Nutzerdatenbank laden / hashen / prüfen

Nutzerdatenbank laden / hashen

Für das Laden und ggf. Rehashen der Nutzerdatenbank (`users.toml`) kann folgendes Script genutzt werden. Es prüft zunächst, ob die Konfiguration `bffh.dhall` von BFFH valid ist. Wenn nicht, wird nichts unternommen. Im Anschluss werden die Nutzer neu geladen und anschließend in die gleiche Datei **optional** wieder exportiert, um etwaige unverschüsselte Passwörter automatisch zu hashen. BFFH prüft beim Laden die users.toml auf Syntaxfehler. Wem diese Checks nicht ausreichen, der kann sich dem erweiteren Validator-Script widmen,

> Hinweis: Das Script basiert auf einem auf dem System aktiven **systemd** Service namens `bffh.service`

```
mkdir -p /opt/fabinfra/scripts/
vim /opt/fabinfra/scripts/bffh-load-users.sh
```

```
#!/bin/bash
#check config
BFFHD="/usr/bin/bffhd"
DATA="/etc/bffh"
CFG="$DATA/bffh.dhall"
USERS="$DATA/users.toml"

while [[ $# -gt 0 ]]; do
  case $1 in
    -h|--help)
      echo "-h|--help   - show help"
      echo "-r|--rehash - overwrite users.toml with hashed passwords (ensure secure secrets)"
      exit 1
      ;;
    -r|--rehash)
      REHASH="y"
      shift
      ;;
```

```
□□-*)
□□□;;
□esac
done

echo "use -h|--help to show additional script options!"

$BFFHD --check --config $CFG > /dev/null
if [ $? == 0 ]; then
□#pre-check bffh.dhall
□echo "Config is valid. Loading users ..."
□$BFFHD --verbose --config $CFG --load-users=$USERS

□if [ $? == 0 ]; then
□□#then load users.toml
□□$BFFHD --verbose --config $CFG --dump-users /tmp/users.toml --force
□else
□□echo "Error: Newly given users.toml is invalid!"
□□exit 1
□fi

□#if this was successful and service is running, restart it, else do nothing
□if [ $? == 0 ]; then
□□if [[ $REHASH == "y" ]]; then #overwrite users if --rehash option is given (not null)
□□□echo "Rehasing users.toml!"
□□□cat /tmp/users.toml > $USERS
□□□rm /tmp/users.toml
□□fi
□□FAS="bffh.service"
□□STATUS="$(systemctl is-active $FAS)"
□□if [ "${STATUS}" = "active" ]; then
□□□echo "restarting $FAS"
□□□systemctl restart $FAS
□□else
□□□echo -e "\n\n$FAS not active/existing. Not restarting bffh service!"
□□fi
□fi

else
□echo "Error: Currently loaded users.toml is invalid!"
```

```
exit 1
fi
```

```
chmod +x /opt/fabinfra/scripts/bffh-load-users.sh
```

Nutzerdankenbank prüfen (users.toml validator)

Ein Python-Script erlaubt die Auswertung einer `users.toml` Datei mit folgenden Features:

- zählt die Nutzer und deren zugewiesene Rollen
- überprüft auf Duplikate bei Nutzernamen, Passwörtern und Cardkeys
- validiert Passwörter auf Verschlüsselung (Argon2)
- validiert eventuell vergebene Cardkeys (UUID)
- gibt Hinweise bei möglichen Datenbankfehler (z.B. falsche Datentypen)
- erzeugt eine Statistik über die Verwendung von Passwörtern, Cardkeys und Rollen

> Das Script benötigt mindestens Python 3.11. Erst ab dieser Version wird `tomllib` unterstützt!

Tool installieren:

```
cd /opt/fabinfra/tools/
git clone https://github.com/vmario89/fabaccess-users-toml-validator.git
```

Benutzen:

```
python3 /opt/fabinfra/tools/fabaccess-users-toml-validator/validate.py
```

> Über den optionalen Parameter `--db /opt/fabinfra/bffh-data/config/users.toml` kann auch eine andere Benutzerdatenbankdatei an Stelle der Standarddatei `/etc/bffh/users.toml` angegeben werden!

Fehlermeldungen und deren Bedeutung

Invalid initial character for a key part (at line x, column y)

Möglicher enthält der Benutzername Sonderzeichen wie Umlaute und ist nicht in Hochkommas geführt. In diesem Falle bricht das Script ab. `[Ö]` ist kein gültiger Benutzername, `["Ö"]` schon.

Version #30
Erstellt: 2024-11-14 16:33:57 CET von Mario Voigt (Stadtfabrikanten e.V.)
Zuletzt aktualisiert: 2025-03-11 11:01:17 CET von Mario Voigt (Stadtfabrikanten e.V.)