Managing Certificates

These Instructions are for an ubuntu installation with nginx as the server. This method enables a user to get (free) certificates from an opensource provider and requires the website name to be publicly accessible. These instructions may not be applicable in other environments. Follow all applicable certificate policies when installing.

Instructions for creating and renewing a certificate are here.

Before obtaining the certificates ensure that there are two DNS A record for the website name (i.e. demonodepublicdns).

Getting the Certificates (letsencrypt example):

Certification Example

```
root@ubuntu:~# sudo apt-get update
root@ubuntu:~# sudo apt-get -y install nginx
root@ubuntu:~# wget https://dl.eff.org/certbot-auto
root@ubuntu:~# chmod a+x certbot-auto
root@ubuntu:~# ./certbot-auto
root@ubuntu:~# ./certbot-auto certonly --webroot -w /usr/share/nginx/html -d demonodepublicdns

                                                        Enter email address (used
                                                        for urgent notices and
                                                        lost key recovery)

                                                        xxxx@xxxx.xx


                                                          <  OK  >  <Cancel>


                                        Please read the Terms of Service at
                                        https://letsencrypt.org/documents/LE-SA-v1.1.1-August-1-2016.pdf.
                                        You must agree in order to register with the ACME server at
                                        https://acme-v01.api.letsencrypt.org/directory

                                                        <Agree >          <Cancel>



IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at
   /etc/letsencrypt/live/demonodepublicdns/fullchain.pem. Your cert
   will expire on 2016-09-29. To obtain a new or tweaked version of
   this certificate in the future, simply run letsencrypt-auto again.
   To non-interactively renew *all* of your certificates, run
   "letsencrypt-auto renew"
 - If you like Certbot, please consider supporting our work by:
   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
root@ubuntu:/opt/letsencrypt# ls /etc/letsencrypt/live/demonodepublicdns/
cert.pem  chain.pem  fullchain.pem  privkey.pem
```

Renewing the Certificates:

Renewing the Certificates on a DATIM Global

- Renew the certificates on global server

Renewing certificates on Global

```
maurya@test3:~$ chmod a+x certbot-auto
maurya@test3:~$ wget https://dl.eff.org/certbot-auto
maurya@test3:~$ sudo ./certbot-auto --config /etc/letsencrypt/configs/test3.global.ohie.datim.org.conf
certonly
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Cert is due for renewal, auto-renewing...
Renewing an existing certificate
Performing the following challenges:
http-01 challenge for test3.global.ohie.datim.org
Using the webroot path /usr/share/nginx/html for all unmatched domains.
Waiting for verification...
Cleaning up challenges
Unable to clean up challenge directory /usr/share/nginx/html/.well-known/acme-challenge
Generating key (4096 bits): /etc/letsencrypt/keys/0001_key-certbot.pem
Creating CSR: /etc/letsencrypt/csr/0001_csr-certbot.pem
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at
   /etc/letsencrypt/live/test3.global.ohie.datim.org/fullchain.pem.
   Your cert will expire on 2017-05-14. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot-auto
   again. To non-interactively renew *all* of your certificates, run
   "certbot-auto renew"
 - If you like Certbot, please consider supporting our work by:
   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
maurya@test3:~$ sudo vim nginx.conf
maurya@test3:~$ sudo vim /etc/nginx/nginx.conf
maurya@test3:~$ sudo vim /etc/nginx/sites-available/openhim-console
maurya@test3:~$ sudo service nginx restart
 * Restarting nginx
nginx
[ OK ]
maurya@test3:~$ sudo restart openhim-core
openhim-core start/running, process 963
```

- Replace these with the certificates in OpenHIM Certificates tab
- Replace these with the certificates in OpenHIM clients

Renewing the Certificates on a DATIM node

- Renew the certificates on node server
- Enable default nginx from sites-available and disable datim and openhim-console.

