

13.8 Prüfungszusammenfassung - Virtualisierung und Cluster

Einordnung

Diese Seite gehört zum Kapitel:

Server, Virtualisierung und Hochverfügbarkeit

Diese Seite fasst die wichtigsten Begriffe und Zusammenhänge aus den vorherigen Seiten zusammen.

Sie eignet sich besonders zur Wiederholung vor Klassenarbeiten, IHK-Aufgaben oder Prüfungsvorbereitung.

Themenüberblick

In diesem Kapitel wurden folgende Themen behandelt:

Seite	Thema
1	Server-Grundlagen
2	Virtualisierung und virtuelle Maschinen
3	Hypervisor und VM-Verwaltung
4	Storage, Snapshots und Backups bei VMs
5	Cluster und Hochverfügbarkeit
6	Failover, Quorum und Split-Brain
7	Load Balancing und Skalierung

Grundzusammenhang

Moderne Serverumgebungen bestehen oft nicht mehr aus einzelnen physischen Servern für jeden Dienst.

Stattdessen werden mehrere virtuelle Maschinen auf leistungsfähigen Hosts betrieben.

Mehrere Hosts können zu einem Cluster verbunden werden.

Dadurch entstehen mehr Flexibilität, bessere Ressourcennutzung und höhere Verfügbarkeit.

Vereinfacht:



Server

Ein Server ist ein System, das anderen Geräten Dienste, Daten oder Anwendungen bereitstellt.

Clients nutzen diese Dienste.

Beispiele:

Serverrolle	Aufgabe
Domain Controller	Benutzer und Anmeldungen verwalten
DNS-Server	Namen in IP-Adressen auflösen
DHCP-Server	IP-Adressen vergeben
Fileserver	Dateien bereitstellen
Webserver	Webseiten bereitstellen
Datenbankserver	Daten speichern
Backupserver	Sicherungen verwalten
Monitoring-Server	Systeme überwachen

Client-Server-Prinzip

Beim Client-Server-Prinzip fordert ein Client einen Dienst an und der Server stellt ihn bereit.

Beispiel:

Client	Server
PC öffnet Netzlaufwerk	Fileserver stellt Datei bereit
Browser ruft Webseite auf	Webserver liefert Webseite
PC fragt DNS-Namen ab	DNS-Server liefert IP-Adresse

Client	Server
Benutzer meldet sich an	Domain Controller prüft Anmeldung

Merksatz Server

Ein Server stellt Dienste bereit. Ein Client nutzt diese Dienste.

Virtualisierung

Virtualisierung bedeutet, dass mehrere virtuelle Systeme auf einer physischen Hardware betrieben werden.

Ein physischer Server kann dadurch mehrere virtuelle Maschinen ausführen.

Beispiel:

Physischer Host	Virtuelle Maschinen
HV01	DC01, FILE01, WEB01, DB01

Virtuelle Maschine

Eine virtuelle Maschine ist ein simulierter Computer.

Sie besitzt eigene virtuelle Hardware:

Virtuelle Komponente	Bedeutung
vCPU	Virtuelle CPU
vRAM	Virtueller Arbeitsspeicher
vDisk	Virtuelle Festplatte
vNIC	Virtuelle Netzwerkkarte
Gastbetriebssystem	Betriebssystem innerhalb der VM

Host und Guest

Begriff	Bedeutung
Host	Physischer Server, auf dem VMs laufen
Guest	Virtuelle Maschine
Gastbetriebssystem	Betriebssystem innerhalb der VM

Begriff	Bedeutung
Hypervisor	Virtualisierungsschicht

Beispiel:

Ebene	Beispiel
Hardware	Physischer Server
Hypervisor	Proxmox, ESXi, Hyper-V
Guest	Windows Server VM oder Linux VM

Hypervisor

Ein Hypervisor ist die Virtualisierungsschicht.

Er verwaltet virtuelle Maschinen und verteilt Ressourcen.

Aufgaben:

Aufgabe	Erklärung
VMs erstellen	Neue virtuelle Maschinen anlegen
VMs starten und stoppen	Betrieb steuern
CPU zuteilen	Rechenleistung bereitstellen
RAM zuteilen	Arbeitsspeicher bereitstellen
Storage verwalten	Virtuelle Festplatten bereitstellen
Netzwerk bereitstellen	Virtuelle Netzwerkkarten und Switches
Snapshots verwalten	Zustände speichern
Migration ermöglichen	VMs verschieben

Typ-1-Hypervisor

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

Beispiele:

Hypervisor	Beschreibung
VMware ESXi	Häufig in Unternehmen
Microsoft Hyper-V	Microsoft-Virtualisierung
Proxmox VE	Open-Source-Virtualisierungsplattform

Hypervisor	Beschreibung
KVM	Linux-basierte Virtualisierung
Xen	Virtualisierungstechnologie

Typischer Aufbau:



Typ-2-Hypervisor

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

Beispiele:

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

Typischer Aufbau:



