On the Road to Cross-Domain Event Correlation

Cisco IT Insights

What

Network operators everywhere understand the need for event correlation. Who couldn't benefit from a technique that can make sense of a large number of event streams, separate the few events that are really important, and generate smaller streams with more useful information to act on? Without an event correlation tool or system, troubleshooting incidents that arise in the data center is a people-intensive process.

Like many other large IT organizations, Cisco IT's event correlation efforts have been mostly reactive. In a complex, virtualized IT environment with disparate systems on multi-data center technology stacks, being in reactive mode simply isn't good enough. It doesn't help us shorten our Mean Time to Resolve (MTTR), readily identify the root cause and business impact of incidents, or bolster the productivity of engineers and subject matter experts (SMEs). These are the goals of our current cross-domain event correlation pilot.

Today, alerts from systems and internal configuration management databases funnel through our Operations Command Center (OCC). When there's a problem, someone in the OCC summons SMEs that are knowledgeable about the topic to participate in a virtual triage session. Because the root cause of the issue is unknown, a wide SME net is cast. For example, if an alert indicates a slow-running database or users are complaining about a sluggish finance application, the fault could be with storage, compute, or the database itself. The OCC will rally SMEs from all three areas. It can take several hours to determine the root cause and recommended remediation.

"We're good at pinpointing issues within individual domains," says Jag Kahlon, Cisco IT architect, Global Infrastructure Services. "The challenge comes in sorting through events and all their possible dependencies across different domains. What's the impact upstream or downstream? That has been a weak point for us."

There's also the matter of sheer volume. In a data center alone, there are thousands of servers, components, and devices with sensors that continuously collect and spew out data. Simple Network Management Protocol (SNMP) traps, logs, alarms, thresholds, etc., factor in the mind-spinning amount of data that will be churned out by the Internet of Everything (IoE) as new categories of things, people, and types of information are connected to the Internet at exponential rates.

"First we have to be able to instrument, correlate, and manage all this output. Then we can build intelligence on top of it," says Kahlon.

Cross-Domain Event Correlation Pilot

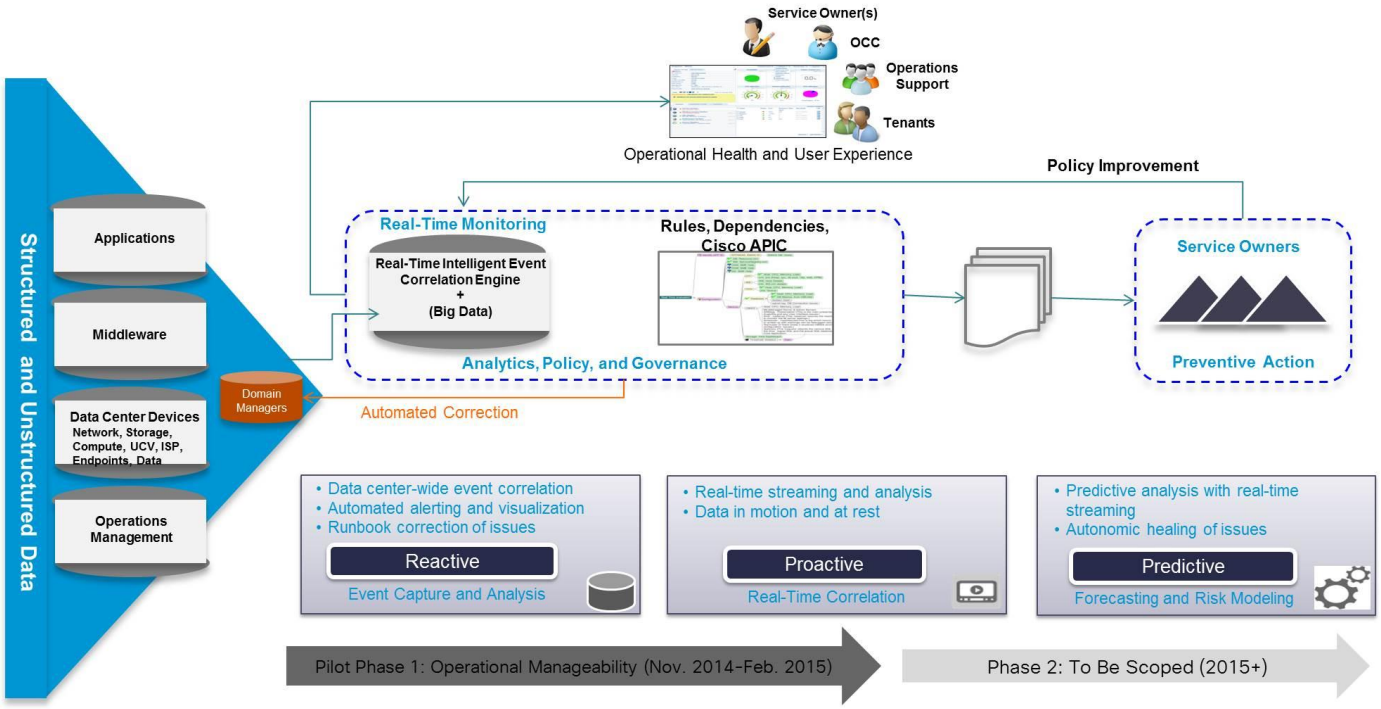
Teams in Cisco IT Operations, Service Assurance, and Cloud Services, along with IoE SMEs, came together to develop and pilot a common architecture, scalable event correlation solution. We sought an analytics-based tool that would adapt easily to configuration changes in a dynamic data center environment. A tool that would not only move us from reactive to proactive mode, but give us the ability to identify problems as they unfold across domains, relate them to the root cause quickly, and, ultimately, help us to forecast problems before they arise.

