Eine Themenbeilage der
Heise Medien GmbH & Co. KG

I
2016

RECHENZENTREN UND INFRASTRUKTUR

KOMPONENTEN, KABEL, NETZWERKE

Wer weiß, ob die Server noch durchhalten

powered by:

Server & Storagesysteme

Wir schaffen Platz für das wirklich Wichtige!

Storage Unlimited

BigFoot Storagesystem XXLarge

BigFoot Storagesystem Flash

BigFoot Storagesystem XXCold

BigFoot Storagesystem Object

BigFoot Storagesystem XXFast

BigFoot Storagesysteme

Die Idee: Es sollte ein Storage-System geben, das in zahlreichen Anwendungsgebieten einsetzbar ist. Es muss individuell konfigurierbar und flexibel erweiterbar sein, egal ob 10TB oder 10PB Speicherkapazität benötigt werden.

Aus dieser Idee haben wir die BigFoot Storage Produktfamilie entwickelt. Die Systeme lassen sich nahezu beliebig konfigurieren und eignen sich als Datenbankserver genauso, wie als Enterprise-Storage-Server, Nearline-Storage, als Virtual Tape Labrary oder ebenso für den Einsatz im Cloud Computing oder für Big-Data-Anwendungen.

Wir konfigurieren auch Ihren BigFoot Storage passend zu Ihren Anforderungen.

Überzeugend in Leistung und Preis – das und mehr schafft die BigFoot Storage Familie.

Rausch Netzwerktechnik GmbH
Englerstraße 26 · D-76275 Ettlingen
Telefon (07243) **5929-0** · Telefax -14 · info@rnt.de
www.rnt.de

>> Mehr erfahren!

RAUSCH NETZWERKTECHNIK
www.rnt.de

Sympathisch und gut beraten. Bestens betreut.

Wer weiß, ob die Server noch durchhalten

Die Alten sind zufrieden – und die Jungen. Unzufrieden mit ihrer eigenen Leistung sind vor allem die Rechenzentren mittendrin, die ihre Arbeit zwischen 2000 und 2012 aufgenommen haben. Dieses Kernergebnis des ersten Studienberichts zum Optimized-Data-Center-Benchmark erklärt sich aus dem rasant steigenden Anforderungen: Durch die Altbestände ist bereits eine Modernisierungswelle geschwappt – sie erreichen einen überdurchschnittlichen Effizienzindex von 65 Punkten. Beispielhaft zeigt das die im August 2015 fertiggestellte Neueinrichtung der Klimatechnik für die Universität Mannheim (Seite 24). Die neueren Anlagen wiederum konnten schon beim Bau aktuelle Best Practices berücksichtigen und neue Technologien nutzen; hier liegt der eher selbstkritische Effizienzindex bei immerhin 60 Punkten und damit knapp über dem Durchschnitt von 59.

Das ist insgesamt kein gutes Ergebnis. Es ist umso bedenkenswerter, als es die Selbsteinschätzung der RZ-Betreiber widerspiegelt. Auf www.optimized-datacenter.de haben RZ-Experten, techconsult und iX ein kostenfreies Online-Tool entwickelt, mit dessen Hilfe Verantwortliche in 60 bis 90 Minuten herausfinden, wie sie im Vergleich mit anderen Unternehmen ihrer Branche und Größe dastehen. Die Fragen reichen vom Rechenzentrumsbetrieb über die physische und virtuelle IT-Infrastruktur bis hin zur Gebäudeinfrastruktur und der externen Anbindung. Einen ausführlichen, individuellen Statusbericht bekommt man sofort; der übergreifende Studienbericht 1 („Die Effizienz deutscher Rechenzentren 2015/2016“) ist dort seit Kurzem verfügbar.

Die Rechenzentren Baujahr 2000 bis 2010, die eigentlich in den besten Jahren sein sollten, bekommen offenbar heftig zu spüren, dass das Bessere der Feind des Guten ist. CIOs und Admins ist sehr wohl klar, dass sie den Überblick über ihr gewachsenes RZ-Gebilde zu verlieren drohen. Das ist der Grund, warum sich das Thema Komplexität und Monitoring wie ein roter Faden durch dieses Heft zieht. Gleich eingangs zeigt Oliver Lindner einen interessanten Aspekt im Data Center Infrastructure Management auf: Predictive Maintenance kann die optimalen Wartungsintervalle je nach Standort, Modell und Situation berechnen und damit Downtimes und Kosten im Griff behalten (Seite 4). Mittlerweile können sogar intelligente Stromschaltleisten umfangreiche Steuer- und Kontrollfunktionen übernehmen. Wie das funktioniert – und wo die Sicherheitsrisiken liegen –, erklärt Ralf Ploenes ganz zum Schluss (Seite 25). Dazwischen geht es darum, wie Microsoft Azure Stack Cloud-Funktionen ins Rechenzentrum übersetzt (Seite 20) und was Hyperkonvergenz zur Datensicherheit beitragen kann (Seite 16). Außerdem gibt Dirk Paessler persönlich einen guten Überblick über die Relevanzkriterien bei der Entscheidung für oder gegen eine Netzwerkmonitoring-Lösung (Seite 22). Sein Tenor: Es nützt nur das, was tatsächlich genutzt wird.

Dazwischen sehen wir uns zum einen die Treiber der Komplexität an, zum anderen zeigen wir mögliche Lösungen auf. Zuerst das Pflichtprogramm. Vier Teile von DIN EN 50600 sind bereits erschienen, aber bislang berücksichtigt die Energieeffizienznorm die Systemauslastung nicht als Kriterium, moniert Ariane Rüdiger (Seite 11). Zugleich kommen 2016 neue Verkabelungsnormen für Rechenzentren heraus. Doris Piepenbrink hat bei den zuständigen Arbeitsgruppen nachgehakt und berichtet, was für Highspeed-Kupferkabel bis 100 GBit/s vorgesehen ist (Seite 18). Selbst Software-defined-Ansätze erweisen sich als Lösung und Druckverstärker zugleich: Einerseits gibt es softwaredefinierte IT-Infrastrukturen bereits als fertige Komplett-Appliances, andererseits argumentiert Matthias Hain, dass frei definierte Netzwerke auf Provider-Seite bald ganz andere Geschäfts- und Abrechnungsmodelle erfordern werden (Seite 6). Auf Anwenderseite wird man sich mit weniger sicher nicht zufriedengeben.

Thomas Jannot

Infrastrukturmanagement mit Echtzeitprognosen

Vorausschauende Analysen berechnen optimale Wartungsintervalle

Wartungsausfälle sind lästig, aber Stillstand wäre reines Gift. Mit vorausschauender Wartung versuchen Betreiber nun, den Betrieb ihres Rechenzentrums zu optimieren. Statt Bauchgefühl und Erfahrungswerten kommen zunehmend moderne Analytics-Verfahren zum Einsatz, um Aufwand und Bedarf anzugleichen.

Die IT-Domänen Analytics und Business Intelligence stellen eifrig genutzte Werkzeuge bereit, um – meist historische – Datenreihen auszuwerten, Lehren aus der Vergangenheit zu ziehen und zu erklären, warum die Dinge so sind, wie sie sind. Ihre Nachfolger aus dem Bereich Data Science können bereits einen recht verlässlichen Blick in die Zukunft werfen. Diese Wahrsagekunst gibt es nicht als Kristallkugel im Jahrmarktzelt, sondern als DCIM-Software (Data Center Infrastructure Management) im Rechenzentrum.

Intelligente Problemerkennung

Die einfachste Form einer Analyse ist die reine Statistik, die gängige Kennzahlen erfasst und sie grafisch darstellt. Ein deutlich höherer Informationsgehalt lässt sich durch zusätzliche Dimensionen erreichen; hierbei handelt es sich um klassische Data-Warehouse-Technik mit OLAP (Online Analytical Processing). Den höchsten Erkenntniswert liefert aber die vorausschauende Analyse, die das künftige Verhalten von Systemen anhand von Modellen prognostiziert, die sich aus historischen Verhaltensdaten speisen oder aus logischen Zusammenhängen ergeben. Dabei ist die Validität der Vorhersage abhängig von der Qualität der Datengrundlage und des verwendeten Modells. Der Drei-Tage-Wetterbericht ist deshalb verlässlicher, weil das Datenmodell hierfür ausreichend komplex und zuverlässig ist, während die langfristige Wetterprognose an vielen „Unberechenbarkeiten“ leidet.

Auch in Rechenzentren halten diese Verfahren Einzug. Im Zentrum stehen Vorhersagemodelle für die vorausschauende Wartung (Predictive Maintenance); sie sollen Störungen vermeiden und gleichzeitig die Wartungsintervalle anhand des tatsächlichen Bedarfs optimieren. Ein Beispiel: Filter von Klimageräten verschmutzen nicht gleichmäßig, sondern je nach dem Staubgehalt der Luft. Hier sind Rechenzentren mit freier Kühlung in städtischen Bereichen (oder in der Nähe zu aktiven Vulkanen) gegenüber klassischen, isolierten Innenräumen im Nachteil. Deshalb ist es nicht sinnvoll, für beide Szenarien im Wartungsvertrag dasselbe zeitliche Raster für den Tausch oder die Reinigung der Filter festzuschreiben; stattdessen führt man die Arbeiten besser nach Bedarf durch. Wie bei den Filtern sind natürlich auch die Wartungsintervalle von Batterien der USV-Anlage, von Pumpen, Generatoren und anderen RZ-Komponenten automatisiert anpassbar.

Da es andererseits nicht hilfreich ist, so lange zu warten, bis der Filter vollkommen verstopft ist und das Gerät seinen Betrieb einstellt, muss der richtige Zeitpunkt unter Berücksichtigung des Vorlaufs für die Wartungsplanung vorherberechnet werden. Neben einfachen Ansätzen wie der Laufzeit (Betriebsstunden) gibt es auch fortschrittlichere und zuverlässigere Verfahren, die aus Messdaten und Vergleichen Rückschlüsse auf den aktuellen Zustand ziehen: Ein verstopfter Filter bedeutet in Konsequenz einen zu geringen Luftdurchsatz, der sich leicht erkennen lässt, wenn ein angepasster Algorithmus die Drehzahl der Lüfter und die tatsächliche erzeugte Luftmenge vergleicht. Für die Vorhersage von Veränderungen stellen Veränderungen selbst wieder die Basis dar, da die Systeme teilweise selbstlernend sind (Stichwort: Machine Learning) und immer mehr Einflussfaktoren in die Modelle aufgenommen werden.

Automatisiert arbeitet effizienter

Da moderne Rechner ausreichend Leistung zur Verfügung stellen, laufen diese Vorhersagen in der Regel in Echtzeit ab. Der große Nutzen von Predictive Maintenance liegt darin, dass sie heraufziehende technische Probleme erkennen kann, bevor es zu einem Stillstand kommt. Gegenüber periodischen Wartungen ergeben sich sowohl eine Reduktion der Ausfallzeiten als auch kürzere Zeitspannen, in denen die Anlagenteile im Wartungsmodus nicht aktiv genutzt werden können. Gleichzeitig sinken die Wartungskosten für den Erhalt des gesicherten Zustands deutlich, wenn man sich auf die erforderlichen Maßnahmen beschränkt und weniger Ersatzteile beschaffen muss.

Im optimalen Fall erhält man mit DCIM-Unterstützung einen umfassenden und stets aktuellen Überblick über sämtliche Verbrauchs- und Temperaturwerte. Mit diesen Daten lässt sich wiederum prüfen, ob zum Beispiel Umbauten die ursprünglichen Planungserwartungen erfüllen, an welchen Stellen in Zukunft strukturelle Engpässe zu erwarten sind und wie die weitere Kapazitätsplanung aussehen sollte. Nicht zuletzt sind diese Informationen maßgeblich relevant für die verpflichtende energetische Bewertung des Rechenzentrums.

Ein Produktiveinsatz ist heute in Rechenzentren vor allem bei Steuerungen neuer Kühlsystemgenerationen zu beobachten. Diese Systeme haben sich bewährt und als zuverlässig erwiesen, sodass davon auszugehen ist, dass das Verfahren in nicht allzu ferner Zukunft als Off-the-Shelf-Technologie zum Stand der Technik wird. Das ist in jedem Fall eine gute Nachricht, denn derart effizient gewartete Rechenzentren könnten sich zunehmend den wirklich wichtigen Aufgaben widmen – etwa der vorausschauenden Berechnung einer zuverlässigen 14-Tage-Wetterprognose.

Oliver Lindner,
Head of Business Line DCIM bei FNT

Besuchen Sie uns auf der
CeBIT in Halle 12, Stand A53!

Komplexität reduzieren.

Für mehr Flexibilität.

Integrierte Datacenter-Infrastruktur für Upgrades und neue Installationen

Damit sind Sie vorbereitet auf Big Data und komplexe IT-Anforderungen. Mit integrierten Infrastruktur-Systemen, Software und Lifecycle Services vereinfachen wir jedes Datacenter-Projekt - von der Planung über das Design bis zum Betrieb. Das Ergebnis? Ein zuverlässiges, flexibles und effizientes Datacenter für Ihre Geschäftsanforderungen.

schneider-electric.com

Life Is On | Schneider Electric

SDN verändert die Nutzung der Netzwerke

Das Geschäfts- und Abrechnungsmodell der Provider steht auf dem Prüfstand

Vor drei Jahren erklärte die Fachpresse Software-defined Networking zum „heißen Thema“, und die Hersteller von Netzwerkkomponenten überboten einander mit neuen Strategien und Produkten. Mittlerweile wird klar, dass sich mit SDN nicht nur die Netze selbst wandeln, sondern auch das Kundenverhalten.

Es ist meist ein weiter Weg vom Hype unter den Herstellern und in den Medien bis zur Anwendung durch Service Provider und in den Unternehmen. Die Analysten von Gartner sahen sich noch im Lauf des vergangenen Jahres dazu genötigt, SDN zu erklären und deutlich zu machen, dass es dabei im Wesentlichen nicht um eine Technologie geht, sondern um ein neues Konzept für eine effizientere und intelligentere Nutzung von Netzwerken: Mit SDN erreicht die Trennung von Hard- und Software, wie sie aus dem Cloud Computing bekannt ist, die Netzwerke. Die Nutzung der Netze, vor allem aber die Beziehungen der Netzwerkbetreiber zu ihren Kunden, werden sich dadurch grundlegend verändern.

Vom Hype zur Anwendung

Dank realer Anwendungsszenarien hat SDN zur Jahreswende den Status des Technologie-Hypes verlassen und entfaltet seine Wirkung im produktiven Netzbetrieb. Wie sieht ein solches Anwendungsszenario aus?

Rechenzentren spielen eine zentrale Rolle in der Digitalisierung. So schätzt beispielsweise der Global Cloud Index von Cisco, dass Cloud Services und Anwendungen bis zum Jahr 2018 für 76 % der 8,6 Zettabyte des weltweiten Datenverkehrs in Rechenzentren verantwortlich sein werden. Dieses Volumen entspricht rund 9 Trillionen Stunden (eine Zahl mit 18 Nullen) Online-Streaming in HD.

