Server-, Storage- und Rechenzentren

Kenntnis der Unterschiede von Rackmount-Server und Blade-Server

Rackmount Server:

- Rackmount Server sind Server die in ein 19" Rack eingebaut werden können.
- Können 1, 2, 3 oder 4 HE (Höheneinheit) hoch sein (1 HE = 1,75 Zoll oder 44,45 mm).
- Werden horizontal angeordnet.
- Es gibt mehr Erweiterungs-Steckplätze für Netzwerk und Storage-Adapter.
- Verfügen über serielle, parallele und USB-Anschlüsse.
- Es können mehr interne Festplatten verbaut werden (Ist ein Vorteil, wenn viele virtuelle Maschine betreibt werden sollen).
- Er besitzt mehr CPU-Sockeln.
- Zusätzlich Komponenten sind einfach zu installieren. Bei Blade Server muss, wenn das Blade Center voll ist, ein zusätzliches Gehäuse gekauft werden. > teuer!

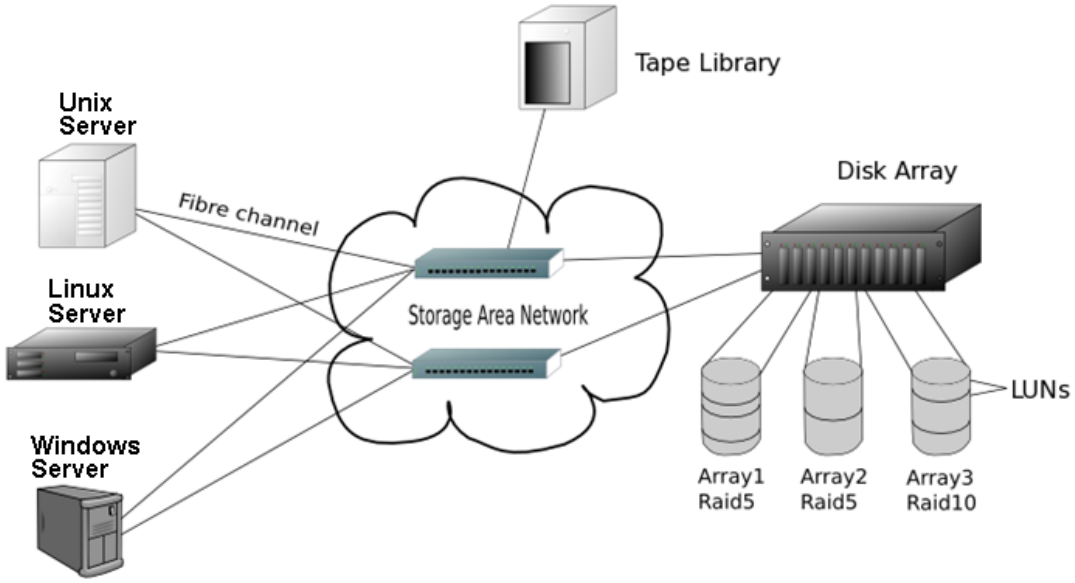
Blade Server:

- Benötigt weniger Platz, Kabel und Strom
- Blade Server teilen sich ein Gehäuse, das sogenannten Blade Center, das wiederum im 19" Rack verbaut ist.
- Sie Werden vertikal angeordnet
- Blade Server haben eine gemeinsame Stromversorgung und Lüftung, die an der Rückseite des Blade Center Gehäuse eingebaut sind.
- Hohe Skalierbarkeit und Flexibilität, dadurch leichter erweiterbar.
- Hohe Leistungsdichte.
- Die Blades werden zentral verwaltet.
- Schnelle und einfache Wartung.

Fachbegriff SAN

SAN (Storage Area Network):

- Ist ein Datenspeicher-Netzwerk in den großen Datenmengen gespeichert werden können.
- Der gesamte Speicher ist unabhängig von Standort und Betriebssystem, und wird zentral von Server verwaltet.
- Dabei werden einzelne Festplatten zu wenigen großen Speichergeräten virtuellen zusammengefasst. Sogenannte Disk Arrays. Oder Tape Librarys.
- Die Laufwerke müssen dabei nicht am selben Ort sein wie der Server.
- Die Zugriffe werden durch den zugreifenden Rechner verwaltet.
- Der freie Speicherplatz lässt sich mit einem SAN einfacher zuweisen.
- Das SAN wird parallel zum LAN betrieben.



Schnittstellen zur Verbindung vom Server zum SAN durch:

- Fibre Channel (meist genutzt, 90% Nutzauslastung)
- iSCSI
- Ethernet, Fast Ethernet, Gigabit-Ethernet (nur 20-60% Nutzauslastung)
- Infiniband

Zugriffsprotokolle für die Anwendungen:

- SCSI
- FCP (Fibre Channel Protocol)
- iSCSI (Internet SCSI)
- IFCP (Internet FCP)

Gateway und Tunneling-Protokolle:

- IPFC (IP over Fibre Channel)
- FCIP (Fibre Channel over IP)

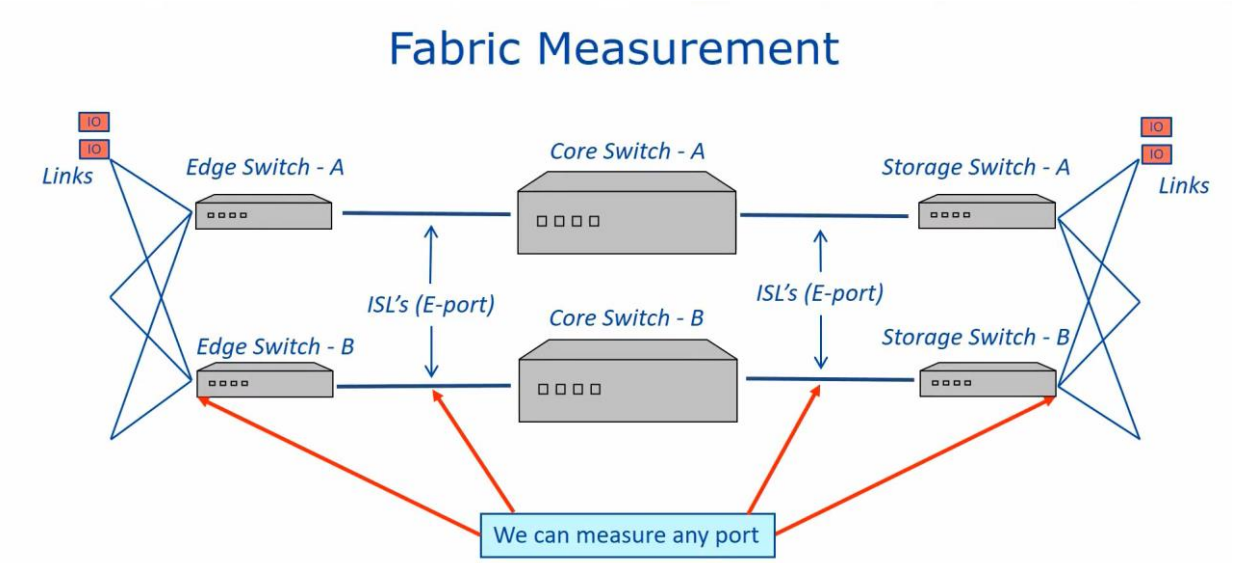
Transport-Protokolle:

