

Block 1: Einführung

- Auftrag 1.1: Grundlagen der Virtualisierung
- Auftrag 1.2: Physikalische Hardware
- Auftrag 1.3: Virtualisierungstypen
- Info: Zugangsdaten hosttech
- Auftrag 1.4: Remote Management

Auftrag 1.1: Grundlagen der Virtualisierung

1. Vorteile der Virtualisierung:

- **Effizienzsteigerung:** Bessere Auslastung von Hardware-Ressourcen.
- **Kostenersparnis:** Reduzierung von Hardware- und Energiekosten.
- **Flexibilität:** Schnelle Bereitstellung und Skalierung von Ressourcen.
- **Isolation:** Getrennte Betriebsumgebungen erhöhen die Sicherheit.
- **Wartung:** Einfachere Backups, Updates und Disaster Recovery.

2. Nachteile der Virtualisierung:

- **Leistungseinbußen:** Overhead durch den Virtualisierungslayer.
- **Komplexität:** Management und Überwachung können komplizierter werden.
- **Lizenzkosten:** Kosten für Virtualisierungssoftware und möglicherweise erhöhte Lizenzkosten für Betriebssysteme und Anwendungen.
- **Sicherheitsrisiken:** Hypervisor kann ein zusätzliches Angriffsziel sein.

3. TCO (Total Cost of Ownership): TCO bezeichnet die Gesamtbetriebskosten eines IT-Systems über seine gesamte Lebensdauer, einschließlich Anschaffung, Wartung, Betrieb und Entsorgung.

4. Sinkende TCO durch Virtualisierung:

- **Hardware-Einsparungen:** Weniger physische Server sind notwendig.
- **Energieeffizienz:** Reduzierung des Energieverbrauchs.
- **Administrative Effizienz:** Zentralisiertes Management spart Zeit und Personalressourcen.
- **Reduzierte Ausfallzeiten:** Verbesserte Disaster-Recovery-Optionen und schnellere Wiederherstellung.
- **Schulungs oder Wartungskosten**

5. Server Konsolidierung:

- Das Zusammenfassen mehrerer physischer Server auf weniger oder einem einzelnen physischen Server durch Virtualisierung. Ziel ist die Reduzierung der Anzahl der benötigten Hardware-Server und die Steigerung der Auslastung der vorhandenen Hardware.

6. Drei Virtualisierungsprodukte:

- **VMware vSphere:** Weit verbreitete Virtualisierungslösung.
- **Microsoft Hyper-V:** Virtualisierungslösung von Microsoft.
- **Citrix XenServer:** Open-Source-basierte Virtualisierung.

7. Erfahrung mit Virtualisierungsprodukten:

- Eigenes vCenter zuhause aufgebaut und ich arbeite auch in der Firma mit vSphere. Erfahrungen auch schon mit proxmox gesammelt

8. LXC und OpenVZ:

- **LXC (Linux Containers) und OpenVZ:** Eine Virtualisierungstechnologie auf Betriebssystemebene, die es ermöglicht, mehrere isolierte Linux-Systeme (Container) auf einem Host zu betreiben. (OpenSource)

Auftrag 1.2: Physikalische Hardware

1. CPU:

- **Hohe Kernanzahl:** Mehr Kerne ermöglichen die parallele Ausführung mehrerer virtueller Maschinen (VMs).
- **Virtualisierungsfunktionen:** CPU-Features wie Intel VT-x oder AMD-V zur Verbesserung der Virtualisierungsleistung.
- **Gute Leistung pro Kern:** Wichtig für VMs, die einzelne leistungsstarke Kerne benötigen.
- **Skalierbarkeit:** Möglichkeit, die CPU später bei Bedarf aufzurüsten.

2. Memory (Arbeitsspeicher):

- **Große Kapazität:** Jede VM benötigt eigenen Speicher. Hohe Gesamtkapazität ist wichtig.
- **Hohe Geschwindigkeit:** Schneller RAM kann die Gesamtleistung verbessern.
- **Erweiterbarkeit:** Möglichkeiten zur späteren Aufrüstung sollten vorhanden sein.
- **Fehlerkorrektur (ECC):** Reduziert das Risiko von Datenkorruption, wichtig für Serverstabilität.

3. Festplattencontroller und Disks:

- **Schnelle Disk-Zugriffszeiten:** SSDs sind herkömmlichen HDDs vorzuziehen, insbesondere für hohe I/O-Anforderungen.
- **RAID-Konfiguration:** Für erhöhte Datensicherheit und Leistung. RAID 10 bietet eine gute Balance zwischen Geschwindigkeit und Datensicherheit.
- **Große Speicherkapazität:** Für die Speicherung von VM-Images und Daten.
- **Skalierbarkeit und Flexibilität:** Möglichkeit zur Erweiterung des Speichers.

