Leidos optimiert durch Splunk ITSI sein Ereignis-Management

Kurzfassung

In seinem über 50-jährigen Bestehen hat Leidos zu den Erfolgen des US-Space-Shuttle-Programms ebenso beigetragen wie zum Sieg eines America's-Cup-Gewinners. Heute arbeitet der Fortune 500-Marktführer in Wissenschafts- und Technologielösungen an der Lösung globaler Herausforderungen etwa in den Bereichen Verteidigung, Nachrichtendienste und Gesundheitswesen – und begegnet dabei eigenen Herausforderungen, wenn es darum geht, sicherzustellen, dass seine Dienstleistungen für Kunden durchgängig verfügbar sind. Seitdem die IT-Abteilung von Leidos ihre alte Event-Management-Lösung durch Splunk IT Service Intelligence (ITSI) ersetzt hat, profitiert sie unter anderem von den folgenden Vorteilen:

- Unternehmensweites Infrastruktur-Monitoring in Echtzeit
- Robuste Lösung zum Aufbrechen von IT-Silos und Korrelieren von Ereignissen
- Dashboards für verschiedene Zielgruppen, von problemlösenden Technikern bis hin zu Big-Picture-Managern

Warum Splunk

Don Mahler, Director of Performance Management bei Leidos, erklärt: „Infrastruktur-Monitoring ist wirklich unsere Leidenschaft. Unsere operativen Mitarbeiter schauen nicht nur auf das, was funktioniert; sie möchten auch wissen, was nicht funktioniert. Viele Probleme haben eher Leistungsabfälle und nicht gleich Serviceausfälle zur Folge. Aus operativer Sicht ist es wichtig, hier immer einen Schritt voraus zu sein, bevor die Situation eskaliert."

Das ist ein Rund-um-die-Uhr-Job, bei dem Mahler Splunk ITSI in vier Funktionsbereichen einsetzt: Die erste Funktion ist der Situationsbefund, bei dem ermittelt wird, was reibungslos läuft und wo es Probleme gibt. Die zweite ist die Performance- und Kapazitätsplanung; hier wird die Performance der Komponenten im zeitlichen Verlauf betrachtet, um festzustellen, ob Speicherplatz, CPU, Linknutzung oder andere Metriken ihre dynamischen Schwellenwerte überschreiten. Der dritte Bereich ist das Logging – aus Gründen der Sicherheit, Forensik und Verfügbarkeit. Viertens kommt schließlich das Reporting über die Bereitstellung der Services hinzu, mit dem Leidos Echtzeittransparenz in seiner operativen Umgebung gewinnt.

Im Kern geht es darum, Störungen zu finden und zu beheben, bevor die Kunden etwas davon mitbekommen. Leidos benötigte eine Lösung, die alle Unterabteilungen und die gesamte IT inklusive Silos zusammenführen konnte und aus der Event-Flut die relevanten Ereignisse selektiert – bei insgesamt über 120 IT-Services.

leidos

Branche

- Technologie

Anwendungsfälle

- IT Operations Management
- Log-Management
- Security

Herausforderungen

- 24/7-Kundenzugriff braucht Monitoring und Reaktion
- Abgeschottete Silos hatten eine stark zerklüftete IT zur Folge
- Die Notwendigkeit, Tausende von Benachrichtigungen und Events auf ein Minimum zu reduzieren

Auswirkungen für das Unternehmen

- Automatisierung der Event-Handhabung durch ein Regelmodul und Echtzeitkorrelation
- Nahtlose Integration in Management-Systeme, Apps und Add-ons
- Dashboards, die einfach geteilt und angepasst werden können, sowie klassische Glass-Table-Ansichten, die Geschäftsprozesse abbilden

Datenquellen

- Anwendungen
- Geräte
- Firewall
- Netzwerk
- Server

Splunk-Produkte

- Splunk Enterprise
- Splunk IT Service Intelligence (ITSI)
- Splunk DB Connect
- Splunk App for Microsoft Exchange

Mehr als Log-Management – Transformierter Rechenzentrumsbetrieb

Leidos begann mit einer kleinen Splunk-Enterprise-Lizenz, um die Logs der Router und Switches zu sammeln. Aber dabei blieb es nicht. Die Implementierung wurde rasch ausgeweitet und sollte bald auch Benachrichtigungen, Ticket-Erstellung sowie die Netzwerk-, Änderungs- und Performance-Daten aus Tausenden von Geräten zusammenführen – lauter unstrukturierte Daten, die nun zentral auf den Dashboards von Splunk Enterprise visualisiert werden konnten.