Für Unternehmen aus datenintensiven Branchen bedeutet das, dass die Rechenzentrumsstrategie immer wichtiger für den Unternehmenserfolg wird. Zu diesen datenintensiven Branchen zählen neben den Anbietern von Cloud-Computing-Services unter anderem Finanzdienstleister, die sich schnell mit neuen Märkten und Kunden verbinden möchten, um Handelsoptionen zu nutzen, Medienunternehmen, die ihren Zuschauern online HD-Inhalte zur Verfügung stellen möchten, oder auch Touristik-, Entertainment- und Handelsunternehmen, die über ihre Online-Plattformen Buchungen und Verkäufe abwickeln. Für all diese Unternehmen ist nicht nur die Leistungsfähigkeit eines einzelnen Rechenzentrums von Bedeutung, sondern auch die Möglichkeit, den Datenverkehr zwischen verschiedenen Rechenzentren zu lenken und damit robustere Strategien zur Rechenzentrumsdiversifikation einzuschlagen. Denn viele dieser Unternehmen haben kein regelmäßig starkes Datenaufkommen; vielmehr ist ihr Geschäftsbetrieb geprägt von geplanten und ungeplanten Lastspitzen, die sich durch Jahresabschlüsse, Marketing-Kampagnen, Filmpremieren, Black Fridays, Cyber Mondays oder den Vorverkaufsstart für Konzertkarten großer Stars ergeben.

Selfservice und Flexibilität

Beim Umgang mit diesen Lastspitzen kommt nun Software-defined Networking zum Zuge. Denn SDN ermöglicht es, Netzwerkverbindungen beispielsweise zwischen Rechenzentren über ein Selfservice-Portal schnell und einfach selbst zu konfigurieren. Die Services werden innerhalb von Minuten bereitgestellt statt wie bislang in Tagen oder gar Wochen. Und sie können jederzeit wieder abbestellt werden. Die Abrechnung erfolgt nach Nutzungsdauer und eingesetzter Bandbreite. Dieser Selbstbedienungsgedanke und die Flexibilität stellen Anwender und Anbieter gleichermaßen vor Herausforderungen.

Damit Unternehmen ihre Verbindungen selbst einrichten können, werden sie entsprechendes Know-how brauchen, auch wenn die SDN-Anwendungen intuitiv aufgebaut sind. Administratoren müssen die Än-

DER MARKT BEGINNT ZU ZAPPELN

Zu den jüngeren Buzzwords gehört „Agility“, und zwar in ganz unterschiedlichen Zusammenhängen, vom Agile Management bis zur IT Agility mit Blick auf konkrete Cloud-Dienste. Tatsächlich steckt hinter der unscharfen „Beweglichkeit“ eine richtige Beobachtung: dass Services sich zunehmend von der Infrastruktur abkoppeln. Im Hinblick auf ein – selbstverständlich: mobiles – Internet der Dinge heißt das, dass Product und Corporate-IT zusammenwachsen, dass Applikationen in Microservices heruntergebrochen werden und dass CIOs von jetzt auf gleich neue Ressourcen aktivieren müssen. Auch von daher ist zu erwarten, dass softwaredefinierte Rechenzentren eher früher als später Standard werden. Modelle wie Network as a Service (NaaS) entstehen aus dem ungeduldigen Bedarf auf Anwenderseite.

Zu bedenken ist, dass diese Entwicklung nicht unmittelbar technologiegetrieben ist – den Agility-Druck erzeugen die betriebswirtschaftlichen Notwendigkeiten. Personalisierung und individuelle User Experience im Verbund mit niedrigen Margen und schnelleren Märkten jagen den Bedarf an absolut flexiblen IT-Kapazitäten weit über das hinaus, was bislang brav „Skalierbarkeit“ hieß. Auf technologischer Seite tobt daher zurzeit der Kampf um Schnittstellen und Standards. Auf der Seite der Anwenderunternehmen wird künftig das Thema Service Level Agreement noch eine große Rolle spielen: Je flexibler die Dienste sind, desto transparenter sollten die Gütevereinbarungen sein. (fe)

Der transtec Virtualisierungsansatz:

durchdacht, effizient und zuverlässig

Investitionssicherheit
bei realistischer Budgetplanung

Arbeitsplatz
- Desktops, Notebooks, Tablets, Thinclients nach Bedarf
- Wirtschaftl. Betrieb durch zentrales Management
- Sicherer Einsatz privater Geräte (BYOD)
- Anwendungsbereitstellung auf Knopfdruck

Storage
- Zentrale Datenhaltung und Datensicherung
- Hochverfügbarkeit
- Einfache Speicherzuteilung

Server
- Flexibilität bei der Ressourcenzuteilung
- Automatische Ausfallsicherheit

07121/2678 - 400
http://bit.ly/server2280

CALLEO Application Server 2280

intel inside XEON

Intel® Xeon® Prozessor

transtec

derungen der Verbindungen managen, und sie müssen wissen, was sie tun, wenn sie kurzfristig zusätzliche Verbindungen und Bandbreiten einrichten. Denn während der Lastspitze muss das Netz verlässlich funktionieren, andernfalls drohen Umsatz- und Imageverlust.

Diese Know-how-Anforderung gilt zumindest für eine Übergangszeit, denn in der Zukunft sollen die Anwendungen selbst über standardisierte Schnittstellen die Anforderungen an die Netzdienste verändern. Das MEF (Metro Ethernet Forum) arbeitet bereits an einem neuen API-Modell, das Lifecycle Service Orchestration (LSO) heißt und es unterschiedlichen Systemen erlauben soll, miteinander Informationen zu Bandbreitenbedarf und Verbindungswahl auszuhandeln.

Prozesse und Kommunikation

Wollen Unternehmen SDN nutzen und von den Vorteilen der kurzen Bereitstellungszeiten und geringeren Kosten profitieren, sind neue Prozesse erforderlich. Die IT-Abteilung und die Fachabteilungen, die IT-Unterstützung für bestimmte Projekte benötigen, müssen sich zur Kapazitätsplanung regelmäßig und eng abstimmen, um den Bandbreitenbedarf abzuschätzen. Im Hinblick darauf, dass für eine erfolgreiche Digitalisierung von Unternehmen ohnehin der Abschied vom Silodenken der Abteilungen gefordert wird, ist das eine gute Nachricht.

Eine möglichst exakte Vorhersage des Bandbreitenbedarfs hat auch Einfluss auf die Budgetplanung. Denn Bezahlung nach Verbrauch bedeutet auch Flexibilität in der Bereitstellung von Geldern. Und um im Budget zu bleiben, wird es wichtig sein, neben der Ad-hoc-Einrichtung von Verbindungen auch deren Terminierung nicht zu vergessen, wenn die Lastspitze vorbei ist.

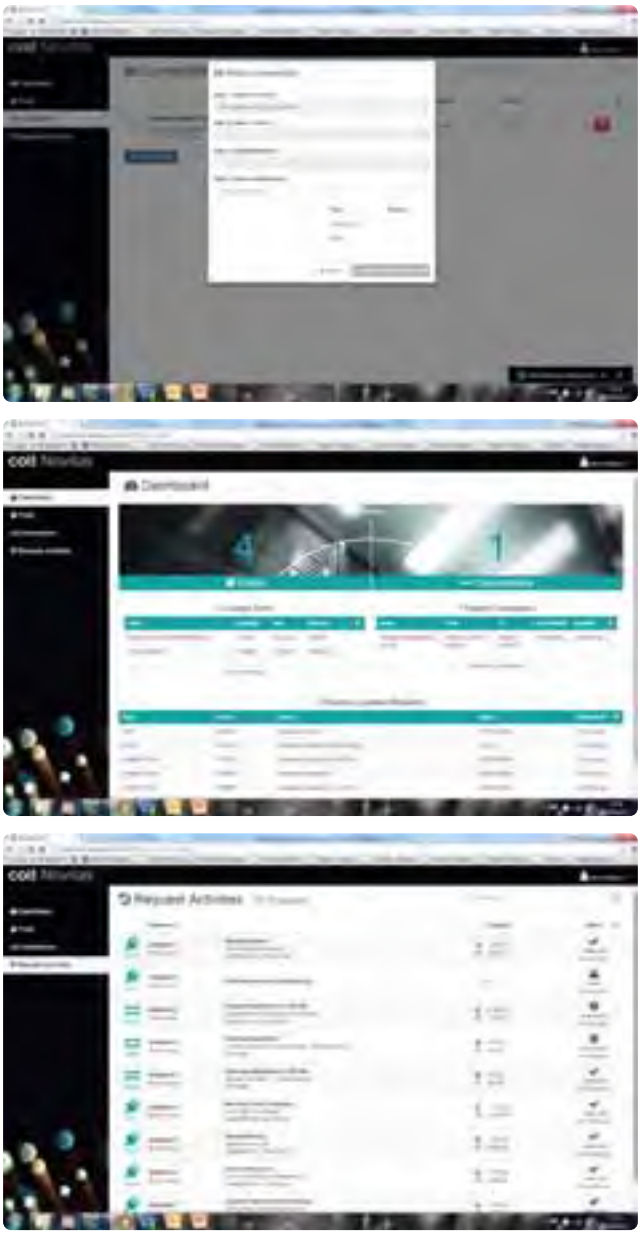
Ein verändertes Betriebsmodell beim Anwender erfordert im Gegenzug ein verändertes Servicemodell beim Anbieter. Wenn der Kunde seine Verbindungen künftig selbst einrichten kann und wenn dies langfristig sogar automatisiert wird, kommt der Beratung des Kunden eine noch wichtigere Rolle zu: Die Unternehmen brauchen Unterstützung beim Aufbau des internen Know-hows. Dabei wird auch der Datenschutzaspekt ein wichtiger Punkt sein. Die Anwenderunternehmen benötigen Unterstützung, um die Daten aus der Überwachung der Netzwerkaktivitäten zu interpretieren und die richtigen Rückschlüsse auf künftigen Bedarf zu ziehen. Servicemanagement und Technik des Netzwerkbetreibers müssen dafür sorgen, dass die Performance der kurzfristig angeforderten Leitungen stimmt und die Sicherheit der Verbindungen gewährleistet ist.

Es gilt für die Service Provider insgesamt, dass sie, um als Dienstleister attraktiv zu bleiben, ihren Kunden noch stärker als bislang einen Mehrwert bieten müssen, der über die Bereitstellung von Infrastruktur hinausgeht. Denn die Bezahlung nach Verbrauch erschwert nicht einfach nur die Umsatzplanung, sie beeinflusst das Geschäftsmodell. Die Festnetz-Carrier werden wahrscheinlich ähnliche Entwicklungen bei den Tarifmodellen erfahren wie die Mobilfunkbetreiber bei den Handytarifen. Daher wird es entscheidend sein, sich an den Bedarf der Kunden nach variabler Abrechnung anzupassen. So könnten in einer Übergangsphase etwa Modelle mit einer teilweise variablen Abrechnung oder auch Flat-Tarife mit einer bestimmten Anzahl von Änderungen und einer maximalen Durchschnittsbandbreite angeboten werden. Immer neue Tarifmodelle auf den Markt zu bringen, wird – wenn überhaupt – nur kurzfristig funktionieren, denn es verwirrt die Kunden.

Infrastruktur und Innovation

Das Netzwerk kann sich dem allgemeinen Trend zur bedarfsabhängigen Nutzung von Ressourcen und der damit verbundenen verbrauchsabhängigen Bezahlung nicht entziehen. Die Zeit langfristiger, hochdotierter Serviceverträge ist vorbei. Das Geschäft verändert sich. Das muss keine Hiobsbotschaft für Service Provider sein, denn der grundsätzliche Bedarf an Rechenzentrumskapazität und an Verbindungen mit hohen Bandbreiten wird weiter steigen. Für Netzwerkbetreiber gilt es, sich entsprechend aufzustellen. Mit einer Infrastruktur auf Basis einer zukunftsfähigen Technologie und mit innovativen Services. Doch es liegt nicht ganz allein in der Hand der Marktteilnehmer selbst. Denn sie brauchen darüber hinaus einen regulatorischen Rahmen, der einen fairen Wettbewerb ermöglicht. Nur so haben die Netzwerkbetreiber ein tragfähiges Geschäftsmodell und ihre Kunden die Möglichkeit, die Chancen der Digitalisierung zu nutzen.

Quelle: Colt



Auf dem Weg zum Next Generation Network: Über die Colt-Novitas-Plattform lassen sich Software-defined Networks im Selfservice-Verfahren aufbauen, konfigurieren und abrechnen.

Matthias Hain,
Director Product Management Ethernet Services, Colt

NetWork'16

FORUM für Service- und Infrastrukturmanagement in IT und Telekommunikation

www.network16.de

Jetzt anmelden!
26. + 27. April 2016 – Congress Center Leipzig

FNT
// when transparency matters.

Software für Data Center Infrastructure Management

Wir bringen Transparenz und Effizienz in Ihr Rechenzentrum.

Sie wollen Rechenzentren effizient betreiben. Kapazitäten, Aus- und Umbau verlässlich planen können. Sie benötigen Transparenz – vom Gebäude, der Energieversorgung über die IT-Systeme bis zu den Services und Prozessen. In Echtzeit, jedes Detail, integriert, auf Knopfdruck visualisiert.

Unsere DCIM-Softwarelösung bietet das – dank des einzigartigen, durchgängigen FNT Datenmodells.

Jetzt informieren: www.fntsoftware.com

Kompakt als konvergente Appliance

Agile Geschäftsmodelle brauchen frei skalierbare Datacenter

Die Fachbereiche geben sich mit einer IT-Grundversorgung nicht mehr zufrieden. Sie erwarten heute, dass die IT in der Lage ist, in kurzer Zeit und flexibel neue Geschäftsanforderungen umzusetzen. Dazu müssen die Rechenzentren auf Basis softwaredefinierter IT-Infrastrukturen grundlegend modernisiert werden.

Für den Anfang empfiehlt sich eine Bestandsaufnahme der bestehenden IT-Systemlandschaft, beispielsweise in Form eines Data Center Future Readiness Assessments. Darauf aufbauend sollten Unternehmen einen Soll-Zustand definieren, der letztlich Meilensteine auf dem Weg zu einem Software-defined Datacenter fixiert.

Von der Server-Virtualisierung zu SDS ...

Die weitverbreitete Server-Virtualisierung bildet ein ideales Fundament für den Einstieg in ein Software-defined Datacenter. Vor wenigen Jahren noch war die Virtualisierungstechnologie auf Server beschränkt. In der Zwischenzeit hat sie weitere IT-Infrastrukturkomponenten wie die Storage-Systeme erobert.

