Virtualisierung

Virtualisierung bildet eine Schicht zwischen Software und Hardware oder Software und Software. Diese bezeichnet man als Anwender und Resource, manchmal auch Wirt und Gast. Hauptsächlich wird Virtualisierung genutzt, um einem Anwender eine Umgebung vorzutäuschen.

Grundsätzlich unterscheidet man drei Arten der Virtualisierung: Software-, Hardware-, und Netzwerkvirtualisierung.

# Inhaltsverzeichnis

[**Inhaltsverzeichnis**](#_429d6dr5882c) **1**

[**Softwarevirtualisierung**](#_nk1fthx8xk56) **2**

[Containervirtualisierung](#_qxk2mcuwvtzs) 2

[Virtuelle Maschinen](#_uv9rgw8vy9cf) 2

[Hypervisor](#_ijjusa11kpot) 2

[Arten von Virtuellen Maschinen](#_jc2mesl0bxu7) 3

[Systembasierte virtuelle Maschinen](#_c48pr7f5l3zy) 3

[Prozessbasierte virtuelle Maschinen](#_7j8k9fdzf2xi) 3

[**Hardwarevirtualisierung**](#_a8cap2kxgf5z) **4**

[Systemvirtualisierung](#_3nrk4w1aoqwf) 4

[Partitionierung and Pooling](#_30jnv2agl5il) 4

[Domaining](#_wecuih5zt2q0) 5

[Prozessorvirtualisierung](#_vp3zmke61mmi) 5

[Speichervirtualisierung](#_z50i3kjaoewi) 5

[Block-Virtualisierung](#_6ivz3wguncda) 6

[Datei-Virtualisierung](#_fxizpfw3voyn) 7

[**Netzwerkvirtualisierung**](#_oocxoxa6kxla) **7**

[Virtual Local Area Network](#_phi4wcucjtx) 7

[Virtual Private Network](#_ybn8duh6m6ob) 8

# Softwarevirtualisierung

Die Form der Virtualisierung mit der wir am meisten zu tun haben. Hier werden bestimmte Umgebungen vorgetäuscht. Außerdem bietet die Virtualisierung eine zusätzlich Schutzschicht.

Bei dieser Art der Virtualisierung werden Gastsysteme auf einem Host-System betrieben. Diese Gastsysteme können von einzelnen Anwendungen bis zu ganzen Betriebssystemen reichen.

## Containervirtualisierung

Bei der Containervirtualisierung werden die Gastsysteme in, wie der Name schon sagt, Containern ausgeführt und sind im Idealfall vollständig vom Host isoliert. Der große Vorteil von Containervirtualisierung ist, dass es leichter ist Programme zu transportieren und ihren einwandfreien Betrieb zu garantieren.

Der erste Vertrete dieses Ansatzes war OpenVZ. Es gab zwar zuvor schon ähnliche Projekte in Linux diese waren aber wenig relevant. Heute findet man Containervirtualisierung in den meisten PaaS Systemen und anderer Verwaltungssoftware wie zum Beispiel Docker.

## Virtuelle Maschinen

Durch virtuelle Maschinen ist es möglich ein Betriebssystem in einem Betriebssystem zu starten. Dazu wird ein sogenannter Hypervisor(Typ 2) verwendet.

### Hypervisor

Der Hypervisor, “Aufseher”, oder auch Virtual Machine Monitor(VMM), bildet eine abstrahierende Schicht zwischen tatsächlicher Hardware bzw. dem Host-System und den Gastsystemen. Er ist dafür zuständig dem Gastsystem Ressourcen zur Verfügung zu stellen.Dadurch ist es möglich den Gästen eine bestimmte Umgebung vorzutäuschen die nicht der realen Umgebung entspricht.

Es gibt zwei Typen von Hypervisoren:

* **Typ 1: Native Hypervisor**

Setzt direkt auf der Hardware auf. Braucht bestimmte Treiber für Hardwarezugriff.

* **Typ 2: Hosted Hypervisor**

Setzt auf einem Hostsystem auf. Nutzt Gerätetreiber für Hardwarezugriff.

Die meisten CPUs haben heute speziell für Virtualisierung eingeführte Befehle die die Virtualisierung beschleunigen und vereinfachen.

### Arten von Virtuellen Maschinen

Virtuelle Maschinen werden nach dem Umfang der Funktionalität des Gastsystems eingeteilt. Ist das System vollständig funktionsfähig, so spricht man von vollständiger Virtualisierung.

