

13.3 Hypervisor und VM-Verwaltung

Einordnung

Diese Seite gehört zum Kapitel:

Server, Virtualisierung und Hochverfügbarkeit

Auf der vorherigen Seite ging es um Virtualisierung und virtuelle Maschinen.

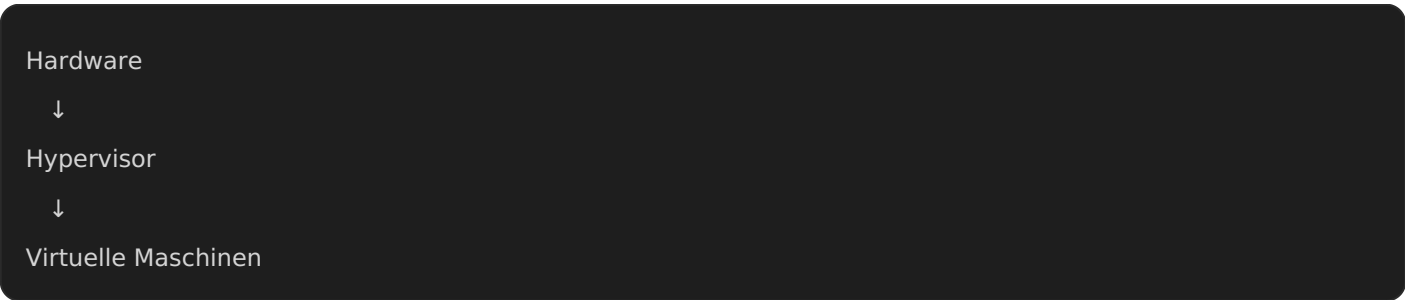
Jetzt geht es genauer um den **Hypervisor** und die praktische Verwaltung von virtuellen Maschinen.

Was ist ein Hypervisor?

Ein Hypervisor ist die Virtualisierungsschicht, die virtuelle Maschinen bereitstellt und verwaltet.

Er sitzt zwischen der physischen Hardware und den virtuellen Maschinen.

Vereinfacht:



Der Hypervisor sorgt dafür, dass mehrere virtuelle Maschinen gleichzeitig auf einem physischen Server laufen können.

Merksatz

Der Hypervisor verwaltet virtuelle Maschinen und teilt ihnen CPU, RAM, Storage und Netzwerk zu.

Aufgaben eines Hypervisors

Aufgabe	Erklärung
VMs erstellen	Neue virtuelle Maschinen anlegen
VMs starten	Virtuelle Maschinen hochfahren
VMs stoppen	Virtuelle Maschinen herunterfahren oder ausschalten

Aufgabe	Erklärung
Ressourcen zuteilen	CPU, RAM, Storage und Netzwerk bereitstellen
Virtuelle Hardware verwalten	vCPU, vRAM, vDisk und vNIC konfigurieren
Snapshots verwalten	Zustände von VMs speichern
Backups unterstützen	Sicherung von VMs ermöglichen
Migration ermöglichen	VMs auf andere Hosts verschieben
Netzwerk bereitstellen	Virtuelle Switches und VLANs verwalten
Monitoring unterstützen	Auslastung und Zustand überwachen
Rechte verwalten	Zugriff für Administratoren steuern

Typ-1-Hypervisor

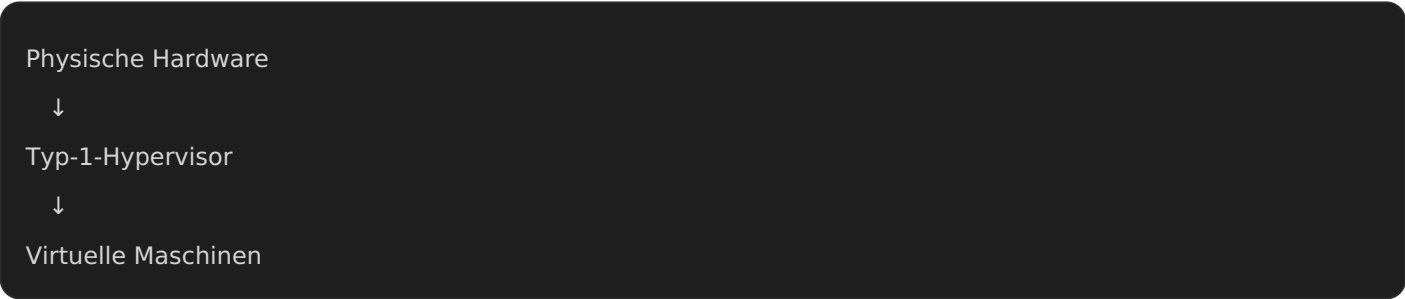
Ein Typ-1-Hypervisor läuft direkt auf der physischen Hardware.

Er wird auch Bare-Metal-Hypervisor genannt.

Beispiele:

Hypervisor	Beschreibung
VMware ESXi	Häufig in Unternehmensumgebungen
Microsoft Hyper-V	Microsoft-Virtualisierung
Proxmox VE	Open-Source-Virtualisierungsplattform
KVM	Linux-basierte Virtualisierung
Xen	Virtualisierungstechnologie
Nutanix AHV	Hypervisor von Nutanix

Typischer Aufbau:



Vorteil:

Typ-1-Hypervisoren sind für produktive Serverumgebungen geeignet.

Typ-2-Hypervisor

Ein Typ-2-Hypervisor läuft auf einem vorhandenen Betriebssystem.