Ziel der Storage-Virtualisierung ist eine effizientere und flexiblere Speicherung, Sicherung und Wiederherstellung der Daten. Eine Lösung dafür bieten modulare, softwarebasierte Systeme. Deren Funktionen zum dynamischen Tiering platzieren die Daten automatisch – je nach Zugriffshäufigkeit – auf teuren flashbasierten Storage-Medien mit schnellen Zugriffszeiten oder auf kostengünstigeren Festplatten mit längeren Zugriffszeiten.

Darüber hinaus testet bereits eine Reihe von Unternehmen neue softwarebasierte Lösungen und konvergente Appliances. Diese kombinieren in einem Gehäuse Rechen- und Speicherkapazitäten, Netzwerkkomponenten und Virtualisierungssoftware. Konvergente Appliances zeichnen sich durch eine modulare Architektur aus und erlauben damit eine vertikale und horizontale Skalierung.

Einer der zentralen Vorteile konvergenter Appliances besteht darin, dass sich damit virtuelle Maschinen für unternehmenskritische Applikationen sehr effizient bereitstellen lassen. Typische Anwendungsszenarien sind Mail- und Messaging-Projekte auf Basis von Microsoft Exchange, Datenbankprojekte auf Basis von Microsoft SQL Server und Oracle, SAP-Applikationen, Desktop-Virtualisierung und Private Clouds. Viele der aktuell verfügbaren konvergenten Appliances nutzen Nutanix-Software, genauer: das Nutanix Distributed File System (NDFS). Es verbindet die Speicher- und Rechenressourcen mit dem Hypervisor zu einer vollständig integrierten Einheit und kann damit virtualisierte Workloads nahezu beliebiger Größe verarbeiten. Die IT-Administratoren verwalten dann keine Storage-Volumina oder RAID-Gruppen, sondern virtuelle Maschinen und nutzen dazu Regeln, die sich aus konkreten Anwendungsszenarien ergeben.

... und weiter ins SDN

Als Folge der weitgehenden Server-Virtualisierung hat sich auch das Umfeld für Networking geändert. Da zwischen den Servern immer größere Datenmengen transportiert werden, steigen auch die Anforderungen an die Bandbreite. Die proprietären, zentralistisch ausgerichteten Netzwerke sind dafür aber nicht ausgelegt.

Software-defined Networking entkoppelt den Datenfluss (Data Plane) von der Steuerlogik (Control Plane). Durch die Trennung von Switch-Hardware und Netzwerkbetriebssystem stehen die Verwaltungsfunktionalitäten explizit über Software bereit. Im Vergleich zu den bisherigen zentralistischen Architekturen erhält der Administrator so über die Control Plane einen besseren Einblick in das Geschehen im Netz und kann den Datenfluss effizienter steuern.

Software-defined Networking bietet Unternehmen die Vorteile einer höheren Flexibilität und weniger Aufwand bei der Verwaltung. Optimal aufeinander abgestimmt bilden virtualisierte Serverplattformen, Software-defined Storage und Software-defined Networking die zentralen Komponenten für zukunftsfähige Rechenzentren.

Peter Dümig,
Senior Server Product Manager Dell, Frankfurt

Quelle: Dell

Aus Sicht von Dell umfasst das Future Ready Enterprise, dessen Kern ein Software-defined Datacenter bildet, sowohl die Legacy IT als auch die neue IT.

Auslastung ist keine Effizienzklasse

Eine neue Normreihe legt die Grundlagen künftiger RZ-Zertifizierungen

Rechenzentren wurden bisher europaweit nicht nach einheitlichen Kriterien entwickelt und gebaut. Das soll sich mit der neuen Norm DIN EN 50600 ändern. Das erklärte Ziel ist mehr Energieeffizienz, doch gerade in diesem Punkt wäre noch sehr viel mehr möglich.

Wer in Zukunft in Deutschland ein Rechenzentrum baut, muss sich schon in der Planungsphase an sehr detaillierte Vorgaben halten. Bisher konnte man zwar diverse Zertifizierungen, etwa des eco-Verbandes oder des TÜV Süd, oder den Blauen Engel für Rechenzentren erwerben, einheitlich waren die Herangehensweisen jedoch nicht. Das soll sich nun ändern. Auf deutschen Antrag hin hat das TC (Technical Committee) 215 „Elektrotechnische Aspekte von Telekommunikationseinrichtungen“ der europäischen Freihandelsorganisation CENELEC die Europanorm-Serie DIN EN 50600 entwickelt. In Deutschland ist für das Thema die Arbeitsgruppe 715.2 „Informationstechnische Verkabelung von Gebäudekomplexen“ der DKE (Deutsche Kommission Elektrotechnik Elektronik Informationstechnik) im DIN und VDE zuständig.

Die Norm legt den Grundstein zu längerfristig stärker vereinheitlichten Netzknoten in der europaweiten IT-Infrastruktur. Längerfristig

deshalb, weil das Normwerk nicht für bereits bestehende Rechenzentren gilt. Da diese Einrichtungen durchaus Standzeiten haben, die gut im zweistelligen Bereich liegen, ist eher mit Jahrzehnten als mit Jahren zu rechnen, bis der Standardisierungseffekt eintritt. Andererseits entstehen gerade jetzt durch den Trend zu Cloud-Computing sehr viele neue Rechenzentren und ältere Anlagen werden neu eingerichtet. Wer heute neu baut oder gründlich renoviert, wird natürlich die Norm in seine Planungen einbeziehen, damit er später die von Kunden erwarteten Zertifizierungen vorweisen kann und diese nicht kostspielig nachholen muss.

Die wichtigste Neuerung: Die Standardserie DIN EN 50600 berücksichtigt als erste die Tatsache, dass Rechenzentren in vielen Bereichen zu wichtigen Komponenten unverzichtbarer Infrastrukturen werden. Dazu gehören das Finanz- und Gesundheitswesen, die Energieversorgung, die öffentliche Verwaltung und vieles mehr. Bisher blieb es der Sorgfalt der RZ-Betreiber überlassen, ob und wie viel Energie sie in eine Risikoanalyse im Vorfeld stecken, und die bestehenden Zertifizierungsmöglichkeiten machten Rechenzentren nur beschränkt vergleichbar. In Zukunft aber wird es eine einheitliche Bezugsbasis geben, nämlich die neue Europanorm.

Das amerikanische Pendant zur DIN EN 50600 ist TIA-942. Die Anwendung dieser Norm hierzulande ist allerdings schwierig, weil sie zum Beispiel in vielen Bereichen wenig detailliert ist und häufig auf weitere Normen verweist. Die DIN-Norm ist meist technisch detaillierter. TSI (Trusted Site Infrastructure), das Zertifizierungsprogramm des TÜV Süd, umfasst bereits viele, insbesondere technische Elemente von DIN EN 50600. Aber es gibt auch Gemeinsamkeiten mit der US-Richtlinie: So weisen die US- wie die EN-Norm vier Verfügbarkeitsklassen aus, die in etwa den aus den USA bekannten Tier-Klassifikationen 1 bis 4 entsprechen. Hinzu kommen vier Schutzklassen und noch zwei Flächenklassen, die Rechenzentren nach ihrer Größe differenzieren.

DIN EN 50600: Klassifikationen und Gliederung

Die Schutzklassen befassen sich mit den Sicherheitsmaßnahmen gegen nicht autorisierten Zugang, dem Schutz gegen Brände im RZ, gegen interne umgebungsbedingte und externe umgebungsbedingte Ereignisse. In den Schutzklassen 2, 3 und 4 sind gegen interne und externe Ereignisse gezielte Vorkehrungen gefordert, ohne dass Details genannt werden. Die Schutzmaßnahmen gegen interne Brände steigen von Stufe zu Stufe. In Schutzklasse 4 muss zum Beispiel sichergestellt sein, dass die Rechenzentrumsaufgaben auch während eines Brandes weiter erfüllt werden können. Das Schutzniveau muss allerdings nicht für alle Bereiche des RZ gleich sein. Es kann ausreichen, den Eingangsbereich der Schutzklasse 1, die USV der Schutzklasse 2 und die Rechner der höchsten Schutzklasse 4 zuzuordnen – Schutzklasse 4 für den Empfangstresen wäre wohl zu viel des Guten. Die Norm insgesamt gliedert sich in drei Teile: 1. Risiko- und Anforderungsanalyse, 2. auszuführende technische Infrastruktur sowie 3. Management und Betrieb. Das Ganze umfasst insgesamt sieben Abschnitte. Dem eigentlichen Bauprozess vorgeschaltet sind, beschrieben in Teil 1, die „allgemeinen Konzepte“.

Quelle: Ackermann/dc-ce

Beispiel für die Schutzklassen, die verschiedenen Infrastrukturelementen zugeordnet werden.

Was wie zu schützen ist, ergibt sich aus Teil 1, der unter anderem eine umfassende Geschäfts- und Risikoanalyse einschließlich der Betriebskosten fordert. Das Bemerkenswerte daran ist, dass nun nicht mehr nur zu berücksichtigen ist, welchen Risiken das Rechenzentrum als technische Struktur ausgesetzt ist – etwa durch Sabotage, Überflutungen, Stromausfälle etc. Vielmehr geraten nun auch die geschäftlichen Risiken und die Betriebskosten in den Blick: Die Standzeitenanalyse beschäftigt sich mit Kosten von ungeplanten Ausfällen und Wartungsfenstern, in denen das RZ nicht zur Verfügung steht.

In Zukunft dürfte also schon hier beachtet werden, was der Ausfall des Rechenzentrums oder einiger seiner Komponenten für das Kerngeschäft des RZ-Betreibers bedeutet. Können keine Operationen mehr durchgeführt werden, wenn das RZ im Krankenhaus ausfällt? Ist es nicht mehr möglich, fällige Zahlungen zu begleichen, sobald das IT-System der Bank steht? Welche Fertigungsanlagen sind auf das Funktionieren des Rechenzentrums eines produzierenden Unternehmens direkt angewiesen? Wie lange darf ein Ausfall dauern, bis alles steht, und was bedeutet ein längerer Ausfall – finanziell oder beispielsweise im Hinblick auf die lokale oder nationale Sicherheit? – Je nachdem, wie die Risikoanalyse ausfällt, ergibt sich, welcher Schutz- und Verfügbarkeitsklasse entsprechend das Rechenzentrum baulich und technisch geplant wird.

Der funktionale Rahmen lässt Spielraum

Die Risikoabwägungen sind aber nicht alles im ersten Teil. Dort werden auch die gemeinsamen Aspekte aller Rechenzentren beschrieben, terminologische Festlegungen getroffen, Parameter definiert und Referenzmodelle dargestellt, die übergreifend beschreiben, wo die einzelnen funktionalen Elemente von Rechenzentren unterzubringen sind – dies alles unter Berücksichtigung des späteren Verwendungszwecks. Außerdem beschreibt Teil 1 alle Infrastrukturen, die man braucht, um das RZ später ans Telekommunikationsnetz und ans Internet anzubinden. Auch die Klassifikation nach Verfügbarkeit, Betriebssicherung und Energieeffizienz wird bereits hier festgelegt. Schließlich stellt der erste Teil noch dar, wie Rechenzentren im Allgemeinen auszulegen sind, wie man die einzelnen Bereiche kennzeichnet oder etikettiert, wie Pläne zu codieren sind, welche Formen der Qualitätssicherung vorgeschrieben sind und welche Ausbildung RZ-Mitarbeiter brauchen.

Fertig formuliert sind inzwischen neben dem allgemeinen ersten Teil vier Teile: Gebäudekonstruktion (Teil 2-1), Stromversorgung (Teil 2-2), die Regelung der Umgebungsbedingungen (Teil 2-3) sowie die Infrastruktur der Telekommunikationsverkabelung (Teil 2-4).

Teil 2-1 bringt die Grundlagen der Gebäudekonstruktion von Rechenzentren und alle sie betreffenden Aspekte. Allerdings gibt es keine genauen Bestimmungen dazu, wie diese Grundlagen umzusetzen sind.

Zu den behandelten Aspekten gehören auch die Auswahl eines geeigneten Standorts und dessen Konfiguration.

Im Teil 2-2 geht es um die Stromversorgung und -verteilung. Die Norm beschreibt, wie sie anforderungsgerecht zu dimensionieren sind, welche Verfügbarkeitsklassen jeweils geeignet sind, außerdem geht es um die physische Sicherheit. Hier kommt auch die Energieeffizienz ins Spiel: Die Norm legt drei Granularitätsniveaus fest, auf denen gemessen wird: das gesamte Rechenzentrum, bestimmte Einrichtungen und Infrastrukturen des Rechenzentrums oder einzelne Elemente, etwa ein Server.

Teil 2-3 befasst sich mit den Umgebungsbedingungen im Rechenzentrum und hinsichtlich der Infrastruktur; dabei macht er jeweils spezifische Vorgaben für die definierten Schutz-, Verfügbarkeits- und Energieeffizienzklassen. Es finden sich Festlegungen und Empfehlungen zur Temperatursteuerung, zur Handhabung von Flüssigkeitsströmen, zur Behandlung von Luftverunreinigungen (Schwebeteilchen) und zum Umgang mit mechanischen Schwingungen. Des Weiteren liefert dieser Teil prototypische Etagengrundrisse und Standortvorgaben, nennt geeignete Verfahren zur Energieeinsparung und gibt weitere Details zur physischen Sicherheit der Systeme mit Bezug zu den Umgebungsbedingungen vor.

Teil 2-4 widmet sich umfassend der Verkabelung im Rechenzentrum selbst: von den Netzwerk- und Storage-Leitungen über Überwachung, Regelung und Gebäudeautomation bis hin zu Schaltschränken und Kabelwegen.

Noch in der Entwurfsphase befinden sich zwei weitere Teile: die Sicherungssysteme (Teil 2-5), die Zutrittskontrolle, Brandschutz und andere Umgebungsgefährdungen betreffen, sowie die Informationen für das Management und den Betrieb (Teil 2-6).

Keine Effizienzvorgaben für die Systemauslastung

Derzeit beginnt in der RZ-Branche eine Diskussion darüber, dass PUE (Power Usage Effectiveness) und ähnliche Normen die reale Effizienz der Rechenzentren zu günstig darstellen, weil sie die Auslastung des IT-Equipments nicht berücksichtigen: Ein Datacenter kann durchaus einen niedrigen PUE-Wert haben, aber trotzdem ineffizient sein, weil man die gleiche Rechenleistung auch mit sehr viel weniger Hardware erbringen könnte. Angesichts realer Auslastungsgrade, die – so übereinstimmend eine ganze Reihe von Fachleuten – selten 30 % übersteigen dürften, stellt sich schon die Frage, ob hier nicht der Effizienzerhöhung auf die Beine geholfen werden könnte, zum Beispiel durch die Vorgabe von durchschnittlichen Mindestauslastungen der Infrastruktur.

