LANline

9,– €

Juli 2016
20. Juni

ITP VERLAG

IT ■ Netze ■ Infrastruktur www.lanline.de

Datacenter Security und Hochverfügbarkeit

IT-Abwehrstrategie als Voraussetzung

Physische RZ-Sicherheit gemäß DIN EN 50600

Incident-Response-Management

Mit Marktübersicht USVs

Citrix Synergy in Las Vegas
Windows 10 aus der Cloud

Sonderschwerpunkt Monitoring
Blick auf Performance und Schwachstellen

Sonderdruck Consistec
Dienste unter der Lupe

Service-Monitoring in verteilten Umgebungen

Dienste unter der Lupe

Verteilte IT-Systeme stellen hohe Anforderungen an den Rollout, die Interoperabilität und die Analysefähigkeit der Monitoring-Tools. Die Anforderungen steigen nochmals, wenn solche Systeme die Dienste erbringen, die über Unternehmensstandorte oder – wie im Fall vieler Konzerne – auch über Länder verteilt sind.

Die zunehmende Vernetzung von Unternehmen mit Lieferanten, Partnern und Kunden, die Automatisierung von Fertigungsprozessen und die intensive Auswertung von geschäftsrelevanten Daten führt zu einer immer stärkeren Kopplung des Unternehmenserfolgs an die Leistungsfähigkeit und Zuverlässigkeit der IT-Systeme sowie der geschäftskritischen Anwendungen und Dienste. Die Überwachung der Performance und Sicherheit dieser Dienste gehören daher zu den elementaren und wichtigen Aufgaben von IT-Abteilungen.

Dabei ist Performance- und Security-Monitoring in räumlich weit verteilten Systemen keineswegs ein reines Konzernthema. Durch die systematische Vernetzung von Fertigungs- und Geschäftsprozessen im Rahmen von Industrie 4.0 ist auch der Mittelstand – unter anderem angestoßen durch gesetzliche Regularien – gefordert, geeignete Monitoring-Maßnahmen zu implementieren. Darüber hinaus bieten Techniken zum Monitoring von räumlich weit verteilten IT-Systemen auch für einfachere Infrastrukturen einen direkten und spürbaren Mehrwert.

Die Performance-Überwachung kann grundsätzlich mithilfe von Flow-basierenden oder paketbasierenen Monitoring-Systemen erfolgen. Beide Varianten haben Vor- und Nachteile, die bei einer Investitionsentscheidung genau zu betrachten sind. Werden die zu überwachenden Dienste durch räumlich weit verteilte IT-Systeme erbracht, ergeben sich zusätzliche, spezielle Anforderungen an die eingesetzten Monitoring-Lösungen.

Monitoring-Arten

Bei der Überwachung von Diensten lassen sich verschiedene Monitoring-Ansätze unterscheiden, die folgende Themen adressieren: Verfügbarkeit (Nagios und Co.), Leistungsfähigkeit (Performance), Sicherheit (Security) und Service-Monitoring (Layer-7-Monitoring bei Dienstketten: Session-Verfolgung, Application Logging, Extraktion von kundenspezifischen Key-Performance-Indikatoren, Überwachung von Service-Level-Agreements etc.).

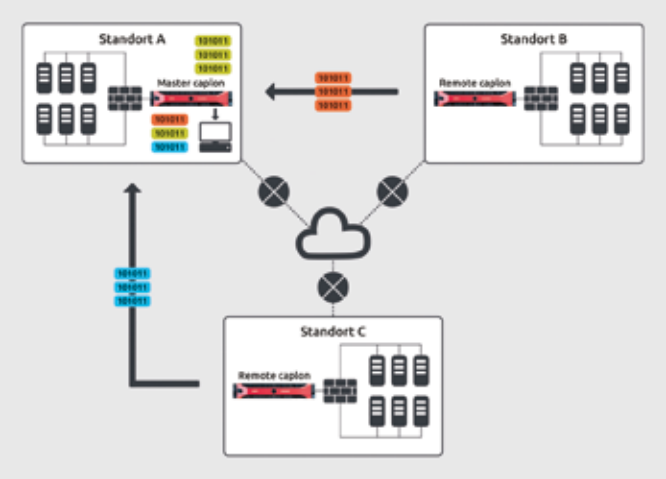
Erkennt der Betreiber Probleme beim Netzwerk oder bei den Applikationen, ist es hilfreich, wenn die verwendeten Überwachungslösungen auch Möglichkeiten zur Root-Cause-Analyse bieten.