- Fibre Channel

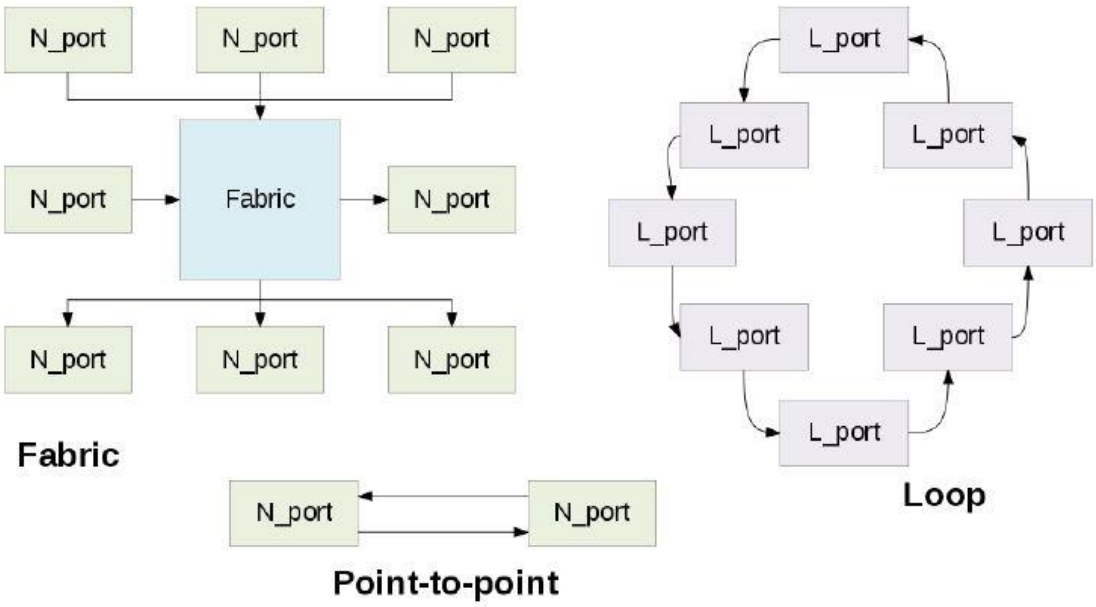
- TCP/IP
- UDP/IP

Fabric:

- Als Fabric bezeichnet man in einem SAN ein Netzwerk, das mehrere Anbindungen besitzt, und daher die Bandbreite und Redundanz verbessert.



- Ein SAN bestehend aus zwei eigenständigen Fabrics zur Redundanz und Steigerung der Bandbreite.
- Im Gegensatz zu Point to Point (direkte Verbindung vom Server zum Storage) und Arbitrated Loop, bei den Geräten als Kreis verbunden werden, bietet Fabric mehr Flexibilität und Skalierbarkeit, allerdings wird zusätzliche Hardware (Switche) benötigt.

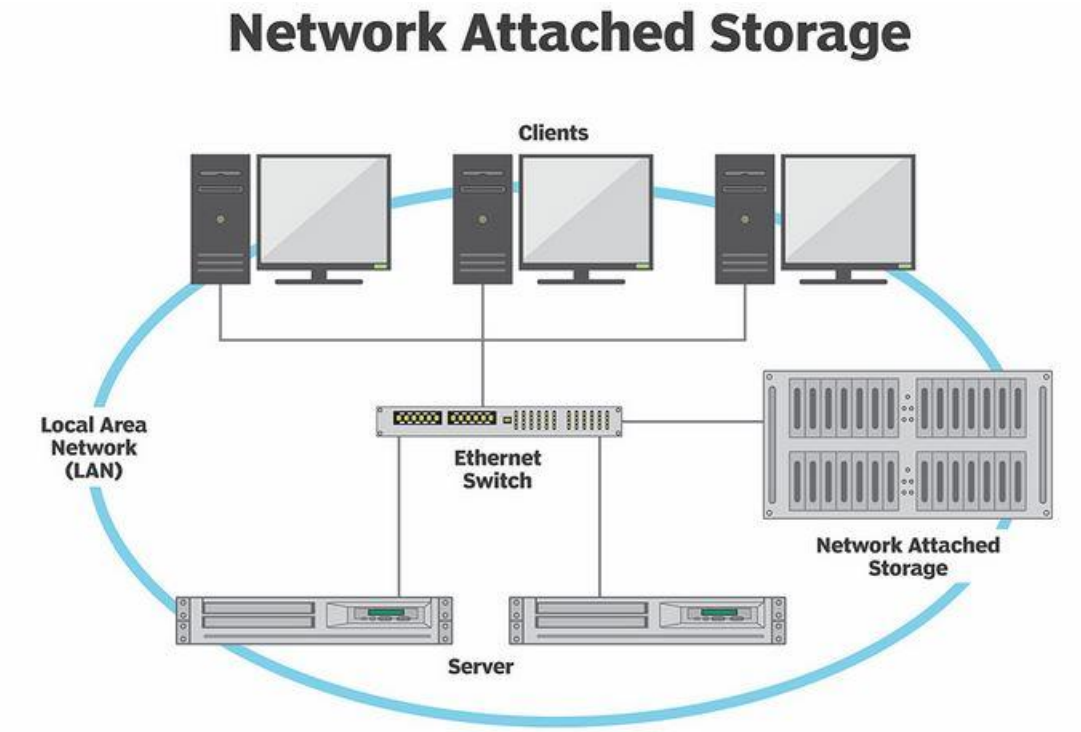


LUN (Logical Unit Numbers):

- LUNs dienen zum Adressieren von SCSI Protokoll Speicher. Dies können einzelne Platten oder Verbünde sein. Sind im Gegensatz zu den SCSI Device IDs nicht an die Hardware gebunden, und damit global einzigartig, sondern können zwischen verschiedenen Hosts variieren.

