BorgBackup – Verschlüsselung und SSH

Installation (Debian; Borg 1.x)

```
sudo apt update
```

```
sudo apt install borgbackup
```

Version prüfen:

```
borg --version
```

Versionshinweis: Die folgenden Befehle beziehen sich auf Borg 1.x. Borg 2.x verwendet teilweise andere Befehle und Repository-Formate.

Zwei unabhängige Sicherheitsebenen

BorgBackup kann Backup-Archive verschlüsseln. Bei einem entfernten Repository wird häufig zusätzlich SSH für Transport und Anmeldung verwendet. **Der SSH-Schlüssel ist nicht der Borg-Verschlüsselungsschlüssel.**

Repository-Verschlüsselung

Borg unterstützt verschiedene Verschlüsselungsmodi. Für neue Repositories sollte ein aktueller, zur installierten Borg-Version passender authentifizierter Verschlüsselungsmodus gewählt werden. Die genauen Optionen unterscheiden sich zwischen Borg 1.x und Borg 2.x.

Beispiel mit Borg 1.x

Die folgenden Befehle sind ausdrücklich für Borg 1.x formuliert. Sie verwenden ein lokales Test-Repository und erfordern eine sichere Passphrase:

Repository initialisieren (nur einmal):

```
borg init --encryption=repokey-blake2 /pfad/zum/test-repository
```

Archiv anlegen:

```
borg create /pfad/zum/test-repository::beispiel-001 /home/beispiel/Dokumente
```

Archive anzeigen:

```
borg list /pfad/zum/test-repository
```

Hinweis: Ein lokales Test-Repository ersetzt kein räumlich getrenntes Backup. Bei Borg 2.x sind Befehle und Repository-Verwaltung anders; die jeweilige Dokumentation beachten.

SSH für entfernte Repositories

Für unbeaufsichtigte Backups kann ein eigener SSH-Schlüssel mit eng begrenzten Berechtigungen verwendet werden. Der öffentliche Schlüssel wird auf dem Backup-Ziel hinterlegt. Wo möglich, sind serverseitige Einschränkungen für den Backup-Zugang sinnvoll.

Archiv wiederherstellen (Borg 1.x)

Zunächst ein leeres Zielverzeichnis erstellen:

```
mkdir -p ~/borg-wiederherstellung
```

In dieses Verzeichnis wechseln:

```
cd ~/borg-wiederherstellung
```

Danach das gewünschte Archiv in das aktuelle Verzeichnis extrahieren:

```
borg extract /pfad/zum/test-repository::beispiel-001
```

Die Entschlüsselung erfolgt bei gültigem Schlüsselmaterial und korrekter Passphrase automatisch. Vor einer Wiederherstellung die enthaltenen Pfade prüfen.

Voraussetzungen für die Wiederherstellung

Wesentlich sind Repository-Adresse, Borg-Version, Passphrase und – abhängig vom Verschlüsselungsmodus – gesicherte Schlüsselmaterialien. Ein Zugriff auf das Repository allein garantiert noch keine Entschlüsselung.

Sicherungsprüfung

Backups regelmäßig auf Vollständigkeit prüfen und testweise einzelne Dateien wiederherstellen. Ein erfolgreiches Backup-Protokoll ersetzt keinen Wiederherstellungstest.

Schlüssel und Löschschutz

Verschlüsselung schützt Vertraulichkeit, nicht automatisch vor Löschung oder Erpressung. Ein SSH-Zugang mit Schreib- und Löschrechten kann verschlüsselte Archive zerstören. Separate Rechte, Aufbewahrungsregeln und unabhängige Sicherungskopien sind wichtig.

Zurück zur Übersicht

From:
https://wiki.bluegnu.de/ - **wiki**

Permanent link:
https://wiki.bluegnu.de/doku.php/open:it:secure:borg

Last update: **2026/11/15 16:36**