Betriebssysteme

Virtualisierung

Von

Prof. Dr. Franz-Karl Schmatzer

Literatur Verzeichnis

- Mandl, Peter; Grundkurs Betriebssysteme; 5.Aufl. 2020; Springer Verlag
- Baun, Christian, Betriebssysteme kompakt, 2.Aufl., Springer 2020
- W. Stallings; Operating Systems; 9.ed; Pearson 2018

Gliederung

- Einführung
- Terminologien
- Virtuelle Maschinen
- Anwendungsvirtualisierung

Einführung Virtualisierung

Was ist Virtualisierung?

- Allgemeine Definition:
  - Unter Virtualisierung versteht man Methoden zur Abstraktion von Ressourcen mit Hilfe von Software
- Virtuelle Maschine verhält sich wie die reale Maschine
- Diverse Varianten:
  - Virtuelle Computer: Server- und Desktopvirtualisierung (= Betriebssystem- bzw. Plattformvirtualisierung)
  - Storage Virtualisierung
  - Anwendungsvirtualisierung
  - Virtuelle Prozessumgebungen (Prozessmodell und virtueller Speicher)
  - Virtuelle Prozessoren: Java Virtual Machine (JVM)
  - Netzwerkvirtualisierung (vLAN)

Terminologie zur Betriebssystemvirtualisierung

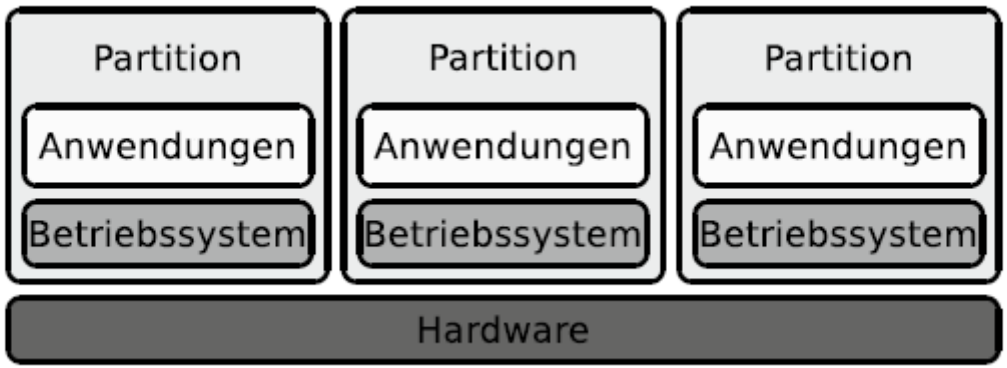
- Reale Maschine
- Virtuelle Maschine (VM)
- Hostbetriebssystem
  - Synonyme: Wirt, Host, Gastgeberbetriebssystem oder Hostsystem
- Gastbetriebssystem
  - Synonyme: Gast, Guest oder Gastsystem
- Virtual Machine Monitor (VMM)
  - Synonym: Hypervisor

Abgrenzung zur Emulation

- Unterscheidung Emulation – Virtualisierung
  - Emulation: **Komplette** Nachbildung der Hardware in Software
  - Virtualisierung: **Geringer Teil** der Befehle müssen nachgebildet werden, die meisten Befehle laufen direkt auf der Hardware (direkter Aufruf aus VM aus)

Partitionierung

- In der Mainframe-Welt spricht man von Partitionierung als spezielle und umfassendere Form der Virtualisierung.
- In Mainframe- und Midrange-Systemen wird
  - die CPU,
  - der Hauptspeicher,
  - die Ein- und Ausgabe und
  - der Datenspeicher unterstützt durch Firmware virtualisiert.
- Das ganze Betriebssysteme mit allen Ressourcen kann daher partitioniert werden.
- Änderungen sind im laufenden Betrieb möglich
- Mehrere 100 bis 1000 Linux Instanzen sind möglich



Aufgabe Virtualisierung

- Erläutern Sie die Vor- und Nachteile einer Virtualisierung

Vorteile der Virtualisierung

- Weniger Hardware notwendig,
- bessere Hardwareauslastung durch Serverkonsolidierung
  - Heutige Server sind meist bei weitem nicht ausgelastet
- Weniger Leistungsaufnahme für Rechner und Klimatisierung
- Flexibilität bei Aufbau einer Infrastruktur, schnelle Bereitstellung wird unterstützt, VMs beliebig vervielfältigbar und archivierbar
- Vereinfachte Wartung, Life-Migration, unterbrechungsfrei, auch Technologiewechsel ohne Betriebsunterbrechung
- Unterstützt Verfügbarkeits- und Ausfallsicherheitskonzepte
- Unterstützung auch historischer Anwendungen