Der abschließende Teil der Norm, in dem es um den Betrieb des Rechenzentrums geht – die Stichworte sind Ausfallsicherheit, Verfügbarkeit, Sicherheit und Energieeffizienz –, wäre für solche Vorgaben ein geeigneter Ort. In höheren Auslastungen jeder einzelnen Infrastrukturkomponente sehen nämlich viele weitaus größere Sparpotenziale als bei der zweiten Nachkommastelle des PUE.

Ariane Rüdiger,
freie Autorin, München

Hinter dem Netzknoten beginnt die Tiefsee

Globale Datendrehscheiben müssen sich auf stabile Fernkabel verlassen können

Für Rechenzentren entscheidend ist ihre Fähigkeit zur Kommunikation, sowohl innerhalb der Betonwände als auch mit externen Datenquellen und -abnehmern. Wie gut das klappt, hängt an der Backbone-Vernetzung, über Land und unter Wasser. Diese Nervenstränge der virtuellen Welt sind sehr empfindlich.

Ließen die ersten Kupfer-Unterseekabel im 19. Jahrhundert nur eine einzige telegrafische Verbindung gleichzeitig zu, bündeln moderne Glasfaserkabel innerhalb eines einzigen Kabelsystems mehrere Glasfasern, auf denen wiederum teilweise mehr als hundert unterschiedliche Lichtwellenlängen übertragen werden. Jede einzelne davon erreicht Übertragungsgeschwindigkeiten von bis zu 40 GBit/s, im Labor sogar schon bis zu 400 GBit/s. Das aktuell kapazitätsstärkste Seekabelsystem TGN-Pacific zwischen Japan und Kalifornien, betrieben von Tata Communications, hat eine maximal mögliche Kapazität von 20 TBit/s.

Doch auch die Datentransporte benötigen, bevor sie das Kabel durch den Atlantik erreichen, Umschlagplätze, ähnlich wie große Häfen oder Airports. Bei digitalen Waren übernehmen Rechenzentren diese Aufgabe. Dort enden sowohl die Glasfaserstrecken der regionalen Netze als auch der großen Überseekabel, dort werden sie über die Infrastruktur der Netzbetreiber zusammengeschaltet und weitergeleitet.

Da alle Betreiber von Kabelsystemen daran interessiert sind, an den jeweiligen Endpunkten ihrer Strecken so viele andere Betreiber wie irgend möglich zu konnektieren, haben sich über die Zeit diese Lokationen in den großen Geschäftszentren dieser Welt herausgebildet, an denen eine Vielzahl dieser Kabelsysteme endet. Ein gutes Beispiel hierfür sind die Hauptstandorte des größten Internet-Austauschknotens der Welt, des DE-CIX in Frankfurt, mit einer übertragenen Bandbreite von inzwischen über 4 TBit/s. An einem seiner Standorte, in der Kleyerstraße im Frankfurter Gallusviertel, treffen sich über 400 unterschiedliche Netzwerkbetreiber, um miteinander Daten auszutauschen.

Quelle: Equinix

Zum Kerngeschäft von Colocation-Providern gehören eine starke, stabile Anbindung über See- und Landkabelstrecken sowie die Verfügbarkeit der Rechenzentren selbst.

Die größte Gefahr liegt unter Wasser

Die Nähe zu einer Vielzahl von unterschiedlichen Datenrouten ist insbesondere für die Unternehmen interessant, für die Millisekunden bares Geld bedeuten, so beim Hochfrequenzhandel mit Wertpapieren. Diese Händler nutzen etwa in Frankfurt teilweise eine Richtfunkverbindung mit dem Börsen-Exchange in London, die mit circa 6 ms RTD (Round Trip Delay) als schnellste verfügbare Verbindung zwischen den beiden Städten jede Glasfaserstrecke in den Schatten stellt.

Während Landkabel – teilweise aufwendigen Tiefbauarbeiten zum Trotz – relativ einfach zu verlegen und zu sichern sind, sind Seekabelstrecken etlichen Unwägbarkeiten mehr ausgesetzt. Ereignisse wie das Erdbeben in der Straße von Taiwan 2006 oder die mehrfache Unterbrechung der Verbindungen zwischen Europa und Asien 2012 – die Risse des SEA-ME-WE-Kabels verursachten vermutlich Schiffsanker vor der Küste Ägyptens – zeigen dies. Das Erdbeben von Taiwan unterbrach innerhalb weniger Stunden mehr als zehn wichtige Kabelsysteme und brachte den Kommunikationsverkehr zwischen Europa und Asien nahezu zum Erliegen.

Ein eminent wichtiger Aspekt bei der Planung und Realisierung internationaler Seekabel ist daher die ausfallsichere Auslegung. So werden die meisten Kabelsysteme so redundant wie möglich geplant, mit mindestens zwei unterschiedlichen Wegen durch die Ozeane, getrennten Übergabepunkten von See zu Land und natürlich auch separaten Verbindungen zu unterschiedlichen Rechenzentren im Binnenbereich. So verteilt der Seeweg des TGN-Pacific mit seiner Kapazität von insgesamt mehr als 20 TBit/s seinen Traffic aus Sicherheitsgründen auf zwei getrennte Kabelwege.

Im Gebirge ist Ankern verboten

Wenn es von Land ins Wasser geht, wird es gleich richtig gefährlich. Denn dieser Übergang an den sogenannten Landing Stations führt die Kabel oft zunächst in einen flachen Küstenbereich beziehungsweise über den Festlandssockel. Die dabei erreichten Tiefen liegen zwischen 0 und 200 m – eine Region, in die auch Schiffsanker reichen.

Um hier dennoch für möglichst große Sicherheit zu sorgen, sind Seekabel gerade im Küstenbereich äußerst robust ausgeführt: Um den eigentlichen Kern mit den Glasfasern liegen mehrere Isolationsschichten aus Gummi sowie meist noch eine stromführende Schicht beziehungsweise Kupferkabel zur Energieübertragung für eventuelle Verstärker auf der Kabelstrecke. Als Mantel soll eine besonders verstärkte Stahlarmierung physikalische Schäden verhindern. Ein entsprechend belasteter Schiffsanker kann jedoch auch diesen Schutz zerstören.

Geht es tiefer hinab, ist der Kabelverlauf dann zwar vor Schäden durch Anker und, ab einer gewissen Tiefe, auch vor Treibnetzen geschützt. Dafür bereitet aber die Topografie Schwierigkeiten bei der Routenführung. Wenn man sich deutlich macht, dass der maximale Höhenunterschied von der Wasseroberfläche bis zum Meeresgrund etwa im Pazifik bei mehr als 11.000 m liegt und man mit einem Kabel dem Weg ganzer unterseeischer Gebirgszüge folgen muss, wird klar, welche Schwierigkeiten zu meistern sind, um es auf einer stabilen und vor allem vor Erdbeben möglichst sicheren Route zu verlegen.

Oft kollidieren hier auch die Anforderungen. Die Verlegung muss einerseits aus wirtschaftlichen Gründen möglichst direkte und damit kostengünstige, schnelle Routen schaffen, sie muss andererseits dennoch sicher sein. Zudem ist es durch die geografischen und auch politischen Gegebenheiten in den betroffenen Gebieten nicht immer einfach, alternative Kabelwege zu finden. Es ist jedoch gerade die Verfügbarkeit von Alternativen und Ausweichrouten, welche die internationalen Kommunikationsverbindungen sicher macht.

Sicherheit im Rechenzentrum vor Ort

Geht es bei der Absicherung von See- und Landkabelstrecken eher um das große Ganze, müssen sich Rechenzentrumsbetreiber auch um Details sorgen. Denn ein RZ, in dem eine Vielzahl von Kabelstrecken zusammenläuft, ist ein weiterer neuralgischer Punkt der Infrastruktur, der entsprechende Sicherheitsmaßnahmen benötigt.

Neben der physikalischen Sicherung durch Zutrittskontrollen, Sicherheitsdienste, Videoüberwachung und weitere Maßnahmen ist es vor allem die Sicherung der Verfügbarkeit der Infrastruktur, die besonders im Fokus steht. Ein Rechenzentrumsbetreiber wird alles tun, damit die wichtigste Ressource, der elektrische Strom, jederzeit zur Verfügung steht. Hier kommen unterbrechungsfreie Stromversorgungen zum Einsatz, die oft die Größenordnungen kleiner Kraftwerke erreichen.

Mit der weiteren Digitalisierung der Wirtschaft und der unverminderten Zunahme von Kommunikation über Video und mit neuen Trends wie dem Internet der Dinge, die alle einen noch stärkeren, schnelleren und effizienteren Austausch von Daten erfordern, steht nicht nur der Ausbau der internationalen Seekabelrouten, sondern vor allem auch der Ausbau der Datenaustauschpunkte auf dem Programm. Vielleicht wird in Zukunft der Stromverbrauch von Rechenzentren den von Flughäfen überflügeln.

Klaas Mertens,
Global Solutions Architect, Equinix

Datensicherheit durch Hyperkonvergenz

Ein Data Center in a Box löst die Backup-Probleme virtualisierter Rechenwelten

In den meisten Rechenzentren beißt sich die Virtualisierung mit der Datensicherheit, weil die klassische Eins-zu-eins-Replikation nicht mehr praktikabel ist. Hyperkonvergente Systeme mit Inline-Deduplizierung können die Wiederherstellung im Katastrophenfall enorm vereinfachen.

Im Rechenzentrum eines Unternehmens potenzieren sich die Probleme, die unweigerlich in jeder professionellen IT-Umgebung auftreten, wenn sie mit wachsendem Datenaufkommen konfrontiert wird. Im Rechenzentrum ist ein heterogener Mix von Systemen und Prozessen der Normalfall. Mit zunehmenden Datenmengen und Verarbeitungsanforderungen stellt dieser IT-Mix sehr schnell extrem hohe Anforderungen an die IT-Mitarbeiter. Manchmal sind sie sogar nur durch die kostenintensive Einbindung externer Dienstleister für Verwaltungs- und Wartungsarbeiten zu bewältigen oder führen gar dazu, dass die IT-Umgebung unübersichtlich und schwer kontrollierbar wird. Dies sind natürlich sehr ungünstige Voraussetzungen für Unternehmen, die darauf angewiesen sind, dass ihre Server schnell, flexibel und skalierbar zur Verfügung stehen. Lange Wartezeiten bei der Bereitstellung angeforderter Daten sind hier nicht akzeptabel.

Virtualisierung, Konvergenz und Hyperkonvergenz

Abhilfe für das Problem der Kapazitätsengpässe und der unzureichenden Bandbreite im Netzwerk sollen virtuelle Maschinen schaffen, die eine flexiblere Zuordnung der Serverkapazitäten zu den jeweiligen Workloads ermöglichen. Gleichzeitig verändert die Virtualisierung jedoch traditionelle Strukturen und Zuordnungen in der IT-Umgebung von Grund auf. Was bedeutet dies konkret für die Datensicherheit? Sogenannte konvergente IT-Umgebungen waren ein erster Lösungsversuch. Hierbei werden die über das gesamte Rechenzentrum und möglicherweise auch über verschiedene Standorte verteilten Einzelkomponenten so zusammengefasst, dass der Systemadministrator sie in einer einzigen Ansicht überschauen und verwalten kann. Dies schafft eine gewisse Übersichtlichkeit im Rechenzentrum, löst aber noch nicht das Problem, dass weiterhin separate Hardwarekomponenten gepflegt werden müssen – von Mitarbeitern mit den entsprechenden Zuständigkeiten.

Das noch relativ junge Konzept der Hyperkonvergenz ist die logische Weiterführung dieses Ansatzes: Man nehme die klassischen Kernkomponenten eines Rechenzentrums – Server, Speicher, Netzwerk, Hypervisor und Backup-Systeme – und konsolidiere diese in einer einzigen Plattform. Das Ergebnis ist eine hochintegrierte Appliance, ein „Data Center in a Box“. Hyperkonvergenz bietet die Vorteile der Cloud-Technologie, da sich Server einfach als Bausteine nach Bedarf hinzufügen lassen und damit das Problem der Unter- oder Überdimensionierung lösen, mit dem traditionelle IT-Strukturen zu kämpfen haben.

Bereits die Virtualisierung der IT-Umgebung erforderte ein grundlegendes Umdenken in der Backup-Strategie. Virtuelle Maschinen brauchen dedizierte Speichernetze, die sogenannten LUNs (Logical Unit Numbers), in denen die VMs abgelegt sind. Eine LUN definiert einen logischen Teil oder einen kompletten Plattenspeicher in einem SAN. Und hierin liegt auch die eigentliche Problematik der Backup-Verfahren. Vor der Virtualisierung erfolgte die Datensicherung auf Festplatte und/oder Bandspeicher mithilfe einer Backup-Software. Hierfür war ein Ansatz mit Array-basierten Snapshots und Replikation sinnvoll. Es bestand eine Eins-zu-eins-Zuordnung der auf einem physischen Server residierenden Anwendung zu einer zugewiesenen LUN (bei Speicherung auf Blockebene) oder einem Netzlaufwerk (bei Speicherung auf Dateiebene). In einer virtualisierten IT-Umgebung ist die gewohnte Datensicherheitsstrategie problematisch geworden.

Die traditionelle Eins-zu-eins-Zuordnung zwischen Anwendungen und Speichern wird durch eine Viele-zu-eins-Beziehung ersetzt: Ein Datenspeicher auf einer LUN enthält die Daten mehrerer virtueller Maschinen. Die Richtlinien der LUN gelten für alle VM, die den Datenspeicher nutzen. Über Snapshots kann nicht mehr definiert werden, welche Backup-Häufigkeit, Aufbewahrungszeit und welcher Speicherort für eine bestimmte VM gelten soll. Für Backup-Zwecke können nun die APIs des Hypervisors genutzt werden, um die VM als Image unabhängig vom LAN zu sichern. Während dies zur Beseitigung von Ineffizienzen und Ressourcenkonflikten beiträgt, entstehen wieder Komplexitäten anderer Art – und ein relativ hoher Aufwand, z.B. für Deduplizierungsfunktionen. In jedem Fall bleibt die Sicherheit der Daten, auch im Fall von Störungen oder katastrophalen Ereignissen (Disaster Recovery), eine lebenswichtige Aufgabe für jedes Unternehmen. Die nötigen Umstellungen bei der Backup-Strategie, die sich aus der Virtualisierung – bei all ihren sonstigen Vorteilen – ergeben, haben in der Praxis viele Unternehmen bisher davon abgehalten, beispielsweise große Oracle-Datenbanken auf virtualisierte oder Cloud-Umgebungen umzustellen. Dabei lässt sich dieser Innovationsbremse im Rechenzentrum durch Hyperkonvergenz-Technologie wirksam begegnen.

Datensicherheit durch Hyperkonvergenz

Eine hyperkonvergente Infrastruktur hat etliche bekannte Vorteile – zentrale Administrierung und Überwachung aller Systemkomponenten der Appliance, optimales Zusammenspiel aller Bestandteile und einfache Fehlersuche –, aber oft wird übersehen, dass Hyperkonvergenz gerade im Bereich der Datensicherheit die Schlüssellösung sein kann.

