

13.4 Storage, Snapshots und Backups bei VMs

Einordnung

Diese Seite gehört zum Kapitel:

Server, Virtualisierung und Hochverfügbarkeit

Auf den vorherigen Seiten ging es um Server-Grundlagen, Virtualisierung, virtuelle Maschinen und Hypervisor-Verwaltung.

Jetzt geht es um ein besonders wichtiges Thema im VM-Betrieb:

Storage, Snapshots und Backups

Diese Themen sind wichtig, weil virtuelle Maschinen ihre Daten auf Speichersystemen ablegen und bei Fehlern wiederherstellbar sein müssen.

Grundidee

Eine virtuelle Maschine besteht nicht nur aus CPU und RAM.

Sie benötigt auch Speicherplatz für:

Bestandteil	Bedeutung
Betriebssystem	Windows Server, Linux usw.
Anwendungen	Serverdienste, Programme, Datenbanken
Konfiguration	Einstellungen der VM
Virtuelle Festplatten	Daten der VM
Snapshots	Zwischenstände
Backups	Sicherungskopien

Der Speicherbereich, auf dem virtuelle Maschinen liegen, wird häufig als **Storage** bezeichnet.

Was bedeutet Storage?

Storage bedeutet Speicherplatz für Daten.

In einer Virtualisierungsumgebung speichert Storage vor allem:

Datenart	Beispiel
----------	----------

VM-Konfiguration	Name, RAM, CPU, Netzwerk
Virtuelle Festplatten	VHDX, VMDK, QCOW2, RAW
ISO-Dateien	Installationsmedien
Snapshots	Zustände von VMs
Backups	Sicherungskopien
Templates	Vorlagen für neue VMs

Merksatz

Storage ist der Speicherbereich, auf dem virtuelle Maschinen, virtuelle Festplatten, Snapshots, ISO-Dateien, Templates und Backups abgelegt werden.

Warum Storage bei VMs besonders wichtig ist

Bei Virtualisierung greifen oft viele VMs gleichzeitig auf denselben Speicher zu.

Beispiel:

VM	Zugriff auf Storage
DC01	Betriebssystem, Active Directory
FILE01	Dateien und Freigaben
DB01	Datenbankdateien
WEB01	Webdaten
APP01	Anwendungsdaten

Wenn der Storage langsam oder voll ist, werden oft viele VMs gleichzeitig langsam oder fallen aus.

Typische Storage-Probleme bei VMs

Problem	Auswirkung
Storage voll	VMs können stehen bleiben oder abstürzen
Storage zu langsam	VMs reagieren träge
Hohe Latenz	Anwendungen wirken langsam
Defekte Festplatte	Datenverlust möglich
Alte Snapshots	Speicherverbrauch und Performanceprobleme
Kein Backup	Wiederherstellung nicht möglich
Falsches Provisioning	Speicher wird falsch eingeschätzt

Problem	Auswirkung
Fehlende Überwachung	Probleme werden zu spät erkannt

Virtuelle Festplatte

Eine virtuelle Festplatte ist der Datenträger einer VM.

Die VM sieht diese virtuelle Festplatte wie eine normale Festplatte.

Auf dem Host oder Storage liegt sie als Datei oder Block-Volume.

Typische Formate:

Format	Plattform
VHD	Älteres Hyper-V-Format
VHDX	Modernes Hyper-V-Format
VMDK	VMware
QCOW2	KVM / Proxmox
RAW	KVM / Proxmox
IMG	Allgemeines Image-Format

Beispiel

Eine VM mit dem Namen **WEB01** kann so aufgebaut sein:

Bestandteil	Beispiel
VM-Name	WEB01
Betriebssystem	Debian 12
Virtuelle Festplatte	WEB01.qcow2
Größe	80 GB
Speicherort	Datastore01
Netzwerk	VLAN 20

Die Datei **WEB01.qcow2** enthält dann die virtuelle Festplatte der VM.

Datastore

Ein Datastore ist ein Speicherbereich, auf dem VMs und ihre Dateien liegen.

Der Begriff wird besonders in VMware-Umgebungen verwendet, ist aber allgemein gut verständlich.

Beispiele:

Datastore	Inhalt
Datastore01	Produktive VMs
Datastore02	Test-VMs
ISO-Store	ISO-Dateien
Backup-Store	Sicherungen

Storage Pool

Ein Storage Pool ist ein zusammengefasster Speicherbereich aus mehreren Datenträgern oder Speicherressourcen.

Beispiel:

Mehrere SSDs werden zu einem Pool zusammengefasst.

Aus diesem Pool können dann Volumes oder virtuelle Festplatten bereitgestellt werden.

Begriff	Bedeutung
Physische Datenträger	Einzelne SSDs oder HDDs
Storage Pool	Zusammengefasster Speicher
Volume	Logischer Speicherbereich
Virtuelle Festplatte	Festplatte einer VM

Lokaler Storage

Lokaler Storage befindet sich direkt im Virtualisierungshost.

Beispiel:

Ein Proxmox-Host hat interne SSDs oder NVMe-Laufwerke.

Vorteile:

Vorteil	Erklärung
Einfach	Keine externe Storage-Infrastruktur nötig
Schnell möglich	Lokale NVMe kann sehr schnell sein

Vorteil	Erklärung
Günstiger Einstieg	Weniger zusätzliche Hardware

Nachteile:

Nachteil	Erklärung
Host-Abhängigkeit	VM liegt nur auf diesem Host
Schlechter für HA	Andere Hosts kommen nicht direkt an die Daten
Migration schwieriger	VM-Daten müssen übertragen werden
Ausfallrisiko	Host- oder Disk-Ausfall betrifft lokale VMs

Gemeinsamer Storage

Gemeinsamer Storage wird von mehreren Hosts genutzt.

Beispiel:

Drei Hypervisor-Hosts greifen auf dasselbe SAN oder NAS zu.

Host	Zugriff auf Storage
HV01	Ja
HV02	Ja
HV03	Ja

Vorteil:

VMs können leichter zwischen Hosts verschoben oder bei Ausfall auf einem anderen Host gestartet werden.

