# Leitfaden Cloud-Architektur

**Ausgabe vom: 2.5.2013**

**Autoren**


| Name | Firma |
|---|---|
| Roman Hochuli | Nexellent AG |
| Marco Kuendig | Cisco Systems GmbH |
| Cyrill Schildknecht | Steria Schweiz AG |
| Marco Schmid | itsystems AG |


Es wird darauf hingewiesen, dass nicht sämtliche Abschnitte und Kapitel in diesem Dokument die Meinung aller Autoren widerspiegeln.

# SUMMARY

Um die oft gepriesenen Vorteile von Cloud-Computing nutzbar zu machen, ist es wichtig, auch die technischen Aspekte der Architektur zu betrachten. Den Schlüssel zum Verständnis von Cloud-Computing als Werkzeug der IT-Industrialisierung insbesondere ist das ganzheitliche Verständnis von der Facility bis hin zum Client. Dieser Leitfaden geht daher auf die einzelnen Komponenten der Cloud-Computing-Architektur und deren Interaktion ein. Dabei liegt der Fokus auf „Private Infrastructure as a Service Clouds“.

Der Leitfaden strukturiert die Cloud-Computing-Architektur in sieben Schichten. Die Schichten selber werden durch Building-Blocks aufgebaut, welche einzelne Themenbereiche behandeln. Die Architektur erlaubt es, konkrete Implementationen von Clouds zu verstehen und selber zu erstellen. Es handelt sich um einen Bauplan für Private Infrastructure as a Service Clouds.

Die sieben Schichten der Architektur mit den primären Building-Blocks sind:

- Facility (Struktur, Datacenter, Cooling, Power)
- Hardware (Computing Nodes, Storage Nodes, Physical Network & Network Components)
- Virtual (Server Virtualization, Storage Virtualization, Network Virtualization)
- Service (Cloud Services, Operation Support Services, Business Support Services)
- Orchestration (Ressource Management, Workload Management, Process Management)
- Access (Cloud-Service-Portal, API, Cloud Integration, Cloud Federation)
- Client (Clouds, Client Applications, Client Services)

Die Spannweite der Architektur reicht von der Stromversorgung für das Rechenzentrum bis zu den Clients, mit welchen die Nutzer auf die Cloud zugreifen. Der Leitfaden hilft deshalb dabei, konkrete Implementationen von Clouds besser zu verstehen, unterstützt aber auch bei der Integration von Cloud Services, da der Kontext besser ersichtlich wird.

# INHALTSVERZEICHNIS

## ZIELGRUPPE

Das vorliegende Dokument richtet sich an Führungskräfte und Entscheidungsträger mit technischem Verständnis, welche direkten Einfluss auf die IT-Strategie ihres Unternehmens haben.

## MOTIVATION

Dem Dokument liegt die Motivation zugrunde, das Thema Cloud-Computing-Architektur in kompakter und prägnanter Art aufzubereiten und dies mit Blick auf den Schweizer Markt. Dieser Leitfaden, welcher insbesondere auch den technischen Bereich des Themas abdeckt, soll dazu beitragen, Unsicherheiten abzubauen und damit die Adaptierung von Cloud-Computing zu fördern.

## ÜBERSICHT

Cloud-Computing kann als neuer Ansatz der IT verstanden werden, der es ermöglicht, dynamisch erweiterbare und virtualisierte IT-Ressourcen über ein Netzwerk zu beziehen. Mit dem Einsatz von Cloud-Technologien können Benutzer mit unterschiedlichsten Endgeräten via Internet auf Applikationen, Speicher, Rechenleistung und weitere Ressourcen zugreifen, welche als Services angeboten werden. Die Vorteile für den Kunden sind Kostensenkung, hohe Verfügbarkeit, kürzere Time-to-Service durch Self-Service und einfache Skalierbarkeit.

Der Fokus dieses Dokuments liegt auf privaten Clouds im Bereich IaaS (Infrastructure as a Service), da insbesondere in diesem Bereich ein erhöhter Informationsbedarf besteht. Der in der Abbildung auf Seite 7 abgebildete Architektur-Blueprint wurde ursprünglich für Public Clouds entwickelt, er ist aber ebenfalls auf private Clouds anwendbar. Sollten Sie weiterführende Informationen benötigen, insbesondere zu Public Clouds, möchten wir Sie zur direkten Kontaktaufnahme mit den Autoren ermutigen.