Moderne hyperkonvergente Infrastrukturen können auf x86-Standardservern laufen.

Quelle: Simplivity

Dies ist besonders dann der Fall, wenn die Datensicherheit kein Zusatzfeature der Hyperkonvergenz ist, sondern von Anfang an fester Bestandteil. Optimal ist es, wenn die Datensicherheit anhand von Richtlinien für Backup-Häufigkeit, Aufbewahrungszeiten, Speicherorte und Anwendungskonsistenz automatisiert wird. Die Datenübertragung zwischen Haupt- und Backup-Standorten muss optimiert erfolgen und zentral verwaltet werden können, und zwar auch für die Daten von Außenstellen und Niederlassungen, da dort oft kein geeignetes IT-Personal verfügbar ist. Ideal ist es auch, wenn die hyperkonvergente Lösung unabhängig von den Hypervisor-Ressourcen arbeitet. Dies löst die Probleme, die in der Vergangenheit aufgetreten sind (z.B. mit vSphere-Snapshots), und beseitigt Abhängigkeiten von bestimmten Hypervisoren oder APIs (mit dem entsprechenden Aufwand bei Änderungen).

Kompakte Disaster Recovery

Eine Datensicherungsstrategie ohne Disaster Recovery ist undenkbar – schließlich müssen die Daten für das Tagesgeschäft unter allen Umständen verfügbar bleiben, auch bei Ausfällen eines Servers oder Datenträgers. Hier bringt bereits die Virtualisierung der IT-Umgebung wichtige Verbesserungen, da man eine virtuelle Maschine in Form einer einzigen Datei flexibel verschieben kann. Außerdem ist keine Spiegelung des physischen Systems erforderlich, und die Überprüfung der wiederhergestellten Anlagen ist wesentlich einfacher.

Eine durchdachte Hyperkonvergenzlösung kann noch einen Schritt weitergehen: Durch Bereitstellung der hyperkonvergenten Infrastruktur an zwei verschiedenen Standorten, wobei eine Infrastrukturinstanz das Disaster-Recovery-Ziel der jeweils anderen darstellt, wird die Wiederherstellung enorm vereinfacht. Dass die Daten – einschließlich der Sicherungskopien – von Anfang an und während ihrer gesamten Nutzungsdauer in einem deduplizierten, komprimiert und optimiert gespeichert werden, erleichtert ihre Übertragung an den jeweils anderen Standort.

Falls kein zweiter Standort für die Disaster-Recovery-Kopien zur Verfügung steht, ist die öffentliche Cloud eine praktikable Lösung – und auch eine besonders wirtschaftliche, da nur die letzte komplette Kopie für die Wiederherstellung benötigt wird und Speicherservices in einer Public Cloud nutzungsabhängig berechnet werden, d.h. auf Basis der benötigten Kapazität. Durch geeignete Integration der Hyperkonvergenzlösung mit einer öffentlichen Cloud wie Amazon Web Services lassen sich Vorgaben definieren, wie die sichere Verlagerung der Daten in den Cloud-Speicher und wieder aus ihm heraus geschehen soll.

Deduplizierung von Grund auf

Deduplizierung reduziert den Bandbreiten- und Speicherplatzbedarf, indem sie doppelte Daten beseitigt, lediglich eine einzige Instanz auf Speichermedien beibehält und durch einen Zeiger dann auf diese Instanz verweist. Eine Inline-Deduplizierung nimmt im Vergleich zu einer Post-Process-Deduplizierung wesentlich weniger Ressourcen in Anspruch und sorgt dafür, dass mehr Verarbeitungsleistung für die Anwendungen zur Verfügung steht. Im Idealfall beschleunigt ein Accelerator die Echtzeitdeduplizierung zusätzlich. Die Deduplizierung löst quasi nebenbei auch ein noch größeres Problem in modernen Rechenzentren. Mit der Virtualisierung der IT-Umgebungen haben sich nämlich die IOPS-Anforderungen (Input/Output Operations Per Second) verzehnfacht. Herkömmliche Plattenspeicher gelangen hier schnell an ihre Grenzen. Eine mögliche Lösung sind Flash-Speicher, die allerdings wegen ihrer hohen Kosten nicht für alle Abschnitte im Lebenszyklus der Daten eine wirtschaftliche Lösung darstellen. Hier kann die direkt bei der Erstellung der Daten durchgeführte und dann dauerhaft gültige Deduplizierung, Komprimierung und Optimierung der Daten IOPS sparen und die Leistung verbessern.

Einsatz auf Standardservern

Für hyperkonvergente Infrastrukturen ist keine spezielle Hardware nötig. Die Technologie lässt sich mit x86-Standardservern betreiben. Die Intelligenz, die sich dahinter verbirgt, steckt in der Software, die auf der Appliance läuft. In Verbindung mit den Vorteilen für die Datensicherheit ist daher zu erwarten, dass umfassende Hyperkonvergenz – also Lösungen, die auch Sicherheitsfragen beantworten können – in vielen Rechenzentren nicht mehr nur eine Option bleibt, sondern zum State of the Art wird.

Wolfgang Huber,
Regional Sales Director Central Europe, Simplivity

40 GBit/s auf dem Sprung zu 100 GBit/s

2016 kommen neue Verkabelungsnormen für Rechenzentren heraus

Im März verabschiedet IEEE 802.3bq den Standard für 25/40GBase-T. Etwa zeitgleich werden auch ISO/IEC 11801 und EIA/TIA PN-568-C.2-1 die Verkabelungsstandards für 25 und 40 GBit/s über Kupfer veröffentlichen. Eine erste Machbarkeitsstudie zu 100GBase-T zeigt, dass auch diese Datenraten via Kupfer übertragbar sind.

Vor allem Cloud Computing und das Arbeiten mit mächtigen Unternehmensanwendungen per Virtual Machines erfordert schnelle Netze und insbesondere in Rechenzentren Highspeed-Anbindungen für die Server. Noch reichen 10 GBit/s aus; danach könnte man auf Glasfaser umstellen. Doch für 40-Gigabit-Ethernet nach IEEE 802.3ba sind acht Multimode-Fasern notwendig, allerdings über hundert und mehr Meter. Die Projektgruppe PT 40G, die seit 2012 für ISO/IEC 11801 und in Kooperation mit IEEE 802.3 die Kriterien für eine 40GBase-T-Verkabelung erarbeitet hat, schätzte einen Port-Preis von unter 400 Euro für 40GBase-T. Eine entsprechende Glasfaserverbindung mit Multimodefasern käme demnach grob geschätzt auf das Doppelte. Selbst bei Übertragungen im HF-Bereich scheint Kupfer demnach immer noch die preisgünstigere Technik zu sein.

Für die Übertragung von 25/40GBase-T setzte das Gremium eine maximale Verbindungslänge von 30 m fest. In den meisten Rechenzentren wird das ausreichen. IEEE 802.3bq nutzt dabei die Modulationsalgorithmen von 10-Gigabit-Ethernet. Auch die entscheidenden Übertragungsparameter sind gleich geblieben: Einfügedämpfung (Insertion Loss), Rückflussdämpfung (Return Loss), Nebensprechen zwischen den Adernpaaren am nahen (NEXT) und am entfernten Ende (FEXT) sowie das Übersprechen von benachbarten Leitungen (Alien Crosstalk). Um 40 GBit/s zu erreichen, übertragen die Netzwerkkarten dann jeweils 10 GBit/s über ein Adernpaar.

Quelle: Leoni Kerpen

Anschlusskomponenten für 40GBase-T der Kategorie 8.2 sind schnell verfügbar, da kaum Kompensationsaufwand notwendig ist.

25 GBit/s kam 2014 in die Diskussion, nachdem das 25G-Ethernet-Konsortium um Cisco und Google eine Technik präsentieren konnte, mit der die gesamte Datenrate parallel über alle Adernpaare gesendet wird, analog zu 10-Gigabit-Ethernet. PHY-Schnittstellen für 25GBase-T benötigen weniger Leistung als solche zur Parallelübertragung von 4×10-Gigabit-Ethernet. Für 25-GBit/s-Übertragungen gibt es bereits aktive Komponenten, unter anderem von Cisco und Broadcom. Broadcom hat außerdem letzten Sommer mit der NetXtreme-C-Serie Controller-Chips für 25/40/50-GBit/s-Ethernet vorgestellt. Darin ist auch die Zukunftsstrategie des 25G-Ethernet-Konsortiums erkennbar: Im nächsten Schritt sollen jeweils 25 GBit/s über zwei Adernpaare laufen, um auf 50 GBit/s zu kommen.

Die Verkabelungsnormen

Zu 25/40GBase-T bringt ISO/IEC 11801 im Frühjahr zwei Verkabelungsvarianten als Standard heraus, die beide auf einem 30 m langen Channel ohne die Anschlussstecker basieren: Kategorie-8.1-Komponenten für einen Klasse-I-Channel sowie Kategorie-8.2-Komponenten für einen Klasse-II-Channel.

Die amerikanische EIA/TIA Category 8 unterscheidet sich nicht wesentlich von Kategorie 8.1, Klasse I. Dieser regionale Standard basiert auf foliengeschirmten F/UTP-Komponenten der amerikanischen Cat.6_A. Bisher ist noch keine Anschlusstechnik nach EIA/TIA Category 8 verfügbar.

Kategorie 8.1, Klasse I

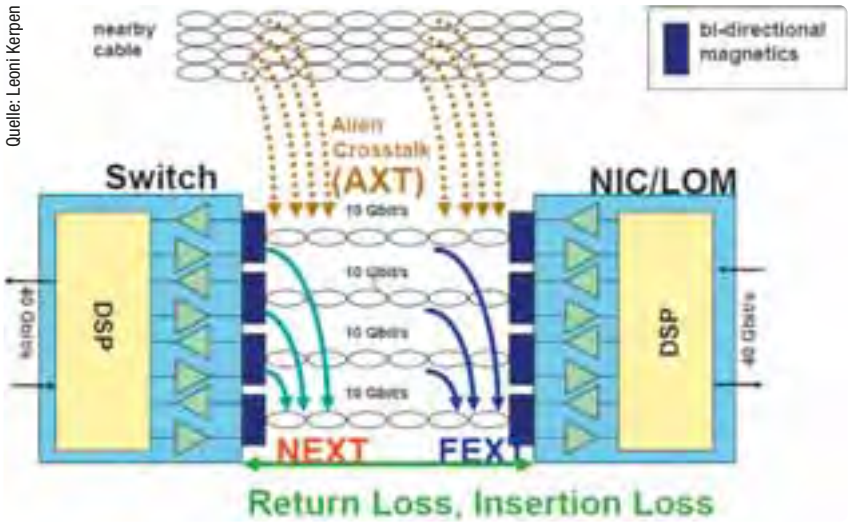
Bei der Festlegung der Kriterien für die Verkabelung ging die zuständige Projektgruppe PT 40G bei ISO/IEC JTC1 SC25 WG3 für Kategorie-8.1-Komponenten von optimierten Kategorie-6_A-Komponenten (500 MHz) aus, deren Übertragungseigenschaften für Frequenzen bis 1,6/2 GHz interpoliert wurden. Die Komponenten sind rückwärtskompatibel zu Kategorie 6_A.

Kategorie-8.1-Stecker/Module nach IEC 60603-7-81/82 sind derzeit noch nicht verfügbar, werden aber im Wesentlichen Cat.6_A-Komponenten sein, deren Kompensation für Frequenzen bis 2 GHz optimiert ist. Kabel für bis zu 2 GHz sind mit den in Deutschland häufig verlegten PiMF-Kabeln (Paare in Metallfolie) kein großes Problem und verfügbar. Die zugehörige Komponentennorm ist IEC 61156-9.

Kategorie 8.2, Klasse II

Verkabelungen nach Kategorie 8.2, Klasse II, basieren auf Kategorie-7_A-Komponenten und sind hierzu rückwärtskompatibel. Somit findet man in den neuen Normen IEC 61076-3-110/104 die Buchsen und Steckgesichter Tera, GG45 und ARJ. Diese müssen allerdings für Übertragungsraten bis 2 GHz ausgelegt sein. Bereits heute geben viele Hersteller an, dass ihre Kategorie-7_A-Komponenten deutlich höhere Frequenzen als die geforderten 1 GHz unterstützen. Hier ist der Kompensationsaufwand für NEXT und FEXT um etwa 20 dB geringer als bei Kategorie 8.1. So werde es laut Yvan Engels von Leoni Kerpen, Projektleiter der Arbeitsgruppe PT 40G in der WG3, schnell Anschlusstechnik für Kategorie 8.2 geben. Das Gleiche gilt für die Kabel. Hier sind S/FTP-Kabel vorgeschrieben, also die in Deutschland verbreiteten PiMF-Kabel.

Quelle: Leoni Kerpen



Die Übertragung von 40GBase-T mit je 10 GBit/s über vier Adernpaare.

VDE-AR-E 2800 902 2014-10

Der VDE beruft sich mit seiner Anwendungsregel VDE-AR-E 2800 902 2014-10 auf die installierte Basis in Deutschland: Hier seien S/FTP Kabel stark verbreitet, und bei Frequenzen über 500 MHz setzen die Netzbetreiber in der Regel Verkabelungslösungen der Klassen F und FA ein. So schreibt die im Sinne von VDE 0022 beschlossene Anwendungsregel bei Datenraten von 40 GBit/s und darüber die Verwendung der Kategorie 8.2 vor. Dabei sei der Kompensationsaufwand deutlich geringer als bei Kategorie 8.1.

Next hop: 100GBase-T

Während die neuen 25/40-GBit/s-Standards noch nicht verabschiedet sind, arbeitet Prof. Dr. Albrecht Oehler an der Hochschule Reutlingen im Rahmen eines Verbundprojekts bereits an einer Machbarkeitsstudie für 100 GBit/s über Kupfer. Auf der 22. Fachtagung der Informationstechnischen Gesellschaft im VDE im Dezember 2015 in Köln stellte er erste Ergebnisse vor: Die Übertragung von 4×25 GBit/s funktioniert. Das Team hat dafür eine PAM-32-Modulation eingesetzt. Bei dieser hochwertigen Leitungsmodulation ist laut Prof. Oehler eine HF-Signalentzerrung notwendig. Für die Messungen wurde ein PiMF-Kabel verwendet. Die Anschlusskomponenten werden voraussichtlich auf einem Steckgesicht der Kategorie $7/7_A$ basieren.

Die international stark verbreitete ungeschirmte Technik ist bei Datenraten jenseits der 10 GBit/s an ihre Grenzen gestoßen. Das schlägt sich auch in der Normierung nieder. Und selbst mit foliengeschirmten Kabeln ist der Aufwand nach Einschätzung von Prof. Oehler, Leiter der WG3 in ISO/IEC JTC1 SC25, noch viel zu hoch, um marktfähige Lösungen zu entwickeln. Deshalb normiert das US-Gremium TIA derzeit zahlreiche Zwischenstandards für 5- bis 40-Gigabit-Ethernet. Es ist fraglich, ob diese eine Marktdurchdringung wie die 10/100/1000Base-T erzielen werden.

