

20.12 Trainer – Backup, Restore, RPO, RTO und Notfallmaßnahmen

Diese Trainer-Seite wiederholt Backup, Restore, RPO, RTO, Retention, Restore-Test, Ransomware-Schutz und Notfallmaßnahmen.

Ziel ist, typische Prüfungsfragen zu Datensicherung, Wiederherstellung, Backup-Arten, Notfallplanung und Verfügbarkeit sicher zu beantworten.

Merksatz:

Backup ist die Sicherung.

Restore ist die Wiederherstellung.

Ein Backup ist nur so gut wie sein getesteter Restore.

Lernziele

Nach dieser Seite solltest du sicher können:

- Backup und Restore unterscheiden
- Vollbackup, inkrementelles Backup und differenzielles Backup unterscheiden
- RPO und RTO erklären
- Retention erklären
- Restore-Tests begründen
- 3-2-1-Regel erklären
- Offline- und Immutable-Backups einordnen
- Snapshots, Replikation, Synchronisation und Redundanz von Backup unterscheiden
- typische Backup-Fehler erkennen
- Notfallmaßnahmen fachlich beschreiben

Kurzüberblick

Begriff	Bedeutung
---------	-----------

Backup	Sicherung von Daten, Systemen oder Konfigurationen
Restore	Wiederherstellung aus einer Sicherung
RPO	maximal akzeptabler Datenverlust
RTO	maximal akzeptable Wiederherstellungszeit
Retention	Aufbewahrungsregel für Backups
Restore-Test	Prüfung, ob Wiederherstellung funktioniert
Offline-Backup	nicht dauerhaft verbundenes Backup
Immutable Backup	unveränderliches Backup
Notfallhandbuch	Anleitung für Störungen und Wiederanlauf

Merksatz:

RPO fragt:

Wie viel Datenverlust ist erlaubt?

RTO fragt:

Wie lange darf die Wiederherstellung dauern?

Aufgabe 1

Was ist ein Backup?

Antwort anzeigen

Ein Backup ist eine Sicherung von Daten, Systemen, Anwendungen oder Konfigurationen.

Ziel:

Daten oder Systeme nach Fehler,
Ausfall,
Löschung,
Defekt
oder Angriff wiederherstellen können.

Beispiele:

Dateisicherung

Datenbanksicherung

VM-Backup

Systemabbild

Konfigurationsbackup

Merksatz:

Backup = Sicherung zur späteren Wiederherstellung.

Aufgabe 2

Was ist ein Restore?

Antwort anzeigen

Restore bedeutet:

Wiederherstellung von Daten,
Systemen
oder Konfigurationen aus einem Backup.

Beispiele:

gelöschte Datei wiederherstellen

Datenbank auf früheren Zustand zurücksetzen

Server nach Ausfall wiederherstellen

Konfiguration zurückspielen

Merksatz:

Restore = Wiederherstellung aus Backup.

Aufgabe 3

Was ist der Unterschied zwischen Backup und Restore?

Antwort anzeigen

Backup:

Daten werden gesichert.

Restore:

gesicherte Daten werden wiederhergestellt.

Merksatz:

Backup ist Vorbereitung.
Restore ist der Ernstfall.

Aufgabe 4

Warum ist ein Restore-Test wichtig?

Antwort anzeigen

Ein Restore-Test prüft, ob ein Backup wirklich nutzbar ist.

Ohne Restore-Test weiß man nicht sicher:

ob Daten vollständig sind

ob Dateien lesbar sind

ob Datenbanken konsistent sind

ob Schlüssel vorhanden sind

ob Rechte stimmen

ob die Wiederherstellungszeit ausreicht

Merksatz:

Backup ohne Restore-Test ist unsicher.

Aufgabe 5

Was ist ein Vollbackup?

Antwort anzeigen

Ein Vollbackup sichert alle ausgewählten Daten vollständig.

Vorteile:

einfache Wiederherstellung

vollständiger Sicherungsstand

weniger Abhängigkeiten

Nachteile:

benötigt viel Speicherplatz

dauert länger

erzeugt mehr Last

Merksatz:

Vollbackup sichert alles,
braucht aber mehr Speicher und Zeit.

