How To Create a Self-Signed SSL Certificate for Nginx on debian

217 Manu Chacko June 8, 2018 Tweaks & Configuration 5955

How to Create a SSL Certificate on ezeelogin jump server for Nginx on debian 8

Create a Self Signed Certificate

When we request a new certificate, we can specify how long the certificate should remain valid by changing the 365 to the number of days we prefer. As it stands this certificate will expire after one year.

```
root@gateway:~#sudo openssl req -x509 -nodes -days 365 -newkey
rsa:2048 -keyout /etc/ssl/private/nginx-selfsigned.key -out
/etc/ssl/certs/nginx-

selfsigned.crt
```

With this command, we will be both creating the self-signed SSL certificate and the server key .

This command will prompt terminal to display a lists of fields that need to be filled in.Fill out the prompts appropriately. The most important line is the one that requests the Common Name (e.g. server FQDN or YOUR name). You need to enter the domain name associated with your server or, more likely, your server’s public IP address.

```
Output

Country Name (2 letter code) [AU]:US

State or Province Name (full name) [Some-State]:New York

Locality Name (eg, city) []:New York City

Organization Name (eg, company) [Internet Widgits Pty Ltd]:Bouncy
Castles, Inc.

Organizational Unit Name (eg, section) []:Ministry of Water Slides

Common Name (e.g. server FQDN or YOUR name) []:server_IP_address

Email Address []:admin@your_domain.com
```

Both of the files you created will be placed in the appropriate subdirectories of the /etc/ssl directory.

Configure Nginx to Use SSL

Let’s create a new Nginx configuration snippet in the /etc/nginx/snippets directory.

```
root@jumpserver:~# nano /etc/nginx/snippets/self-signed.conf
```

Within this file, we just need to set the ssl_certificate directive to our certificate file and the ssl_certificate_key to the associated key. In our case, this will look like this:

```
ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;

ssl_certificate_key /etc/ssl/private/nginx-selfsigned.key;
```

When you’ve added those lines, save and close the file.

Adjust the Nginx Configuration to Use SSL

Before we go any further, let’s back up our current server block file:

```
root@jumpserver:~# sudo cp /etc/nginx/sites-available/default
/etc/nginx/sites-available/default.bak
```

Open the server block file to make adjustments

```
root@jumpserver:~# sudo nano /etc/nginx/sites-available/default
```

```
server {

    listen 80 default_server;

    listen [::]:80 default_server;

    server_name server_domain_or_IP;

    return 302 https://$server_name$request_uri;

}
```

```
server {


    # SSL configuration


    listen 443 ssl default_server;

    listen [::]:443 ssl default_server;

    include snippets/self-signed.conf;

    . . .
```

Your virtual host is now all set up! Save and Exit

Restart Apache

```
root@jumpserver:~# sudo systemctl restart nginx
```

Online URL:
https://www.ezeelogin.com/kb/article/how-to-create-a-self-signed-ssl-certificate-for-nginx-on-debian-217.html