Hauptseminar Virtualisierung von IT-Systemen: Herausforderungen und Risiken

Block A: Netz- und Speichervirtualisierung

A1: Virtualiserung von Netzen (VLAN, VPN, VNET)

- Inhalt: Das Thema Virtualisierung im Netzen bewegt die IT-Welt bereits seit mehreren Jahren und wird hauptsächlich durch verbesserte Flexibilität des Netzes und erhöhte Sicherheit motiviert. Derzeit wird die Virtualisierung in Netzen hauptsächlich mit zwei Begriffen in Verbindung gebracht: VLAN (Virtual Local Area Network) und VPN (Virtual Private Network). In dieser Arbeit sollen Motivation, Hintergründe, Einsatzgebiete und Techniken von unterschiedlichen Netzvirtualisierungstechnologien dargestellt werden. Weiterhin soll gezeigt werden, welche Vorteile sie mit sich bringen und welche Probleme sie verursachen.
- Literatur:
  - VLAN – mit virtuellen Netzen zu mehr Sicherheit und Komfort
  - Virtual Local Area Networks, Überblick
  - How Virtual Private Networks Work, Überblick
  - VPN - Virtual Private Network
  - VPNs and WAN Evolution & weitere Links

A2: Trend zur Virtual Infrastructure (VRouter, VFirewall) – Virtualisierung von Komponenten

- Inhalt: Virtualisierung von Netzen erfordert die Trennung von Verkehrsströmen und Adressräumen, um "private" Kommunikationspfade über eine gemeinsam verwendete Infrastruktur zu ermöglichen. Das Gebiet Netzvirtualisierung umspannt im Wesentlichen drei Problemstellungen:
  - Virtualisierung von Netzkomponenten: Wie kann die Netzvirtualisierung in Netzkomponenten verschiedener Schichten (z.B. Schichten 2, 3, 4) realisiert werden?
  - Virtualisierung von Netzpfaden: Wie können Verkehrsströme entlang eines virtuellen Pfades geführt und isoliert werden?
  - Control Plane: Die Virtualisierung von Netzpfaden führt zur Einrichtung von Overlay-Topologien. Welche Änderungen an Routing-Verfahren werden dadurch erforderlich?
- In der Arbeit sollen die Möglichkeiten und technischen Optionen in der Virtualisierung von Netzkomponenten mit ihren spezifischen Vor- und Nachteilen sowie die Konsequenzen für den Aufbau und das Management von virtuellen Netzen dargestellt werden. Insbesondere sollten folgende Ansätze dargestellt werden:
  - Virtuelle Switches
  - Virtual Routing and Forwarding (VRF), Virtual Forwarding Instances (VFI), logische und virtuelle Router
  - Virtuelle Firewalls
- Literatur:
  - Moreno, V, Reddy, K: A Virtualization Technologies Primer

- Moreno, V, Reddy, K:Network Virtualization (relevante Kapitel werden zur Verfügung gestellt)
- Maier, S., Grau, A.: A Comparison of Virtual Routing and Virtual Machines, Proceedings of the IEEE Symposium on Computers and Communications (ISCC'07), Aveiro, Portugal, July 1-4, pp. 395-402
- LRZ: Virtuelle Firewalls für Institutsnetze

A3: Virtualisierung von Speichern

- Inhalt: Speichervirtualisierung ist eines der aktuellen Schlagworte der IT-Industrie, spätestens seit der zunehmenden Akzeptanz "vernetzter Speicher" in organisationsübergreifenden Anwendungen. Trotz dieses Interesses herrscht jedoch nach wie vor eine nicht unerhebliche Verwirrung, da der Begriff "Virtualisierung" bei Speichern in unterschiedlichen Ausprägungen in der Industrie und Wissenschaft verwendet wird. In dieser Arbeit sollen deshalb die Motivation, Hintergründe, Vor- und Nachteile sowie Techniken von Speichervirtualisierungen aus einer technischen und anbieterneutralen Sicht dargestellt werden. Dazu wird auf das Shared Storage Model der Storage Networking Industry Association (SNIA) und deren Storage Virtualization Taxonomie zurückgegriffen. Folgende Ansätze sollen anschließend an Beispielen näher erläutert werden:
  - Block-Virtualisierung über Storage Area Networks (SAN) am Beispiel des IBM System Storage SAN Volume Controller und des IBM General Parallel File Systems (GPFS)
  - Filesystem-Virtualisierung über Network Attached Storage (NAS) am Beispiel des Network File System (NFS)
  - Disk-Virtualisierung am Beispiel des Veritas Volume Managers VxVM
- Literatur:
  - SNIA Technical Tutorial Storage Virtualization
  - IBM System Storage SAN Volume Controller
  - Veritas VxVM Admin Guide
  - IBM General Parallel File System (GPFS)

