ComConsult Research

Der Netzwerk Insider

Januar 2018

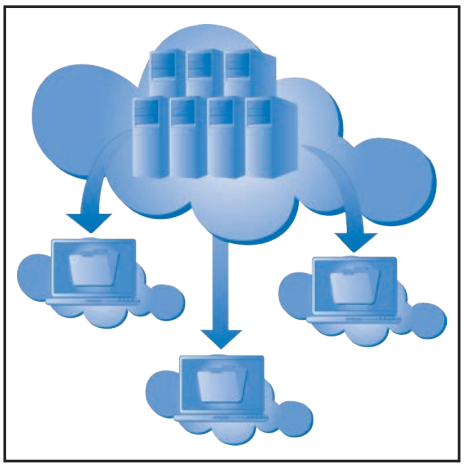
Systematische Weiterbildung für Netzwerk- und IT-Professionals

Netzzugang zu Public Clouds

von Dr. Behrooz Moayeri

Unternehmen nutzen Public Clouds immer stärker. Dieser Beitrag befasst sich mit dem Netzzugang zu Public Clouds.

Je nach Servicetyp in der Cloud (SaaS, PaaS oder IaaS) kann es unterschiedliche Anforderungen an den Netzzugang zu Public Clouds geben. Während in vielen Fällen die Nutzung des Internet als Zubringer zu Public Clouds ausreicht, gibt es Szenarien, in denen vom Internet getrennte Zugänge gefordert sind. Diese können zum Beispiel die Verbindung zu einem Standort nutzen, an dem diverse Public Clouds über kurze Wege erreichbar sind.



Da die Public Clouds in der Regel getrennt nach Weltregionen organisiert sind, stellt sich die Frage, wie die überregionale Nutzung einer Cloud aussehen muss.

Andere relevante Fragen, auf die im Folgenden eingegangen wird, beziehen sich auf die Nutzung von Netz- und Sicherheitsfunktionen in der Cloud, wie zum Beispiel Zonen- und VPN-Bildung.

Ferner wird auf Authentisierung, Autorisierung und Verschlüsselung beim Cloud-Zugriff eingegangen.

weiter ab Seite 10

Enterprise Server-based Storage: VMware vSAN

von Dipl.-Math. Cornelius Höchel-Winter

Speicher ist neben der Rechenleistung und dem Netzwerk eine der drei wesentlichen Säulen im Rechenzentrum. Klassisch war dieser Speicher lokal in den Servern verbaut, der Zugriff erfolgte direkt über interne Bussysteme, das war einfach, eine eigene Infrastruktur hierfür nicht nötig.

Aber schon länger gibt es Anwendungen, die zentralen, über das Netzwerk erreichbaren Speicher erfordern (Datenbanken, Failover-Cluster etc.) und spätestens mit dem Einzug der Servervirtualisierung wurde zentraler Speicher ein unverzichtbares Designelement in modernen Rechenzentren. Die Antwort darauf waren große monolithische Speichersysteme, basierend auf proprietärer Hard- und Software und oft genug angebunden über ein eigenes Fibre-Channel-Netzwerk. Das ist teuer, komplex und aufwändig.

Die Servervirtualisierung zeigt aber in eine prinzipiell andere Richtung: Nutzung von Standardkomponenten, Abstraktion von der physischen Hardware und automatisierbare Steuerung der virtualisierten Ressourcen durch Software. „Server-based Storage“ ist ein Technologietrend, der diese Konzepte umsetzt und so eine enge Integration mit der Servervirtualisierung zulässt.

weiter ab Seite 22

Geleit

Handlungsbedarf: IT-Infrastrukturen für neue Gebäude werden zu einem Risiko

auf Seite 2

Standpunkt

Manchmal sucht man sich „einen Wolf“

auf Seite 30

Neue Sonderveranstaltungen

Herausforderung Cloud

auf Seite 16

Office 365 in der Praxis

auf Seite 17

Kriterien und Erfolgs-Szenarien für den Einsatz von UCC-Produkten

auf Seite 18

Aktueller Kongress

ComConsult Netzwerk Forum 2018

ab Seite 6

Geleit

Handlungsbedarf: IT-Infrastrukturen für neue Gebäude werden zu einem Risiko

Wir haben dieses Thema schon 2017 adressiert, aber die Brisanz ist weiterhin zunehmend und die aktuellen Projekte machen dies mehr als deutlich. Auslöser des Problems ist die zunehmende Gebäude-Automatisierung in Kombination mit vertraglichen Grundlagen, die schlicht unzureichend sind.

