Certbot and SSL

The docs on EFF:

<https://certbot.eff.org/lets-encrypt/debianbuster-nginx.html>

My goal today is to get the subdomains running. For testing I prefer off 80 port numbers rather than advertising DNS values. And that was running with SSL; however, apparently it causes some pain to the web developers (marc ;-). So lets try subdomains.

## The first trip up ..

In the server block of the html\_css\_js\_reasoningtechnology.conf file I changed a directive saying:

listen 443 ssl;

I changed this to:

listen 127.0.0.1:443 ssl;

And now the site does not work. It comes up with an “Unable to Connect” panel.

Apparently I’m going to have to learn how these SSL certificates work in more detail.

## Install

certbot is an SSL certificate installer and maintainer. Apparently we already ran it when doing the website (see the nginx install journal), so it is on the system. But if we did have to install it, maybe this:

apt install certbot python-certbot-nginx

## Certificates are Expire in 90 days

<https://linuxhostsupport.com/blog/install-lets-encrypt-ssl-certificates-using-certbot/>: “The SSL certificates that have been issued by Let’s Encrypt are valid for 90 days and are trusted by most web browsers today.” They suggest setting up a cron job to renew it.

According to EFF:

“The Certbot packages on your system come with a cron job or systemd timer that will renew your certificates automatically before they expire. You will not need to run Certbot again, unless you change your configuration. You can test automatic renewal for your certificates by running this command:”

# certbot renew --dry-run

## One step get certificate and install

Only websites that are up and running can get certificates. If the site is not configured, certbot will not list it in the initial selection menu. If the site is not running, certbot will give an ‘Invalid response’ error after the site is selected. It appears that the script also restarted nginx, as the site immediately came up with https after the script ran.

2020-03-08T11:11:23Z root@reasoning-technology-server-1§/etc/nginx/sites-available§

# certbot --nginx

Saving debug log to /var/log/letsencrypt/letsencrypt.log

Plugins selected: Authenticator nginx, Installer nginx

Which names would you like to activate HTTPS for?

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

1: reasoning-tech.com

2: reasoning-tech.ai

3: reasoning-technology.ai

4: reasoning-technology.com

5: reasoningtech.ai

6: reasoningtechnology.ai

7: reasoningtechnology.com

8: iphttp.reasoningtechnology.com

9: unixuwsgi.reasoningtechnology.com

10: www.reasoningtechnology.com

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

Select the appropriate numbers separated by commas and/or spaces, or leave input

blank to select all options shown (Enter 'c' to cancel): 8

Obtaining a new certificate

Deploying Certificate to VirtualHost /etc/nginx/sites-enabled/customer\_gateway.conf

Please choose whether or not to redirect HTTP traffic to HTTPS, removing HTTP access.

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

1: No redirect - Make no further changes to the webserver configuration.

2: Redirect - Make all requests redirect to secure HTTPS access. Choose this for

new sites, or if you're confident your site works on HTTPS. You can undo this

change by editing your web server's configuration.

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

Select the appropriate number [1-2] then [enter] (press 'c' to cancel): 2

Redirecting all traffic on port 80 to ssl in /etc/nginx/sites-enabled/customer\_gateway.conf

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

Congratulations! You have successfully enabled

https://iphttp.reasoningtechnology.com

You should test your configuration at:

https://www.ssllabs.com/ssltest/analyze.html?d=iphttp.reasoningtechnology.com

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

IMPORTANT NOTES:

- Congratulations! Your certificate and chain have been saved at:

/etc/letsencrypt/live/iphttp.reasoningtechnology.com/fullchain.pem

Your key file has been saved at:

/etc/letsencrypt/live/iphttp.reasoningtechnology.com/privkey.pem

Your cert will expire on 2020-06-06. To obtain a new or tweaked

version of this certificate in the future, simply run certbot again

with the "certonly" option. To non-interactively renew \*all\* of

your certificates, run "certbot 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

2020-03-08T11:12:25Z root@reasoning-technology-server-1§/etc/nginx/sites-available§

#

No help here, it ignored the server blocks for the subdomains. I will have to come back and get the aliases.