Beispiele:

Hypervisor	Einsatz
VirtualBox	Test- und Lernumgebungen
VMware Workstation	Desktop-Virtualisierung
VMware Fusion	macOS-Virtualisierung
Parallels Desktop	macOS-Virtualisierung
UTM	macOS / Apple Silicon

Typischer Aufbau:



Typ-2-Hypervisoren sind gut zum Lernen und Testen, aber weniger typisch für produktive Serverumgebungen.

Typ-1 vs. Typ-2-Hypervisor

Merkmal	Typ-1-Hypervisor	Typ-2-Hypervisor
Läuft auf	Direkt auf Hardware	Auf vorhandenem Betriebssystem
Einsatzgebiet	Server, Rechenzentrum, Unternehmen	Desktop, Test, Lernen
Performance	Hoch	Meist geringer
Stabilität	Sehr hoch	Abhängig vom Host-Betriebssystem
Beispiele	ESXi, Hyper-V, Proxmox	VirtualBox, VMware Workstation
IHK-Relevanz	Sehr wichtig	Grundlegend wichtig

Virtualisierungsplattform

Eine Virtualisierungsplattform besteht nicht nur aus dem Hypervisor.

Dazu gehören oft auch Verwaltung, Netzwerk, Storage, Backup und Clusterfunktionen.

Beispiele:

Plattform	Bestandteile
VMware vSphere	ESXi, vCenter, vMotion, HA, DRS
Microsoft Hyper-V	Hyper-V, Failover Cluster, Windows Admin Center, SCVMM
Proxmox VE	KVM, LXC, Weboberfläche, Cluster, HA, Ceph
Nutanix	AHV, Prism, verteilter Storage

VMware ESXi

VMware ESXi ist ein Typ-1-Hypervisor.

Typische Begriffe:

Begriff	Bedeutung
ESXi	Hypervisor
vCenter	Zentrale Verwaltung mehrerer ESXi-Hosts
vMotion	Live Migration von VMs
HA	Hochverfügbarkeit
DRS	Automatische Lastverteilung
Datastore	Speicherbereich für VMs
VMDK	Virtuelle Festplatte
VMFS	VMware-Dateisystem

Microsoft Hyper-V

Hyper-V ist die Virtualisierungslösung von Microsoft.

Hyper-V kann als Rolle auf Windows Server installiert werden.

Typische Begriffe:

Begriff	Bedeutung
Hyper-V	Microsoft-Hypervisor
Hyper-V Manager	Verwaltung einzelner Hosts

Begriff	Bedeutung
Failover Cluster	Clusterfunktion für Hochverfügbarkeit
Live Migration	Laufende VM auf anderen Host verschieben
Checkpoint	Snapshot-ähnlicher Zustand
VHDX	Virtuelle Festplattendatei
CSV	Cluster Shared Volume
SCVMM	System Center Virtual Machine Manager

Proxmox VE

Proxmox VE ist eine Virtualisierungsplattform auf Linux-Basis.

Sie nutzt KVM für virtuelle Maschinen und LXC für Container.

Typische Begriffe:

Begriff	Bedeutung
Proxmox VE	Virtualisierungsplattform
KVM	Virtualisierung für VMs
LXC	Container-Virtualisierung
Node	Einzelner Proxmox-Host
Cluster	Zusammenschluss mehrerer Nodes
VMID	Eindeutige Nummer einer VM oder eines Containers
Ceph	Verteilter Storage
HA Manager	Hochverfügbarkeitsverwaltung
QEMU Guest Agent	Gast-Agent für bessere VM-Integration

KVM

KVM steht für Kernel-based Virtual Machine.

KVM ist eine Virtualisierungstechnologie im Linux-Kernel.

Viele Plattformen nutzen KVM als technische Grundlage.

Beispiele:

Plattform	Nutzt KVM
-----------	-----------

Proxmox VE	Ja
OpenStack	Häufig
Linux-Virtualisierung	Ja
Nutanix AHV	KVM-basiert

KVM ist kein vollständiges Verwaltungsprodukt, sondern eine Virtualisierungstechnologie.

Verwaltung von virtuellen Maschinen

Virtuelle Maschinen werden über eine Verwaltungsoberfläche oder über Befehle administriert.

Beispiele:

Plattform	Verwaltung
VMware	vSphere Client / vCenter
Hyper-V	Hyper-V Manager, Windows Admin Center, PowerShell
Proxmox	Weboberfläche, Shell, API
VirtualBox	GUI oder VBoxManage
KVM	virsh, virt-manager, Cockpit, Proxmox

Typische Verwaltungsaufgaben

Aufgabe	Beschreibung
VM erstellen	Virtuelle Maschine neu anlegen
VM konfigurieren	CPU, RAM, Disk und Netzwerk einstellen
Betriebssystem installieren	ISO einbinden und OS installieren
VM starten	Virtuelle Maschine hochfahren
VM stoppen	Virtuelle Maschine herunterfahren
VM neu starten	Reboot ausführen
Snapshot erstellen	Zustand sichern
Snapshot löschen	Alten Zustand entfernen
VM klonen	Kopie einer VM erzeugen
VM migrieren	VM auf anderen Host verschieben
VM sichern	Backup ausführen
VM überwachen	Auslastung und Status prüfen

VM erstellen

Beim Erstellen einer VM werden grundlegende Eigenschaften festgelegt.