Kenntnisse über NAS-Systeme und deren Einsatzbereiche

NAS (Network Attached Storage):



Eine NAS ist ein Netzwerkspeicher, ein konfigurierbarer Datenspeicher, der in einem Netzwerk Speicherplatz und Dienste zur Verfügung stellt.

- Ist nicht an einen Server gebunden, sondern ein eigenständiges Gerät
- Wird eingesetzt um ohne viel Aufwand Speicherkapazität in einem Netzwerk bereitzustellen.
- Das NAS Gerät verwaltet die Speichermedien selbst.
- Es besteht aus einer oder mehrerer Festplatten, die für den Dauerbetrieb geeignet sind. (Disk Array)
- Je mehr Festplatten verwendet werden, umso höher ist die Kapazität, Sicherheit oder Geschwindigkeit.
- Verwendet die Hot-Plug Funktion, bei der Festplatten im laufenden Betrieb hinzugefügt und entfernt werden können.
- Es verwendet für die Übertragung die Protokolle: SMB/CIFS, NFS, AFP, http, FTP
- Verbindungsherstellung erfolgt über TCP/IP. Das geringe Performance und Latenzzeiten durch Protokoll Overheads verursacht.
- Benötigt weniger Strom als ein PC-System, und ist kosteneffizient.

Komponenten und Vorhandene Schnittstellen:

- Gehäuse, Platine, Netzteil, Lüfter, LAN, USB 3 für Erweiterungen oder für einen Printserver (Netzwerkdrucker), eSATA, Resetknopf;

Funktionen und Dienste:

- Fileserver, Medienserver, Webserver (HTTP, HTTPS, DDNS), Datensicherheit durch RAID, Active Directory Integration (Benutzer- und Rechteverwaltung, Freigaben).

Einsatz:

- Fileserver - Privat oder in Firmen, Medienserver, Sicherungslösung für Computer.

Fachbegriff Snapshot

- Unter Snapshot (Schnappschuss) versteht man eine Momentaufnahme eines Systems oder Objekts. Ein Wiederherstellungspunkt.
- Ein Snapshot/Schnappschuss speichert den Momentan Zustand einer bspw. Virtuelle Maschine, um sie zu einem späteren Zeitpunkt auf diesen Zustand zurücksetzen zu können.
- Es handelt sie dabei um die Kopie eines Datenträgers zu einem bestimmten Zeitpunkt. Datenänderungen, die nach dem Snapshot vorgenommen werden, bleiben unberücksichtigt.

Andere Beispiele:

- Bildschirmfoto
- Schnappschuss einer Internetseite (nicht nur vom Bildschirmausschnitt)
- Programmversion
- Massenspeicher – Snapshot von deinem Speicherbereich.
- Dateisystem – Zugriff auf ältere Versionen des Verzeichnisbaums.

Fachbegriff Daten-Redundanz

Eine Datenredundanz liegt vor, wenn in einem Datenbank- oder Datenspeichersystem dieselben Daten gehalten werden. Identische Daten können in zwei unterschiedlichen Feldern innerhalb einer einzigen Datenbank oder zwei unterschiedlichen Punkten in mehreren Softwareplattformen oder Umgebungen vorliegen.

- Datenredundanz bedeutet, dass die Daten mehrfach an verschiedenen Stellen gespeichert werden, damit die Daten im Falle eines Verlusts wiederhergestellt werden können.
- Dient zur Sicherung von Daten.
- Kann sich auch auf Netze, Übermittlungsstrecken, Protokolle, Geräte und Systemkomponenten beziehen.

Fachbegriff RAID-Level (0/1/5)

RAID (Redundant Array of Independent Disks):

- Ist ein Verbund von Festplatten zu einem logischen Laufwerk.
- Das Betriebssystem sieht dann nur ein Laufwerk.

Arten von RAID:

Software RAID:
- Software gesteuert
- Erhöhte CPU-Last
- niedriger I/O (= niedriger Datendurchsatz)
- Billig

Hardware RAID:
- „RAID-Controller"
- Eigene CPU und Pufferspeicher
- Kaum CPU-Last
- Relativ teuer
- Ersatz alter Controller oft schwierig

„Fake" RAID:

- „OnBoard Controller"
- meist abgespeckte Funktionalität (RAID 0, 1)
- Erhöhte CPU-Last

Ziele:
- Fehlertoleranz
- Geschwindigkeit
- Kapazität
- Gruppierung mehrerer Festplatten.
- Hot Swap (Austausch einer Festplatte im laufenden Betrieb).

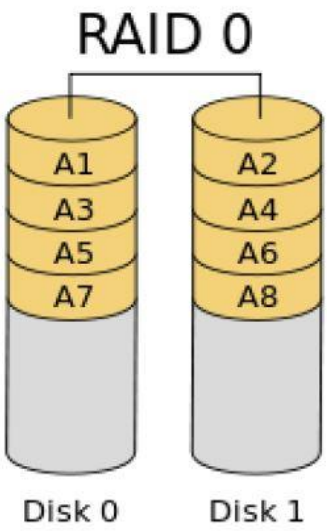
Vorteile:
- Erhöhung der Ausfallsicherheit (Redundanz).
- Steigerung der Transferraten (Performance).
- Aufbau großer logischer Laufwerke.
- Austausch von Festplatten während des Systembetriebs.

Nachteile:
- RAID-Controller meist teurer.
- Höhere Anforderungen an RAID-Controller.
- Bei Software RAID wird eine leistungsstarke CPU benötigt.
- Wiederherstellen der Daten nach Plattenausfall aufwändig.
- Systemleistung eingeschränkt.

Ist der Zusammenschluss mehrerer Speichermedien als Zusammenschluss zu einem logischen Laufwerk. Raid kann hardwareseitig durch Controller implementiert sein oder aber softwareseitig. Ziel ist die Erhöhung der Kapazität und der Leistung.

Kombinationsformen:

RAID 0:



Stripping:

- Die Daten werden auf alle zur Verfügung stehende Laufwerke aufgeteilt.
- Mindestens 2 Festplatten notwendig. Bei 2 Platten > Kapazität = 2 x die kleinste Platte

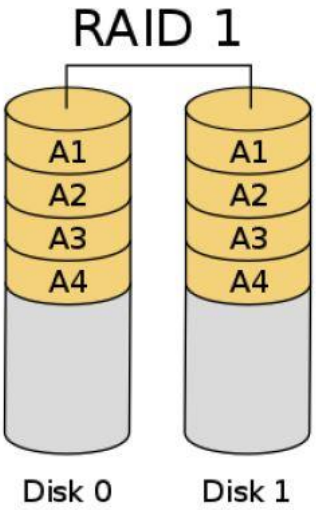
Vorteile:

- Bietet Beschleunigung und Kapazität zu erhöhen.
- Bietet keine Redundanz

Nachteile:

- Bei Ausfall einer Platte sind die Daten nicht mehr wiederherstellbar

RAID 1:



Mirroring: (Spiegelung)

- Die Daten werden gespiegelt, d.h. jeder Datenträger enthält alle Daten. (1:1)
- Mindestens 2 Festplatten notwendig. Bei 2 Platten > Kapazität = 1 x die kleinste Platte.

