Systemtechnik

- Datenverfügbarkeit - RAID
- Datenschutz, Datensicherheit und Informationssicherheit: Prinzipien und Methoden
- Testfragen
    - Datenschutz, Datensicherheit, Datenverfügbarkeit

Datenverfügbarkeit - RAID

Datenverfügbarkeit

Verwaltung von Daten

Datenschutz vs Datensicherheit vs Informationssicherheit

Datenschutz

Datensicherheit

Informationssicherheit

Datenschutz vs Datensicherheit (485)

Datenschutz -Schutz von Personen

- Schutz von personenbezogenen Daten
- Schutz des allgemeinen Persönlichkeitsrechtes
- Stichworte: Datenschutz-Grundverordnung DSGVO und Bundesdatenschutz-Gesetz BDSG

Datensicherheit -Schutz von Daten

Informationssicherheit -Schutz von Informationen

Datenschutz vs Datensicherheit (485)

Datenschutz -Schutz von Personen

- Schutz von personenbezogenen Daten
- Schutz des allgemeinen Persönlichkeitsrechtes
- Stichworte: Datenschutz-Grundverordnung DSVGO und Bundesdatenschutz-Gesetz BDSG

Datensicherheit -Schutz von Daten

Schutz vor :

- Unbefugter Zugriff Dritter
- Manipulation
- Verlust der Daten

Informationssicherheit -Schutz von Informationen

Datenschutz vs Datensicherheit (485)

Datenschutz -Schutz von Personen

- Schutz von personenbezogenen Daten
- Schutz des allgemeinen Persönlichkeitsrechtes
- Stichworte: Datenschutz-Grundverordnung DSVGO und Bundesdatenschutz-Gesetz BDSG

Informationssicherheit -Schutz von Informationen

- Gewährleistung von:
- Vertraulichkeit
- Integrität
- Verfügbarkeit von Daten

Datensicherheit -Schutz von Daten

- Schutz vor :
- Unbefugter Zugriff Dritter
- Manipulation
- Verlust der Daten

Datenverfügbarkeit / Data Availibility

Produkte und Dienste, die sicherstellen, dass

- Daten bis zu einem vorgegebenen Leistungsniveau
- unter allen Umständen (von normal bis katastrophal)
- verfügbar bleiben

Datensicherheit vs. Datenverfügbarkeit

Datensicherheit vs. Datenverfügbarkeit

RAID

RAID Buch S. 362-365

RAID -Redundant Array of Independent Disks

Mehrere Festplatten werden zu einer logischen Einheit zusammengefasst

Ist für den User wie eine Festplatte ansprechbar Werden häufig auf Servern oder NAS eingesetzt

RAID -Redundant Array of Independent Disks

Wofür wird RAID eingesetzt

RAID 0

Steigerung der Schreib- und LesezugriffeRAID 1

RAID 1

Verbesserung der Datensicherheit Daten sollen ständig abrufbar sein

RAID -Redundant Array of Independent Disks

Wofür wird RAID eingesetzt

RAID 0

Steigerung der Schreib- und LesezugriffeRAID 1

RAID 1

Verbesserung der Datensicherheit Daten sollen ständig abrufbar sein

RAID -Redundant Array of Independent Disks

RAID -Redundant Array of Independent Disks

!!!RAID ersetzt kein Backup!!!

RAID -Redundant Array of Independent Disks

!!!RAID ersetzt kein Backup!!!