Aufgabe 6

Was ist ein inkrementelles Backup?

Antwort anzeigen

Ein inkrementelles Backup sichert nur Änderungen seit dem letzten Backup.

Das letzte Backup kann sein:

Vollbackup

oder

inkrementelles Backup

Vorteile:

schnell

spart Speicherplatz

Nachteile:

Restore braucht die Backup-Kette

beschädigte Kette kann Wiederherstellung gefährden

Merksatz:

Inkrementell = Änderungen seit letztem Backup.

Aufgabe 7

Was ist ein differenzielles Backup?

Antwort anzeigen

Ein differenzielles Backup sichert alle Änderungen seit dem letzten Vollbackup.

Vorteile:

Restore einfacher als bei langer inkrementeller Kette

weniger Speicherbedarf als tägliches Vollbackup

Nachteile:

wird bis zum nächsten Vollbackup immer größer

Merksatz:

Differenziell = Änderungen seit letztem Vollbackup.

Aufgabe 8

Ordne die Backup-Arten zu.

Backup-Art	Bedeutung
Vollbackup	?
inkrementelles Backup	?
differenzielles Backup	?

Antwort anzeigen

Backup-Art	Bedeutung
Vollbackup	sichert alle ausgewählten Daten
inkrementelles Backup	sichert Änderungen seit letztem Backup
differenzielles Backup	sichert Änderungen seit letztem Vollbackup

Merksatz:

Voll = alles.

Inkrementell = seit letztem Backup.

Differenziell = seit letztem Vollbackup.

Aufgabe 9

Was ist ein Snapshot?

Antwort anzeigen

Ein Snapshot ist eine Momentaufnahme eines Systems, Datenträgers, Dateisystems oder einer virtuellen Maschine.

Typische Nutzung:

vor Updates

vor Tests

vor Konfigurationsänderungen

Wichtig:

Ein Snapshot ersetzt kein vollständiges Backup.

Merksatz:

Snapshot = Momentaufnahme,
nicht automatisch Backup.

Aufgabe 10

Warum ersetzt ein Snapshot kein Backup?

Antwort anzeigen

Snapshots liegen oft auf demselben System oder Speicher wie die Produktivdaten.

Risiken:

Speicherdefekt betrifft Snapshot ebenfalls

Ransomware kann Snapshot erreichen

Snapshot kann gelöscht werden

Snapshot-Kette kann beschädigt werden

Speicherplatz kann volllaufen

Merksatz:

Backup muss getrennt,
geschützt
und wiederherstellbar sein.

Aufgabe 11

Was bedeutet RPO?

Antwort anzeigen

RPO steht für:

Recovery Point Objective

Bedeutung:

maximal akzeptabler Datenverlust.

Beispiel:

RPO 1 Stunde

Bedeutung:

Es dürfen höchstens Daten von einer Stunde verloren gehen.

Merksatz:

RPO = Datenverlust.

Aufgabe 12

Was bedeutet RTO?

Antwort anzeigen

RTO steht für:

Recovery Time Objective

Bedeutung:

maximal akzeptable Wiederherstellungszeit.

Beispiel:

RTO 4 Stunden

Bedeutung:

Der Dienst soll spätestens nach 4 Stunden wieder laufen.

Merksatz:

RTO = Zeit bis Wiederherstellung.

Aufgabe 13

Ordne zu.

Begriff	Frage
RPO	?
RTO	?

Antwort anzeigen

Begriff	Frage
RPO	Wie viel Datenverlust ist maximal erlaubt?
RTO	Wie lange darf die Wiederherstellung maximal dauern?

Merksatz:

RPO betrifft Daten.

RTO betrifft Zeit.

Aufgabe 14

Ein Unternehmen sagt:

Es dürfen maximal 2 Stunden Daten verloren gehen.

Welcher Begriff ist gemeint?

Antwort anzeigen

Gemeint ist:

RPO

Begründung:

Es geht um maximal akzeptablen Datenverlust.

Merksatz:

Datenverlust = RPO.

Aufgabe 15

Ein Unternehmen sagt:

Der Dienst muss spätestens nach 6 Stunden wieder verfügbar sein.

Welcher Begriff ist gemeint?