# ENTWICKLUNGSSTADIEN AUF DEM WEG IN DIE CLOUD

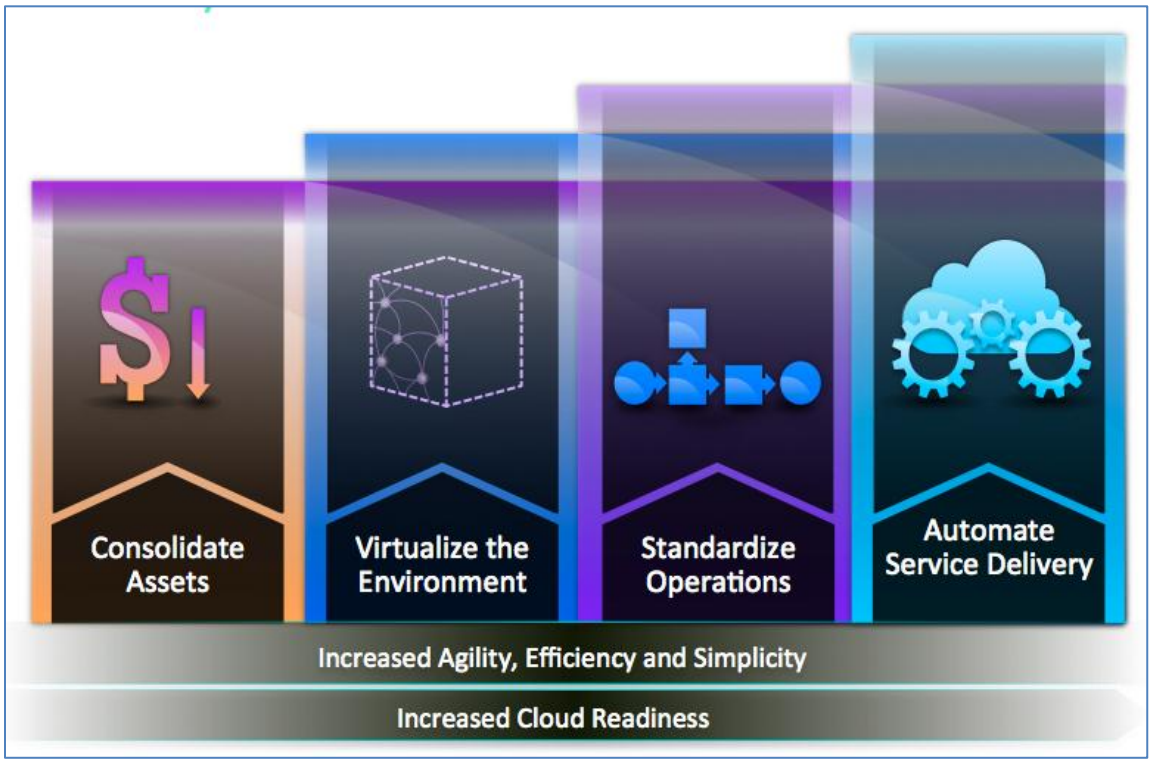


**ABBILDUNG 1 – DER WEG IN DIE CLOUD**

Viele Unternehmen befinden sich auf dem Weg in die Cloud. Die Grafik zeigt die verschiedenen Stufen, die durchlaufen werden müssen, um eine Cloud nach NIST-Definition[1] zu erhalten.

In der ersten Stufe der Konsolidierung werden physische Lokationen und einzelne Server zusammengenommen. Rechenzentrums- und Serverkonsolidierungsprojekte wurden vor ca. sechs bis acht Jahren bei vielen Unternehmen angestossen und dürften mittlerweile mehrheitlich abgeschlossen sein. Die Autoren kennen Unternehmen, die von 50 Rechenzentren auf vier konsolidiert haben und dadurch grosse operationelle Vorteile geschaffen und Kosten gesenkt haben. Die Virtualisierung der Server- und Storage-Ressourcen ist bei vielen Unternehmen in vollem Gange. Virtualisierungsraten von über 50% sind keine Seltenheit mehr und es sind auch Unternehmen bekannt, die bereits 95% aller physischen Server auf virtuellen Maschinen konsolidiert haben.

Bevor ein Automatisierungsprojekt gestartet werden kann, muss zwingend eine Standardisierung der IT-Dienstleistungsangebote gemacht werden. Nur standardisierte Leistungen können automatisch abgewickelt werden. Jede vom Standardkatalog abweichende Anforderung muss als eigenständiges Projekt abgewickelt werden und bindet wertvolle IT-Ressourcen. Viele Unternehmen haben begonnen, Ihre IT-Dienstleistungen zu dokumentieren, zu strukturieren und versuchen nun, ihre Angebote zu konsolidieren, um einen Standardkatalog von Dienstleistungen publizieren zu können. Jedes Automatisierungsprojekt ist also auch ein Standardisierungsprojekt. Das Standardisieren der Angebote ist fast schwieriger zu bewerkstelligen als das

[1] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Automatisieren der unterliegenden Infrastruktur. Sobald ein Servicekatalog vorliegt, kann mit der Implementierung der Automatisierung begonnen werden. Es ist relativ einfach, IaaS basierend auf simplen virtuellen Maschinen auf einer hochvirtualisierten Infrastruktur anzubieten. Das automatisierte Deployment von nichtvirtualisierten Maschinen hingegen ist nur mit speziellen Tools möglich, die sowohl virtuelles als auch nonvirtuelles Provisionieren beherrschen. Im Automatisierungsumfeld ist zudem ein Application Programming Interface (API) essentiell. Die Cloud-Architektur ist vollständig umgesetzt, wenn die User ihre Anything-as-a-Service-Dienstleistungen (XaaS) aus einem Servicekatalog beziehen können. Dieser Katalog listet alle Dienstleistungen auf und die User können diese selbständig bestellen und erhalten dank der Automatisierung innerhalb weniger Minuten Zugang zur provisionierten Dienstleistung.

Weitere Evolutionsschritte bilden Hybride Clouds oder eine vollständige Auslagerung der Ressourcen zu Cloud-Providern. Der Servicekatalog, welcher für die Private Cloud gebaut wurde, wird in diesem Fall nicht mehr gebraucht, um interne Dienste zu verwalten, sondern um die Angebote von verschiedenen Service-Providern im Katalog zu erfassen und zu verwalten.

Da eine Cloud sehr viele Bereiche abdeckt, gehen die Autoren in den nachfolgenden Kapiteln auf den Aufbau der Cloud-Architektur ein, gefolgt von den jeweiligen Detailbeschreibungen.

# ARCHITEKTUR

Der Cloud-Computing-Architektur-Blueprint ist in sieben Ebenen (Layer, Schichten) unterteilt. Die Architektur erstreckt sich von der Facility- bis hin zur Client-Ebene und umfasst damit ein Spektrum, welches vom Datacenter bis zur Nutzung der Cloud Services reicht. Innerhalb der Ebenen fassen Building-Blocks die unterschiedlichen Themenbereiche zusammen. Die nachstehende Grafik verdeutlicht die Situation:

