Hochschule Harz
Rechenzentrum

Serverzertifikate automatisiert verwalten ACME / Certbot

Stand: 24.06.2025

Mit der neuen CA von Harica ist es möglich Zertifikate automatisiert mittels ACME-Protokoll erstellen zu lassen.

Beispiele für unterstützte Clients: certbot, acme.sh oder win-acme

ACME- Account beantragen

Beim Rechenzentrum können die Zugangsdaten per E-Mail beantragt werden. Dazu schicken Sie einfach eine formlose E-Mail mit der FQDN des Servers an ca@hs-harz.de. Sie bekommen dann die notwendigen Werte für das externe Accountanbindung (eab-kid, eab-hmac-key und HaricaAcme Server) zugeschickt.

Lokale Installation z.B. certbot

Red Hat 8

```
yum install epel-release
yum install certbot python2-certbot-apache
```

Debian

```
apt install certbot
```

Zertifikatsverwaltung mit certbot

Zertifikat erstellen

```
# certbot certonly --standalone --non-interactive --agree-tos --email <admin.mail@b-tu.de> --server <sectigo_server> --eab-kid <Wert von EAB-KID> --eab-hmac-key <Wert von EAB-HMAC-KEY> --domain <FQDN des Servers>
```

Mit den Werten von eab-kid und eab-hmac-key sind so umzugehen, wie mit dem privaten Schlüssel vom Zertifikat. Wenn certbot das erste Zertifikat heruntergeladen und sich beim Server registriert hat, werden beide Werte nicht mehr benötigt. certbot speichert sich die Anmeldedaten für das Zertifikat im dazugehörigen Account. Die Accountdaten sind deshalb zu schützen.

Die aktuellen Zertifikate sind dann unter /etc/letsencrypt/live/<FQDN des Servers>/ zu finden und können direkt verlinkt werden.

Unter dem Verzeichnis /etc/letsencrypt/live/FQDN des Serverzertifikats + Kette abgelegt. Unter dem Verzeichnis */etc/letsencrypt/account/ wird ein entsprechender LetsEncrypt-Account angelegt.

Das Zertifikat in die WebServer-Config eintragen.

Zertifikat erneuern

```
# certbot renew --standalone --non-interactive --agree-tos --server <server>
```

Renew kann regelmäßig, zum Beispiel per Cronjob, aufgerufen werden. Certbot prüft daraufhin alle installierten Zertifikate auf Ihre Laufzeit. Zertifikate mit einer verbleibenden Laufzeit von weniger als 30 Tagen werden aktualisiert.

Zertifikat erneuern obwohl es noch nicht abgelaufen ist

```
# certbot certonly --standalone --non-interactive --agree-tos --email <mailadresse> --eab-kid <eab-kid-ID> --eab-hmac-key <eab-hmac-key> --server <server> --domain <FQDN> --force-renewal
```

Zertifikat sperren

```
# certbot revoke --cert-path <Pfad zum zu sperrenden Zertifikat> --server <server>
```

Bei Fragen und Problemen stehen wir Ihnen gern zur Verfügung.
Ihr HS-Harz-CA Team