Cloud Computing Plattformen
Cloud Infrastrukturen und Cloud Security
Detailliertes Inhaltsverzeichnis

1 Der Trend: Cloud Computing
1.1 IT im Wandel
1.2 Wachstumsmarkt Cloud
1.3 Die Motivation aus Kundensicht
1.3.1 Verfügbarkeit des Business
1.3.2 Von fixen zu variablen Kosten
1.3.3 Agile Infrastruktur
1.3.4 Technologisch immer aktuell
1.3.5 Hohe Ressourcen-Ausnutzung und Energieeffizienz
1.3.6 Hohe Performance, Verfügbarkeit und Servicequalität
1.3.7 Sicherheit und Compliance
1.3.8 Kostenreduktion und Zeitersparnis
1.4 Typische Herausforderungen und Einwände
1.4.1 Herausforderungen beim Cloud Computing
1.4.2 Sicherheit beim Cloud Computing
1.5 Virtualization – Enabler für Cloud Computing
1.6 Definition: Cloud Computing
1.6.1 Service-Modelle des Cloud Computings
1.6.2 Die verschiedenen Cloud-Varianten
1.6.3 Multi-Cloud
1.7 Typische Services aus der Cloud
1.7.1 Typische Services
1.7.2 Praktische Umsetzung
1.8 Grid Computing

2 Server- und Desktop-Virtualisierung
2.1 Server-Zentralisierung
2.1.1 Vorteile: Schnelles Provisioning und Pooling
2.1.2 Vorteile: Automation und Hochverfügbarkeit
2.1.3 Vorteile: Konsolidierung und Green IT
2.2 VMware, KVM, Xen und Hyper-V im Vergleich
2.3 Server-Virtualisierung mittels VMware
2.3.1 Aufgaben der Virtualisierungsschicht
2.3.2 CPU-Virtualisierung
2.3.3 Arbeitsspeicher
2.3.4 Virtuelle Netzwerke
2.3.5 Festplatten und Laufwerke
2.3.6 Werdegang von VMware
2.3.7 Die Produktpalette
2.3.8 Lizenzierung in vSphere 6
2.4 Einsatzgebiete und Nutzen der Server-Virtualisierung (VMware)
2.4.1 Migration virtueller Maschinen
2.4.2 vMotion
2.4.3 Storage vMotion
2.4.4 Cross-Host vMotion
2.4.5 Long Distance vMotion
2.4.6 Distributed Resource Scheduling (DRS)
2.4.7 Distributed Power Management (DPM)
2.4.8 High Availability (HA)
2.4.9 Fault Tolerance
2.5 Hyper-V
2.6 Citrix XenServer
2.7 KVM
2.7.1 QEMU
2.7.2 libvirt
2.8 Vagrant

2.9 Container-Virtualisierung
2.9.1 Linux Containers (LXC)
2.9.2 LXD (Linux Container Hypervisor)
2.10 Docker
2.11 Server Hard- und Software
2.12 Virtual Desktop Infrastructure

3 Modernes Data Center Design
3.1 Klassische Methoden der Netzwerkvirtualisierung
3.2 Data Center Network Design
3.3 Rechenzentrums-Infrastruktur
3.4 Service Virtualization
3.5 Data Center Design Trends
3.6 Die Hersteller
3.6.1 HP
3.6.2 Brocade
3.6.3 Cisco

4 Das Netzwerk im Wandel
4.1 Das Netzwerk im Wandel
4.1.1 Shortest Path Bridging (SPB)
4.1.2 Transparent Interconnection of Lots of Links (TRILL)
4.1.3 FabricPath
4.1.4 Beispiel: VCS von Brocade
4.2 Overlay-Netze
4.2.1 VXLAN-Tunnel
4.2.2 NVGRE
4.2.3 Overlay Transport Virtualization – OTV
4.3 Der Switch auf dem Server
4.3.1 Nexus 1000V: Die Vorteile
4.4 Netzwerk und Applikation
4.4.1 Die Idee
4.5 Definition von SDN
4.5.1 Stimmen zu SDN
4.5.2 Der SDN-Markt
4.5.3 Klassische Router/Switch-Netze
4.5.4 Software Defined Networking
4.5.5 Substruktur der Control Plane
4.5.6 Vernetzung mit SDN
4.5.7 Bewertung der Konzepte
4.5.8 Entwicklungen zu SDN hin: Switch Cluster
4.6 Open Networking Foundation
4.7 OpenDaylight
4.8 Architektur des Controllers
4.8.1 Der Service Abstraction Layer
4.8.2 Erreichbarkeit des Controllers
4.8.3 Positionierung des Controllers
4.9 North- & Southbound Protocols
4.9.1 Netconf
4.9.2 Openflow-Architektur
4.9.3 Ein Cisco Ansatz: OpFlex
4.10 Übersicht: Controller-Produkte
4.10.1 Open Source in der Übersicht
4.10.2 Hersteller in der Übersicht
4.11 Application Centric Infrastructure (ACI) von Cisco
4.11.1 Application Policy Infrastructure Controller - Enterprise Module (APIC-EM)
4.12 VMware NSX
4.13 Network Function Virtualisation
4.13.1 NFV Rahmenwerk
4.13.2 Virtualisierung auf Routern und Switches
4.13.3 Virtualisierung von IMS und EPC