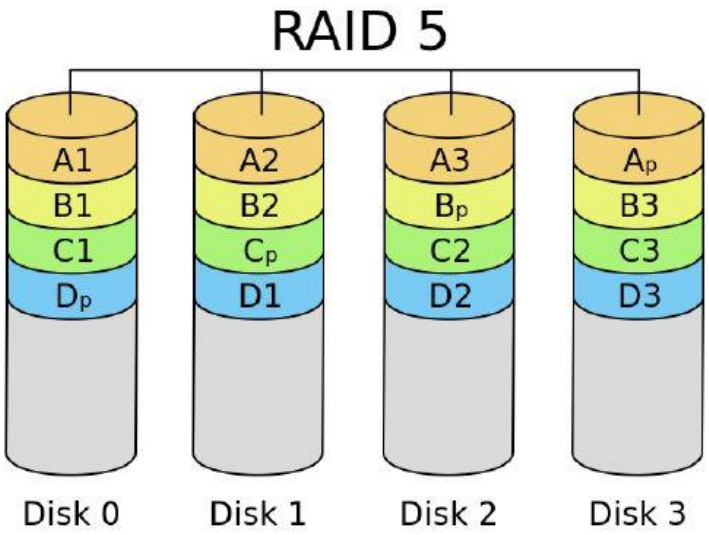
Vorteile:

- Kein Datenverlust bei Ausfall einer Platte.
- Bietet höhere Leseleistung, durch Lesen von mehreren Platten gleichzeitig.
- Bietet Vollständige Redundanz und Sicherheit.

Nachteile:

- Kein Kapazitätsgewinn
- Schreibleistung max. wie eine einzelne Festplatte.

RAID 5:



- Performance & Parität – Die Daten werden verteilt auf die Platten geschrieben
- Daten zur Rekonstruktion (Paritätsdaten) werden auf die Platten verteilt, so kann bei Ausfall eines Datenträgers anhand der Parität das Fehlende berechnet werden.
- Min. 3 Festplatten notwendig.
- Nutzbare Gesamtkapazität = s x (n-1)
- n … Anzahl der Platten
- s … Kapazität der kleinsten Platte
- Bsp.: 4 x 500 GB Festplatten
- (4-1) x 500 = 1500 GB Daten + 500 GB Parität
- Hot-Spare Festplatten - Austausch der Festplatte im laufenden Betrieb.
- Ist eine Reserve. Wenn eine Festplatte ausfällt, wird die Hot-Spare-Platte automatisch anstatt der defekten eingebunden.

Vorteile:

- Kein Datenverlust bei Ausfall einer Festplatte.
- Verbindet die Vorteile von RAID 0 und RAID 1:

Höhere Geschwindigkeit
Schafft Redundanz

- Kostengünstige Datenspeicher mit Redundanz.
- Aufbau großer logischer Laufwerke.

Nachteile:
- Bei Ausfall einer Festplatte geht die Geschwindigkeit zurück, weil die Daten aus der Parität berechnet werden müssen. Wiederherstellung aufwändig.
- Höhere Anforderung an den RAID-Controller.
- RAID-Controller meist teuer.

Fachbegriffe Hot-Plugging und Hot-Spare

Hot-Plugging:
- Festplattentausch während des Betriebs.
- Das heißt, wenn eine Festplatte im Betrieb ausfällt, kann sie während des Betriebs durch eine Hot-Spare Festplatte getauscht werden, ohne das Fehler entstehen.

Hot-Spare:
- Bezeichnet meist eine Festplatte die aktiv im System mitläuft (RAID 5), aber nicht genutzt wird.
- Wenn eine Festplatte ausfällt, springt die Hot-Spare Festplatte automatisch ein und übernimmt deren Aufgaben ohne Zeitverzögerung und zusätzlichen Eingreifen.

Fachbegriff Teaming in Zusammenhang mit Netzwerk-Ports

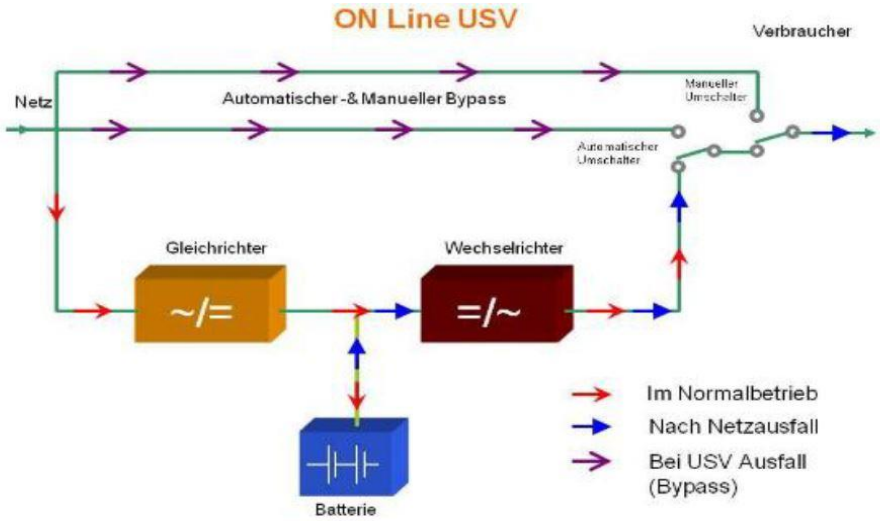
- Unter Teaming versteht man eine logische Netzwerkkarte (NIC), die mehrere physikalische Netzwerkkarten zu einer Gruppe zusammenfasst und so eine Redundanz von Netzwerkkarten erlaubt.
- Bei Ausfall einer physikalischen Netzwerkkarte ist die Verbindung nach einer Unterbrechung beinahe sofort wieder da.
- Es fällt im Schnitt höchstens ein Ping ab, meistens wird aber nichts bemerkt.