Typ-1 vs. Typ-2

Merkmal	Typ-1	Typ-2
Läuft auf	Direkt auf Hardware	Auf Betriebssystem

Merkmal	Typ-1	Typ-2
Einsatz	Server / Rechenzentrum	Desktop / Test
Performance	Höher	Meist geringer
Stabilität	Sehr hoch	Abhängig vom Host-OS
Beispiel	ESXi, Hyper-V, Proxmox	VirtualBox, VMware Workstation

Vorteile von Virtualisierung

Vorteil	Erklärung
Bessere Ressourcennutzung	Hardware wird effizienter genutzt
Weniger physische Server	Konsolidierung
Schnellere Bereitstellung	Neue VMs schnell erstellen
Einfachere Sicherung	Ganze VMs können gesichert werden
Flexibilität	Ressourcen können angepasst werden
Migration	VMs können verschoben werden
Testumgebungen	Schnell erstellbar und zurücksetzbar
Grundlage für HA	Clusterbetrieb möglich

Nachteile und Risiken von Virtualisierung

Risiko	Erklärung
Host-Ausfall	Mehrere VMs gleichzeitig betroffen
Ressourcenengpass	CPU, RAM oder Storage überlastet
Komplexität	Mehr Planung bei Netzwerk, Storage und Backup
Hypervisor-Sicherheit	Hypervisor ist besonders kritisch
Storage-Abhängigkeit	Viele VMs hängen am gleichen Speicher
Lizenzierung	Kann komplizierter werden

Storage bei VMs

Storage ist der Speicherbereich für virtuelle Maschinen.

Dort liegen zum Beispiel:

Bestandteil	Beispiel
-------------	----------

Virtuelle Festplatten	VHDX, VMDK, QCOW2
VM-Konfiguration	CPU, RAM, Netzwerk
ISO-Dateien	Installationsmedien
Snapshots	Zwischenstände
Templates	Vorlagen
Backups	Sicherungen

Virtuelle Festplattenformate

Format	Plattform
VHD / VHDX	Hyper-V
VMDK	VMware
QCOW2	KVM / Proxmox
RAW	KVM / Proxmox

Thin Provisioning

Thin Provisioning bedeutet, dass eine virtuelle Festplatte nur den tatsächlich genutzten Speicher belegt, obwohl sie eine größere Maximalgröße hat.

Beispiel:

Eingestellte Größe	Tatsächlich belegt
100 GB	25 GB

Vorteil:

Speicher wird effizient genutzt.

Nachteil:

Der echte Storage kann unerwartet voll laufen.

Thick Provisioning

Thick Provisioning bedeutet, dass der Speicher direkt vollständig reserviert wird.

Beispiel:

Eingestellte Größe	Tatsächlich belegt
--------------------	--------------------

100 GB	100 GB
--------	--------

Vorteil:

Besser planbar.

Nachteil:

Weniger flexibel und weniger platzsparend.

Thin vs. Thick

Merkmal	Thin	Thick
Speicherbelegung	Wächst nach Bedarf	Sofort vollständig reserviert
Effizienz	Hoch	Geringer
Risiko	Storage kann voll laufen	Besser planbar
Überwachung	Sehr wichtig	Trotzdem wichtig

Snapshot

Ein Snapshot speichert den Zustand einer VM zu einem bestimmten Zeitpunkt.

Typische Nutzung:

Situation	Warum Snapshot?
Vor Updates	Rückkehr möglich
Vor Softwareinstallation	Test rückgängig machen
Vor Konfigurationsänderung	Absicherung
Schulung / Labor	Ausgangszustand wiederherstellen

Snapshots sind kein Backup

Snapshots sind nur kurzfristige Zustände.

Sie ersetzen kein Backup.

Gründe:

Grund	Erklärung
Gleicher Storage	Snapshot liegt oft neben der VM

Grund	Erklärung
Kurzfristig gedacht	Nicht für Langzeitaufbewahrung
Kein Schutz bei Storage-Ausfall	Snapshot ist dann auch betroffen
Performanceprobleme möglich	Lange Snapshot-Ketten können bremsen
Kein vollständiges Restore-Konzept	Backup bleibt notwendig

Backup

Ein Backup ist eine Datensicherung.

Ziel:

Daten oder Systeme sollen nach einem Fehler wiederhergestellt werden können.

Typische Gründe für Restore:

Ursache	Beispiel
Datei gelöscht	Benutzerfehler
Ransomware	Daten verschlüsselt
Hardwaredefekt	Storage defekt
Fehlkonfiguration	Falsche Änderung
Updatefehler	Anwendung funktioniert nicht mehr
Datenkorruption	Daten beschädigt

Backuparten

Backupart	Erklärung
Vollbackup	Sichert alle Daten
Inkrementelles Backup	Sichert Änderungen seit letztem Backup
Differenzielles Backup	Sichert Änderungen seit letztem Vollbackup
Image-basiertes Backup	Sichert ganze VM
Datei-basiertes Backup	Sichert einzelne Dateien
Applikationskonsistentes Backup	Berücksichtigt laufende Anwendungen

RAID ist kein Backup

RAID schützt vor bestimmten Festplattenausfällen.

