Netzwerk-Monitoring von Private Clouds

Whitepaper

Autoren: Dirk Paessler, CEO bei der Paessler AG
Dorte Winkler, Technischer Redakteur bei der Paessler AG

Erstveröffentlichung: Mai 2011 – Stand: Februar 2012

Inhalt

Einleitung

Das Konzept, das heute mit dem Begriff Cloudcomputing beschrieben wird, ist gar nicht so neu, wie man bei dem gegenwärtigen Hype denken könnte. Früher gab es ähnliche Ansätze unter den Stichworten Outsourcing und Server-Hosting, allerdings setzten lange Zeit die unzureichende Prozessorleistung, enorme Hardwarekosten sowie eine zu langsame Internetverbindung einer produktiven Nutzung im Alltag Grenzen. Mit heutiger Technik und Breitbandinternetverbindungen sowie schnellen, kostengünstigen Servern eröffnet sich nun endlich die Möglichkeit, nur die Services und Speicherkapazität vorzuhalten, die man tatsächlich benötigt, und diese erst bei aktuellem Bedarf flexibel zu skalieren. Die Nutzung von virtualisierter Serverleistung bei einem Dienstleister bietet ein breites Feld an Möglichkeiten zur Einsparung von Kosten, Steigerung der Performance und zu größerer Datensicherheit. Ziel des Einsatzes solcher Cloud-Lösungen ist eine konsolidierte IT-Umgebung, die Nachfrageschwankungen flexibel abfängt und vorhandene Ressourcen optimal ausnutzt.

Das Private-Cloud Konzept

Aus dem Public Cloud-Konzept ergeben sich verschiedenen Herausforderungen, denen sich die IT-Verantwortlichen eines Unternehmens stellen müssen. Die Sorge um die Datensicherheit und die Angst vor dem „aus der Hand geben“ der Kontrolle über die Systeme spielt dabei eine große Rolle. War es die IT-Abteilung bisher gewohnt, ihre Systeme per Firewalls nach außen abzuschotten und mit einer umfassenden Netzwerk-Monitoring-Lösung Verfügbarkeit, Performance und Auslastung ihrer Netzwerkinfrastruktur zu überwachen, sind beide Maßnahmen in der Cloud zunächst wesentlich schwieriger zu implementieren. Natürlich bieten alle großen Public Cloud-Anbieter hierfür durchdachte Absicherungsmechanismen und Kontrollsysteme an, trotzdem ist der Nutzer dieser Services immer darauf angewiesen, dass der Betreiber der Cloud ihm Einblick gewährt bzw. seine Daten schützt.

Private Clouds bieten viele der Vorteile von Cloud-Computing und minimieren gleichzeitig die Risiken.

Aus diesen Gründen ist der Aufbau einer „Private Cloud“ für viele IT-Entscheider eine interessante Alternative zur Nutzung von „Public Cloud“-Diensten. In diesem Fall erhalten Mitarbeiter und Anwendungen auf Basis des Cloud-Computings je nach Bedarf ihre IT-Ressourcen, während im Hintergrund jedoch das eigene Rechenzentrum steht oder eigene Server in einem großen Datacenter. Bei einer Private Cloud befinden sich alle genutzten Dienste und Ressourcen auf fest definierten und nur dem Nutzer zugänglichen Systemen, die gegen den Zugriff von außen entsprechend abgeschirmt sind. Private Clouds bieten viele der Vorteile von Cloud-Computing und minimieren gleichzeitig die Risiken. Im Unterschied zu vielen Public Clouds kann man hier die zu erfüllenden Qualitätskriterien bezüglich Performance und Verfügbarkeit selbst festlegen, deren Einhaltung überwachen und so sicherstellen, dass diese auch erreicht werden.

Netzwerk-Monitoring als Grundlage für die Planung einer Private Cloud

Grundvoraussetzung für eine konstante IT-Performance im Zusammenspiel zwischen verschiedenen virtualisierten Systemen ist eine bedarfsgerechte Ressourcenplanung.