Typische Angaben:

Einstellung	Beispiel
Name	WEB01
Betriebssystemtyp	Linux / Windows
vCPU	2
RAM	4 GB
Festplatte	60 GB
Netzwerk	Servernetz / VLAN 20
ISO-Datei	Debian oder Windows Server
Boot-Reihenfolge	ISO zuerst, danach Disk

Beispiel für eine einfache VM-Planung

Einstellung	Wert
VM-Name	WEB01
Aufgabe	Interner Webserver
Betriebssystem	Debian 12
vCPU	2
RAM	4 GB
vDisk	60 GB
Netzwerk	VLAN 20
IP-Adresse	192.168.20.30
Backup	Täglich
Kritikalität	Mittel

VM-Namen

Virtuelle Maschinen sollten klare Namen bekommen.

Beispiele:

Name	Bedeutung
------	-----------

DC01	Domain Controller 1
DC02	Domain Controller 2
FILE01	Fileserver 1
WEB01	Webserver 1
DB01	Datenbankserver 1
APP01	Applikationsserver 1
BKP01	Backupserver 1
MON01	Monitoringserver 1
HV01	Hypervisor Host 1

Vorteil:

Man erkennt schnell, welche Aufgabe die VM hat.

VMID

Manche Plattformen vergeben zusätzlich eine VMID.

Beispiel bei Proxmox:

VMID	Name
100	DC01
101	FILE01
102	WEB01
103	DB01

Die VMID ist eine eindeutige technische Nummer.

Der VM-Name ist für Menschen leichter verständlich.

vCPU konfigurieren

Eine VM erhält eine bestimmte Anzahl virtueller CPUs.

Beispiel:

VM	vCPU
DC01	2
WEB01	2

VM	vCPU
DB01	4
FILE01	2

Wichtig:

Mehr vCPUs bedeuten nicht automatisch bessere Leistung.

Zu viele vCPUs können die Planung durch den Hypervisor verschlechtern.

CPU-Planung

Bei CPU-Planung muss man unterscheiden:

Begriff	Bedeutung
Physische Kerne	Tatsächliche CPU-Kerne im Host
Threads	Logische Ausführungseinheiten
vCPU	Virtuelle CPU für eine VM
CPU-Ready	Wartezeit einer VM auf CPU-Zeit
Overcommitment	Mehr vCPUs vergeben als physische Kerne vorhanden

CPU-Overcommitment

CPU-Overcommitment bedeutet, dass mehr vCPUs vergeben werden, als physische Kerne vorhanden sind.

Beispiel:

Physische CPU-Kerne	Vergebene vCPUs
16	40

Das kann funktionieren, weil nicht alle VMs dauerhaft volle CPU-Leistung brauchen.

Risiko:

Wenn viele VMs gleichzeitig Last erzeugen, kommt es zu Wartezeiten und Performanceproblemen.

RAM konfigurieren

Eine VM bekommt eine feste oder dynamische Menge Arbeitsspeicher.

Beispiel:

VM	RAM
DC01	4 GB
WEB01	4 GB
FILE01	8 GB
DB01	16 GB

RAM ist bei Virtualisierung besonders wichtig.

Wenn der Host nicht genug RAM hat, werden VMs langsam oder instabil.

RAM-Planung

Wichtige Fragen:

Frage	Bedeutung
Wie viel RAM braucht das Betriebssystem?	Grundbedarf
Wie viel RAM braucht die Anwendung?	Arbeitslast
Gibt es Spitzenlasten?	Reserven einplanen
Wie viele VMs laufen auf dem Host?	Gesamtauslastung
Gibt es HA-Reserve?	Ausfall eines Hosts abfangen

Merksatz:

RAM ist oft kritischer als CPU, weil fehlender RAM schnell zu starker Verlangsamung führt.

Virtuelle Festplatte konfigurieren

Eine VM benötigt mindestens eine virtuelle Festplatte.

Typische Angaben:

Einstellung	Beispiel
Größe	60 GB
Format	VHDX, VMDK, QCOW2, RAW
Provisioning	Thin oder Thick
Storage	Datastore, Volume oder Pool

Einstellung	Beispiel
Bus / Controller	SCSI, VirtIO, SATA
Cache-Modus	Plattformabhängig

Thin Provisioning

Thin Provisioning bedeutet:

Die virtuelle Festplatte hat eine Maximalgröße, belegt aber zunächst nur den tatsächlich genutzten Speicher.

Beispiel:

Eingestellte Größe	Tatsächlich belegt
100 GB	20 GB

Vorteil:

Speicher wird effizient genutzt.

Nachteil:

Der echte Storage kann voll laufen, wenn viele VMs wachsen.

Thick Provisioning

Thick Provisioning bedeutet:

Der Speicherplatz wird direkt vollständig reserviert.

Beispiel:

Eingestellte Größe	Tatsächlich belegt
100 GB	100 GB

Vorteil:

Besser planbar.

Nachteil:

Weniger flexibel und weniger platzsparend.

Virtuelle Netzwerkkarte konfigurieren

Eine VM bekommt eine oder mehrere virtuelle Netzwerkkarten.

Typische Einstellungen:

Einstellung	Bedeutung
Netzwerk / Bridge	Verbindung zum virtuellen Switch
VLAN	Logisches Netzwerk
MAC-Adresse	Hardwareadresse der vNIC
Treiber	VirtIO, E1000, VMXNET3 usw.
Firewall	Plattformabhängige Netzwerkfilter
Bandbreitenlimit	Begrenzung des Netzwerkverkehrs

Virtueller Switch

Ein virtueller Switch verbindet VMs mit Netzwerken.

