

Kapitel 5 - Massenspeicher

- 5.1 Massenspeicher allgemein
- 5.2 HDD
- 5.3 SSD
- 5.4 RAID
- 5.5 Hot Spare
- 5.6 JBOD
- 5.7 NAS
- 5.8 Optische Medien
- 5.9 Dateisysteme
- Datenschutz, Datensicherheit und Informationssicherheit: Prinzipien und Methoden

5.1 Massenspeicher allgemein

Definition

Massenspeicher dienen zur dauerhaften Speicherung großer Datenmengen.

Im Gegensatz zum Arbeitsspeicher behalten Massenspeicher ihre Daten auch ohne Stromversorgung.

Eigenschaften

- nichtflüchtiger Speicher
- dauerhaftes Speichern von Daten
- größere Speicherkapazität als RAM
- langsamer als Arbeitsspeicher

Beispiele

Massenspeicher	Beschreibung
HDD	magnetischer Massenspeicher
SSD	elektronischer Flash-Speicher
USB-Stick	mobiler Flash-Speicher
Speicherkarte	mobiler Flash-Speicher
Optische Medien	CD, DVD, Blu-ray
NAS	Netzwerkspeicher

Abgrenzung zu RAM

RAM	Massenspeicher
flüchtig	nichtflüchtig
sehr schnell	langsamer
für laufende Programme	für dauerhafte Daten
Datenverlust ohne Strom	Daten bleiben erhalten

Merksatz

Massenspeicher speichern Daten dauerhaft.
RAM speichert Daten nur vorübergehend.

Prüfungshinweis

In IHK-Aufgaben wird häufig zwischen **Arbeitsspeicher**, **Cache** und **Massenspeicher** unterschieden.

Typische Fehler:

- RAM mit Massenspeicher verwechseln.
- SSD und RAM gleichsetzen.
- Speichergröße und Geschwindigkeit nicht unterscheiden.

Quellen

- IT-Handbuch für Fachinformatiker

5.2 HDD

Definition

Eine **HDD** ist ein magnetischer Massenspeicher.

HDD steht für **Hard Disk Drive**.

Aufbau

Eine HDD besteht unter anderem aus:

- Magnetscheiben
 - Schreib-/Lesekopf
 - Motor
 - Controller
 - Gehäuse
-

Funktionsweise

Daten werden magnetisch auf rotierenden Scheiben gespeichert.

Der Schreib-/Lesekopf liest und schreibt die Daten auf den Magnetscheiben.

Eigenschaften

Eigenschaft	Beschreibung
Speicherart	magnetisch
Geschwindigkeit	langsamer als SSD
Kapazität	oft sehr groß
Preis pro GB	meist günstig
Geräusch	hörbar durch bewegliche Teile
Empfindlichkeit	empfindlich gegen Stöße

Vorteile

- große Speicherkapazität
 - günstiger Preis pro GB
 - gut für große Datenmengen
-

Nachteile

- mechanische Bauteile
 - langsamer als SSD
 - empfindlich gegen Erschütterungen
 - hörbare Betriebsgeräusche
-

Merksatz

Eine HDD speichert Daten magnetisch auf rotierenden Scheiben.

Prüfungshinweis

In IHK-Aufgaben wird häufig zwischen **HDD** und **SSD** unterschieden.

Typische Fehler:

- HDD und SSD gleichsetzen.
 - HDD als Flash-Speicher bezeichnen.
 - bewegliche Teile der HDD vergessen.
-

Quellen

- IT-Handbuch für Fachinformatiker

5.3 SSD

Definition

Eine **SSD** ist ein nichtflüchtiger Massenspeicher auf Basis von Flash-Speicher.

SSD steht für **Solid State Drive**.

Funktionsweise

Daten werden elektronisch in Speicherzellen gespeichert.

Eine SSD besitzt keine beweglichen Teile.

Eigenschaften

Eigenschaft	Beschreibung
Speicherart	Flash-Speicher
Geschwindigkeit	schneller als HDD
Geräusch	geräuschlos
Stoßempfindlichkeit	unempfindlicher als HDD
Preis pro GB	meist höher als HDD

Vorteile

- hohe Geschwindigkeit
 - kurze Zugriffszeiten
 - geräuschlos
 - stoßunempfindlich
 - geringer Stromverbrauch
-

Nachteile

- höherer Preis pro GB
 - begrenzte Schreibzyklen
 - Datenrettung oft schwieriger als bei HDD
-

Schnittstellen

Typische SSD-Schnittstellen:

- SATA
 - M.2
 - NVMe
 - PCIe
-

Merksatz

Eine SSD speichert Daten elektronisch und besitzt keine beweglichen Teile.

