Backups mit Restic und resticprofile

Rainer Rose, Andreas Scherbaum

Wer hat schon mal Daten (unwiederbringlich) verloren?

Wer hat Backups für alle Daten?

Wer hat sein Restore schon mal getestet?

Wer hat mehr als ein Backup?

Wer sind wir

Rainer Rose

- Linux seit 1997
  - Beruflich seit 2004
- Senior DevOps bei der AD IT Systems GmbH
- Beruflich viel
  - Ansible
  - git
  - OpenTofu / Terraform
  - Openstack
- Und natürlich Backups (restic und resticprofile)
- Hiring!
  - Linux Admin, System Engineer (DevOps)



Rainer Rose - Online

- Blog: https://www.RainerRose.de
- Mastodon: https://norden.social/@Kaffee_Junkie42



Andreas Scherbaum

- PostgreSQL seit ~1997
- Freelancer seit 2004
  - Hauptsächlich etwas mit Datenbanken
- Board of Directors: PostgreSQL User Group Europe
- Organisiert Konferenzen
- Deutscher Pressekontakt PostgreSQL
- Interviewt die PostgreSQL Community
- Privat überall Ansible
- Mehr Backups - mit Restic - als notwendig
- Autor: ein Buch über PostgreSQL

Andreas Scherbaum - Online

- Blog: https://andreas.scherbaum.la/
- Mastodon: https://mastodon.social/@ascherbaum
- Weitere: https://postgresql.life/social/#ads



Blog



Mastodon



Weitere

Inhalte

Worüber reden wir

- Was ist Restic
  - Storages
  - Verschlüsselung
  - Snapshots
  - Restore
- Was ist resticprofile
- Wir erstellen ein Backup
- Fragen & Antworten

Was ist Restic

Restic

- Open Source Backup Software
- Entwicklung: seit 2015
- Sprache: Go
- Lizenz: BSD (2 clause)
- Unterstützt: Linux, MacOS, (Open|Free)BSD, Windows
- Rückwärts kompatibel: eine Version (Semantic Versioning)

Backups mit Restic

- Backup: komplett, inkrementell
- Deduplizierung
- Verschlüsselung (nicht optional)
- Komprimierung
- Ziel: lokal, diverse Netzwerkziele, …

Terminology

- Repository: hier liegt das Backup
  - Format: seit v0.14: v2
- Snapshot: Backup Zeitpunkt
- Pack: Dateien, als 16 MB Blöcke
- Pack Size: Größe der Backup Dateien (16 MB)
- Dry Run: Änderungen nur anzeigen
- Exclude/Include: was (nicht) gesichert wird
- Blob: Anzahl Bytes, mit SHA256 Prüfsumme

Wohin mit dem Backup

- Lokal (nach Möglichkeit auf ein anderes Laufwerk)
- S3 und kompatible (Minio, Wasabi, Alibaba)
- SFTP (copy over ssh), REST (http/https) + optional Auth
- OpenStack Swift
- Backblaze B2 (problematisch, S3 kompatibel verwenden)
- Microsoft Azure Blob Storage
- Google Cloud Storage
- rclone-kompatibel

Online Backups

- Ingress und Egress Kosten
  - Restic muss die Metadaten herunterladen
  - Siehe auch: Cache
- Stabile Internetverbindung
  - Unterbrochene Backups hinterlassen Locks

Verschlüsselung

- Implizit
- Option `--insecure-no-password`
  - Seit Version 0.17
  - Muss immer angegeben werden
- Repository Keys: mehrere Passwörter möglich

Restic Backup am Beispiel

Repository initialisieren

```
$ mkdir ~/repository
$ restic -r ~/repository/ init
enter password for new repository:
enter password again:
created restic repository 977eb753ca at ~/repository/

Please note that knowledge of your password is required to access
the repository. Losing your password means that your data is
irrecoverably lost.
```