Vor dem Umzug in die Private Cloud müssen sich die IT-Verantwortlichen damit auseinandersetzen, welche Leistungsansprüche der einzelnen Applikationen und welche zyklischen Schwankungen zu erwarten sind. Anhand von Auswertungen eines umfassenden Netzwerk-Monitoring können Langzeitanalysen, Trends und Lastspitzen erfasst sowie die in der Cloud erforderlichen Ressourcen bedarfsgerecht eingeplant werden. Dies ist eine der Grundvoraussetzungen, um eine konstante IT-Performance im Zusammenspiel zwischen verschiedenen virtualisierten Systemen zu gewährleisten.

Eine Private Cloud funktioniert jedoch nur dann reibungslos, wenn ein schnelles und hochgradig zuverlässiges Netzwerk die physikalischen Server verbindet. Deshalb muss die gesamte Netzwerkinfrastruktur vor dem Aufsetzen einer Private Cloud eingehend analysiert werden. Sie soll den Anforderungen in Bezug auf Übertragungsgeschwindigkeit und Stabilität genügen, andernfalls müssen Hardware oder Netzwerk-Anbindungen aufgerüstet werden. Schließlich können schon geringe Einbußen in der Übertragungsgeschwindigkeit zu hohen Leistungseinbrüchen führen. Dabei kann der versierte IT-Administrator sich genauso von einer umfassenden Netzwerk-Monitoring-Lösung, wie z.B. PRTG Network Monitor, unterstützen lassen wie bereits bei der Planung der Architektur seiner Private Cloud. Wenn in der Private Cloud eine Applikation (was meist mehreren virtualisierten Servern entspricht) auf mehreren Host-Servern („Cluster“) verteilt betrieben werden soll, verlangt dies als zentrale Speicherlösung die Nutzung von SANs (Storage Area Networks), welche die Daten über das Netzwerk übertragen. Damit rückt das Monitoring der Netzwerkperformance weiter in den Mittelpunkt.

Konsequente Überwachung des Netzwerks gewinnt in der Cloud an Bedeutung

Die neue Cloud entspricht dem alten Mainframe.

Bereits bei den in den 1980er Jahren eingesetzten Terminals konnte der Ausfall eines Zentralrechners ein komplettes Unternehmen lahmlegen. Das gleiche Schreckensszenario stellt heute der Ausfall von Systemen in der Cloud dar. Die aktuellen Entwicklungen zeigen, dass wir – vom Konzept des Mainframe-Computers kommend – über die Phase der stark verteilten Rechen- und Speicherleistung (jeder Arbeitsplatz hatte einen „vollwertigen" PC) nun wieder bei den zentralisierten IT-Konzepten angekommen sind. Die Daten liegen in der Cloud, und die Endgeräte werden wieder schlanker (RDP/Citrix-Terminals, Tablets, Smartphones usw.). Die neue Cloud entspricht also dem alten Mainframe.

Eine Private Cloud – genau wie jede Cloud – steht und fällt mit der Effizienz und Zuverlässigkeit der IT-Infrastruktur.

Der Ausfall einer einzigen VM in einer hoch virtualisierten Cloud-Umgebung kann schnell den Zugriff auf 50 oder 100 zentrale Anwendungen unterbrechen. Die Ausfälle versucht man mit modernen Clustering-Konzepten zu vermeiden, aber wenn ein System trotzdem ausfällt, muss umgehend gehandelt werden. Stürzt gar ein Host-Server ab und reißt eine größere Zahl von virtuellen Maschinen mit sich oder wird seine Netzwerkverbindung langsam oder unterbrochen, sind davon sofort alle auf diesem Host virtualisierten Dienste betroffen, was oft auch durch die besten Clustering-Konzepte nicht abzufangen ist.

