SSL Enabled Apache and Let's Encrypt

Synopsis:

Having an SSL connection to your web server ensures that all traffic is encrypted. This avoids any "man in the middle" attack and it has also been shown that Google's search engine gives https sites higher ranking. We're going to use a free domain certificate provider, Let's Encrypt, that offers free certificates that are valid for 90 days. We'll setup to get a signed certificate and then setup a cron to automatically renew the certificate before it expires. Throughout this example, the fake domain "www.mydomain.com" will be used. Substitute your host's name in these examples.

Prepare Apache for SSL

Open the httpd.conf file for editing.

```
# cd /usr/local/etc/apache24
# ee httpd.conf
```

Un-comment modules; mod_ssl.so, mod_log_config.so, mod_setenvif.so, mod_socache_shmcb.so
Next, uncomment the following two lines:

```
Include etc/apache24/extra/httpd-ssl.conf
Include etc/apache24/extra/httpd-vhosts.conf
```

Edit the httpd-ssl.conf file

```
# ee extra/httpd-ssl.conf
```

Find <VirtualHost _default_:443> and modify:
ServerName, ServerAdmin
example: www.mydomain.com, webmaster@mydomain.com

Install Certbot:

```
# cd /usr/ports/security/py-certbot && make install clean
```

Get Certificates:

```
#
# cd
# service apache24 stop
# certbot certonly --webroot -w /usr/local/www/apache24/data -d www.mydomain.com
#
```

Note that the web root path is the default for an Apache install on FreeBSD. Place the fully qualified domain name of the server after the "-d" parameter. The screen will display something like this:

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Obtaining a new certificate
Performing the following challenges:
tls-sni-01 challenge for www.mydomain.com
Waiting for verification...
Cleaning up challenges
Generating key (2048 bits): /usr/local/etc/letsencrypt/keys/0000_key-certbot.pem
Creating CSR: /usr/local/etc/letsencrypt/csr/0000_csr-certbot.pem
```

```
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at
   /usr/local/etc/letsencrypt/live/www.mydomain.com/fullchain.pem.
   Your cert will expire on 2017-09-17. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot
   again. 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
```

Edit httpd-vhosts.conf

```
#
# cd /usr/local/etc/apache24/extra
# ee httpd-vhosts.conf
#
```

```
<VirtualHost *:80>
ServerAdmin www.mydomain.com
Redirect permanent / https://www.mydomain.com/
</VirtualHost>
```

Remove or comment out any other Virtualhosts

Edit httpd-ssl.conf

```
#
# ee httpd-ssl.conf
#
```

Make sure the following is modified

```
Listen 443
SSLCipherSuite HIGH:MEDIUM:!SSLv3:!kRSA
SSLProxyCipherSuite HIGH:MEDIUM:!SSLv3:!kRSA



<VirtualHost _default_:443>

# General setup for the virtual host
DocumentRoot "/usr/local/www/apache24/data"
ServerName www.mydomain.com:443
ServerAdmin root@mydomain.com
ErrorLog "/var/log/httpd-error.log"
TransferLog "/var/log/httpd-access.log"

# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on
```

Add/modify only these two lines:

```
SSLCertificateFile "/usr/local/etc/letsencrypt/live/www.mydomain.com/fullchain.pem"
SSLCertificateKeyFile "/usr/local/etc/letsencrypt/live/www.mydomain.com/privkey.pem"
```

Restart the Apache Service:

```
#
# service apache24 start
#
```

Test renewal:

```
# certbot renew --dry-run

Saving debug log to /var/log/letsencrypt/letsencrypt.log
-------------------------------------------------------------------------------
Processing /usr/local/etc/letsencrypt/renewal/www.mydomain.com.conf
-------------------------------------------------------------------------------
Cert not due for renewal, but simulating renewal for dry run
Plugins selected: Authenticator webroot, Installer None
Renewing an existing certificate
Performing the following challenges:
http-01 challenge for www.mydomain.com
Waiting for verification...
Cleaning up challenges

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
new certificate deployed without reload, fullchain is
/usr/local/etc/letsencrypt/live/www.mydomain.com/fullchain.pem
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
** DRY RUN: simulating 'certbot renew' close to cert expiry
**          (The test certificates below have not been saved.)