#### Systembasierte virtuelle Maschinen

Auch vollständige Virtualisierung, bildet einen realen Rechner vollständig nach. So vollständig, dass normale Betriebssysteme, die für reale Rechner entworfen sind auf der virtuellen Maschine laufen.

Virtuelle Maschinen bieten im Vergleich zu normalen Betriebssystemen einige Vorteile:

* Betrieb von mehreren Betriebssystemen gleichzeitig

Dieses Feature wird von den meisten professionellen virtuellen Maschinen unterstützt.

Plattformunabhängig

* Durch eine virtuelle Maschine ist es möglich Betriebssysteme auszuführen die auf der realen Hardware gar nicht laufen würden.

Höhere Effizienz im Parallelbetrieb

* Wenn viele virtuelle Maschinen auf einem Rechner laufen wird die Hardware effizienter genutzt, als im separaten Betrieb.
* Sicherheit

Durch die Unabhängigkeit vom Betriebssystem ist dieses sicherer.

* Wartbarkeit

Da die virtuellen Maschinen einfach gespeichert und geladen werden können ist es um ein Vielfaches einfacher und risikofreier diese zu warten.

Sie kommen jedoch nicht ohne Nachteile:

* Effizienzverlust

Durch den betrieb des Hypervisors geht Leistung verloren

* Abhängigkeit

Da sich die virtuellen Maschinen die selbe Hardware teilen beeinflussen sie sich untereinander obwohl sie strikt getrennt sind.

* Sicherheit

Durch den Betrieb des Hypervisors wird dieser zum neuen Angriffspunkt

Virtuelle Maschinen können mit verschiedenen Methoden umgesetzt werden. Dazu zählen Hypervisoren, Hardwarevirtualisierung, Paravirtualisierung und sogar Hardware-Emulation obwohl Emulation keine wirkliche Virtualisierung ist.

#### Prozessbasierte virtuelle Maschinen

Auch Anwendungsvirtualisierung, ermöglicht es einzelne Anwendungen unabhängig vom Host-System auszuführen. Der bekannteste Vertreter dieser Art ist das JRE (Java Runtime Environment) das Java plattformunabhängig macht. Diese Abhängigkeit ist immer noch ein großes Problem beim erstellen von Software.

Prozessbasierte virtuelle Maschinen bringen folgende Vorteile:

* **Plattformunabhängigkeit**

Für eine neue Plattform müssen nicht alle Programme umgeschrieben werden, sondern nur die virtuelle Maschine.

* **Dynamische Optimierung**

Ist möglich weil die virtuelle Maschine für die Ausführung verantwortlich ist und nicht das Betriebssystem

Nachteile:

* **Geschwindigkeitsverlust**

Durch die Ausführung in der virtuellen Maschine ist langsamer als eine native Anwendung.

# Hardwarevirtualisierung

Bei der Hardwarevirtualisierung wird direkt von der Hardware virtualisiert, anstatt auf einem Hostsystem. Es kann entweder ein gesamtes System virtualisiert werden, oder nur Teile des Systems z.B. Speicher.

## Systemvirtualisierung

Als Systemvirtualisierung bezeichnet man die Trennung eines Computersystems in eigenständige Betriebssysteme, d.h. Auf einem einzelnen Rechner laufen mehrere (verschiedene) Betriebssysteme. Die Systemvirtualisierung findet heute vielfach in Form der Server-Partitionierung Einsatz, besonders in Rechenzentren.

Die Server-Partitionierung funktioniert folgendermaßen:

Alle Systeme teilen sich dieselbe Hardware. Diese wird durch einen Hypervisor, nach Bedarf, den Systemen zugewiesen.

Vorteile der Systemvirtualisierung sind unter anderen geringerer Platzbedarf, geringere Kosten aufgrund der effizienteren Nutzung der Hardware und erleichterte Wartbarkeit.

## Partitionierung and Pooling

Partitionierung ist eine weitere Form der Hardwarevirtualisierung. Hierbei wird eine große Hardwarekomponente virtuell auf mehrere kleine abgebildet. Gängige beispiele sind zum Beispiel Speicher oder Netzwerkverbindung. Partitionierung spielt auch in Storage Area Networks in Form von Zoning eine große Rolle.