4. Netzwerkkarten:

- **Hohe Bandbreite:** Gigabit- oder 10-Gigabit-Ethernet, um den Datenverkehr effizient zu bewältigen.
- **Mehrere Anschlüsse:** Ermöglicht die Trennung von Verwaltungs-, Speicher- und Anwendungsverkehr.
- **Unterstützung für Netzwerkvirtualisierung:** Features wie SR-IOV können die Leistung verbessern.
- **Zuverlässigkeit und Qualität:** Server-grade Netzwerkkarten wählen, die Dauerbelastung standhalten.

Auftrag 1.3:

Virtualisierungstypen

1. Unterschiede zwischen Hypervisor Typ 1 und Typ 2:

- **Typ 1 (Bare-Metal):** Direkt auf der Hardware installiert, ohne zugrundeliegendes Betriebssystem. Bietet höhere Leistung und Effizienz, da eine zusätzliche Betriebssystemschicht entfällt. Beispiele: VMware ESXi, Microsoft Hyper-V (wenn direkt installiert). (Ressourcen werden vom HV Gemanaged)
- **Typ 2 (Hosted):** Läuft auf einem vorhandenen Betriebssystem (wie Windows, Linux). Einfacher in der Einrichtung und Verwendung, aber mit potenziellem Leistungsverlust durch das zusätzliche Betriebssystem. Beispiele: VMware Workstation, Oracle VirtualBox. (Ressourcen werden vom OS Gemanaged)

2. Applikationsvirtualisierung:

- Dabei wird eine Anwendung vom Betriebssystem isoliert. Die Anwendung wird auf einem Server ausgeführt und auf dem Client angezeigt, als ob sie lokal installiert wäre. Dies ermöglicht eine zentrale Verwaltung und Verteilung von Software, ohne dass die Anwendung auf jedem Endgerät installiert werden muss. Mehrere Versionen.

3. Desktop-Virtualisierung (VDI):

- VDI (Virtual Desktop Infrastructure) bezieht sich auf das Hosting von Desktop-Umgebungen auf einem zentralen Server. Diese virtuellen Desktops werden dann über das Netzwerk an Endbenutzergeräte übertragen. VDI ermöglicht Flexibilität, zentrale Verwaltung und Zugriff von verschiedenen Geräten aus.

4. Unterschiede zwischen Containern und virtuellen Maschinen:

- **Isolierungsebene:** Container virtualisieren auf Betriebssystemebene und teilen sich das gleiche Betriebssystemkernel, während VMs die gesamte Hardware inklusive des Betriebssystems virtualisieren.
- **Ressourceneffizienz:** Container sind in der Regel leichtgewichtiger und starten schneller, da sie weniger Ressourcen benötigen (kein separates Betriebssystem pro Container).
- **Portabilität:** Container bringen ihre eigenen Bibliotheken und Abhängigkeiten mit, was sie portabler und konsistenter über verschiedene Umgebungen hinweg macht.
- **Sicherheit:** VMs bieten eine stärkere Isolierung, da sie vollständig separate Betriebssysteminstanzen haben. Bei Containern besteht ein höheres Risiko, dass Prozesse auf den Host oder andere Container zugreifen.

5. Unterschiede zwischen Emulation und Virtualisierung:

- **Emulation:** Ein Emulator ahmt eine andere Hardware- oder Softwareumgebung nach und ermöglicht es, darauf ausgelegte Programme auszuführen. Es ist oft langsamer, da jede Operation des emulierten Systems nachgebildet werden muss.

- **Virtualisierung:** Bezieht sich auf die Erstellung einer virtuellen Version einer IT-Ressource wie eines Betriebssystems, eines Servers oder eines Netzwerks. Virtualisierung nutzt die tatsächliche Hardware effizienter, indem sie mehrere Betriebssysteme und Anwendungen auf einer einzigen physischen Hardware ausführt.

6. Weitere virtualisierbare physische IT-Ressourcen neben Servern:

- **Speicher:** Virtualisierung von Speicherressourcen (wie SAN oder NAS) zur effizienten Nutzung und Verwaltung von Speicherplatz.
- **Netzwerk:** Netzwerkvirtualisierung, um Netzwerkressourcen wie Switches, Router und Bandbreite zu abstrahieren und zu verwalten.
- **Desktops:** Wie bereits bei VDI erwähnt, die Virtualisierung von Desktop-Umgebungen.
- **Anwendungen:** Applikationsvirtualisierung, um Anwendungen von den zugrundeliegenden Betriebssystemen zu trennen.
- **Daten:** Virtualisierung von Datenbanken und Datenspeicher, um eine flexible und effiziente Datenverwaltung zu ermöglichen.
- **GPU:** Virtualisierung von Grafikprozessoren für Anwendungen, die hohe Grafikleistung benötigen, aber physisch getrennt sind.