Im Kern stehen folgende Problembereiche:

- Gewerke-übergreifende universelle Verkabelung
- Funk-Technologien
- Netzwerk-Infrastrukturen
- Power over Ethernet
- Sicherheit

Ich gehe später auf diese Problembereiche ein. Aber ich möchte an dieser Stelle direkt mit der Tür ins Haus fallen und das dominante Problem ansprechen, das wir bereits haben, das aber in den nächsten Jahren zu einem Riesen-Problem werden wird: IT-Sicherheit in modernen "Smart-Buildings".

Die Gründe für dieses Problem sind vielseitig:

- Die an der Gebäudeplanung beteiligten Parteien haben zu 90% schlicht keine Ahnung von IT-Sicherheit
- IT-Sicherheit kann nicht als Puzzle umgesetzt werden, in dem jedes Gewerk ein bisschen Sicherheit für sich selber macht. Das Puzzle geht nicht auf
- Die bisherigen Rechts- und Vertragsgrundlagen für die Planer und die installierenden Gewerke decken das Thema nicht ausreichend ab. So ist vertraglich unklar, welche Verpflichtungen der einzelne Planer hat und wofür er eigentlich haftet. Damit ist auch unklar, wie weitgehend dieses Thema in den Ausschreibungen berücksichtigt werden muss
- Planer werden für das Thema nicht angemessen bezahlt
- Sicherheit kostet Geld und erhöht die Komplexität des kompletten Projekts

Warum sind dies Problembereiche? Was hat den Markt und die Planung so verändert, dass die traditionell erfolgreiche Planung auf einmal nicht mehr funktioniert?

Die zentralen Indikatoren für Probleme sind:

- Die gewählte Planungs-Methodik
- Zunehmender Einsatz von Sensor-Technik und Automatisierung

- Zunehmende Abhängigkeiten zwischen Gewerken auch im Betrieb
- Die Größe des Projekts
- Die angestrebte Nutzung des Gebäudes
- Die Kernfaktoren für eine spätere Vermarktung und die entstehende Wirtschaftlichkeit
- Der angestrebte spätere Betrieb und dessen Kosten

Kommen wir zurück auf die Problembereiche. Was sind die Gründe dafür, dass es diese Problembereiche gibt?

- Immer mehr Gewerke arbeiten mit eigenen Kabelsystemen. Dies führt zu Konflikten in der Nutzung von Kabelwegen und Verteilerräumen. Gleichzeitig ist nicht mehr sicher, dass wirklich eine universell nutzbare Verkabelung entsteht. Es kommt zu einem Verlust an Transparenz für den Infrastrukturplaner auf der Architektenseite. Auch BIM löst dieses Problem nicht. Im Idealfall macht BIM das Problem sichtbar. Aber dann ist es bereits zu spät und signifikante Neuplanungen und Verzögerungen sind die Folge. Und vor allem: dies ist häufig in den Planungsverträgen nicht vorgesehen und führt zu Nachforderungen seitens der Planer.

- Funk-Technologien breiten sich aus wie ein Grippe-Virus. Von Bluetooth über ZigBee über das WLAN bis zu 5G. Und viele dieser Technologien nutzen dieselben Frequenzen. Das Desaster ist hier vorprogrammiert. Und vor allem: die Probleme sind nicht unbedingt bei der Abnahme sichtbar, da zu diesem Zeitpunkt viele der möglichen Funk-Teilnehmer gar nicht aktiv sind.

- Die zunehmende Nutzung von IT erfordert ein zentrales Netzwerk-Konzept. Dieses ist eng verbunden mit dem Thema Funk und mit dem Thema Sicherheit. Tatsächlich wird das Netzwerk eine der Schlüssel-Technologien für den späteren Schutz von Gebäuden sein. Und die Tragweite möglicher Probleme wird angesichts der Sicherheitslücken in den CPU-Chips mehr als deutlich. Diese Chips werden heute in Brandmeldeanlagen, Zugangskontrollsystemen, Aufzugssteuerungen, Videoüberwachungen, Beleuchtungssteuerungen, … eingesetzt. Und dies wird nicht die letzte Sicherheitslücke dieser Dimension sein, die wir in den nächsten Jahren erleben werden. Die Planung der Gebäude-Sicherheit muss schlicht unterstellen, dass einzelne Technologiebereiche gehackt werden. Dabei gilt: je größer oder je wichtiger ein Gebäude, desto größer der Sicherheitsbedarf. Die reine Größe in Etagen und Quadratmetern ist direkt proportional zum Erpressungspotenzial, die Nutzung ist direkt proportional zu möglichen inhaltlichen Angriffsmotivationen.

- Es gibt einen globalen Trend hin zu Gleichstrom-Versorgern, die über PoE versorgt werden (Leuchten, Schalter, kleine Steuerungen, …). Speziell im Beleuchtungsbereich oder allgemeiner in allen Bereichen, in denen LEDs eingesetzt werden, ist dies der Trend. Hier muss zwingend vermieden werden, dass die einzelnen Gewerke wie Beleuchtung oder HKL mit autonomen Planungen beginnen. Gleichstromversorgung bedeutet mehr Kabel, passende Stecksysteme und potenzielle Abwärmeprobleme in Kombination mit einem nicht unerheblichen Raumbedarf. Gleichstrom ist nicht Wechselstrom. Die Planungs-Parameter und eine flächendeckende Auslegung unterscheiden sich deutlich.