Wenn Insider von Monitoring jenseits von Nagios-ähnlichen Systemen sprechen, dann ist meist ein sogenanntes Application-Aware Network Performance Monitoring (AANPM) gemeint. Für AANPM sind im Allgemeinen keine Nutzdaten (Payload) erforderlich. Um typische Performance-Indikatoren wie Lauf- und Antwortzeiten, Protokollverteilung, Auslastung, Anzahl an Retransmissions etc. zu ermitteln, genügen die Informationen aus dem Protokoll-Header. Daher ist der Einsatz von Flow-basierenden Monitoring-Systemen ein naheliegender Ansatz zum Performance-Monitoring.

Flow-basierende Monitoring-Systeme

Flow-basierende Monitoring-Systeme sammeln die aus Protokoll-Headern gewonnenen Performance-Kennwerte, die Flow-fähige Netzwerkkomponenten wie Router, Switches, Firewalls etc. zur Verfügung stellen, und werten diese aus. Dieser Ansatz kann bei einer überwiegend homogenen Infrastruktur mit vielen Flow-fähigen Netzwerkkomponenten und bei ausschließlichem Performance-Monitoring vorteilhaft sein. Aufgrund der technischen Basis existieren jedoch drei grundsätzliche Problemfelder:

– Da nicht alle Netzwerkkomponenten Flow-fähig sind, sind die Lücken im Netzwerk durch zusätzliche Flow-Generatoren zuschließen,
– die Übertragung der Flow-Informationen an die Flow-Kollektoren erfolgt über herstellerspezifische Flow-Protokolle wie Netflow, Netstream, Cflow, Jflow, Sflow. Bei gemischtem Einsatz kann es daher zu inkonsistenten Analyseergebnissen kommen. Bei Verwendung von



Beim standortübergreifenden Service-Monitoring ist es wichtig, dass nicht alle Daten von den Remote-Datenerfassungssystemen zur zentralen Analyse-Appliance gehen. Da bei den wenigsten Unternehmen separate breitbandige LAN/WAN-Verbindungen zur Verfügung stehen, muss auf den Datenerfassungssystemen eine sinnvolle Filterung der erfassten Daten inklusive einer Vorabanalyse erfolgen.

Sflow lassen sich zudem aufgrund der zugrunde liegenden statistischen Methoden bei der Datenauswertung keine schnellen Laständerungen erkennen, die sogenannten Microbursts, und
– bei räumlich weit verteilten Systemen stoßen viele Flow-basierende Monitoring-Systeme konzeptbedingt an ihre Grenzen.

Paketbasiertes Monitoring

Paketbasierende Monitoring-Systeme zeichnen sich dadurch aus, dass sie unabhängig von Netzwerkkomponenten und Flow-Protokollen alle übertragenen Pakete aufzeichnen können. Es ist nicht für jeden Anwendungsfall notwendig und aus Datenschutzgründen (BDSG, EU-DSGVO, TKG) auch problematisch, alle Pakete aufzuzeichnen. Aus diesen Gründen und zur Speicherplatzoptimierung kann in der Regel bei paketbasierenden Monitoring-Systemen die Anzahl der je Paket aufzuzeichnenden Daten konfiguriert werden. Damit ein paketbasiertendes Monitoring-System ein umfassendes und komfortables Performance-Monitoring bieten kann, benötigt es eine Port-unabhängige Applikationserkennung und präzise Zeitstempel.

Ein großer Vorteil der Technik von paketbasierenden Monitoring-Systemen ist der wesentlich breitere Einsatzbereich. Beispielsweise ist ein Performance-Monitoring sehr elegant und sinnvoll mit Security-Monitoring kombinierbar. Die komplexere Technik bei paketbasierenden Monitoring Systemen und die von der zu überwachenden Infrastruktur abhängige Anzahl an Datenerfassungssystemen kann – muss jedoch nicht zwangsläufig – zu höheren Investitionskosten führen.

Beim standortübergreifendem Performance-Monitoring ist es erforderlich, dass die Datenerfassung auch räumlich verteilt erfolgen kann (Remote Tracing). Dazu sind möglichst feingranulare Zeitstempel für jedes Paket erforderlich. Professionelle Spezialhardware zur Datenerfassung bietet nanosekundengenaue Zeitstempel pro Trace-Port. Die tatsächliche Genauigkeit reduziert sich jedoch bei der Zeitsynchronisation zwischen einzelnen Trace-Ports und nochmals bei der Zeitsynchronisation mehrerer Trace-Karten in einem Monitoring-System auf einen zweistelligen Nanosekundenbereich.