Nachteile der Virtualisierung

- Geringere Leistung als reale Hardware,
- Overhead von 5 bis 10 %
- Schwierig bei spezieller Hardwareunterstützung
  - z.B. Hardware-Dongles, spezielle Grafikkarten
- Bei Ausfall eines Serverrechners fallen gleich mehrere virtuelle Rechner aus
  - → hohe Anforderungen an Ausfallkonzepte und Redundanz

Historie zur Virtualisierung

- VM/370 hieß zuerst CP/CMS (1970 Jahre)
  - Herz ist der Virtuelle Machine-Monitor.
  - Es werden mehrere virtuelle Maschinen bereitgestellt.
  - Sind exakte Kopien der zugrunde liegenden Hardware
- Nachfolger z/VM, welches auf den Mainframes der z-Serie von IBM läuft.

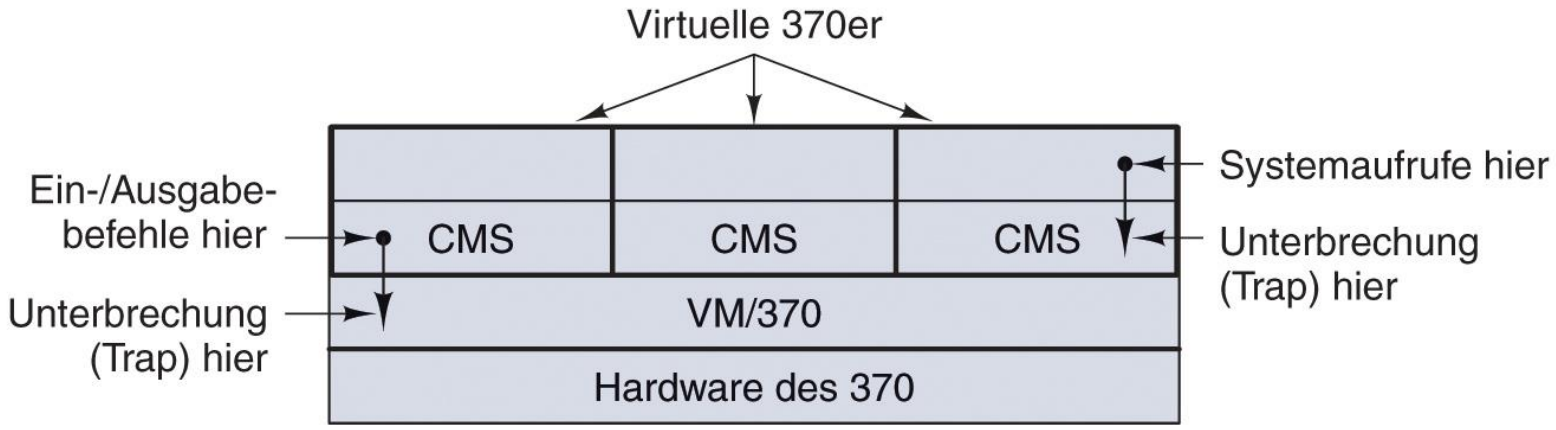
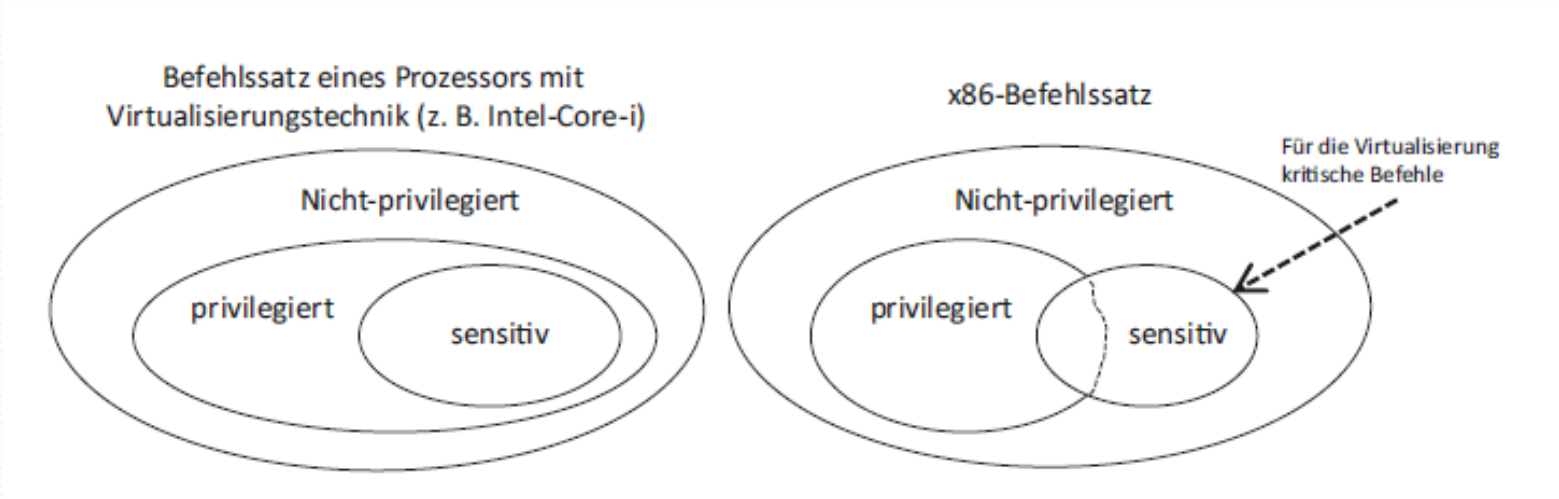