4.13.4 Virtualisierung des Home Networks
4.13.5 Integration von NFV in SDN
4.13.6 Chancen für den Provider
4.13.7 Risiken für den Provider
4.14 Auswirkungen von Cloud auf das Netzwerk

5 Speicherkonsolidierung und -Virtualisierung
5.1 Bedeutung des Datenspeichers
5.1.1 Direct Attached Storage
5.2 Netzwerkstorage
5.2.1 Network Attached Storage
5.2.2 Storage Area Networks
5.3 Die Cisco-Produkte und deren Positionierung
5.4 Die Brocade-Produkte und deren Positionierung
5.5 NFS, iSCSI, FC und FCoE im Vergleich
5.6 Datenspeicher in der Cloud
5.7 Storage-Konsolidierung und Datendeduplizierung
5.8 Speichervirtualisierung
5.8.1 Speichersystem-basierte Virtualisierung
5.8.2 Network-based Virtualization
5.8.3 Virtualization Appliances
5.8.4 Kernfragen bei der Auswahl von Virtualisierungstechniken
5.8.5 Storage Virtualisierung – Herstellerüberblick
5.9 Storage-Markt
5.10 Software-Defined Storage
5.10.1 Ceph
5.10.2 GlusterFS
5.10.3 VMware Virtual SAN
5.10.4 EMC ViPR

6 Das Software-Defined Data Center
6.1 Das Software-Defined Data Center
6.2 VMware Cloud in drei Ebenen
6.2.1 End-User Computing
6.2.2 Cloud-Anwendungsplattform
6.3 vCloud Suite (Cloud Infrastruktur und Management)
6.3.1 Abstraktion der Ressourcen
6.3.2 Disaster Recovery
6.3.3 vRealize Operations
6.3.4 vRealize Automation
6.4 Erweiterungen
6.5 Ausblick: Microsoft Azure Pack
6.6 OpenStack
6.6.1 Merkmale von OpenStack I
6.6.2 Module von OpenStack

7 Server-Hardware, konvergente und hyperkonvergente Systeme
7.1 Der Server-Markt
7.2 Cisco Unified Computing System
7.2.1 Cisco UCS B-Series
7.2.2 Die C-Series Server
7.2.3 Cisco UCS Mini
7.3 HPE c-Class Series
7.3.1 HPE Rackmount Servers
7.4 Dell
7.5 Lenovo
7.6 Komplettlösungen
7.6.1 FlexPod – Cisco und NetApp
7.6.2 Vblock
7.6.3 EMC VSPEX
7.7 Entwicklungsstufen der DC-Infrastruktur

7.8 Hyperkonvergente Systeme (Hyper Convergence)
7.8.1 SimpliVity
7.8.2 NUTANIX
7.8.3 Dell EMC VxRail
7.8.4 Cisco HyperFlex HX Data Platform

8 WAN-Anbindung
8.1 WAN Basics
8.1.1 WDM zwischen den Rechenzentren
8.1.2 Redundanzkonzepte
8.1.3 Synchrones und asynchrones Mirroring
8.2 Die Anforderungen der Anwendungen
8.2.1 Typische Stolperfallen
8.2.2 Mögliche Lösungen
8.3 Applikationsbeschleuniger
8.3.1 Beispiel: Cisco vWAAS
8.4 SD-WAN
8.4.1 Cisco Intelligent WAN (iWAN)
8.5 Cloud-untaugliche Anwendungen

9 Management-Zugriff auf die Cloud
9.1 Zugriff mit SNMP
9.1.1 SNMPv1 und SNMPv2c
9.1.2 SNMP v3
9.2 Cloud Management Tools
9.2.1 Beispiel einer Cloud NMS-Struktur
9.2.2 Netzwerkmanagementsysteme
9.2.3 Element Manager – Z. B. vCenter Server von VMware
9.2.4 Element Manager – Cisco UCS Manager
9.2.5 Ende-zu-Ende Management –Z.B. BMC BladeLogic

10 Transition Phase und Fallstricke
10.1 Transition Phase
10.1.1 Technische Planung
10.1.2 Organisatorische Planung
10.2 Fallstricke

11 Aufbau eines DC aus Sicht der Security
11.1 Cloud Security Basics
11.2 Cloud Security – Organisatorische Aspekte
11.2.1 Multi-Cloud
11.2.2 Verantwortlichkeiten bei der Cloud Security
11.3 Physischer Zugriff
11.4 Netzwerk-Security in virtualisierten Umgebungen
11.5 Data Center Edge Security
11.6 Data Center Core Security
11.7 Security im Aggregation Layer
11.7.1 IP Access-Listen
11.7.2 Quality of Service
11.8 Sicherheit im Access-Bereich
11.9 Virtualization
11.10 Einführung in die SAN Security

