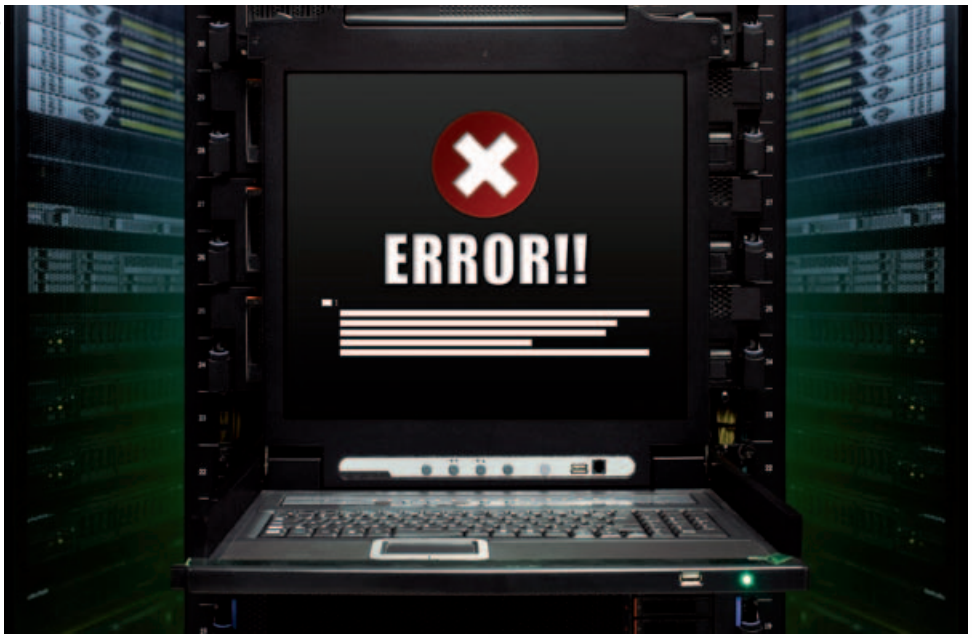
SCHNELLES NETZWERK-TROUBLESHOOTING



Bilder: Sawitree Jaiwanglok

Heiße Serverräume, eine dröhnende Kühlung, eine Vielzahl bunter Kabel und blinkende Lämpchen. So sieht das klassische Datacenter aus. Wie können in diesem Umfeld effizient Unstimmigkeiten im Netzwerk aufgeklärt werden?

Autor: Klaus Degner **Redaktion: Sabine Narloch**

➤ Das Netzwerk muss stabil laufen. 24/7, auch wenn der Administrator Feierabend hat. Ununterbrochen laufen Server mit großen Datenraten auf hohen Bandbreiten mit vielen unterschiedlichen Diensten gleichzeitig. Es gibt immer wieder Lastspitzen und Paketverluste. Bei dieser Komplexität muss der Administrator alle Netzwerkvorgänge im Auge behalten, auf verschiedene Fehlerklassen eingestellt sein und schnell reagieren können.

Dazu kommen Beschwerden von Usern über das langsame Netzwerk, die schlechte Qualität der VoIP-Anlage oder über Serverprobleme. Die Schuld wird oft beim Administrator gesucht, dabei gibt es eine Vielzahl möglicher Fehlerquellen, die in Frage kommen. Unstimmigkeiten können auf allen Netzwerkschichten auftreten.

Tipps für das Troubleshooting im Datacenter

Je nach Anwendungsfall geben spezifische Indikatoren wichtige Informationen über mögliche Problemquellen.

Storage-System: Bei Storage-Systemen ist die zu prüfende Größe die Geschwindigkeit der Datentransfers. Dabei sollte speziell berücksichtigt werden, ob Server-Hardware, Clients oder andere verbundene Netzwerke die vorgegebene Geschwindigkeit auch unterstützen. Mit dem Datendurchsatz über den Verlauf der Zeit lässt sich herauslesen, welche Anwendungen/IPs besonders viel Traffic verursachen beziehungsweise erhalten. Damit werden zeitliche Kollisionen von besonders großen Transfers deutlich, wie etwa Backups während der Bürozeit. Zudem lässt sich herausfinden, welche Komponente der Engpass ist. Eine Untersuchung von TCP-Zero-Window ist hilfreich bei der Erkennung von Empfängerüberlast.

WEB-SERVER: Nicht immer liegt der Fehler im Einflussbereich des Administrators. Möglicherweise kann der Web-Server die angefragten Web-Inhalte für intern und extern nicht schnell genug beantworten. Zur Feststellung von Problemen, die auf den Web-Server zurückzuführen sind, müssen die Anfragen an den Server analysiert werden können. Indikatoren sind dabei die Anzahl der Anfragen an den Server pro Sekunde, der Zeitpunkt der Anfragespitzen sowie deren Ursache, aber auch die Anzahl und Größe der übertragenen Daten. Über eine passive Messung der Antwortzeit lässt sich herausfinden, ob sich die Antwortzeiten über die Zeit verändern und welche Dienste besonders lange auf eine Antwort warten mussten. Vor allem bei nicht beantworteten Anfragen sollte geprüft werden, welche Anfragen es betrifft und warum. Auch seltene TCP-Retransmissions führen leicht zu sporadischen Problemen durch steigende Latenz von Anfragen.

VOIP: VoIP-Datenpakete sollten immer Vorrang vor anderen Paketen haben, um die Gesprächsqualität sicherzustellen. Bei Problemen helfen folgende Kennzahlen die Ursache zu identifizieren: die Anzahl der gleichzeitig geführten Telefonate, die in Anspruch genommene Bandbreite, die Richtigkeit der verwendeten Codecs, Jitter, Packetloss, MOS sowie nicht zustande gekommene Telefonate. Ebenfalls sollte immer betrachtet werden, ob QoS in beiden Kommunikationsrichtungen richtig eingesetzt wird.