Abbildung 1.28: Die Struktur des VM/370-Systems mit CMS

@Tanenbaum

Virtualisierbarkeit der Hardware

- Im Großrecherumfeld werden Prozessoren schon länger so gebaut, dass Virtualisierungen unterstützt werden.
- INTEL und AMD haben dies bis vor kurzem außer bei der virtuellen Speichertechnik nicht getan.
- Um Virtualisierung effizient zu unterstützen müssen einige Hardware-Voraussetzungen erfüllt sein.
  - privilegierte und nicht privilegierte Befehle
  - Sensitive und kritische Befehle



privilegierte und nicht privilegierte Befehle

- Die grundlegenden Anforderungen an die Virtualisierbarkeit ist eng mit dem Konzepten des Zugriffsschutzes von Prozessoren verknüpft.
- Privilegiert heißt:
  - eine Ausnahme und damit einen Trap kann in dem höher privilegierten Modus erzeugt werden, falls er im user-Modus ausgeführt wird.
  - Im Kernel-Modus wird keine Ausnahme generiert.
- Nicht privilegierte Befehle können in allen Modi, ohne eine Ausnahme zu erzeugen, ausgeführt werden.

sensitive und kritische Befehle

- **Sensitiven Befehle**
  - Können zustandsverändernd sein oder
  - Verhalten sich je nach Modus unterschiedlich.
  - Hierzu gehören z. B. Befehle für den Zugriff auf I/O-Geräte oder auf spezielle interne Adress- und Steuerregister.
- Sensitive Befehle sollten eine Teilmenge der privilegierten Befehle sein und bei einem Aufruf in einem nicht privilegierten Betriebsmodus eine Ausnahme und damit einen Sprung in einen privilegierten Betriebsmodus erzwingen.
- **kritischen Befehle**
  - sind sensitiv, aber nicht privilegiert
  - Sie lösen bei Aufruf im Benutzermodus keinen Trap aus und können somit von einer VMM nicht abgefangen werden.
  - Die kritischen Befehle stellen, wie die Bezeichnung schon andeutet, ein Problem dar.

Generelle Hardware-Anforderungen

- Popek und Goldberg untersuchten bereits 1974 die Hardware-Anforderungen für eine effiziente Virtualisierbarkeit.
- Eine Rechnerarchitektur ist virtualisierbar, wenn
  - alle sensitiven Operationen privilegiert sind,
  - alle sensitiven Befehle eine Teilmenge der privilegierten Befehle darstellen
- Unter diesen Bedingungen kann auf jeden Fall ein Hypervisor konstruiert werden.
- Dies ist eine hinreichende, aber nicht notwendige Bedingung.