But our long-term vision of event correlation is broader than a single tool. It's a solution that also needs process and people to tap into the full potential (see Figure 1).

For phase one of the pilot (running November 2014 to February 2015), we chose a third-party situation management tool that can process operational data in real time across IT silos. The tool isn't constricted by coding requirements, and doesn't rely on rules, or behavior or topology models. It applies sophisticated algorithms to events within different domains, groups them based on dependencies or other mutual relationships such as time or natural language processing, and converts the information into definable alerts (situations) that the OCC can act on efficiently and collaboratively.

Cisco IT is piloting this tool on a large-scale service involving a customer care application with a high number of reported incidents. Cross-domain event correlation is required, from the infrastructure layers through storage, network, and compute. We built the use case on virtual machines running on the Cisco® Unified Computing System™ (Cisco UCS®).

Figure 1. A Forward Look at Cross-Domain Event Correlation



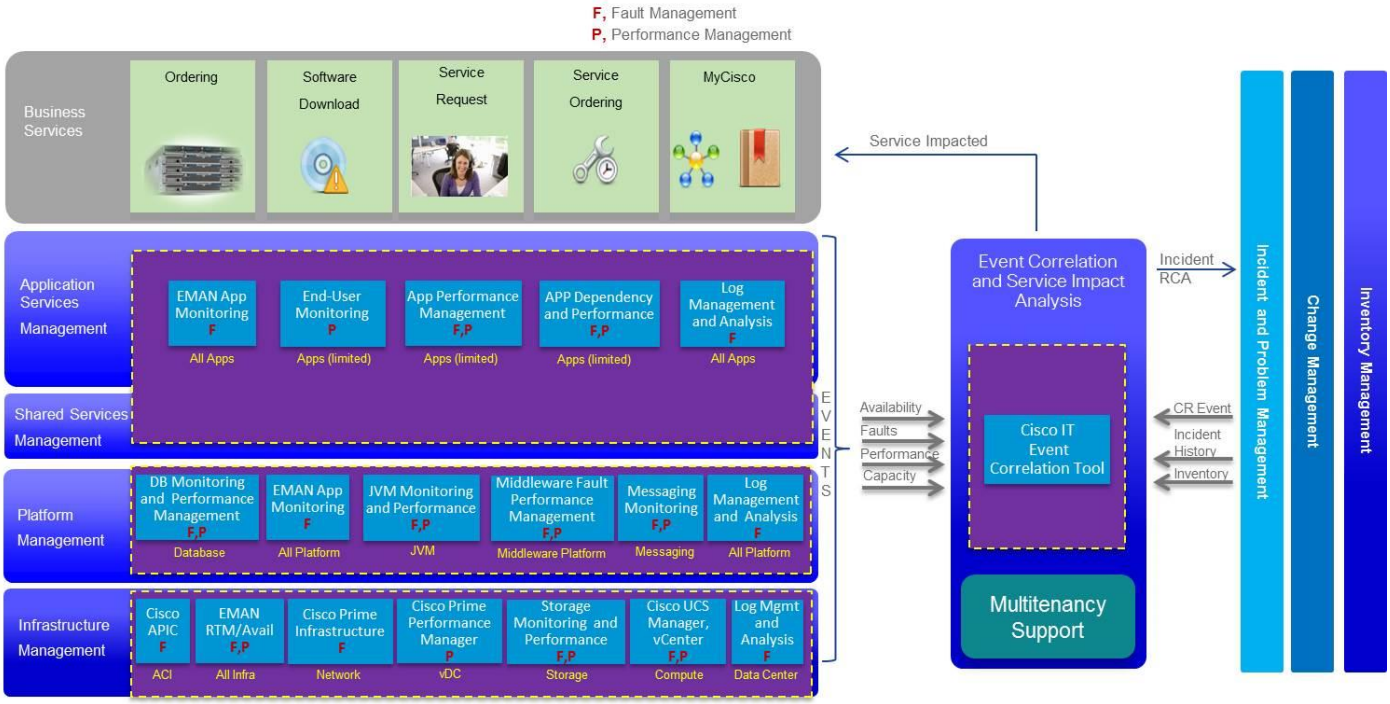
Why

Today, 60 percent of problems arising in the data center are reported by end users. Only 40 percent are detected through our existing tools. A primary objective of the pilot is to reduce service-impacting incidents count and MTTR by 30 percent. That is, pinpoint and resolve many more service-impacting incidents before employees or customers are affected. Armed with a tool that can filter out insignificant events and calculate cause-and-impact inferences, we can also bring down our Mean Time to Detect (MTTD).

Being able to group related events that traverse domains is vital to achieving our target state (see Figure 2). Information from Inventory Management and other teams must be input into the tool so it can create and group cross-domain dependencies. Down the road, we'll also feed in data from our Application Centric Infrastructure and Cisco Application Policy Infrastructure Controller (APIC) when they are deployed in our production data centers.

So, back to the aforementioned slow-running database example. If around the same time users are complaining about a sluggish finance application, alerts are coming into the OCC about a malfunctioning storage path. **Traffic being failed over to an alternate route. Transactions going through smoothly until there's a dropped link in the storage domain. I/O throughput impacted, clogging up the database that runs the finance application**. Now staff in the OCC has correlated, intelligent event information to act on. Instead of casting a wide net, the right SMEs are targeted up front.