## Domaining

Domaining, auch Virtual Hosting, ist ein Verfahren das es ermöglicht mehrere Domains auf einem physischen Server anzubieten. Der Vorteil ist, dass, wie bei den meisten Anwendungen der Virtualisierung, Kosten gespart werden. Außerdem ist es so möglich mehrere Domains mit sprechenden Namen auf einem Server anzulegen.

Es gibt drei Arten von Virtual Hosting

* **Name-based**

Mehrere Domains auf einer IP-Addresse. Spart im Gegensatz zu IP-based Virtual hosting IP-Overhead. Der Client muss den Host-Header setzen um die richtige Domain anzusprechen. Es ergeben sich jedoch Probleme mit SSL/TLS Zertifikaten.

* **IP-based**

Jede Domain erhält eine eigene IP-Adresse, dadurch kann jedes beliebige Protokoll verwendet werden. Komplett serverseitig da der Client nur die IP braucht.

* **Port-based**

Jede Domain erhält ihren eigenen Port. Wird in der Praxis selten verwendet, da es vergleichsweise user-unfreundlich ist.

Es können verschiedene Formen von Virtual Hosting kombiniert werden.

Die wichtigste Anwendung von Virtual Hosting/Domaining is das Shared Web Hosting, hierbei werden eine große Anzahl verschiedener Websites auf dem selben System(häufig auch virtualisiert) angeboten.

## Prozessorvirtualisierung

Wenn ein Gast Befehle ausführen will, schickt er diese nicht an den Prozessor sondern an den Hypervisor, welcher sie dann an die native Hardware anpasst und an den Prozessor schickt. Prozessorvirtualisierung ermöglicht eine schnellere Kommunikation zwischen Gast-System und Hardware da sich der Prozessor um die Unterscheidung zwischen Gast- und Host-System kümmert.

Prozessoren die Virtualisierung nativ unterstützen, verstehen zehn Prozessorbefehle mehr (das *Virtual Machine Extensions* Anweisungsset).

Beispiele dafür sind AMD-V und VT-x.

## Speichervirtualisierung

Der Zugriff auf den Speicher erfolgt nicht mehr direkt, der angezeigte Speicher muss nicht mit dem physischen Speicher übereinstimmen. Dadurch ergeben sich Vorteile, sowohl für Verwender (Angepasste Verzeichnisstruktur), als auch für Anbieter (erhöhte Effizienz/Auslastung). Beispiel: RAID-Systeme.

Es gibt grundsätzlich zwei Methoden der Speichervirtualisierung.

### Block-Virtualisierung

Es wird ein logisches Interface geschaffen über das man auf den gesamten Speicher zugreifen kann. Diese Trennung der Hardware vom Zugriff bringt erhöhte Flexibilität in der Speicherverwaltung. Ressourcen erhalten eine sogenannte Logical Unit Numbers (LUN) und eine Logical Block Address (LBA).

Die Speichervirtualisierung erfolgt in mehreren Schritten:

* **Speicher Neuzuordnung**

Die Ansicht des Users ergibt sich aus einer oder mehreren Virtualisierungsschichten die den physischen Speicher verwalten. Im Hintergrund werden alle Speichermedien zu einem sogenannten *Storage Pool* zusammengefasst.

* **Metadaten**

Da der Zugriff nicht mehr über den realen Pfad erfolgt, muss die Virtualisationssoftware/-hardware Metadaten zu den gespeicherten Daten anlegen um diese wiederzufinden und zu verwalten. Dies kann entweder mit einer Mapping-Table oder Hashing umgesetzt werden.

* **Input/Output Umleitung**

Das virtualisierte System erhält Zugriffsanfragen, findet den tatsächlichen Speicherort und liefert die geforderten Daten zurück.

Speichervirtualisierung erschwert Replikation, da die Replikation über der Virtualisationsschicht passieren muss, weil erst hier ein sinnvolles Image des Speichers vorliegt.

Grundsätzlich wird die Replikation mit zwei Methoden implementiert:

* **Mirroring**

Jeder Zugriff/jede Veränderung wird sofort repliziert.

* **Snapshots**

An einem Zeitpunkt wird das gesamte System repliziert.

Vorteile von Block-Virtualisierung sind vor allem die sicherere Speicherverwaltung, da die Mapping Table für den Zugriff verantwortlich ist, und die leichtere Speicheranpassung bzw. Speicheroptimierung.

Nachteile von Block-Virtualisierung sind die erhöhte Komplexität des Systems, Fehler zu finden wird sehr aufwendig, und verminderte Lese-/Schreibgeschwindigkeiten, selbst die performantesten Virtualisierungen verursachen Verzögerungen.