Prüfungshinweis

In IHK-Aufgaben wird häufig zwischen **HDD** und **SSD** unterschieden.

Typische Fehler:

- SSD als magnetischen Speicher bezeichnen.
 - SSD und RAM verwechseln.
 - M.2 und NVMe gleichsetzen.
 - SATA-SSD und NVMe-SSD nicht unterscheiden.
-

Quellen

- IT-Handbuch für Fachinformatiker

5.4 RAID

Definition

RAID steht für **Redundant Array of Independent Disks**.

RAID verbindet mehrere physische Laufwerke zu einem logischen Laufwerk.

Ziele

RAID kann verwendet werden für:

- höhere Ausfallsicherheit
- höhere Geschwindigkeit
- größere zusammenhängende Speicherkapazität

Wichtige RAID-Level

RAID-Level	Beschreibung
RAID 0	Striping ohne Redundanz
RAID 1	Spiegelung der Daten
RAID 5	Striping mit verteilter Parität
RAID 6	Striping mit doppelter verteilter Parität
RAID 10	Kombination aus RAID 1 und RAID 0

RAID 0

- Daten werden auf mehrere Laufwerke verteilt.
- hohe Geschwindigkeit
- keine Ausfallsicherheit

RAID 1

- Daten werden gespiegelt.
- hohe Ausfallsicherheit
- nutzbare Kapazität halbiert sich

RAID 5

- Daten und Paritätsinformationen werden verteilt gespeichert.
 - ein Laufwerk darf ausfallen.
 - mindestens 3 Laufwerke erforderlich
-

RAID 6

- wie RAID 5, aber mit doppelter Parität
 - zwei Laufwerke dürfen ausfallen.
 - mindestens 4 Laufwerke erforderlich
-

RAID 10

- Kombination aus Spiegelung und Striping
 - hohe Geschwindigkeit
 - hohe Ausfallsicherheit
 - mindestens 4 Laufwerke erforderlich
-

Merksatz

RAID erhöht die Verfügbarkeit, ersetzt aber kein Backup.

Prüfungshinweis

In IHK-Aufgaben wird häufig nach **Ausfallsicherheit**, **nutzbarer Kapazität** und **Mindestanzahl der Laufwerke** gefragt.

Typische Fehler:

- RAID als Backup bezeichnen.
 - RAID 0 als ausfallsicher ansehen.
 - Brutto- und Netto-Kapazität verwechseln.
 - Parität bei RAID 5 und RAID 6 nicht beachten.
-

Quellen

- IT-Handbuch für Fachinformatiker

5.5 Hot Spare

Definition

Ein **Hot Spare** ist ein Ersatzlaufwerk, das in einem RAID-System bereits eingebaut ist und automatisch genutzt werden kann, wenn ein Laufwerk ausfällt.

Aufgabe

Ein Hot Spare dient dazu, ein ausgefallenes Laufwerk automatisch zu ersetzen.

Dadurch kann der Wiederaufbau des RAID-Verbunds schneller beginnen.

Eigenschaften

- bereits im System eingebaut
 - normalerweise nicht aktiv genutzt
 - wird bei Laufwerksausfall automatisch aktiviert
 - unterstützt den schnellen Wiederaufbau des RAID
-

Beispiel

In einem RAID 5 fällt eine Festplatte aus.

Das Hot-Spare-Laufwerk übernimmt automatisch die Rolle der ausgefallenen Festplatte.

Der RAID-Verbund wird anschließend wiederhergestellt.

Vorteile

- schnellere Reaktion bei Laufwerksausfall
 - weniger manuelles Eingreifen
 - höhere Verfügbarkeit
 - sinnvoll bei Servern und NAS-Systemen
-

Nachteile

- zusätzliche Festplatte erforderlich
 - verursacht zusätzliche Kosten
 - Speicherplatz des Hot Spare wird im Normalbetrieb nicht genutzt
-

Merksatz

Ein Hot Spare ist ein eingebautes Ersatzlaufwerk für den automatischen Austausch bei einem Laufwerksausfall.

