LETSENCRYPT

Doku: http://letsencrypt.readthedocs.io/en/latest/using.html#apache

Ausgestellte Zertifikate zeigen

```
root@devel:/etc/letsencrypt# certbot certificates
Saving debug log to /var/log/letsencrypt/letsencrypt.log

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
Found the following certs:
  Certificate Name: devel.netzwissen.de
    Domains: devel.netzwissen.de gitea.netzwissen.de hugo.netzwissen.de
    Expiry Date: 2021-09-25 06:10:15+00:00 (VALID: 56 days)
    Certificate Path:
/etc/letsencrypt/live/devel.netzwissen.de/fullchain.pem
    Private Key Path: /etc/letsencrypt/live/devel.netzwissen.de/privkey.pem
  Certificate Name: devel.netzwissen.de_old
    Domains: devel.netzwissen.de gitea.netzwissen.de hugo.netzwissen.de
    Expiry Date: 2021-09-25 06:10:15+00:00 (VALID: 56 days)
    Certificate Path:
/etc/letsencrypt/live/devel.netzwissen.de/fullchain.pem
    Private Key Path: /etc/letsencrypt/live/devel.netzwissen.de/privkey.pem
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
```

Zertifikate ergänzen

The way to add a domain with Certbot is to **reissue the certificate with a complete list of all of the names that should be covered in the new certificate**. There’s no command that adds a domain without the need to respecify the old names.

Zertifikate löschen

```
certbot delete
```

Zu viele Logfiles, daher "out of inodes"

https://community.letsencrypt.org/t/so-many-logfiles/32849

"As your distro uses systemd there is no need to remove /etc/cron.d/certbot, it executes nothing if it detects that systemd is working on your system but you can remove it, no problem. To stop/disable the certbot systemd timer.

```
systemctl stop certbot.timer
systemctl disable certbot.timer
```

And to be sure that in case a new debian certbot update doesn't activate certbot.timer again you could mask the certbot.timer.

```
systemctl mask certbot.timer
```

This mask creates a symlink from /etc/systemd/system/certbot.timer to /dev/null and this timer will run nothing. Cheers, sahsanu"

Als regelmässiger Job, um die Zertifikate zu prüfen, reicht ein cron.weekly Aufruf

```
#!/bin/sh
certbot renew
```

LetsEncrypt für Mailserver nutzen

Siehe auch https://kofler.info/lets-encrypt-zertifikate-fuer-web-und-mail-unter-ubuntu-16-04/

Let's-Encrypt-Zertifikate sind grundsätzlich universell verwendbar. Allerdings muss man für die passenden Hostnamen des SMTP- und IMAP-Servers entsprechende Zertifikate anfordern. Also z.B. für mail.meine-domain.de oder imap.meine-domain.de. Der Befehl dafür lautet

```
''certbot --apache --staging -d www.meine-domain.de
  -d meine-domain.de -d imap.meine-domain.de
  -d smtp.meine-domain.de''
```

Mit –staging werden Fake Certs angelegt. Wenn alles funktioniert, den Schalter weglassen! Danach die Configs von postfix und dovecot auf den neuen Cert Pfad anpassen (''/etc/letsencrypt/live/www.meine-domain.de/...). Falls dieser Fehler kommt

```
Client with the currently selected authenticator does not support any
combination of challenges that will satisfy the CA.
```

braucht man einen anderen Authentikator:

```
certbot --authenticator standalone --installer apache -d mail.miteinander-
esslingen.de --pre-hook "service apache2 stop" --post-hook "service apache2
start"
```