Eine Private Cloud – genau wie jede Cloud – steht und fällt mit der Effizienz und Zuverlässigkeit der IT-Infrastruktur. Ausfälle von physikalischen oder virtuellen Servern, Verbindungsunterbrechungen, defekte Switches oder Router können teuer werden, wenn dadurch Mitarbeiter, automatisierte Produktionsprozesse oder Internet-Shops keinen Zugang mehr zu betriebswichtigen IT-Funktionalitäten haben. Deshalb stellt eine Private Cloud auch das Netzwerk-Monitoring vor neue Herausforderungen.

Eine Netzwerk-Monitoring-Lösung alarmiert den zuständigen IT-Administrator sofort, bei auftretenden Störungen innerhalb der IT-Landschaft, vor Ort und in der Private Cloud.

Um sicherzustellen, dass Nutzer jederzeit Zugriff auf ausgelagerte Geschäftsanwendungen haben, muss die Performance der Verbindung zur Cloud auf allen Ebenen und aus allen Perspektiven überwacht werden. Gleichzeitig muss sichergestellt werden, dass alle Systeme und Verbindungen innerhalb der Private Cloud reibungslos funktionieren. Und natürlich sollten die Verantwortlichen auch das Zusammenspiel zwischen Private Cloud und der eigenen lokalen IT-Landschaft am Unternehmensstandort im Auge behalten. Eine geeignete Netzwerk-Monitoring-Lösung leistet dies alles mit einem zentralen System und alarmiert den zuständigen IT-Administrator sofort, sowohl bei eventuell auftretenden Störungen innerhalb der eigenen IT-Landschaft vor Ort, als auch bei Störungen in der Private Cloud – auch wenn diese in einem externen Rechenzentrum betrieben wird.

Eine eigene Private Cloud ermöglicht bei Bedarf einen uneingeschränkten Zugriff auf alle relevanten Systeme direkt mit der eigenen Netzwerk-Monitoring-Lösung.

Eine Besonderheit beim Monitoring von Private Clouds ist, dass externe Monitoring Services nicht in die Cloud „hineinschauen" können, weil diese, wie der Name bereits sagt, privat, d.h. nach außen abgeschottet ist. Daher muss der Betreiber oder Kunde eine Monitoring-Lösung „mit in die Private Cloud" stellen, die dann vor Ort das Monitoring übernimmt. Dafür können die IT-Verantwortlichen die Private Cloud genauer und individueller überwachen als die Services, die man bei einer Public Cloud einkauft. Die Systeme einer eigenen Private Cloud ermöglichen bei Bedarf einen uneingeschränkten Zugriff. Damit ist der IT-Administrator in der Lage, den Zustand aller relevanten Systeme direkt mit einer eigenen Netzwerk-Monitoring-Lösung zu verfolgen. Das umfasst sowohl die Überwachung jeder einzelnen virtuellen Maschine als auch des VMware Host und aller physikalischen Server, Firewalls, Netzwerk-Anbindungen usw.

Monitoring der Privat Cloud aus zwei Perspektiven

Zur umfassenden Überwachung einer Private Cloud sollte das Netzwerk-Monitoring die Systeme sowohl aus Nutzer- als auch aus Server-Perspektive auf dem Radar haben. Betreibt ein Unternehmen zum Beispiel eine umfangreiche Website inklusive Webshop in einer Private Cloud, dann könnte das Netzwerk-Monitoring wie folgt eingesetzt werden.

