



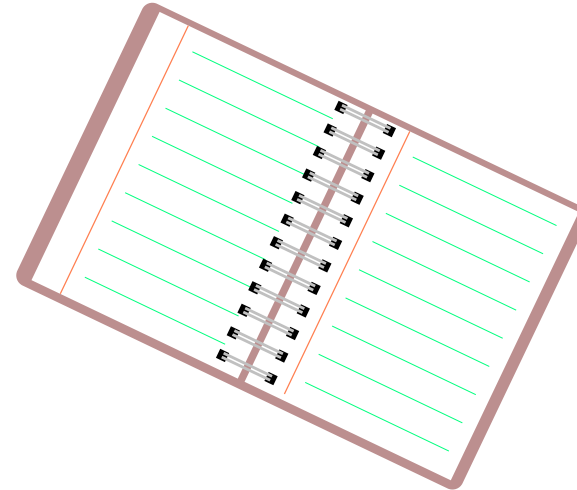
3-2-1-0 ... frisch ans Werk! Helfertools für Backups

Stefan Kirsch

14. Dezember 2023

Worüber will ich heute sprechen?

- Ausgangspunkt
- Wiederherstellungsszenarien - für welche Fälle brauche ich Backups?
- Tools für Backups zur Disaster Recovery
 - Fokus: Nextcloud-Sync
- Tools für Backups zur Point-in-time Recovery
 - Fokus: Duplicati
- "0 Fehlertoleranz bei der Wiederherstellung"
- Abschluss



Ausgangspunkt



3-2-1-0 Backup-Regel:

- ✓ 3 Kopien
- ✓ 2 verschiedene Speichermedien
- ✓ 1 externer Ort
- ✓ 0 Fehlertoleranz bei der Wiederherstellung

- es geht um:
 - Backups von (Forschungs-)Daten
 - Backups selber machen
- Aufwand für Backups:
 - Wie groß wäre im Vergleich der Schaden bei Datenverlust?
 - Tools zur Unterstützung, um den Backup-Aufwand gering zu halten

Warum Softwaretools?

Tools können helfen

- die richtigen Ordner zu sichern und unnötige Dateien vom Backup auszuschließen
- Backups zu komprimieren
- automatisch nach Zeitplan zu sichern oder mehrere zeitliche Schnappschüsse anzulegen, die ggf. nach bestimmten Vorgaben automatisch aufgeräumt werden
- durch Verschlüsselung den Zugriff auf die angelegten Backups zu beschränken
- Backups zu überprüfen und bei der Wiederherstellung unterstützt zu werden
- für die verschiedenen Wiederherstellungsszenarien vorbereitet zu sein



Wiederherstellungsszenarien

"Wann sind Sicherheitskopien die Rettung?" (BSI)

→ 2 Szenarien für die Wiederherstellung:

- Disaster-Recovery



- z.B. „Laptop explodiert“, jemand stolpert über das Netzkabel, Diebstahl
- Ziel: letztmöglichen Stand wiederherstellen
- Strategie: kontinuierliche Sicherung

- Point-in-time Recovery



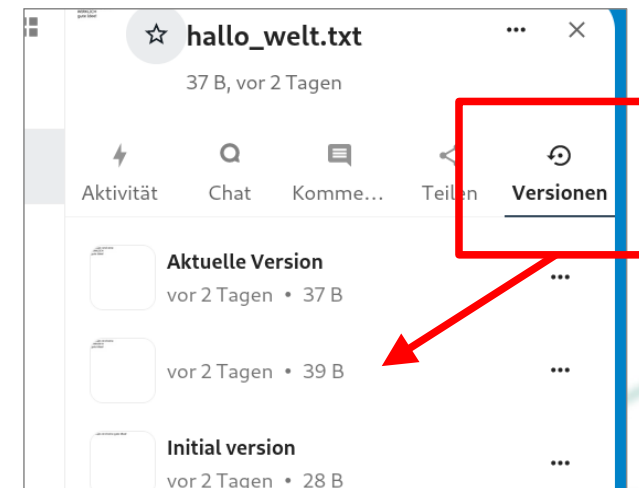
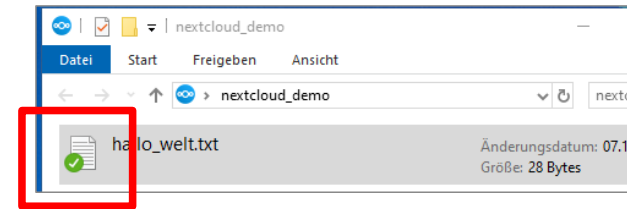
- z.B. Fehler unbemerkt synchronisiert, Daten kompromittiert
- Ziel: Stand zu bestimmtem Zeitpunkt wiederherstellen
- Strategie: Snapshots – kontextuell oder nach Zeitplan