Prüfungshinweis

Ein Hot Spare erhöht die Verfügbarkeit, ersetzt aber kein Backup.

Typische Fehler:

- Hot Spare als zusätzlichen Speicherplatz zählen.
 - Hot Spare mit Backup verwechseln.
 - Hot Spare mit RAID 1 gleichsetzen.
-

Quellen

- IT-Handbuch für Fachinformatiker

5.6 JBOD

Definition

JBOD steht für **Just a Bunch of Disks**.

Bei JBOD werden mehrere physische Laufwerke ohne RAID-Funktion zusammengefasst oder einzeln genutzt.

Eigenschaften

- keine Spiegelung
- keine Parität
- keine automatische Ausfallsicherheit
- Laufwerke können unterschiedliche Größen haben
- einfache Nutzung mehrerer Datenträger

Unterschied zu RAID

JBOD	RAID
keine Redundanz	je nach RAID-Level mit Redundanz
keine Parität	RAID 5/6 nutzen Parität
keine Leistungssteigerung durch Striping	RAID 0 nutzt Striping
einfache Laufwerksverwaltung	strukturierter Laufwerksverbund

Vorteile

- einfache Einrichtung
- unterschiedliche Festplattengrößen möglich
- gesamte Kapazität kann genutzt werden
- kein spezieller RAID-Aufbau notwendig

Nachteile

- keine Ausfallsicherheit
- kein Schutz bei Festplattenausfall
- keine Leistungssteigerung wie bei RAID 0
- kein Ersatz für Backup

Merksatz

JBOD ist kein RAID und bietet keine automatische Ausfallsicherheit.

Prüfungshinweis

In IHK-Aufgaben wird JBOD häufig von RAID abgegrenzt.

Typische Fehler:

- JBOD als RAID-Level bezeichnen.
 - JBOD als ausfallsicher ansehen.
 - JBOD mit RAID 0 verwechseln.
 - JBOD als Backup betrachten.
-

Quellen

- IT-Handbuch für Fachinformatiker

5.7 NAS

5.7 NAS

Definition

NAS steht für **Network Attached Storage**.

Ein NAS ist ein Speichergerät, das über das Netzwerk erreichbar ist.

Aufgabe

Ein NAS stellt Speicherplatz zentral im Netzwerk bereit.

Mehrere Benutzer oder Geräte können auf die gespeicherten Daten zugreifen.

Eigenschaften

- zentraler Netzwerkspeicher
 - Zugriff über LAN oder WLAN
 - häufig mit mehreren Festplatten
 - oft mit RAID-Unterstützung
 - Benutzer- und Rechteverwaltung möglich
-

Typische Einsatzbereiche

- Dateifreigaben
 - Backups
 - Medienserver
 - gemeinsame Projektordner
 - zentrale Datenspeicherung
-

Vorteile

- zentrale Speicherung
 - Zugriff von mehreren Geräten
 - einfache Erweiterbarkeit
 - Benutzerrechte können verwaltet werden
 - geeignet für Backup-Ziele
-

Nachteile

- abhängig vom Netzwerk
 - bei falscher Konfiguration Sicherheitsrisiko
 - kein Ersatz für ein zusätzliches Backup
 - bei Ausfall des NAS kein Zugriff auf die Daten
-

Merksatz

Ein NAS ist ein zentraler Speicher im Netzwerk.

Prüfungshinweis

Ein NAS ist kein Backup an sich.

Ein NAS kann aber als Ziel für Backups verwendet werden.

Typische Fehler:

- NAS mit RAID gleichsetzen.
 - NAS als vollständiges Backup ansehen.
 - Netzwerkverbindung und Zugriffsrechte nicht beachten.
-

Quellen

- IT-Handbuch für Fachinformatiker

5.8 Optische Medien

Definition

Optische Medien sind Massenspeicher, bei denen Daten mithilfe von Laserlicht gelesen oder geschrieben werden.

Wichtige optische Medien

Medium	Bedeutung
CD	Compact Disc
DVD	Digital Versatile Disc
Blu-ray	optisches Medium mit hoher Speicherkapazität

Funktionsweise

Daten werden auf einer reflektierenden Schicht gespeichert.