Antwort anzeigen

Gemeint ist:

RTO

Begründung:

Es geht um die maximal akzeptable Wiederherstellungszeit.

Merksatz:

Wiederherstellungszeit = RTO.

Aufgabe 16

Warum muss die Backup-Frequenz zum RPO passen?

Antwort anzeigen

Wenn das RPO klein ist, muss häufiger gesichert werden.

Beispiel:

RPO 24 Stunden:

tägliches Backup kann reichen.

RPO 1 Stunde:

stündliches Backup oder kontinuierliche Sicherung nötig.

Merksatz:

Je kleiner das RPO,
desto häufiger muss gesichert werden.

Aufgabe 17

Warum muss der Restore-Prozess zum RTO passen?

Antwort anzeigen

Das RTO beschreibt, wie schnell ein Dienst wiederhergestellt sein muss.

Der Restore-Prozess muss daher schnell genug sein.

Einflussfaktoren:

Backup-Größe

Netzwerkgeschwindigkeit

Speicherleistung

Abhängigkeiten

Personal

Dokumentation

Tests

Merksatz:

RTO wird durch den gesamten Wiederherstellungsprozess bestimmt.

Aufgabe 18

Was bedeutet Retention?

Antwort anzeigen

Retention bedeutet:

Aufbewahrungsregel für Backups.

Beispiele:

tägliche Backups 14 Tage behalten

wöchentliche Backups 8 Wochen behalten

monatliche Backups 12 Monate behalten

Merksatz:

Retention regelt,
wie lange Backups behalten werden.

Aufgabe 19

Was ist die 3-2-1-Regel?

Antwort anzeigen

Die 3-2-1-Regel lautet:

3 Kopien der Daten

2 unterschiedliche Speicherarten

1 Kopie extern oder getrennt

Beispiel:

Produktivdaten

Backup auf NAS

zusätzliches externes oder Cloud-Backup

Merksatz:

3-2-1 reduziert das Risiko,
dass alle Kopien gleichzeitig verloren gehen.

Aufgabe 20

Was bedeutet die 3-2-1-1-0-Regel?

Antwort anzeigen

Die 3-2-1-1-0-Regel ist eine erweiterte Backup-Regel.

Sie bedeutet:

3 Kopien

2 unterschiedliche Medien

1 Kopie extern

1 Kopie offline oder immutable

0 Fehler bei Restore-Tests

Merksatz:

Die 0 steht für fehlerfrei getestete Wiederherstellung.

Aufgabe 21

Was ist ein Offline-Backup?

Antwort anzeigen

Ein Offline-Backup ist nicht dauerhaft mit dem Produktivsystem verbunden.

Beispiele:

getrennte Festplatte

Band

ausgelagertes Medium

abgeschottetes Backup-System

Vorteil:

besserer Schutz gegen Ransomware
und versehentliche Löschung.

Merksatz:

Offline-Backup ist nicht dauerhaft erreichbar.

Aufgabe 22

Was ist ein Immutable Backup?

Antwort anzeigen

Immutable bedeutet:

unveränderlich.

Ein Immutable Backup kann für eine festgelegte Zeit nicht verändert oder gelöscht werden.

Schützt gegen:

Ransomware

Manipulation

versehentliche Löschung

kompromittierte Adminzugänge

Merksatz:

Immutable Backup schützt die Wiederherstellungsmöglichkeit.

Aufgabe 23

Warum sind Offline- oder Immutable-Backups bei Ransomware wichtig?

Antwort anzeigen

Ransomware versucht häufig, auch Backups zu löschen oder zu verschlüsseln.

Offline-Backups sind nicht dauerhaft verbunden.

Immutable Backups können für eine festgelegte Zeit nicht verändert oder gelöscht werden.

Dadurch bleibt eine Wiederherstellung möglich.

Merksatz:

Backups müssen auch vor Angreifern geschützt werden.

Aufgabe 24

Was ist Backup-Verschlüsselung?

Antwort anzeigen

Backup-Verschlüsselung schützt Sicherungsdaten vor unberechtigtem Lesen.

Wichtig:

Schlüssel sicher aufbewahren

Zugriff begrenzen

Wiederherstellung mit Schlüssel testen

Schlüsselverlust vermeiden

Merksatz:

Verschlüsseltes Backup ist nur nutzbar,
wenn der Schlüssel verfügbar ist.