RAID schützt nicht zuverlässig gegen:

Risiko	Beispiel
Versehentliches Löschen	Datei wird gelöscht
Ransomware	Daten werden verschlüsselt
Datenkorruption	Fehlerhafte Daten
Brand / Diebstahl	Gesamtes Gerät weg
Fehlkonfiguration	Falsche Änderung bleibt bestehen

Merksatz:

RAID erhöht Verfügbarkeit, ersetzt aber kein Backup.

RPO und RTO

Begriff	Bedeutung	Frage
RPO	Recovery Point Objective	Wie viele Daten dürfen maximal verloren gehen?
RTO	Recovery Time Objective	Wie lange darf die Wiederherstellung dauern?

Beispiel:

Wert	Bedeutung
RPO 1 Stunde	Maximal Datenverlust von 1 Stunde
RTO 4 Stunden	Dienst muss nach 4 Stunden wieder laufen

Cluster

Ein Cluster ist ein Zusammenschluss mehrerer Server, die gemeinsam arbeiten.

Die einzelnen Server heißen Nodes.

Ziele:

Ziel	Erklärung
Hochverfügbarkeit	Dienste sollen bei Ausfall weiterlaufen oder schnell wieder starten
Lastverteilung	Arbeit wird verteilt
Skalierbarkeit	Weitere Systeme können ergänzt werden

Ziel	Erklärung
Wartbarkeit	Systeme können nacheinander gewartet werden

Cluster-Node

Ein Cluster-Node ist ein einzelner Server innerhalb eines Clusters.

Beispiel:

Cluster	Nodes
Virtualisierungscluster	HV01, HV02, HV03
Webserver-Cluster	WEB01, WEB02, WEB03
Datenbankcluster	DB01, DB02

Cluster-Ressource

Eine Cluster-Ressource ist ein Dienst, eine VM, eine IP-Adresse oder ein Speicherbereich, der vom Cluster verwaltet wird.

Beispiele:

Cluster-Ressource	Erklärung
Virtuelle Maschine	Kann auf anderem Host starten
IP-Adresse	Wandert mit aktivem Dienst
Dateifreigabe	Hochverfügbare Freigabe
Datenbankdienst	Kann auf Ersatznode starten
Anwendung	Wird überwacht und verschoben

Hochverfügbarkeit

Hochverfügbarkeit bedeutet, dass ein Dienst möglichst dauerhaft erreichbar bleibt.

Wichtig:

Hochverfügbarkeit bedeutet nicht automatisch unterbrechungsfrei.

Oft gibt es bei einem Failover eine kurze Unterbrechung.

Single Point of Failure

Ein Single Point of Failure ist eine einzelne Komponente, deren Ausfall einen Dienst oder ein System lahmlegen kann.

Beispiele:

Single Point of Failure	Risiko
Einziges Server	Dienst fällt komplett aus
Einziges Switch	Netzwerk fällt aus
Einziges Storage	VM-Daten nicht erreichbar
Einziges Internetleitung	Externer Zugriff fällt aus
Einziges Load Balancer	Dienst trotz Backends nicht erreichbar

Redundanz

Redundanz bedeutet, dass wichtige Komponenten mehrfach vorhanden sind.

Beispiele:

Komponente	Redundanz
Server	Mehrere Hosts
Netzteil	Zwei Netzteile
Netzwerk	Mehrere Netzwerkkarten
Switch	Zwei Switches
Storage	RAID, Replikation, verteiltes Storage
Backup	Mehrere Sicherungen

Failover

Failover bedeutet, dass ein Dienst bei Ausfall auf ein anderes System wechselt oder dort neu gestartet wird.

Beispiel:

Schritt	Ereignis
1	VM läuft auf HV01
2	HV01 fällt aus
3	Cluster erkennt Fehler
4	VM wird auf HV02 gestartet

Schritt	Ereignis
5	Dienst ist wieder verfügbar

Merksatz:

Failover bedeutet Übernahme bei Ausfall.

Failback

Failback bedeutet, dass eine Ressource nach Reparatur wieder auf das ursprüngliche System zurückwechselt.

Beispiel:

Schritt	Ereignis
1	VM läuft ursprünglich auf HV01
2	Failover auf HV02
3	HV01 wird repariert
4	VM wird zurück auf HV01 verschoben

Live Migration

Live Migration bedeutet, dass eine laufende VM geplant auf einen anderen Host verschoben wird.

Beispiel:

Situation	Begriff
Admin verschiebt VM vor Wartung	Live Migration
Host fällt plötzlich aus	Failover

Failover vs. Live Migration

Failover	Live Migration
Reaktion auf Fehler	Geplante Verschiebung
Häufig kurze Unterbrechung	Möglichst ohne Unterbrechung
Beispiel: Host-Ausfall	Beispiel: Wartung
Ressource startet woanders	VM läuft weiter beim Verschieben

Quorum

Quorum ist ein Entscheidungsmechanismus im Cluster.

Es sorgt dafür, dass nur der Cluster-Teil mit gültiger Mehrheit weiterarbeiten darf.

