**M143**

**Automatisiertes Bash-Backup-Script**

Luan Stauffer, Vladan Vranjes & Yanis Riedo

22.03.2024

Inhalt

[Einführung 1](#_Toc1596864866)

[Lizenzen & Hardware 1](#_Toc1452894323)

[Lizenzen 1](#_Toc1016455793)

[Hardware 1](#_Toc41637439)

[Disks 1](#_Toc405308657)

[Server / Firewall 1](#_Toc1181079444)

[Sicherheitsanforderungen 1](#_Toc417525268)

[Sicherheit gegen Angriffe 2](#_Toc2065033090)

[Sicherheit gegen Datenverlust 2](#_Toc1248242619)

[Zu sichernde Daten 2](#_Toc289656034)

[Was wird gesichert 2](#_Toc1768345361)

[Wo liegen die Daten 2](#_Toc875935057)

[Vertraulichkeit 2](#_Toc710654567)

[Datenwachstum (abgeschätzt) 2](#_Toc1259673374)

[Modalitäten 3](#_Toc1299561470)

[Speichermedien & Volllaufen 3](#_Toc54264446)

[Sicherungssoftware (LUAN-Ergänze) 5](#_Toc1134516126)

[Script 5](#_Toc1416678642)

[Anwendung 6](#_Toc2120300809)

[Aufbewahrung 6](#_Toc109379280)

[Verantwortung 6](#_Toc1181368503)

[Anleitung Backup 6](#_Toc1027590117)

[Anleitung Restore 7](#_Toc1564641345)

# Einführung

Wir nutzen Linux als unsere Plattform, bei der wir automatische Backups mit einem Bash-Skript durchführen. Dieses dient der Sicherung eines spezifischen Ordners, welcher heikle Daten beinhaltet (hier simuliert mit dem Randomfiles Programm).

# Lizenzen & Hardware

## Lizenzen

Ubuntu Server VMs: bereitgestellt von Cloud (OpenSource)

Randomfiles-Programm: Open-Source

Firewall VMs: Cloudintegriert

## Hardware

### Disks

|  |  |  |  |
| --- | --- | --- | --- |
| **Was** | **Anzahl** | **Kosten pro Stück** | **Total** |
| 512 GB SSD | 4 | 279.- | 837.- |
| 4 TB SSD | 3 | 72.90 | 291.60 |
| 20 TB HDD | 12 | 123.- | 1476.- |

Totalkosten: 2604.60

### Server / Firewall

Virtualisiert auf Cloud

* Webapp
* Firewall (VPN, FW-Rules, etc..)
* Kosten = Je nach Gebrauch / Skalierung

Backup Server

* Persönlicher Laptop Demnach Kosten = 0.-

# Sicherheitsanforderungen

Da wir mit schützenswerten Daten umgehen, müssen wir weitere Vorkehrungen beachten, damit man nicht gegen das Gesetz verstösst und / oder Daten an die Öffentlichkeit kommen.

Diese werden nämlich von Hackern besonders bevorzugt, da diese ein Chaos auslösen können.

Deswegen haben wir folgende Vorbeugungen getroffen.

## Sicherheit gegen Angriffe

* Intrusion Detection System [Snort](https://www.snort.org/) (oder sogar eins mit Prävention)
* Firewall Proxys und Regeln schärfen (nur gewollten Traffic zulassen)
* Netzabtrennungen mit Firewall
  + Internet
    - Snort Filtering Proxy
    - Ungenutzte Ports sperren
  + Intranet
    - Arbeitsplätze
    - Backup Server
    - Inbound: kein Zugriff vom Internet nach innen
    - Outbound: In alle Richtungen
  + DMZ
    - Webapp
    - Inbound: Von beiden netzen
    - Outbound: Von beiden Netzen

## Sicherheit gegen Datenverlust

* Schulung des Fachpersonals gegen Attacken (z.B. Phishing)
* Physische Abtrennung von Backupdisks (nirgendwo angeschlossen)
* Regelmässige Backups
  + Diese auch Testen!
* Sicherheit der Disketten garantieren
* Starke Passwörter verwenden und regelmässig wechseln

# Zu sichernde Daten

## Was wird gesichert

Es werden besonders schützenswerte Daten gesichert wie:

* Religiöse und politische Ansichten oder Tätigkeiten
* Daten über die Zugehörigkeit zu einer Rasse oder Ethnie

## Wo liegen die Daten

Die Daten befinden sich an 2 Orten:

* API-Server
* Disketten

## Vertraulichkeit

Die daten sind privat und werden auf achtsamer weise verarbeitet. Kundendaten, vor allem schützenswerte, müssen von Angriffen und unbefugten Zugriffen geschützt werden.