Ein Laser liest die gespeicherten Informationen aus.

Typische Varianten

Variante	Bedeutung
ROM	nur lesbar
R	einmal beschreibbar
RW	wiederbeschreibbar

Beispiele

- CD-ROM
- CD-R
- CD-RW
- DVD-ROM
- DVD-R
- DVD-RW
- Blu-ray Disc

Vorteile

- günstig
 - einfach zu transportieren
 - geeignet zur Archivierung kleiner Datenmengen
-

Nachteile

- geringe Geschwindigkeit
 - begrenzte Speicherkapazität
 - empfindlich gegen Kratzer
 - heute seltener verwendet
-

Merksatz

Optische Medien werden mit Laserlicht gelesen und beschrieben.

Prüfungshinweis

In IHK-Aufgaben wird häufig zwischen **ROM**, **R** und **RW** unterschieden.

Typische Fehler:

- ROM als beschreibbar einordnen.
 - R und RW verwechseln.
 - optische Medien mit magnetischen Medien verwechseln.
-

Quellen

- IT-Handbuch für Fachinformatiker

5.9 Dateisysteme

Definition

Ein **Dateisystem** legt fest, wie Daten auf einem Datenträger gespeichert, organisiert und wiedergefunden werden.

Aufgabe

Ein Dateisystem verwaltet unter anderem:

- Dateien
- Ordner
- Dateinamen
- Speicherorte
- Zugriffsrechte
- freie und belegte Speicherbereiche

Wichtige Dateisysteme

Dateisystem	Typische Verwendung
FAT32	USB-Sticks, ältere Systeme
exFAT	USB-Sticks, Speicherkarten
NTFS	Windows-Systeme
ext4	Linux-Systeme
APFS	macOS
HFS+	ältere macOS-Systeme

FAT32

- sehr kompatibel
- unterstützt viele Geräte
- maximale Dateigröße: 4 GB

exFAT

- geeignet für große Dateien
- häufig bei USB-Sticks und Speicherkarten
- gute Kompatibilität zwischen Windows und macOS

NTFS

- Standard-Dateisystem von Windows
 - unterstützt Rechteverwaltung
 - geeignet für interne Laufwerke
-

ext4

- häufiges Dateisystem unter Linux
 - stabil und leistungsfähig
-

APFS

- modernes Dateisystem von macOS
 - optimiert für SSDs
-

Merksatz

Das Dateisystem bestimmt, wie Dateien auf einem Datenträger gespeichert und verwaltet werden.

Prüfungshinweis

In IHK-Aufgaben wird häufig nach dem passenden Dateisystem für einen bestimmten Einsatzzweck gefragt.

Typische Fehler:

- FAT32 für Dateien größer als 4 GB wählen.
 - Dateisystem und Datenträger verwechseln.
 - NTFS als Standard-Dateisystem für Linux einordnen.
 - exFAT und FAT32 verwechseln.
-

Quellen

- IT-Handbuch für Fachinformatiker

Datenschutz, Datensicherheit und Informationssicherheit: Prinzipien und Methoden

Datenschutz Informationssicherheit Datensicherheit

Datenschutz vs Datensicherheit

Datenschutz Datensicherheit

Datenschutz vs Datensicherheit

Datenschutz Schutz von Personen Datensicherheit Schutz von Daten

Datenschutz

Datenschutz -Schutz von Personen

- ☐ Rechtlich/organisatorisches Thema
- ☐ Schutz von personenbezogenen Daten
- ☐ Schutz des allgemeinen Persönlichkeitsrechtes
- ☐ Stichworte: Datenschutz-Grundverordnung DSGVO und Bundesdatenschutz-Gesetz BDSG

Schutzziele der Informationssicherheit

CIA

Schutzziele der Informationssicherheit

Schutz von Informationen vor

- unbefugtem Zugriff
- Manipulation
- Verlust.

Umfasst verschiedene

- Maßnahmen und Konzepte,
- um Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu gewährleisten.

Grundprinzipien (CIA)

1. Vertraulichkeit (Confidentiality)
2. Integrität (Integrity)

3. Verfügbarkeit (Availability)

Grundprinzipien (CIA)

1. Vertraulichkeit (Confidentiality)

Nur autorisierte Personen dürfen auf Informationen zugreifen.