Ziel:

Split-Brain verhindern.

Witness

Ein Witness ist eine zusätzliche Entscheidungsinstanz für das Quorum.

Beispiele:

Witness-Art	Erklärung
File Share Witness	Netzwerkfreigabe als Zeuge
Disk Witness	Gemeinsamer Datenträger als Zeuge
Cloud Witness	Cloud-Dienst als Zeuge

Besonders bei Clustern mit gerader Node-Anzahl ist ein Witness wichtig.

Split-Brain

Split-Brain ist ein gefährlicher Zustand.

Dabei verlieren Cluster-Teile die Verbindung zueinander und glauben gleichzeitig, aktiv sein zu dürfen.

Gefahr:

Gefahr	Erklärung
Datenkorruption	Zwei Seiten schreiben gleichzeitig
Inkonsistente Daten	Unterschiedliche Datenstände
Datenverlust	Änderungen überschreiben sich
Lange Wiederherstellung	Manuelle Reparatur nötig

Merksatz:

Quorum und Witness helfen, Split-Brain zu verhindern.

Fencing

Fencing bedeutet, einen unsicheren oder isolierten Node vom Zugriff auf gemeinsame Ressourcen auszuschließen.

Ziel:

Ein unsicherer Node darf nicht weiter auf Daten schreiben.

STONITH

STONITH steht für:

Shoot The Other Node In The Head

Gemeint ist technisch:

Ein unsicherer Node wird ausgeschaltet oder isoliert, um Datenkonsistenz zu schützen.

Heartbeat

Heartbeat ist ein regelmäßiges Signal zwischen Cluster-Nodes.

Damit prüfen Nodes, ob andere Nodes noch erreichbar sind.

Wichtig:

Ein fehlender Heartbeat bedeutet nicht automatisch, dass der Server aus ist.
Es kann auch ein Netzwerkproblem sein.

Shared Storage

Shared Storage ist gemeinsamer Speicher, auf den mehrere Hosts zugreifen können.

Vorteil:

VMs können leichter auf anderen Hosts gestartet werden.

Nachteil:

Der gemeinsame Storage darf selbst kein Single Point of Failure sein.

Shared-Nothing-Cluster

Bei einem Shared-Nothing-Cluster hat jeder Node eigenen lokalen Speicher.

Daten werden repliziert oder verteilt.

Beispiele:

Technologie	Prinzip
Ceph	Verteilter Storage
VMware vSAN	Verteilter Speicher
Storage Spaces Direct	Microsoft verteilter Storage
GlusterFS	Verteiltes Dateisystem

N+1-Prinzip

N+1 bedeutet:

Es gibt eine zusätzliche Reservekomponente.

Beispiel:

Benötigt	Vorhanden
2 Hosts	3 Hosts

Wenn ein Host ausfällt, können die verbleibenden Hosts die Last übernehmen.

Load Balancing

Load Balancing bedeutet Lastverteilung.

Ein Load Balancer verteilt Anfragen auf mehrere Backend-Server.

Beispiel:



Load Balancer

Ein Load Balancer nimmt Anfragen entgegen und verteilt sie.

Beispiele:

Art	Beispiel
Software	HAProxy, Nginx, Traefik
Hardware	Load-Balancer-Appliance
Cloud	Cloud Load Balancer
Container	Kubernetes Service / Ingress

Backend und Frontend

Begriff	Bedeutung
Frontend	Adresse, die der Client anspricht
Backend	Zielservers hinter dem Load Balancer

Beispiel:

Bereich	Beispiel
Frontend	intranet.firma.local
Backend	WEB01, WEB02, WEB03

Health Check

Ein Health Check prüft, ob ein Backend-Server erreichbar und funktionsfähig ist.

Wenn ein Server nicht gesund ist, nimmt der Load Balancer ihn aus der Verteilung.

Beispiele:

Health Check	Prüfung
Ping	Server erreichbar?
TCP-Port	Port offen?
HTTP-Status	Webserver antwortet korrekt?
API-Check	Anwendung funktioniert?

Load-Balancing-Methoden

Methode	Erklärung
Round Robin	Anfragen der Reihe nach verteilen

Methode	Erklärung
Least Connections	Server mit wenigsten Verbindungen bevorzugen
Weighted Round Robin	Stärkere Server bekommen mehr Anfragen
IP Hash	Client-IP entscheidet über Zielservers
Random	Zufällige Verteilung

Sticky Session

Sticky Session bedeutet, dass ein Benutzer während einer Sitzung immer wieder beim gleichen Backend-Server landet.

Das ist nötig, wenn die Anwendung Sitzungsdaten lokal speichert.

Nachteil:

Die Lastverteilung kann ungleichmäßiger werden.

Stateless und Stateful

Begriff	Bedeutung
Stateless	Server speichert keinen wichtigen Sitzungsstatus lokal
Stateful	Server speichert Status oder Sitzungsdaten lokal

Stateless-Anwendungen sind einfacher zu skalieren.

Stateful-Anwendungen benötigen oft Sticky Sessions, zentralen Session-Speicher oder besondere Clusterkonzepte.