Unterscheidung von Offline- und Online-USV-Anlagen

Zweck von USVs:
- Störungsfreier Betrieb bei Stromausfall von wichtigen Geräten (Server, Router, SAN, NAS, …)
- Schutz vor Unter- und Überspannungen

Online USV:
Klasse 1
- Akku wird ständig geladen und entladen.
- Dabei wird durch einen Gleichrichter Wechselspannung in Gleichspannung umgewandelt und damit der Akku geladen.
- Entkopplung von Eingang und Ausgang.
- Keine Umschaltzeit auf Akku.
- Verbraucher werden dauerhaft mit besserer Qualität der Ausgangspannung versorgt.
- Liefert eine sinusförmige Ausgangsspannung.
- Keine Störspannungen, Frequenzstörungen und Spannungsverzerrungen.
- Nur 90% Wirkungsgrad (Dauerbelastung - Wärme und elektrische Verluste).
- Lebensdauer der Akkus beträgt wegen der Dauerbelastung nur 3 bis 4 Jahre.
- Einsatz bei Server
- Hohe Kosten

Funktionsweise:



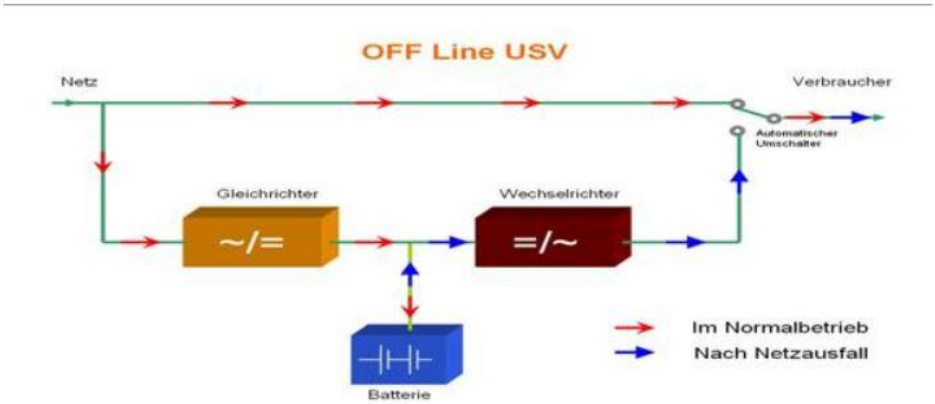
- Die angeschlossenen Geräte werden ständig von der USV Analog über den Wechselrichter mit Strom versorgt.
- Der Akku der USV Anlage wird ständig geladen und entladen.
- Bei Stromausfall werden die angeschlossenen Geräte von der USV Anlage versorgt.
- Es gibt keine Umschaltzeiten, und Spannungsspitzen werden ausgefiltert.

Offline USV:

Klasse 3

- Bietet bei Netzausfall Akkubetrieb.
- Umschaltdauer von 4-10 ms.
- Liefert eine Rechteck-ähnliche Ausgangsspannung (Für manche Geräte nicht geeignet).
- Schutz vor Netzausfall, kurzzeitige Spannungsschwankungen.
- Zu kurze Störungen werden nicht erkannt (kann Probleme verursachen).
- 95% Wirkungsgrad
- Einsatz bei einzelnem Computer.
- Niedrige Kosten

Funktionsweise:



- Die angeschlossenen Geräte werden im Normalbetrieb über das öffentliche Stromnetz versorgt.
- Bei Stromausfall schaltet die USV innerhalb von 10ms auf Batteriebetrieb.

Fragen vor der Anschaffung:

- Welche Geräteklasse?
- Wie viel Shutdown-Zeit benötige ich?
- Wie viel Leistung benötige ich?
- Wie viel Überbrückungszeit benötige ich?
- Welche Bauarten sind möglich? (Rack, Standgerät, Einbau-USV, Zugänglichkeit).

Leistung:

- Scheinleistung bzw. Gesamtleistung ist, was aus dem Stromnetz gezogen wird.
- Wirkleistung ist was beim Verbraucher ankommt.
- Blindleistung ist die überschüssige Energie die mehr fließt als der Verbraucher aus dem Stromnetz gezogen hat.

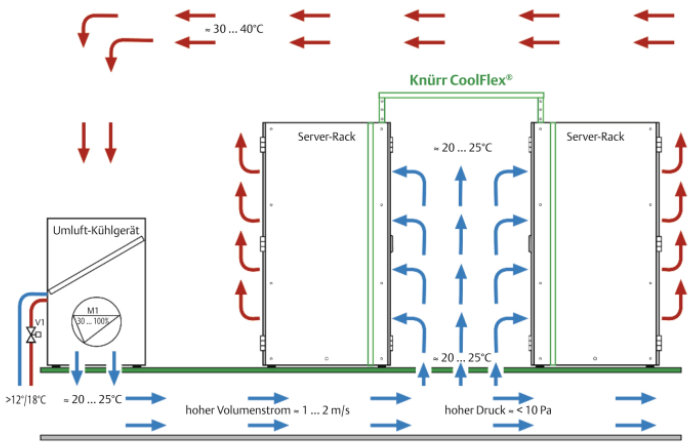
Kenntnisse über optimale Klimatisierung in Rechenzentren

Kalt/Warm Gang Konzept:

- Bau eines Doppelten Bodens. Dazwischen ein Kalt Gang durch dem die Luft zirkuliert. An der Decke ist ein Warm Gang installiert.
- Die Serverschränke sind immer Rücken an Rücken, und Vorne an Vorne angeordnet. Zwischen denn Vorderseiten der Schränke strömt die Kalte Luft. An den Rückseiten strömt die warme Luft nach oben.

Funktionsweise:

- Ein Umluft-Kühlgerät bläst die kalte Luft in den Kalt-Gang.
- Durch Öffnungen im Boden gelangt die kalte Luft zu den Serverschränken.
- Die kalte Luft wird von den Lüftern des Servers angesaugt, strömt durch ihn hindurch und wird auf der Rückseite des Servers rausgeblasen. Die warme Luft steigt auf und gelangt durch Zirkulation wieder zum Umluft Kühlgerät.
- Luftfeuchtigkeit darf nicht zu hoch sein. Es entsteht Kondenswasser > das kann zu Korrosionsschäden an den Geräten führen.
- Nicht einfach Lüften. Es muss eine Zirkulation von kalter Luft herrschen.
- Die Racks müssen so ausgerichtet sein, dass die Server mit der jeweils zu kühlenden Seite in den Kalt-Gang zeigen.
- Konsequent abgedichtete/abgeschottete Kaltgänge damit die kalte Luft effizient die Server kühlen kann.