Block B: Hostvirtualisierung

B1: Vollvirtualisierung am Beispiel von VMware Workstation

- Inhalt: VMware war einer der ersten und ist nach wie vor einer der bekanntesten Hersteller von Virtualisierungslösungen. Das Produkt VMware Workstation ist somit ein sehr weit verbreitetes Beispiel für eine Vollvirtualisierung und wendet sich bewusst auch an mobile Anwender, die z.B. virtuelle Maschinen für Produktpräsentationen beim Kunden einsetzen wollen. In dieser Arbeit sollen deshalb einerseits die Einsatzbereiche, Möglichkeiten und Grenzen des Produkts und seiner Ableger wie dem VMware Player untersucht werden, andererseits die technische Umsetzung der Vollvirtualisierung im Detail analysiert und aufbereitet werden. Die Arbeit soll darüber hinaus auch auf Aspekte der Administration und Verwaltung von virtuellen Maschinen eingehen und auch vergleichbare Produkte anderer Hersteller nicht unberücksichtigt lassen.
- Literatur:
  - Produktseite VMware Workstation, aktuelle Version

        - VMware Informationen zur Funktionsweise der Virtualisierung
        - Vergleich mit anderen Virtualisierungstechniken
        - Anwenderforum für VMware-Produkte

B2: Paravirtualisierung am Beispiel von Xen

- Inhalt: Xen ist eine Virtualisierungslösung, die es ermöglicht, mehrere virtuelle Instanzen von Betriebssystemen auf einem einzigen realen Rechner parallel zu bertreiben und mehrere Gastbetriebssysteme hochperformant in Isolation auszuführen. Anders als VMware ist Xen als Open Source-Projekt unter GPL verfügbar. Es unterscheidet sich dadurch, dass es nicht die gesamte Hardware wie z.B. Grafikkarte, Festplatte und Netzwerkkarte emuliert, sondern dem Gastsystem für diese I/O-Funktionen eine API zum kontrollierten Direktzugriff bietet. Da die Hardware nicht vollständig emuliert wird, muss das Gastbetriebsystem für Xen angepasst werden, bevor es unter Xen ausgeführt werden kann. Diese Art der Virtualisierung bezeichnet man als "Paravirtualization", welche schon von IBMs Logical Partitioning (LPAR) bekannt ist. In dieser Arbeit sollen die Motivation, Einsatzbereiche sowie die Vor- und Nachteile der Paravirtualisierung mittels Xen untersucht und beschrieben werden. Die technischen Details für den Aufbau eines Xen-Systemes wie Installation, Konfiguration und Administration der Xen-basierten virtuellen Maschinen sollen ebenfalls dargestellt werden.
- Literatur:
    - FAQ, User Manual, Developer Manual, Xen Guide
    - Xen Produktseite, aktuelle Version
    - Xen Community
    - Xen - Paravirtualisierung, IBMs Logical Partitioning (LPAR)
    - Xen-Installation, Anleitungen, Hinweise

B3: Betriebssystem-Virtualisierung am Beispiel von OpenVZ und Virtuozzo

- Inhalt: Zu den Hauptaufgaben moderner Betriebssysteme gehören die Verwaltung von Prozessen, Dateien, angeschlossenen Geräten, Benutzern und Objekten, die der Interprozesskommunikation dienen (Beispiele sind Signale, SHM-Segmente und Pipes). Traditionell befindet sich auf einem physischen Rechner genau eine Betriebssystem-Installation, die die genannten Aufgaben für die physischen und logischen Betriebsmittel dieses Rechners übernimmt. Zwar lassen sich auf einem Rechner auch mehrere Betriebssysteme installieren, in der Regel aber nicht parallel nutzen. Betriebssystem-Virtualisierung verfolgt das Ziel, innerhalb einer einzigen Betriebssystem-Installation mehrere virtuelle Umgebungen (Virtual Environments, VEs) zu schaffen, in denen unabhängig voneinander Prozesse ablaufen, die auf die zur Verfügung stehenden physischen Ressourcen konfliktfrei zugreifen können. Obwohl Ressourcen wie CPU oder Netzwerkinterface nur einmal für alle VEs zur Verfügung stehen, können sie in jeder VE pseudo-exklusiv genutzt werden. Durch Betriebssystem-Virtualisierung können Hardware- und ggf. auch Softwarelizenzkosten eingespart werden. Haupt-Einsatzbereich ist die Server-Virtualisierung. Als Softwarelösungen in diesem Bereich sollen die Produkte OpenVZ sowie das darauf aufsetzende Virtuozzo betrachtet werden. Ziel der Hauptseminararbeit ist es, die Thematik der Betriebssystem-/Server-Virtualisierung aus verschiedenen Perspektiven (technische Perspektive, Administration/Management, ökonomische Aspekte) erschöpfend darzustellen und dabei den aktuellen Stand der Entwicklung zu reflektieren. Außerdem

