ılıılı
CISCO

The bridge to possible

Cisco Nexus Dashboard Insights and Splunk Integration

Customizable dashboards, security and operational analytics, alerting, troubleshooting and cross-tier correlation

Challenges

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 can challenge administrators from an operations standpoint. When errors or conflicts occur, it's not always evident what is happening, where it is happening, or why. The problem is further exacerbated in situations that involves multiple devices or networks, where administrators are burdened to sift through enormous amounts of logistics data for root-cause analysis, including large volumes of raw logs.

With newer and advanced cloud-networking solutions, 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 and the operational intelligence of Cisco Nexus® Dashboard Insights with a data analytics, correlation, and monitoring platform such as Splunk can help troubleshoot network problems faster and more efficiently.

Cisco Nexus Dashboard Insights incorporates a set of advanced alerting, baselining, correlation, and forecasting algorithms to provide deep insights into the behavior of the network by utilizing telemetry data obtained from networking and compute components. Cisco Nexus Dashboard Insights automates troubleshooting and helps rapid root-causing and early remediation. It also helps infrastructure owners comply with SLA requirements for their users.

Splunk Enterprise, a machine data platform with collection, indexing, search, reporting, analysis, alerting, monitoring, and data management capabilities; and Splunk Cloud. The company also provides Splunk Light, which offers log search and analysis for small IT environments.

The Nexus Dashboard Insights and Splunk integration enables customers to gain deeper insights into the operational state of their infrastructure, accelerate troubleshooting, and improve operational efficiency. The solution achieves this through the CIM-compliant Nexus Dashboard Insights data on Splunk Enterprise, which enables customers monitor their unique KPIs, create custom dashboards and alerts for Nexus Dashboard Insights data indexed on Splunk, and build cross-tier correlations with the data from other tiers, such as applications, compute and security.

ılıılıı
CISCO

The bridge to possible

Benefits

- Get comprehensive network insights, simplified troubleshooting, and granular control

- Visualize real-time, contextually relevant network insights

- Create automated alerts for network problems, errors, and conflicts

- Correlate multitier and multidevice anomalies, advisories

- Perform flexible, query-driven searches for anomalies and advisories over time

- Analyze trends related to anomalies and advisories over a specified period

- Create rules that automate the response of the network to recurring events

Solution

The solution describes the Nexus Dashboard Insights application on Splunk Enterprise.