- Sensoren und Aktoren in modernen Gebäuden haben alle Probleme, die je im Zusammenhang mit IoT diskutiert wurden. Viele der eingesetzten Produkte sind nie auf ihre Sicherheit überprüft worden. Dies geht hin bis zum Staubsauger oder der Kaffeemaschine. Nun ist es vielleicht egal oder maximal amüsant, wenn ein Hacker die Kaffeedosis umstellt oder die vorhandenen Staubsauger zu einem Rennen antreten lässt. Nicht egal ist aber, wenn die Mikrofone in zukünftigen Kaffeeautomaten (Alexa

Netzzugang zu Public Clouds

Fortsetzung von Seite 1

Dr.-Ing. Behrooz Moayeri hat viele Großprojekte mit dem Schwerpunkt standortübergreifende Kommunikation geleitet. Er gehört der Geschäftsleitung der ComConsult Beratung und Planung GmbH an und betätigt sich als Berater, Autor und Seminarleiter.

Typen von Cloud Services

Es wird zwischen verschiedenen Typen von Cloud Services unterschieden:

- Software as a Service (SaaS): Bei diesem Servicemodell ermöglicht der Cloud Provider dem Kunden die Nutzung einer Anwendung in der Cloud. Die Applikation ist über einen Web Browser oder eine andere Software auf dem Endgerät des Benutzers erreichbar. Der Cloud Provider administriert und betreibt die gesamte für die Anwendung erforderliche Infrastruktur, einschließlich des Netzes, der Server, der Betriebssysteme und des Speichers. Der Kunde kann höchstens eingeschränkte kundenspezifische Einstellungen der Anwendung vornehmen.

- Platform as a Service (PaaS): Dieses Servicemodell befähigt den Kunden zur Bereitstellung von eigenen Applikationen in der Cloud. Dabei kann der Kunde Programmierwerkzeuge, Bibliotheken und Dienste nutzen, die der Cloud Provider zur Verfügung stellt. Dieser administriert und steuert die zugrundliegende Cloud-Infrastruktur, einschließlich des Netzes, der Server, der Betriebssysteme und des Speichers. Der Kunde hat die administrative Hoheit über die auf diesem Servicetyp basierenden Anwendungen und kann möglicherweise die Umgebung, die von der Applikation genutzt wird, konfigurieren.

- Infrastructure as a Service (IaaS): Der IaaS Provider setzt den Kunden in die Lage, Prozessor-, Speicher- und Netz-Ressourcen in der Cloud in Betrieb zu nehmen. Der Kunde kann beliebige Software in der Cloud zur Ausführung bringen. Das schließt Applikationen und möglicherweise auch Betriebssysteme ein. Der Kunde hat keine Kontrolle über die Cloud-Infrastruktur, kann aber die eigenen Instanzen der Betriebssysteme, des Speichers und die eigene Anwendung steuern. Der Kunde hat möglicherweise auch eingeschränkten Zugriff auf Netz- und Sicherheitskomponenten wie Firewalls.

Die drei oben genannten verschiedenen Cloud-Servicemodelle sind in der Abbildung 1 dargestellt.

Je nachdem, welches der oben genannten Modelle genutzt wird, gibt es unterschiedliche Anforderungen an den Netzzugang zur Cloud. Diese Anforderungen sind in der Regel bei SaaS am einfachsten und bei IaaS am komplexesten. Bei SaaS kann der Kunde nicht viel in der Cloud steuern und benötigt daher einen relativ einfachen Zugang zur Cloud. Meistens reicht eine Internet-Verbindung zur Cloud. Dagegen kann ein IaaS-Kunde zum Beispiel die Anforderung haben, administrative Aufgaben wie Bereitstellung von Diensten und Applikationen sowie Datensicherung über einen anderen Netzkanal wahrzunehmen als der Kanal, der für Zugriffe der Benutzer auf die Applikationen in der Cloud eingesetzt wird.