Backup für Disaster Recovery

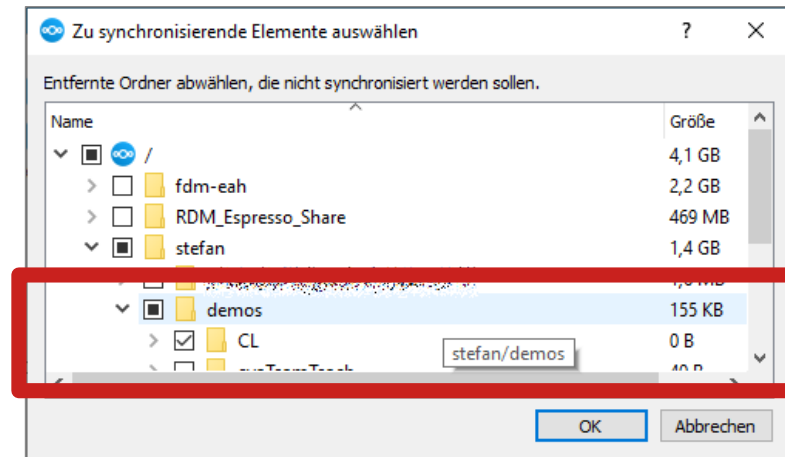
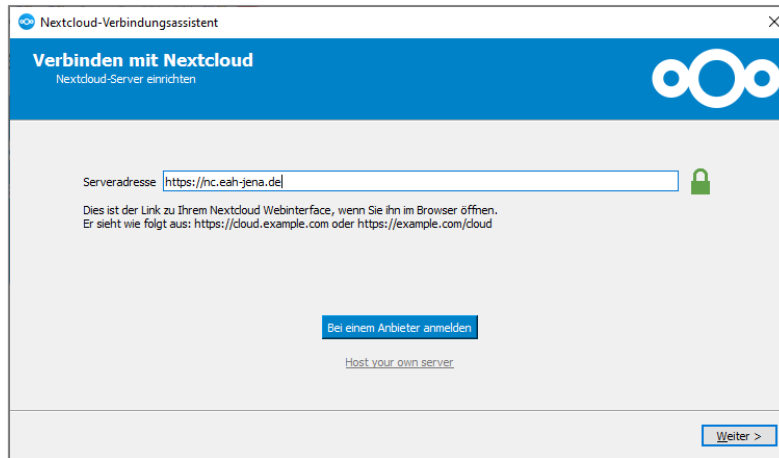


Letztmöglichen Stand wiederherstellbar machen durch kontinuierliche Synchronisation

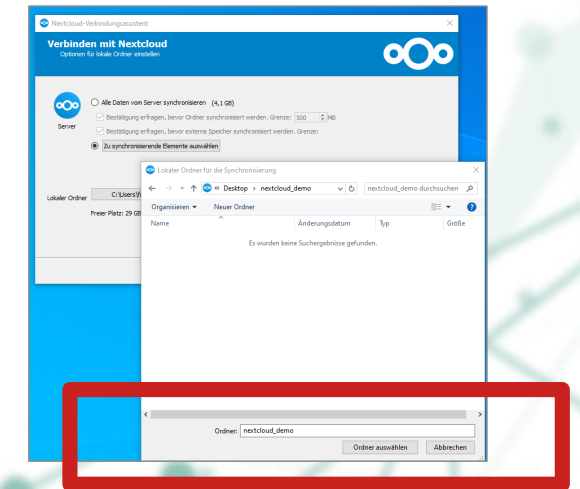
- z.B. auf Cloud, Backup-Partition, RAID-Systeme
- Das Sync-Tool Nextcloud nutzen:
 - Verfügbarkeit (Thüringer Hochschulen; GPL)
 - reife Software
 - Clients für viele Betriebssysteme
 - Integration in grafische Datei-Explorer (z.B. Windows-Explorer)
 - eingeschränkte Versionierung
 - „Papierkorb/ „zuletzt gelöscht“
 - andere Funktionen z.B. Groupware-Funktionen, Office im Browser