Er kann VMs untereinander und mit dem physischen Netzwerk verbinden.

Beispiel:



Bridge

Eine Bridge verbindet virtuelle Netzwerke mit dem physischen Netzwerk.

Beispiel bei Proxmox:

Bridge	Zweck
vmbr0	Verbindung zum LAN

Bridge	Zweck
vmbr1	Internes VM-Netz
vmbr2	DMZ-Netz

Eine VM wird mit einer Bridge verbunden und kann darüber kommunizieren.

VLAN-Zuordnung

VLANs trennen Netzwerke logisch voneinander.

Beispiel:

VLAN	Zweck
VLAN 10	Management
VLAN 20	Servernetz
VLAN 30	Storage
VLAN 40	Clientnetz
VLAN 50	DMZ
VLAN 60	Backup

Eine VM kann über ihre virtuelle Netzwerkkarte einem VLAN zugeordnet werden.

ISO einbinden

Zum Installieren eines Betriebssystems wird häufig eine ISO-Datei eingebunden.

Ablauf:

Schritt	Erklärung
ISO hochladen	Installationsmedium bereitstellen
VM erstellen	Virtuelle Hardware anlegen
ISO als Laufwerk einbinden	VM kann davon booten
VM starten	Installation beginnt
Betriebssystem installieren	OS auf vDisk installieren
ISO entfernen	Nach Installation nicht mehr benötigt

Boot-Reihenfolge

Die Boot-Reihenfolge legt fest, von welchem Medium die VM startet.

Beispiel:

Reihenfolge	Medium
1	Virtuelles CD/DVD-Laufwerk mit ISO
2	Virtuelle Festplatte
3	Netzwerkboot

Nach der Installation sollte die VM meistens von der virtuellen Festplatte starten.

Gastbetriebssystem installieren

Das Gastbetriebssystem ist das Betriebssystem innerhalb der VM.

Beispiele:

Betriebssystem	Einsatz
Windows Server	Active Directory, Fileserver, Anwendungen
Debian	Webserver, Dienste, Container
Ubuntu Server	Cloud, Anwendungen, Webdienste
pfSense	Firewall oder Router
Rocky Linux	Unternehmensnahe Linux-Umgebung

Guest Tools

Guest Tools verbessern die Zusammenarbeit zwischen VM und Hypervisor.

Beispiele:

Plattform	Tool
VMware	VMware Tools
Hyper-V	Integration Services
Proxmox/KVM	QEMU Guest Agent
VirtualBox	Guest Additions

Vorteile:

Vorteil	Erklärung
---------	-----------

Bessere Treiber	Netzwerk, Storage und Grafik
Sauberes Herunterfahren	Hypervisor kann VM kontrolliert stoppen
IP-Anzeige	Hypervisor erkennt IP-Adresse der VM
Zeitsynchronisation	Uhrzeit bleibt korrekt
Bessere Performance	Optimierte Kommunikation
Snapshot-Unterstützung	Bessere Konsistenz möglich

QEMU Guest Agent

Der QEMU Guest Agent wird häufig bei KVM und Proxmox verwendet.

Er läuft innerhalb der VM.

Typische Vorteile:

Vorteil	Erklärung
IP-Adressen sichtbar	Proxmox kann IP der VM anzeigen
Sauberes Herunterfahren	VM kann korrekt beendet werden
Dateisystem einfrieren	Hilfreich für Backups
Bessere Kommunikation	Host und VM tauschen Informationen aus

VM starten

Beim Starten einer VM stellt der Hypervisor die virtuelle Hardware bereit.

Ablauf vereinfacht:

Schritt	Erklärung
VM-Konfiguration lesen	CPU, RAM, Disk, Netzwerk
Ressourcen reservieren	Host stellt Ressourcen bereit
Virtuelles BIOS/UEFI startet	Bootvorgang beginnt
Betriebssystem startet	Gastbetriebssystem wird geladen
Dienste starten	Serverdienste werden verfügbar

VM sauber herunterfahren

Eine VM sollte möglichst sauber heruntergefahren werden.

Beispiel:

Methode	Bewertung
Herunterfahren im Gastbetriebssystem	Sauber
Shutdown über Hypervisor mit Guest Tools	Sauber
Power Off erzwingen	Nur im Notfall

Ein erzwungenes Ausschalten kann Daten beschädigen, ähnlich wie das Ziehen des Stromsteckers bei einem physischen Server.

Autostart

Autostart legt fest, ob eine VM automatisch mit dem Host startet.

Beispiel:

VM	Autostart
DC01	Ja
DNS01	Ja
FILE01	Ja
TEST01	Nein

Produktive Dienste sollten nach einem Host-Neustart automatisch wieder starten.

Testsysteme müssen nicht unbedingt automatisch starten.

Startreihenfolge

Bei mehreren VMs ist die Startreihenfolge wichtig.

Beispiel:

Reihenfolge	VM	Grund
1	DC01	Authentifizierung und DNS
2	DB01	Datenbank für Anwendung
3	APP01	Anwendung benötigt Datenbank
4	WEB01	Webserver nutzt Anwendung

Wenn abhängige Systeme zu früh starten, funktionieren Dienste eventuell nicht korrekt.

VM-Konsole

Die VM-Konsole ist der direkte Bildschirmzugriff auf eine virtuelle Maschine.