Cloud Exchange

Damit die Nutzung einer Public Cloud nicht zu einer Einbahnstraße wird, auf der es kein Zurück mehr gibt, muss ein Unternehmen den Zugang zu Public Clouds

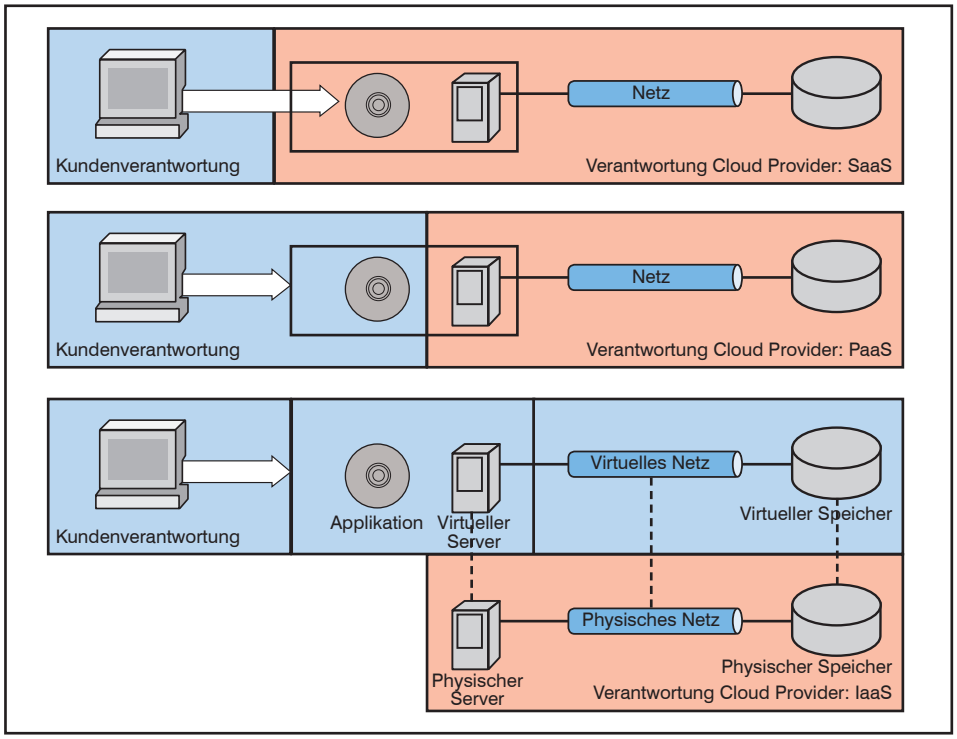


Abbildung 1: Cloud-Servicemodelle

möglichst offen gestalten. Im Falle eines reinen Internet-Zugangs ohne jegliche auf die Cloud zugeschnittene Besonderheit ist dies gegeben. In diesem Fall kann man von einer Cloud zur anderen wechseln, ohne den Netzzugang zur Cloud zu ändern. Andere Voraussetzungen müssen natürlich erfüllt werden. Insbesondere ist die Frage zu klären, wie man die Unternehmensdaten von einer zur anderen Cloud bewegen kann. Diese Frage ist kein Gegenstand des vorliegenden Beitrags, dessen Schwerpunkt der Netzzugang zur Cloud ist.

Der Netzzugang zur Cloud ist im Falle der reinen Internet-Nutzung maximal offen und Proivder-unabhängig. Was aber, wenn auf der Verbindung zur Public Cloud Bedingungen zu erfüllen sind, die eine Internet-Verbindung nicht erfüllen kann? Solche Bedingungen können zum Beispiel sein: Sicherstellung von Verfügbarkeits- und anderen Garantien im Rahmen eines Service Level Agreement (SLA) von Ende zu Ende, Quality of Service (QoS) oder Realisierung eines Übertragungskanals, der aus Sicherheitsgründen völlig unabhängig vom Internet sein soll?

Je stärker die Public Cloud einer Private Cloud ähneln soll, umso wahrscheinlicher ist es, dass man mit einer ausschließlichen Internet-Verbindung nicht auskommt. In einigen Fällen wird in einer Public Cloud zum Beispiel eine Virtual Private Cloud (VPC) gebildet. Eine VPC ist eine logisch getrennte Umgebung in der Public Cloud. Sie wird typischerweise im Zusammenhang mit IaaS genutzt. In einer VPC können in der Regel auch private IP-Adressen des Kunden eingesetzt werden. Der Zugang zu einer VPC muss ein zumindest logisch dedizierter Zugang sein, denn private IP-Adressen werden im Internet bekanntlich nicht geroutet (sonst wären sie nicht privat).

Man kann natürlich auch für den Zugang zu einer VPC das Internet nutzen, indem man im Internet ein Virtual Private Network (VPN) nutzt. Cloud Provider unterstützen solche Zugänge. In einigen Fällen will man aber die Nutzung einer VPC auch mit mehr SLA, QoS und Sicherheit verbinden als im Internet möglich ist. Dann entscheidet man sich für einen vom Internet unabhängigen Cloud-Zugang. Man kann zum Beispiel zu dem Standort des Cloud-Providers, an dem die VPC gebildet wird, eine Punkt-zu-Punkt-Verbindung aufbauen, oder diesen Standort in das eigene private Wide Area Network (WAN) einbinden. In beiden Fällen braucht man natürlich die Dienste eines WAN-Providers.