# Datenwachstum (abgeschätzt)

Da man nicht von Tag zu Tag seine Glaubensrichtung wechselt, bleibt pro Person der Datensatz etwa gleich. Deswegen hängt die Rate von der Anzahl der Personen ab, die die Webapp nutzen.

Die Datensätze sind in einer Tabelle von der Datenbank der Webapp. Demnach wird diese Tabelle gebackupt.

Ein Eintrag in eine SQL-Tabelle liegt etwa bei 200KB. Wenn pro Tag 500 Leute unsere Seite nutzen, dann kommen wir zu einem Wachstum von 100MB pro Tag. Das System der Webapp wird monatlich grösser anhand von Updates/ Verbesserungen. Rechnen wir dafür 200MB ein.

# Modalitäten

Für das Wechselschema nutzen wir GVS (Grossvater Vater Sohn), da dieses am besten für unser Konzept ist. Zudem brauchen Versionen bis zu vor einem Jahr.

Wir machen abends tägliche Backups mit insgesamt 19 Disketten mit je einem Ordner unterteilt.

Der Ausgangsordner wird abwechselnd auf die Disketten kopiert mit folgendem Schema:

* Täglich Inkrementellbackup auf vorheriges Wochen-Fullbackup (erstes Backup Full)
* Wöchentlich Jeden Montag ein Fullbackup (Statt Inkr. auf Tagesdisk)
* Monatlich Fullbackup (Jedes 4 Wochenbackup geht auf Monatsdisk)
* Jährlich Monatsdisken gehen in einem Kreislauf.

Backups erfolgen immer um 23:00, damit beim Hotbackup sich die Datensätze möglichst nicht verändern währenddessen.

# Speichermedien & Volllaufen

19 Disketten total. Davon:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Speicherplatz** | **Anz.** | **Form** | **Leserate** | **Schreibrate** | **Zeit ca.** | **Link** | |
| 500 GB | 4 Tage | SSD | 1050MB/s | 1000MB/s | 1 Sek. | [Link](https://www.digitec.ch/de/s1/product/sandisk-extreme-portable-500-gb-externe-ssd-13951674) |
| 4 TB | 3 Wochen | SSD | 1050MB/s | 1000MB/s | 1-20 Min. | [Link](https://www.digitec.ch/de/s1/product/sandisk-extreme-portable-4000-gb-externe-ssd-14594598?supplier=406802&utm_source=google&utm_medium=cpc&utm_campaign=PROD_CH_PMAX_CSS_Cluster_9&campaignid=20501673545&adgroupid=&adid=&dgCidg=EAIaIQobChMIqKv5qfKHhQMVoIjCCB1wigcVEAQYAiABEgIqvvD_BwE&gad_source=1&gclid=EAIaIQobChMIqKv5qfKHhQMVoIjCCB1wigcVEAQYAiABEgIqvvD_BwE&gclsrc=aw.ds) |
| 20 TB | 12 Monate | HDD | 500MB/s | 500MB/s | Ab 20 Min. | Link |

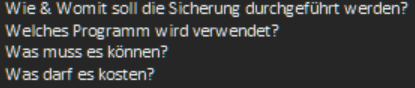
Mit einer Wachstumsrate von 3200 MB/ Monat, würde es etwa:

* Unendlich lange dauern, bis die Tagesdisk voll ist, da diese nur Inkremetelle macht
* 1’250 Monate dauern, bis die Wochendisk voll ist
* 6’250 Monate, bis die Monatsdisk voll ist.

# Sicherungssoftware (LUAN-Ergänze)

Kompression mit Zip

Backup mit Rsync



# Script

Das Script muss auf dem Backupserver hinterlegt sein und auf dem Applikationsserver muss ein Ordner namens Data vorhanden sein.

## Anwendung

* Skript in eine nano-datei mit der Endung .sh
* Skript speichern
* “sudo chmod a+x filename.sh” ausführen
* Ordner namens Data auf dem Applikationsserver einrichten.
* Mit “./filename.sh” Skript ausführen

# Aufbewahrung

Disks werden nur angeschlossen, wenn sie benötigt werden, damit sie auch eine physische Trennung haben gegen Datenverlust.