Nutzen:

Situation	Nutzen
OS-Installation	Installation durchführen
Netzwerkfehler	Zugriff auch ohne RDP/SSH
Bootprobleme	Fehlermeldungen sehen
Notfallzugriff	Anmeldung direkt an der VM

Remotezugriff auf VMs

Nach der Installation werden VMs oft über normale Verwaltungsprotokolle administriert.

Beispiele:

System	Zugriff
Windows Server	RDP, PowerShell Remoting
Linux Server	SSH
Webserver	Browser, SSH
Datenbankserver	Datenbankclient, SSH/RDP

Die VM-Konsole ist eher für Installation und Notfälle gedacht.

Snapshot erstellen

Ein Snapshot speichert einen Zustand der VM.

Typische Nutzung:

Situation	Grund
Vor Updates	Rückkehr möglich
Vor Softwareinstallation	Test rückgängig machen
Vor Konfigurationsänderung	Fehler absichern
Schulungsumgebung	Ausgangszustand wiederherstellen

Snapshot löschen

Snapshots sollten nicht dauerhaft bestehen bleiben.

Warum?

Problem	Erklärung
Speicherverbrauch	Änderungen wachsen in Snapshot-Dateien
Performanceverlust	Mehr Verwaltungsaufwand beim Lesen/Schreiben
Komplexität	Lange Snapshot-Ketten werden riskanter
Kein Backup	Snapshot liegt meist auf gleichem Storage

Merksatz:

Snapshots nur kurzfristig nutzen und danach wieder entfernen.

Checkpoint

Bei Hyper-V wird häufig der Begriff Checkpoint verwendet.

Ein Checkpoint ist ähnlich wie ein Snapshot.

Es gibt unterschiedliche Arten:

Art	Bedeutung
Standard Checkpoint	Speichert VM-Zustand für Tests
Production Checkpoint	Besser für produktive Systeme geeignet

Auch Checkpoints sind kein Ersatz für Backups.

VM klonen

Beim Klonen wird eine VM kopiert.

Arten:

Clone-Art	Erklärung
Full Clone	Vollständige unabhängige Kopie
Linked Clone	Abhängige Kopie von einer Basis-VM

Typische Nutzung:

Situation	Beispiel
-----------	----------

Testsystem erstellen	Produktivsystem kopieren
Schulungsumgebung	Gleiche VM mehrfach bereitstellen
Vorlage nutzen	Aus Basis-VM neue Server erstellen

Template verwenden

Ein Template ist eine vorbereitete Vorlage für neue VMs.

Typischer Ablauf:

Schritt	Erklärung
Basis-VM installieren	Betriebssystem einrichten
Updates installieren	System aktualisieren
Grundkonfiguration setzen	Zeitzone, Tools, Benutzer
Bereinigen	Temporäre Daten entfernen
In Template umwandeln	Vorlage erstellen
Neue VM aus Template erzeugen	Schnelle Bereitstellung

Warum Templates sinnvoll sind

Vorteil	Erklärung
Zeitersparnis	Neue VMs schneller bereitstellen
Einheitlichkeit	Gleiche Grundkonfiguration
Weniger Fehler	Standardisierte Einrichtung
Automatisierung	Gut für größere Umgebungen
Dokumentation	Klarer Ausgangszustand

VM migrieren

Migration bedeutet, dass eine VM verschoben wird.

Arten:

Art	Bedeutung
Cold Migration	VM wird ausgeschaltet verschoben
Live Migration	Laufende VM wird verschoben
Storage Migration	Virtuelle Festplatte wird auf anderen Storage verschoben

Cold Migration

Cold Migration bedeutet:

Die VM wird heruntergefahren und dann verschoben.

Vorteil:

Einfacher und weniger anspruchsvoll.

Nachteil:

Die VM ist währenddessen nicht verfügbar.

Live Migration

Live Migration bedeutet:

Eine laufende VM wird von einem Host auf einen anderen Host verschoben.

Die VM soll dabei weiterlaufen.

Nutzen:

Situation	Vorteil
Wartung	Host kann ohne VM-Ausfall gewartet werden
Lastverteilung	VMs können besser verteilt werden
Hardwaretausch	VM kann vorher verschoben werden
Clusterbetrieb	Grundlage für flexible Verwaltung

Voraussetzungen für Live Migration

Voraussetzung	Erklärung
Mehrere Hosts	Es braucht Quell- und Zielhost
Gemeinsamer oder replizierter Storage	Zielhost muss VM-Daten erreichen
Netzwerkverbindung	RAM-Zustand wird übertragen
Kompatible CPUs	VM muss auf Zielhost laufen können
Gemeinsame Verwaltung	Hosts müssen im Cluster oder Management eingebunden sein

Storage Migration

Storage Migration verschiebt die virtuellen Festplatten einer VM auf einen anderen Speicher.

Beispiel:

Vorher	Nachher
VM-Disk auf Storage A	VM-Disk auf Storage B

Nutzen:

Situation	Vorteil
Storage wird voll	Daten verschieben
Storage wird ersetzt	Migration vorbereiten
Performance verbessern	VM auf schnelleren Speicher legen
Last verteilen	Storage entlasten

VM sichern

VMs müssen regelmäßig gesichert werden.

Mögliche Backuparten:

Backupart	Erklärung
Image-basiert	Ganze VM wird gesichert
Datei-basiert	Einzelne Dateien werden gesichert
Agent-basiert	Backupsoftware läuft in der VM
Agentless	Backup über Hypervisor
Applikationskonsistent	Laufende Anwendungen werden berücksichtigt

Applikationskonsistentes Backup

Ein applikationskonsistentes Backup ist besonders wichtig bei Systemen mit aktiven Daten.