12 Network Security
12.1 Service Virtualization
12.1.1 Virtuelle Firewalls – Contexte
12.1.2 Lokales Server Load Balancing
12.2 Next Generation Firewalls
12.2.1 Stateful Inspection
12.2.2 Content Awareness and URL-Filtering
12.2.3 Bot Detection

12.2.4 IDS und IPS
12.2.5 Malware Protection
12.2.6 Identity Based Firewalling
12.2.7 Markt und Funktionsübersicht
12.2.8 Fortinet
12.2.9 ASA – Cisco Systems
12.2.10 Palo Alto
12.3 Security und Network Function Virtualization
12.3.1 Sicherheitslücken von NFV
12.3.2 Schutzmaßnahmen
12.3.3 NFV Security Management Lifecycle
12.3.4 NFV Security Framework
12.4 Konzepte mit SDN
12.4.1 Definition des VNF Forwarding Graph
12.4.2 Realisierung des VNF FG
12.4.3 Vorteile des VNF FG
12.5 Beispiel anhand von ACI von Cisco
12.5.1 Nutzung von Device Packages
12.5.2 Service Graphs Templates

13 Virtualization Security
13.1 Server Security in virtualisierten Umgebungen
13.2 Hypervisor-Security
13.2.1 VMware
13.2.2 KVM
13.2.3 Hyper-V
13.2.4 Container-Virtualisierung (Docker)
13.3 Beispiel anhand von Cisco
13.3.1 VXLAN
13.3.2 Cisco Prime Network Services Controller
13.3.3 Cisco Virtual Security Gateway (VSG)
13.3.4 Cisco ASAv
13.4 Beispiel anhand von OpenStack
13.5 Beispiel anhand von VMware NSX
13.5.1 NSX Distributed Firewall
13.5.2 Edge Devices
13.5.3 Check Point vSec

14 Workplace Security
14.1 Sicherheitsmaßnahmen für Clients
14.1.1 Virenschutzprogramme
14.1.2 Personal Firewalls
14.1.3 Patch Management
14.1.4 Festplattenverschlüsselung
14.2 Security-Awareness-Maßnahmen
14.2.1 Die Benutzer einbinden
14.2.2 Gründe offenbaren
14.2.3 Einschränkungen begreifbar machen
14.3 Cisco AMP
14.4 Der Begriff des Proxies
14.4.1 Transparente Proxies
14.4.2 Reverse Proxies
14.4.3 Generische Proxies
14.4.4 Applikation Layer Gateways
14.4.5 Arbeitsweise
14.4.6 Limitierungen
14.4.7 Web Proxies
14.4.8 Authentisierung an der Firewall
14.5 Mail Relays
14.6 Markt und Funktionsübersicht
14.6.1 Blue Coat Proxy Appliance

14.6.2 Zscaler
14.6.3 Forcepoint
14.6.4 Cisco IronPort - Web Security Appliance
14.7 Die Mobility Story – BYOD
14.7.1 Mobile Endgeräte angreifen
14.7.2 Mobile Device Management
14.7.3 VDI und Gruppenrichtlinien
14.8 DNS-Layer Security

15 Identity & Access Management
15.1 User-Accounts und Passwörter
15.1.1 Zugriff per CLI
15.1.2 Default-Parameter
15.2 Identity Management
15.2.1 Zentrale User-Verwaltung
15.2.2 Was ist ein Verzeichnisdienst?
15.2.3 Active Directory Domain Services
15.3 Markt und Funktionsübersicht
15.3.1 Free Radius
15.3.2 Windows Server
15.3.3 Cisco Identity Services Engine (ISE)
15.4 Informationen über die User-Aktivität
15.5 Beispiel: Microsoft Azure Active Directory
15.6 Security und Identity Management
15.7 Beispiel: Keystone von OpenStack

16 Zugriff auf die Cloud
16.1 Aufbau von Cloud- Infrastrukturen
16.1.1 Public Cloud: Was gilt es zu beachten?
16.1.2 Hybrid Cloud: Auswirkungen auf alle Layer
16.2 VPNs im Überblick
16.2.1 MPLS-VPNs
16.2.2 IP-VPNs
16.3 VPN Gateways zur Cloud-Anbindung
16.3.1 virtueller Router (CSR1000v)
16.3.2 Beispiel virtueller Edge Router: Juniper vMX
16.3.3 Cloud based VPN
16.4 Beispiel: MS Express Route
16.5 vCloud Air Hybrid Cloud Manager
16.6 Cisco CloudCenter
16.7 SaaS-Einbindung
16.7.1 Schatten-IT
16.7.2 Schatten-IT-Risiko-Assessment
16.7.3 CASB und CASM
16.8 Applikationssicherheit in Cloud-Umgebungen
16.8.1 OWASP Top 10