Nextcloud nutzen



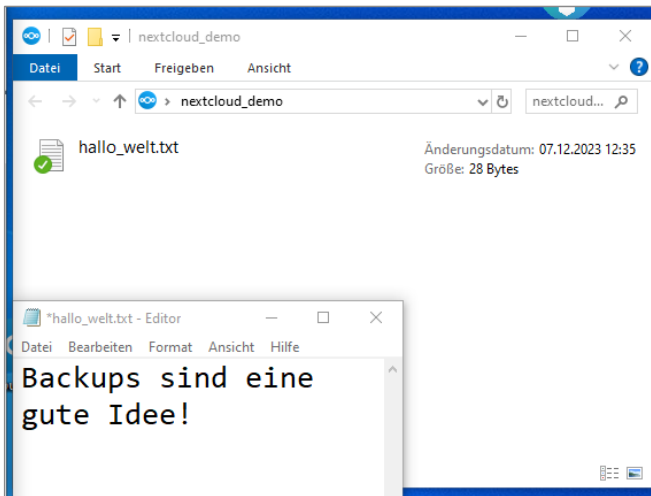
- 1) Zu Nextcloud verbinden
- 2) Zu synchronisierende Elemente auswählen
 - I. Ziel-Unterordner in der Cloud auswählen
 - II. lokalen Quellordner auswählen



