

1 Teilnehmer/innen des Teams:

Klasse: AP23b	Team: Cédric Ackermann, Silvio Brändle
------------------	---

2 Anforderungsdefinition (Meilenstein A)

Bombackup

Fachlicher Inhalt:
(Allgemeine Beschreibung)

Kundennutzen: Mit dem Skript sollen die Benutzer ihre Ordner sichern können und diese wiederherstellen, im Falle eines Datenverlustes.

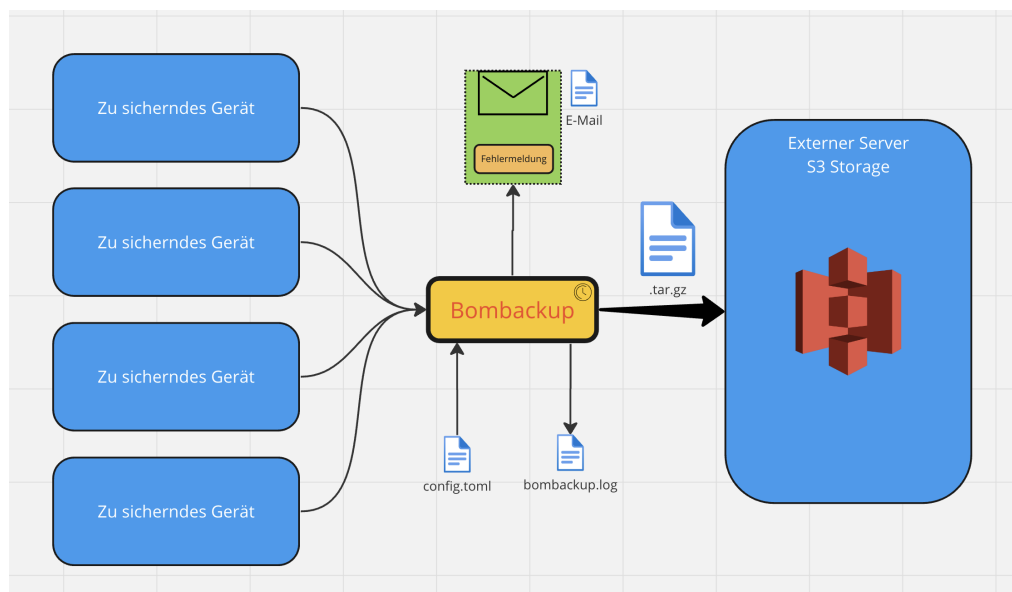
Setup und Automation:

Der Kundenserver / -dienst sind die einzelnen Geräte, von denen ein Backup erstellt wird.

Das Skript verarbeitet die Daten zu einer komprimierten Backup-Datei, welche auf einem externen Server hochgeladen wird.

Details:

- Konfiguration (.toml): Konfiguration von Geräten und Ordnern, externer Speicherdienst, Backup-Intervall und Fehlerbehandlung
- Get-Prozedur (Ordner): Anfrage Ordnern, die zu Sichern sind
- Verarbeitung (process): Verpackung und Komprimierung in eine Datei
- Weiterreichung (.tar.gz): Sicherung auf einem externen Server und evt. Dashboard für eine Übersicht auf das System
- Sicherheitsaspekte: Zugriff auf Backups nur mit Autorisation



Erkenntnisse aus der Machbarkeitsabklärung in Python:

Folgende Features sind vorab untersucht worden und die Umsetzung wurde sichergestellt:

	<ul style="list-style-type: none"> • .toml Dateien können mit der Python Library "toml" ausgelesen und geschrieben werden. • Zugriff auf den S3 Speicher wird durch das AWS SDK "boto3" ermöglicht. • Mit dem "tarfile" Modul kann einen Ordner als komprimierte Datei gespeichert werden. • Mittels dem Courier Service können Mails versendet werden. (Python Library "courier-python")
MUSS Kriterien: (Konkrete Features, die umzusetzen sind)	Folgende Features sollen implementiert werden, um einen produktiven Ablauf sicherzustellen: <ul style="list-style-type: none"> • Hauptskript ist zuständig für Konfigurationsänderungen und Überwachung. • Ein Backupskript wird entweder von geplanten Cronjob oder direkt vom Hauptskript ausgeführt. • Die Backups werden komprimiert und als eine Datei auf einem externen Server abgespeichert. • Beim Auftreten von Fehlern wird eine E-Mail an die konfigurierte Adresse geschickt. • Es können mehrere Geräte konfiguriert und gesichert werden. • Statusupdates und generelle Informationen werden in einem Logfile protokolliert.
KANN Kriterien: (Konkrete Features, die optional sind)	Folgende Features können zusätzlich implementiert werden: (Varianten, Kreativität): <ul style="list-style-type: none"> • Der Benutzer hat Zugriff auf ein Dashboard, auf dem er einen Überblick auf die Statusinformationen bekommt. • Auf dem Dashboard kann man Backups manuell auslösen. • Ein gescheitertes Backup wird nach 10 Minuten erneut versucht. • Wiederherstellung kann mit einem Button direkt ausgelöst werden. • Die Backup-Datei kann zusätzlich verschlüsselt werden.

3 Betriebsdokumentation

3.1 Installationsanleitung für Administratoren

3.1.1 Voraussetzungen

Bevor die Installation von Bombbackup erfolgen kann, müssen folgende Programme installiert sein:

- git
- python3.10
- python3.10-venv

3.1.2 Anleitung

- GitHub Repository herunterladen mit:

```
git clone https://github.com/cediackermann/m122-bombbackup.git
cd m122-bombbackup
```
- Danach muss die virtuelle Python-Umgebung initialisiert werden:

```
python 3 -m venv .venv
source .venv/bin/activate
pip install -r requirmenets.txt
```
- Folgende Abschnitte gehören auch noch dazu:
 - 3.1.3
 - 3.1.4
 - 3.1.5

3.1.3 Google Account für Email aufsetzen

- Gmail-Account auf <https://accounts.google.com/signup> erstellen
- E-Mail adresse in der Konfigurationsdatei unter email angeben

3.1.4 AWS S3 Bucket aufsetzen

- Amazon AWS Account auf <https://aws.amazon.com/> erstellen
- Bucket erstellen auf <https://s3.console.aws.amazon.com/s3/home>
- Bucket-name in der Konfigurationsdatei notieren
- Erstellen Sie eine neue Policy in Amazon IAM:
<https://console.aws.amazon.com/iam/home#/policies>
Wählen Sie zuerst S3 als Service aus, unter «Actions allowed» «All S3 actions» und unter «Resources» «All».

- Erstellen Sie einen neuen Benutzer:
<https://us-east-1.console.aws.amazon.com/iam/home#/users>
 Bei «Permissions options» wählen Sie «Attach policies directly». Bei «Permissions policies» suchen Sie nach der zuvor erstellten Policy und fügen Sie sie hinzu.
- Gehen Sie in die Detailsansicht des zuvor erstellten Benutzers. Im Tab «Security credentials» gibt es einen Abschnitt «Access keys». Erstellen Sie einen Access Key mit dem «Third-party service» Use case. Sie sollten nun Zugriff auf die Access key ID und Secret access key haben.
- Ergänzen Sie die key_id und den access_key in der Konfigurationsdatei.

3.1.5 Konfigurationsdatei

In der Konfigurationsdatei config.toml müssen folgende Dinge konfiguriert werden:

Email:

- courier_token
- email_address
- log_level

Storage:

- type
- bucket
- access_key
- secret_key

Logging

- log_level
- log_file

Geräte:

- type
- host
- user
- password
- remote_dir
- cron_schedule

3.2 Bedienungsanleitung für Benutzer

Siehe Abschnitt 3.1.5 für die Konfiguration. Um ein zu sicherndes Gerät hinzuzufügen, muss SSH für das Gerät aufgesetzt sein. Die Webseite <https://crontab.guru/> erleichtert das Schreiben von Cron Schedules.