Cisco Network Assurance Engine Integration with Splunk Enterprise

Continuous network verification and analysis with automated event correlation and response

Challenge

Modern analytics and monitoring tools collect machine data—including massive amounts of logs and network traffic flows—from varied sources in a network. This data comes in an array of unpredictable formats, creating a situation that could challenge administrators to understand.

When errors or conflicts occur, it’s not always evident what is happening, where it is happening, or why. In cases where the problem involves multiple devices or networks, administrators must sift through enormous amounts of logistics, including large volumes of raw logs for Root Cause Analysis. With newer solutions such as Software-Defined Networking (SDN) where multiple layers of abstraction are involved, a comprehensive understanding of the logical and physical structure of the network is required to troubleshoot network problems, thus adding another layer of complexity.

Combining the deep network knowledge of SDN and assurance capabilities of Cisco® Network Assurance with an operational intelligence platform such as Splunk can help troubleshoot network problems faster and more efficiently.
Cisco Network Assurance Engine with Splunk Enterprise

Cisco Network Assurance Engine, the industry's first SDN-ready intent-assurance suite, integrates with Splunk Enterprise to enable unprecedented network insight, troubleshooting, and control. The combination of Cisco Network Assurance Engine with Splunk software delivers exceptional data center visibility, which allows network administrators to quickly identify, characterize, and correlate network problems.

With continuous network monitoring, Network Assurance Engine can proactively identify, characterize, and present network problems, errors, and conflicts. These “SmartEvents” tell the network administrator not only what has happened, but also where and why the problem occurred. Using Splunk software, administrators can visualize these problems in real time and easily correlate them with problems across multiple infrastructure devices, network tiers, and applications.

Network Assurance Engine provides recommendations for how to resolve each SmartEvent, and also helps identify recurring network problems and trends. Network administrators can then establish rules and alerts in Splunk Enterprise to automate the response to known SmartEvents, further reducing the time and cost of network administration and troubleshooting.

Superior network insight, troubleshooting, and control

- Visualize real-time, contextually relevant network insights.
- Create automated alerts for network problems, errors, and conflicts.
- Correlate multitier and multidevice events.
- Quickly review new, resolved, and persistent network events.
- Perform flexible, query-driven searches across events and intervals.
- Analyze trends related to events and intervals.
- Create rules that automate the response of the network to recurring events.

Use case: Event visualization and monitoring

Cisco Network Assurance Engine provides events across the Cisco Application Centric Infrastructure (Cisco ACI™) fabric, helping you understand any impending problems, or assurance events confirming expected behavior from your network. Splunk Enterprise integration with Cisco Network Assurance Engine helps you visualize these events to make troubleshooting faster and easier through multiple dashboards.

- The Home dashboard provides a comprehensive view of epochs and events that Network Assurance Engine reports. If errors occur, the error timeline helps you understand trends in network problems over time. For a single event, you can drill down to details such as when, where, and how a problem has been occurring in the network.
- Epoch Delta dashboard helps you understand differences in Network Assurance Engine reported events across timelines, so it becomes easier to assess any new events arising out of a change to the network, or any events resolved after a change.
- Event Delta dashboard helps you understand differences between seemingly similar events that Network Assurance Engine reports. A single click takes you to the relevant Cisco Network Assurance Engine page for an event.
- For multiple fabrics, a single pane of visualization is available to track events of interest across all fabrics instead of having to monitor each fabric individually.
- Cisco Network Assurance Engine custom SmartEvent search allows you to search and identify events; reports are returned in an easy, human-readable format.
Use case: Event correlation and response

The combination of Cisco Network Assurance Engine and Splunk Enterprise can help correlate and make sense of data from multiple network devices. It can dramatically reduce the time and manual effort required to troubleshoot complex network problems and outages.

In addition to identifying the source of a problem, Network Assurance Engine provides critical context for why the problem occurred, what was affected, and how to resolve it. This process helps narrow down the moves or changes that caused the outage, allowing a more proactive, automated response to problematic conditions or sequences.

As Network Assurance Engine identifies and characterizes these SmartEvents—which are divided by category, subcategory, and mnemonic (Figure 1)—you can use Splunk Enterprise to analyze event-related trends. New, persistent, resolved, and unresolved events are shown across timelines, allowing network administrators to quickly determine when an event originated and how long it has persisted. And you can easily correlate these events with other data or events surfaced within Splunk Enterprise.

If the status of a virtual machine is listed as inaccessible, for example, the network administrator can easily search for events related to that IP address. Network Assurance Engine shows the changes (or lack thereof) to the network, any underlying problems the changes may have caused, and suggested steps for resolving the problem. When the problem is fixed, it is listed as “resolved” in the Splunk Enterprise dashboard, providing assurance that the virtual machine is now operational.

As events are identified and characterized, you can establish rules and alerts within Splunk Enterprise to automate the response and resolution. These rules and alerts can significantly reduce the time and cost of network administration and troubleshooting (Figure 1).

Figure 1. Cisco Network Assurance Engine data within the Splunk Enterprise dashboard
Conclusion

SDN technologies have revolutionized IT management, allowing administrators to establish policies and automate the configuration of underlying systems from a centralized console. But these intent-based network solutions need an assurance platform that can verify administrators’ intent is being implemented correctly, validate past or future changes, improve capacity management, and help with troubleshooting.

The combination of Cisco Network Assurance Engine and Splunk Enterprise provides continuous network verification with real-time, contextually relevant problem identification, characterization, and automation. This continuous verification not only streamlines troubleshooting efforts and reduces downtime, but also gives Splunk Enterprise users greater insight and control over their network.

For more information


www.cisco.com/go/dcecosystem

www.splunk.com

The Cisco Network Assurance Engine application is now available on splunkbase.