Kenntnisse über Zutrittsschutz/Zutrittskontrolle bei Rechenzentren

Zutrittsschutz:

- Eine Brandschutztür mit einem Sicherheitsschloss, wobei nur befugte Personen Zugang mit dem Schlüssel bekommen.
- Eingeschränkter Personenkreis, sicherheitsüberprüfte Personen.

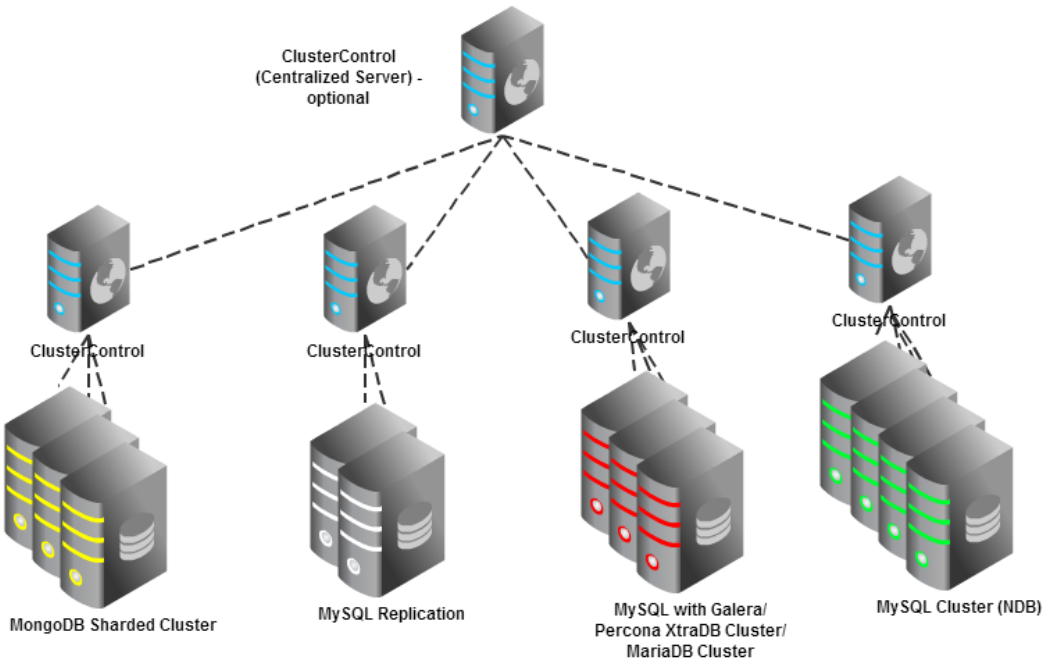
Zutrittskontrolle:

- Mit einer Smartcard wobei mit protokolliert wird Wer Wann sich Zugang verschafft hat.
- 2 Faktor Authentifizierung mit z.B. Schlüsselkarte und Biometrie, Finger-Scan, Iris-Scan, Face-Scan;

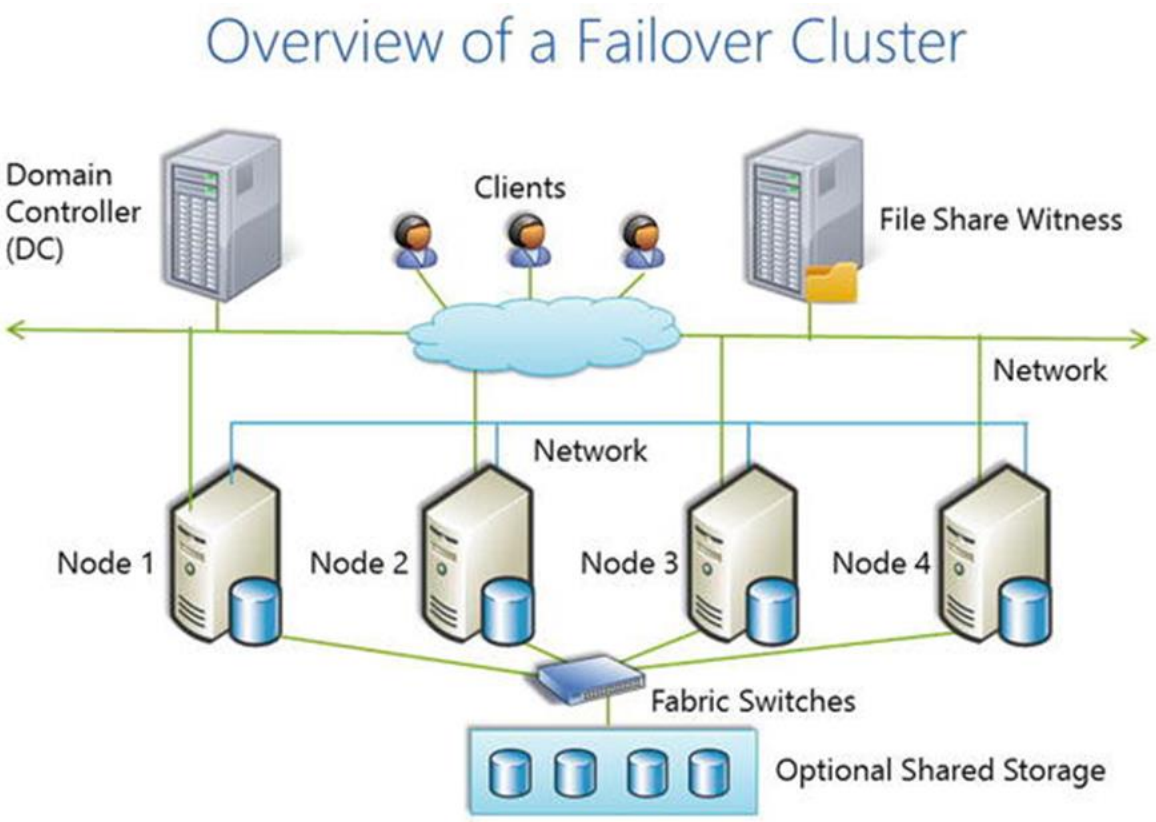
Kenntnisse über Cluster-Technologien (High Availability, Heart-Beat)

Cluster:

- Ein Cluster bezeichnet eine Anzahl von vernetzten Computern. Ein Rechnerverbund.
- Dadurch erhöht sie die Rechenkapazität und die Verfügbarkeit.
- Die im Cluster befindlichen Computer werden auch als Serverfarm bezeichnet.