Maßnahmen: Verschlüsselung, Zugriffskontrollen, VPNs

2. Integrität (Integrity)

Informationen dürfen nicht unbemerkt verändert oder manipuliert werden.

Maßnahmen: Hashing, digitale Signaturen, Prüfmechanismen

3. Verfügbarkeit (Availability)

Informationen müssen für berechtigte Nutzer jederzeit zugänglich sein.

Maßnahmen: Backups, Redundanz, DDoSSchutz

Gefahren für Informationssicherheit

Hackerangriffe

- z. B. Phishing, Malware, Ransomware, Viren

Menschliche Fehler

- z. B. schwache Passwörter, versehentliches Löschen

Technische Fehler

- z. B. Hardware-Ausfälle, Software-Bugs

Naturkatastrophen

- z. B. Feuer, Überschwemmung

Datensicherheit

Schutz vor

Gewährleistung von



Unbefugter Zugriff Dritter,



Manipulation,

- ☐ Verlust der Daten
- ☐ Vertraulichkeit,
- ☐ Integrität,
- ☐ Verfügbarkeit von Daten

Datenschutz vs Datensicherheit vs Informationssicherheit

Datenschutz Schutz von Personen

- ☐ Regelwerk • Rechtlich/organisatorisches Thema
- ☐ Schutz von personenbezogenen Daten
- ☐ Schutz des allgemeinen Persönlichkeitsrechtes
- ☐ Stichworte: Datenschutz-Grundverordnung DSGVO und Bundesdatenschutz-Gesetz BDSG

Datensicherheit Schutz von Daten

- ☐ Maßnahmen • Technisches Thema
- ☐ Sichere Verarbeitung von Daten
- ☐ Schutz vor : Unbefugter Zugriff Dritter, Manipulation, Verlust der Daten
- ☐ Gewährleistung von: Vertraulichkeit, Integrität, Verfügbarkeit von Daten

Informationssicherheit

- ☐ Grundprinzipien
- ☐ Vertraulichkeit
- ☐ Integrität
- ☐ Verfügbarkeit

Datenschutz

'Du darfst diese Daten nur unter bestimmten Bedingungen nutzen'

Datensicherheit

'Wenn du sie nutzt, musst du sie schützen'

Schutzziele

'Was bedeutet schützen'

Datensicherheit

Aspekt: Schutz vor Verlust von Daten

Datensicherung

Prozess des Sicherns von Daten

Ziel

- Daten im Falle des Verlusts wiederherstellen können

Redundanz

- Daten werden mehrfach erstellt
- Begriffe: Sicherungskopie/ Backup

Speicherung der Kopien

- Online vs offline
- Unterschiedliche Medien

Räumliche Trennung von Backup und Daten

Ziel: Datensicherheit/ Ausfallsicherheit erhöhen

Georedundanz

Offsite-Backup

- Backup an einem anderen Standort

Onsite-Backup

- Backup am gleichen Standort

Räumliche Entfernung von der EDV-Anlage

Räumliche Entfernung von der EDV-Anlage

Räumliche Entfernung von der EDV-Anlage

Lokal (gleicher Standort)

Vorteile:

- Sehr schnell verfügbar
- Einfach umzusetzen

Nachteile:

- Kein Schutz bei Brand, Wasser, Diebstahl
- Beide Daten können gleichzeitig verloren gehen

Standortnah (gleiches Gebäude / Gelände)

Vorteile:

- Etwas mehr Sicherheit als lokal · Schneller Zugriff bleibt erhalten

Nachteile:

- Risiken wie Feuer oder Stromausfall betreffen oft trotzdem alles

Remote / Cloud

Vorteile:

- Automatisierbar
- Geografisch weit entfernt
- Oft redundant gespeichert

Nachteile:

- Abhängigkeit vom Internet
- Laufende Kosten
- Datenschutz beachten

Offsite bzw AirGapped Backup (physisch getrennt)

Vorteile:

- Sehr hoher Schutz vor Hackerangriffen und Ransomware
- Kann nicht übers Netzwerk kompromittiert werden
- Schutz vor lokalen Katastrophen

Nachteile:

- Manuelles Handling nötig
- Organisation aufwendig
- Wiederherstellung langsamer