Sinnvoll für IEEE 802.3 wären nach Einschätzung von Prof. Oehler im nächsten Schritt 100 GBit/s. Doch dazu müsste IEEE 802.3 PiMF-Kabel bewusst in die Normung integrieren, um damit den Schaltungsaufwand in den Netzwerkkarten klein zu halten. Die Verkabelung würde dann auf Komponenten der international genormten Kategorien 7 und 7_A zurückgreifen. Dazu müssten auch die Hersteller der aktiven Technik mit auf diesen Zug springen. Derzeit sieht es noch nicht danach aus, wenn das 25G-Ethernet-Konsortium im nächsten Schritt 50-Gigabit-Ethernet auf RJ45-Basis sieht und hierzu bereits erste Produkte präsentiert: Die Controller der NetXtreme-C-Serie von Broadcom sind nicht nur für 40GBase-T, sondern auch für 25 und 50 GBit/s ausgelegt. Da ist es klar, dass das über Anschlüsse der ISO/IEC-Kategorie 8.1 laufen wird, sobald für 2 GHz ausgelegte Anschlusstechnik verfügbar ist.

Doris Piepenbrink,
freie Journalistin, München

Der Artikel basiert auf Informationen von Yvan Engels von Leoni Kerpen, Projektleiter der Arbeitsgruppe PT 40G in ISO/IEC JTC1 SC25 WG3, und Prof. Dr. Albrecht Oehler, Hochschule Reutlingen, Leiter der WG3 in ISO/IEC JTC1 SC25 – diese Arbeitsgruppe erarbeitet die ISO/IEC 11801.

DIE ISO/IEC-KATEGORIEN 8.1 UND 8.2 IM VERGLEICH

ISO/IEC 11801, Ausgabe 3	Kategorie 8.1, Klasse I	Kategorie 8.2, Klasse II
max. Übertragungsfreqenz	2,0 GHz	2,0 GHz
basiert auf/rückwärtskompatibel zu	ISO/IEC Kat. 6_A (500 MHz)	ISO/IEC Kat. 7_A (1000 MHz)
neue Kabelnorm	IEC 61156-9	IEC 61156-10
neue Norm Stecker/Buchse	IEC 60603-7-81/82	IEC 61076-3-110/104

Quelle: Doris Piepenbrink

Cloud-Verwaltung im eigenen Datacenter

Azure Stack macht lokale Rechenzentren IaaS- and PaaS-tauglich

Nach der Runderneuerung der Client- und der mobilen Betriebssysteme bei Microsoft im vergangenen Jahr folgt 2016 die neue, erweiterte Version von Windows Server. Neu hinzu kommt Azure Stack, das bereits bekannte Azure-Cloud-Funktionen aufs Rechenzentrum überträgt.

Windows Server 2016, das in der zweiten Hälfte des Jahres 2016 auf den Markt kommen soll, hat eine Reihe von Neuerungen im Gepäck: Failover-Cluster lassen sich im laufenden Betrieb und auf Windows Server 2016 umstellen („Rolling-Upgrade"). Hyper-V unterstützt Secure Boot nun auch für Linux-Gäste und kann VMs inklusive ihrer Daten vor neugierigen Administratoren abschirmen („Host Guardian Service"). Mit Storage Spaces Direct lässt sich lokal zugänglicher Festplattenspeicher von Cluster-Knoten als gemeinsamer Speicher nutzen. Storage Replica erlaubt eine synchrone Replikation zwischen Servern oder Clustern zur leichten Notfallwiederherstellung.

Abgesehen davon hat Windows Server 2016 etliche neue Features, die die Verwaltung vereinfachen sollen, darunter PowerShell 5.0 mit seiner Desired State Configuration (DSC) zur konsistenten Bereitstellung.

Abgespeckter Nano Server

Die Minimal-Installationsvariante Nano Server eignet sich mit 92 % weniger Critical Bulletins und 80 % weniger Neustarts speziell für Rechenzentren, in denen Sicherheit und Verfügbarkeit eine wichtige Rolle spielen. Denn das Footprint bei dieser Bereitstellungsform ist nochmals um rund 93 % kleiner als beim Windows-Server-Core-Installationsmodus (der gegenüber der vollständigen Installation ohnehin schon stark verkleinert ist). Dadurch muss der Administrator weniger Patches einspielen und der Server weniger Neustarts ausführen. Aufgrund der minimierten Angriffsfläche steigt zudem die Sicherheit, während das Rechenzentrum wertvolle Ressourcen einspart.

Möglich macht dies der vollständige Verzicht auf die Unterstützung von 32-Bit-Anwendungen, auf die Installation von Software im klassischen MSI-Verfahren (Microsoft Installer) sowie auf alle Komponenten, die für die Benutzeroberfläche erforderlich sind. Dabei wurde die lokale Anmeldung ebenso gestrichen wie der Zugriff per Remote Desktop. Stattdessen erledigt bei dem im Headless-Modus arbeitenden Nano Server ein Administrator alle Verwaltungsaufgaben mittels WMI (Windows Management Instrumentation) oder PowerShell.

Gleichwohl handelt es sich beim Nano Server um einen vollwertigen Windows Server, der sich beispielsweise als Hyper-V-Host, als Gast-Installationsvariante in einer virtuellen Maschine, als Knoten in einem Speichercluster, als DNS- oder Webserver, als Plattform für 64-Bit-Branchenanwendungen oder in Verbindung mit Containern nutzen lässt.

Container – in der Linux-Welt schon länger gang und gäbe – sind eine weitere wichtige Neuheit von Windows Server 2016. Mit diesem Verfahren lassen sich vorkonfektionierte Serveranwendungen mit minimalem Aufwand schnell installieren, konfigurieren und isoliert voneinander betreiben. Im Laufe der Betaphase ist diese Funktionalität sukzessive gewachsen, sodass seit Windows Server 2016 TP4 neben Windows-Server-Containern auch Hyper-V-Container möglich sind.

Windows- und Hyper-V-Container

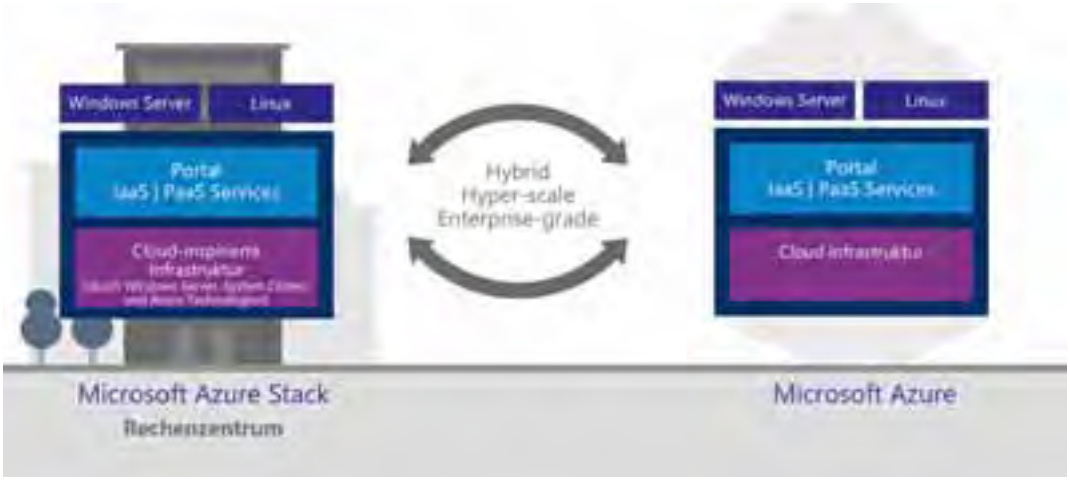
Der Unterschied zwischen beiden Varianten liegt im Grad der Abstraktion: Windows-Container teilen sich das Betriebssystem mit dem Host. Somit eignet sich dieses Modell vor allem für Szenarien, in denen das Betriebssystem des Hosts den darauf laufenden Serveranwendungen vertraut. Für Szenarien, in denen sich mehrere Mandanten das Host-Betriebssystem teilen sollen, besteht die Möglichkeit, eine strikte Isolation der Container durchzusetzen. Dann sind die Anwendungen auch gegen eventuelle Bugs im Betriebssystem immun, die eine Rechteerhöhung (Elevation of Privilege) nach sich ziehen – und somit eventuell Zugriff auf andere Container gestatten. Davor schützten Hyper-V-Container: Diese erhalten jeweils eine Kopie des Windows-Kernels und eigene Arbeitsspeicherbereiche zugewiesen. Ähnlich wie bei einer virtuellen Maschine werden zudem CPU- und Input/Output-Zugriffe abstrahiert. Diesem Plus an Sicherheit bei Hyper-V-Containern steht die schnelle Inbetriebnahme der schlankeren Windows-Container gegenüber.

Welche Form den Vorzug erhält, hängt somit vom jeweiligen Einsatzzweck ab. Die Erstellung selbst ist simpel: Das Attribut „RuntimeType" gibt an, ob es sich um einen Windows- oder Hyper-V-Container handeln soll. Dasselbe Attribut gestattet es, einen vorhandenen Container bei Bedarf in die jeweils andere Form umzuwandeln.

Docker und verschachtelte Virtualisierung

Beide Container-Arten lassen sich mit der in der Linux-Welt bekannten Docker-Technologie verwalten, um die Idee von DevOps abzubilden. Die dazu erforderlichen API-Schnittstellen mitsamt den benötigten Tools und Clients hat Microsoft in Windows Server 2016 serienmäßig implementiert. Auf diese Weise können sowohl Entwickler als auch Administratoren einheitliche Verfahren nutzen, um containerisierte Anwendungen bereitzustellen und zu verwalten. Die einzige Einschränkung, die es hierbei zu beachten gilt, liegt systembedingt beim jeweiligen Betriebssystem: Linux-Container, die Linux-APIs erfordern, lassen sich nicht auf der Windows-Plattform bereitstellen – und vice versa.

Microsoft Azure Stack holt bereits vertraute Cloud-Funktionen ins Rechenzentrum.



Quelle: Microsoft

Hyper-V-Container können auch innerhalb einer virtuellen Maschine laufen. Um dies zu ermöglichen, hat Microsoft bei Windows Server 2016 TP4 und höher ein Feature implementiert, das sich auch für andere Zwecke eignet. Die Rede ist von Nested Virtualization, also der verschachtelten Virtualisierung. Für Demo- und Testlaborumgebungen lässt sich dieses Verfahren sinnvoll nutzen, um die vielfältigen Möglichkeiten der Virtualisierung auf Basis eines einzigen physischen Hosts darzustellen, etwa wenn es darum geht, die Failover-Funktionalität von Hyper-V-Clustern zu demonstrieren.

Verwaltung im System Center 2016

Gemeinsam mit Windows Server 2016 wird Microsoft die Verwaltungssuite System Center 2016 auf den Markt bringen. Diese ist vor allem auf die Unterstützung der neuen Betriebssysteme Windows Server 2016 und Windows 10 abgestimmt.

Generell bietet System Center 2016 bessere Verwaltungsmöglichen inner- und außerhalb der Microsoft-Welt. Ein Beispiel hierfür ist das Management von Nicht-Microsoft-Technologien, namentlich von Anbietern, die nur in einzelnen Cloud-Bereichen vertreten sind, wie AWS (Amazon Web Services) in der Public Cloud und VMware in der Private Cloud. Diese Systeme kann System Center 2016 ebenso wie Microsoft Azure und Hyper-V einheitlich mitverwalten. Somit brauchen Administratoren dafür nicht auf andere Verwaltungsoberflächen und -tools mit jeweils eigenem Bedienkonzept auszuweichen.

VMs im Azure Stack

Ebenfalls interessant ist Azure Stack. Dieses komplett neue Produkt bringt IaaS- (Infrastructure as a Service) sowie PaaS-Technologien (Platform as a Service) aus Microsoft Azure ins lokale Rechenzentrum. Zu Azure Stack gehören dieselben Entwicklungstools, Selfservice-Funktionen und APIs, die es auch in Microsoft Azure gibt. Azure Stack vollendet sozusagen die vom Hersteller seit Jahren skizzierte Vision einer einzigen, konsistenten Cloud-Plattform.

Microsofts Public-Cloud-Angebot Azure sowie das für Rechenzentren gedachte Produkt Azure Stack teilen sich dasselbe Konzept für virtuelle Maschinen. Somit brauchen IT-Verantwortliche VM-Vorlagen nur noch einmal zu erstellen, ohne dass sie sich Gedanken darüber machen müssten, ob die Vorlagen in der Public Cloud (sprich: in Microsoft Azure) oder im lokalen Rechenzentrum (also auf Basis von Azure Stack) eingesetzt werden sollen. Auch nutzt Azure Stack dieselben Azure-Merkmale, wenn es um Sicherheit um Compliance geht. Beispiele hierfür sind die rollenbasierte Zugriffssteuerung RBAC (Role-based Access Control) sowie die Überwachungsprotokollierung (Audit Logging).

Die Komponente Azure Resource Manager erlaubt ferner die konsistente Anwendungsbereitstellung entweder in der Public Cloud mittels Microsoft Azure oder aber im lokalen Rechenzentrum via Azure Stack. Durch diesen Ansatz können sich Entwickler auf die Erstellung von Anwendungen fürs Geschäft konzentrieren. Das Unternehmen wiederum hat die Flexibilität, später noch zu entscheiden, wo die Anwendung laufen soll.

Lizenzierung und Editionen

Wichtige Neuerungen von Windows Server 2016 und System Center 2016 betreffen die Lizenzierung sowie die verfügbaren Editionen. Denn im Gegensatz zu den bisherigen 2012-R2-Produkten der Windows-Server- und System-Center-Familien werden die 2016er-Produkte nicht mehr pro CPU, sondern pro physischem Core lizenziert. Der Vorteil dieses Verfahrens liegt in der Konformität zu Cloud-basierten Abrechnungsmodellen. Wie bisher lassen sich mit der Standard-Edition pro Server maximal zwei verwaltete Betriebssysteminstanzen betreiben, während bei der Datacenter-Edition unlimitierte Betriebssysteminstanzen möglich sind.

Eine weitere Änderung betrifft das Feature-Set der jeweiligen Editionen. Da die Standard-Edition von Windows Server 2016 auf Umgebungen mit geringer oder keiner Virtualisierung ausgelegt ist, bleiben weitergehende, speziell für hochvirtualisierte Private- oder Hybrid-Cloud-Umgebungen relevante Merkmale der Datacenter-Edition vorbehalten. Dies gilt unter anderem für die Funktionen Storage Spaces Direct, Storage Replica, Shielded Virtual Machines, Host Guardian Service sowie den neuen Netzwerk-Stack.