Nun stelle man sich vor, das Unternehmen möchte zu einer anderen Cloud wechseln oder eine andere Cloud zusätzlich nutzen. Bei einer dedizierten WAN-Anbindung pro Cloud werden viele teure WAN-Verbindungen erforderlich. Außerdem kennt man ja die relativ langen Bereitstellungszeiten für Anbindungen von Standorten an das WAN. Man kann nicht einfach, schnell und kostengünstig von einer Cloud zur anderen wechseln oder zusätzlich eine bisher nicht genutzte Public Cloud hinzufügen, wenn jedes Mal eine neue WAN-Verbindung erforderlich wird.

Das Problem wird noch komplexer, wenn die neue WAN-Verbindung aufgrund ihrer Kritikalität auch noch redundant sein muss.

Und es gibt einen weiteren Nachteil, wenn die Nutzung einer Public Cloud nicht isoliert erfolgt, sondern in Verbindung mit der Nutzung anderer Clouds. Man stelle sich zum Beispiel vor, dass in einer bestimmten Applikation auf die Daten einer anderen Applikation zugegriffen wird. Wenn sich die beiden Applikationen in verschiedenen Clouds befinden, dann werden für diese Kommunikation die WAN-Verbindungen zu beiden Clouds belastet. Außerdem entsteht eine höhere Latenz aufgrund der Nutzung von zwei WAN-Verbindungen.

Solche Probleme würden gar nicht entstehen, wenn es Standorte gäbe, an denen möglichst viele Cloud-Infrastrukturen zusammenkämen. Man baut einfach Verbindungen zu solchen Standorten auf, und nutzt diese Verbindungen gleich für den Zugriff auf mehrere Clouds. Innerhalb solcher Standorte könnten zwischen den Clouds direkte Verbindungen genutzt werden.

Die gute Nachricht ist, dass es solche Standorte gibt. Die Cloud Provider haben nämlich das gleiche Problem. Sie müssen ihre Standorte auch unter Rücksicht auf möglichst kurze Wege zu möglichst vielen Kunden und anderen Clouds auswählen. Also haben sich Knotenpunkte gebildet, nicht zufällig in räumlicher Nähe zu einem Internet-Knoten (Internet Exchange). Das nennt sich dann Cloud Exchange. Einige Firmen haben sich darauf spezialisiert, an solchen interessanten Standorten Flächen für Rechenzentren (RZs) anzubieten, mit allem was dazu gehört: Zutrittsschutz, redundante Stromversorgung mit skalierbarer Leistung, ausfallsichere Klimatisierung, Überwachung rund um die Uhr und eben auch redundante Netzzugänge. Anbieter wie Equinix, E-Shelter und Interxion betreiben solche Standorte, die man auch Co-Location nennt.

Die Nutzung von zwei Co-Locations für den Zugriff auf Public Clouds ist in der Abbildung 2 dargestellt.

Wie aus der Abbildung 2 hervorgeht, können aus Redundanzgründen zwei Co-Locations für den Zugang zu Public Clouds genutzt werden. An diesen Standorten