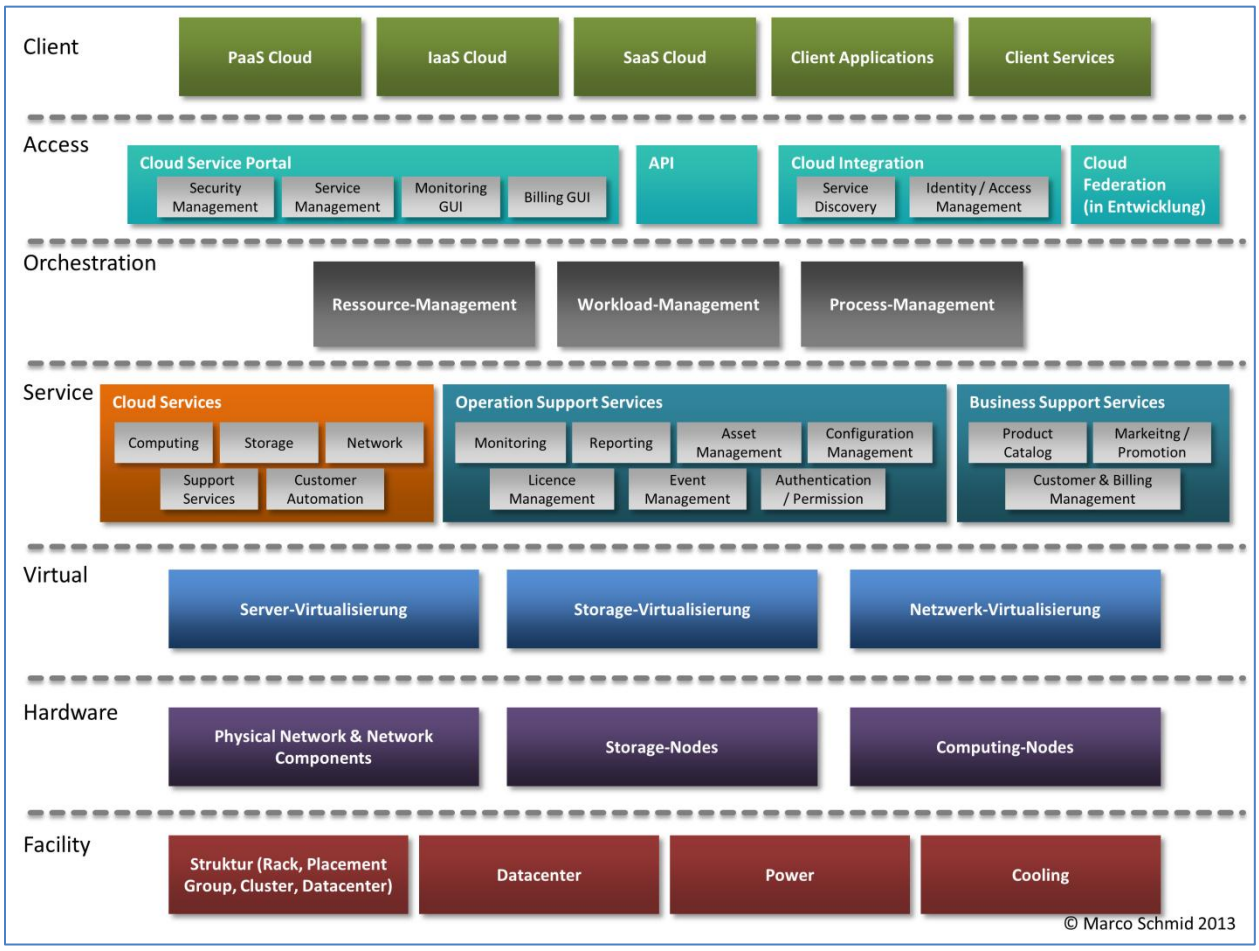


**ABBILDUNG 2 – CLOUD-COMPUTING-ARCHITEKTUR**

Die Ebenen dürfen nicht streng hierarchisch verstanden werden. Diese Architektur ermöglicht es, dass Services tieferer Ebenen direkt verwendet werden können und nicht immer sämtliche Layer verwendet werden müssen. Es gilt daher aber auch, dass die verschiedenen Schichten und Services nur eine lose Kopplung aufweisen. Eine starke Kopplung würde dazu führen, dass es kaum oder nur mit grossem Aufwand möglich wäre, Komponenten zu erweitern oder zu ersetzen.

In den folgenden Abschnitten wird nun auf die einzelnen Ebenen im Detail eingegangen.

## Client Layer

Der Client Layer bildet die oberste Architekturebene. Der Layer wird nicht durch den Cloud-Provider selber realisiert, sondern durch die Nutzer der Cloud. Trotzdem gehört er zur Gesamtarchitektur und soll daher thematisiert werden.

Der Cloud-Provider gibt durch die Gestaltung der Services zu einem gewissen Grad vor, wie die Cloud genutzt wird. Sind die Services sehr offen entworfen, können die Cloud Consumer weitgehend selber bestimmen, wie sie die Cloud nutzen wollen. Wird ein allgemeiner Computing und Storage Service angeboten, ist davon auszugehen, dass die Kunden die Services für unterschiedlichste Anwendungszwecke nutzen. Als Clients kommen fast alle denkbaren Systeme in Frage. Die Auswahl geht von Applikationen, welche auf die Ressourcen in der Cloud zugreifen, über mobile Endgeräte, welche einen – auf einer Computing-Instanz ausgeführten – Webservice benützen, bis hin zu anderen Clouds. Der Cloud-Provider muss demnach davon ausgehen, dass fast jede Art von Clients auf seine Services zugreifen könnte. Er passt daher seine Services nicht auf einen dedizierten Client an, sondern stellt sie lediglich mit möglichst standardisierten Zugriffsmöglichkeiten bereit. Es bleibt Sache des Kunden, wie diese genutzt werden. Dennoch ist es für den Provider interessant, Daten über die Nutzung zu sammeln. Daraus lassen sich Optimierungsmöglichkeiten ableiten oder gegebenenfalls neue Services anbieten. Folglich ist es auch sinnvoll, dem Kunden im Rahmen des Portals Feedbackmöglichkeiten zu bieten.