Vorteile von gemeinsamem Storage

Vorteil	Erklärung
Besser für Cluster	Mehrere Hosts können auf VM-Daten zugreifen
Live Migration einfacher	VM-Daten müssen nicht komplett kopiert werden
Zentrale Verwaltung	Speicher wird zentral bereitgestellt
Bessere HA-Möglichkeiten	VMs können auf anderem Host starten
Einfacheres Kapazitätsmanagement	Speicher zentral planen

Nachteile von gemeinsamem Storage

Nachteil	Erklärung
Komplexer	Netzwerk, Rechte und Storage müssen passen
Teurer	SAN/NAS kann kostenintensiv sein
Single Point of Failure möglich	Wenn Storage nicht redundant ist
Netzwerkabhängig	Storage-Verkehr benötigt stabile Verbindung
Performanceplanung nötig	Viele VMs greifen gleichzeitig zu

SAN

SAN steht für Storage Area Network.

Ein SAN stellt Blockspeicher über ein spezielles Storage-Netz bereit.

Typische Technologien:

Technologie	Bedeutung
Fibre Channel	Sehr schnelles dediziertes Storage-Netz
iSCSI	Blockspeicher über IP-Netzwerk
FCoE	Fibre Channel über Ethernet

SAN wird häufig in größeren Unternehmensumgebungen eingesetzt.

NAS

NAS steht für Network Attached Storage.

Ein NAS stellt Speicher über Netzwerkprotokolle bereit.

Typische Protokolle:

Protokoll	Einsatz
SMB	Windows-Dateifreigaben
NFS	Linux/Unix-Dateifreigaben
iSCSI	Blockspeicher über Netzwerk

Ein NAS kann auch als Speicherziel für VMs oder Backups verwendet werden.

SAN vs. NAS

Merkmal	SAN	NAS
Zugriff	Blockbasiert	Dateibasiert oder teils iSCSI
Typische Protokolle	Fibre Channel, iSCSI	SMB, NFS
Einsatz	Große Virtualisierungsumgebungen, Datenbanken	Dateifreigaben, Backups, kleinere VM-Umgebungen
Komplexität	Höher	Meist einfacher
Kosten	Oft höher	Oft günstiger

iSCSI

iSCSI stellt Blockspeicher über ein IP-Netzwerk bereit.

Der Client nennt sich Initiator.

Das Storage-Ziel nennt sich Target.

Begriff	Bedeutung
iSCSI Initiator	System, das den Speicher nutzt
iSCSI Target	System, das den Speicher bereitstellt
LUN	Logischer Speicherbereich

Beispiel:

Ein Hypervisor verbindet sich per iSCSI mit einem NAS und nutzt den bereitgestellten Speicher wie eine lokale Festplatte.

NFS

NFS steht für Network File System.

Es wird häufig in Linux- und Unix-Umgebungen verwendet.

NFS kann für VM-Speicher, ISO-Dateien oder Backups genutzt werden.

Beispiel:

Ein Proxmox-Host bindet ein NFS-Share vom NAS ein und speichert dort Backups oder ISO-Dateien.

SMB

SMB steht für Server Message Block.

Es ist besonders in Windows-Umgebungen verbreitet.

Typische Nutzung:

Nutzung	Beispiel
Dateifreigaben	Netzlaufwerke
Benutzerordner	Home-Verzeichnisse
Backupziel	Sicherungen auf NAS
Hyper-V Storage	SMB 3.0 kann für Hyper-V genutzt werden

RAID im Storage

RAID kombiniert mehrere Festplatten zu einem logischen Speicher.

Ziele:

Ziel	Erklärung
Ausfallsicherheit	Eine oder mehrere Platten dürfen ausfallen
Leistung	Daten werden verteilt
Kapazität	Mehrere Platten bilden größeren Speicher

Wichtige RAID-Level:

RAID-Level	Bedeutung	Vorteil	Nachteil
RAID 0	Striping ohne Redundanz	Schnell, volle Kapazität	Kein Ausfallschutz
RAID 1	Spiegelung	Eine Platte darf ausfallen	Weniger nutzbarer Speicher
RAID 5	Parität	Eine Platte darf ausfallen	Rebuild belastet System
RAID 6	Doppelte Parität	Zwei Platten dürfen ausfallen	Weniger nutzbarer Speicher
RAID 10	Spiegelung und Striping	Schnell und sicher	Benötigt viele Platten

RAID ist kein Backup

RAID schützt vor bestimmten Festplattenausfällen.

RAID schützt nicht zuverlässig gegen:

Risiko	Warum RAID nicht reicht
--------	-------------------------

Versehentliches Löschen	Gelöschte Daten werden auf allen Platten gelöscht
Ransomware	Verschlüsselte Daten werden ebenfalls gespeichert
Datenkorruption	Fehler können sich auf den RAID-Verbund auswirken
Brand oder Diebstahl	Alle Platten können betroffen sein
Fehlkonfiguration	Falsche Änderungen bleiben bestehen

Merksatz:

RAID erhöht die Verfügbarkeit des Speichers, ersetzt aber niemals ein Backup.

SSD, HDD und NVMe

Speicherart	Eigenschaften
HDD	Günstig, viel Speicher, mechanisch, langsamer
SSD	Schnell, keine mechanischen Teile, teurer pro TB
NVMe	Sehr schnell, geringe Latenz, ideal für hohe Last

Für Virtualisierung ist nicht nur die Kapazität wichtig, sondern auch Geschwindigkeit und Latenz.

IOPS

IOPS bedeutet Input/Output Operations Per Second.

Also:

Wie viele Lese- und Schreiboperationen ein Speicher pro Sekunde schafft.

Wichtig bei:

System	Warum IOPS wichtig sind
Datenbanken	Viele kleine Zugriffe
Mailserver	Viele Transaktionen
Fileserver	Viele Benutzerzugriffe
VDI	Viele gleichzeitige Desktop-VMs
Backup	Große Datenmengen

Latenz

Latenz ist die Verzögerung bei einem Zugriff.

Beispiel:

Eine VM fordert Daten vom Storage an.

Je niedriger die Latenz, desto schneller reagiert die VM.

Hohe Storage-Latenz führt oft zu langsamen Anwendungen.

Durchsatz

Durchsatz beschreibt, wie viele Daten pro Sekunde übertragen werden.

Beispiele:

Einheit	Bedeutung
MB/s	Megabyte pro Sekunde
GB/s	Gigabyte pro Sekunde
Gbit/s	Gigabit pro Sekunde im Netzwerk

Durchsatz ist wichtig bei großen Datenmengen, zum Beispiel Backups oder großen Dateiübertragungen.

IOPS vs. Durchsatz

Begriff	Wichtig bei
IOPS	Viele kleine Zugriffe
Durchsatz	Große zusammenhängende Datenmengen
Latenz	Reaktionszeit

Beispiel:

Eine Datenbank braucht oft viele IOPS und niedrige Latenz.

