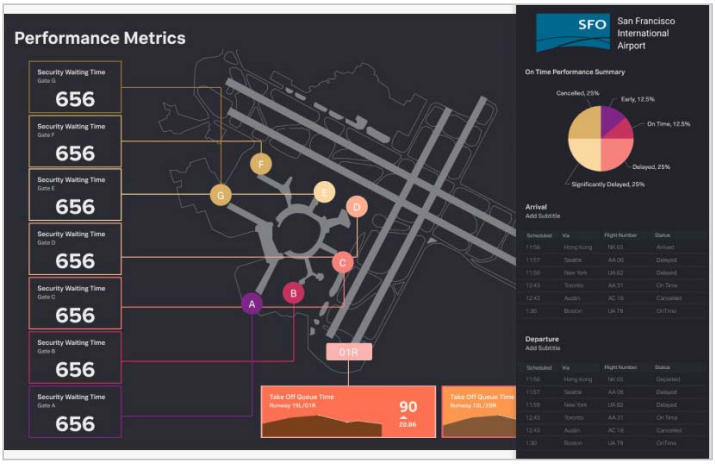
Splunk: Kubernetes-Monitoring mit künstlicher Intelligenz und Tracing

2019 kaufte der Logging-Experte Splunk die Firmen SignalFX und Omnition, um die Fähigkeiten seiner gleichnamigen Plattform für zentralisiertes Logging und Monitoring von Container-Workloads und Kubernetes zu verbessern. Weniger als ein Jahr später scheint der Plan aufzugehen: Die neueste Splunk-Version möbelt sowohl die Erfassung von Metrikdaten als auch das Tracing innerhalb von Containerumgebungen radikal auf und will dabei aus einem Logging-Tool eine komplette Monitoringumgebung für Kubernetes machen.

In die Containerumgebung selbst schleust Splunk dazu mehrere Aufpasser ein, die laut Hersteller auf Basis offener Standards agieren und zum Teil auf Open Source setzen. Ihre Kernaufgabe besteht darin, verschiedenste Formen von Daten zu sammeln: Ganz klassisch im Stile von Nagios überwachen sie die Verfügbarkeit einzelner Programme und sammeln gleichzeitig Metrikdaten von Laufzeitwerten wie der CPU-Last.



Quelle: Splunk

Zudem implementiert Splunk nun auch Tracing, mit dem Administratoren nachvollziehen können, wie der Status ihrer Cloud ist, was gerade mit welchen Daten passiert und wie diese verarbeitet werden. Die neue Splunk-Version wildert damit in den angestammten Gefilden von Produkten wie Prometheus oder Jaeger. Mit dem Tracing-Tool Jaeger beschäftigt sich der Artikel auf Seite 122 in diesem Heft.

Zusätzlich verspricht der Hersteller diverse zum Teil KI-basierte Funktionen, die Fehler automatisiert abarbeiten sollen. Fällt Splunk ein Verhalten auf, das außerhalb von Grenzwerten liegt, die der Administrator vorgab, dann schlägt die Software Lösungen vor und implementiert diese auf Wunsch automatisch.

Für von Menschen vorgenommene Auswertungen der eingehenden Monitoring- und Metrikdaten bringt Splunk verschiedene neue Dashboards. Die sollen einen schnellen Überblick verschaffen, ermöglichen per Zoom und Auswahl von Detailbereichen aber auch hohe Genauigkeit beim Betrachten von Werten.

Die neue Ausrichtung ändert allerdings nichts an der Zielgruppe von Splunk. Dass das eindeutig größere Unternehmen sind, zeigt sich auch in der Preisgestaltung. Dazu passt dann auch die jüngst angekündigte strategische Partnerschaft mit Google im Rahmen der Data-to-Everything-Plattform, wo Splunk seine Dienste als SaaS-Angebot anbietet – bisher allerdings nur für Early-Access-Kunden. (mfe@ix.de)

Zabbix erweitert QNAP-NAS zur Monitoringzentrale

QNAP und Zabbix haben ein gemeinsames Featurepaket auf die Beine gestellt, das den Storage-Geräten erweiterte Monitoringfunktionen beibringt. Es lässt sich dem Hersteller zufolge sehr einfach installieren, aber auch über viele Instanzen in die Breite skalieren. Wer mehrere QNAP-Geräte nutzt, kann beispielsweise auf jedem davon separat Monitoring für alle Geräte einer Etage betreiben. Unter einer einheitlichen Oberfläche lassen sich eingehende Meldungen anschließend sammeln, sodass ein Single Point of Administration entsteht, SNMP-Compliance und ein Managementinterface für den Browser inklusive.

Das umfasst natürlich auch die von anderen Monitoringsystemen her bekannten Benachrichtigungen: Mit Zabbix, das kurz vor Redaktionsschluss in Version 5 erschienen ist, können Administratoren Server, Hardware und andere Geräte verschiedener Hersteller überwachen und Warnungen verschicken lassen, falls kritische Werte erreicht werden. Fällt ein Drucker oder ein Switch aus, informiert Zabbix auf Wunsch den zuständigen Administrator. Auch Automatismen sind möglich, zum Beispiel um Geräte beim Auftreten einer bekannten Fehlermeldung ohne erneute Interaktion neu zu starten.

Seinen Weg auf die QNAP-Systeme findet Zabbix als virtuelle Maschine aus dem QNAP-Marketplace, laut Zabbix auch schnell deployt in Umgebungen mit mehreren NAS und auf den von QNAP vertriebenen QGD-Switches. (mfe@ix.de)

PRTG Enterprise Edition bringt neues Dashboard zur Geräteüberwachung

Ums Monitoring klassischer Infrastrukturhardware auf Netzwerkebene kümmert sich PRTG und überwacht Switches, Router und ähnliche Hardware. Hersteller Paessler bringt nun ein zusätzliches Produkt – die PRTG Enterprise Edition – auf den Markt, das als eine Art organisatorische Klammer um mehrere PRGT-Instanzen fungiert und ein neues GUI mitbringt. Bis dato hatte ein Admin zwar die Möglichkeit, verschiedene PRTG-Instanzen zu betreiben; diese waren jedoch nicht verknüpft, einen Single Point of Administration gab es noch nicht.

Das neu entwickelte ITops-Dashboard dockt im Hintergrund an eine nahezu beliebige Anzahl bestehender PRTG-Instanzen an und sammelt Informationen wie bestehende Alarmmeldungen, Logs und Metrikdaten ein, um sie grafisch aufbereitet anzuzeigen und gegebenenfalls auch automatisiert zu reagieren. Auch die Modellierung von SLAs ist möglich: Der Administrator kann beispielsweise seine Geräte verschiedenen Gruppen zuordnen. Je nach Gruppenzugehörigkeit implementiert das ITops-Board dann auf Wunsch die Priorisierung sowie das Alarmieren bei bestimmten Vorkommnissen nur zu festgelegten Zeiten.

Auch das Lizenzmodell hinter PRTG hat Paessler angepasst. Es gibt keine unterschiedlichen Lizenzen mit verschiedenen Levels mehr, die Bepreisung des Produkts richtet sich stattdessen nach den genutzten Sensoren. Das macht die operativen Kosten planbarer, und ein Unternehmen weiß, was die Erweiterung des Set-ups im Hinblick auf PRTG-Lizenzen kostet. (mfe@ix.de)

Alle Meldungen: Martin Gerhard Loschwitz

© Copyright by Heise Medien.
Persönliches PDF für alle Leser der iX aus 30625 Hannover

© Copyright by Heise Medien.
Persönliches PDF für alle Leser der iX aus 30625 Hannover