Figure 2. Pilot Phase One Target State



Using social collaboration technology, the tool we're piloting can create a virtual room and invite cross-silo experts there to view and resolve the problem together. Because the tool has the capability to contextualize participants' relationship to the situation (e.g., owner of the causal indicator or impacted user), the appropriate people are engaged faster. Different views of the same data can be tailored for specific teams. What's more, the output is available in a central location for everyone across domains to see.

SME/support time and duplicated efforts are minimized. Virtual triage sessions are more productive. Users are up and running faster. Silos between IT, development, and operations personnel are reduced. Fewer incidents. Shorter MTTD. Faster MTTR.

Proactive Today, Predictive Tomorrow

When fully deployed, our event correlation solution will see millions of events flowing in daily. As the volume of connected devices increases, we have to step up their ability to keep all these things up and running: detecting when a service is starting to fail, deducing how a problem with one device affects another, diagnosing the root cause of problems, and resolving those problems quickly and efficiently. Today, we're moving our event correlation efforts from being reactive to proactive in a scalable way. Eventually, we'll have the capability to operate in predictive mode.

"It will take us a few years to reach the predictive stage," according to Kahlon. "That's when we'll be able to truly harness the intelligence built on our IoE platform."

That's when we'll be able to unleash all the insight flowing from vast volumes of data to help us solve business problems faster and optimize and simplify operations further.

For More Information

Cisco IT Insights Series, Part 1: The Network: Artery and Brain for Big Data

Cisco IT Insights Series, Part 2: Big Data: Not Just Big, But Different

Cisco It Insights Series, Part 3: Seven Essential Network Capabilities for the Internet of Everything

Cisco Trends in IT article: The Internet of Everything Is the New Economy

To read additional Cisco IT case studies about a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT.

To view Cisco IT webinars and events about related topics, visit Cisco on Cisco Webinars & Events.

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described. Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties; therefore, this disclaimer may not apply to you.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA 01/15