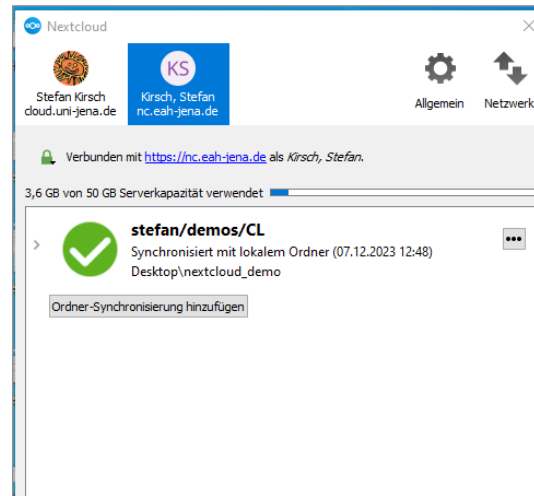
Nextcloud nutzen



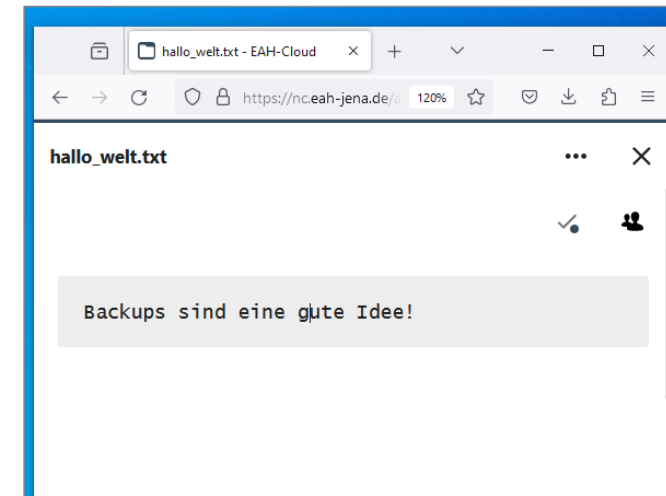
Lokale Textdatei



Sync-Client



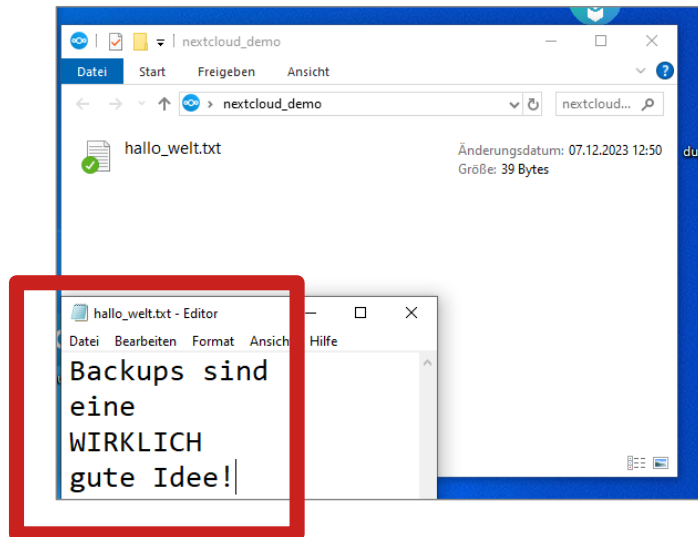
In der Cloud (via Browser)



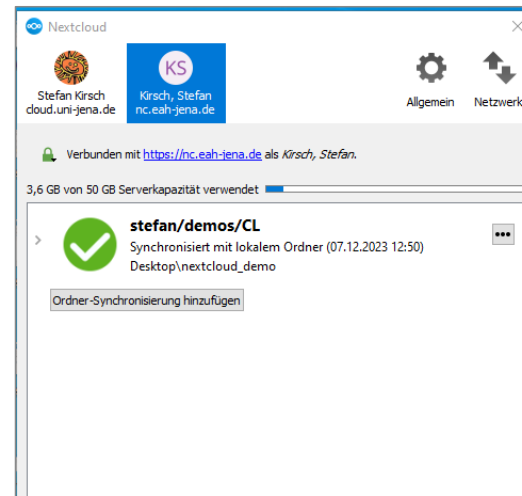
Nextcloud nutzen



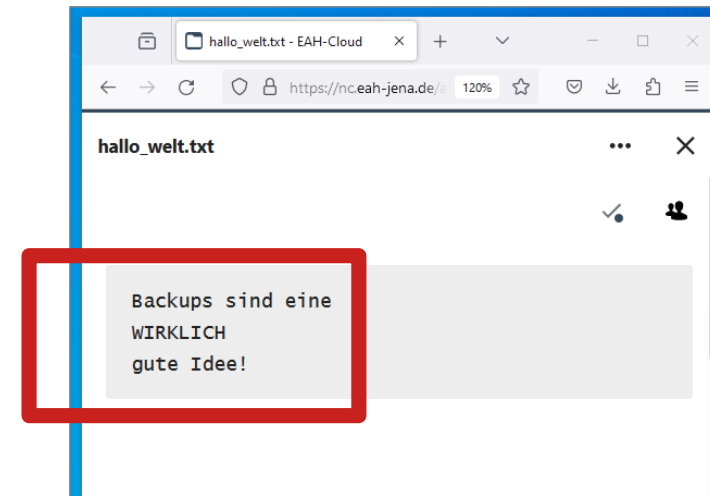
Lokale Textdatei (geändert)



Sync-Client



In der Cloud (geändert)