Räumliche Entfernung von der EDV-Anlage: Sicherheitsniveau

Sicherheits- niveau	Typisch	Schützt vor	Schützt nicht vor / Risiken	Besonderheiten / Beispiel
Lokal gespeicherte Backups (z. B. USB-Platte am selben PC)	• versehentlichem Löschen • einfachen Softwarefehlern	• Hardwaredefekt (wenn beide betroffen sind) • Diebstahl / Brand / Wasser • Ransomware	Nur Minimallösung, kein echtes Sicherheitskonzept	Niedrig

Sicherheits- niveau	Typisch	Schützt vor	Schützt nicht vor / Risiken	Besonderheiten / Beispiel
Standortnahes Backup (z. B. NAS im selben Gebäude)	• einzelnen Geräteausfällen	• größere Schäden (Feuer, Stromausfall) • Angriffe im Netzwerk	NAS von Synology im Serverraum	Mittel
Remote/ Cloud-Backups	• lokale Katastrophen • Hardwareausfälle	• Ransomware (bei erreichbaren Backups) • Fehlkonfiguration • Internetabhängigkeit	Microsoft Azure oder Amazon Web Services	Hoch
Offsite + Air-Gap	• Ransomware • gezielten Angriffen • Manipulation von Backups	-	physisch getrenntes Backup Beispiel: Cloud + externe Platte im Safe	Sehr hoch
3-2-1-Regel (3 Kopien, 2 Medien, 1 offsite)	• nahezu allen realistischen Ausfallszenarien	-	Ergänzt durch: Air-Gap, Verschlüsselung, Wiederherstellungstechniken	Maximal (Best Practice)

Backup Varianten, Methoden und Strategien

Prozess der Sicherung

Wie werden die Daten gesichert

Wie werden die Ressourcen eingesetzt

- Speicherkapazität
- Dauer der Datensicherung
- Dauer der Wiederherstellung

Prozess: Backup-Varianten

Speicherabbild- Sicherung	Ein Abbild des gesamten Systems wird erstellt Vorteil: Nur 1 Datei Nachteil: Zeitaufwand + hoher Speicheraufwand
Komplett-/ Vollsicherung	Alle Daten werden gesichert
Komplett-/ Vollsicherung	Nachteil: Zeitaufwand + hoher Speicheraufwand
Differenzielles Backup	Jeden Tag: Änderungen seit Vollsicherung

Inkrementelles Backup

Tag 1 nach Vollsicherung: Änderungen seit Vollsicherung

Später: Änderungen seit letztem Backup

Allgemein: Änderungen seit letztem Backup

Backup Methoden

Differenziell

Step 1: Vollsicherung

Differenziell

Backups werden Tag für Tag größer

- Mit jeder Teilsicherung werden die vorherigen Daten erneut mit gespeichert

Vorteil

- Deutlich schneller als Vollsicherung

Nachteil

- Dateien, die nach Vollsicherung nur einmal geändert werden, werden jedesmal wieder gesichert
- Alle Änderungen seit dem letzten vollständigen Backup werden gesichert
- Benötigt mehr Speicherplatz

Wiederherstellung

- Aus Vollbackup und 1 Datei des entsprechenden Tages

Inkrementell

Unterschied

- mit jeder Teilsicherung werden nur die Daten gesichert, die seit der letzten Sicherung (egal, ob Voll- oder Teilsicherung) erstellt oder verändert wurden

Verknüpfung

- einzelne Datensätze sind miteinander verknüpft

Vorteil

- geringer Speicherbedarf
- gehen schnell

Nachteil

- Wiederherstellung aus Vollsicherung und allen nachfolgenden inkrementellen Sicherungen wird komplexer

Änderungsverfolgung

Change Detection

Verfahren

Verfahren	Fachbegriff
Archivbit nutzen	Archive Bit Tracking
Zeitstempel vergleichen	Timestamp-based Change Detection
Prüfsummen vergleichen	Checksum-based Detection
Dateisystem protokolliert Änderungen	Journal-based Change Detection

Archiv-Bit

Dateimerkmal von Windows um zu markieren, ob eine Datei seit der letzten Sicherung verändert wurde.

Es hilft Backup-Programmen zu entscheiden, welche Dateien gesichert werden müssen.