Scale-Up

Scale-Up bedeutet vertikale Skalierung.

Ein einzelnes System wird stärker gemacht.

Beispiele:

Maßnahme	Wirkung
Mehr RAM	Mehr Arbeitsspeicher
Mehr CPU	Mehr Rechenleistung
Schnellere SSD	Bessere Storage-Performance

Maßnahme	Wirkung
Größere VM	Mehr Ressourcen

Scale-Out

Scale-Out bedeutet horizontale Skalierung.

Es werden weitere Systeme hinzugefügt.

Beispiel:

Vorher	Nachher
Ein Webserver	Drei Webserver hinter Load Balancer

Scale-Up vs. Scale-Out

Merkmal	Scale-Up	Scale-Out
Prinzip	Ein System stärker machen	Mehr Systeme hinzufügen
Beispiel	Mehr RAM für DB01	WEB01, WEB02, WEB03
Komplexität	Meist einfacher	Komplexer
Grenze	Hardwarelimit	Architekturabhängig
Ausfallsicherheit	Nicht automatisch besser	Kann besser werden

Failover vs. Load Balancing

Failover	Load Balancing
Übernahme bei Ausfall	Verteilung von Anfragen
Häufig eine aktive Ressource	Mehrere aktive Server
Ziel: Verfügbarkeit	Ziel: Lastverteilung und Verfügbarkeit
Beispiel: VM startet auf anderem Host	Beispiel: Webanfragen auf mehrere Server

Cluster vs. Backup

Cluster	Backup
Erhöht Verfügbarkeit	Schützt vor Datenverlust
Hilft bei Serverausfall	Hilft bei gelöschten oder beschädigten Daten
Kein Ersatz für Backup	Kein Ersatz für Hochverfügbarkeit

Cluster	Backup
Aktueller Zustand bleibt aktiv	Ältere Zustände wiederherstellbar

Merksatz:

Ein Cluster ersetzt kein Backup.

Snapshot vs. Backup

Snapshot	Backup
Kurzfristiger Zustand	Echte Datensicherung
Meist gleicher Storage	Separater Speicher möglich
Für Updates und Tests	Für Wiederherstellung
Kein Ersatz für Backup	Notwendig für Datenverlustfälle

Merksatz:

Snapshots sind kein Backup.

RAID vs. Backup

RAID	Backup
Schutz vor bestimmten Festplattenausfällen	Schutz vor Datenverlust
Erhöht Verfügbarkeit	Ermöglicht Wiederherstellung
Kein Schutz vor Löschen/Ransomware	Kann alte Zustände liefern
Kein Ersatz für Backup	Echte Sicherung

Merksatz:

RAID ist kein Backup.

Wichtige Unterschiede auf einen Blick

Begriff 1	Begriff 2	Unterschied
VM	Container	VM hat eigenes OS, Container nutzt Host-Kernel
Host	Guest	Host betreibt VMs, Guest ist VM
Typ-1	Typ-2	Direkt auf Hardware vs. auf Betriebssystem

Begriff 1	Begriff 2	Unterschied
Snapshot	Backup	Zustand vs. Sicherung
RAID	Backup	Festplattenschutz vs. Wiederherstellung
Failover	Live Migration	Fehlerfall vs. geplante Verschiebung
Failover	Load Balancing	Übernahme vs. Verteilung
Scale-Up	Scale-Out	Stärker machen vs. mehr Systeme
Stateful	Stateless	Mit Zustand vs. ohne lokalen Zustand
RPO	RTO	Datenverlust vs. Ausfallzeit
HA	Fault Tolerance	Schnelle Wiederherstellung vs. möglichst unterbrechungsfrei

Typische IHK-Frage: Was ist Virtualisierung?

Mögliche Antwort:

Virtualisierung bedeutet, dass mehrere virtuelle Maschinen auf einer gemeinsamen physischen Hardware betrieben werden. Jede VM verhält sich wie ein eigener Computer mit virtueller CPU, virtuellem Arbeitsspeicher, virtueller Festplatte und virtueller Netzwerkkarte.

Typische IHK-Frage: Was ist ein Hypervisor?

Mögliche Antwort:

Ein Hypervisor ist die Virtualisierungsschicht, die virtuelle Maschinen bereitstellt und verwaltet. Er verteilt Ressourcen wie CPU, RAM, Storage und Netzwerk an die VMs.

Typische IHK-Frage: Unterschied Typ-1 und Typ-2-Hypervisor

Mögliche Antwort:

Ein Typ-1-Hypervisor läuft direkt auf der Hardware und wird typischerweise im Serverbetrieb eingesetzt. Ein Typ-2-Hypervisor läuft auf einem vorhandenen Betriebssystem und wird häufig für Tests oder Lernumgebungen genutzt.

Typische IHK-Frage: Warum nutzt man virtuelle Maschinen?

Mögliche Antwort:

Virtuelle Maschinen ermöglichen eine bessere Ressourcennutzung, schnellere Bereitstellung, einfachere Sicherung, flexible Verwaltung und den Betrieb mehrerer Server auf einer physischen

Hardware. Außerdem bilden sie eine Grundlage für Hochverfügbarkeit und Clusterbetrieb.