Cloud-first-Konsolidierung

Obgleich die im November 2015 erschienene Technical Preview 4 (TP4) von Windows Server 2016 noch nicht der finalen Fassung entspricht und es auf der Funktionsseite durchaus noch Änderungen geben kann, zeichnet sich schon jetzt ab, dass Microsoft mit den neuen Versionen seiner Serverbetriebssystem- und Management-Produkte mehr Einheitlichkeit bei der Verwaltung anstrebt. Vom lokalen Rechenzentrum bis hin zur Public Cloud folgt dieses Konzept dem Motto „Cloud first".

Jennifer Lierenfeld,
Produkt Manager Server & Cloud Infrastruktur, Microsoft

Minimaler Aufwand, maximaler Überblick

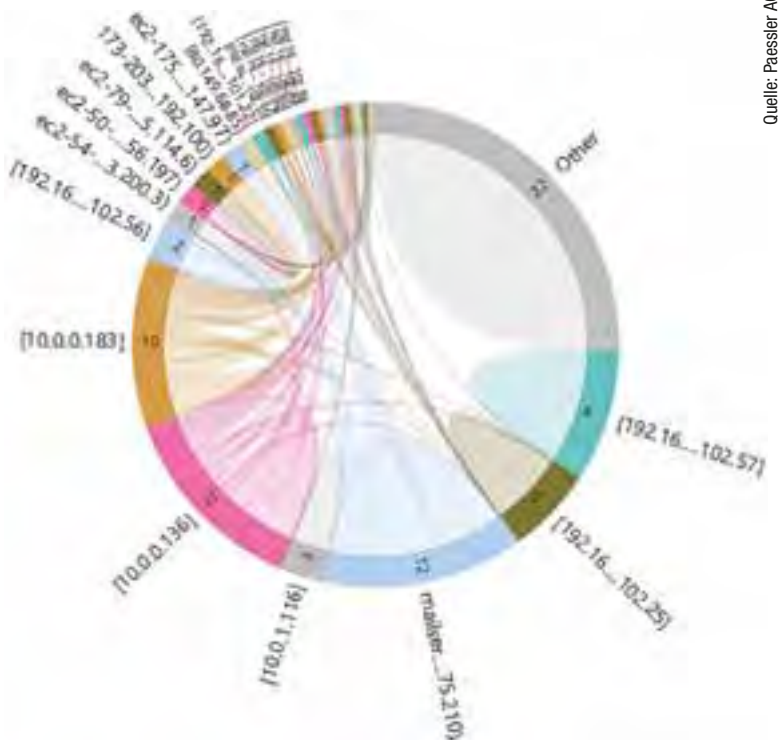
Gutes Netzwerkmonitoring ist einfach, umfassend und kostentransparent

Netzwerkmonitoring ist heute fester Bestandteil eines professionellen Netzwerkmanagements. Allerdings gibt es noch Optimierungspotenzial. Vor allem für kleinere und mittlere Netzwerke sind viele Lösungen zu komplex und zu aufwendig. Solche Monitoring-Tools werden zuerst implementiert, dann aber kaum genutzt.

Manche Tools sind einfach zu spezialisiert und konzentrieren sich beispielsweise auf die Überwachung von Bandbreiten mittels NetFlow oder von virtuellen Umgebungen. Hier finden sich auch Herstellerlösungen, die lediglich die Hard- oder Softwareprodukte aus ihrem Haus einbeziehen. Zwar leisten spezialisierte Lösungen ebenso wie die meisten Herstellertools einiges in Hinblick auf die Tiefe der Überwachung, sie können (und müssen) aber nicht den großen und umfassenden Überblick über die komplette IT-Infrastruktur liefern.

Daneben gibt es Open-Source-Monitoring-Tools. Zwar lassen sich hiermit breit angelegte Monitoring-Szenarien aufsetzen, allerdings erfordert das ein entsprechendes Know-how und viel Aufwand. Auch Betrieb und Wartung stellen hohe Ansprüche an den Administrator. Letzten Endes kann keine der drei Varianten das liefern, was Netzwerkmonitoring im Idealfall mitbringen sollte, nämlich erstens einen umfassenden Überblick über die gesamte IT-Infrastruktur, zweitens einfach einzurichtende Benachrichtigungsmechanismen für den Störungsfall und drittens eine übersichtliche Aufbereitung der ermittelten Daten für die langfristige Optimierung des Netzwerks. All das kann man einfach umschreiben: Eine gute Monitoring-Lösung sollte dem Administrator den Alltag erleichtern und ihm Arbeit abnehmen, statt neue Baustellen zu schaffen.

Der Markt bietet hier mittlerweile durchaus Alternativen: schlanke Unified-Monitoring-Lösungen, die sich durch Einfachheit in der Benutzung und Breite bei der Funktionalität statt durch Komplexität und Spezialisierung auszeichnen. Diese Tools liefern einen umfassenden und herstellerunabhängigen Überblick über die gesamte IT-Infrastruktur, zeichnen sich durch einfache Implementierung und Pflege aus und sind preislich auch für mittelständische Unternehmen erschwinglich. Um die optimale Lösung für das eigene Unternehmen zu finden, gilt es bei der Auswahl einige Kriterien zu beachten.



Quelle: Paessler AG

Der PRTG Network Monitor der Nürnberger Paessler AG stellt Datenströme im Netzwerk in einer interaktiven Grafik dar.

Unterstützung gängiger Standards

Je mehr Standards eine Lösung unterstützt, desto breiter ist sie aufgestellt und eher kann sie umfassende Informationen liefern. Hier einige der wichtigsten Protokolle im Überblick:

SNMP (Simple Network Management Protocol) ist eine Art kleinster gemeinsamer Nenner. Über MIB-Dateien (Management Information Base), die Gerätehersteller zur Verfügung stellen, lassen sich Switches, Server und Firewalls, aber auch Software und sogar manche Kaffeemaschinen relativ einfach in geeignete Monitoring-Lösungen einbinden. Dabei generiert SNMP Daten zum Netzwerktraffic ebenso wie zu Verfügbarkeit und Zustand. Idealerweise liefert die Monitoring-Software fertige Templates für die gängigsten Geräte bereits mit und integriert diese vollautomatisch in die Überwachung.

WMI (Windows Management Instrumentation) liefert umfassende Daten in Windows-Umgebungen. Allerdings ist WMI nicht unkompliziert in der Handhabung und fehleranfällig. Für WMI spricht die Möglichkeit, dass man im Bedarfsfall Geräte oder Dienste mittels WMI booten kann.

Packet Sniffing: Hier werden einzelne Datenpakete ausgelesen und daraus sehr detaillierte Traffic-Informationen gewonnen. Da alle Daten dazu über einen Mirror-Port oder über ein dediziertes Sniffing-Gerät geleitet werden müssen, erzeugt Sniffing vor allem im größeren Maßstab enorme Lasten und bildet einen Engpass im Netzwerk.

NetFlow, sFlow oder jFlow sind Protokolle zum Auswerten von Traffic-Daten. Ähnlich wie Packet Sniffing findet eine mehr oder weniger tiefe Analyse statt. Dazu werden die Flow-Informationen von den Geräten bereitgestellt und an das Monitoring-Tool geliefert, sodass die Belastung des Netzwerktraffics deutlich geringer ist als beim Sniffing. Allerdings unterstützt nicht jeder Switch oder Router Flow, sondern in der Regel nur die kostspieligeren Premium-Varianten.

Speziell im Flow- und Sniffing-Bereich gibt es hochspezialisierte Lösungen, die aus Performance-Gründen oft als Appliance angeboten werden. Diese können sehr detaillierte Traffic-Daten liefern und auf dieser Grundlage dann auch Informationen über End-User-Experience und die Performance von Applikationen. Für einen umfassenden Überblick über die komplette IT-Infrastruktur eignen sie sich weniger.

Viele breit aufgestellte Monitoring-Lösungen bieten Flow- und IP-SLA-Funktionalität in Form von Zusatzmodulen an. Hier ist allerdings Vorsicht geboten: Nur allzu schnell kommen für solche Add-ons erstaunliche Summen zusammen.

Monitoring virtueller Umgebungen

Auch bei mittelständischen Unternehmen ist Virtualisierung mittlerweile eher die Regel als die Ausnahme. Ob es dabei um die Virtualisierung einzelner Server geht, um Private oder Hybrid Clouds oder um die Nutzung cloudbasierter Software-Angebote: Die Überwachung der virtuellen Umgebungen ist essenziell, wenn es um die Sicherstellung der IT-Performance geht. Entscheidend ist, dass die Monitoring-Lösung die komplette Bandbreite der virtualisierten Umgebung einbezieht: Hardware, Virtualisierungsebene, Applikationen. Nur so ist eine genaue Analyse und Lokalisierung von Störungen oder Problemen möglich.

Wie bei Flow und IP SLA werden auch zur Überwachung von Virtualisierungssystemen oft kostenpflichtige Add-ons angeboten. Um nachträgliche Zusatzkosten zu vermeiden, ist es daher sinnvoll, nach Lösungen Ausschau zu halten, die gängige Virtualisierungslösungen von VMware, Microsoft oder Citrix ohne Extrakosten unterstützen oder zumindest eventuelle Zusatzkosten von Anfang an in die Kalkulation einzubeziehen. Ein hilfreiches Extra ist die Möglichkeit, gängige cloudbasierte Services wie beispielsweise Dropbox, Facebook, Office 365 oder Salesforce auf Erreichbarkeit zu überprüfen.

Weil die IT-Infrastruktur vieler mittelständischer Unternehmen über mehrere Standorte verteilt ist – als verteilte Rechenzentren, Filialen mit eigener IT oder als Kundennetzwerke – sollte eine Monitoring-Lösung auch das ohne große Mehrkosten abbilden und einen zentralen Überblick über die IT des gesamten Unternehmens liefern.

API-Dokumentation und Usability

Ob es um die Einbindung von Nicht-IT-Geräten geht, um die Überwachung selbst entwickelter Software oder um die Integration von Produktionsanlagen im Rahmen von Industrie 4.0 – ohne eine gut dokumentierte API kommen Monitoring-Lösungen nicht weit. Hier gilt es, bei Open-Source-Tools die Community bzw. bei kommerziellen Angeboten das Partnernetzwerk des Anbieters abzufragen: Besteht die Möglichkeit, professionellen Support für individuelle Anpassungen zu bekommen? Nicht immer reichen Know-how und interne Ressourcen, um solche Projekte erfolgreich umzusetzen.

SCHNELLE EVALUATIONSKRITERIEN

Für kleinere Unternehmen mit wenig eigenen Admin-Ressourcen ist wichtig, dass sie anhand der Testversion rasch und eindeutig herausfinden, ob die Lösung alle Netzwerkgeräte und -komponenten automatisch erkennt und berücksichtigt und ob die Berichte vollständig und richtig sind. Außerdem sollte die Lösung bei kritischen Vorkommnissen alarmieren, zum Beispiel per SMS. Zu prüfen ist auch, ob mobile Zugriffe auf die Dashboards und Berichte erforderlich sind oder nicht.

Außerdem bringt eine Monitoring-Software keinen Mehrwert, wenn sie so komplex ist, dass sie niemand benutzen kann oder möchte. Eine einfache und intuitive Benutzerführung, Best-Practice-basierte Automatismen und Hilfen sowie umfassende Benachrichtigungs- und Publikationsmöglichkeiten steigern die Akzeptanz und damit den Praxisnutzen einer Monitoring-Lösung. Je nach Anforderung können auch Apps für Mobilgeräte, gegebenenfalls mit Möglichkeit zur Push-Benachrichtigung, einen willkommenen Zusatznutzen bieten.

Als eine erweiterte Form der Usability sind die Aspekte von Implementierung und Betrieb zu sehen. Das reicht von der Erstinstallation über die Konfiguration und die Einrichtung des konkreten Monitoring-Szenarios bis hin zur Sicherung der Monitoring-Daten und zum Einspielen von Updates. Ebenso wie die Usability lässt sich all das im Prinzip nur über eine Testinstallation sinnvoll evaluieren. Womit dann gleich noch eine weitere Frage ins Spiel kommt: Gibt es eine Testversion der Software?

Lizenzierung, Preis und Support

Open Source, Baukastensystem oder All-in-Lizenzierung? Kostenlos ist keine der drei Varianten. Auch wenn die Open-Source-Alternative zunächst keine Lizenzkosten verursacht, hängt es doch sehr von den individuellen Umständen ab, ob sie bei den Gesamtkosten am Ende wirklich günstiger ist als lizenzkostenpflichtige Varianten. Leitfragen sind: Gibt es ausreichend Know-how und Ressourcen (im Haus oder in Form eines erfahrenen Dienstleisters)? Was sind die langfristigen Anforderungen an die Monitoring-Lösung? Überwiegen individuelle Szenarien oder sollen hauptsächlich Standards überwacht werden?

Dort, wo Open Source keine Option ist, gilt es, verschiedene Lizenzierungsmodelle gegeneinander abzuwägen. Viele Hersteller bieten zahlreiche Funktionen in Form von Add-ons oder Zusatzmodulen an. In diesem Fall muss man die noch benötigten Module in die Kalkulation einbeziehen. Auch sollte man Architektur und Usability im Auge behalten: Bekomme ich eine Lösung aus einem Guss oder handelt es sich um eine Reihe von einzelnen Tools, die mehr oder weniger effizient unter einer Oberfläche zusammengefasst sind?

Die dritte Option sind Lösungen, deren Lizenzen sich nach der Anzahl der überwachten Geräte und Applikationen berechnen und die in jeder Lizenz die komplette Monitoring-Funktionalität zur Verfügung stellen. Hier gilt es zu prüfen, ob der Funktionsumfang auch künftigen Anforderungen gewachsen ist, sonst endet man in einer Sackgasse und muss womöglich nach kurzer Zeit schon wieder eine neue Lösung einführen.

Schließlich bleibt noch die Frage nach dem Support. Wichtig ist ein kompetenter und zeitnaher Kundendienst, bei kommerzieller Software idealerweise direkt vom Hersteller. Ist der Support auch auf Deutsch verfügbar, ist das ein nettes Extra.

Dirk Paessler,
Gründer und CEO der Paessler AG

Super omnia frigus

Die Universität Mannheim muss eine Wärmelast von bis zu 220 kW bewältigen

Rund 12.000 Studierende und 1600 Mitarbeiter, von denen bis zu 6000 gleichzeitig online sind – hoch über dem Mannheimer Schloss, im 11. Stockwerk des RUM-Gebäudes muss das Rechenzentrum der Universität Mannheim in etwa die gleiche Leistung erbringen wie die Datacenter von KUKA oder Zalando.

Ein 15-köpfiges Team ist dafür zuständig, den laufenden Betrieb des Datennetzes, der Medientechnik sowie der Infrastruktur zu gewährleisten. Keine leichte Aufgabe, bei einer Auslastung des Backbones mit 10 GBit/s, 6000 am LAN angeschlossenen Rechnern, 600 Switches und 500 WLAN-APs. Die Leistungsfähigkeit des Rechenzentrums wird dabei durch zwei wichtige Komponenten sichergestellt: den Forschungsclusterrechner der Universität und eine smarte Kühlungslösung.