Ein Backup braucht oft hohen Durchsatz.

Thin Provisioning

Thin Provisioning bedeutet, dass eine virtuelle Festplatte eine Maximalgröße bekommt, aber auf dem echten Storage nur den tatsächlich genutzten Speicher belegt.

Beispiel:

Eingestellte Größe	Tatsächlich belegt
100 GB	25 GB

Vorteil:

Speicher wird effizient genutzt.

Nachteil:

Wenn viele VMs wachsen, kann der Storage 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:

Speicherverbrauch ist besser planbar.

Nachteil:

Weniger flexibel und weniger platzsparend.

Thin vs. Thick Provisioning

Merkmal	Thin Provisioning	Thick Provisioning
Speicherbelegung	Wächst nach Bedarf	Wird sofort reserviert
Effizienz	Hoch	Geringer
Risiko	Storage kann voll laufen	Weniger Überraschung
Planung	Muss gut überwacht werden	Einfacher planbar
Einsatz	Häufig bei flexiblen Umgebungen	Kritische oder klar geplante Systeme

Overprovisioning beim Storage

Storage-Overprovisioning bedeutet:

Es wird mehr virtueller Speicher vergeben, als physisch vorhanden ist.

Beispiel:

Physischer Storage	Vergebener VM-Speicher
2 TB	5 TB

Das kann funktionieren, solange die VMs nicht den gesamten Speicher tatsächlich nutzen.

Risiko:

Wenn viele VMs wachsen, wird der Storage voll.

Warum voller Storage gefährlich ist

Ein voller Storage kann schwere Probleme verursachen.

Mögliche Folgen:

Folge	Erklärung
VMs frieren ein	Schreibvorgänge sind nicht mehr möglich
VMs stürzen ab	Betriebssysteme können Fehler bekommen
Snapshots können nicht konsolidiert werden	Alte Daten bleiben liegen
Backups schlagen fehl	Kein Platz für Sicherungen
Datenbanken werden beschädigt	Schreibvorgänge brechen ab
Dienste fallen aus	Anwendungen können nicht mehr arbeiten

Merksatz:

Ein voller VM-Storage ist ein kritischer Zustand und muss unbedingt vermieden werden.

Storage-Monitoring

Storage muss dauerhaft überwacht werden.

Wichtige Werte:

Wert	Bedeutung
Freier Speicherplatz	Wie viel Platz ist noch vorhanden?
Wachstum	Wie schnell wächst der Speicherverbrauch?
IOPS	Anzahl Speicheroperationen

Wert	Bedeutung
Latenz	Verzögerung beim Zugriff
Durchsatz	Datenmenge pro Sekunde
Fehler	Defekte Blöcke, Controllerfehler
Snapshot-Größe	Alte oder wachsende Snapshots
Backupstatus	Sicherungen erfolgreich?

Snapshot

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

Typische Nutzung:

Situation	Warum Snapshot?
Vor Updates	Rückkehr möglich, wenn Update fehlschlägt
Vor Softwareinstallation	Test kann rückgängig gemacht werden
Vor Konfigurationsänderung	Absicherung gegen Fehler
Schulungsumgebung	Zurück zum Ausgangszustand

Was speichert ein Snapshot?

Je nach Plattform kann ein Snapshot Folgendes speichern:

Bestandteil	Erklärung
Festplattenzustand	Zustand der virtuellen Festplatte
VM-Konfiguration	Einstellungen der VM
Arbeitsspeicherzustand	Optional laufender RAM-Zustand

Nicht jeder Snapshot enthält automatisch den Arbeitsspeicherzustand.

Wie funktioniert ein Snapshot vereinfacht?

Vor dem Snapshot schreibt die VM direkt in ihre virtuelle Festplatte.

Nach dem Snapshot werden neue Änderungen getrennt gespeichert.

Vereinfacht:

Zeitpunkt	Speicherung
-----------	-------------

Vor Snapshot	VM schreibt in die ursprüngliche virtuelle Festplatte
Nach Snapshot	Änderungen werden in eine zusätzliche Snapshot-Datei geschrieben
Beim Zurücksetzen	VM kehrt zum alten Zustand zurück
Beim Löschen	Änderungen werden zusammengeführt

Snapshot-Kette

Wenn mehrere Snapshots erstellt werden, kann eine Kette entstehen.

Beispiel:

Ebene	Bedeutung
Basisdisk	Ursprüngliche virtuelle Festplatte
Snapshot 1	Änderungen nach erstem Snapshot
Snapshot 2	Änderungen nach zweitem Snapshot
Snapshot 3	Änderungen nach drittem Snapshot

Je länger und komplexer die Snapshot-Kette ist, desto riskanter wird die Verwaltung.

Probleme durch alte Snapshots

Problem	Erklärung
Speicherverbrauch	Snapshot-Dateien wachsen mit Änderungen
Performanceverlust	Lesen und Schreiben wird komplexer
Backupfehler	Backups können länger dauern oder fehlschlagen
Konsolidierungsprobleme	Zusammenführen kann schwierig werden
Storage voll	Snapshot-Wachstum kann Speicher füllen

Merksatz:

Snapshots nur kurzfristig verwenden und nach erfolgreicher Änderung wieder entfernen.

Snapshots sind kein Backup

Ein Snapshot ist kein Backup.

Warum?

Grund	Erklärung
Gleicher Storage	Snapshot liegt oft auf demselben Speicher
Kurzfristig gedacht	Nicht für langfristige Sicherung
Kein Schutz vor Storage-Ausfall	Fällt Storage aus, ist auch Snapshot betroffen
Kein Schutz vor Ransomware	Angreifer können Snapshots löschen oder beschädigen
Kein Ersatz für Restore-Konzept	Backup muss separat wiederherstellbar sein

Snapshot vs. Backup

Merkmal	Snapshot	Backup
Zweck	Kurzfristiger Zustand	Datensicherung
Speicherort	Meist gleicher Storage	Separater Speicher möglich
Zeitraum	Kurzfristig	Mittel- bis langfristig
Schutz bei Storage-Ausfall	Nein	Ja, wenn extern gespeichert
Einsatz	Updates, Tests	Wiederherstellung nach Datenverlust
Ersatz für Backup?	Nein	Ja, echte Sicherung

Checkpoint

Bei Hyper-V wird häufig der Begriff Checkpoint verwendet.

Ein Checkpoint ist ähnlich wie ein Snapshot.