Typische IHK-Frage: Warum ist ein einzelner Virtualisierungshost riskant?

Mögliche Antwort:

Wenn viele VMs auf einem einzelnen Host laufen, fallen bei Ausfall dieses Hosts mehrere virtuelle Server gleichzeitig aus. Der Host ist dann ein Single Point of Failure. Abhilfe schaffen Cluster, Redundanz, Backups und Monitoring.

Typische IHK-Frage: Was ist ein Cluster?

Mögliche Antwort:

Ein Cluster ist ein Zusammenschluss mehrerer Server, die gemeinsam Dienste bereitstellen oder absichern. Ziel ist meistens Hochverfügbarkeit, Lastverteilung, Skalierbarkeit oder bessere Wartbarkeit.

Typische IHK-Frage: Was ist Failover?

Mögliche Antwort:

Failover bedeutet, dass ein Dienst oder eine Ressource bei Ausfall eines Systems auf ein anderes System wechselt oder dort neu gestartet wird. Dadurch wird die Ausfallzeit reduziert.

Typische IHK-Frage: Was ist Quorum?

Mögliche Antwort:

Quorum ist ein Entscheidungsmechanismus im Cluster. Es stellt sicher, dass nur der Cluster-Teil mit gültiger Mehrheit weiterarbeiten darf. Dadurch wird verhindert, dass mehrere Cluster-Teile gleichzeitig aktiv werden.

Typische IHK-Frage: Was ist Split-Brain?

Mögliche Antwort:

Split-Brain ist ein gefährlicher Zustand, bei dem getrennte Cluster-Teile gleichzeitig aktiv werden. Wenn beide Seiten auf dieselben Daten schreiben, kann es zu Datenkorruption oder Datenverlust kommen.

Typische IHK-Frage: Warum braucht ein Zwei-Node-Cluster oft einen Witness?

Mögliche Antwort:

Bei zwei Nodes gibt es ohne Witness keine klare Mehrheit, wenn die Verbindung zwischen den Nodes gestört ist. Ein Witness liefert eine zusätzliche Stimme und hilft dem Cluster, eindeutig zu entscheiden, welcher Teil weiterarbeiten darf.

Typische IHK-Frage: Was ist Load Balancing?

Mögliche Antwort:

Load Balancing bedeutet Lastverteilung. Ein Load Balancer verteilt eingehende Anfragen auf mehrere Backend-Server, damit Last besser verteilt und die Verfügbarkeit erhöht wird.

Typische IHK-Frage: Unterschied Failover und Load Balancing

Mögliche Antwort:

Failover bedeutet Übernahme bei Ausfall. Load Balancing bedeutet Verteilung von Anfragen auf mehrere aktive Systeme. Failover dient vor allem der Ausfallsicherheit, Load Balancing dient der Lastverteilung und kann zusätzlich die Verfügbarkeit verbessern.

Typische IHK-Frage: Was ist Scale-Up?

Mögliche Antwort:

Scale-Up bedeutet, ein einzelnes System leistungsfähiger zu machen, zum Beispiel durch mehr CPU, mehr RAM oder schnelleren Storage.

Typische IHK-Frage: Was ist Scale-Out?

Mögliche Antwort:

Scale-Out bedeutet, weitere Systeme hinzuzufügen, zum Beispiel mehrere Webserver hinter einem Load Balancer.

Typische IHK-Frage: Warum sind Datenbanken schwieriger zu skalieren als Webserver?

Mögliche Antwort:

Datenbanken müssen Daten konsistent halten. Schreibzugriffe, Transaktionen und gleichzeitige Änderungen dürfen keine widersprüchlichen Daten erzeugen. Deshalb benötigen Datenbanken spezielle Replikations-, Cluster- oder Failover-Konzepte.

Typische IHK-Frage: Warum sind Snapshots kein Backup?

Mögliche Antwort:

Snapshots speichern nur einen kurzfristigen Zustand einer VM und liegen meist auf demselben Storage. Sie sind für Tests oder Updates geeignet, aber kein Ersatz für eine getrennte Datensicherung.

Typische IHK-Frage: Warum ist RAID kein Backup?

Mögliche Antwort:

RAID schützt vor bestimmten Festplattenausfällen, aber nicht vor versehentlichem Löschen, Ransomware, Datenkorruption oder Standortausfall. Deshalb wird zusätzlich ein Backup benötigt.

Typische IHK-Frage: Was bedeutet RPO?

Mögliche Antwort:

RPO steht für Recovery Point Objective. Es beschreibt, wie viele Daten maximal verloren gehen dürfen. Ein RPO von einer Stunde bedeutet, dass höchstens Daten der letzten Stunde verloren gehen dürfen.

Typische IHK-Frage: Was bedeutet RTO?

Mögliche Antwort:

RTO steht für Recovery Time Objective. Es beschreibt, wie lange die Wiederherstellung maximal dauern darf. Ein RTO von vier Stunden bedeutet, dass der Dienst innerhalb von vier Stunden wieder verfügbar sein soll.