Die Disketten werden in separat abgeschlossenen, isolierten Schränken aufbewahrt und beschriftet mit Backupdatum. So werden sie weder schnell altern noch versehentlich vertauscht.

Die Daten müssen sicher aufbewahrt werden da sie Sensibel sind, deswegen befinden sich die oben genannten Schränke in einem abgeschlossenen Raum mit limitiertem Zugriff zu den Personen, die für die Backups zuständig sind.

# Verantwortung

Die Verantwortung wird auf 4 Personen verteilt. Je 2 hauptbeauftragte die dies als ihre Aufgabe ausführen und 2 die einspringen können, falls die vorher genannten gehindert an der Aufgabe sind. So kann man in jedem Fall auch das 4 Augen Prinzip anwenden. Dabei ist einer der Hauptausführende und spricht jeden Schritt vor sich, während die andere Person aufmerksam zuschaut und hört.

# Anleitung Backup

1. **Vorbereitung des Servers:**

Stelle sicher, dass der Server, auf dem du das Backup spielen möchtest, korrekt eingerichtet ist und über genügend Speicherplatz verfügt, um das Backup zu halten.

1. **Auswahl der Backup-Methode:**

Wir verwenden ein automatisiertes Backup Script mit rsync für dieses Backup.

1. **Erstellung des Backups:**

Führe ein Backup deiner Daten auf deinem lokalen System durch. Dies kann je nach Größe und Art der Daten unterschiedlich lange dauern.

1. **Übertragung des Backups auf den Server:**

Wenn du ein manuelles Backup durchführst, nutze am besten ein Tool wie rsync oder scp. So kannst du den folgenden Befehl verwenden, um das Backup auf den Server zu übertragen:

rsync -avz benutzername@server\_ip:/pfad/zur/webapp /pfad/zum/lokalen/backupordner/

1. **Überprüfung der Übertragung:**

Überprüfe, ob das Backup erfolgreich auf den Server übertragen wurde, indem du dich auf den Server einloggst und den Speicherort des Backups mit der md5summe überprüfst.

1. **Überwachung und Wartung:**

Überwache regelmäßig die Backup-Prozesse, um sicherzustellen, dass sie wie geplant funktionieren und auch den verfügbaren Speicherplatz auf dem Server, um sicherzustellen, dass genügend Platz für zukünftige Backups vorhanden ist.

# Anleitung Restore

1. **Vorbereitung des Servers:**

Stelle sicher, dass der Server, auf den du das Backup wiederherstellen möchtest, korrekt eingerichtet ist und über genügend Speicherplatz verfügt, um das Backup zu halten.

1. **Auswahl der Backup-Dateien:**

Entscheide, welche Backup-Dateien du wiederherstellen möchtest. Abhängig von deinem Backup-Verfahren könnten dies alle Daten oder nur bestimmte Dateien und Ordner sein.

1. **Transfer des Backups auf den Server:**

Übertrage das Backup von seinem Speicherort auf den Server, falls es nicht bereits dort gespeichert ist. Dies kann über FTP, rsync, scp oder ein ähnliches Protokoll erfolgen.

1. **Entpacken des Backups (falls erforderlich):**

Falls das Backup komprimiert oder archiviert ist, entpacke es auf dem Server in einen temporären Ordner. Verwende dafür geeignete Befehle wie tar für Tar-Archive oder unzip für ZIP-Archive.

1. **Wiederherstellung der Daten:**

Navigiere zu dem Verzeichnis, in dem sich die wiederherzustellenden Daten befinden.

Verwende geeignete Befehle oder Tools, um die Daten aus dem Backup in die richtigen Verzeichnisse auf dem Server zu extrahieren oder zu kopieren. Dies könnte einfach das Kopieren von Dateien und Ordnern sein oder das Ausführen spezifischer Befehle je nach Backup-Format.

1. **Überprüfung der Wiederherstellung:**

Überprüfe, ob die wiederhergestellten Daten korrekt auf dem Server platziert wurden.

Vergewissere dich, dass keine Fehler während des Wiederherstellungsprozesses aufgetreten sind.

1. **Testen der Wiederherstellung:**

Teste die Funktionalität der wiederhergestellten Daten, indem du sicherstellst, dass alle relevanten Dienste oder Anwendungen ordnungsgemäß funktionieren.