sollen Einsatzbereiche, Möglichkeiten und Grenzen der genannten Virtualisierungstools aufgezeigt und praktisch evaluiert werden.

- Literatur:
  - http://openvz.org/
  - http://www.swsoft.com/products/virtuozzo/

B4: Hardware-unterstützte Virtualisierung (Intel VT-x, AMD-V, Intel VPro)

- Inhalt: Virtualisierungprodukte aus dem Desktopbereich gibt es mittlerweile seit mehreren Jahren. Um Virtualisierungsprodukte auch im Serverbereich sicher und performant einsetzen zu können, werden neuartige Technologien benötigt, die einen Teil der Virtualisierung bereits in Hardware realisieren. Ein wesentlicher Anteil hierbei ist die logische Trennung von Betriebssystemen und Virtual Machine Monitor (VMM)/Hypervisor die durch eine Erweiterung des Ringkonzeptes der x86-Architektur realisiert werden kann. Diese Aufgabe übernehmen neue Befehlssätze zur Unterstützung von Virtualisierung in den Prozessoren. Sowohl Intel als auch AMD haben im vergangenen Jahr entsprechende Befehlssätze entwickelt und in ihre aktuellen Prozessorgenerationen integriert. Ziel dieser Arbeit ist es, die Idee und Funktionsweise dieser Befehlssätze zu beschreiben und miteinander zu vergleichen. Ausblickend gilt es, neuartige Ansätze Hardware-unterstützter Virtualisierung wie z.B. Intel VPro kritisch zu betrachten.
- Literatur
  - http://www.intel.com/design/processor/manuals/253669.pdf
  - http://www.intel.com/cd/ids/developer/asmo-na/eng/197666.htm
  - http://download.microsoft.com/download/9/8/f/98f3fe47-dfc3-4e74-92a3-088782200fe7/TWAR05015_WinHEC05.ppt
  - http://download.microsoft.com/download/9/8/f/98f3fe47-dfc3-4e74-92a3-088782200fe7/TWAR05014_WinHEC05.ppt

B5: Unterstützende Hardwaretechnologien: Hyperthreading, Multi-Socket, Multi-Core und Blades

- Inhalt: Virtualisierung von Systemen wird von modernen Hardware-Konzepten und -Technologien zunehmend unterstützt. Dabei spielen Ansätze zur parallelen Verarbeitung eine Rolle, wie etwa Hyperthreading oder die Multi-Core-Bauweise. Auch bei der Organisation der Rechen-Hardware gewinnen Ansätze an Bedeutung, die parallele Verarbeitung unter geringen räumlichen Anforderungen unterstützen, z.B. Multi-Socket-Produkte oder Blade-Bauweisen für Servermaschinen. Die genannten Konzepte und Lösungen erlauben eine bessere Abbildung einer Menge virtueller Maschinen auf die reale Hardware, stellen aber auch erhöhte Anforderungen mit Bezug auf z.B. die Kapazität der Hauptspeicheranbindung oder Ein-/Ausgabe-Geräte. Im Rahmen dieses Themas sollen verschiedene Hardwaretechnologien, die zur Unterstützung von Host-Virtualisierung in Frage kommen, recherchiert, bewertet und verglichen werden. Beispielhaft sollen erweiterte Anforderungen identifiziert werden.
- Literatur:
  - http://www.intel.co.jp/technology/magazine/computing/multi-core-0905.pdf

B6: Neue Angriffsmuster durch Hostvirtualisierung am Beispiel von Bluepill als Rootkit-Ansatz