Arten:

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

Auch Checkpoints sind kein Ersatz für Backups.

Backup

Ein Backup ist eine Sicherung von Daten oder Systemen.

Ziel:

Daten oder ganze Systeme sollen nach einem Fehler wiederhergestellt werden können.

Typische Ursachen für Wiederherstellung:

Ursache	Beispiel
Versehentliches Löschen	Benutzer löscht Datei
Hardwaredefekt	Storage oder Server fällt aus
Malware	Daten werden verschlüsselt
Fehlkonfiguration	System wird falsch geändert
Updatefehler	Anwendung funktioniert nicht mehr
Datenbankfehler	Daten werden beschädigt
Katastrophe	Brand, Wasser, Diebstahl

Backuparten

Backupart	Erklärung
Vollbackup	Sichert alle ausgewählten Daten
Inkrementelles Backup	Sichert Änderungen seit dem letzten Backup
Differenzielles Backup	Sichert Änderungen seit dem letzten Vollbackup
Image-basiertes Backup	Sichert eine ganze VM oder ein ganzes System
Datei-basiertes Backup	Sichert einzelne Dateien und Ordner
Applikationskonsistentes Backup	Berücksichtigt laufende Anwendungen
Agent-basiertes Backup	Backupsoftware läuft im Gastbetriebssystem
Agentless Backup	Backup erfolgt über Hypervisor-Schnittstelle

Vollbackup

Ein Vollbackup sichert alle ausgewählten Daten vollständig.

Vorteil:

Einfach wiederherzustellen.

Nachteil:

Benötigt viel Speicherplatz und Zeit.

Beispiel:

Jeden Sonntag wird eine vollständige Sicherung der VM erstellt.

Inkrementelles Backup

Ein inkrementelles Backup sichert nur die Änderungen seit dem letzten Backup.

Beispiel:

Tag	Sicherung
Sonntag	Vollbackup
Montag	Änderungen seit Sonntag
Dienstag	Änderungen seit Montag
Mittwoch	Änderungen seit Dienstag

Vorteil:

Schnell und speichersparend.

Nachteil:

Für eine Wiederherstellung werden mehrere Backupstände benötigt.

Differenzielles Backup

Ein differenzielles Backup sichert alle Änderungen seit dem letzten Vollbackup.

Beispiel:

Tag	Sicherung
Sonntag	Vollbackup
Montag	Änderungen seit Sonntag
Dienstag	Änderungen seit Sonntag
Mittwoch	Änderungen seit Sonntag

Vorteil:

Wiederherstellung ist einfacher als bei vielen inkrementellen Backups.

Nachteil:

Differenzielle Backups werden mit der Zeit größer.

Vollbackup vs. inkrementell vs. differenziell

Merkmal	Vollbackup	Inkrementell	Differenziell
Speicherbedarf	Hoch	Niedrig	Mittel
Backupdauer	Lang	Kurz	Mittel
Restore	Einfach	Abhängig von Backupkette	Einfacher als inkrementell
Typischer Einsatz	Basisbackup	Tägliche Sicherung	Alternative tägliche Sicherung

Image-basiertes VM-Backup

Bei einem image-basierten Backup wird die ganze VM gesichert.

Gesichert werden können:

Bestandteil	Beispiel
VM-Konfiguration	CPU, RAM, Netzwerk
Virtuelle Festplatten	VHDX, VMDK, QCOW2
VM-Zustand	Je nach Verfahren
Metadaten	Name, ID, Einstellungen

Vorteil:

Die ganze VM kann wiederhergestellt werden.

Datei-basiertes Backup

Beim datei-basierten Backup werden einzelne Dateien oder Ordner gesichert.

Beispiel:

Daten	Beispiel
Benutzerdateien	Dokumente
Konfigurationen	config-Dateien
Webdaten	HTML, PHP, Bilder
Anwendungsdaten	Exportordner

Vorteil:

Einzelne Dateien können gezielt wiederhergestellt werden.

Nachteil:

Das komplette System ist damit nicht immer schnell wiederherstellbar.

Agent-basiertes Backup

Beim agent-basierten Backup läuft eine Backupsoftware innerhalb der VM.

Vorteile:

Vorteil	Erklärung
Anwendung kennt das Betriebssystem	Gute Kontrolle innerhalb der VM
Dateibasierte Sicherung möglich	Einzelne Dateien sichern
Applikationsintegration	Datenbanken können berücksichtigt werden

Nachteile:

Nachteil	Erklärung
Agent muss gepflegt werden	Installation und Updates nötig
Mehr Verwaltungsaufwand	Pro VM konfigurieren
Belastung der VM	Backup läuft innerhalb der VM

Agentless Backup

Beim agentless Backup wird die VM über den Hypervisor gesichert.

Vorteile:

Vorteil	Erklärung
Zentrale Sicherung	Backup über Hypervisor
Kein Agent in jeder VM nötig	Weniger Pflege
Ganze VM leicht sicherbar	Image-basierte Sicherung
Gut für viele VMs	Skalierbar

Nachteile:

Nachteil	Erklärung
Anwendungskonsistenz beachten	Datenbanken brauchen besondere Behandlung
Hypervisor-Integration nötig	Plattform muss unterstützt werden
Rechte erforderlich	Backupsoftware braucht Zugriff auf Hypervisor

Applikationskonsistentes Backup

Ein applikationskonsistentes Backup berücksichtigt laufende Anwendungen.

Besonders wichtig bei:

Anwendung	Warum wichtig?
Datenbanken	Schreibvorgänge müssen sauber abgeschlossen werden
Active Directory	Verzeichnisdienst muss konsistent bleiben
Mailserver	Viele Transaktionen
ERP-Systeme	Geschäftsdaten dürfen nicht beschädigt werden
Dokumentenmanagement	Datenbank und Dateien müssen zusammenpassen

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

Crash-konsistentes Backup

Ein crash-konsistentes Backup entspricht ungefähr dem Zustand nach einem Stromausfall.

Das Dateisystem ist meist in einem wiederherstellbaren Zustand, aber Anwendungen können unvollständige Transaktionen haben.

Art	Bedeutung
Crash-konsistent	Wie nach hartem Ausschalten
Applikationskonsistent	Anwendung wurde sauber berücksichtigt

Für einfache Systeme kann crash-konsistent reichen.

Für Datenbanken ist applikationskonsistent besser.

Backupziel

Ein Backupziel ist der Speicherort für Sicherungen.