Repository Layout

```
$ ls -ld ~/repository/*
-r--------   1 ads ads  155 13. Feb 13:37 ~/repository/config
drwx------ 258 ads ads 4096 13. Feb 13:37 ~/repository/data
drwx------   2 ads ads 4096 13. Feb 13:37 ~/repository/index
drwx------   2 ads ads 4096 13. Feb 13:37 ~/repository/keys
drwx------   2 ads ads 4096 13. Feb 13:37 ~/repository/locks
drwx------   2 ads ads 4096 13. Feb 13:37 ~/repository/snapshots
```

Verzeichnisse im Repository

- `config`: verschlüsselte JSON-Datei
- `data`: hier liegt das Backup
- `index`: hier liegen Metainformationen zum Backup
- `keys`: ein oder mehrere Schlüssel für das Backup
- `locks`: schreibende Operationen halten hier einen Lock
  - Parallele schreibende und lesende Operationen sind möglich
- `snapshots`: Informationen über Backups (Snapshots)
- `tmp`: temporäre Dateien

Backup erstellen

```
$ du -sh wichtige-daten/
51M  wichtige-daten/

$ restic -r ~/repository --verbose backup ~/wichtige-daten/
open repository
enter password for repository:

repository 977eb753 opened (version 2, compression level auto)
[0:00]          0 index files loaded
start scan on [wichtige-daten/]
start backup on [wichtige-daten/]
scan finished in 0.002s: 50 files, 50.000 MiB

Files:              50 new,       0 changed,         0 unmodified
Dirs:               1 new,    0 changed,         0 unmodified
Data Blobs:         69 new
Tree Blobs:         2 new
Added to the repository: 50.019 MiB (50.010 MiB stored)

processed 50 files, 50.000 MiB in 0:00
snapshot 148acc51 saved
```

Erstes Backup erstellen

```
$ du -sh wichtige-daten/
51M wichtige-daten/

$ restic -r ~/repository --verbose backup ~/wichtige-daten/
open repository
enter password for repository:

repository 977eb753 opened (version 2, compression level auto)
[0:00]          0 index files loaded
start scan on [wichtige-daten/]
start backup on [wichtige-daten/]
scan finished in 0.002s: 50 files, 50.000 MiB

Files:          50 new,     0 changed,     0 unmodified
Dirs:            1 new,     0 changed,     0 unmodified
Data Blobs:     69 new
Tree Blobs:      2 new
Added to the repository: 50.019 MiB (50.010 MiB stored)

processed 50 files, 50.000 MiB in 0:00
snapshot 148acc51 saved
```

Passwort und Key

- Manuell eingeben
- Per Kommandozeile
  - `--password-file`
  - `--password-command`
- Per Umgebungsvariable
  - `$RESTIC_PASSWORD_COMMAND`
  - `$RESTIC_PASSWORD_FILE`
  - `$RESTIC_PASSWORD`
- Key angeben (falls mehrere Keys) mittels:
  - `--from-key-hint`
  - `$RESTIC_KEY_HINT`

password-command und password-file

- `password-command`:
  - Gibt beim Aufruf nur das Passwort auf STDIN aus
  - Kann beliebig komplex werden:
    - PAM fragen
    - HashiCorp Vault fragen
    - LDAP fragen

```
$ ./Setec-Astronomy.sh
ganz&geHeim23!
```

password-command und password-file

- `password-file`:
  - Enthält das Passwort
  - Auf Zugriffsrechte achten!

```
$ cat Setec-Astronomy.txt
ganz&geHeim23!

$ ls -ld Setec-Astronomy.txt
-r-------- 1 ads ads 14 13. Feb 13:37 Setec-Astronomy.txt
```

Backup erneuern

```
$ du -sh wichtige-daten/
56M  wichtige-daten/

$ restic -r ~/repository --verbose backup --password-command=~/Setec-Astronomy.sh wichtige-daten/

open repository
repository 977eb753 opened (version 2, compression level auto)
using parent snapshot 148acc51
[0:00] 100.00%  1 / 1 index files loaded
scan finished in 0.003s: 60 files, 55.000 MiB

Files:          10 new,         0 changed,           50 unmodified
Dirs:                0 new,          1 changed,           0 unmodified
Data Blobs:     10 new
Tree Blobs:          2 new
Added to the repository: 5.023 MiB (5.005 MiB stored)

processed 60 files, 55.000 MiB in 0:00
snapshot 58213830 saved
```