Aufgabe 25

Warum brauchen Backups besondere Zugriffsrechte?

Antwort anzeigen

Backups enthalten oft besonders viele oder besonders sensible Daten.

Risiken bei zu breiten Rechten:

Datenabfluss

Manipulation

Löschung

Ransomware kann Backups verschlüsseln

Maßnahmen:

getrennte Adminrechte

MFA

keine normalen Benutzerrechte auf Backup-Speicher

Löschrechte begrenzen

Zugriffe protokollieren

Merksatz:

Backups brauchen starken Zugriffsschutz.

Aufgabe 26

Was ist Backup-Monitoring?

Antwort anzeigen

Backup-Monitoring prüft, ob Sicherungen erfolgreich laufen.

Zu überwachen:

letzter erfolgreicher Backup-Lauf

Fehlermeldungen

Datenmenge

Laufzeit

Speicherplatz

Retention

ungewöhnliche Löschungen

Restore-Test

Merksatz:

Fehlgeschlagene Backups müssen auffallen,
bevor ein Restore nötig ist.

Aufgabe 27

Was ist ein Datenbank-Backup?

Antwort anzeigen

Ein Datenbank-Backup sichert eine Datenbank so, dass sie konsistent wiederhergestellt werden kann.

Wichtig:

laufende Transaktionen

Schreibzugriffe

Transaktionslogs

Konsistenz

Wiederherstellungszeitpunkt

Merksatz:

Datenbanken nicht einfach blind als Datei kopieren.

Aufgabe 28

Was bedeutet Point-in-Time-Recovery?

Antwort anzeigen

Point-in-Time-Recovery bedeutet:

Wiederherstellung auf einen bestimmten Zeitpunkt.

Beispiel:

Datenbank auf Zustand von 10:15 Uhr zurücksetzen.

Nützlich bei:

versehentlichem Löschen

fehlerhaftem Import

falscher Änderung

beschädigten Daten

Merksatz:

Point-in-Time-Recovery stellt gezielt einen früheren Zeitpunkt wieder her.

Aufgabe 29

Was ist Replikation?

Antwort anzeigen

Replikation bedeutet:

Daten werden auf ein anderes System kopiert,
oft nahezu aktuell.

Vorteil:

schnelle Umschaltung

aktuelle Kopie

höhere Verfügbarkeit

Risiko:

Fehler,
Löschung
oder Ransomware können mitrepliziert werden.

Merksatz:

Replikation ist kein Backup.

Aufgabe 30

Was ist Synchronisation?

Antwort anzeigen

Synchronisation bedeutet:

Daten werden zwischen Speicherorten abgeglichen.

Problem:

Löschungen,
Fehländerungen,
beschädigte Dateien
oder Ransomware-Verschlüsselung können mitsynchronisiert werden.

Merksatz:

Synchronisation hält Daten gleich,
stellt aber nicht automatisch alte Stände wieder her.

Aufgabe 31

Was ist Redundanz?

Antwort anzeigen

Redundanz bedeutet:

wichtige Komponenten sind mehrfach vorhanden.

Beispiele:

RAID

zwei Netzteile

mehrere Server

zweite Firewall

mehrere Internetleitungen

Ziel:

Ausfall vermeiden oder abfedern.

Wichtig:

Redundanz ersetzt kein Backup.

Merksatz:

Redundanz erhöht Verfügbarkeit,
stellt aber keine alten Datenstände wieder her.

Aufgabe 32

Ordne zu.

Begriff	Ersetzt Backup?
Snapshot	?
Replikation	?
Synchronisation	?
Redundanz	?

Antwort anzeigen

Begriff	Ersetzt Backup?
Snapshot	nein
Replikation	nein
Synchronisation	nein
Redundanz	nein

Begründung:

Diese Verfahren können nützlich sein,
ersetzen aber kein vollständiges Backup-Konzept mit Restore-Möglichkeit.

Merksatz:

Nicht alles,
was Daten kopiert oder verfügbar hält,
ist ein Backup.

Aufgabe 33

Was ist ein Notfallhandbuch?