Virtuelle Maschinen

- Hypervisor-1 und Hypervisor-2

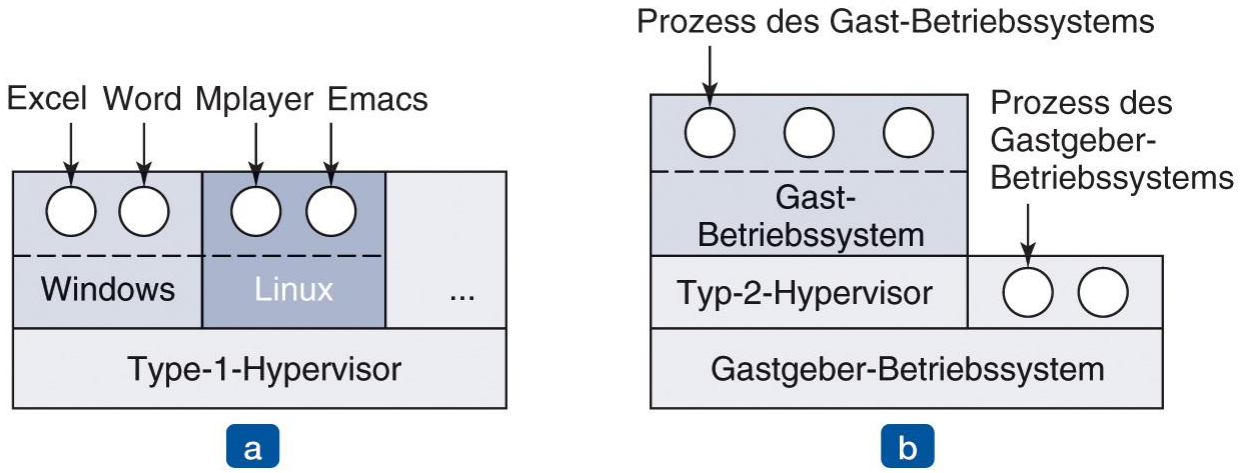
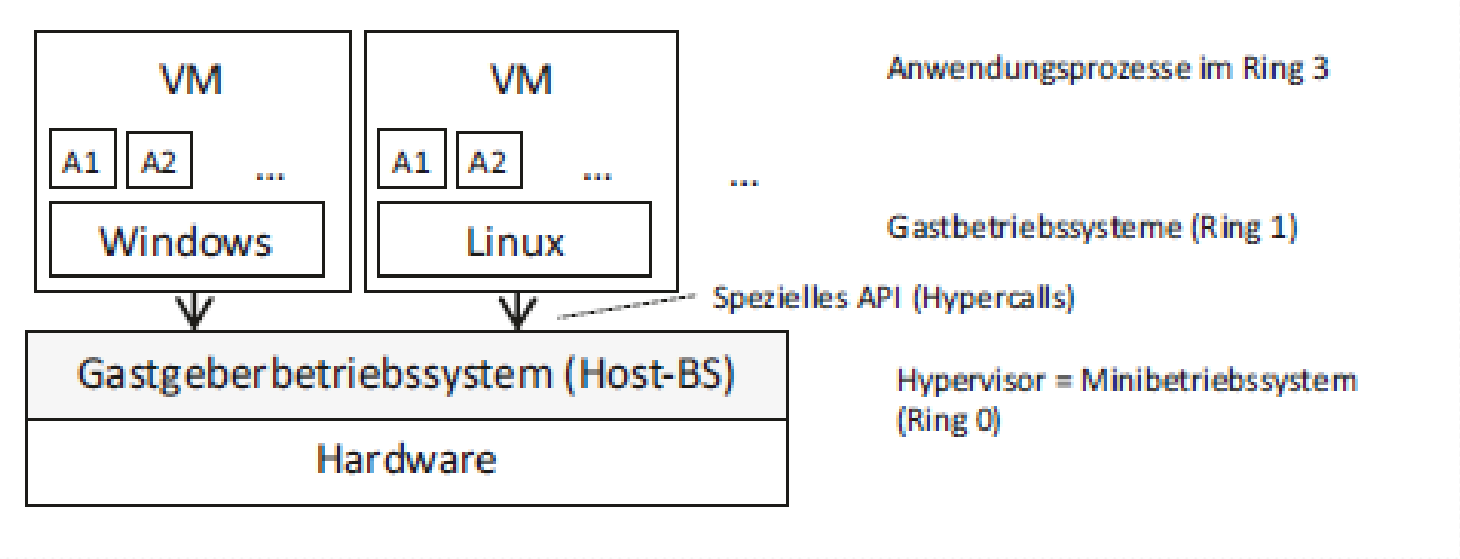