Typische IHK-Frage: Warum braucht ein Cluster trotzdem Backups?

Mögliche Antwort:

Ein Cluster erhöht die Verfügbarkeit, schützt aber nicht zuverlässig vor Datenverlust. Wenn Daten gelöscht, verschlüsselt oder beschädigt werden, wird der fehlerhafte Zustand weiterhin aktiv sein. Für die Wiederherstellung alter Datenstände benötigt man Backups.

Prüfungsnahes Szenario 1

Ein Unternehmen betreibt mehrere wichtige Serverrollen auf einem einzelnen physischen Server.

Auf diesem Server laufen:

Dienst	Aufgabe
DC01	Domain Controller
FILE01	Dateiserver
DB01	Datenbank
WEB01	Webserver

Frage:

Welches Risiko besteht?

Mögliche Antwort:

Der einzelne physische Server ist ein Single Point of Failure. Wenn er ausfällt, sind alle darauf betriebenen Dienste betroffen. Eine bessere Lösung wäre Virtualisierung auf mehreren Hosts, ein Cluster für Hochverfügbarkeit, regelmäßige Backups und Monitoring.

Prüfungsnahes Szenario 2

Ein Administrator erstellt vor einem Update einen Snapshot einer VM und lässt diesen danach mehrere Monate bestehen.

Frage:

Warum ist das problematisch?

Mögliche Antwort:

Snapshots sind nur kurzfristig gedacht. Lange bestehende Snapshots können Speicher verbrauchen, die Performance verschlechtern und Probleme bei der Konsolidierung verursachen. Außerdem sind Snapshots kein Backup.

Prüfungsnahes Szenario 3

Ein Zwei-Node-Cluster ohne Witness verliert die Verbindung zwischen den Nodes.

Frage:

Welches Problem kann entstehen?

Mögliche Antwort:

Es gibt keine klare Mehrheit. Beide Nodes könnten den jeweils anderen als ausgefallen betrachten. Dadurch besteht die Gefahr von Split-Brain oder der Cluster stoppt aus Sicherheitsgründen. Ein Witness hilft, eine eindeutige Entscheidung zu treffen.

Prüfungsnahes Szenario 4

Ein Unternehmen nutzt drei Webserver hinter einem Load Balancer. Einer der Webserver fällt aus.

Frage:

Was sollte passieren?

Mögliche Antwort:

Der Load Balancer sollte den Ausfall durch Health Checks erkennen und keine neuen Anfragen mehr an den defekten Webserver senden. Die Anfragen werden auf die verbleibenden funktionierenden Webserver verteilt.

Prüfungsnahes Szenario 5

Ein Unternehmen speichert produktive VMs und Backups auf demselben Storage.

Frage:

Warum ist das gefährlich?

Mögliche Antwort:

Wenn dieser Storage ausfällt, sind sowohl die produktiven VMs als auch die Backups betroffen. Backups sollten getrennt vom Produktivsystem gespeichert werden, idealerweise zusätzlich offsite, offline oder immutable.

Prüfungsnahes Szenario 6

Eine VM mit Thin Provisioning hat eine virtuelle Festplatte von 500 GB. Auf dem echten Storage sind aber nur noch 20 GB frei.

Frage:

Warum ist das kritisch?

Mögliche Antwort:

Bei Thin Provisioning wächst die virtuelle Festplatte nach Bedarf. Wenn die VM weiter Daten schreibt, kann der echte Storage voll laufen. Dadurch können VMs einfrieren, abstürzen oder Daten beschädigt werden. Storage muss daher überwacht werden.

Prüfungsnahes Szenario 7

Ein Unternehmen möchte wissen, wie lange ein Dienst maximal ausfallen darf und wie viele Daten maximal verloren gehen dürfen.

Frage:

Welche Begriffe werden dafür verwendet?

Mögliche Antwort:

Die maximal akzeptierte Ausfallzeit heißt RTO.
Der maximal akzeptierte Datenverlust heißt RPO.

Prüfungsnahes Szenario 8

Eine Anwendung speichert Benutzersitzungen lokal auf dem Webserver. Hinter einem Load Balancer gibt es mehrere Webserver.

Frage:

Welches Problem kann entstehen?

Mögliche Antwort:

Wenn ein Benutzer bei verschiedenen Anfragen auf unterschiedliche Webserver geleitet wird, kennt der neue Webserver die lokale Sitzung nicht. Dadurch kann die Sitzung verloren gehen. Mögliche Lösungen sind Sticky Sessions oder ein zentraler Session-Speicher.

