NGINX: Deploy SSL Certificate

Here's quick instructions for deploying an SSL key/cert pair to an NGINX instance.

> NOTE: These steps are assumed to be executed as root.

Elevate to Root

Elevate to root with this:

```
sudo -i
```

Create SSL Folder

By default, a fresh NGINX install doesn't yet contain a folder for certificates.

Create the ssl folder, with this:

```
mkdir /etc/nginx/ssl
```

Set Folder Permissions

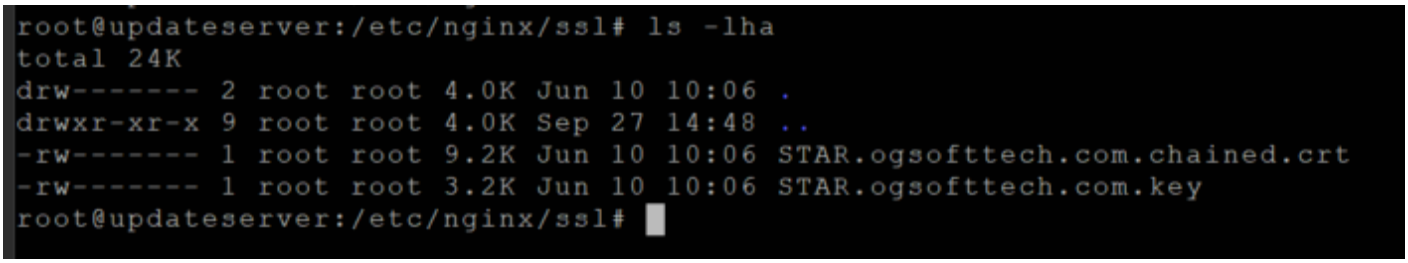
We need to constrain access to the private SSL keys, with the following:

> NOTE: NGINX runs as root, so this is fine.

```
chmod 0600 -R /etc/nginx/ssl
chown root:root -R /etc/nginx/ssl
```

Copy SSL Cert

Create files in the SSL folder for the public crt and private key files, like this:



Paste the content of your private key and public cert into the files.

Set File Permissions

Once added, constrain access, with the following:

```
# All certs readable
chmod 644 *.crt

# All keys locked down
chmod 600 *.key

# Make sure ownership is correct
chown root:root *.crt *.key
```

Restart NGINX

Once certs are pasted in, you need to restart NGINX for the new certs to take effect, with this:

```
nginx -s reload
```

Revision #3
Created 28 September 2025 04:40:01 by glwhite
Updated 28 September 2025 04:55:46 by glwhite