RAID -Redundant Array of Independent Disks

'RAID' erstmals 1988 Universtity of Berkley

Frage damals:

- Wie kann man kostengünstige PC-Festplatten zu einem Verbund zusammenschließen und
- als ein großes logisches Laufwerk betreiben

Problem:

- Höheres Ausfallrisiko

Lösung:

- Konzept der redundanten Speicherung

RAID -Redundant Array of Independent Disks

Folgezeit

- Standardisierung von RAID

- Einsatz in Serverumgebung rückte in Vordergrund

Verschiebung des Einsatzgrundes

- Kostenersparnis: rückte zunehmend in Hintergrund

Neuer Hauptaspekt

- problemloser Austausch von Festplatten im laufenden Betrieb
- 'Redundant Array of Indepentdet Disks'
- 'redundante Anordnung unabhängiger Festplatten'

RAID -Verhältnis zwischen Schutzniveau und Leistung

Unterschiede bei RAID: Umsetzung und Level

Software/ Hardware Level

Unterschiede bei RAID: Umsetzung und Level

Software/ Hardware

Unterschiede bei RAID: Umsetzung und Level

Software

- Host-based-RAID
- Verwaltung der Speichermedien direkt auf der CPU des Hosts
- Möglichkeiten auf gängigen OS implementiert
- Vorteil
- deutlich schneller und kostengünstiger eingerichtet
- Nachteil
- hoche CPU-Auslastung
- schlechtere Performance

Hardware

- RAID-Controller
- übernimmt Organisation der einzelnen Speichermedien
- im Computer selbst als Erweiterungskarte
- Auf dem Mainboard selbst
- In einem DiskArray ('Plattensubsystem') bsp. NAS
- Hohe Performance
- hohe Datentransferraten

Software für Windows und Mac

Windows

- → 'Speicherplatz verwalten'
- → 'Neuen Pool und Speicherplatz erstellen'

MacOS

- → Festplattendienstprogramm
- → Ablage
- → RAID-Assistent

Software vs Hardware

	Software-RAID	Hardware-RAID
Kosten	niedrig	hoch
CPU-Auslastung (Host)	hoch	niedrig
Performance	niedrig	hoch
Plattformunabhängigkeit	nein	ja
Betriebssystemabhängigkeit	ja	ja

Unterschiede bei RAID: Umsetzung und Level

Level

RAID-Level

Level

- Art, wie Festplatten in einem RAID kombiniert werden

Vorsicht

- Level-Nummern stehen in keiner Verbindung
- kennzeichnen lediglich verschiedene Ansätze für Aufbau und Funktion des RAID

RAID-Level

Mehrere Stufen

- Standard
- RAID 0, RAID 1, RAID 5, RAID 6
- Verschachtelt
- RAID 10 (RAID 1 + RAID 0)
- RAID 01

Leistungs -und Redundanzanforderungen

- RAID 0 am schnellsten
- RAID 1 am zuverlässigsten
- RAID 5 gute Kombination

RAID-Level 0

Striping

- Daten werden im 'Reißverschluss -Verfahren' gespeichert

Vorteil

- Erhöhung der Zugriffsgeschwindigkeit
- Erhöhung Lesegeschwindigkeit

Nachteil

- Bei Ausfall einer Festplatte sind Daten nicht rekonstruierbar

RAID-Level 0

Striping

- Daten werden im 'Reißverschluss -Verfahren' gespeichert

Vorteil

- Erhöhung der Zugriffsgeschwindigkeit
- Erhöhung Lesegeschwindigkeit

Nachteil

- Bei Ausfall einer Festplatte sind Daten nicht rekonstruierbar

RAID-Level 1

RAID 1 -min. 2 Festplatten

- Daten Mirroring (Spiegelung)
- Jeder Datenblock wird auf 2 Festplatten gespeichert

Vorteil

- Redundanz
- Evt bessere Lesegeschwindigkeit

Nachteil

- Schreibgeschwindigkeit genauso schnell oder langsamer wie bei Einzellaufwerk
- Festplattenredundanz

RAID-Level 5

RAID 5 -min. 3 Festplatten

- Kompromiss aus Performanz (Level 0) und Datensicherheit (Level 1)
- Durch Hinzufügen von Paritätsinformationen Möglichkeit der Wiederherstellung von Daten bei Ausfall einer Festplatte