Block-Virtualisierung kann auf drei Arten geschehen:

* **Host-basiert**

Ein Softwarelayer zwischen Anwender und Hardware abstrahiert den Speicher. Moderne Betriebssysteme wie Linux und Windows unterstützen dies automatisch.

* **Speicher-basiert**

Dazu zählen alle RAID Systeme, d.h. Die Speichermedien werden zusammengefasst und zusätzlich wird Replikation und erhöhte Performance angeboten.

* **Netzwerk-basiert**

Die Virtualisierung passiert zwischen einem Storage Area Network und den Nutzern. Das ist besonders nützlich da es einen einzelnen Zugriffspunkt für den gesamten Speicher definiert.

### Datei-Virtualisierung

Auch *Virtual File System*, ermöglicht den einheitlichen Zugriff auf unterschiedlichste File-Systeme. So kann man zum Beispiel auf eine lokale Datei genau gleich zugreifen, wie auf ein Netzwerk-Datei.

Unter normalen Umständen ist Block-Virtualisierung immer besser als Datei-Virtualisierung.

# Netzwerkvirtualisierung

Durch Netzwerkvirtualisierung werden die physischen Netzwerkressourcen in logische Einheiten geteilt, d.h. die Virtualisierungsschicht liegt im Netzwerk. Durch diese Trennung von Hardware und Logik ist es möglich mehrere Netzwerke auf derselben Hardware einzurichten und so leichter zu verwalten.

## Virtual Local Area Network

Eine Layer 2 Technologie, die es ermöglicht die oben genannte Nutzung von mehreren Netzwerken auf einer Hardware, oder auch mehrere physische Geräte zu einem Netzwerk zusammenzufassen, indem die Pakete mit Tags versehen werden um ihr Ziel zu erreichen. Dadurch können Anschaffungskosten gespart werden und die Netzwerkplanung wird stark vereinfacht.

Es entsteht jedoch die Möglichkeit, durch das sogenannte VLAN-Hopping, von einem Netzwerk aus auf Traffic in einem anderen Netzwerk zuzugreifen. VLAN-Hopping kann aber mit einer angemessenen Switch-Port-Konfiguration verhindert werden.

* **Switch Spoofing**

Beim Switch Spoofing täuscht das Paket vor, von einem Trunking Switch zu kommen und erhält dadurch segmentübergreifenden Zugriff.

* **Double Tagging**

Bei Double Tagging wird das Paket mit zwei Headern versehen. Dadurch wird das Paket von einem Netzwerk ins nächste weitergeleitet.

## Virtual Private Network

Durch ein VPN wird, durch ein VPN-Gateway, der Fernzugriff auf ein Netzwerk ermöglicht, als wäre man physisch Teil des Netzwerks. Dabei wird das Internet als Zwischennetz verwendet (als Verlängerungskabel). VPNs habe den großen Vorteil, dass sie auf Basis eines unverschlüsselten Netzwerks eine sichere Kommunikation zwischen den Teilnehmern ermöglicht (Tunneling). Virtual Private Networks sind rein softwarebasiert, die dazugehörige Hardware bilden die beteiligten Netzwerke.

Dabei kann das VPN-Gateway entweder in einem physischen Netz enden (End-To-Site), oder in einem weiteren virtuellen Netzwerk münden, das aus anderen Teilnehmer besteht (End-To-End).

Wichtig für eine funktionierende VPN sind die Verbindungsgeräte zwischen den Netzwerken, auf ihnen muss spezielle VPN-Software installiert werden.

Virtual Private Networks bringen einige Vorteile mit sich:

* **Sicherheit**

Die Kommunikation über VPN ist, im Vergleich zur Kommunikation über einen öffentlichen Zugriffspunkt, um ein vielfaches sicherer, da das Paket komplett verschlüsselt wird und nur noch der Weg zum VPN-Gateway auslesbar ist.

* **Positionsvortäuschen**

Durch die Verbindung mit einem VPN, kann man beispielsweise das Internet nutzen als ob man in diesem Netzwerk ist, d.h. man kann auf Internetseiten zugreifen die im eigenen Netzwerk gesperrt sind.

VPNs werden hauptsätzlich verwendet, um verschiedene Netzwerke eines Unternehmens zu verbinden, die Arbeit im Firmennetz von zuhause aus zu ermöglichen, oder ein Local Area Network zu simulieren.