- Inhalt: Neben all den Anreizen und Versprechungen von Virtualisierungslösungen, gibt es wie so oft auch beim Thema Virtualisierung eine Kehrseite der Medaille. Betrachtet man z.B. Sicherheitsaspekte insbesondere von Lösungen zur Hostvirtualisierung, so stellt sich sehr schnell die Frage nach der Sicherheit verschiedener Produkte und Konzepte. Jedoch ist nicht nur die Sicherheit der jeweiligen Produkte von Bedeutung, sondern auch die Möglichkeit, ihre Konzepte missbräuchlich als Angriffsmuster einzusetzen. Ziel dieser Arbeit ist es, die Sicherheit der Konzepte zur Hostvirtualisierung zu evaluieren und hinter die Kulissen des Bluepill-Projekts zu blicken. Es ist darzustellen, wie exemplarisch anhand dieses Beispiels Virtualisierung zu Angriffszwecken z.B. als Rootkit Ansatz oder durch den Ausbruch aus einer virtuellen Umgebung eingesetzt werden kann.
- Literatur
  - http://bluepillproject.org/
  - http://theinvisiblethings.blogspot.com/2006/06/introducing-blue-pill.html
  - http://blackhat.com/presentations/bh-usa-06/BH-US-06-Rutkowska.pdf

Block C: Management virtualisierter Umgebungen

C1: Konvertierung zwischen verschiedenen Hostsystemen: P2V, V2V und V2P

- Inhalt: Der Trend zur Virtualisierung in großen Rechenzentren ist zur Zeit so ausgeprägt wie noch nie. Mit der Umstellung von physischen auf virtuelle Infrastrukturen ist jedoch ein erheblicher Aufwand verbunden. Die Erstellung der Installationen für die virtuellen Maschinen ist manuell aufgrund der Anzahl und Komplexität der zu migrierenden Systeme nicht durchführbar bzw. kann oft wegen fehlender Installationsmedien nicht mehr durchgeführt werden. Für diesen Zweck haben beinahe alle Anbieter von Virtualisierungslösungen sogenannte P2V- (Physical-to-Virtual-) Konverter entwickelt, die ausgehend von einem physischen Server eine virtuelle Maschine erstellen. Dieser Vorgang kann oft sogar zeit- und kostensparend ohne Unterbrechung des Produktivbetriebs durchgeführt werden. Daneben existieren Tools, die virtuelle Maschinen einer Virtualisierungslösung in Formate anderer Hersteller konvertieren. Konverter dieser Art heißen V2V (Virtual-to-Virtual) und sind nötig, um Images und Konfigurationsdateien zwischen Virtualisierungsprodukten austauschen zu können. Um die Kompatibilität von Virtualisierungslösungen zusätzlich zu erhöhen, haben sich einige Hersteller in einer Taskforce zusammengeschlossen und auf ein einheitliches Datenformat (Open Virtual Machine Format, OVF) geeinigt. Auch die bisher noch nicht genannten V2P- (Virtual-to-Physical-) Konverter haben ihre Daseinsberechtigung. Mit ihrer Hilfe können bei auftretenden Problemen virtuelle Maschinen zurück auf physische Rechner portiert werden. Dies ist nötig, um Supportansprüche bei Problemen geltend machen zu können, die sowohl im virtuellen als auch im physischen Fall auftreten. Ziel dieser Arbeit ist es, entsprechende Produkte zu finden und ihren Funktionsumfang sowie ihre grobe Funktionsweise zu beschreiben sowie Kompatibilitätsmatrizen zu entwerfen und darzustellen.
- Literatur:
  - http://www.vmware.com/support/v2p/index.html

- http://www.virtualization.info/2003/09/p2v-and-v2p-rumors.html

C2: High Availability, Migration und Dynamic Resource Scheduling

- Inhalt: Ein System kann als hochverfügbar bezeichnet werden, wenn die erwartete Funktionalität trotz eines Fehlerfalls oder einer Überlast des Hostsystems zur Verfügung steht. Die Virtualisierungstechnik bietet zu diesem Zweck flexible und kostensparende Lösungsansätze wie das Live Migration-Konzept von Xen. Dieses bietet die Möglichkeit, eine virtuelle Maschine im Bruchteil einer Sekunde auf einen anderen Host zu migrieren und dort weiter auszuführen. Die Firma VMware hingegen offeriert vollständige Lösungsansätze wie VMotion und VMware High Availability, um Hochverfügbarkeit zu sichern. Um den Migrationsprozess fehlerfrei und effizient durchführen zu können, muss gesichert sein, dass eine passende Menge an Ressourcen im Sinne von z.B. CPU-Zeit, Speicherplatz und Arbeitsspeicher für diesen Prozess zugewiesen werden kann. Dieser Vorgang muss genau geplant werden, da es ansonsten bei der Migration zu unerwünschten Effekten wie Resource Contention kommen kann. Hierbei hilft die sogenannte dynamische Ressourcen-Zuweisung (Dynamic Resource Allocation). Ziel dieser Arbeit ist es vor allem,
  - die klassischen Ansätze für Hochverfügbarkeit kurz vorzustellen,
  - Virtualisierung als Lösungsansatz für Hochverfügbarkeit darzustellen,
  - Migration als wichtiges Konzept der Hochverfügbarkeit zu untersuchen und
  - die Dynamic Resource Allocation für die Migration von virtuellen Maschinen einzuführen und zu erklären.
- Literatur:
  - Liver Migration of Virtual Machine
  - SuSE Linux XEN live migration demo
  - VMware Site Recovery Manager
  - High Availability with Virtualization