Abbildung 1.29: (a) Typ-1-Hypervisor (b) Typ-2-Hypervisor

@Tanenbaum

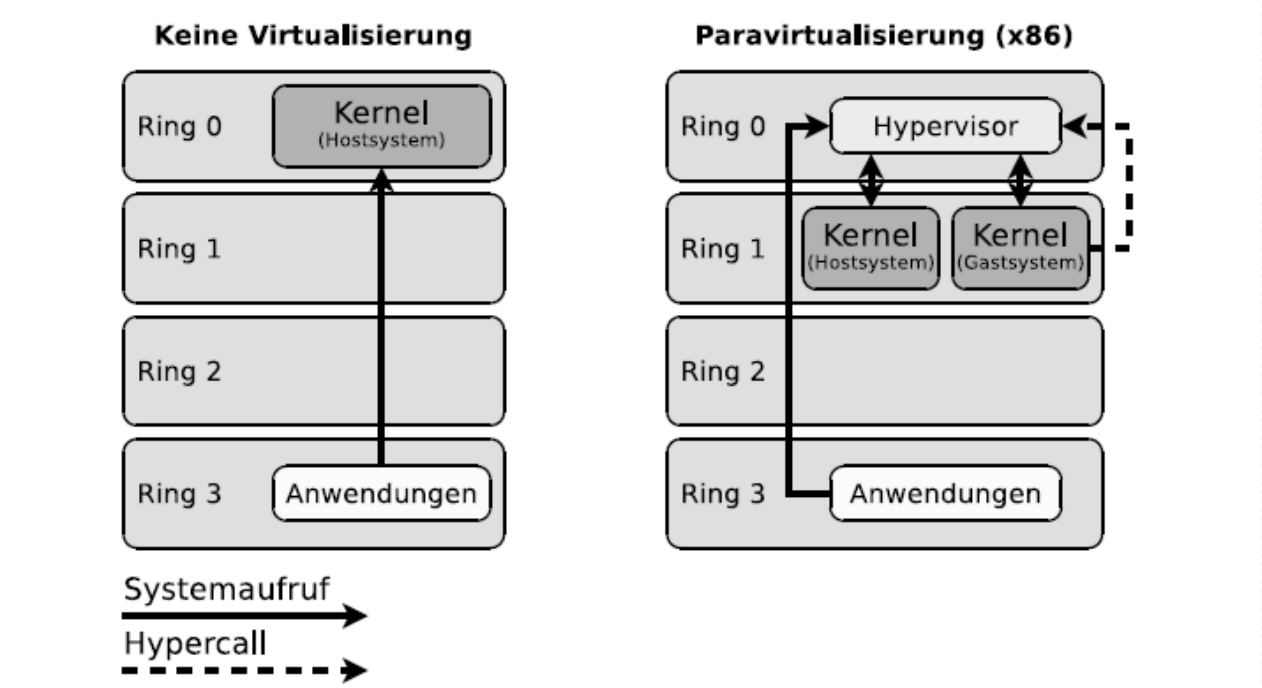
Paravirtualisierung

- Paravirtualisierung
  - Gastbetriebssystem verwendet eine abstrakte Verwaltungsschicht, den Hypervisor, um auf die Hardware zuzugreifen.
  - man benötigt drei Schutzringe.
    - Hypervisor auf Schicht 0,
    - Betriebssystem auf Schicht 1
    - Betriebssystem kann keine privilegierte Befehle ausführen. Daher werden vom Hypervisor Hypercalls zur Verfügung gestellt.



Paravirtualisierung

- Umsetzung der Systemaufrufe



- Beispiele für Paravirtualisierung:
  - Xen, Citrix Xenserver, Virtual Iron und VMware ESX Server.