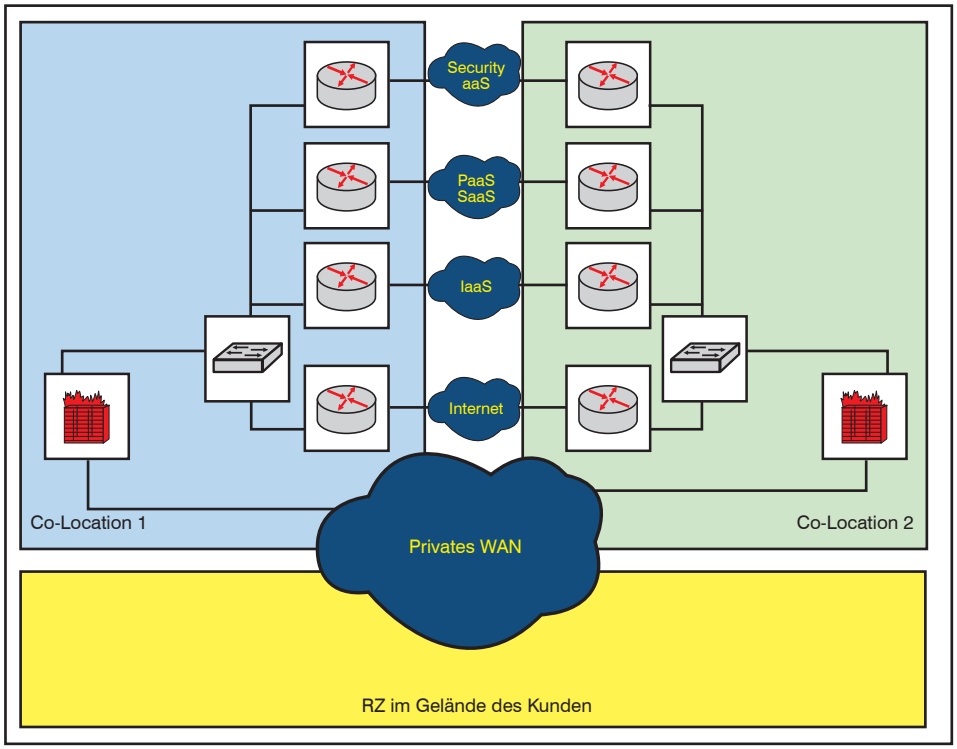


Abbildung 2: Nutzung von Co-Locations für den Zugang zu Public Clouds

Enterprise Server-based Storage: VMware vSAN

Fortsetzung von Seite 1

Dipl. Math. Cornelius Höchel-Winter ist Leiter des Technologie-Labors und des Bereichs Systemintegration bei der ComConsult Research GmbH. In dem Labor werden regelmäßig Messungen und Evaluierungen neuester Hard- und Softwareprodukte durchgeführt und ausgewertet. Herr Höchel-Winter besitzt langjährige Erfahrung in der Konzeptionierung, im Aufbau und Betrieb von RZ- und Campusnetzen und von Windows- und Linux-Umgebungen. So hat er als verantwortlicher Projektmanager die Rechenzentren und Netzwerke auf dem Gelände der EXPO2000 in Hannover aufgebaut und während der Weltausstellung betrieben. Für die ComConsult Akademie ist er außerdem seit 2001 als Autor, Trainer und Referent auf Seminaren und Kongressen schwerpunktmäßig in den Bereichen Data Center, Virtualisierung, Storage, Netzwerke und Cloud Computing tätig.

Schon lange gelten große, zentrale Speichersysteme als Kernkomponente der Datenhaltung in Unternehmensrechenzentren. Failover-Cluster und andere Redundanzmechanismen erfordern eine von den reinen Compute-Ressourcen unabhängige Datenhaltung. Aber spätestens mit dem Einzug der Virtualisierung von Servern wurde zentraler Speicher ein unverzichtbares Designelement im Rechenzentrum.

Der Grund hierfür ist einfach und liegt im Basiskonzept der Servervirtualisierung begründet: Virtuelle Maschinen werden unabhängig von konkreten physischen Ressourcen beschrieben und können daher prinzipiell auf beliebigen Virtualisierungshosts betrieben werden. Eines der wichtigsten Funktionsmerkmale der Servervirtualisierung ist daher die Möglichkeit, virtuelle Maschinen zur Laufzeit und unterbrechungsfrei auf andere Hosts verschieben zu können (bei VMware heißt dieses Feature vMotion, Microsoft und KVM nennen es Live Migration).

Alle Hypervisor-Hersteller unterstützen hierbei jetzt zwar das Verschieben der kompletten virtuellen Maschine inklusive zugeordneter virtueller Festplatten („Storage Migration“), jedoch ist es offensichtlich, dass solche Vorgänge deutlich mehr Zeit in Anspruch nehmen als wenn die Festplatten-Images auf einer zentralen Storage-Instanz liegen, auf die sowohl der Quell- als auch der Ziel-Host Zugriff haben, – von der zusätzlichen Last im Netzwerk ganz zu schweigen.

Das Verschieben aktiver virtueller Maschinen im laufenden Betrieb funktioniert nur dann innerhalb akzeptabel kurzer Zeitspannen, wenn nicht gleichzeitig mit der virtuellen Maschine – was in erster Linie der Hauptspeicher der virtuellen Maschine ist – auch die persistenten Daten, also die zugeordneten virtuellen Festplatten der Maschine bewegt werden müssen. (siehe Abbildung 1)

Das heißt:

1. Betriebskonzepte produktiver RZ-Umgebungen, die auf eine dynamische Positionierung von virtuellen Servern und auf ein automatisiertes Ausrollen neuer Workloads setzen, sind ohne zentralen Speicher kaum realisierbar.

2. Klassische lokale Festplatten in physischen Servern waren hierbei bislang eher hinderlich.

Die standardmäßige Realisierung des Zugriffs auf einen gemeinsamen zentralen Speicher erfolgt bislang durch die großen Speichersysteme von EMC², Dell, IBM, Hitachi, HP, NetApp etc., die wir heute in praktisch jedem Unternehmensrechenzentrum sehen.