Beispiele:

Backupziel	Beispiel
Lokales NAS	Backup auf Netzwerkspeicher
Externes NAS	Zweites Gerät an anderem Ort
Externe Festplatte	Offline-Backup
Cloudspeicher	Offsite-Sicherung

Backupziel	Beispiel
Tape	Bandlaufwerk für Langzeitarchivierung
Backup-Appliance	Spezielles Backup-System

Offsite-Backup

Offsite bedeutet:

Eine Sicherung liegt außerhalb des Hauptstandorts.

Warum wichtig?

Risiko am Hauptstandort	Warum Offsite hilft
Brand	Externe Kopie bleibt erhalten
Diebstahl	Externe Kopie bleibt erhalten
Wasserschaden	Externe Kopie bleibt erhalten
Ransomware	Getrennte Kopie kann geschützt sein
Totalausfall	Wiederherstellung an anderem Ort möglich

Offline-Backup

Offline-Backup bedeutet:

Die Sicherung ist nicht dauerhaft mit dem Netzwerk verbunden.

Beispiel:

Eine externe Festplatte wird nach dem Backup getrennt.

Vorteil:

Besserer Schutz gegen Ransomware.

Nachteil:

Mehr manueller Aufwand.

Immutable Backup

Immutable bedeutet unveränderbar.

Ein immutable Backup kann für eine bestimmte Zeit nicht gelöscht oder verändert werden.

Vorteil:

Schutz gegen Ransomware und versehentliches Löschen.

Beispiel:

Backups werden 30 Tage unveränderbar gespeichert.

3-2-1-Regel

Eine bekannte Backup-Regel ist die 3-2-1-Regel.

Regel	Bedeutung
3 Kopien	Original plus zwei Sicherungen
2 verschiedene Medien	Zum Beispiel NAS und externe Festplatte
1 Kopie extern	Eine Kopie außerhalb des Standorts

Erweiterung:

Erweiterung	Bedeutung
3-2-1-1-0	Zusätzlich eine Offline/Immutable-Kopie und 0 Fehler bei Backupprüfung

RPO

RPO steht für Recovery Point Objective.

Es beantwortet die Frage:

Wie viele Daten dürfen maximal verloren gehen?

Beispiel:

RPO	Bedeutung
24 Stunden	Datenverlust von bis zu einem Tag wäre akzeptiert
1 Stunde	Maximal eine Stunde Datenverlust
15 Minuten	Sehr geringe Datenverlust-Toleranz

Je kleiner das RPO, desto häufiger müssen Backups oder Replikationen erfolgen.

RTO

RTO steht für Recovery Time Objective.

Es beantwortet die Frage:

Wie lange darf die Wiederherstellung dauern?

Beispiel:

RTO	Bedeutung
24 Stunden	Dienst darf bis zu einem Tag ausfallen
4 Stunden	Dienst muss am selben Tag wieder laufen
30 Minuten	Sehr schnelle Wiederherstellung nötig

Je kleiner das RTO, desto schneller muss die Wiederherstellung funktionieren.

RPO vs. RTO

Begriff	Frage	Beispiel
RPO	Wie viele Daten dürfen verloren gehen?	Maximal 1 Stunde Daten
RTO	Wie lange darf der Ausfall dauern?	Maximal 4 Stunden

Merksatz:

RPO betrifft den Datenverlust. RTO betrifft die Ausfallzeit.

Restore

Restore bedeutet Wiederherstellung aus einem Backup.

Mögliche Restore-Arten:

Restore-Art	Erklärung
Full Restore	Ganze VM wiederherstellen
File Restore	Einzelne Datei wiederherstellen
Disk Restore	Einzelne virtuelle Festplatte zurückholen
Application Restore	Datenbank oder Anwendung wiederherstellen
Instant Recovery	VM direkt aus Backup starten
Bare-Metal-Recovery	System auf neuer Hardware wiederherstellen

Backup ohne Restore-Test ist unsicher

Ein Backup ist nur dann wirklich wertvoll, wenn es wiederhergestellt werden kann.

Deshalb müssen Restore-Tests durchgeführt werden.

Typische Tests:

Test	Ziel
Einzelne Datei wiederherstellen	Prüfen, ob File Restore funktioniert
Ganze VM wiederherstellen	Prüfen, ob System bootet
Datenbank wiederherstellen	Anwendungskonsistenz prüfen
Restore-Zeit messen	RTO prüfen
Backup-Protokolle prüfen	Fehler erkennen

Merksatz:

Ein ungeprüftes Backup ist nur eine Hoffnung, keine Sicherheit.

Backupfenster

Das Backupfenster ist der Zeitraum, in dem Sicherungen durchgeführt werden sollen.

Beispiel:

Backups laufen nachts zwischen 22:00 Uhr und 06:00 Uhr.

Problem:

Wenn das Backup länger dauert als das Backupfenster, kann es den produktiven Betrieb stören.

Aufbewahrungszeit

Die Aufbewahrungszeit legt fest, wie lange Backups gespeichert werden.

Beispiel:

Backup	Aufbewahrung
Täglich	14 Tage
Wöchentlich	8 Wochen
Monatlich	12 Monate
Jährlich	10 Jahre

Die Aufbewahrung hängt von technischen, organisatorischen und rechtlichen Anforderungen ab.

Backup-Rotation

Backup-Rotation bedeutet, dass alte Backups nach festen Regeln ersetzt oder gelöscht werden.

Beispiel:

Sicherung	Zweck
Täglich	Kurzfristige Wiederherstellung
Wöchentlich	Mittelfristige Wiederherstellung
Monatlich	Langfristige Wiederherstellung
Jährlich	Archivierung

GFS-Prinzip

GFS steht für Grandfather-Father-Son.

Ebene	Bedeutung
Son	Tägliche Backups
Father	Wöchentliche Backups
Grandfather	Monatliche Backups

Dieses Prinzip wird häufig für Backup-Aufbewahrung genutzt.

Replikation

Replikation bedeutet, dass Daten oder VMs auf ein anderes System kopiert werden.

Ziel:

Bei Ausfall kann schneller auf eine Kopie umgeschaltet werden.

Arten:

Art	Erklärung
Synchrone Replikation	Daten werden gleichzeitig auf Zielsystem geschrieben
Asynchrone Replikation	Daten werden zeitversetzt übertragen

Synchrone Replikation

Bei synchroner Replikation wird ein Schreibvorgang erst bestätigt, wenn er auf beiden Seiten angekommen ist.

Vorteil:

Sehr geringer Datenverlust.

Nachteil:

Höhere Anforderungen an Netzwerk und Latenz.