Snapshots anzeigen

```
$ restic -r ~/repository --verbose --password-command=~/Setec-Astronomy.sh
snapshots

repository 977eb753 opened (version 2, compression level auto)
ID       Time                 Host         Tags     Paths            Size
-----------------------------------------------------------------------------
148acc51  2025-02-13 13:37:42  diamond     ~/wichtige-daten  50.000 MiB
58213830  2025-02-13 14:37:42  diamond     ~/wichtige-daten  55.000 MiB
-----------------------------------------------------------------------------
2 snapshots
```

Restic Befehle für Nutzer

- `backup`: Backup erstellen
- `snapshots`: Snapshots anzeigen
- `cat` (`blob`, `tree`, `snapshot`): Zeige Objekte
- `find`: Suche Dateinamen
- `dump`: Zeige Inhalt einer Datei
- `ls`: Zeige Dateien
- `list` (`snapshot`, `blobs`, `trees`, `packs`, `locks`): `snapshots` und `locks` sind wichtig
- `restore`: Backup wiederherstellen
- `tag`: Tagge einen Snapshot
- `mount`: Backup als Mountpoint bereitstellen

Restic Befehle für Admins

- `init`: Repository initialisieren
- `check`: Repository prüfen
- `forget`: Snapshot löschen (löscht keine Daten)
- `key (list, add, remove, passwd)`: Key Management
- `prune`: Löscht nicht mehr benötigte Daten
- `recover`: Stellt nicht referenzierte Daten wieder her
- `repair`: Repository reparieren
- `rewrite`: Dateien aus Snapshots löschen
- `stats`: Statistiken für Repository
- `unlock`: Locks anderer Prozesse löschen

Restic: mount

- Repository als Mountpoint
- Erlaubt Nutzung aller Linux-Befehle (`find`, `cp`, ...)
- Benötigt Fuse (Filesystem in Userspace)

Restic: mount - Backup öffnen

```
$ mkdir ~/restore
$ restic -r ~/repository --verbose --password-command=~/Setec-Astronomy.sh
mount ~/restore

repository 977eb753 opened (version 2, compression level auto)
[0:00] 100.00%  2 / 2 index files loaded
Now serving the repository at ~/restore
Use another terminal or tool to browse the contents of this folder.
When finished, quit with Ctrl-c here or umount the mountpoint.
```

Restic: mount - Backup anzeigen

```
$ ls -ld ~/restore/*

dr-xr-xr-x 1 ads ads 0 14. Feb 13:23 ~/restore/hosts
dr-xr-xr-x 1 ads ads 0 14. Feb 13:23 ~/restore/ids
dr-xr-xr-x 1 ads ads 0 14. Feb 13:23 ~/restore/snapshots
dr-xr-xr-x 1 ads ads 0 14. Feb 13:23 ~/restore/tags

$ ls -ld ~/restore/snapshots/*

dr-xr-xr-x 2 root root  0 13. Feb 13:37 ~/restore/snapshots/2025-02-13T13:37:00+01:00
dr-xr-xr-x 2 root root  0 13. Feb 14:37 ~/restore/snapshots/2025-02-13T14:37:00+01:00
lrwxrwxrwx 1 ads  ads  25 14. Feb 14:37 ~/restore/snapshots/latest -> 2025-02-13T14:37:00+01:00
```

Restic: mount - im Backup suchen

```
$ find ~/restore/snapshots/latest/ -type f
~/restore/snapshots/latest/wichtige-daten/file12
~/restore/snapshots/latest/wichtige-daten/file14
~/restore/snapshots/latest/wichtige-daten/file2

…
```