Diese Storage-Appliances haben unbestreitbar große Vorteile wie:

- Alle (elektronische) Unternehmensdaten werden über ein System gehandhabt.
- Der gesamte oder Teile der physischen Speicherkapazität können als Pool im Rechenzentrum zur Verfügung gestellt und damit optimal ausgenutzt werden.
- Zugriffsrechte werden zentral verwaltet (wiewohl dies in der Regel nur auf der

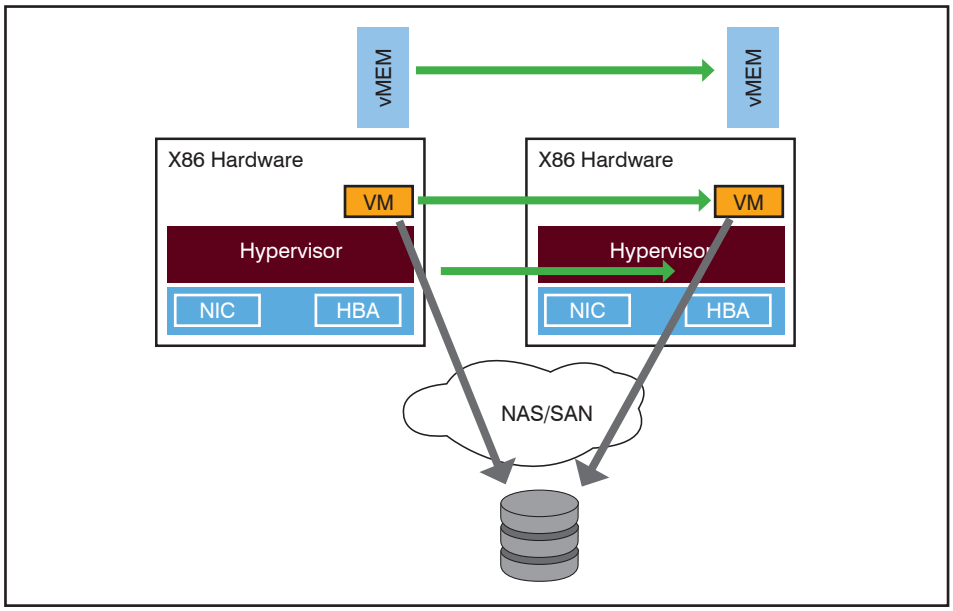


Abbildung 1: vMotion/Live Migration von virtuellen Maschinen

Ebene von LUNs oder Speicherbereichen und nicht auf Benutzer- oder Anwendungsebene erfolgen kann).
- Zentraler Speicher kann nach Bedarf zugeteilt werden.
- Es müssen wenige, meist lediglich zwei Systeme, die sich gegenseitig absichern, administriert werden.
- Die Systeme beherrschen eine überbordende Funktionsvielfalt.
- Hierzu gehören auch Möglichkeiten zu Datensicherung wie VTL (Virtual Tape Libraries) und Snapshots.

Die Nachteile solcher Appliances sind:

- Proprietäre Betriebssysteme und proprietäre Bedienoberflächen benötigen speziell zugeschnittenes Know-how.
- Spezial-Hardware und -Software, noch dazu in relativ kleinen Stückzahlen produziert, sind sehr teuer.
- Der Zugriff (Disk-IOs) erfolgt über wenige Netzwerkschnittstellen.
- Ein Ausbau der Speicherkapazität durch größere Festplatten oder zusätzliche Festplatten ist oft schwierig, aufwändig und meist klar begrenzt.
- Die Systeme skalieren damit eher schlecht als recht.
- Die Systeme sind wenig bis gar nicht in das Virtualisierungskonzept der Server integriert (Management, Automatisierung, Speicherzuordnung).
- Von Hardware-Unabhängigkeit kann keine Rede sein – ganz im Gegenteil.

Beim Einsatz von Fibre Channel kommen noch eine ganze Reihe weiterer Probleme hinzu:

- Die separate Netzwerk-Infrastruktur verursacht eine höhere Komplexität im RZ.
- Zum Betrieb dieser Infrastruktur muss separates Know-how (inkl. zusätzlicher Zertifizierungen) aufgebaut werden.
- Durch die zusätzliche Hardware (HBAs und FC-Switches) entstehen weitere Mehrkosten.
- Im Vergleich zu Ethernet ist Fibre Channel klar ins Hintertreffen geraten:
  - Ethernet bietet pro Port Geschwindigkeiten von 100 Gbit/s gegen maximal 32 Gbit/s bei Fibre Channel.
  - 40/100-Gbit-Ethernet-Komponenten sind kostengünstiger als 16/32-Gbit-FC-Komponenten.
  - Viele Server haben heute 10-Gbit-Ethernet-Schnittstellen auf dem Mainboard.
  - Ethernet-Fabrics skalieren deutlich höher als FC-Fabrics.
- Cloud-Umgebungen basieren auf IP! Damit können in der Cloud praktisch alle Storage-Protokolle unterstützt werden – aber nicht Fiber Channel.