Ein großer Vorzug der Splunk-Plattform besteht laut Mahler darin, dass sie die Silos überwindet und den Teams einen Überblick über die Daten im gesamten Service-Stack verschafft. So bekommen Anwender die Informationen, die sie brauchen, und die Zuständigen für die Server können beispielsweise auf relevante Firewall-Daten zugreifen. „In meinen Augen ist die Lösung ein gemeinsames Informationsmodell für die ganze Umgebung. Außerdem ist es ein Tool, das IT-Mitarbeitern – und Führungskräften aus dem kaufmännischen Bereich – Antworten auf all ihre Fragen zu den IT-Services geben kann."

Mahler weiter: „Ich bin seit über 20 Jahren im IT-Management und habe noch nie ein Produkt gesehen, das so etwas kann. Es ist das allererste Mal, dass ich wirklich ein heterogenes Monitoring quer durch den gesamten Technologie-Stack meiner IT-Umgebung machen kann, weil Splunk alle Daten hat und ich sie alle mit Splunk auf ein und dieselbe Weise durchsuchen kann."

Intelligentes Event-Management

Der nächste logische Schritt war das Alert-Management. Leidos hatte seit über 15 Jahren eine Lösung im Einsatz, die nicht nur veraltet war, sondern trotz komplizierter Backend-Regelsprache auch nur das Minimum leistete. Das Unternehmen wollte jetzt ein modernes Produkt mit sofort einsatzbereiter Korrelation und einem Regelmodul, um kritische von kleineren Events zu unterscheiden. Die Lösung war Splunk ITSI.

„Es gibt Tage, an denen die Events nur so hereinprasseln", sagt Mahler. „Splunk ITSI priorisiert die Events und sagt mir nicht nur, dass ein Fehler vorliegt, sondern auch, was von der Störung betroffen ist – und das beim ersten Blick auf den Benachrichtigungsbildschirm." Neben grundlegenden Anforderungen wie der Konsolidierung von Events aus der heterogenen IT-Umgebung, der Erkennung und Ausblendung von Duplikaten, der Löschung gelöster Warnungen und der Übersetzung von Event-Meldungen in geeignete Maßnahmen brauchte das Unternehmen noch erweiterte Funktionen, etwa um Warnmeldungen nach einer bestimmten Zeit automatisch zu eskalieren oder um Benachrichtigungen zu unterdrücken, wenn ein Gerät absichtlich offline genommen wurde. All dies konnte Leidos mit Splunk ITSI umsetzen.

„Dank Splunk haben wir dermaßen viele Informationen direkt griffbereit. So gelingt es uns ständig, Geschäftsprobleme auf kreative Weise zu lösen."

— Don Mahler, Director of Performance Management, Leidos

Heute speisen bei Leidos rund 20 Managementsysteme – vom Microsoft System Center Configuration Manager (SCCM) bis zu den Netzwerkmanagement-Tools von SolarWinds– sowie mehr als 4.500 Konfigurationselemente (CIs) aus 120 IT-Services und 240 Standorten weltweit Daten in Splunk ITSI ein. Im Endeffekt kann das Unternehmen damit die 3.500 bis 5.000 Benachrichtigungen pro Tag auf etwa 50 Tickets für die Betriebsverantwortlichen von Netzwerk und Rechenzentrum reduzieren. Und weil Splunk ITSI CMDB-Informationen übernimmt, sind auch unterschiedliche Warnanzeigen für unterschiedliche Zuständigkeiten möglich.

Fazit: Einfacherer Zugriff auf relevantere Daten – und Beschäftigte, die ihre kostbare Zeit den Dingen widmen, die wirklich wichtig sind. „Unterm Strich kommt es mir vor allem darauf an, dass wir etwas bewegen, dass wir einen Service leisten, der zuverlässig ist und die Leute weiterbringt", so Mahler abschließend. „Weil Splunk sämtliche Informationen zusammenführt, bekommen wir jetzt bessere Antworten, und zwar schneller und effizienter."

20-14987-Leidos-A4-102-CS_DE