Congratulations, all renewals succeeded. The following certs have been renewed:
  /usr/local/etc/letsencrypt/live/www.mydomain.com/fullchain.pem (success)
** DRY RUN: simulating 'certbot renew' close to cert expiry
**          (The test certificates above have not been saved.)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Running post-hook command: service apache24 restart
Output from post-hook command service:
Performing sanity check on apache24 configuration:
Stopping apache24.
Waiting for PIDS: 2019.
Performing sanity check on apache24 configuration:
Starting apache24.
```

Troubleshooting: challenge failed

Here is an example of a failed renew.

```
# certbot renew --dry-run
Saving debug log to /var/log/letsencrypt/letsencrypt.log
-------------------------------------------------------------------------------
Processing /usr/local/etc/letsencrypt/renewal/www.mydomain.com.conf
-------------------------------------------------------------------------------
Cert not due for renewal, but simulating renewal for dry run
Renewing an existing certificate
Performing the following challenges:
http-01 challenge for www.mydomain.com
```

```
Waiting for verification...
Cleaning up challenges
Attempting to renew cert from
/usr/local/etc/letsencrypt/renewal/www.mydomain.com.conf
produced an unexpected error: Failed authorization procedure. www.mydomain.com (http-
01):
urn:acme:error:connection :: The server could not connect to the client to verify the
domain ::
Fetching https://www.mydomain.com.well-known/acme-
challenge/MNQFLMzKmbmr1ZA0g5WTr9cvhmwf5_0-nKVC3IlaJqY:
Error getting validation data. Skipping.
** DRY RUN: simulating 'certbot renew' close to cert expiry
**          (The test certificates below have not been saved.)

All renewal attempts failed. The following certs could not be renewed:
  /usr/local/etc/letsencrypt/live/www.mydomain.com/fullchain.pem (failure)
** DRY RUN: simulating 'certbot renew' close to cert expiry
**          (The test certificates above have not been saved.)
1 renew failure(s), 0 parse failure(s)

IMPORTANT NOTES:
 - The following errors were reported by the server:

   Domain: www.mydomain.com
   Type:   connection
   Detail: Fetching
   https://www.mydomain.com.well-known/acme-
challenge/MNQFLMzKmbmr1ZA0g5WTr9cvhmwf5_0-nKVC3IlaJqY:
   Error getting validation data

   To fix these errors, please make sure that your domain name was
   entered correctly and the DNS A record(s) for that domain
   contain(s) the right IP address. Additionally, please check that
   your computer has a publicly routable IP address and that no
   firewalls are preventing the server from communicating with the
   client. If you're using the webroot plugin, you should also verify
   that you are serving files from the webroot path you provided.
```

Check the above for DNS errors. Another reason for failure could be the webroot .htaccess file's RewriteEngine.

Edit the .htaccess file in Webroot and add the following after **RewriteEngine On**

```
RewriteRule ^.well-known/acme-challenge - [L]
```

Setup a crontab to auto renew:

Create a shell file, as root

```
# cd
# mkdir bin
# cd bin
# ee certbot.sh
```

Place the following contents into the file.

```
#/bin/sh
# shell file for cron to auto renew certificate
# this will stop apache to open the port for certbot and then restart apache after
/usr/local/bin/certbot renew --pre-hook "service apache24 stop" --post-hook "service
apache24 start"
```

Save the file. Make it executable:

```
# chmod 755 certbot.sh
```

Next edit the crontab.

```
# cd
# crontab -e
```

Place the following into crontab to check the certificate every Sunday morning.

```
SHELL=/bin/sh
PATH=/etc:/bin:/sbin:/usr/bin:/usr/sbin
# Order of crontab fields
# minute        hour    mday    month   wday    command
12              3       *       *       sun     /root/bin/certbot.sh
```

This will run the cron every Sunday at 3:12am and will auto renew
when only 30 days are left before expiration.

Sites of Interest:
https://letsencrypt.org/docs/
https://certbot.eff.org/