INDUSTRIESERVER: Da Produktionsausfälle mit erheblichen Umsatzeinbußen verbunden sein können, sollte permanent geprüft werden, ob die Server zuverlässig arbeiten, ob es Ausfälle gab und ob der Server eventuell mit zusätzlichen Aufgaben belastet wird, die nicht

notwendig sind. Der Netzwerkverkehr im Industriebereich ist meistens relativ gleichmäßig. Es gilt dabei ein Auge auf Ausreißer, Ausfälle sowie Bandbreite und Latenz im Verlauf der Zeit zu richten. Natürlich sollten auch die Industrieprotokoll-spezifischen Antwortzeiten überwacht werden.

Um ein Problem aufzuklären, müssen oft verschiedene Netzwerk-Klassen beziehungsweise -Layer betrachtet werden. Daher bieten sich generische Messtools an, die Schicht für Schicht analysieren und die Ergebnisse übersichtlich darstellen. Mit dieser Methode können sowohl hausgemachte Probleme als auch sporadische Fehler analysiert werden. Außerdem werden Paket-Bursts sichtbar.

Zugriff auf die Daten zur Beurteilung des Datacenter-Zustands

Um den Datacenter-Zustand zu beurteilen, kann mit einem entsprechenden Netzwerkmessgerät vor Ort ein spezifischer Server überwacht werden. Diese Vorgehensweise erlaubt nur einen kurzen Einblick in den aktuellen Zustand des Netzwerkes. Tritt ein bestimmter Fehler in diesem Zeitfenster nicht auf, wird er nicht erfasst. Daher empfiehlt es sich, Messgeräte im Netzwerk zu integrieren, auf die der Admin remote zugreifen kann. Ein einfacher Zugriff kann über Managed Switches erfolgen. Managed Switches erlauben die Konfiguration eines Mirror-Ports. Dieser kann den gesamten Verkehr oder Teile davon zu einem Messsystem ausleiten. Diese Methode ist dauerhaft oder für einen gewissen Zeitraum möglich. Erforderlich ist die Installation des Messgeräts am Mirror-Port. Das Monitoring-Tool kann diese Daten empfangen, lesen und grafisch aufbereiten. Viele Switches unterstützen auch ERSPAN/GRE zum Weiterleiten von Netzwerkverkehr an eine andere IP-Adresse. Der Vorteil ist, dass der zu überwachende Server an einem anderen Ort stehen kann als das Messsystem und keine Verbindungen getrennt werden müssen. Allerdings muss dabei das Netzwerk den zusätzlichen Verkehr verkraften können.

Vorteilhaft sind Messsysteme, die über den normalen Web-Browser remote erreichbar sind. Somit muss man nicht vor Ort am Gerät sein, ist flexibel in der Nutzung von Endgeräten (Deskop-PC, Smartphone) und mehrere Administratoren können ein Gerät nutzen, um unterschiedliche Messungen zu untersuchen. Wertvolle Zeit kann außerdem mit dem Monitoring virtueller Maschinen gespart werden.

Wenn virtuelle Probleme real werden

Virtualisierung ist ein alltägliches Thema im Datacenter. Das bedeutet, es gibt mehrere physische Server, auf denen sehr viele virtuelle Maschinen laufen. Wie können in solch einer Umgebung Probleme analysiert werden? Virtuelle Maschinen erfordern zusätzliche Vorkehrungen. Geht der Verkehr ins physikalische Netzwerk, können die bekannten Wege benutzt werden, um den Verkehr ins Messsystem zu leiten. Interner Verkehr zwischen mehreren virtuellen Maschinen muss aber auch untersucht werden können. Dortige Probleme können zu Beeinträchtigungen nach außen führen. Hier kann ERSPAN innerhalb der virtuellen Maschine benutzt werden, um den Verkehr auszuleiten. Außerdem ist es möglich auf demselben VM-Host eine virtuelle Messumgebung einzurichten, um den Verkehr zu empfangen, ohne das physikalische Netzwerk betreten zu müssen. Der Vorteil ist weniger Netzwerklast.

Effizientes Troubleshooting

Die hohen Bandbreiten mit 10/25/40/100 GBit/s erfordern dedizierte Messgeräte. Ein herkömmlicher Laptop wird entweder überlastet mit der Menge an IP-Adressen und Verbindungen oder Verkehr muss stark gefiltert werden, damit zum Beispiel die Gigabit-Schnittstelle ausreicht. Da neben Laptops auch jedes Messsystem Grenzen hat, ist die Aufzeichnung von Rohdaten essentiell wichtig. Ausschließlich diese Rohdaten befähigen den Netzwerkverantwortlichen, auch nachträglich noch tiefer in eine Problematik einzutauchen. Dazu wird mit dem Messsystem der Fehler eingegrenzt und die Rohdaten zur tieferen Analyse extrahiert. Das ist auch bei sporadischen Fehlern besonders interessant, da man diese nicht in einer gezielten Aufzeichnung erfassen kann. Daher ist ein Messsystem unabdingbar, welches dauerhaft aufzeichnen kann. Eine nachträgliche Paket-Extraktion spart in diesem Fall viel Zeit. Um Fehler zu entdecken, bevor sie zum Problem werden, sollten möglichst viele Messdaten direkt live verfügbar sein, um einen Gesamtüberblick zu bekommen und bei Veränderungen schnell reagieren zu können. Ein aufbereiteter generischer Überblick erlaubt mit einem Blick auf die wichtigsten Kennzahlen den Netzwerkstatus zu kennen.

Klaus Degner ist Geschäftsführer bei der Allegro Packets GmbH