Vorteil

- Hohe Fehlertoleranz
- höhere Lesegeschwindigkeit entsprechend Anzahl der Platten

Nachteil

- Schreibintensive Arbeiten werden durch Berechung der Parität weniger effizient

Paritätsinformationen

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

Paritätsinformationen

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

Ungerade Zahl 1 → 1

Paritätsinformationen

A	B	A XOR B
0	0	0
0	1	1

A	B	A XOR B
1	0	1
1	1	0

Paritätsinformationen

Platte 1	Platte 2	Platte 3	Parität
0	1	1	
1	0	0	
1	1	0	
1	1	0	

Paritätsinformationen

Platte 1	Platte 2	Platte 3	Parität
0	1	1	0
1	0	0	1
1	1	0	0
1	1	0	0

Paritätsinformationen

Platte 1	Platte 2	Platte 3	Parität
0	1	1	0
1	0	0	1
1	1	0	0
1	1	0	0

Paritätsinformationen

Platte 1	Platte 2	Platte 3	Parität
0	1	1	0
1	0	0	1
1	1	0	0
1	1	0	0

Paritätsinformationen: Entferne Platte 2 (CRASH)

Platte 1	Platte 3	Parität
0	1	0
1	0	1
1	0	0
1	0	0

Paritätsinformationen: Entferne Platte 2 (CRASH)

Platte 1	Platte 3	Parität
0	1	0
1	0	1
1	0	0
1	0	0

Paritätsinformationen: Entferne Platte 2 (CRASH)

Platte 1	Platte 3	Parität
0	1	0
1	0	1
1	0	0
1	0	0

Platte	2
1	
0	
1	
1	

RAID-Level

RAID 6 -min. 4 Festplatten

- ähnlich RAID 5
- 2 Paritätsinformationen
- Verlust von 2 Laufwerken verkraftbar

Nachteil

- noch rechenintensiver als RAID 5

Vorteil

- Hohe Fehlertoleranz
- höhere Lesegeschwindigkeit

Risiko von Datenverlust minimiert

RAID-Level

RAID 10 -Strip of Mirrors

- Verbund von RAID 0 …
- … über mehrere RAID 1
- Benötigt mindestens 4 Festplatten
- Auf jeden Fall gerade Anzahl

Vorteil

- Schnelle Datenrekonstruktion nach einem Plattenausfall …
- … da nur ein Teil der Daten rekonstruiert werden muss

Nachteil

- Nur 50% der Festplattenkapazität

Raid 10, weil

- zuerst Spiegelung von Datum 1
- dann Striping von Datum 2 mit anschließender Spiegelung

RAID 1+0

RAID-Level

RAID 01 -Mirror of Stripes

- RAID 1 …
- … über mehrere RAID 0
- Benötigt mindestens 4 Festplatten

Vorteil

- Schnelle Datenrekonstruktion nach einem Plattenausfall …
- … da nur ein Teil der Daten rekonstruiert werden muss

Nutzbares Volumen

- 50% der Festplattenkapazität

RAID 01, weil

- zuerst werden Daten 1 und 2 gestriped
- anschließend gespiegelt

RAID O+1

Übungen RAID

Übung 1

Ein RAID-5 ist bitweise XOR-Verknüpft.

Welche Bit müssen in die fehlenden Stellen eingetragen werden?

Übung 1

Ein RAID-5 ist bitweise XOR-Verknüpft.

Welche Bit müssen in die fehlenden Stellen eingetragen werden?

Übung 2

Eine zusammenhängende Datei wird aufgeteilt in die Datenpakete A-E auf einem RAID aus 5 Laufwerke gespeichert.

Wie werden die Datenpakete auf die Laufwerke verteilt? Verbinde

- gespiegelte Platten mit einer Linie mit der Beschriftung mirror ,
- verbinde gekoppelte Platten mit einer Linie mit der Beschriftung stripe ,
- Benenne Paritäten mit P P und
- streiche nicht genutzte Platten durch.