C3: Automatisierte Bereitstellung virtueller Maschinen durch Template-Mechanismen, Snapshots und Versionierung

- Inhalt: Durch den Einsatz von Host-Virtualisierung verändern sich einige Aufgaben bei der Bereitstellung von Servern, wie z.B. die Ressourcenauswahl, Erstinstallation und Folgeinstallationen. Es ist außerdem anzunehmen, dass eine recht große Anzahl virtueller Maschinen viele Ähnlichkeiten aufweisen, die durch Management-Tools ausgenutzt werden können. Teil der Arbeit ist es, die Organisation von Templates für virtuelle Maschinen sowie die Mechanismen zu beschreiben, die Template-basierte VMs instanziieren. Für eine schnelle Bildung eines Wiederherstellungspunktes bieten sich bei VMs Snapshots an, die einen Zustand einer VM einfach einfrieren und später wieder reaktivieren können. Da schnell eine große Zahl von Templates und Snapshots erreicht wird, ist eine Versionierung eine erhebliche Hilfe bei der Administration, die – ergänzt um eine entsprechende nutzergeführte Dokumentation – alle von Administratoren getätigten Management-Aktivitäten enthalten kann. Ziel dieser Arbeit ist es, Templates und Snapshots als Konzepte vorzustellen und dann die Implementierung der genannten Aktionen bei ausgewählten Host-Virtualisierungsplattformen darzustellen.
- Literatur:

- VMware VirtualCenter 1.3.x Support Documentation: Working with Templates
- Dennis Zimmer, VMWare und Microsoft Virtual Server, Kapitel 13: Templates (in VMware bzw. VirtualCenter und auch in Virtual PC), ISBN: 978-3-89842-701-2
- Xen Templates
- Xen Dokumentation, Chapter 2. Creating VMs
- Xen-Tutorial I und II, iX 1 und 2/2007
- Virtuelle Maschinen für Test, Demo und Schulung, iX 02/2007, S. 44
- Virtuozzo Whitepaper, More Efficient Virtualization Management: Templates, Download von http://www.swsoft.com/en/splp
- MLN (Manage Large Networks) virtual machine administration tool, http://mln.sourceforge.net/

C4: Management-Herausforderungen durch Virtualisierung

- Inhalt: Der heute immer stärker werdende Trend zum Einsatz von Virtualisierung bringt eine Vielzahl von Problemen hinsichtlich des Managements mit sich. Grundlegendes Problem hierbei ist die Abbildung von virtuellen Ressourcen auf die physischen Ressourcen, auf denen diese realisiert sind. Eine übersichtliche Verwaltung und Pflege dieser Abbildung, vor allem in übersichtlicher und ausreichender Integration mit der bestehenden Managementinfrastruktur, die meist nur auf die physischen Ressourcen ausgerichtet ist, erweist sich als schwierig. Es existieren meist keine einheitlichen Standards bezüglich des Managements dieser Abbildung, sondern oft nur herstellerspezifische Lösungen. Überdies gibt es nahezu keine ausgereiften Werkzeuge, um diese Abbildung in übersichtlicher Weise für Administratoren darzustellen, so etwa im Bereich des Netzmanagements für eine übersichtliche Darstellung von VLANs oder MPLS-Netzen. In dieser Arbeit sollen diese Management-relevanten Probleme von Virtualisierung vor allem im Hinblick auf Fehlermanagement, Dokumentation und Modellierung (Ansätze wie z.B. ITIL CMDB), sowie speziell der Integration in bestehende Managementumgebungen (z.B. Asset-Management-Anwendungen) behandelt werden.
- Literatur:
  - ITSM - The ITIL Configuration Management Plan
  - VLAN Membership Policy Server (VMPS) / Dynamic VLANs - Cisco Systems
  - Cisco - Understanding VLAN Trunk Protocol (VTP)
  - Simplified SAN Management - Cisco Systems
  - Virtual Desktop Infrastructure (VDI) Overview