Beispiele:

System	Grund
Datenbankserver	Schreibvorgänge müssen konsistent sein
Domain Controller	Active Directory muss sauber gesichert werden

System	Grund
Mailserver	Viele Transaktionen
ERP-System	Geschäftsdaten dürfen nicht beschädigt werden

Ein reines Kopieren einer laufenden virtuellen Festplatte kann inkonsistente Daten erzeugen.

VM wiederherstellen

Eine VM kann aus einem Backup wiederhergestellt werden.

Möglichkeiten:

Wiederherstellung	Bedeutung
Ganze VM	Vollständige VM zurückspielen
Einzelne Datei	Datei aus VM-Backup wiederherstellen
Einzelne Disk	Nur virtuelle Festplatte wiederherstellen
Instant Recovery	VM direkt aus Backup starten
Restore auf neuen Host	VM auf anderer Hardware wiederherstellen

Wichtig:

Wiederherstellungen sollten regelmäßig getestet werden.

VM-Monitoring

Virtuelle Maschinen müssen überwacht werden.

Wichtige Werte:

Bereich	Messwert
CPU	Auslastung, CPU-Ready
RAM	Nutzung, Swapping, Ballooning
Storage	IOPS, Latenz, freier Speicher
Netzwerk	Bandbreite, Paketverlust
Backup	Erfolgreich oder fehlgeschlagen
Dienste	Läuft die Anwendung?
Snapshots	Alte Snapshots vorhanden?
Host	Gesamtlast des Virtualisierungshosts

CPU-Ready

CPU-Ready beschreibt, wie lange eine VM auf CPU-Zeit warten muss.

Wenn CPU-Ready hoch ist, möchte die VM rechnen, bekommt aber nicht schnell genug CPU-Zeit vom Host.

Mögliche Ursachen:

Ursache	Erklärung
Zu viele VMs	Host überlastet
Zu viele vCPUs	Schlechte CPU-Planung
Hohe Last auf Host	Viele VMs aktiv
Falsche Ressourcenverteilung	Kritische VM bekommt zu wenig Ressourcen

Ballooning

Ballooning ist eine Speichertechnik in Virtualisierungsumgebungen.

Dabei wird Speicher aus VMs zurückgeholt, wenn der Host unter RAM-Druck steht.

Das kann sinnvoll sein, zeigt aber auch, dass RAM knapp werden kann.

Merksatz:

Ballooning kann ein Hinweis auf knappe RAM-Ressourcen sein.

Swapping

Swapping bedeutet, dass Arbeitsspeicher auf langsamere Datenträger ausgelagert wird.

Das ist bei VMs problematisch.

Folge:

Die VM wird deutlich langsamer.

Merksatz:

Swapping ist meistens ein schlechtes Zeichen für Performance.

Storage-Monitoring

Bei Virtualisierung ist Storage sehr wichtig.

Viele VMs greifen gleichzeitig auf denselben Speicher zu.

Wichtige Werte:

Wert	Bedeutung
Freier Speicher	Reicht Platz für VMs und Snapshots?
IOPS	Anzahl Speicheroperationen pro Sekunde
Latenz	Verzögerung beim Speicherzugriff
Durchsatz	Datenmenge pro Sekunde
Snapshot-Größe	Wächst ein Snapshot zu stark?

Alte Snapshots erkennen

Alte Snapshots sind ein häufiges Problem.

Risiken:

Risiko	Erklärung
Speicher läuft voll	Snapshot-Dateien wachsen
Performance sinkt	Mehr Verwaltungsaufwand
Backupprobleme	Backups können fehlschlagen
Schwierige Konsolidierung	Lange Snapshot-Ketten sind riskanter

Gute Praxis:

Snapshots nur kurzfristig verwenden und danach löschen oder konsolidieren.

VM-Rechteverwaltung

Nicht jeder Administrator sollte alle Rechte auf alle VMs haben.

Beispiele für Rollen:

Rolle	Rechte
Viewer	Nur ansehen
Operator	VM starten und stoppen
VM-Admin	VM verwalten

Rolle	Rechte
Storage-Admin	Datenspeicher verwalten
Netzwerk-Admin	Virtuelle Netzwerke verwalten
Volladministrator	Gesamte Plattform verwalten

Grundprinzip:

Least Privilege

Nur die Rechte vergeben, die wirklich benötigt werden.

Hypervisor-Updates

Auch der Hypervisor muss aktualisiert werden.

Gründe:

Grund	Erklärung
Sicherheitsupdates	Schwachstellen schließen
Stabilität	Fehler beheben
Hardwareunterstützung	Neue Hardware unterstützen
Performance	Verbesserungen erhalten
Kompatibilität	Neue Gastbetriebssysteme unterstützen

In produktiven Umgebungen sollten Updates geplant und getestet werden.

Wartungsmodus

Ein Host kann in den Wartungsmodus versetzt werden.

Bedeutung:

Der Host soll vorübergehend keine produktiven VMs betreiben.

Typischer Ablauf:

Schritt	Erklärung
Wartungsmodus aktivieren	Host für Wartung vorbereiten
VMs migrieren	VMs auf andere Hosts verschieben
Updates installieren	Hypervisor aktualisieren
Host neu starten	Falls erforderlich

Schritt	Erklärung
Funktion prüfen	Host kontrollieren
Wartungsmodus beenden	Host wieder produktiv nutzen

VM-Dokumentation

VMs müssen dokumentiert werden.

