

[zurück](#)

Certbot - Grundlagen und Beispiele

Diese Seite erklärt die Nutzung von 'Certbot', dem offiziellen ACME-Client von Let's Encrypt, zur automatisierten Beantragung und Erneuerung von TLS-Zertifikaten.

Was ist Certbot?

Ein Kommandozeilen-Tool zur Interaktion mit Let's Encrypt

Unterstützt HTTP-01 und DNS-01 Challenges

Kann Webserver wie Apache oder NGINX automatisch konfigurieren

Installation (Beispiel: Debian/Ubuntu)

Für Apache:

```
sudo apt install python3-certbot-apache
```

Für reine Zertifikatserzeugung (ohne Webserver-Plugin):

```
sudo apt install certbot
```

Zertifikat ausstellen (HTTP-Challenge)

Für Apache oder NGINX:

```
sudo certbot -nginx -d example.com -d www.example.com
```

Nur Webroot (z. B. bei Reverse Proxies):

```
sudo certbot certonly -webroot -w /var/www/html -d example.com
```

Zertifikat anzeigen

```
sudo certbot certificates
```

Automatische Erneuerung testen

```
sudo certbot renew -dry-run
```

Die automatische Erneuerung erfolgt i. d. R. via Cronjob oder Systemd-Timer.

DNS-01 Challenge (für Wildcard-Zertifikate)

Beispiel mit Cloudflare:

```
sudo certbot -d '*.example.com' --authenticator dns-cloudflare --dns-cloudflare-credentials ~/secrets\(cf.ini\) --installer nginx
```

Tipps

Certbot prüft standardmäßig vorzeitig ablaufende Zertifikate und erneuert nur bei Bedarf
-dry-run hilft bei Testläufen, ohne echte Zertifikate zu erzeugen

Häufige Fehler

too many certificates → Rate-Limit von Let's Encrypt erreicht

unauthorized → Challenge konnte nicht validiert werden

Port 80/443 nicht offen → Firewall oder Router prüfen

Siehe auch

[Let's Encrypt + ACME mit Traefik](#)

[Grundlagen zu TLS & SSL](#)

From:

<http://wiki.nctl.de/dokuwiki/> - **Veni. Vidi. sudo rm -rf / vici.**

Permanent link:

http://wiki.nctl.de/dokuwiki/doku.php?id=linux:certbot_grundlagen

Last update: **02.08.2025 14:10**