Eine Spezialität bei den Clients bilden andere Clouds oder Cloud-Service-Modelle: Wenn ein Cloud-Provider zusätzlich als Provider von Platform as a Service (PaaS) oder Software as a Service (SaaS) auftreten möchte, sollte er idealerweise als Basis eine IaaS-Cloud verwenden. Es gilt in diesen Fällen zu vermeiden, dass die aufsetzenden Cloud-Service-Modelle einen direkteren Zugang zu den Ressourcen erhalten oder direkt in die Orchestration eingreifen. Dadurch bleiben die höheren Servicemodelle lose gekoppelt und Änderungen in den verschiedenen Schichten der Cloud können weiterhin unabhängig voneinander durchgeführt werden.

## Access Layer

Der Zugriff auf Cloud-Ressourcen ist je nach Provider über verschiedene Zugangsarten möglich. Am gebräuchlichsten ist das Cloud-Service-Portal (oft auch Self-Service-Portal genannt).

### Cloud-Service-Portal

Das Cloud-Service-Portal ist ein webbasiertes Frontend, welches meist die vier folgenden Basisanforderungen erfüllt:

1. Zugriffssteuerung – wer darf auf die Cloud-Ressourcen und deren Verwaltung zugreifen?
2. Dienstverwaltung – Dienste auf- und abschalten
3. Monitoring – Übersicht über laufende Dienste erhalten
4. Billing – Übersicht über anfallende Kosten bekommen

Jede Cloud hat in irgendeiner Art ein Portal zur Verwaltung der Cloud-Ressourcen. Das Portal sieht je nach Lösung oder Provider etwas anders aus, erfüllt indes in den meisten Fällen die oben genannten Basisanforderungen. Das Portal bildet die zentrale Anlaufstelle für den Cloud-Konsumenten.

### API

Der Programmierschnittstelle, der API, kommt in der immer stärker werdenden Automatisierung der Cloud-Nutzung ein grosses Gewicht zu. In den meisten Fällen wird der Zugriff über ein modernes REST-API gewährleistet. Wenige, meist bereits etwas länger existierende Portale/Provider bieten einen sogenannten Webservice oder ein SOAP-API an. Als Grundsatz bei der Bewertung gilt: Je mehr publizierte Funktionen vom Cloud-Service-Portal auch via API zur Verfügung gestellt werden, desto besser. Im Optimalfall benutzt auch das Cloud-Service-Portal ausschliesslich das eigene API.

## ORCHESTRATION LAYER

Die Orchestration ist ein eher neues Konstrukt, welches zusammen mit Services Einzug in IT-Architekturen fand. Sie spielt auch in der Cloud-Computing-Architektur eine wichtige Rolle. Die Orchestration der Cloud wird oft als Management Layer missverstanden. Die Orchestrierung soll richtig verstanden werden als das Arrangieren sämtlicher Komponenten auf ein definiertes und gewünschtes Ergebnis hin. Der Begriff der Orchestrierung ist zwar im Bereich Infrastruktur noch neu, aber beispielsweise im Kontext von Services schon länger im Gebrauch. Gemäss IBM[2] wird Service-Orchestrierung folgendermassen definiert:

*Represents the prevalent mechanism for composing services into larger ones and building enterprise solutions out of services. - B. Lubinsky: Defining SOA as an Archtectural Style. IBM, Januar 2007*

Da in einer Cloud nicht nur Services, sondern auch physische und virtuelle Ressourcen beachtet werden müssen, lässt sich die Definition in erweiterter Form auf die Cloud übertragen. In dieser Definition beschreibt die Orchestrierung in der Cloud-Computing-Architektur die Möglichkeit, sämtliche Elemente im Hinblick auf ein definiertes Businessziel zu arrangieren. Nachstehend die Definition der Orchestrierung gemäss NIST:

*Orchestration refers to the composition of system components to support the Cloud Provider activities in arrangement, coordination, and management of computing resources in order to provide Cloud Services to Cloud Consumers. – P.Mell, T.Grance: The NIST Definition of Cloud Computing. NIST, September 2011*

Die Managementwerkzeuge sind wichtige Instrumente, um dieses Ziel zu erreichen, aber nur ein Teil des Layers. Zusätzlich kommen Rule und Workflow Engines zum Einsatz, welche es erlauben, Prozesse in der Cloud zu modellieren und automatisiert ausführen zu lassen. Nur durch diese Automatisierung lassen sich Cloud-Infrastrukturen stark skalieren und überhaupt in einem Self-Service-Betrieb anbieten.

Unterteilt wird der Layer in drei Bereiche:

1. Ressource Management
2. Workload Management
3. Process Management

## SERVICE

Im Service Layer werden die Komponenten sichtbar gemacht, welche sich auch als kleinste verrechenbare Einheit eines IT-Service verstehen. Grundsätzlich sind diese in drei Servicegruppen unterteilt:

1. Cloud Services
2. Operation Support Services
3. Business Support Services

Den Gruppen unterliegt ein Servicekatalog. Dieser ist so zusammengefasst, dass sowohl die zugrundeliegende Technologie als auch die Kundenanforderungen an den Service modular erfüllt werden können.

### Cloud Services

Sind die Grundkomponenten (Server Storage und Netzwerk) und deren Support-Services (Backup, Patchmanagement, Malware Defence) bereitgestellt, so gilt es, diese schnell, in der richtigen Menge und Zeit dem jeweiligen Service zur Verfügung zu stellen. Ziel ist es, skalierbare Ressourcen in Form von virtuellen Maschinen, aber auch Entwicklungsplattformen bedarfsgerecht (on Demand) bereitzustellen. Via Portal (meistens ein Webinterface) werden alle Komponenten in wählbaren Güteklassen dargestellt. Das Portal besitzt auch eine oder mehrere Programmierschnittstellen (API), über welche automatisiert zusätzliche, servicespezifische Informationen einfliessen können. Der Nutzer kann nun die Komponenten in der richtigen Menge und Qualität zu einem Service zusammenstellen und automatisiert in Betrieb nehmen.