Nextcloud-Sync: zu bedenken



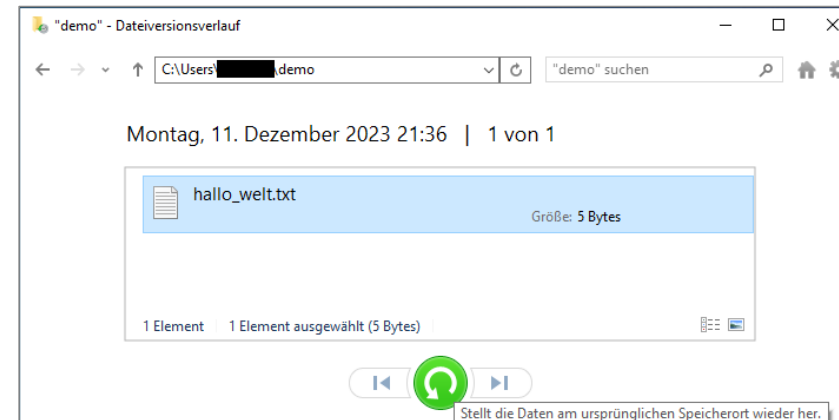
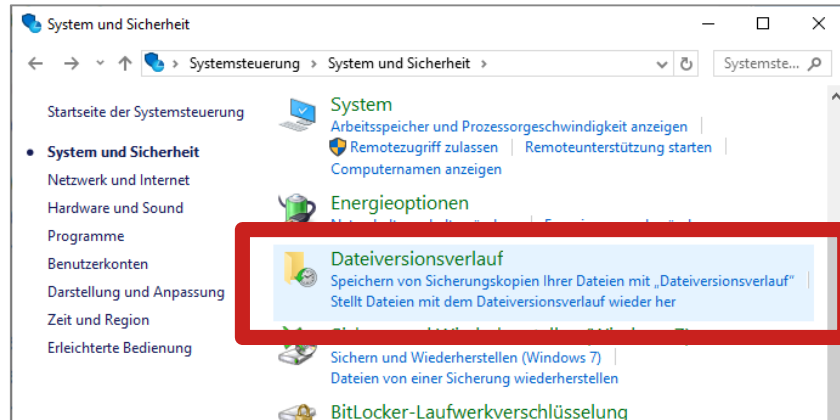
- Speicherplatzbeschränkung kann Eignung einschränken
- Fehler werden mitsynchronisiert (ohne dass man es bemerkt?)
- Kein Schutz vor Ransomware?
- Bei zentraler (Next-/Own-)Cloud sind z.T. auch Vorkehrungen für Point-in-time Recovery
→ Konfigurationen unterschiedlich
- für die Wiederherstellung von solchen zentralen Sicherungen:
 - mögliche Wiederherstellungszeiträume sind vom Rechenzentrum festgelegt
 - im Bedarfsfall ist man aufs Rechenzentrum angewiesen
 - möglich: aus Aufwandsgründen nur „große Blöcke“ wiederherstellbar, z.B. der Speicher einer Arbeitsgruppe

Backup für Point-in-time Recovery



Stand zu bestimmten Zeitpunkten wiederherstellbar machen durch Erzeugen von Snapshots

- Betriebssystemtools (z.B. Apple Time Machine, Back In Time (BIT), Windows Dateiversionsverlauf)



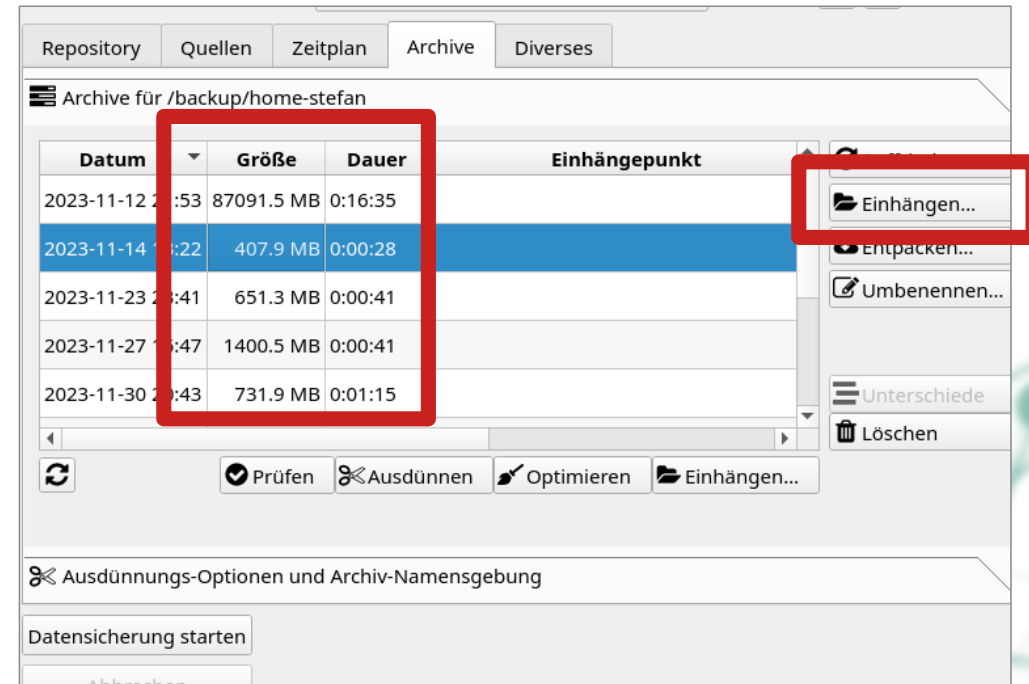
- kommerzielle Software (Stiftung Warentest/ SRF) / Software mit unterschiedlichen Lizenzen (Wikipedia)