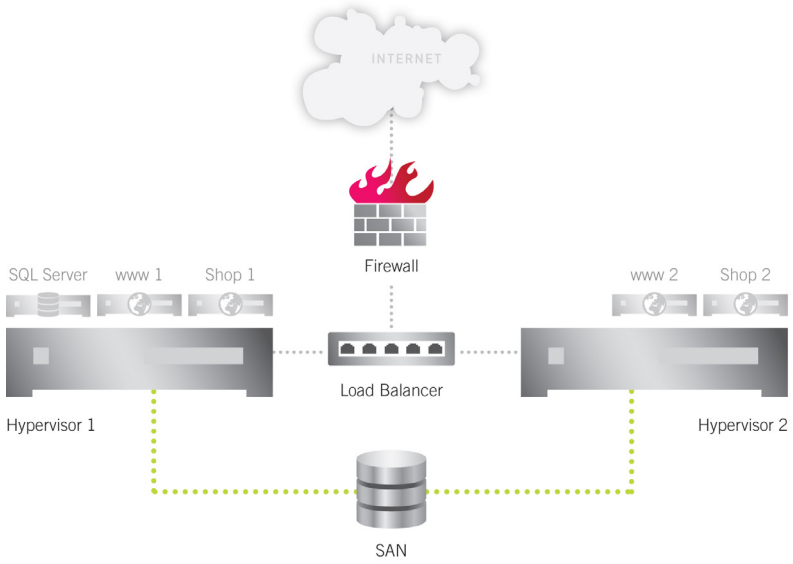


Abbildung 1:
Schemazeichnung des Web-Hostings der Paessler AG in einer Private Cloud

Aus Sicht des Nutzers

Der Betreiber einer Website möchte für alle Besucher sicherstellen, dass tatsächlich alle Funktionen permanent zur Verfügung stehen, unabhängig davon, wie diese technisch realisiert sind. Dafür sind insbesondere die folgenden Fragen relevant:

- Ist die Website online?
- Liefert der Webserver auch tatsächlich die richtigen Inhalte aus?
- Wie schnell lädt die Seite?
- Funktioniert der Warenkorb-Prozess?

Alle diese Fragen können nur beantwortet werden, wenn das Netzwerk-Monitoring von außerhalb der zu überwachenden Server erfolgt, am besten sogar von außerhalb des entsprechenden Rechenzentrums. Es bietet sich daher an, eine Network-Monitor-Lösung auf anderen Cloud-Servern oder in anderen Rechenzentren aufzusetzen. Dazu ist es entscheidend, dass alle Standorte eine hohe Zuverlässigkeit aufweisen bzw. das Monitoring durch ein Failover-Cluster abgesichert ist, so dass eine unterbrechungsfreie Überwachung gewährleistet werden kann.

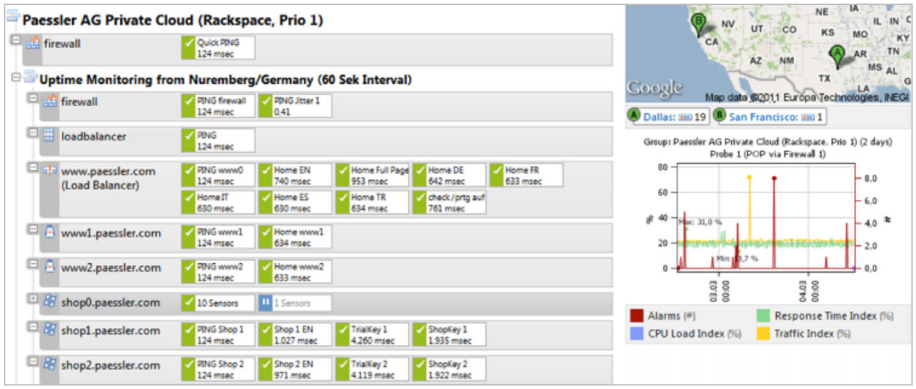


Abbildung 2:
Diese Webserer-Überwachung zeigt einige Sensoren, die zum Monitoring aus Benutzerperspektive eingesetzt werden

Diese Überwachung aus der Ferne sollte bei dem oben genannten Beispiel des Monitorings einer Website z.B. das Folgende umfassen:

- Ping der Firewall, des HTTP Loadbalancer und des Webservers
- HTTP/HTTPS-Sensoren für
  - die Überwachung der Ladezeit der wichtigsten Seiten
  - die Überwachung der Ladezeit alle Assets einer Seite wie CSS, Bilder, Flash etc.
  - die Überprüfung, ob Seiten bestimmte Wörter enthalten wie z.B. „Error“
  - die Messung der Ladezeit bei Downloads
- HTTP-Transaktions-Überwachung, zur Simulation des Einkaufsprozesses
- Sensoren, die die Restlaufzeiten der Gültigkeit von SSL-Zertifikaten überwachen

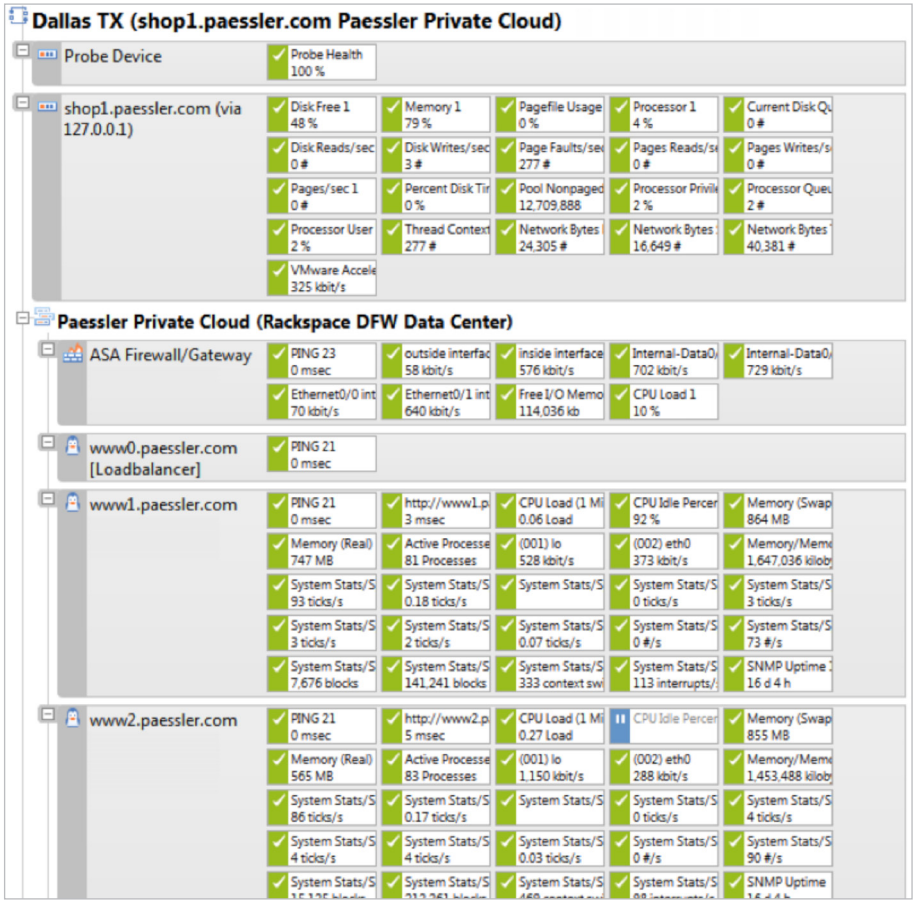
Immer wenn einer dieser Sensoren ein Problem findet, sollte die Netzwerk-Monitoring-Lösung einen entsprechend aussagekräftigen Alarm an den zuständigen Administrator senden. Dabei hilft es, ein regelbasierendes Monitoring einzurichten. PRTG Network Monitor bietet zum Beispiel die Möglichkeit bei einem Time-out des Ping-Sensors für die Firewall, alle anderen Sensoren pausieren zu lassen, um eine Alarmflut zu vermeiden, da in diesem Fall offensichtlich die Verbindung zur Private Cloud insgesamt unterbrochen ist.