Renew Certificate for node

```
maurya@ls:~$ wget https://dl.eff.org/certbot-auto
--2017-02-14 15:54:52--  https://dl.eff.org/certbot-auto
Resolving dl.eff.org (dl.eff.org)... 173.239.79.196
Connecting to dl.eff.org (dl.eff.org)|173.239.79.196|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46789 (46K) [application/octet-stream]
Saving to: ‘certbot-auto’
100%
[=============================================================================================================
===>] 46,789      30.5KB/s   in 1.5s
2017-02-14 15:55:05 (30.5 KB/s) - ‘certbot-auto’ saved [46789/46789]
maurya@ls:~$ chmod a+x certbot-auto
maurya@ls:~$ sudo ./certbot-auto --config /etc/letsencrypt/configs/ls.datim4u.org.conf certonly
Creating virtual environment...
Installing Python packages...
Installation succeeded.
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Cert is due for renewal, auto-renewing...
Renewing an existing certificate
Performing the following challenges:
http-01 challenge for ls.datim4u.org
Using the webroot path /usr/share/nginx/html for all unmatched domains.
Waiting for verification...
Cleaning up challenges
Generating key (4096 bits): /etc/letsencrypt/keys/0001_key-certbot.pem
Creating CSR: /etc/letsencrypt/csr/0001_csr-certbot.pem
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at
   /etc/letsencrypt/live/ls.datim4u.org/fullchain.pem. Your cert will
   expire on 2017-05-15. To obtain a new or tweaked version of this
   certificate in the future, simply run certbot-auto again. To
   non-interactively renew *all* of your certificates, run
   "certbot-auto renew"
 - If you like Certbot, please consider supporting our work by:
   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
maurya@ls:~$ sudo vim /etc/nginx/sites-available/datim
maurya@ls:~$ sudo service nginx restart
 * Restarting nginx
nginx
[ OK ]
maurya@ls:~$ sudo service openhim-core restart
openhim-core stop/waiting
openhim-core start/running, process 25326
maurya@ls:~$ sudo service nginx restart
```

- Disable site default and enable sites openhim-console and datim
- Replace these with the certificates in OpenHIM Certificates tab
- Replace these with the certificates in OpenHIM global
- Select the newly added certificate in global OpenHIM to the client for the node
- Update the new certificate and key in the sync-mediator in the node OpenHIM
- Restart the mediator

Restarting the mediator

```
maurya@ls:~$ sudo restart openhim-mediator-openinfoman-dhis2-sync
openhim-mediator-openinfoman-dhis2-sync start/running, process 4508
```

Automatic Certificate Renewal:

Automatic certificate renewal can be installed on a DATIM box to ensure that the certificate on this machine is automatically renewed. The process consists of Two Parts:

1. Install the package `datim-auto-cert-updater`
    a. Ensure the PPA is installed
    b. Configure the installation
2. Test the installation
    a. Immediately check that all functionality works
    b. Return in a few days and check that the cronjob is called successfully

The instructions to do these steps are outlined at the following link: https://github.com/OHIEDATIM/datim-auto-cert-updater/blob/master/docs/testing/readme.md

Certificate creation on CentOS:

BAO has created custom scripts to aid in the creation of certificates on CentOS and Amazon Linux hosts. That script is called `certbot-new` and is available on hosts with the BAO yum repository installed. In order to create a new certificate, use the following steps:

- If you need a cert for `$( hostname )`:
    - Use the wrapper script: `certbot-new --domain=$( hostname )`
    - Add the Nginx config from `certbot-new` to `/etc/nginx/conf.d/ssl-files.conf`
- Create another certificate if `$( hostname )` begins with `www.` or is a naked domain:
    - Use the wrapper script: `cerbot-new --domain=www.example.com`
    - Add the Nginx config to the non-default `server{}` in Nginx, NOT the `conf.d/ssl-files.conf` file (that is intended for the default hostname/domain)

Certificate Renewal:

If the server was installed by BAO, or using BAO's tools, the cron job will automatically be installed in `/etc/cron.daily/certbot-renew`.

Essentially, the `certbot-renew` script runs the following:

```
certbot \
  renew \
  --quiet \
  --non-interactive \
  --agree-tos \
  --preferred-challenges 'http-01' \
  --pre-hook '/bin/mkdir -pv /var/lib/letsencrypt/html/' \
  --renew-hook "$RENEW_HOOK"
```