Backup für Point-in-time Recovery



Stand zu bestimmten Zeitpunkten wiederherstellbar machen durch Erzeugen von Snapshots

- rsync → grsync
 - keine Zusatzprogramme für Anzeige/ Restore nötig
 - „Zwischending“ → nur 1 Snapshot: abgleichen, exkludieren, spiegeln
- Back In Time
 - Snapshots mit rsync
 - nur veränderte Dateien werden neu kopiert (Speicher-, Zeitbedarf sinkt)
- BorgBackup → borgmatic, Vorta/ Pika
 - Deduplizierung, Komprimierung, Verschlüsselung
 - Snapshots können ins Dateisystem eingehängt werden



Duplicati nutzen



Stand zu bestimmten Zeitpunkten wiederherstellbar machen durch Erzeugen von Snapshots

Neues Backup anlegen:
Verschlüsselung, Passwort

Unterstützte Speicherziele

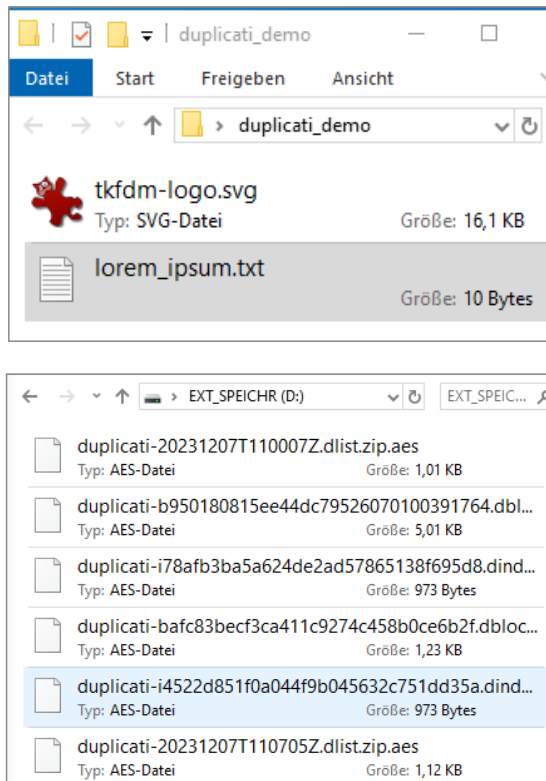
Optional:
Zeitplan, Auto-Aufräumen

Duplicati nutzen

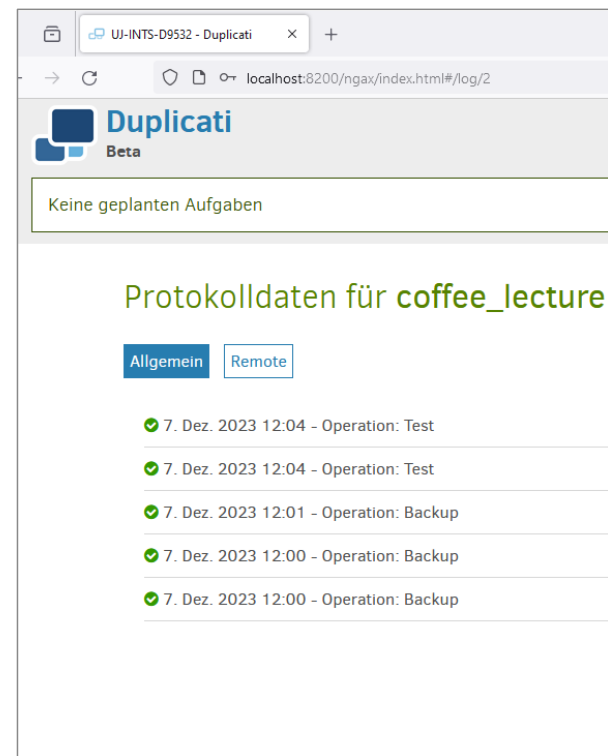


Stand zu bestimmten Zeitpunkten wiederherstellbar machen durch Erzeugen von Snapshots

