Let's Encrypt Certbot

The following walk through works on Debian 9, 10, and 11.

Installation

1. Install snapd

```
sudo apt update
sudo apt install snapd
sudo snap install core
sudo snap refresh core
```

2. Remove previously installed certbot packages

```
sudo apt remove --purge certbot
sudo rm /usr/local/bin/certbot-auto
```

3. Remove certbot renewal entry in crontab
4. Install certbot through snap

```
sudo snap install --classic certbot
sudo ln -s /snap/bin/certbot /usr/bin/certbot
```

5. Test automatic renewal

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

6. Check that the certbot renewal service has been set up

```
systemctl list-timers
```

Maintenance

- If you have existing SSL VirtualHost definitions you need to copy a certificate from another site or webserver to /etc/letsencrypt/live and point the certificate in the virtual host file to that certificate before starting/restarting apache. This is necessary for certbot to run, and certbot will later replace the certificate with a valid one.
- Run certbot and register sites:

```
certbot
```

- Check certificates:

```
certbot certificates
```

- Add domains to certificate:

```
certbot --expand -d example.com,www.example.com,click.example.com
certbot certonly --webroot --agree-tos -w /srv/www/letsencrypt/ --
expand -d example.com,www.example.com,click.example.com
```

- Revoke and optionally delete certificate:

```
certbot revoke --cert-path /etc/letsencrypt/live/example.com/cert.pem
```

- Delete certificate:

```
certbot delete --cert-name www.example.com
```

- Delete listed domains:

```
certbot delete
```

- Remove and/or add domains from existing certificate:

```
certbot certonly --force-renew --cert-name mycertificate.com -d
remove.mycertificate.com -d add.mycertificate.com
```

- Remove domain from certificate:
  1. Delete certificate where domain is listed in
  2. Change all apache conf files for the remaining domains in the deleted certificate to another certificate which is active
  3. Recreate the certificate for the remaining domains

     ```
     certbot -d example.com -d example.net
     ```

- All sites must be accessible through port 80 when renewing certificates.

Disable

- Comment the 2 *OnCalendar* lines in file `/etc/systemd/system/snap.certbot.renew.timer` which removes the times set when certbot is called

```
$ sudo vim /etc/systemd/system/snap.certbot.renew.timer
[Timer]
Unit=snap.certbot.renew.service
# OnCalendar=*-*-* 08:46
# OnCalendar=*-*-* 15:37
```

OUTDATED: Crontab

- Root

```
$ sudo crontab -e
35 3 * * 6 certbot renew && /etc/init.d/apache2 restart
```

Links

- certbot instructions: Apache on Debian 10
- Uninstalling certbot-auto
- How do I disable auto-renew without removing config files?
- Load Balancers

From:
https://wiki.condrau.com/ - **Bernard's Wiki**

Permanent link:
https://wiki.condrau.com/deb11:certbot

Last update: **2023/03/06 12:39**