Wenn die Tracing- oder Monitoring-Systeme an verteilten Standorten stehen, muss die Lösung zur Zeitsynchronisation auf externe Zeitquellen wie GPS (erfordert bisweilen bauliche Maßnahmen, um Satellitenempfang sicherzustellen) oder DCF77 und netzwerkbasierende Synchronisationsmethoden wie PTP (Precision Time Protocol) und NTP (Network Time Protocol) zurückgreifen. Abhängig von der Methode ist dann eine unterschiedliche Genauigkeit der Zeitsynchronisation realisierbar: bei GPS bis zu einer Mikrosekunde, bei PTP im Mikrosekundenbereich und bei NTP und DCF77 im Millisekundenbereich.

Standortübergreifendes Service-Monitoring

Das Service-Monitoring erfasst die komplette Kommunikation zwischen Applikationen auf der Anwendungsschicht. Aus den mitgeschnittenen Daten lassen sich alle in den Anfragen (Requests) oder Antworten (Responses) enthaltenen Informationen extrahieren und nahezu beliebige Leistungsdaten ableiten. Auf diese Weise ist es beispielsweise möglich, die Application Response Time (Time to First Byte) und die Network Response Time (Zeit für den TCP Handshake) in Beziehung zueinander zu setzen.

Ebenso ist es möglich, die sogenannte User Experience zu ermitteln oder den Verlauf einer Session eines Dienstes über die verschiedenen Systeme einer Dienstkette zu verfolgen. Dazu ist es notwendig, dass eine Korrelation mehrerer zur Session gehörender Request-Response-Paare durchgeführt wird. Bei komplexen Datendiensten kann diese Korrelation oft nicht auf Basis eines einzelnen, gleichbleibenden Parameters erfolgen. Wird der Dienst zudem von räumlich weit verteilten Systemen bei hohen Datenraten erbracht, erschwert dies die Korrelation durch „ungenauere“ Zeitstempel zusätzlich. Bei diesen Fällen gilt es dann, anspruchsvolle heuristische Ansätze zu verwenden.

Beim Thema Security-Monitoring ist die Analyse der Anwendungsschicht von entscheidender Bedeutung. Viele Angriffe lassen sich nur über diesen Weg erkennen. Die Dekodierung des Application Layers ermöglicht somit vielfältige, nutzbringende Analysen, erfordert jedoch aus Datenschutzgründen (BDSG, EU-DSGVO, TKG) außerhalb zeitbegrenzter und zweckgebundener Monitoring-Einsätze besondere technische Maßnahmen zum Schutz personenbezogener Daten.

Die Datenerfassung beim Service-Monitoring sollte rein passiv und ohne Beeinflussung der Systeme und Dienste erfolgen. Dies ermöglichst einen einfachen Rollout, und es kommt nicht zu Gewährleistungsproblemen. Notwendige Voraussetzung dafür ist, dass bei der Datenerfassung kein Bit verloren geht. Diese Anforderung wirkt trivial, ist jedoch technisch anspruchsvoll. Letztendlich werden erst durch die Erfüllung dieser Anforderung die vollständige Rekonstruktion der Anwendungsschicht und eine korrekte Analyse der darin enthaltenen Daten möglich. Bereits ein verlorenes Paket kann zu einem „False Positive“ führen, also zu einem falschen Alarm. Bei lang anhaltenden TCP-Sessions, über die viele Einzel-Requests laufen (zum Beispiel SIP over TCP), kann ein verlorenes Paket sogar dazu führen, dass die Protokollanalyse temporär „aus dem Tritt“ gerät und der komplette Rest der Session nicht mehr analysierbar ist.

Beim standortübergreifendem Service-Monitoring ist es wichtig, dass nicht alle Daten von den Remote-Datenerfassungssystemen zur zentralen Analyse-Appliance zu transportieren sind. Da bei den wenigsten Unternehmen separate breitbandige LAN/WAN-Verbindungen zur Verfügung stehen, muss auf den Datenerfassungssystemen eine sinnvolle Filterung der erfassten Daten inklusive einer Vorabanalyse erfolgen.

Die extrahierten Analyseergebnisse stehen dann der zentralen Session-Monitoring-Appliance zur Verfügung und sollten aus Ressourcengründen nur bei konkretem Bedarf über das Netz gehen.

Dr.-Ing. Thomas Sinnwell/jos

Dr.-Ing. Thomas Sinnwell ist CEO R&D bei Consistec Engineering & Consulting, www.consistec.de.