Antwort anzeigen

Ein Notfallhandbuch beschreibt, was bei schweren Störungen zu tun ist.

Inhalte:

Ansprechpartner

Prioritäten

Systeme

Wiederherstellungsreihenfolge

Backup-Orte

Restore-Anleitungen

Kommunikationswege

Eskalationswege

Merksatz:

Im Notfall darf nicht erst gesucht werden,
wer was weiß.

Aufgabe 34

Warum ist die Restore-Reihenfolge wichtig?

Antwort anzeigen

Systeme hängen oft voneinander ab.

Beispielhafte Reihenfolge:

Netzwerk

Verzeichnisdienst

Speicher

Datenbank

Anwendung

Benutzerzugriff

Wenn Abhängigkeiten fehlen, starten Dienste eventuell nicht korrekt.

Merksatz:

Restore braucht Reihenfolge,
weil Systeme voneinander abhängen.

Aufgabe 35

Was ist Disaster Recovery?

Antwort anzeigen

Disaster Recovery beschreibt:

Wiederherstellung der IT nach schweren Störungen.

Beispiele:

Ransomware

Brand

Rechenzentrumsausfall

massiver Datenverlust

Hardwaredefekt

Cloud-Ausfall

Merksatz:

Disaster Recovery = IT-Wiederherstellung nach schwerem Vorfall.

Aufgabe 36

Was ist Business Continuity?

Antwort anzeigen

Business Continuity bedeutet:

Geschäftsprozesse sollen trotz Störung weiterlaufen
oder schnell wieder anlaufen.

Dazu gehören:

Notfallplanung

Ersatzprozesse

Kommunikation

Verantwortlichkeiten

Wiederanlauf

Tests

Merksatz:

Business Continuity betrachtet den Betrieb insgesamt.

Aufgabe 37

Was ist Failover?

Antwort anzeigen

Failover bedeutet:

Ein Dienst wird bei Ausfall auf ein Ersatzsystem umgeschaltet.

Möglich:

automatisch

oder

manuell

Beispiele:

zweite Firewall übernimmt

Datenbank-Replikat wird aktiv

anderer Server übernimmt Dienst

Wichtig:

Failover ersetzt kein Backup.

Merksatz:

Failover reduziert Ausfallzeit,
ist aber kein Backup.

Aufgabe 38

Welche Antwort ist besser?

Aufgabe:

Warum reicht es nicht,
nur Backups zu erstellen?

Antwort A:

Weil man mehr machen muss.

Antwort B:

Backups müssen regelmäßig überwacht und durch Restore-Tests geprüft werden.
Nur so ist sichergestellt,
dass Daten vollständig,
lesbar
und innerhalb der geforderten Zeit wiederherstellbar sind.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort nennt konkrete Anforderungen:

Monitoring,

Restore-Test,

Vollständigkeit

und Wiederherstellungszeit.

Merksatz:

Backup braucht Prüfung.

Aufgabe 39

Welche Antwort ist besser?

Aufgabe:

Warum ist Replikation kein Backup?

Antwort A:

Weil es anders heißt.

Antwort B:

Replikation erstellt eine aktuelle Kopie.

Fehler,

Löschungen

oder Ransomware-Verschlüsselungen können jedoch mitrepliziert werden.

Ein Backup muss auch ältere Zustände wiederherstellen können.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort erklärt den fachlichen Unterschied zwischen aktueller Kopie und wiederherstellbaren alten Ständen.

Merksatz:

Replikation ist Verfügbarkeit,
Backup ist Wiederherstellung.

Aufgabe 40

Welche Antwort ist besser?

Aufgabe:

Was bedeutet RPO 1 Stunde?

Antwort A:

Das Backup dauert eine Stunde.

Antwort B:

RPO 1 Stunde bedeutet,
dass maximal Daten aus einer Stunde verloren gehen dürfen.
Die Backup-Frequenz oder Sicherungsmethode muss dazu passen.

Antwort anzeigen

B ist besser.

Begründung:

RPO beschreibt Datenverlust,
nicht die Dauer des Backups.

Merksatz:

RPO nicht mit Backup-Dauer verwechseln.