Wichtige Angaben:

Bereich	Beispiel
VM-Name	WEB01
VMID	102
Aufgabe	Interner Webserver
Betriebssystem	Debian 12
Host / Cluster	HV01 oder Cluster01
vCPU	2
RAM	4 GB
Disk	60 GB
Netzwerk	VLAN 20
IP-Adresse	192.168.20.30
Backup	Täglich
Kritikalität	Mittel
Verantwortlich	IT-Abteilung
Abhängigkeiten	DB01

Abhängigkeiten dokumentieren

VMs sind oft voneinander abhängig.

Beispiel:

VM	Benötigt
APP01	DB01
WEB01	APP01
FILE01	DC01 und DNS

VM	Benötigt
BACKUP01	Storage und Netzwerk
MON01	Zugriff auf alle Systeme

Wenn man eine VM wartet oder neu startet, muss man ihre Abhängigkeiten kennen.

Typische Fehler bei VM-Verwaltung

Fehler	Auswirkung
Zu viele vCPUs vergeben	Performance kann schlechter werden
Zu wenig RAM	VM wird langsam
Storage nicht überwacht	Datastore läuft voll
Snapshots zu lange behalten	Speicher- und Performanceprobleme
Keine Guest Tools installiert	Schlechtere Verwaltung
Keine Backups	Datenverlust möglich
Keine Dokumentation	Fehlersuche wird schwer
Keine Startreihenfolge	Dienste starten falsch
Managementzugang offen	Sicherheitsrisiko
Kein Monitoring	Probleme werden zu spät erkannt

Gute Praxis bei VM-Verwaltung

Empfehlung	Grund
VMs sauber benennen	Bessere Übersicht
Ressourcen passend planen	Stabiler Betrieb
Nicht zu viele vCPUs vergeben	Bessere CPU-Planung
RAM ausreichend dimensionieren	Vermeidet Swapping
Storage überwachen	Verhindert volle Datenspeicher
Snapshots nur kurzfristig nutzen	Verhindert Probleme
Guest Tools installieren	Bessere Integration
Backups regelmäßig prüfen	Wiederherstellung sicherstellen
Dokumentation pflegen	Betrieb und Fehlersuche erleichtern
Rechte beschränken	Sicherheit erhöhen
Hypervisor aktuell halten	Sicherheitslücken schließen

Prüfungsnahes Beispiel

Aufgabe:

Eine VM läuft langsam. Die CPU-Auslastung in der VM ist hoch. Der Host betreibt sehr viele VMs mit vielen zugewiesenen vCPUs.

Frage:

Was könnte die Ursache sein?

Mögliche Antwort:

Eine mögliche Ursache ist CPU-Overcommitment. Es wurden mehr vCPUs an VMs vergeben, als der Host sinnvoll bedienen kann. Dadurch müssen VMs auf CPU-Zeit warten. Man sollte die Host-Auslastung, CPU-Ready-Werte und die Anzahl vergebener vCPUs prüfen.

Prüfungsnahes Beispiel

Aufgabe:

Ein Administrator erstellt vor einem Update einen Snapshot und lässt diesen mehrere Wochen bestehen.

Frage:

Warum ist das problematisch?

Mögliche Antwort:

Snapshots sind nur für kurzfristige Zustände gedacht. Wenn ein Snapshot lange bestehen bleibt, kann er viel Speicher verbrauchen und die Performance verschlechtern. Außerdem ist ein Snapshot kein Backup. Nach erfolgreichem Update sollte der Snapshot gelöscht oder konsolidiert werden.

Prüfungsnahes Beispiel

Aufgabe:

Ein Unternehmen möchte einen Virtualisierungshost warten, ohne die darauf laufenden produktiven VMs auszuschalten.

Frage:

Welche Technik kann helfen?

Mögliche Antwort:

Live Migration kann helfen. Dabei werden laufende VMs auf einen anderen Host verschoben. Voraussetzung sind mehrere Hosts, passende Netzwerkverbindungen, kompatible CPUs und gemeinsamer oder replizierter Storage.

Typische Prüfungsfrage: Was macht ein Hypervisor?

Mögliche Antwort:

Ein Hypervisor verwaltet virtuelle Maschinen und teilt ihnen Ressourcen wie CPU, RAM, Storage und Netzwerk zu. Er ermöglicht, dass mehrere virtuelle Maschinen gleichzeitig auf einem physischen Host laufen.

Typische Prüfungsfrage: Warum sind Guest Tools wichtig?

Mögliche Antwort:

Guest Tools verbessern die Zusammenarbeit zwischen Hypervisor und Gastbetriebssystem. Sie ermöglichen bessere Treiber, sauberes Herunterfahren, Zeitsynchronisation, Anzeige von IP-Adressen und oft bessere Backup- oder Snapshot-Funktionen.

Typische Prüfungsfrage: Was ist ein virtueller Switch?

Mögliche Antwort:

Ein virtueller Switch verbindet virtuelle Maschinen untereinander und mit dem physischen Netzwerk. Er übernimmt innerhalb des Hypervisors eine ähnliche Aufgabe wie ein physischer Switch im Netzwerk.

Typische Prüfungsfrage: Warum ist die Startreihenfolge von VMs wichtig?

Mögliche Antwort:

Viele Serverdienste hängen voneinander ab. Ein Applikationsserver benötigt zum Beispiel zuerst die Datenbank, und viele Windows-Server benötigen DNS oder Domain Controller. Wenn VMs in falscher Reihenfolge starten, können Dienste fehlerhaft starten.