RAID 1

RAID 0+1

RAID 10

RAID 5

RAID 6

RAID(n,m) oder RAID n+m

RAID(n,m)

Neuere Bezeichnung von RAID-Systemen

Es werden nicht mehr RAID Level verwendet.

Stattdessen:

- n = Anzahl der benutzten Platten
- m = Anzahl der Parity-Platten

RAID(n,m) Beispiel RAID (5,2)

Fünf Platten im Verbund

Zwei Platten dürfen maximal ausfallen

→ entspricht RAID 6 mit fünf Platten

Leserate, Schreibrate, Gesamt-Speicherkapazität

Leserate (Datendurchsatzrate)

Schreibrate gesamt

GesamtSpeicherkapazität

- n x Leserate Einzelplatte
- (n -m) x Schreibrate Einzelplatte
- (n -m) x Einzelkapazität

Beispiel: Leserate, Schreibrate, Gesamt-Speicherkapazität

RAID 5

Gesamtkapazität

Datendurchsatz

4 Platten

je 1 TB Kapazität

n - m → 3 TB

Platte 4 für Parität

Lesen: 4 mal so groß wie bei Einzelplatte

Schreiben: 3 mal so groß wie bei Einzelplatte

Hot Spare und Hot Swapping

Hot-Spare-Platten + Hot-Swapping

Mehr Festplatten als vom RAID benötigt werden angeschlossen

- Festplatten werden in Reserve (spare) gehalten
- Diese wird normalerweise nicht verwendet

RAID-Controller erkennt Defekt einer Platte:

- Reserve-Platte wird in im laufenden Betrieb (hot) RAID-Verbund integriert
- Fehlende Daten werden aus vorhandenen Daten berechnet
- Diese Daten werden auf Reserve-Festplatte geschrieben

JBOD und NRAID vs RAID

JBOD

- Just a Bunch of Disks ('nur ein Haufen Platten')

NRAID

- NotRAID

JBOD und NRAID

Zusammenschaltungen (Concatenations) von mehreren Festplatten

Kein Sicherheitsgewinn, da keine Redundanz

Kein Geschwindigkeitsgewinn -Daten werden einfach in Reihe geschrieben

RAID -Verhältnis zwischen Schutzniveau und Leistung

RAID-Level	Mindestanzahl Platten	Max. Ausfall ohne Datenverlust	Bedingung	Ausfallwahrscheinlichkeit (vereinfacht)
RAID 0	2	0	keine Redundanz	Sehr hoch (jede Platte kritisch)
RAID 1	2	n-1	solange 1 Platte lebt	Sehr gering
RAID 5	3	1	egal welche Platte	Mittel
RAID 6	4	2	egal welche Platten	Gering
RAID 10	4	1 bis n/2	je 1 pro Spiegelpaar	Sehr gering
RAID 01	4	1 (meist)	abhängig von Gruppe	Höher als RAID 10

Links

RAID-Level	Mindestanzahl Platten	Nettokapazität (bei N Platten gleicher Größe)	Erklärung
2	N × Größe	Volle Kapazität, keine Redundanz	RAID 0
2	1 × Größe	Spiegelung, nur eine Platte nutzbar	RAID 1
3	(N - 1) × Größe	Eine Platte für Parität	RAID 5
4	(N - 2) × Größe	Zwei Platten für Parität	RAID 6
4	(N / 2) × Größe	Spiegelung + Striping	RAID 10
4	(N / 2) × Größe	Striping + Spiegelung	RAID 01

Links

https://www.gservon.de/erklaerung-und-berechnung-raid-0-1-5-6-und-10/

Quellen

- Dokument: Datenverfügbarkeit_RAID
- ID: 137

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 DSVGO 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, Wiederherstellungstests	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 mir 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\a.txt).Hash · $hash2 = (Get-FileHash C:\Test\b.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 goldene3-2-1-1-0Backup-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

Testfragen

Testfragen

Datenschutz, Datensicherheit, Datenverfügbarkeit

1. **Was bedeutet Datenschutz?**

Antwort anzeigen

Datenschutz bedeutet Schutz von Personen bzw. personenbezogenen Daten. Dazu gehört auch der Schutz des allgemeinen Persönlichkeitsrechts.