Asynchrone Replikation

Bei asynchroner Replikation werden Daten zeitversetzt kopiert.

Vorteil:

Weniger Netzwerkabhängigkeit und oft einfacher.

Nachteil:

Bei Ausfall können letzte Änderungen fehlen.

Replikation ist kein Backup

Replikation schützt vor Systemausfall, aber nicht automatisch vor logischen Fehlern.

Beispiel:

Wenn eine Datei versehentlich gelöscht wird, kann diese Löschung auf das Ziel repliziert werden.

Deshalb gilt:

Replikation ersetzt kein Backup.

Backup vs. Replikation

Merkmal	Backup	Replikation
Ziel	Wiederherstellung alter Zustände	Schnelle Verfügbarkeit einer Kopie
Schutz vor versehentlichem Löschen	Ja, wenn Version vorhanden	Nicht unbedingt
Schutz vor Ransomware	Ja, wenn getrennt/immutable	Nicht unbedingt
RTO	Je nach Restore-Zeit	Oft schneller
RPO	Je nach Sicherungsintervall	Oft kleiner

Merkmal	Backup	Replikation
Ersatz füreinander?	Nein	Nein

Disaster Recovery

Disaster Recovery beschreibt die Wiederherstellung nach einem größeren Ausfall.

Beispiele:

Ereignis	Beispiel
Hardwareausfall	Storage defekt
Ransomware	Daten verschlüsselt
Brand	Serverraum beschädigt
Wasserschaden	Hardware zerstört
Fehlkonfiguration	Systeme falsch geändert
Standortausfall	Gebäude nicht nutzbar

Disaster Recovery umfasst Backup, Restore-Pläne, Ersatzsysteme, Dokumentation und regelmäßige Tests.

Disaster-Recovery-Plan

Ein Disaster-Recovery-Plan beschreibt, wie Systeme nach einem größeren Ausfall wiederhergestellt werden.

Wichtige Inhalte:

Inhalt	Erklärung
Kritische Systeme	Welche VMs müssen zuerst wieder laufen?
Abhängigkeiten	Welche Systeme brauchen andere Systeme?
Backupstandorte	Wo liegen die Sicherungen?
Zugangsdaten	Wer darf Systeme wiederherstellen?
Wiederherstellungsreihenfolge	Welche VM zuerst?
Ansprechpartner	Zuständigkeiten
Testverfahren	Wie wird geprüft, ob alles funktioniert?

Wiederherstellungsreihenfolge

Bei mehreren VMs ist die Reihenfolge wichtig.

Beispiel:

Reihenfolge	VM	Grund
1	DC01	Anmeldung und DNS
2	DB01	Datenbank für Anwendungen
3	FILE01	Dateifreigaben
4	APP01	Anwendung benötigt Datenbank
5	WEB01	Webserver nutzt Anwendung

Wenn abhängige Systeme falsch gestartet werden, funktionieren Dienste möglicherweise nicht.

Backup von Domain Controllern

Domain Controller sollten besonders sorgfältig gesichert werden.

Wichtig:

Punkt	Erklärung
System State	Wichtig für Active Directory
Mehrere Domain Controller	Redundanz verbessern
Saubere Wiederherstellung	AD darf nicht inkonsistent werden
DNS beachten	AD hängt stark von DNS ab

Bei Active Directory ist eine einfache Kopie der VM nicht immer ausreichend geplant.

Backup von Datenbanken

Datenbanken benötigen besondere Beachtung.

Mögliche Methoden:

Methode	Erklärung
Datenbankdump	Logischer Export der Datenbank
Applikationskonsistentes VM-Backup	Backup berücksichtigt Datenbankzustand
Transaktionslog-Backup	Feingranulare Wiederherstellung
Replikation	Kopie auf zweitem System

Wichtig:

Eine laufende Datenbank sollte nicht nur durch einfaches Kopieren der Disk gesichert werden.

Backup von Dateiservern

Bei Dateiservern sind einzelne Datei-Wiederherstellungen besonders wichtig.

Typische Anforderungen:

Anforderung	Beispiel
Einzelne Datei wiederherstellen	Benutzer hat Datei gelöscht
Ordner wiederherstellen	Projektordner wurde überschrieben
Versionen wiederherstellen	Ältere Fassung benötigt
Rechte erhalten	NTFS-Rechte oder Linux-Rechte
Große Datenmengen	Backupfenster beachten

Backup von Webservern

Webserver bestehen oft aus mehreren Teilen.

Bestandteil	Beispiel
Webdateien	HTML, CSS, PHP, Bilder
Konfiguration	Nginx, Apache, Zertifikate
Datenbank	MariaDB, PostgreSQL
Zertifikate	TLS-Zertifikate
Umgebung	Container, VM, Pakete

Wichtig:

Bei Webanwendungen reicht es oft nicht, nur die Webdateien zu sichern.
Die Datenbank muss ebenfalls gesichert werden.

Backup von Zertifikaten und Schlüsseln

Zertifikate und private Schlüssel sind wichtig.

Beispiele:

Element	Bedeutung
---------	-----------

TLS-Zertifikat	Verschlüsselte HTTPS-Verbindungen
Private Keys	Schlüsselmaterial
SSH-Keys	Zugriff und Automatisierung
API-Keys	Zugriff auf Dienste
Lizenzdateien	Softwarelizenzen

Verlust von Schlüsseln kann zu Ausfällen oder Sicherheitsproblemen führen.

Verschlüsselung von Backups

Backups sollten geschützt werden.

Maßnahmen:

Maßnahme	Erklärung
Verschlüsselung	Schutz bei Diebstahl
Zugriffsbeschränkung	Nur berechtigte Personen
Getrennte Zugangsdaten	Backupsystem nicht mit normalen Adminrechten
MFA	Schutz für Backupverwaltung
Offline/Immutable	Schutz gegen Ransomware

Backup-Sicherheit

Backupsysteme sind besonders schützenswert.

Warum?

Wenn ein Angreifer Backups löschen kann, wird Wiederherstellung schwierig.

Maßnahmen:

Maßnahme	Erklärung
Eigene Admin-Konten	Nicht gleiche Konten wie Produktivsystem
MFA	Zusätzliche Anmeldung
Immutable Storage	Backups nicht veränderbar
Netzwerksegmentierung	Backupnetz trennen
Keine dauerhafte Freigabe mit Schreibrechten	Schutz vor Ransomware
Monitoring	Backupfehler erkennen

Maßnahme	Erklärung
Restore-Tests	Wiederherstellung prüfen

Backup-Protokolle prüfen

Nach Backups sollten Protokolle geprüft werden.