High Availability Cluster bzw. Failover Cluster:



- Werden zum Schutz von geschäftskritischen Applikationen eingesetzt.
- Dabei werden alle zum Betrieb nötigen Komponenten und die Applikation ständig auf Funktionsfähigkeit getestet.
- Auch die Hardware, das Betriebssystem und die Netzwerkverbindung werden überwacht und geschützt.
- Im Fehlerfall wird durch die Clustersoftware ein Failover ausgelöst, wenn der zuvor veranlasste Neustart der Applikation erfolglos war.
- Wird die Umschaltung der Applikation auf einen anderen Node (ein Computer des Clusters) manuell ausgelöst, spricht man von einem Switch Over. In diesem Fall entfällt der Versuch der Reininitialisierung.
- High Availability Cluster bestehen normalerweise aus wenigen Cluster Nodes (max. 64).

Heartbeat:

- Ist eine Netzwerkverbindung zwischen zwei (oder mehr) Rechnern in einem Cluster, um sich gegenseitig darüber zu benachrichtigen, dass sie betriebsbereit sind und ihre Aufgaben noch erfüllen können, also „am Leben" sind. Das geschieht mittels keepalive und hello Nachrichten über dem Protokoll OSPF.
- Wenn die Benachrichtigung ausbleibt, sorgt ein Programm dafür das dessen Aufgaben ein anderer Rechner übernimmt.
- Bei Windows Servern wird diese Funktion auch Failover Cluster genannt, welches über den Server Manager für alle Server der Domain konfiguriert werden kann.

Kenntnisse über Hypervisor-Technologien (XEN, KVM, ESX, Hyper-V)

XEN (Xen Project):

- Typ 1-Hypervisor (läuft direkt auf der Hardware)
- von Citrix
- Eigenes Server Betriebssystem
- Ermöglicht Clustering
- Ist eine kostenlose Software
- Für Linux Betriebssysteme

KVM (Kernal-based Virtual Maschine):

- Typ 1-Hypervisor (läuft direkt auf der Hardware)
- Für Linux- Betriebssysteme

ESXi (vormals ESX):

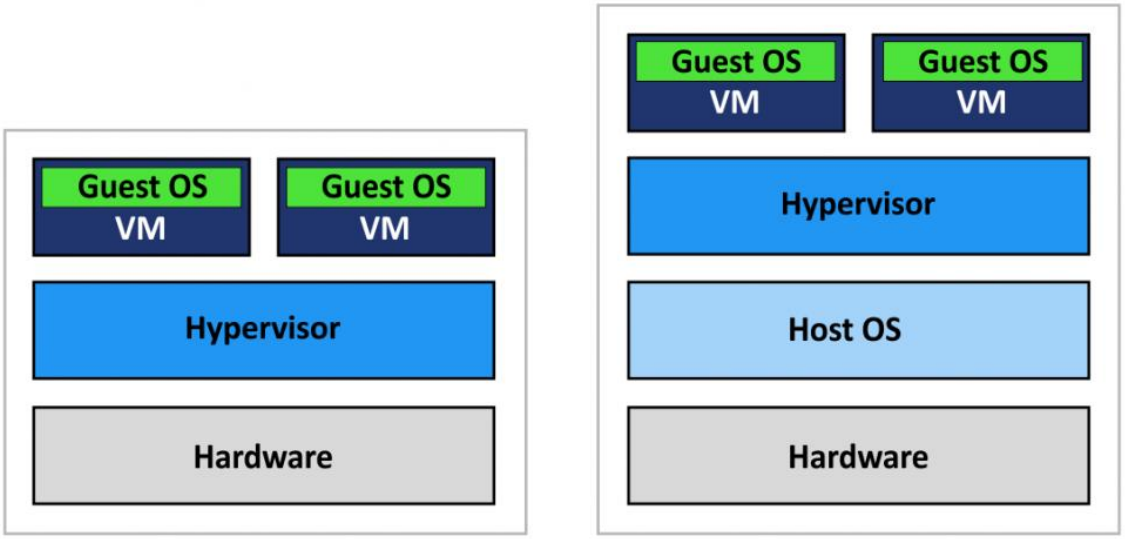
- Von VMWare.
- Typ 1-Hypervisor (läuft direkt auf der Hardware).
- Besitzt eigenen Kernel.

Hypervisor = (Vitalisierung)

- Ein Hypervisor erstellt und verwaltet Virtuelle Maschinen.
- Er stellt die Schnittstellen innerhalb der Virtuellen Maschine zur Verfügung.
- Er verhindert den Zugriff der Treiber auf die Hardware damit sich verschiedene Betriebssysteme nicht in die Quere kommen.

Zwei Hypervisor-Typen:

Der Typ 1-Hypervisor läuft als Betriebssystem direkt auf der Hardware. Er muss alle Treiber mitbringen. Das Gesamtsystem verbraucht wenig Ressourcen.



Type 1 Hypervisor
(Bare-Metal Architecture)

Type 2 Hypervisor
(Hosted Architecture)

Der Typ 2-Hypervisor setzt auf dem vollwertigen Betriebssystem auf (hosted) und nutzt alle Ressourcen, die in dieser Umgebung zur Verfügung stehen.

Hyper-V

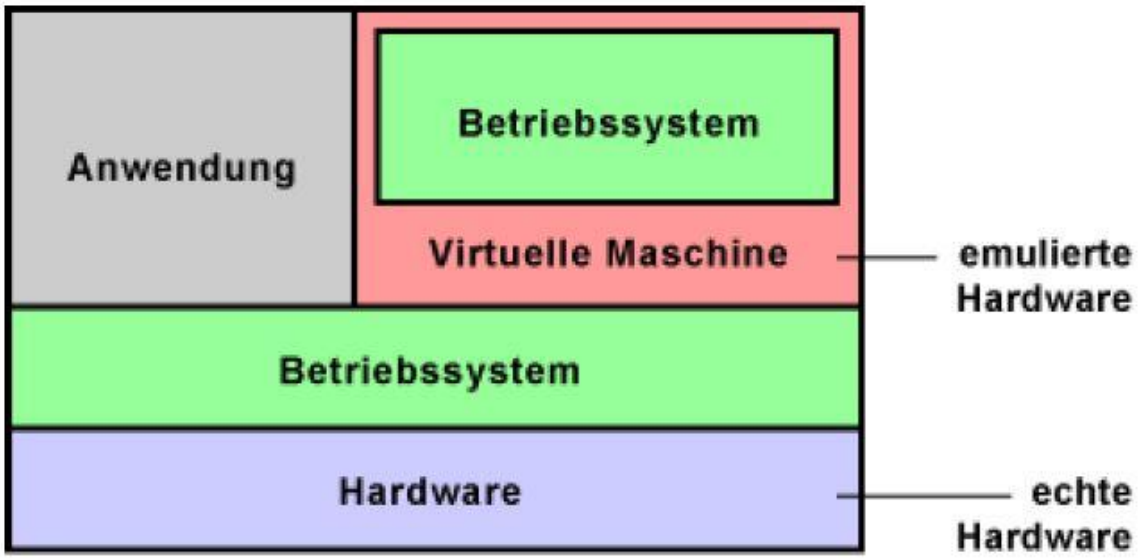
- Typ 1- Hypervisor (läuft direkt auf der Hardware)
- Ist eine Virtualisierungstechnologie von Microsoft für Computer mit x64-fähigem x86-Prozessor.
- Ist in Windows 8 und Windows 10 bereits integriert.
- Ermöglicht Clustering.