Info: Zugangsdaten hosttech

1. **Verfügbare physische Server:** Es scheint, dass Sie Zugang zu mehreren physischen Servern haben, die über verschiedene iLO-Adressen erreichbar sind. Jeder dieser Server ist anscheinend über eine einzigartige URL und Port-Kombination zugänglich, beispielsweise `https://ilo.zli.hosttech.eu:4401`, `https://ilo.zli.hosttech.eu:4402`, usw., bis `https://ilo.zli.hosttech.eu:4415`. Dies deutet auf mindestens 15 physische Server hin.
2. **Zugriff auf die physischen Server:** Sie können auf diese Server über die iLO (Integrated Lights-Out) Schnittstelle zugreifen. Dazu müssen Sie die entsprechende URL im Webbrowser aufrufen und sich mit den bereitgestellten Benutzernamen (wie "ZLI-Teilnehmer") und Kennwörtern anmelden. Jeder Server hat eine spezifische Portnummer (z.B. 4401, 4402, usw.), die in der URL angegeben ist.
3. **Öffentliche IP-Adressen für virtuelle Maschinen:** Für jede iLO-Verbindung sind zwei öffentliche IP-Adressen angegeben. Es ist jedoch nicht klar definiert, ob diese speziell für virtuelle Maschinen gedacht sind. In der Regel werden öffentliche IP-Adressen für den Fernzugriff auf die Server selbst verwendet, nicht unbedingt für darauf gehostete virtuelle Maschinen. Sie sollten überprüfen, ob diese IP-Adressen für virtuelle Maschinen verwendet werden können oder ob sie speziell für den iLO-Zugang reserviert sind.
4. **IP des Storage Servers:** Der Storage Server, benannt als "zli11-storage.hosttech.eu", hat die IP-Adresse 213.167.226.31. Dieser Server wird über das TrueNAS-System verwaltet, und Sie können sich mit dem Benutzernamen "zli-nas" und dem Kennwort "d5MG5ZNK0s" anmelden.

https://moodle.zli.ch/pluginfile.php/190030/mod_page/content/11/UeK-190_Kurs-243774.pdf?time=1704891712170

Auftrag 1.4: Remote Management

1. iLO, DRAC und IPMI:

- **iLO (Integrated Lights-Out):** Dies ist eine proprietäre Embedded-Server-Management-Technologie von Hewlett Packard Enterprise, die in ihren ProLiant-Servern verwendet wird. Es ermöglicht die Fernsteuerung von Servern unabhängig vom Betriebsstatus des Servers.
- **DRAC (Dell Remote Access Controller):** Ähnlich wie iLO ist DRAC eine proprietäre Technologie von Dell, die in Dell-Servern für Fernwartungsaufgaben eingesetzt wird.
- **IPMI (Intelligent Platform Management Interface):** Dies ist ein standardisiertes Computer-Interface, das verwendet wird, um Hardware-Geräte in Servern zu überwachen, zu verwalten und Fehler zu melden. Es ist eine branchenweite Spezifikation.

2. Zweck von Remote Server Management Lösungen:

- Diese Lösungen werden eingesetzt, um Serverhardware aus der Ferne zu überwachen, zu verwalten und zu warten. Sie ermöglichen es, auf das System zuzugreifen, Einstellungen zu ändern, das System neu zu starten und Probleme zu diagnostizieren, ohne physisch vor Ort sein zu müssen.

3. Prozessoren im Server:

- Die Anzahl und Art der Prozessoren in Ihrem Server kann ich nicht spezifizieren, da ich keinen Zugriff auf Ihre spezifische Hardware habe. Diese Information finden Sie normalerweise in der Dokumentation Ihres Servers oder über das Server-Management-Interface.

4. Verfügbarer Speicher (Memory):

- Auch hier kann ich keine spezifischen Informationen über die Menge des in Ihrem Server verfügbaren Speichers geben. Diese Information lässt sich in der Regel über das Server-Management-Interface einsehen.

5. Serverneustart:

- Über das Remote Management Interface können Sie den Server in der Regel durch eine entsprechende Option im Menü oder durch Eingabe eines spezifischen Befehls neu starten.

6. Server von einem ISO Image starten:

- Viele Remote Management Lösungen erlauben es Ihnen, das System von einem ISO-Image zu starten, das Sie über das Interface hochladen oder an eine virtuelle Laufwerkseinheit binden können.

7. Zugriff auf Tastatur, Bildschirm und Maus:

- Remote Management Lösungen bieten in der Regel eine KVM-over-IP-Funktion (Keyboard, Video, Mouse), mit der Sie über das Internet Zugriff auf die Tastatur, den Bildschirm und die Maus des Servers erhalten, als ob Sie direkt davor säßen.

8. Bedeutung der Abkürzung iLO:

- iLO steht für "Integrated Lights-Out". Es handelt sich um eine Technologie, die speziell für das Servermanagement außerhalb der regulären Betriebsstunden entwickelt wurde, was den Namen "Lights-Out" (Lichter aus) erklärt.