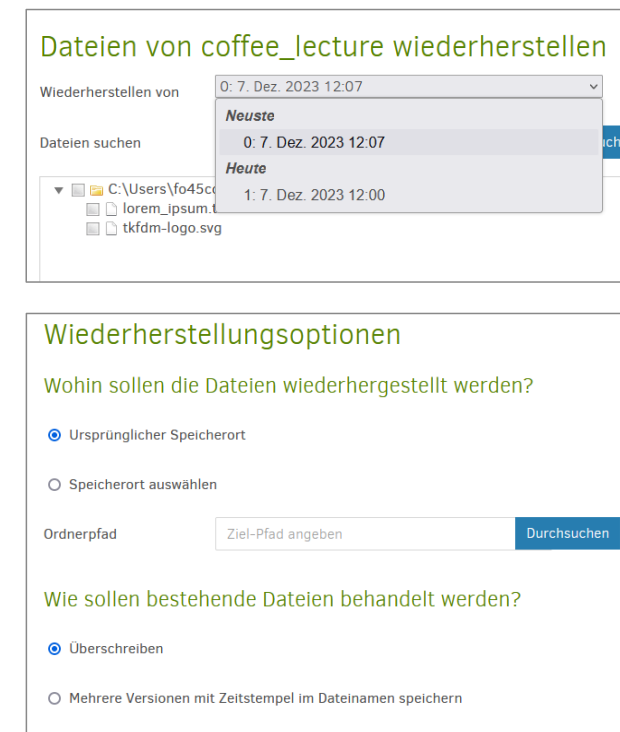
Nach Backup: Quelle+Ziel (Stick)



Protokollierung



Wiederherstellen: Optionen



„0 Fehlertoleranz bei der Wiederherstellung“



- "Backups sollten regelmäßig getestet werden auf ..." (BSI, Checkliste Backup 2023)
 - Vollständigkeit
 - Integrität
 - Verfügbarkeit
 - erfolgreiche Wiederherstellbarkeit
„einwandfrei und in angemessener Zeit"
- vollständiges Wiederherstellen
 - Wiederherstellung auf einem anderen Gerät testen! (Duplicati Docs)
- Stichproben
- Prüfsummen/ Hashes
- Integritätstests der Backup-Programme (borg check)

Zum Mit-nach-Hause nehmen



- Aufwand für Backups: → wie groß wäre der Schaden bei Datenverlust?
→ hilfreiche Tools nutzen, die unterstützen
- letzmöglichen Stand sichern: → Sync auf zentrale Nextcloud
→ Oft mehrere Szenarien abgesichert
- Stand zu Zeitpunkt sichern: → einfaches Tool für Snapshots nutzen,
z.B. 2-wöchentlich mit Duplicati
- wenn kein Tool zur Hand: → Daten manuell kopieren (3-2-1)
- Wiederherstellung testen: → auch auf einem anderen Rechner
- zum Weiterdenken: → Backups unveränderlich machen (z.B. Ransomwareschutz)
→ Sicherung in die Cloud oder auf externe Datenträger:
Verschlüsselung von Dateien und Ordnern

Das Thüringer Kompetenznetzwerk
Forschungsdatenmanagement präsentiert...



Forschungsdatenmanagement

Online Coffee Lectures 23/24



- | | |
|------------|--|
| 24.01.2024 | Tools zur Verschlüsselung von Dateien und Ordnern
Stefan Kirsch (EAH Jena) |
| 21.02.2024 | SQLite als Schweizer Taschenmesser für die
Auswertung von tabellarischen Daten
Philipp Mathias Schäfer (zedif, Uni Jena) |