Zentraler Kaltgang für den Superrechner

Eigentlich wollte die Universität Mannheim 2010 die Klimatechnik respektive die Kühlleiter im Maschinenraum erneuern, um sie der gestiegenen Rechenleistung anzupassen. Nach der Analyse der Ist-Situation entschied sich Ralf-Peter Winkens, Leiter der Abteilung Datennetz und Medientechnik im Rechenzentrum, dann doch für die Neuplanung des kompletten Datacenters. Um den laufenden Betrieb zu gewährleisten, wurde das Projekt in fünf Bauabschnitte unterteilt. Pro Abschnitt wurde zunächst ein Bereich freigeräumt und anschließend mit der neuen Hardware bestückt.

Seit August 2015 stehen nun auf 100 m^2 insgesamt 53 Racks und 21 Seitenkühler. Für den Ausbau des Rechenzentrums wurde mit insgesamt vier Teilaufträgen Schäfer IT-Systems, eine Tochter der in Neunkirchen im Siegerland ansässigen Schäfer-Werke, betraut. Als Hersteller von Netzwerk-, Serverschrank- sowie Rechenzentrumslösungen lieferte und installierte das Unternehmen auch die Hardware.

„Ausschlaggebend war dabei das Konzept", sagt Ralf-Peter Winkens. „Das Unternehmen verbaute schon 2010 die Kühler nicht in den einzelnen Schränken, sondern setzte auf einen zentralen Kaltgang. Diese Variante ist nicht umsonst besser und sicherer: Heute sind Kaltgangeinhausungen Standard." Die Leistungsfähigkeit der Kühlung spielt in Mannheim eine maßgebende Rolle, denn eine Besonderheit des Universitätsrechenzentrums ist der „Superrechner". Er belegt Platz 80 unter den 100 schnellsten Rechnern der Welt. Bei voller Nutzung aller Leistungen des Datacenters entsteht eine maximale Wärmelast von 220 kW, von der allein der Superrechner für 150 kW verantwortlich ist.

Quelle: Universität Mannheim

Seit August 2015 läuft das neue Universitätsrechenzentrum Mannheim unter dem Dach des RUM-Gebäudes. Das Klimakonzept setzte Schäfer IT-Systems mit einer Kaltgangeinhausung um, in der die Rack-Reihen Front zu Front stehen.

Flexible, energetische Klimatisierung

Das steigert entsprechend die Anforderung an die Klimatechnik. Zum einen befindet sich das Rechenzentrum mitten in der Quadratestadt, im 11. Stockwerk des RUM-Gebäudes, direkt unter dem Dach, um die Wege für die Kühlung kurz zu halten. Die Mannheimer Kälteanlage besteht aus drei Komponenten: Die konventionelle Kühlung sichert ein Kompressor mit rund 220 kW Kälteleistung, der direkt auf dem Dach steht. Eine indirekte, freie Kühlung mit 20 m^2 Fläche auf dem Dach nimmt durch Ventilatoren die Umgebungskälte aus der Luft und wirkt auf den Gesamtkreislauf, zusätzlich zu den Loopus-Coolern. Das ist eine wassergekühlte Rack-Klimatisierungslösung, die seitlich geschlossen, jedoch vorne und hinten offen ist. Die Seitenkühler saugen erwärmte Luft von hinten aus dem Raum an und blasen sie gekühlt in den eingehausten Kaltgang. Eine direkte, freie Kühlung bläst als drittes Element der Kühlung zudem 8800 m^3/h Außenluft direkt in den Warmgangbereich ein und entlastet damit wiederum den Kompressor auf dem Dach. Schließlich gewährleistet eine Notkühlung mit insgesamt 70 kW den Betrieb der Systeme im Fall einer Störung. Sie besteht aus sechs unabhängigen Split-Klimageräten, die an einem Notstromdieselgenerator angeschlossen sind.

Winkens zeigt sich mit der Gesamtlösung sehr zufrieden: „Die Leistungsstärke der Klimatisierung respektive die Qualität der Arbeit zeigen sich zunächst in der lückenlosen Versorgung. Aber auch in Details und in nicht planbaren Umständen. So musste der Superrechner in diesem Sommer mit maximaler Auslastung und daraus resultierend auch maximaler Kühlung getestet werden. Am dafür vorgesehenen Tag hatte es zusätzlich 35 °C Außentemperatur. Die Kühlung hat den Test mit Bravour bestanden. Im Regelbetrieb geht es jedoch meist gemäßigter zu. Die 15.000 User nutzen im Wesentlichen den schnellen Internet-Zugang für ihre Web- und Mail-Anwendungen sowie die virtualisierte Serverinfrastruktur hauptsächlich für Verwaltungs- und E-Learning-Dienste. Mit einer durchschnittlichen Wärmelast von 120 kW im Rechnerraum können dann auch die Köpfe unserer Plattenschränke kühl bleiben."

Simon Federle,
freier Journalist

Energiemanagement über die Stromschaltleiste

Die jüngsten iPDUs können weitreichende Steuerfunktionen übernehmen

Mit viel Aufwand hat man in den Serverräumen die Kühlung der Rechner und Router verbessert, und der Strom kommt immer öfter aus einer intelligenten Stromschaltleiste. Solche iPDUs regeln aber nicht nur die Energieversorgung, sondern können auch genaue Abrechnungsdaten liefern – und noch einiges mehr.

Der Stromverbrauch verursacht den größten Kostenanteil beim Betrieb eines Rechenzentrums. Hinzu kommt, dass die maximal verfügbare elektrische Leistung zunehmend die Kapazitätsgrenzen eines Rechenzentrums bestimmt. War vor einigen Jahren noch der Raum ein begrenzender Faktor, so spielen heute – angesichts der Anschlussleistungen moderner Hochleistungsserver von teilweise weit über 10 kW – andere Herausforderungen eine Rolle: zum einen die Kühlleistung, zum anderen die insgesamt verfügbare elektrische Leistung.

Stromreserven ausschöpfen

Um die Räume eines Rechenzentrums optimal auszunutzen, muss man die elektrische Leistung und die Kühlleistung regeln. Voraussetzung hierfür ist die genaue Bestimmung der Verlustleistung der Server. Die Addition der im Datenblatt angegebenen maximalen Leistungsaufnahmen der Servernetzteile wäre sicher eine Möglichkeit. Die tatsächlich von den meist überdimensionierten Netzteilen abgeforderte elektrische Leistung liegt jedoch teilweise deutlich unter der angegebenen Nennleistung, sodass hier Stromreserven brachliegen, die gewinnbringend für den Betrieb weiterer Server genutzt werden könnten. Will man diese ungenutzte Pufferzone an zusätzlich verfügbarer Leistung ausschöpfen, ist jedoch eine präzise und kontinuierliche Messung der abgerufenen elektrischen Leistung unbedingte Voraussetzung. Für eben diese Messungen eignen sich die intelligenten Stromschaltleisten (intelligent Power Distribution Units).

Das Leistungsvermögen und die Funktionsvielfalt moderner PDUs gehen aber weit darüber hinaus: Durch Energieverbrauchsmessung auf Anschlussebene in Echtzeit, Umgebungsüberwachung mittels Plug-and-Play-fähiger Sensoren und eine Erfassung weiterer relevanter Daten können iPDUs die Racks umfassend verwalten.

Über das Display der PDU, einen Webbrowser oder die entsprechende App haben Rechenzentrumsbetreiber den Stromverbrauch und PDU-Zustand, Temperatur und Luftfeuchtigkeit sowie Zuleitungen und einzelne Anschlüsse stets im Blick. Moderne iPDUs übermitteln diese Umgebungsdaten umgehend an die passende DCIM-Software und ermöglichen somit die optimale und sparsame Regulation von Umgebungstemperatur und Lüfteraktivität. CISCO konnte zum Beispiel durch den Einsatz in seinen IT-Laboren nachweisen, dass mithilfe der Kombination aus PDU und Power-IQ-Software eine jährliche Senkung der Stromkosten um mehr als 500 US$ pro PDU möglich ist.

Steuern, regeln, messen

Ein weiteres Einsatzgebiet der PDU-Software-Kombination wäre beispielsweise die präzise Ermittlung einzelner Verbrauchswerte bis hin zur automatisierten und produktdedizierten Rechnungsstellung an den Kunden – diese Funktion ist namentlich für Colocation-Betreiber von Interesse. Das Duett aus PDU und Software bündelt und verwaltet alle ermittelten Informationen in einer Datenbank. Über eine offene ODBC-

Quelle: Raritan

Die Raritan-Software Power IQ zeigt im konfigurierbaren Dashboard die wichtigsten Parameter auf einen Blick.

Schnittstelle gehen die Daten dann an andere Managementsysteme, beispielsweise an eine Billing-Software.

Intelligente Extras

Taugliche PDUs gibt es zudem mit integrierter permanenter Differenzstrommessung. Damit lassen sich Fehlerströme erkennen, sodass die Verantwortlichen sofort reagieren können – eine Maßnahme, die der Gesetzgeber inzwischen aus Sicherheitsgründen verlangt, da der Einsatz von FI-Schaltern in Rechenzentren unüblich ist.

Ein weiterer Vorteil der neuesten PDU-Generation: Via SCAAS (Smart Card Access and Authentication System) lassen sich Serverschränke vor unbefugtem Zugriff schützen. Das in der PDU integrierte System ermöglicht nur befugten Mitarbeitern den Zutritt ins Rechenzentrum oder das Öffnen der Schränke mittels einer Zugangskarte, deren Daten an einem zentralen USB-Kartenleser ausgelesen werden.

Doch iPDUs können noch mehr. Auf dem Markt gibt es zum Beispiel remote schaltbare Modelle mit bistabilen Haftrelais, die den gewünschten Ein- und Ausschaltzustand auch ohne Stromversorgung beibehalten. So kann beispielsweise ein Rechenzentrum mit 100 Serverschränken jährlich rund 5000 Euro an Strom- und Kühlungskosten einsparen. Dabei wird eine neue Schaltung verwendet, die trotz bistabiler Haftrelais sicherstellt, dass sequenzielles Einschalten der Server nach einem Stromausfall oder einer Abschaltung gewährleistet ist, um die Einschaltspitzen gering zu halten. Solche PDU-Modelle lassen sich im Vorfeld so konfigurieren, dass die Relais im Falle eines Stromausfalls ihre jeweilige Schaltstellung beibehalten oder die Server entsprechend spezifischer Vorgaben im Hinblick auf Zeitabstand und Reihenfolge erneut hochgefahren werden.

Die räumlich enge Verbindung von hochgenauer Messtechnik und robuster Stromschalttechnik machen die PDU zu einem hochkomplexen Produkt, das im Alltagsbetrieb hohem mechanischen und thermischen Stress standhalten muss. Unglücklicherweise ist von außen nicht ersichtlich, ob der Hersteller sein Modell zum Beispiel so gebaut hat, dass die Kondensatoren möglichst wenig Hitze ausgesetzt sind. Schwachstellen im Elektronikdesign zeigt allenfalls eine thermografische Untersuchung.

Die Ethernet-Achillesferse

Die PDU wird über eine Ethernet-Schnittstelle gesteuert und über sie werden in letzter Konsequenz auch die angeschlossenen Server ein- oder ausgeschaltet. PDUs versorgen in einem Serverschrank unter Umständen 42 Server und mehr mit Strom. Ein Ausfall einer PDU hat also ernsthafte Folgen für den Betrieb des Rechenzentrums. Daher werden die Stromversorgung und alle verwendeten Komponenten einschließlich der PDUs mindestens doppelt ausgeführt. Da in den weitaus meisten Installationen die beiden redundanten PDUs in einem Schrank zu 100 % identisch sind und von einem gemeinsamen Steuernetzwerk und letztlich von derselben Software gesteuert werden, ist es hier besonders wichtig, auf die Qualität und Zuverlässigkeit der verbauten PDUs zu achten.

Wenn es nämlich mit einem Angriff auf die PDU gelingt, über das Steuernetz die Schaltausgänge zu übernehmen, war die Investition in unterbrechungsfreie Stromversorgungen umsonst und die Dieselaggregate springen gar nicht erst an. Es werden beide PDUs zur gleichen Zeit heruntergefahren oder blockiert und die Server außer Betrieb genommen. Ansatzpunkte für derartige Attacken fand das Testlabor der TU Chemnitz zur Genüge. Als Grund für die „Fahrlässigkeit, mit der eine große Anzahl von PDU-Herstellern für die IT-Sicherheit ihrer Geräte sorgt“, nennen die Wissenschaftler den Umstand, dass viele Produkte rein aus der Elektrik entwickelt sind; Anbieter, die aus der IT oder Netzwerktechnik kommen, sind weit eher hellhörig für Sicherheitsfragen.

Ralf Ploenes,
Geschäftsführer Raritan Deutschland GmbH

Impressum
Themenbeilage Rechenzentren und Infrastruktur

Redaktion just 4 business GmbH
Telefon: 08061 34811100, Fax: 08061 34811109,
E-Mail: tj@just4business.de

Verantwortliche Redakteure:
Thomas Jannot (v. i. S. d. P.), Florian Eichberger (Lektorat)

Autoren dieser Ausgabe:
Peter Dümig, Simon Federle, Matthias Hain, Wolfgang Huber, Jennifer Lierenfeld, Oliver Lindner, Klaas Mertens, Dirk Paessler, Doris Piepenbrink, Ralf Ploenes, Ariane Rüdiger

DTP-Produktion:
Enrico Eisert, Kathleen Tiede, Matthias Timm, Hinstorff Verlag, Rostock

Korrektorat:
Kathleen Tiede, Hinstorff Verlag, Rostock

Technische Beratung:
Uli Ries

Titelbild:
vladimircaribb, fotolia

Verlag
Heise Medien GmbH & Co. KG,
Postfach 61 04 07, 30604 Hannover; Karl-Wiechert-Allee 10, 30625 Hannover;
Telefon: 0511 5352-0, Telefax: 0511 5352-129

Geschäftsführer:
Ansgar Heise, Dr. Alfons Schräde

Mitglieder der Geschäftsleitung:
Beate Gerold, Jörg Mühle

Verlagsleiter:
Dr. Alfons Schräder

Anzeigenleitung (verantwortlich für den Anzeigenteil):
Michael Hanke (-167), E-Mail: michael.hanke@heise.de, www.heise.de/mediadaten/ix

Leiter Vetrieb und Marketing:
André Lux

Druck:
Dierichs Druck + Media GmbH & Co. KG, Frankfurter Straße 168, 34121 Kassel

Die Inserenten

Die hier abgedruckten Seitenzahlen sind nicht verbindlich.
Redaktionelle Gründe können Änderungen erforderlich machen.