Typische Prüfungsfrage: Was ist CPU-Overcommitment?

Mögliche Antwort:

CPU-Overcommitment bedeutet, dass mehr virtuelle CPUs an VMs vergeben werden, als physische CPU-Kerne vorhanden sind. Das kann funktionieren, solange nicht alle VMs gleichzeitig viel CPU-Leistung benötigen. Bei hoher Last kann es aber zu Wartezeiten und Performanceproblemen

kommen.

Typische Prüfungsfrage: Was ist RAM-Overcommitment?

Mögliche Antwort:

RAM-Overcommitment bedeutet, dass mehr Arbeitsspeicher an VMs vergeben wird, als physisch vorhanden ist. Das ist riskant, weil fehlender RAM zu Ballooning oder Swapping führen kann. Dadurch werden VMs oft stark langsamer.

Typische Prüfungsfrage: Was ist ein Template?

Mögliche Antwort:

Ein Template ist eine vorbereitete Vorlage für neue virtuelle Maschinen. Es enthält ein installiertes und vorkonfiguriertes Betriebssystem. Dadurch können neue VMs schneller und einheitlicher erstellt werden.

Typische Prüfungsfrage: Was ist der Unterschied zwischen Snapshot und Backup?

Snapshot	Backup
Kurzfristiger Zustand einer VM	Langfristige Datensicherung
Liegt meist auf demselben Storage	Kann separat gespeichert werden
Für Updates und Tests geeignet	Für Wiederherstellung nach Datenverlust
Kein Ersatz für Backup	Echte Sicherung

Wichtige Begriffe

Begriff	Kurz erklärt
Hypervisor	Virtualisierungsschicht
Typ-1-Hypervisor	Läuft direkt auf Hardware
Typ-2-Hypervisor	Läuft auf Betriebssystem
Host	Physischer Virtualisierungsserver
Guest	Virtuelle Maschine
VM	Virtuelle Maschine
VMID	Eindeutige technische VM-Nummer
vCPU	Virtuelle CPU
vRAM	Virtueller Arbeitsspeicher

Begriff	Kurz erklärt
vDisk	Virtuelle Festplatte
vNIC	Virtuelle Netzwerkkarte
Virtueller Switch	Verbindet VMs mit Netzwerken
Bridge	Verbindung zwischen virtueller und physischer Netzwerkwelt
VLAN	Logische Netztrennung
ISO	Installationsabbild
Guest Tools	Zusatztools für bessere VM-Integration
Snapshot	Kurzfristig gespeicherter VM-Zustand
Checkpoint	Snapshot-ähnliche Funktion bei Hyper-V
Clone	Kopie einer VM
Template	Vorlage für neue VMs
Live Migration	Laufende VM verschieben
Cold Migration	Ausgeschaltete VM verschieben
Storage Migration	Virtuelle Festplatte verschieben
CPU-Ready	Wartezeit auf CPU-Zeit
Ballooning	Speicher wird aus VM zurückgeholt
Swapping	RAM wird auf Datenträger ausgelagert
Wartungsmodus	Host für Wartung vorbereiten

Wichtige Merksätze

Der Hypervisor verwaltet virtuelle Maschinen und verteilt Ressourcen.

Ein Typ-1-Hypervisor läuft direkt auf der Hardware.

Ein Typ-2-Hypervisor läuft auf einem vorhandenen Betriebssystem.

Eine VM sollte nur so viele Ressourcen bekommen, wie sie sinnvoll benötigt.

Zu viele vCPUs können die Performance verschlechtern.

RAM-Mangel führt häufig zu starken Performanceproblemen.

Snapshots sind nur kurzfristig sinnvoll und kein Backup.

Guest Tools verbessern Verwaltung, Performance und Integration.

Live Migration ermöglicht Wartung ohne Abschalten laufender VMs.

VMs müssen genauso dokumentiert, überwacht und gesichert werden wie physische Server.

Kurzzusammenfassung

Der Hypervisor ist die zentrale Komponente einer Virtualisierungsumgebung.

Er stellt virtuelle Hardware bereit, verwaltet virtuelle Maschinen und verteilt Ressourcen wie CPU, RAM, Storage und Netzwerk.

Wichtige Verwaltungsaufgaben sind:

Aufgabe	Bedeutung
VM erstellen	Neue virtuelle Maschine anlegen
Ressourcen planen	CPU, RAM, Disk und Netzwerk passend zuweisen
Betriebssystem installieren	Gastbetriebssystem einrichten
Guest Tools installieren	Integration verbessern
Snapshots nutzen	Kurzfristige Absicherung bei Änderungen
Backups einrichten	Echte Wiederherstellung ermöglichen
Migration durchführen	VMs verschieben
Monitoring nutzen	Auslastung und Probleme erkennen
Dokumentation pflegen	Betrieb nachvollziehbar machen
Rechte verwalten	Sicherheit erhöhen

Für die IHK ist besonders wichtig:

Thema	Kerngedanke
Hypervisor	Verwaltet VMs
Typ-1 / Typ-2	Direkt auf Hardware oder auf Betriebssystem
VM-Ressourcen	vCPU, vRAM, vDisk, vNIC
Snapshots	Kein Backup
Migration	VM kann verschoben werden
Guest Tools	Bessere Integration
Monitoring	Performanceprobleme erkennen
Dokumentation	Professioneller Betrieb

Der nächste logische Schritt ist:

Storage, Snapshots und Backups bei VMs