Lernkarte: VM

Frage	Antwort
Was ist eine VM?	Ein simulierter Computer auf einem Host
Was braucht eine VM?	vCPU, vRAM, vDisk, vNIC
Was läuft in einer VM?	Ein Gastbetriebssystem
Wofür nutzt man VMs?	Serverdienste, Tests, Isolation, Flexibilität

Lernkarte: Hypervisor

Frage	Antwort
Was ist ein Hypervisor?	Virtualisierungsschicht
Was verwaltet er?	VMs und Ressourcen
Was ist Typ-1?	Direkt auf Hardware

Frage	Antwort
Was ist Typ-2?	Auf vorhandenem Betriebssystem

Lernkarte: Snapshot

Frage	Antwort
Was ist ein Snapshot?	Zustand einer VM zu einem Zeitpunkt
Wofür nutzt man ihn?	Vor Updates oder Tests
Ist ein Snapshot ein Backup?	Nein
Warum nicht?	Meist gleicher Storage, kurzfristig gedacht

Lernkarte: Cluster

Frage	Antwort
Was ist ein Cluster?	Verbund mehrerer Server
Was ist ein Node?	Einzelner Server im Cluster
Was ist Ziel?	Hochverfügbarkeit, Lastverteilung, Skalierung
Ersetzt ein Cluster ein Backup?	Nein

Lernkarte: Quorum

Frage	Antwort
Was ist Quorum?	Entscheidungsmechanismus im Cluster
Wozu dient es?	Verhindert falsche Mehrfachaktivität
Was ist ein Witness?	Zusätzliche Stimme
Was verhindert Quorum?	Split-Brain

Lernkarte: Load Balancing

Frage	Antwort
Was ist Load Balancing?	Verteilung von Anfragen
Was ist ein Backend?	Zielservers hinter Load Balancer
Was ist ein Health Check?	Prüfung eines Backends
Was ist Sticky Session?	Benutzer bleibt auf gleichem Backend

Die wichtigsten Merksätze

Ein Server stellt Dienste bereit, ein Client nutzt Dienste.

Virtualisierung ermöglicht mehrere VMs auf einer physischen Hardware.

Eine VM ist ein simulierter Computer mit eigener virtueller Hardware.

Der Hypervisor verwaltet VMs und verteilt Ressourcen.

Ein Typ-1-Hypervisor läuft direkt auf Hardware.

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

Storage ist bei Virtualisierung besonders kritisch.

Thin Provisioning spart Speicher, muss aber überwacht werden.

Snapshots sind kein Backup.

RAID ist kein Backup.

Ein Backup ist nur sicher, wenn der Restore getestet wurde.

Ein Cluster erhöht Verfügbarkeit, ersetzt aber kein Backup.

Failover bedeutet Übernahme bei Ausfall.

Live Migration ist eine geplante Verschiebung einer laufenden VM.

Quorum verhindert gefährliche Split-Brain-Situationen.

Ein Witness hilft bei der Mehrheitsentscheidung im Cluster.

Split-Brain kann Datenkorruption verursachen.

Load Balancing verteilt Anfragen auf mehrere Server.

Scale-Up bedeutet ein System stärker machen.

Scale-Out bedeutet mehr Systeme hinzufügen.

Stateless-Anwendungen sind leichter zu skalieren als stateful Anwendungen.

Sehr kurze Prüfungszusammenfassung

Thema	Ein Satz
-------	----------

Server	Stellt Dienste im Netzwerk bereit
VM	Virtueller Computer auf einem Host
Hypervisor	Verwaltet virtuelle Maschinen
Typ-1	Hypervisor direkt auf Hardware
Typ-2	Hypervisor auf Betriebssystem
Storage	Speicher für VM-Daten
Snapshot	Kurzfristiger VM-Zustand
Backup	Echte Datensicherung
Cluster	Verbund mehrerer Server
Node	Einzelner Server im Cluster
HA	Möglichst geringe Ausfallzeit
Failover	Übernahme bei Ausfall
Quorum	Mehrheitsentscheidung im Cluster
Witness	Zusätzliche Stimme
Split-Brain	Gefährliche doppelte Aktivität
Load Balancing	Lastverteilung
Scale-Up	Ein System stärker machen
Scale-Out	Mehr Systeme hinzufügen
RPO	Maximaler Datenverlust
RTO	Maximale Wiederherstellungszeit

Abschluss

Damit ist das Kapitel **Server, Virtualisierung und Hochverfügbarkeit** inhaltlich vollständig.

Die wichtigsten Prüfungsbereiche sind:

Prüfungsbereich	Besonders wichtig
Virtualisierung	VM, Host, Guest, Hypervisor, Typ-1/Typ-2
VM-Betrieb	vCPU, RAM, Storage, Netzwerk, Guest Tools
Storage	Thin/Thick, IOPS, Latenz, Datastore
Sicherung	Snapshot vs. Backup, RAID vs. Backup, RPO/RTO
Cluster	Node, Ressource, Failover, Failback
Quorum	Witness, Mehrheit, Split-Brain

Prüfungsbereich	Besonders wichtig
Hochverfügbarkeit	Redundanz, SPOF, N+1
Load Balancing	Backend, Health Check, Sticky Session
Skalierung	Scale-Up, Scale-Out, Stateful, Stateless

Wenn du diese Begriffe erklären und voneinander unterscheiden kannst, hast du die wichtigsten Grundlagen für IHK-nahe Aufgaben zu Servern, Virtualisierung, Clustern und Hochverfügbarkeit verstanden.