2. **Was bedeutet Datensicherheit?**

Antwort anzeigen

Datensicherheit bedeutet Schutz von Daten vor unbefugtem Zugriff, Manipulation und Verlust.

3. **Was bedeutet Informationssicherheit?**

Antwort anzeigen

Informationssicherheit schützt Informationen und stellt Vertraulichkeit, Integrität und Verfügbarkeit sicher.

4. **Wofür steht CIA in der Informationssicherheit?**

Antwort anzeigen

CIA steht für:

- Confidentiality = Vertraulichkeit
- Integrity = Integrität
- Availability = Verfügbarkeit

5. **Was bedeutet Vertraulichkeit?**

Antwort anzeigen

Nur autorisierte Personen dürfen auf Informationen zugreifen.

6. **Welche Maßnahmen schützen die Vertraulichkeit?**

Antwort anzeigen

Zum Beispiel:

- Verschlüsselung
- Zugriffskontrollen
- VPNs

7. **Was bedeutet Integrität?**

Antwort anzeigen

Informationen dürfen nicht unbemerkt verändert oder manipuliert werden.

8. **Welche Maßnahmen schützen die Integrität?**

Antwort anzeigen

Zum Beispiel:

- Hashing
- digitale Signaturen
- Prüfmechanismen

9. **Was bedeutet Verfügbarkeit?**

Antwort anzeigen

Informationen müssen für berechtigte Nutzer jederzeit zugänglich sein.

10. **Welche Maßnahmen verbessern die Verfügbarkeit?**

Antwort anzeigen

Zum Beispiel:

- Backups
- Redundanz
- DDoS-Schutz

11. **Welche Gefahren gibt es für die Informationssicherheit?**

Antwort anzeigen

Zum Beispiel:

- Hackerangriffe
- menschliche Fehler
- technische Fehler
- Naturkatastrophen

12. **Was ist Datensicherung?**

Antwort anzeigen

Datensicherung ist der Prozess des Sicherns von Daten, damit diese bei Verlust wiederhergestellt werden können.

13. **Was bedeutet Redundanz?**

Antwort anzeigen

Redundanz bedeutet, dass Daten mehrfach vorhanden sind, zum Beispiel als Sicherungskopie oder Backup.

14. **Was ist ein Onsite-Backup?**

Antwort anzeigen

Ein Onsite-Backup ist ein Backup am gleichen Standort.

15. **Was ist ein Offsite-Backup?**

Antwort anzeigen

Ein Offsite-Backup ist ein Backup an einem anderen Standort.

16. **Was ist ein Air-Gap-Backup?**

Antwort anzeigen

Ein Air-Gap-Backup ist physisch oder logisch vom Netzwerk getrennt und schützt besonders gut vor Ransomware und Hackerangriffen.

17. **Was besagt die 3-2-1-Regel?**

Antwort anzeigen

Die 3-2-1-Regel bedeutet:

- 3 Kopien der Daten
- auf 2 verschiedenen Medien
- 1 Kopie an einem externen Ort

18. **Was ist ein Vollbackup?**

Antwort anzeigen

Beim Vollbackup werden alle Daten gesichert.

19. **Was ist ein differenzielles Backup?**

Antwort anzeigen

Ein differenzielles Backup sichert alle Änderungen seit der letzten Vollsicherung.

20. **Was ist ein inkrementelles Backup?**

Antwort anzeigen

Ein inkrementelles Backup sichert nur die Änderungen seit der letzten Sicherung.