Typ 2 (hosted):

- VMware Workstation/Player (VMware)
- Windows Virtual PC (Microsoft)
- VirtualBox (Oracle)
- Parallels Workstation

3 Methoden der Virtualisierung:

Virtuelle Maschine:

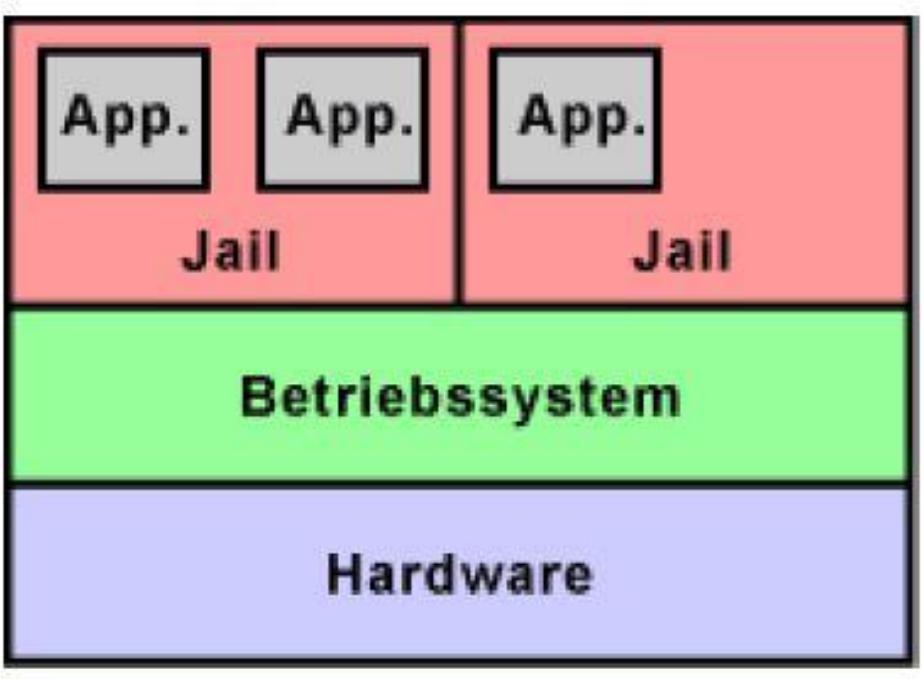


- Die Virtuellen Maschinen können unterschiedliche Betriebssysteme nutzen.
- Sie sind komplett unabhängig voneinander, und können reboot werden, ohne das die anderen davon beeinflusst werden.
- Verfügt über eine eingeschränkte Grafikleistung.
- Die Hardware steht der Maschine nicht direkt zur Verfügung
- Die Virtualisierungssoftware überwacht den Zugriff auf die Hardware, organisiert und verwaltet sie. Das geschieht durch den Hypervisor.

Paravirtuelle Maschinen:

- Gleiches Prinzip wie bei Virtueller Maschine. Nur das die Virtuellen Maschine voneinander wissen, und die angeforderte Rechenleistung der anderen kennen.

Virtualisierung des Betriebssystems:



- Es gibt nur ein Betriebssystem. Darauf laufen virtuelle Laufzeitumgebungen (Jails) die für die Programme als normale Betriebssystem wirken.
- Die Maschinen agieren unabhängig voneinander.
- Das Betriebssystem des Servers übernimmt alle Funktionen, alle Maschinen laufen auf dem gleichen Betriebssystem.

Kenntnisse über Virtualisierung (Server-Virtualisierung/Desktop-Virtualisierung)

Server Virtualisierung:

- Bei einer Server-Virtualisierung kann man mit einer Software virtuelle Maschinen auf einem physischen Server betreiben. (VMware, VirtualBox, Hyper-V)
- Die virtuellen Maschinen sind isoliert voneinander, nutzen aber gemeinsam die Rechnerleistung des physischen Servers.

Vorteile:

- Physische Server werden nicht ausgelastet.
- Einsparen von Hardware, mehr Platz
- Weniger Stromverbrauch
- Ausfallsicherheit (Fällt ein Server aus laufen die anderen weiter)
- Leichtes Testen (Testen neuer Applikationen auf extra gekauten Servern fällt weg)
- Umstellung bei neuer Hardware (Anwendungen die bestimmte Hardware oder ein altes Betriebssystem benötigen können einfach auf Virtuale Maschinen, die die alte Umgebung imitiert, verschoben werden)

Nachteile:

- Ausfall aller VM bei Ausfall des Wirtssystems ergibt ein erhöhtes Risiko.
- Ungenaue Zeitscheiben.
- Höhere Latenzzeiten mit mehr VM pro System.

Desktop Virtualisierung:

- Bei der Desktop Virtualisierung werden Workstation PCs auf einem Server virtualisiert.
- Der Client braucht sich dann nur mehr über Remote zum Server verbinden.
- Das bietet Sicherheit, da der Server redundant aufgebaut ist, und abgesichert ist.
- Anwendungen können über Remote Dienste virtualisiert werden.
- Bei Betriebssystem-Streaming wird ein Image vom Server auf den Client gestreamt
- Das gestreamte Betriebssystem verhält sich so als wäre es am Client installiert.
- Das kann benutzt werden (Infrastruktur ist bei einem Drittanbieter, der sich um die gesamte Server-Konfiguration kümmert.

Vorteile:

- Benutzer kann beinahe von jedem Gerät aus Remote arbeiten.
- Geringe Kosten für die Hardware der Clients.

Nachteile:

- Große Datenlast und hohe Latenzen. Wenn Daten fließen, dann brauchen Sie nicht nur Zeit, sondern auch die entsprechende Bandbreite.
- Online-Zwang für Arbeitsplätze. Wenn der Server nicht im eigenen Gebäude steht, geht ohne Internet nichts mehr.
- Höhere Serverkosten.