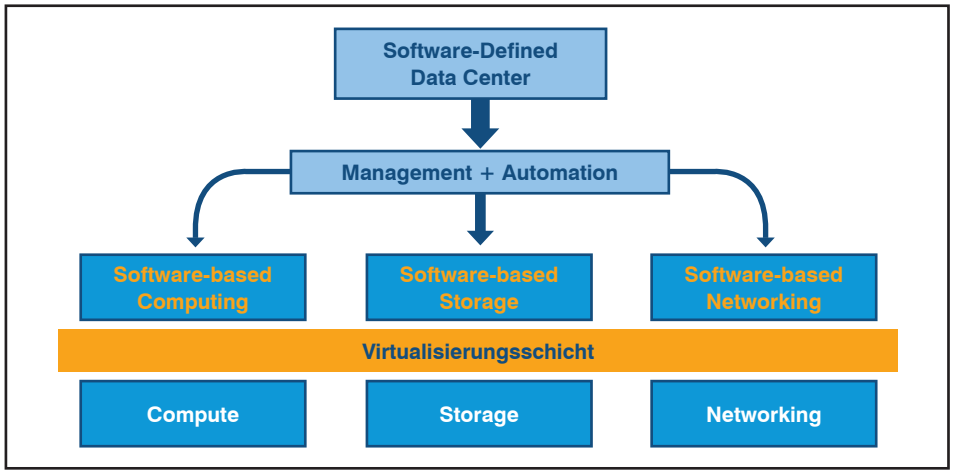


Abbildung 2: Software-defined Data Center

- Der Fibre-Channel-Markt schrumpft:
  - Die Umsätze gehen um 10 – 15 % pro Jahr zurück.
  - Die Anbieter von FC-Equipment werden immer weniger. Zuletzt hat Broadcom Brocade übernommen. Das verspricht keine fallenden Preise.

Alle Aspekte zusammen genommen passen diese Systeme damit jedoch in die alten, klassischen Betriebskonzepte unserer Rechenzentren: Der Betrieb von Servern, von Anwendungen, des Netzwerks und eben auch des Datenspeichers sind fein säuberlich voneinander getrennt und wird jeweils durch eine eigene Betriebsmannschaft geleistet. Mehr oder wenige strenge Vorgaben beschreiben die Schnittstellen zwischen den Technologien und ihrer Administratoren.

Die Speichersysteme selbst bzw. deren Hersteller verstärken diese Separierung von den anderen Betriebsbereichen durch proprietäre Betriebssysteme, proprietäre Bedienoberflächen und unüberschaubar viele Funktionsmerkmale, zugeschnitten exakt auf ihre Klientel.

Diese separierten Betriebskonzepte sind, wenn Sie sich auf den Weg zum SDDC (Software-defined Data Center) oder zur Private Cloud machen wollen, überholt und hinderlich.

Der Begriff „Software-defined Data Center“ steht im Kern für die durchgängige Automatisierung aller RZ-Ressourcen von Compute, Storage und Netzwerk und beschreibt damit die technologische Vorstufe zum Cloud Computing. Nur wenn wirklich alle betroffenen Ressourcen vollautomatisch oder zumindest per Mausklick einer virtuellen Anwendungsumgebung zur Verfügung gestellt werden können, kann die heutzutage notwendige schnelle Umsetzung von geschäftskritischen Projekten oder Kundenanforderungen gelingen – und das geht eben nur softwarebasierend. Der Aufbau dedizierter Hardware-Infrastrukturen und deren Betrieb dauert einfach zu lange.

Anforderungen an den Grundpfeiler „Storage“ des Software-defined Data Center sind daher:

Mit „Server-based Storage“ gibt es jetzt eine Speichertechnologie, die einige der oben angeführten Kritikpunkte adressiert, insbesondere:

- Integration in eine gemeinsame Administration und Management mit der Server-Virtualisierung,
- Hardware-Unabhängigkeit durch die Einführung einer Abstraktionsschicht auf der Basis von Standard-i386-Hardware,
- bessere Skalierbarkeit und Erweiterungsfähigkeiten.

Neben einer Reihe spezieller Produkten haben insbesondere die beiden großen Hypervisor-Hersteller VMware und Microsoft dieses Thema für sich entdeckt und in ihr Virtualisierungsportfolio aufgenommen. Im Folgenden wird die VMware Lösung vSAN detailliert betrachtet.

VMware vSAN

VMware hatte bereits 2014 unter dem Produktnamen „Virtual SAN“ begonnen ihre Version eines im Hypervisor integrierten Software-defined Storage zu veröffentlichen. Aus „Virtual SAN“ wurde dann im Laufe der nachfolgenden Versionen die heute übliche Bezeichnung vSAN.

vSAN wurde entwickelt, um lokalen Speicher in ESXi-Hosts zu verwenden und daraus einen verteilten, ausfallsicheren Speicher-Pool zu bauen. (siehe Abbildung 3)