Bekannte Anbieter für Cloud-Service-Werkzeuge sind: OpenStack, CloudStack, CloudFoundry, VMware vCloud Director, Cisco Cloupia.

### Operation Support Services

Die Operation Support Services beschreiben sämtliche Services, welche benötigt werden, um die eigentlich angebotenen Services zu betreiben. Dies geschieht heute meist komponentenübergreifend, so dass ganze Service- bzw. Auslieferketten (Netzwerk, Storage, Server) via Dashboard in einem einzelnen Werkzeug dargestellt werden.

Diese Werkzeuge sammeln permanent Daten aller Komponenten via Standardschnittstellen oder Agenten und legen diese in eine Configuration Management Database (CMDB) ab. Nun können diese Daten unterschiedlich verwendet werden: so im Servicemanagement zur Kontrolle der Service Level Agreements (SLA) in Form von Lizenzierungsnachweisen, Authentication-, Availability- oder Performance-Reports. Aber auch die IT Operations kann die Daten und Werkzeuge zur täglichen Unterstützung im Betrieb verwenden. Dies zum Beispiel, falls sie eine optimale Lastverteilung anstrebt oder falls sie Performance-Engpässen präventiv entgegenwirken möchte.

Bekannte Anbieter für Monitoringwerkzeuge sind: IBM Tivoli, BMC Patrol, VMware Operation Manager, HP Open View, Accelops, Nimsoft.

### Business Support Services

Sind die eigentlichen Cloud und Operation Support Services via Portal konfigurierbar, werden diese mit den Businessanforderungen in Einklang gebracht. Die für den Kunden verfügbaren und über das Portal wählbaren Services werden hier definiert und mit entsprechenden Preisen hinterlegt. Auch das Marketing kann die Business Support Services nutzen, um spezielle Angebote über das Self-Service-Portal oder verbundene Cloud Broker zu lancieren.

## Virtualization Layer

Vor ein paar Jahren war das Wort „Virtualisierung“ im X86-Server-Umfeld weitestgehend unbekannt. Bestenfalls einige Entwickler verstanden es damit ihre Testinfrastrukturen auf kleinstem Raum nachzustellen. Inzwischen ist es

Standard, die Funktion von der Physik abzukoppeln. In der Cloud-Architektur wird ein Grossteil dieser Techniken übernommen und konsequent weitergeführt.

### SERVERVIRTUALISIERUNG

Am besten bekannt ist die Servervirtualisierung. Hierbei wird mittels eines Hypervisors den Gastbetriebssystemen ein physikalischer x86-Server simuliert. Dies hat zwei Hauptvorteile:

1. Konsolidierung – Studien gehen davon aus, dass der durchschnittliche physikalische Server vor der Virtualisierung einen Auslastungsgrad von ca. 10% auswies. Indem man verschiedene Workloads auf derselben Physik betreibt, steigert man den Auslastungsgrad und kann kosteneffizienter arbeiten.
2. Vereinfachung der Wartung – vor der Virtualisierung musste man bei Ausfällen eines Servers (zum Beispiel wegen defekter Hardware oder geplanter Upgrades) langwierige Planungen vornehmen. Mit der Virtualisierung kann man einfach im laufenden Betrieb die virtuelle Maschine auf einen anderen Server verschieben und so den physikalischen Server für die Wartung freimachen.

Die bekanntesten Vertreter sind: VMware vCloud Suite, Microsoft Hyper-V, Open Source KVM.

### STORAGEVIRTUALISIERUNG

Der Haupttreiber für die Storagevirtualisierung ist neben der Vereinfachung der Wartung die Möglichkeit, gleichzeitig Storagesysteme verschiedener Hersteller im Backend zu nutzen. Die Investitionskosten für Storagesysteme sind meist im mittleren bis grossen Bereich anzusiedeln. Deshalb drängt es sich auf, Storagesysteme möglichst lange in Betrieb halten zu können. Dies ist teilweise auch der Fall, wenn deren Performance den aktuellen Bedarf nicht mehr zu decken vermag. Wenn man die Last durch Storagevirtualisierung über mehrere Backendsysteme verteilen und dadurch grosse Investitionen besser planen kann, ist ein grosses Ziel erreicht. Vielfach verfügen die Virtualisierungssysteme auch über Funktionen, welche die Backendsysteme selbst nicht kennen (zum Beispiel Mirroring/Replikation oder Continuous Data Protection).

Die bekanntesten Vertreter sind: DataCore SANsymphony, FalconStor NSS (IPStor), EMC VPLEX, NetApp V-Series.

### NETZWERKVIRTUALISIERUNG

Die Netzwerkvirtualisierung ist eine Folge der Servervirtualisierung. Die Serveradministrationen können inzwischen Kundenanforderungen extrem schnell und flexibel erfüllen. Die verantwortlichen Netzwerkadministratoren sind gefordert, neue Lösungen zu bieten, die nicht mehr nur auf VLANs aufbauen. Hier soll die Netzwerkvirtualisierung Abhilfe schaffen. Über das physikalische Netz wird eine Virtualisierungsschicht gelegt. Diese Schicht lebt grösstenteils innerhalb der Hypervisoren und spezialisierten Gateways zum physikalischen Netzwerk. Das Feld der Netzwerkvirtualisierung ist zum Zeitpunkt dieser Publikation noch sehr jung und volatil. Es existieren mehrere Protokolle (VXLAN, NVGRE, STT) – teils standardisiert via RFC/IEEE/IETF, teils proprietär – und es gibt unterschiedliche Ansichten, welche Features und Möglichkeiten eine Netzwerkvirtualisierung ausmachen. Kurzum, in diesem Bereich wird noch einiges in Bewegung bleiben, bis sich ein Industriekonsens durchgesetzt hat.

Aktuell aktivste Player in diesem Marktfeld sind: VMware NSX, OpenFlow, Cisco OnePK.