@Baun

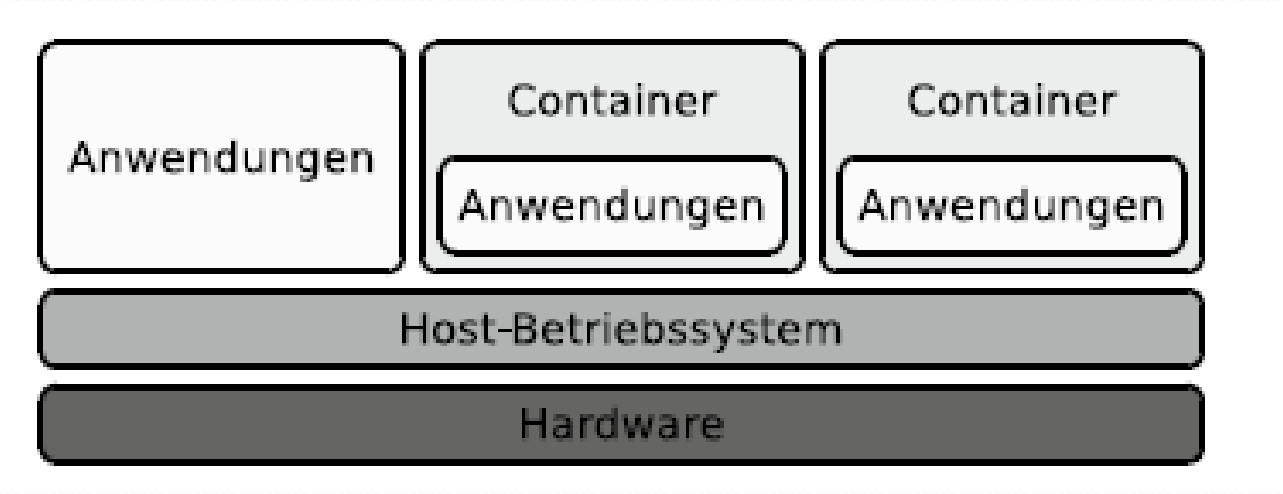
Aufgabe Virtualisierungsarten

- Erläutern folgende Virtualisierungsarten
  - Hardware-Virtualisierung
  - Betriebssystem-Virtualisierung
  - Speicher-Virtualisierung
  - Netzwerk-Virtualisierung
- Wo finden man diese Form der Virtualisierung und geben Sie auch Beispiele an.

Hardware-Virtualisierung

- Erweiterungen in den aktuellen x86-INTEL und AMD Prozessoren.
- Vorteil ist, dass das Betriebssystem als Gastbetriebssystem ausgeführt werden kann.
  - AMD hat den Secure-Virtual-Machine-Befehlssatz (SVM).
  - Bei Intel heißt die Lösung VT-x.
- Die Überarbeitung modifiziert die Privilegien. Ein neuer Ring -1 für den Hypervisor kommt hinzu.
  - Ring -1 und besitzt jederzeit die volle Kontrolle über den Prozessor und die übrigen Hardwareressourcen
  - Die virtuellen Maschinen laufen in Ring 0. Man nennt das auch Hardware Virtual Machine (HVM).
- Vorteil ist, dass Gastsysteme nicht angepasst werden müssen.
- **Beispiele**
  - Xen seit Version 3, Windows Server ab Version 2008 (Hyper-V), VirtualBox und KVM.

Betriebssystem-Virtualisierung



- mehrere voneinander abgeschottete identische Systemumgebungen (Container)
- Anwendungen, die in einem Container laufen, sehen nur Anwendungen im gleichen Container.
- Isolierte Umgebung mit klar definierten Eigenschaften

@Baun

Betriebssystem-Virtualisierung

- Vorteile sind
  - der geringe Verwaltungsaufwand.
  - Anwendung läuft in einer isolierten Umgebungen
- Anwendungsfälle
  - Internet-Service-Provider, die (virtuelle) Root-Server oder Webdienste anbieten
  - automatisierte Installation komplexer Anwendungssoftware in einer definierten Umgebung
- Beispiele für Virtualisierungslösungen:
  - Docker,
  - das Betriebssystem Solaris von Oracle (vormals Sun Microsystems),
  - OpenVZ für Linux,
  - Linux-VServer, das Betriebssystem FreeBSD,
  - Virtuozzo12 und
  - FreeVPS.

Formen der Speichervirtualisierung