Wichtige Fragen:

Frage	Bedeutung
War das Backup erfolgreich?	Keine Fehler?
Wurden alle VMs gesichert?	Keine VM vergessen?
Gab es Warnungen?	Zum Beispiel Snapshot-Probleme
Wie lange dauerte das Backup?	Passt es ins Backupfenster?
Wie groß ist das Backup?	Speicherplanung
Ist Restore möglich?	Test erforderlich

Storage und Backup trennen

Backups sollten nicht nur auf demselben Storage liegen wie die produktiven VMs.

Problem:

Wenn der Storage ausfällt, sind sonst VMs und Backups gleichzeitig weg.

Besser:

Speicherort	Zweck
Produktiv-Storage	Laufende VMs
Backup-Storage	Sicherungen
Offsite-Kopie	Schutz bei Standortausfall
Offline/Immutable-Kopie	Schutz gegen Ransomware

Typische Fehler bei Storage, Snapshots und Backups

Fehler	Auswirkung
Snapshots zu lange behalten	Speicher- und Performanceprobleme
Kein Restore-Test	Backup kann unbrauchbar sein

Fehler	Auswirkung
Backups auf gleichem Storage	Kein Schutz bei Storage-Ausfall
Storage nicht überwacht	Speicher läuft voll
Thin Provisioning ohne Monitoring	Unerwartet voller Storage
Keine applikationskonsistenten Backups	Datenbanken können beschädigt sein
Keine Offsite-Kopie	Standortausfall zerstört alle Daten
Backup-Zugang schlecht geschützt	Ransomware kann Backups löschen
RPO/RTO nicht definiert	Unklare Wiederherstellungsziele

Gute Praxis

Empfehlung	Grund
Storage überwachen	Probleme früh erkennen
Freien Speicher einplanen	Snapshots und Wachstum abfangen
Snapshots nur kurzfristig nutzen	Performance und Speicher schützen
Backups regelmäßig durchführen	Datenverlust vermeiden
Restore regelmäßig testen	Sicherstellen, dass Backups funktionieren
Backups getrennt speichern	Schutz bei Storage-Ausfall
Offsite-Kopie nutzen	Schutz bei Standortausfall
Immutable oder Offline-Kopie nutzen	Schutz gegen Ransomware
RPO und RTO definieren	Anforderungen klar festlegen
Backupdokumentation pflegen	Wiederherstellung erleichtern

Prüfungsnahes Beispiel 1

Aufgabe:

Ein Administrator erstellt vor einem Update einen Snapshot einer VM. Nach erfolgreichem Update bleibt der Snapshot mehrere Monate bestehen.

Frage:

Warum ist das problematisch?

Mögliche Antwort:

Snapshots sind nur für kurzfristige Zustände gedacht. Wenn sie lange bestehen bleiben, können sie viel Speicher verbrauchen, die Performance verschlechtern und zu Problemen bei der

Konsolidierung führen. Außerdem sind Snapshots kein Backup und schützen nicht vor Storage-Ausfall.

Prüfungsnahes Beispiel 2

Aufgabe:

Ein Unternehmen speichert seine produktiven VMs und deren Backups auf demselben Storage-System.

Frage:

Welches Risiko besteht?

Mögliche Antwort:

Wenn dieses Storage-System ausfällt oder beschädigt wird, sind sowohl die produktiven VMs als auch die Backups betroffen. Dadurch ist keine Wiederherstellung möglich. Backups sollten getrennt, möglichst zusätzlich offsite oder immutable gespeichert werden.

Prüfungsnahes Beispiel 3

Aufgabe:

Eine VM besitzt eine virtuelle Festplatte mit 500 GB Thin Provisioning. Tatsächlich sind auf dem Storage nur noch 50 GB frei.

Frage:

Warum ist das gefährlich?

Mögliche Antwort:

Bei Thin Provisioning wächst die virtuelle Festplatte nach Bedarf. Wenn die VM weiter Daten schreibt, kann der echte Storage voll laufen. Das kann dazu führen, dass VMs einfrieren, Backups fehlschlagen oder Daten beschädigt werden. Thin Provisioning muss daher überwacht werden.

Prüfungsnahes Beispiel 4

Aufgabe:

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

Frage:

Welche Begriffe sind gemeint?

Mögliche Antwort:

Die maximale Ausfallzeit wird mit RTO beschrieben. Der maximal akzeptierte Datenverlust wird mit RPO beschrieben.

Typische Prüfungsfrage: Was ist Storage?

Mögliche Antwort:

Storage bezeichnet den Speicherbereich, auf dem Daten abgelegt werden. In Virtualisierungsumgebungen liegen dort virtuelle Festplatten, VM-Konfigurationen, ISO-Dateien, Templates, Snapshots und Backups.

Typische Prüfungsfrage: Warum ist Storage bei VMs kritisch?

Mögliche Antwort:

Viele virtuelle Maschinen greifen gleichzeitig auf denselben Storage zu. Wenn der Storage langsam, voll oder ausgefallen ist, können mehrere VMs gleichzeitig betroffen sein. Deshalb müssen Speicherplatz, IOPS, Latenz, Durchsatz und Fehler überwacht werden.

Typische Prüfungsfrage: Was ist ein Snapshot?

Mögliche Antwort:

Ein Snapshot speichert den Zustand einer virtuellen Maschine zu einem bestimmten Zeitpunkt. Er wird häufig vor Updates oder Konfigurationsänderungen verwendet, um schnell zu einem vorherigen Zustand zurückkehren zu können.

Typische Prüfungsfrage: Warum ist ein Snapshot kein Backup?

Mögliche Antwort:

Ein Snapshot liegt meist auf demselben Storage wie die VM und ist für kurzfristige Änderungen gedacht. Fällt der Storage aus, ist auch der Snapshot betroffen. Ein Backup wird separat gespeichert und dient zur Wiederherstellung nach Datenverlust oder Ausfall.

Typische Prüfungsfrage: Unterschied zwischen Snapshot und Backup

Snapshot	Backup
Kurzfristiger Zustand	Echte Datensicherung

Snapshot	Backup
Meist gleicher Storage	Separater Speicher möglich
Für Tests und Updates	Für Wiederherstellung
Kein Schutz bei Storage-Ausfall	Schutz möglich, wenn getrennt gespeichert
Kein Ersatz für Backup	Backup ist notwendig

Typische Prüfungsfrage: Was bedeutet Thin Provisioning?