## HARDWARE LAYER

Die heutigen verfügbaren Cloud Services basieren mehrheitlich auf X86-Prozessor-Plattformen. Natürlich bieten Hersteller auch proprietäre Systeme basierend auf RISC-Prozessoren oder sogar Mainframes an, dies sind jedoch

sehr spezialisierte Anwendungsnischen. Dieser Artikel fokussiert mehrheitlich offene Plattformen und beschreibt daher keine Nischen. Um Cloud-Dienstleistungen bereitstellen zu können, müssen die klassischen Bereiche Compute, Netzwerk und Storage abgedeckt werden.

### Converged Platforms

Da Cloud-Infrastrukturen durch die Shared-Infrastruktur und die vielen Nutzer von Natur aus eine hohe Agilität bieten müssen, ist darauf zu achten, eine flexible, erweiterbare Infrastruktur zu schaffen. Moderne HW-Architekturen für Private Clouds basieren heute oft auf sogenannten Converged Platforms (CP). Eine CP bezieht so viele Bestandteile wie möglich von einem oder wenigen Herstellern.

Eine CP erlaubt es, eine Cloud-HW-Architektur in wenigen Wochen ab Bestellung in die Produktion zu überführen. Dies im Gegensatz zu traditionellen Architekturen, für welche voneinander unabhängig das Netzwerk, der Server und das Storagesystem evaluiert werden, um diese anschliessend im eigenen Unternehmen über mehrere Monate hinweg zusammenzuführen.

Die bekanntesten Converged Platforms sind laut dem Marktforscher Gartner Technology Research im Moment: Vblock, FlexPod, HP Matrix, HDS UCP, IBM Pure System.

### Compute Nodes

Compute Nodes sind die Bausteine, um CPU- und Memory-Ressourcen als Basis zur Verfügung zu stellen. Diese CPU-Systeme kommen üblicherweise von Intel oder AMD und werden von den Serverherstellern fix verbaut. Memory ist heute ein Commodity-Produkt und wird in Massen von verschiedenen asiatischen Herstellern gefertigt. Die CPU-Hersteller bringen in etwa alle neun bis zwölf Monate neue Prozessoren auf den Markt und die Serverhersteller verbauen diese Komponenten in neue Servergenerationen. Dies erlaubt es, Fortschritte in der Forschung schnell auf den Markt zu bringen. Es birgt aber die Nachteile, dass die ganze Lieferkette konstant neue Produkte entwickeln und vermarkten muss und dass die Endbenutzer ständig neue Server zur Auswahl haben. Die Standardisierung im Server-HW-Bereich bleibt also weiterhin eine Herausforderung.

Die Konnektivität der Serverkomponenten an das Netzwerk wurde in den vergangenen Jahren komplett virtualisiert. Massive Bandbreite wird in die Server eingeführt durch mehrfach 10-Gbit oder neu auch mit physischen 40-Gbit Verbindungen bis zum Server. Neue HW-Virtualisierungstechnologien erlauben es, diese Bandbreite intelligent zu nutzen. Durch PCI-Virtualisierung wird die Bandbreite in mehrere virtuelle Netzwerkkarten aufgesplittet. Dank diesem Evolutionsschritt können mehr Blade-Server für Cloud-Architekturen zum Einsatz kommen als vor fünf Jahren.

Des Weiteren werden sehr oft keine dedizierten SAN Ports mit Fibre-Channel mehr eingesetzt. Die Block-Storage-Verbindungen werden in den neueren Generationen via iSCSI oder FCoE über eine Unified Fabric in den Server geführt. Auch dies spart Platz im Server und erlaubt eine weitere Verdichtung der Serverressourcen.

Bekannte Anbieter von Compute Nodes sind HP, IBM, Dell, Cisco.

### Netzwerk-Nodes

Cloud-Architekturen bedingen heute sehr schnelle, sichere und intelligente Netzwerke. Durch Technologien wie Memory Migration oder vMotion werden enorme Datenmengen im Ost-West-Verfahren, also zwischen physischen Servern, transportiert.

10-Gbit-Ethernet hat sich als Commodity-Protokoll für Cloud-Infrastrukturen etabliert. Durch die Unified Fabric (siehe oben) wird auch der Storageverkehr auf dieser Ethernet-Plattform abgewickelt. Deshalb müssen Netzwerke intelligent sein und Bandbreitenreservationen sowie Bandbreitenmanagement (QoS) bei diesen Durchsätzen gewährleisten können. Da Cloud-Architekturen üblicherweise von mehreren Mandanten (mehreren Unternehmen oder Unternehmensbereichen) genutzt werden, müssen sichere Abtrennungsmöglichkeiten wie Lanes oder Partitionen für den Datenverkehr vorliegen. Die Netzwerk-Nodes sollten auch eine intelligente und einfach handhabbare Integration in die Network-Services-Bereiche bieten: Damit sind physische oder virtuelle Firewalls und Loadbalancer gemeint.

Bekannte Anbieter von Network Nodes sind Cisco, HP, Juniper.

### Storage Nodes

Eine zentrale Rolle in einer Cloud-Architektur kommt dem Datenspeicher zu. Obwohl der Fokus bei Architekturdiskussionen meist auf die Server und das Netzwerk gelegt wird, darf der Datenspeicher nicht in Vergessenheit geraten. Jeder, der einen kompletten Ausfall eines Storagesystems miterlebt hat, wird dies gerne bestätigen, denn ohne Zugriff auf den Datenspeicher funktioniert keine Virtuelle Maschine.

Klassisch wird bei Storage zwischen Block- und File-basierenden Systemen unterschieden. Die Grenzen zwischen diesen Systemen werden für den Anwender aber immer unschärfer, da die Hersteller mit sogenannten Unified-Storage-Systemen beide Varianten aus demselben System anbieten. Aus Sicht einer Cloud-Architektur sind inzwischen beide Varianten als gleichwertig anzusehen und bieten denselben Funktionsumfang und dasselbe Integrationsniveau.