Mini-Prüfung: schnelle Zuordnung

Frage	Antwort
Was ist Backup?	Sicherung
Was ist Restore?	Wiederherstellung
Was bedeutet RPO?	maximal akzeptabler Datenverlust
Was bedeutet RTO?	maximal akzeptable Wiederherstellungszeit
Was bedeutet Retention?	Aufbewahrungsregel
Was ist Vollbackup?	sichert alle ausgewählten Daten
Was ist inkrementell?	Änderungen seit letztem Backup
Was ist differenziell?	Änderungen seit letztem Vollbackup
Was ist Snapshot?	Momentaufnahme
Was ist Offline-Backup?	nicht dauerhaft verbunden
Was ist Immutable Backup?	unveränderliches Backup
Was ist Restore-Test?	Prüfung der Wiederherstellung

Mini-Prüfung: Fehlerbild erkennen

Fehlerbild	Wahrscheinlichstes Thema
Backup vorhanden, Restore geht nicht	Restore-Test fehlt oder Backup defekt
zu viel Datenverlust	RPO nicht eingehalten
Wiederherstellung dauert zu lange	RTO nicht eingehalten
Datenbank nach Restore beschädigt	kein konsistentes Backup
Backupziel voll	Retention oder Speicherplatz
Ransomware verschlüsselt Backups mit	Backup online und beschreibbar
verschlüsseltes Backup nicht nutzbar	Schlüssel fehlt

Fehlerbild	Wahrscheinlichstes Thema
alte Datei fehlt	Retention zu kurz
Replikat enthält auch gelöschte Daten	Replikation ist kein Backup
Dienst startet nach Restore nicht	Abhängigkeiten oder Reihenfolge vergessen

IHK-sichere Kurzformulierung

Ein Backup ist eine Sicherung von Daten, Systemen oder Konfigurationen. Restore bezeichnet die Wiederherstellung aus dieser Sicherung. Ein Backup ist nur zuverlässig, wenn die Wiederherstellung regelmäßig getestet wird. Vollbackups sichern alle ausgewählten Daten, inkrementelle Backups sichern Änderungen seit dem letzten Backup und differenzielle Backups sichern Änderungen seit dem letzten Vollbackup. RPO beschreibt den maximal akzeptablen Datenverlust, RTO die maximal akzeptable Wiederherstellungszeit. Retention legt fest, wie lange Backups aufbewahrt werden. Snapshots, Replikation, Synchronisation, Redundanz und Failover ersetzen kein vollständiges Backup-Konzept. Gegen Ransomware helfen besonders Offline- oder Immutable-Backups und regelmäßige Restore-Tests.

Merksätze

Backup = Sicherung.

Restore = Wiederherstellung.

Backup ohne Restore-Test ist unsicher.

Vollbackup sichert alles.

Inkrementell sichert seit letztem Backup.

Differenziell sichert seit letztem Vollbackup.

Snapshot ist Momentaufnahme.

Snapshot ersetzt kein Backup.

Datenbanken brauchen konsistente Backups.

Point-in-Time-Recovery stellt einen Zeitpunkt wieder her.

RPO = Datenverlust.

RTO = Wiederherstellungszeit.

Retention = Aufbewahrungsregel.

Backup-Frequenz muss zum RPO passen.

Restore-Prozess muss zum RTO passen.

3-2-1 reduziert Gesamtrisiko.

3-2-1-1-0 ergänzt Offline oder Immutable und fehlerfreie Restore-Tests.

Offline-Backup ist nicht dauerhaft verbunden.

Immutable Backup ist unveränderlich.

Verschlüsseltes Backup braucht Schlüssel.

Backups brauchen starke Rechtebegrenzung.

Backup-Monitoring ist Pflicht.

Backup-Logs regelmäßig prüfen.

Redundanz ist kein Backup.

Replikation ist kein Backup.

Synchronisation ist kein Backup.

Failover ist kein Backup.

Notfallhandbuch hilft im Ernstfall.

Restore braucht Reihenfolge.

Business Continuity betrachtet Geschäftsprozesse.

Disaster Recovery betrachtet IT-Wiederherstellung.

Im Notfall zählt nicht,
ob ein Backup irgendwo existiert,
sondern ob es korrekt und rechtzeitig wiederhergestellt werden kann.