Mögliche Antwort:

Thin Provisioning bedeutet, dass einer virtuellen Festplatte eine Maximalgröße zugewiesen wird, aber auf dem echten Storage zunächst nur der tatsächlich genutzte Speicherplatz belegt wird. Das spart Speicher, muss aber überwacht werden, weil der Storage sonst unerwartet voll laufen kann.

Typische Prüfungsfrage: Was bedeutet Thick Provisioning?

Mögliche Antwort:

Thick Provisioning bedeutet, dass der Speicherplatz für eine virtuelle Festplatte sofort vollständig reserviert wird. Dadurch ist der Speicherverbrauch besser planbar, aber weniger flexibel und weniger platzsparend.

Typische Prüfungsfrage: Was ist 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 Prüfungsfrage: Was ist 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 Prüfungsfrage: Warum ist RAID kein Backup?

Mögliche Antwort:

RAID schützt vor bestimmten Festplattenausfällen, aber nicht vor versehentlichem Löschen, Ransomware, Datenkorruption oder Standortausfall. Ein Backup ist eine separate Sicherung, mit der Daten wiederhergestellt werden können.

Typische Prüfungsfrage: Was ist ein applikationskonsistentes Backup?

Mögliche Antwort:

Ein applikationskonsistentes Backup berücksichtigt laufende Anwendungen wie Datenbanken oder Active Directory. Dadurch werden offene Schreibvorgänge und Transaktionen sauber behandelt, damit die Daten nach der Wiederherstellung konsistent sind.

Typische Prüfungsfrage: Was bedeutet Offsite-Backup?

Mögliche Antwort:

Ein Offsite-Backup ist eine Sicherung, die außerhalb des Hauptstandorts gespeichert wird. Es schützt vor Ereignissen wie Brand, Diebstahl, Wasserschaden oder vollständigem Standortausfall.

Typische Prüfungsfrage: Was bedeutet immutable Backup?

Mögliche Antwort:

Ein immutable Backup ist eine Sicherung, die für eine bestimmte Zeit nicht verändert oder gelöscht werden kann. Dadurch schützt es besser gegen Ransomware und versehentliches Löschen.

Wichtige Begriffe

Begriff	Kurz erklärt
Storage	Speicherbereich für Daten
Datastore	Speicherbereich für VM-Dateien
Storage Pool	Zusammengefasster Speicher
Virtuelle Festplatte	Datenträger einer VM
VHDX	Virtuelles Festplattenformat bei Hyper-V
VMDK	Virtuelles Festplattenformat bei VMware
QCOW2	Virtuelles Festplattenformat bei KVM/Proxmox
RAW	Einfaches Festplattenimage
SAN	Storage Area Network
NAS	Network Attached Storage

Begriff	Kurz erklärt
iSCSI	Blockspeicher über IP
NFS	Netzwerkdateisystem
SMB	Windows-Dateifreigabeprotokoll
RAID	Verbund mehrerer Festplatten
IOPS	Speicherooperationen pro Sekunde
Latenz	Verzögerung beim Zugriff
Durchsatz	Datenmenge pro Sekunde
Thin Provisioning	Speicher wächst nach Bedarf
Thick Provisioning	Speicher wird sofort reserviert
Snapshot	Zustand einer VM zu einem Zeitpunkt
Checkpoint	Snapshot-ähnliche Funktion bei Hyper-V
Backup	Datensicherung
Restore	Wiederherstellung
RPO	Maximal akzeptierter Datenverlust
RTO	Maximal akzeptierte Wiederherstellungszeit
Offsite-Backup	Sicherung außerhalb des Standorts
Offline-Backup	Nicht dauerhaft verbundenes Backup
Immutable Backup	Unveränderbare Sicherung
Replikation	Kopie auf anderes System
Disaster Recovery	Wiederherstellung nach großem Ausfall

Wichtige Merksätze

Storage ist bei Virtualisierung besonders kritisch, weil viele VMs gleichzeitig davon abhängig sein können.

Ein voller Storage kann VMs zum Stillstand bringen.

Thin Provisioning spart Speicher, muss aber überwacht werden.

Thick Provisioning ist weniger flexibel, aber besser planbar.

Snapshots sind nur für kurzfristige Änderungen gedacht.

Snapshots sind kein Backup.

RAID ist kein Backup.

Backups müssen getrennt vom Produktivsystem gespeichert werden.

Ein Backup ist nur dann zuverlässig, wenn die Wiederherstellung getestet wurde.

RPO beschreibt den maximal akzeptierten Datenverlust.

RTO beschreibt die maximal akzeptierte Ausfallzeit.

Replikation ersetzt kein Backup.

Immutable oder Offline-Backups schützen besser gegen Ransomware.

Kurzzusammenfassung

Storage, Snapshots und Backups sind zentrale Bestandteile jeder Virtualisierungsumgebung.

Virtuelle Maschinen speichern ihre Daten auf virtuellen Festplatten. Diese liegen auf lokalem, gemeinsamem oder verteiltem Storage.

Wichtig sind dabei:

Thema	Kerngedanke
Storage	Speicher für VMs, Disks, ISO-Dateien und Templates
Performance	IOPS, Latenz und Durchsatz beachten
Thin Provisioning	Spart Speicher, muss überwacht werden
Thick Provisioning	Reserviert Speicher sofort
Snapshots	Kurzfristige Absicherung bei Änderungen
Backups	Echte Wiederherstellung bei Datenverlust
RPO	Wie viele Daten dürfen verloren gehen?
RTO	Wie lange darf Wiederherstellung dauern?
Offsite	Sicherung außerhalb des Standorts
Immutable	Schutz vor Änderung und Löschung
Restore-Test	Prüft, ob Backup wirklich funktioniert

Für die IHK ist besonders wichtig:

Prüfungsrelevanter Punkt	Bedeutung
Snapshot vs. Backup	Snapshot ist kein Backup

Prüfungsrelevanter Punkt	Bedeutung
RAID vs. Backup	RAID ist kein Backup
Thin vs. Thick	Speicher dynamisch oder fest reserviert
RPO vs. RTO	Datenverlust vs. Ausfallzeit
Applikationskonsistenz	Wichtig bei Datenbanken und AD
Offsite/Immutable	Schutz vor Standortausfall und Ransomware
Restore-Test	Backup muss wiederherstellbar sein

Der nächste logische Schritt ist:

Cluster und Hochverfügbarkeit