Figure 1.   Nexus Dashboard Insights – Splunk integration architecture

ı|ıı|ıı
CISCO

The bridge to possible
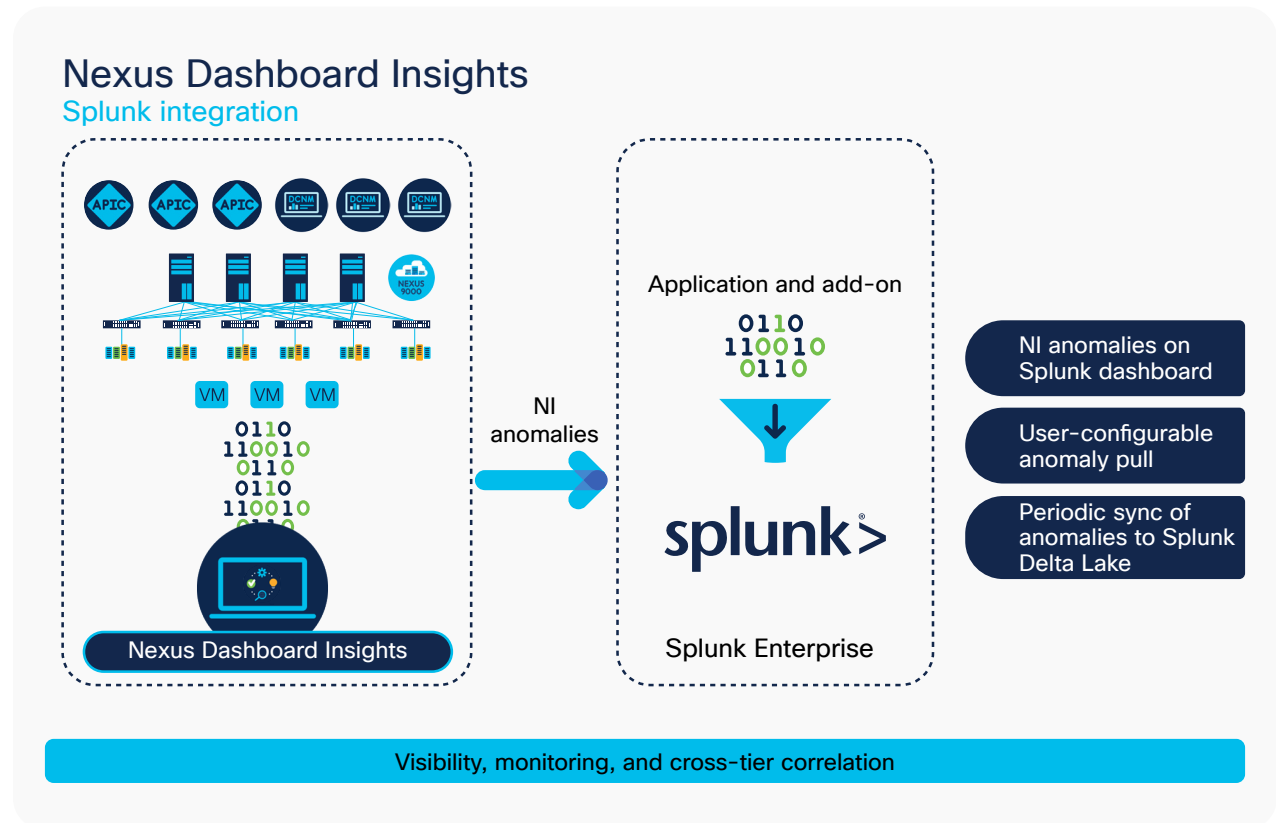
Conclusion

Modern cloud-networking technologies have revolutionized IT management, allowing administrators to establish policies and automate the configuration of underlying systems from a centralized console. With these unprecedented increases in scale and complexity of networks, it is challenging to keep up with the demands of operating a large network without the aid of intelligent and adaptive tools. Cisco Nexus Dashboard Insights and Splunk together provide real-time monitoring and analytics, accelerate troubleshooting, and improve operational efficiency. The integration of Cisco Nexus Dashboard Insights and Splunk Enterprise provides continuous network verification with real-time, contextually relevant problem identification, characterization, and remediation. This continuous verification not only streamlines troubleshooting efforts and reduces downtime, but it also helps network operations adhere to SLAs and ensure business continuity.

Call to action

To learn more, please visit:

Cisco Nexus Dashboard

Cisco DC Ecosystem

Use case: Real-time and historical monitoring and visualization

Cisco Nexus Dashboard Insights generates anomalies and advisories for the Cisco® Application Centric Infrastructure (Cisco ACI®) fabric, helping users understand any impending problems with the network, or assurance events confirming expected behavior from your network. Splunk Enterprise integration with Cisco Nexus Dashboard Insights helps you visualize these anomalies and advisories to make troubleshooting faster and easier through intuitive, easy-to-build dashboards.

- The home dashboard provides a comprehensive view of anomalies and advisories that Nexus Dashboard Insights reports. If errors occur in a single fabric, the error timeline helps you understand trends in network problems over time.

- For multiple fabrics and Nexus Dashboard Insights instances, a single pane of visualization is available to track anomalies and advisories of interest across multiple fabrics and multiple Nexus Dashboard Insights clusters.

Use case: Monitoring custom KPIs

- Network teams can create custom dashboards using Nexus Dashboard Insights data indexed in Splunk Enterprise. This helps them build custom KPIs specific to their organization and make it available to network operators.

Use case: Building cross-tier correlations

- Nexus Dashboard Insights data indexed in Splunk adheres to the Splunk CIM-compliance model. Network teams can also build custom cross-tier correlations (for example, compute, security, applications, etc.) for faster troubleshooting and root-cause analysis.

Use case: Alerting automation

- Network teams can use the solution to create custom dashboards and alerts for anomalies and advisories from Nexus Dashboard Insights. The solution supports granular alerting and periodic reporting configurations for any specific fields (or "their combinations represented as a Splunk search queries") associated with anomalies or advisories and time intervals. This helps customers define specific rules that help them adhere to their organizational standards.