Aus Serversicht

Für das Monitoring der (virtuellen) Server, die in der Private Cloud betrieben werden, sind andere Fragen entscheidend:

- Laufen die virtuellen Server störungsfrei?
- Funktionieren die interne Datenreplikation und der Load-Balancer?
- Wie hoch sind CPU-Last und Speicherverbrauch?
- Steht genügend Speicherplatz zur Verfügung?
- Arbeiten E-Mail- und DNS-Server störungsfrei?

Abbildung 3:
In diesem Screenshot sieht man den größten Teil der Sensoren, die das Produktivsystem aus Serverperspektive überwachen



Diese Fragen können nicht mit einem Netzwerk-Monitoring „von außen“ beantwortet werden. Dazu muss entweder eine Monitoring-Software auf den Servern mitlaufen, oder das Monitoring-Tool muss die Möglichkeit bieten, die Server mittels Remote Probes aus der Ferne zu überwachen. Solche Sonden monitoren dann z.B. die folgenden Parameter, sowohl auf jedem (virtuellen) Server, der in der Private Cloud läuft, als auch auf den Host-Servern:

- CPU-Last
- Speicherverbrauch (page files, swap file, page faults etc.)
- Netzwerk-Traffic
- Festplattenzugriffe, freier Plattenplatz und Lese-/Schreibzeiten beim Plattenzugriff
- Systemnahe Systemparameter (z.B. Länge der Processorqueue, Context Switches)
- http-Antwortzeit des Webservers

Oft werden die kritischen Prozesse wie zum Beispiel SQL-Server oder Web-Server einzeln gemonitort, insbesondere bezüglich CPU- und Speicherverbrauch. Zusätzlich kann auch noch der Zustand der Firewall (Bandbreitennutzung, CPU) überwacht werden. Wenn eine dieser gemessenen Variablen außerhalb eines definierten Bereichs liegt (z.B. CPU-Auslastung über 95 % für mehr als zwei oder fünf Minuten) sollte die Monitoring-Lösung Alarme an den zuständigen Administrator schicken.

Fazit

Mit der zunehmenden Nutzung von Cloud-Computing stehen Systemadministratoren vor neuen Herausforderungen. Eine Private Cloud – genau wie jede Cloud – steht und fällt mit der Effizienz und Zuverlässigkeit der IT-Infrastruktur. Das bedeutet, dass die IT-Verantwortlichen sich schon bei der Planung damit auseinandersetzen müssen, welche Leistungsansprüche die einzelnen Applikationen stellen, um die Ressourcen bedarfsgerecht zu kalkulieren. Im laufenden Betrieb ist es entscheidend, dass Nutzer jederzeit Zugriff auf alle Anwendungen haben. Dazu muss die Performance in der Verbindung zur Cloud umfangreich überwacht werden. Gleichzeitig muss sichergestellt werden, dass alle Systeme und Verbindungen innerhalb der Private Cloud reibungslos funktionieren. Eine Netzwerk-Monitoring-Lösung sollte deshalb alle Dienste und Ressourcen aus allen Perspektiven überwachen. Damit wird die stetige Verfügbarkeit der Systeme sichergestellt, und Überlastungen können durch langfristige Planung auf Basis umfangreicher Monitoring-Daten gezielt vermieden werden.

Über die Paessler AG

Die Paessler AG mit Sitz in Nürnberg entwickelt Software für die Bereiche Netzwerküberwachung und Webserveranalyse seit 1997. Weltweit setzen mehr als 150.000 Administratoren, Webseitenbetreiber, Internet Service Provider und andere IT-Verantwortliche Paessler Software ein. Freeware und Testversionen aller Produkte können unter www.de.paessler.com heruntergeladen werden.

Paessler AG
Bucher Straße 79a, 90419 Nürnberg, Deutschland
www.de.paessler.com, info@paessler.com

UST#: DE 217564187
Steuer#: FA Nürnberg 241/120/60894
Eintragung: Amtsgericht Nürnberg HRB 23757

Vorstand: Dirk Paessler, Christian Twardawa
Vors. d. Aufsichtsrats: Dr. Marc Rössel