Ein Backup mit Restic

```
/usr/bin/mount /backup && /usr/bin/restic --repo=local:~/repository --
cache-dir=~/.cache/restic-cache --cleanup-cache --exclude-caches --
verbose --password-command=~/Setec-Astronomy.sh --exclude="~/wichtige-
daten/*.part" --exclude="~/wichtige-daten/.*-swp" --exclude-if-present
".nobackup" --host="workstation" --tag="daily-backup" --compression max
--ignore-inode --one-file-system --repo-version 2 backup ~/wichtige-
daten/ && /usr/bin/restic --repo=local:~/repository --cache-
dir=~/.cache/restic-cache --verbose --password-command=~/Setec-
Astronomy.sh check && /usr/bin/restic --repo=local:~/repository --cache-
dir=~/.cache/restic-cache --verbose --password-command=~/Setec-
Astronomy.sh list locks && /usr/bin/umount /backup
```

Was stört oder fehlt?

- Viele Parameter
- Mehrere Schritte
  - check
  - forget
  - prune
- Fehlt
  - Vorbereitende Scripte (einsammeln, mounten,...)
  - Metriken
  - Benachrichtigungen
- Regelmäßigkeiten (cron,..)
- …

Wunschziel

- `$tool backup`
- `$tool snapshots`
- `$tool mount`

Ja !

resticprofile

Überblick

- Wrapper um restic
  - Manager für Konfigurationsprofile
- Entwicklung: seit 2019
- Sprache: Go
- Lizenz: GPL-3.0
- Unterstützt
  - Linux
  - MacOS
  - Windows
  - (Open|Free)BSD
  - Solaris

Voraussetzungen

- `restic`
- config-file(s)
- Texteditor nach Wahl
  - Konfigurationsdateien

Installation

- Paket-Verwaltung
- GitHub

Konfiguration - Formate

- TOML
- YAML
- JSON
- HCL

- Empfehlung
  - TOML
  - YAML ←

Konfiguration - Minimum

- Repository
- Passwort
- Name des Profils
- Kommando
  - `backup`
- Parameter
  - Quelle (Pfade, Dateien,..)
  - Optional: Ausnahmen

Minimal-Konfiguration - profiles.yaml

```yaml
version: "1"
global:
  initialize: true
  restic-binary: "/usr/bin/restic"
default:
  repository: "local:./backup"
  password-file: "password.txt"
  password-command: "./Setec-Astronomy.sh"
  backup:
    verbose: true
    source:
      - "./wichtige-daten/"
```

Erstes Backup

```
$ resticprofile backup
2025/02/13 13:23:42 profile 'default': initializing repository (if not
existing)
. . .
created restic repository 9cf6203c29 at local:~/repository
2025/02/13 13:23:42 profile 'default': starting 'backup'
open repository
repository 9cf6203c opened (version 2, compression level auto)
no parent snapshot found, will read all files
[0:00]          0 index files loaded
scan finished in 0.002s: 50 files, 50.000 MiB

Files:          50 new,     0 changed,     0 unmodified
Dirs:            3 new,     0 changed,     0 unmodified
Data Blobs:     73 new
Tree Blobs:      4 new
Added to the repository: 50.020 MiB (50.011 MiB stored)

processed 50 files, 50.000 MiB in 0:00
snapshot 8ce08fbc saved
2025/02/13 13:23:42 profile 'default': finished 'backup'
```

Zweites Backup

```
$ resticprofile backup
2025/02/13 13:26:42 using configuration file: profiles.yaml
2025/02/13 13:26:42 profile 'default': initializing repository (if not existing)
2025/02/13 13:26:42 profile 'default': starting 'backup'
open repository
repository 9cf6203c opened (version 2, compression level auto)
using parent snapshot 8ce08fbc
scan finished in 0.003s: 60 files, 55.000 MiB

Files:          10 new,     0 changed,    50 unmodified
Dirs:            0 new,     3 changed,     0 unmodified
Data Blobs:     10 new
Tree Blobs:      4 new
Added to the repository: 5.024 MiB (5.006 MiB stored)

processed 60 files, 55.000 MiB in 0:00
snapshot b56b8de9 saved
2025/02/13 13:26:42 profile 'default': finished 'backup'
```

