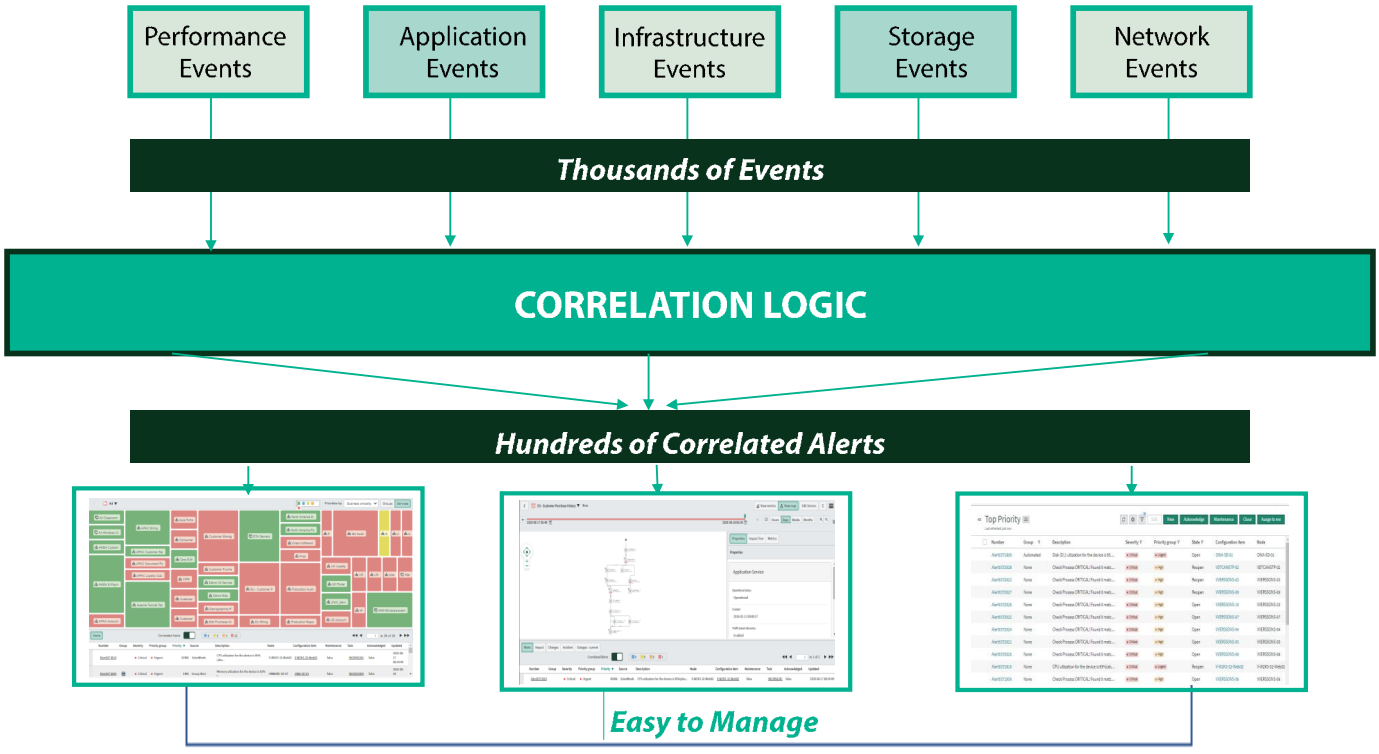


Fig 1: Event noise reduction through alert correlation

Event correlation benefits

Event correlation automatically works on the alerts to reduce the number so that only the relevant ones are displayed. This helps the IT department to reduce effort that was spent on making sense of alerts and focus more on resolving immediate threats. Other benefits of event correlation are:

- Locates the root cause of alerts that help in detecting real threats
- Prevents outages that might affect the application service or business
- Reduces MTTR (mean time to resolve) cost
- Simplifies remediation of network events where many alerts are triggered during failure of a single switch, router or tunnel. Event correlation will help identify the root cause quickly from the flood of events

Conclusion

To deliver enhanced service, it is essential for IT to have smart event handling and correlation techniques. These tools must filter out event noise and focus on solving critical problems. From traditional to hybrid cloud IT landscapes, organizations need smart event correlation technology that adapts to automatically discovered changes in the infrastructure. This will benefit organizations by reducing operational costs and increasing efficiency.

About the author

Rudrangshu Das, *Senior Consultant*

Rudrangshu Das is an IT professional with extensive experience in solution architecture as well as evaluating, assessing and implementing infrastructure monitoring tools. He has managed IT operations for over 13 years and deployed numerous ServiceNow ITOM solutions such as event management and operational intelligence.

For more information, contact askus@infosys.com

Infosys®
Navigate your next