Speicher wird heute in Tiers unterteilt. Diese gestalten sich nach den Anforderungen der Anwendung in Sachen Geschwindigkeit. Die Tiers werden vielfach mit Namen von Metallen oder Edelsteinen versehen, um dem Benutzer das Verständnis für die unterschiedlichen Qualitäten nahezubringen. Hinterlegt werden die Qualitätsunterschiede mit verschiedenen physikalischen Disk-Typen, Rotationsgeschwindigkeiten, RAID-Levels und allenfalls Datenspiegelungen auf Zweitsysteme an anderen Standorten. Die Grenzen zwischen den verschiedenen Tiers werden durch neuere Technologien, die verschiedene Qualitäten zu einem Pool verbinden und die Daten nach deren statistischem Interesse kontinuierlich automatisch verteilen, immer durchlässiger.

Bekannte Anbieter für Storage Nodes sind: EMC, NetApp, IBM, HDS.

Im Storagebereich ist eine sehr hohe Dynamik zu sehen und inzwischen treten fast täglich neue Players im X86-Storage ins Blickfeld: Swift, Whiptail, Nimble, Violin etc.

# Facility

In diesem Abschnitt ist eine Kurzfassung der sehr umfassenden Facility-relevanten Themen beschrieben. Um den reibungslosen Betrieb der Hardware einer Cloud-Plattform sicherzustellen, bedarf es einer Umgebung, die sicher, unterbrechungsfrei, kontrolliert und stabil ist.

Diese Umgebung findet man im Datacenter. Hier steht man vor der Entscheidung, ob man diese Umgebung selbst erstellen und betreiben will, was extrem hohe Investitionen und grosse operative Kosten mit sich bringt, oder man sich in einem Datacenter einmietet, bei welchem einem der Betreiber dies abnimmt. Heutzutage wird meist auf die zweite Option gesetzt, da es bei durchschnittlich grossen Datacenteranforderungen praktisch unmöglich ist, einen positiven Skalierungsfaktor zu erreichen. Zudem sind Facility-Projekte eher im Immobilienbereich mit Investitionshorizonten von zehn Jahren und mehr anzusiedeln. Diese Sicht passt schlicht nicht zu modernen ICT-Infrastrukturen, die meist nach drei bis vier Jahren das Ende Ihres Lebenszyklus erreicht haben, und ebensowenig zu den damit verbundenen Abschreibungszeiten.

Zu den weltweit grössten Betreibern zählen Equinix und Interxion, die beide in den meisten europäischen Ländern Datacenterinfrastrukturen betreiben.

### Floorspace/Rooms/Racks/Cabling

Zu den grundlegenden Anforderungen eines Datacenters gehört die Fläche. Datacenterbetreiber beginnen mit ihren Angeboten meist bei einem ganzen Rack. Einige Nischenanbieter offerieren auch geteilte Racks oder einzelne Höheneinheiten (Rack Unit oder kurz RU).

### Raised Floors / Hollow Ceilings

In Datacenters wird gewöhnlich mit sogenannten Raised Floors (Hohlboden) und Hollow Ceilings (Hohldecken) gearbeitet. Dabei ist der Boden, auf dem man sich bewegt oder die Racks stellt, höher als der Gebäudeboden. So schafft sich der Datacenterbetreiber einen Ort für die Führung von Stromverkabelung und Leitungen des Kühlkreislaufs. Die Hohldecke wird vielfach für die Verkabelung von Monitoringsystemen (Rauch/Feuer) oder die Erschliessung von Leuchtkörpern benutzt. Da mit Hardware gefüllte Racks schnell über eine Tonne wiegen können, muss ein Hohlboden die entsprechende Tragfähigkeit haben.

### Racks

In jedem Fall wird mit standardisierten 19-Zoll-Racks gearbeitet. Diese Racks gibt es aber in verschiedenen Ausführungen. Das kleinste – der Definition eines 19-Zoll-Racks entsprechend – ist ein Modell mit einer Grundfläche von 600 x 800 mm und 42 RU hoch. Hierbei ist neben dem 19-Zoll-Rahmen, in den die Geräte montiert werden, nur noch minimal Platz vorhanden. Dies macht eine saubere Kabelführung praktisch unmöglich. Auch beträgt die Bautiefe vieler Geräte heute bereits 1000 mm, und damit können diese Basis-Racks schlicht nicht mithalten. Am oberen Ende der Skala befinden sich momentan Racks mit einer Grundfläche von 800 x 1200 mm und 48 bis 52 RU. Hierbei hat auf allen Seiten genügend Platz für die Verkabelung und die Kabelführung. Auch kann man ohne weiteres Komponenten mit 1000 mm Bautiefe einsetzen.

### VERKABELUNG

Bei der Verkabelung wird heute meist ein „Daten-oben-Power-unten“-Ansatz verfolgt. So kann global vermieden werden, dass sich Daten- und Stromverkabelung kreuzen, und negative Einflüsse (Störung, Übersprechen etc.) können verhindert werden. Innerhalb des Racks kann dies mit einen „Power-hinten-Daten vorne“-Konzept weiter verfeinert werden, falls genügend Platz zur Verkabelung vorhanden ist. Auch Farbkonzepte bei Kupferverkabelung sind sehr beliebt, um eine sichtbare Separation verschiedener Netzwerksegmente herzustellen. Im Zeitalter von Unified Fabrics und Glasfaserverkabelung mit standardisierten Farben verschwindet dieses Konzept aber zusehends.

Die Stromverkabelung wird vom Datacenterbetreiber meist im Auftrag des Mieters selbst durchgeführt, dies um eine gleichbleibende Qualität und ein durchgängiges Konzept im gesamten Datacenter sicherzustellen. Die Stromverkabelung endet meistens auf Steckdosen, die entweder im Hohlboden oder im Rack montiert werden, und diese gelten als Service-Übergabepunkt zur Abgrenzung der Verantwortlichkeit.