Backup anschauen - (1/2)

```
$ resticprofile snapshots
ID       Time                 Host  Tags  Paths              Size
-----------------------------------------------------------------------
8ce08fbc 2025-03-02 13:23:42  tux         ~/wichtige-daten  20.000 MiB
b56b8de9 2025-03-02 13:26:42  tux         ~/wichtige-daten  40.000 MiB
-----------------------------------------------------------------------
2 snapshots
```

Backup anschauen - (2/2)

```
$ resticprofile ls b56b8de9
snapshot b56b8de9 of [~/wichtige-daten] at 2025-03-02 13:26:42 +0100
CET by rainer@tux filtered by []:
~
~/wichtige-daten
~/wichtige-daten/file1
~/wichtige-daten/file10
~/wichtige-daten/file11
~/wichtige-daten/file12
.
.
.
```

Aufruf - Usage

- Bedient sich fast wie `restic`

```
resticprofile [resticprofile flags] [profile name.] restic-command [restic flags]
```

Restic Pass-through

```
$ resticprofile backup
$ resticprofile snapshots
$ resticprofile mount
$ resticprofile ls
$ resticprofile check
```

- Via Profil-Parameter
  - `forget`
  - `prune`

flags und commands

- `profiles.yaml`
  Standard
- Optional
  `-c Pfad/config-datei.yaml`
- `self-update`
  außerhalb Paketverwaltung
- `generate`
  `$ resticprofile generate --random-key > password.txt`

Aufräumen - Retention

```
retention:
  after-backup: true
  before-backup: false
  prune: true # default: false
  keep-daily: '7'
  keep-weekly: '4'
  keep-monthly: '6'
```

Weitere:

- keep-**within**-hourly
- keep-**within**-monthly
- keep-**within**-....
- keep-last
- ...

Scheduling

- systemd
- crond
- launchd
- Windows (geplante Aufgaben)

Schedule - Konfiguration

```
standard:
  description: 'Timer scheduled Profil'
  schedule: "12:30"
```

Format

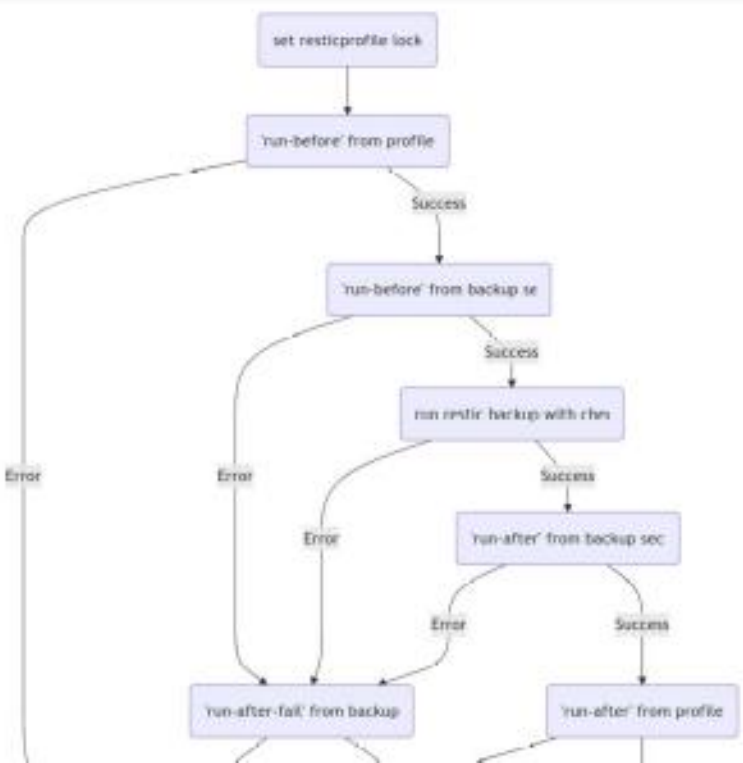
```
weekdays year-month-day hour:minute:second
```

```
  schedule:  "*:00,15,30,45"
```

```
$ resticprofile -n <Name des Profils> schedule
$ resticprofile -n standard schedule
```