Archiv-Bit

Archiv-Bit

Vollbackup

- sichert alle Daten
- Danach Archivbit wieder auf 0

Inkrementelles Backup

- Sichert nur Daten mit Archivbit = 1
- Danach: Archivbit wieder auf 0
- Folge: Jedes inkrementelle Backup hat nur Änderungen seit letztem Backup

Differenzielles Backup

- Sichert nur Daten mit Archivbit = 1
- Danach: Archivbit wird NICHT auf 0 gesetzt
- Folge: Alle Änderungen seit letztem Vollbackup bleiben markiert

Archiv-Bit

PowerShell

```
- Get-Item "C:\Test\datei.txt" | Select-Object Name, Attributes · (Get-Item "C:\Test\datei.txt").Attributes += "Archive"
```

- (Get-Item "C:\Test\datei.txt").Attributes -= "Archive"

CMD

- attrib C:\Test\datei.txt · attrib -A C:\Test\datei.txt · attrib +A C:\Test\datei.txt

Zeitstempel

Linux

- mtime → Inhalt geändert
- ctime → Metadaten/Rechte geändert
- atime → Zugriff auf Datei

Beispiel

- ls -l
- stat datei

Windows

- (Get-Item "C:\Test\datei.txt").LastWriteTime

Prüfsummen/ Hashes/ Hashwerte

Windows

```
- Get-FileHash C:\Test\datei.txt · Get-FileHash C:\Test\datei.txt -Algorithm MD5
```

Dateien vergleichen

- \$hash1 = (Get-FileHash C:\Test\datei.txt).Hash · \$hash2 = (Get-FileHash C:\Test\datei2.txt).Hash · \$hash1 -eq \$hash2

Prüfsummen/ Hashes/ Hashwerte

Linux

- sha256sum datei.txt
- md5sum datei.txt
- sha256sum a.txt b.txt

Beispiel

```
- hash1=$(sha256sum a.txt) · hash2=$(sha256sum a.txt) · [ "$hash1" = "$hash2" ] && echo "gleich" || echo "ungleich"
```

Funktion schreiben in Datei ~/.bashrc

```
sha256cmp() { hash1=$(sha256sum "$1" | cut -d' ' -f1) hash2=$(sha256sum "$2" | cut -d' ' -f1) [ "$hash1" = "$hash2" ] && echo "gleich" || echo "ungleich" }
```

Backup-Strategien

Backup-Strategien

3-2-1 Backup Regel

Großvater-Vater-Sohn

First in, First out (Fifo)

Backup-Strategien: 3-2-1 Backup Regel

Exemplare

Bewahre mindestens 3 Kopien Deiner Unternehmensdaten auf

Die goldene 3-2-1-1-0 Backup-Regel

Datensicherung auf 2 verschiedenen Medien Mindestens eine Kopie an einem externen Ort speichern

Backup-Strategien: Großvater-Vater-Sohn

TAG: Sohn

- Tägliche Sicherung (inkrementell/ differenziell)
- 4 bis 5 Bänder

WOCHE: Vater

- Am Ende jeder Woche
- Vollständiges Backup
- Löschung aller vorangegangenen Backups

MONAT: Großvater

- Nach 4 Wochen:
- Neues Vollständiges Backup
- Löschung der vier wöchentlichen Sicherungen

Backup-Strategien: Großvater-Vater-Sohn

Backup-Strategien: Großvater-Vater-Sohn

Backup-Strategien: Großvater-Vater-Sohn

Backup-Strategien: Fifo

neue oder geänderte Dateien überschreiben die ältesten

Bsp: 14 Tage Backup

an Tag 15 wird Backup von Tag 1 überschrieben

Recovery Point Objective

Wie lange dürfen die neuesten Backups maximal zurückliegen?

Beispiel:

- RPO = 1 Tag : Wenn heute die Platte ausfällt, sind maximal Daten von gestern weg
- RPO = 1 Stunde : Wenn heute ein Fehler passiert, sind maximal die letzten 60 Minuten Arbeit weg
- RPO = 1 Woche : Datenverlust von bis zu 7 Tagen

RPO bestimmt, wie oft Backup gemacht wird

- RPO 1 Tag → täglich backupen
- RPO 1 Stunde → stündlich backupen
- RPO 1 Woche → wöchentlich backupen

Quellen

- Dokument: Datenschutz, Datensicherheit und Informationssicherheit: Prinzipien und Methoden
- ID: 136