21. **Was ist der Vorteil eines inkrementellen Backups?**

Antwort anzeigen

Es benötigt wenig Speicherplatz und geht schnell.

22. **Was ist der Nachteil eines inkrementellen Backups?**

Antwort anzeigen

Die Wiederherstellung ist komplexer, weil die Vollsicherung und alle nachfolgenden inkrementellen Sicherungen benötigt werden.

23. **Was ist das Archivbit?**

Antwort anzeigen

Das Archivbit ist ein Dateimerkmal von Windows. Es zeigt an, ob eine Datei seit der letzten Sicherung verändert wurde.

24. **Was bedeutet RPO?**

Antwort anzeigen

RPO bedeutet Recovery Point Objective. Es beschreibt, wie alt das letzte Backup maximal sein darf.

25. **Was bedeutet RAID?**

Antwort anzeigen

RAID bedeutet Redundant Array of Independent Disks. Mehrere Festplatten werden zu einer logischen Einheit zusammengefasst.

26. **Ersetzt RAID ein Backup?**

Antwort anzeigen

Nein. RAID ersetzt kein Backup.

27. **Wofür wird RAID 0 eingesetzt?**

Antwort anzeigen

RAID 0 wird zur Steigerung der Schreib- und Lesezugriffe eingesetzt.

28. **Was ist der Nachteil von RAID 0?**

Antwort anzeigen

Fällt eine Festplatte aus, sind die Daten nicht rekonstruierbar.

29. **Was macht RAID 1?**

Antwort anzeigen

RAID 1 spiegelt Daten. Jeder Datenblock wird auf zwei Festplatten gespeichert.

30. **Was ist der Vorteil von RAID 1?**

Antwort anzeigen

RAID 1 bietet Redundanz und kann die Lesegeschwindigkeit verbessern.

31. **Was ist RAID 5?**

Antwort anzeigen

RAID 5 ist ein Kompromiss aus Performance und Datensicherheit. Es nutzt Paritätsinformationen und benötigt mindestens 3 Festplatten.

32. **Was ist der Vorteil von RAID 5?**

Antwort anzeigen

RAID 5 bietet hohe Fehlertoleranz und eine höhere Lesegeschwindigkeit entsprechend der Anzahl der Platten.

33. **Was ist der Nachteil von RAID 5?**

Antwort anzeigen

Schreibintensive Arbeiten sind weniger effizient, weil Paritätsinformationen berechnet werden müssen.

34. **Was ist RAID 6?**

Antwort anzeigen

RAID 6 ist ähnlich wie RAID 5, verwendet aber zwei Paritätsinformationen. Dadurch dürfen zwei Laufwerke ausfallen.

35. **Was ist RAID 10?**

Antwort anzeigen

RAID 10 ist ein Verbund aus RAID 1 und RAID 0. Es kombiniert Spiegelung und Striping und benötigt mindestens 4 Festplatten.

36. **Was ist der Nachteil von RAID 10?**

Antwort anzeigen

Nur 50 % der Festplattenkapazität sind nutzbar.

37. **Was ist Hot Spare?**

Antwort anzeigen

Eine Hot-Spare-Platte ist eine Reservefestplatte, die bei Ausfall einer Platte automatisch in den RAID-Verbund integriert werden kann.

38. **Was ist Hot Swapping?**

Antwort anzeigen

Hot Swapping bedeutet, dass eine Festplatte im laufenden Betrieb ausgetauscht werden kann.

39. **Was ist JBOD?**

Antwort anzeigen

JBOD bedeutet Just a Bunch of Disks. Mehrere Festplatten werden zusammengeschaltet, aber ohne echte RAID-Redundanz.

40. **Warum bietet JBOD keinen Sicherheitsgewinn?**

Antwort anzeigen

Weil keine Redundanz vorhanden ist. Die Daten werden nur in Reihe geschrieben.