Next Level - shell commands

- Shell Kommandos (jederzeit)
  - `run-before`
  - `run-after`
  - `run-after-fail`
  - `run-finally`



Next Level - Hooks

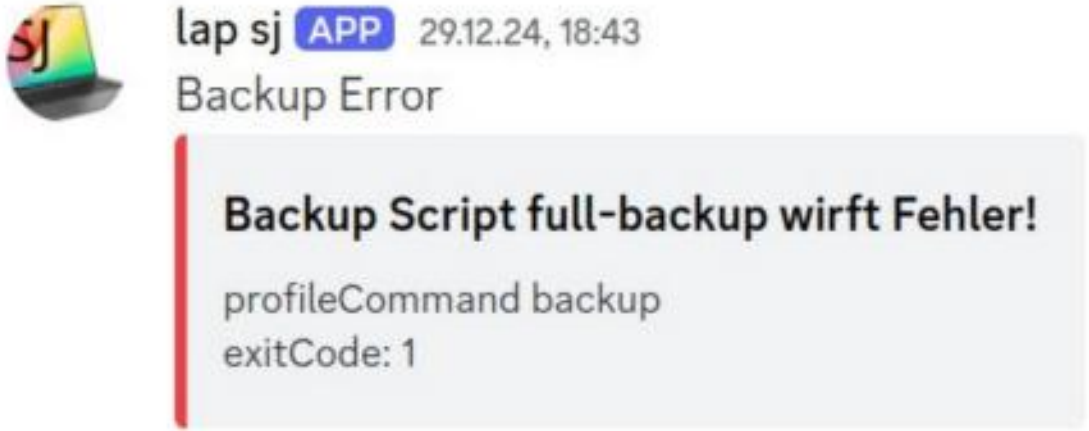
- HTTP-Hooks
  - send-before
  - send-after
  - send-after-fail
  - send-finally



Next Level - Hooks - Beispiel

Einsatz

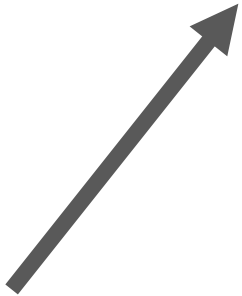
- Nix Prometheus => Discord-Message bei Fail
- Aussehen: `body-template`



Best Practices

resticprofile - Best Practices

- Auslagern über `includes:`
  - `/etc/resticprofile/profiles.d/`
  - `/etc/resticprofile/secrets/`
  - Dateisystem Berechtigungen!
    - `drwxr-x--- 4 root root`



Best Practices

- Passwort/Schlüssel sicher speichern!
- 3-2-1 Backups
  - 3 Kopien, 2 verschiedene Medien, eine Kopie liegt außerhalb
  - Nicht einfach das Backup per `rsync` kopieren!
- Regelmäßig Restore testen
  - Kosten und Dauer für komplettes Restore vorab berechnen
- Backup monitoren
- Cronjob einrichten
- Cache Dateien ignorieren (siehe: `CACHEDIR.TAG`)
- Retention einrichten
  - Vorgaben wie z. B. GDPR beachten

Ausblick

Ausblick - was dieser Vortrag nicht beinhaltet

- Gruppen und Vererbung
- Includes
- Tags
- Konfiguration von Remotes
- Random Keys
- Kopieren von Repositories
- Integration in Monitoring (Prometheus-Metriken)
- Update von Restic & resticprofile
- Dry-run
- Check-Parameter: Genug RAM vorhanden?
- Prevent from Sleep
- Alte LOCKs (Automatisches Löschen veralteter Locks)
- STDIN (Direkte DB-Dumps via Stdin)
- restic-rest-Server

Weitere Links

Links

- Restic Webseite: https://restic.net/
- Restic Code: https://github.com/restic/restic
- Restic Forum: https://forum.restic.net/
- resticprofile Code: https://github.com/creativeprojects/resticprofile
- resticprofile Webseite: https://creativeprojects.github.io/resticprofile/
- Slides: https://www.RainerRose.de/writings/
- Slides: https://andreas.scherbaum.la/writings/





Fragen?

The End - Danke schön!