### POWER

Ohne Strom läuft in einem Datacenter gar nichts. Entsprechend wichtig ist es, eine Stromversorgung zu haben, die genügend gross dimensioniert, redundant ausgelegt und auf Fehlerszenarien vorbereitet ist. Zu einem ganzheitlichen Konzept gehören mehrfache Erschliessungen des Datacenterstandorts von verschiedenen Unterwerken oder, in Ländern, in denen das möglich ist, von verschiedenen Netzbetreibern und mit leistungsstarken Notstromgeneratoren mit genügend Treibstoff, die den kompletten Datacenterbetrieb für eine definierte Zeit übernehmen können.

Theoretisch gesehen kann man ein Rack mit unendlich vielen Stromanschlüssen ausstatten. In der Realität wird man selten mehr als 3 x 32 A pro Rack antreffen. Der Grund dafür ist simpel: Praktisch jede Leistung, welche die Hardware bei der Arbeit verbraucht, wird in Form von Wärme wieder abgegeben. Das heisst, dass man zusätzlich zum verbrauchten Strom dieselbe Menge noch einmal in die Kühlung investieren muss. Hier stösst man irgendwann auf physikalische Grenzen. Diese Verdoppelung des benötigten Stroms für den Hardwarebetrieb erklärt auch die vergleichsweise hohen Rappen pro Kilowatt Preise für Strom im Datacenter zu normalen Industriestromtarifen.

### KÜHLUNG

Wie bereits im Kapitel „Power“ ausgeführt, produziert der Hardwarebetrieb Abwärme. Damit die Hardware betrieben werden kann, muss entsprechend für die Zuführung von kühler Luft gesorgt werden. Klassisch passiert dies im Datacenter in zwei Teilen: Ausserhalb des Datacenters stehen die platzintensiven Kühlmaschinen, welche die Kälte produzieren. Die Kälte wird über den externen Kühlkreislauf zum Wärmetauscher befördert. Beim Wärmetauscher wird die Kälte an den internen Kühlkreislauf abgegeben und die Abwärme der Hardware aufgenommen. Der externe Kühlkreislauf transportiert diese Wärme dann wieder zu den Kühlmaschinen und der Kreislauf beginnt von vorne. Zweitens nimmt der interne Kühlkreislauf die Kälte am Wärmetauscher auf und transportiert diese zu den einzelnen Kühlgeräten in den Räumen des Datacenters. Die Kälte wird im gleichen Wärmetauscherprinzip dazu benutzt, um der Raumluft die Wärme zu entziehen und so den Raum zu kühlen. Die nun erwärmte Kühlflüssigkeit wird zum Wärmetauscher mit dem externen Kühlkreislauf gebracht, um die aufgenommene Wärme abzugeben. Damit dieses Konzept funktioniert, benötigt man grosse Pumpanlagen, welche die beiden geschlossenen Kühlkreisläufe in Betrieb halten. Diese wiederum brauchen Strom für den Betrieb. Die Kühlmaschinen beinhalten Ventilatoren und Kompressoren und benötigen ebenfalls Strom. Je mehr Kühlung man benötigt, desto mehr Energie wird gebraucht.

Die Temperaturen, innerhalb derer die heutige Hardware betrieben werden darf, liegen normalerweise im Bereich von ~ 18 °C bis ~ 30 °C. Je höher die Temperatur der zugeführten Luft sein darf, desto weniger Kühlung bedarf es, und, direkt damit verbunden, weniger Strom beim Produzieren von kalter Luft. Daher wundert es nicht, dass Grössen wie Google und Facebook Druck auf die Hersteller der Hardware ausüben, dass diese die erlaubten Arbeitstemperaturen erhöhen.

### Security

Eine zentrale Funktion eines Datacenters ist es, die physikalische Sicherheit der darin betriebenen Hardware und der damit verbundenen Daten zu gewährleisten. Dies kann nur erreicht werden durch ein durchgängiges Sicherheitskonzept, die nahtlose Überwachung der Infrastruktur und die Nachverfolgbarkeit aller Zugriffe. Dazu gibt es Standards, die von den meisten Audit-Gesellschaften anerkannt werden (ISO27k/SAS70) und an denen sich die meisten Datacenterbetreiber orientieren.

### Risikomanagement

Die beste Sicherheitsmassnahme ist jedoch immer noch, sich über die Probleme und potenzielle Lücken im Klaren zu sein. Die einzige Möglichkeit dabei bildet ein institutionalisiertes Risikomanagement, wie es auch ISO27k bedingt. Die kontinuierliche Analyse jeglicher aufgetretenen Probleme und Fehlerfälle sowie die Umsetzung von Massnahmen zur Verbesserung oder Linderung von Auswirkungen müssen erfolgen. Diese Prozesse müssen offen, transparent und ohne Schuldzuweisungen stattfinden. Nur so kann gewährleistet werden, dass eine offene Fehlerkultur gelebt werden kann.

Das Risiko „Mensch“ ist in den meisten technischen Systemen das grösste: Wo Menschen arbeiten, sind Fehler möglich. Indem man sich mit den gemachten Fehlern auseinandersetzt, kann man Strategien und Prozesse entwickeln, damit diese Fehler nicht wieder passieren.

## Schlusswort und Kommentar der Arbeitsgruppe

Die zur Erstellung dieses Dokuments gebildete Arbeitsgruppe setzt sich aus Personen mit sehr unterschiedlichen Hintergründen zusammen. Bei der Erarbeitung zeigte sich, dass zu einzelnen Themen unterschiedliche Meinungen bestehen, und man konnte sich nicht immer einigen bzw. repräsentieren die festgehaltenen Inhalte nicht die Meinung jedes einzelnen Mitglieds der Arbeitsgruppe. Dies verdeutlicht auch, dass nach wie vor einzelne Komponenten der Cloud-Architektur in der Entwicklung sind und man sich noch nicht in allen Bereichen einig ist, wie die Implementierung zu erfolgen hat. Auch möchte die Arbeitsgruppe darauf hinweisen, dass es sich bei dem Dokument um eine Momentaufnahme handelt.