**Step 1 — Creating the TLS Certificate**

cd /home/webadmin

mkdir portalcerts

cd portalcerts

* Create a self-signed key and certificate pair with OpenSSL in a single command:

*sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout portal-selfsigned.key -out portal-selfsigned.crt*

* While using OpenSSL, create a strong Diffie-Hellman (DH) group, which is used in negotiating Perfect Forward Secrecy with clients.

*sudo openssl dhparam -out /etc/nginx/dhparam.pem 4096*

**Step 2 — Configuring Nginx to Use SSL**

1. Creating a Configuration to Pointing to the SSL Key and Certificate

* Create “self-signed.conf”

*sudo nano /etc/nginx/snippets/self-signed.conf*

* Open “self-signed.conf” & set ssl\_certificate directive to your certificate file and the ssl\_certificate\_key to the key.

*ssl\_certificate /home/webadmin/portalcerts/portal-selfsigned.crt;*

*ssl\_certificate\_key /home/webadmin/portalcerts/portal-selfsigned.key;*

1. Creating a Configuration Snippet with Strong Encryption Settings
   * Create ssl-params.conf

*sudo nano /etc/nginx/snippets/ssl-params.conf*

* + Add below content

ssl\_protocols TLSv1.3;

ssl\_prefer\_server\_ciphers on;

ssl\_dhparam /etc/nginx/dhparam.pem;

ssl\_ciphers EECDH+AESGCM:EDH+AESGCM;

ssl\_ecdh\_curve secp384r1;

ssl\_session\_timeout 10m;

ssl\_session\_cache shared:SSL:10m;

ssl\_session\_tickets off;

ssl\_stapling on;

ssl\_stapling\_verify on;

resolver 8.8.8.8 8.8.4.4 valid=300s;

resolver\_timeout 5s;

# Disable strict transport security for now. You can uncomment the following

# line if you understand the implications.

#add\_header Strict-Transport-Security "max-age=63072000; includeSubDomains; preload";

add\_header X-Frame-Options DENY;

add\_header X-Content-Type-Options nosniff;

add\_header X-XSS-Protection "1; mode=block";

1. Adjusting the Nginx Configuration to Use SSL
   * Backup old nginx config file “self-signed.conf”

*sudo cp /etc/nginx/sites-available/ partner-portal-reverse-proxy-nginx.conf /etc/nginx/sites- available/ partner-portal-reverse-proxy-nginx.conf.bak*

* + Open the configuration file to make adjustments:

*server {*

*listen 443 ssl;*

*listen [::]:443 ssl;*

*include snippets/self-signed.conf;*

*include snippets/ssl-params.conf;*

*server\_name partner-portal-reverse-proxy-nginx.conf;*

*}*

*server {*

*listen 80;*

*listen [::]:80;*

*server\_name partner-portal-reverse-proxy-nginx.conf;*

*}*

1. Restart the nginx and test it with https