SSL Certificates on AWX without DOCKER

SSL certificates are used to encrypt the data between client and server and vice-versa. It has two steps.

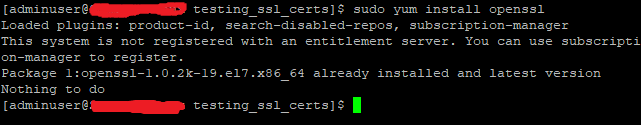
**1. Generation of SSL certificates**

**2. Perform changes in /etc/nginx/nginx.conf file**.

Step 1 : Commands to generate SSL certificate locally

1. Install openssl

**sudo yum install openssl**



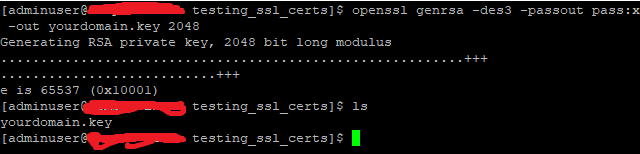
1. Create directory and move inside that directory

**mkdir testing\_ssl\_certs**

**cd testing\_ssl\_certs**

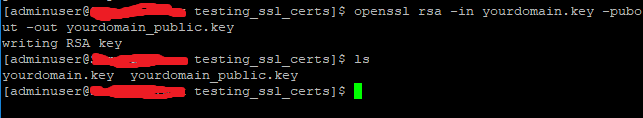
1. Generation of private key : This will generate the private key named “yourdomain” with 2048 bit encryption.

**openssl genrsa -out yourdomain.key 2048**



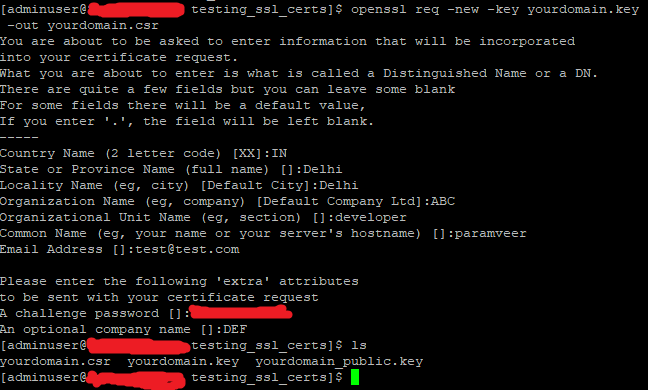
1. Extract Public key: Now you have to generate public key named “yourdomain\_public.key” form private key which is generated above.

**openssl rsa -in yourdomain.key -pubout -out yourdomain\_public.key**



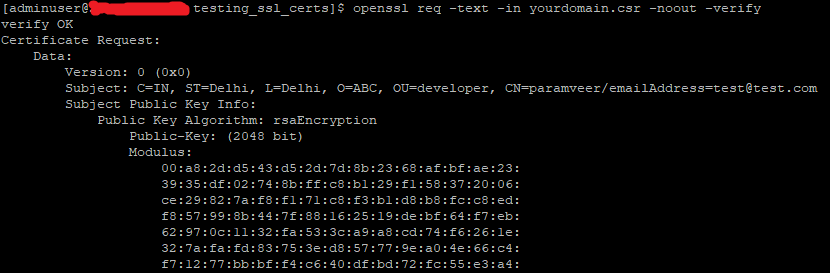
1. Generate CSR (certificate signing request) : Fill the required information.

**openssl req -new -key yourdomain.key -out yourdomain.csr**



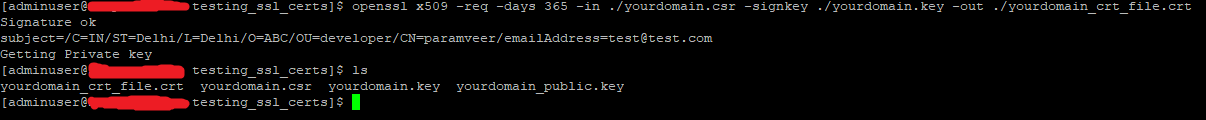
1. Verify CSR information

**openssl req -text -in yourdomain.csr -noout –verify**



1. Creating the Certificate “.crt” File

**openssl x509 -req -days 365 -in ./yourdomain.csr -signkey ./yourdomain.key -out ./yourdomain\_crt\_file.crt**



Step 2: Commands to change into the /etc/nginx/nginx.conf file

1. Copy file which are generated above to /etc/nginx/certs directory:

**sudo cp ./\* /etc/nginx/**

1. Make below changes into **“/etc/nginx/nginx.conf“** file under **“http”**

http {

server {

listen 8052 default\_server;

# If you have a domain name, this is where to add it

#server\_name \_;

keepalive\_timeout 65;

ssl\_certificate /etc/nginx/certs/yourdomain\_crt\_file.crt;

ssl\_certificate\_key /etc/nginx/certs/yourdomain.key;

ssl on;

ssl\_session\_cache builtin:1000 shared:SSL:10M;

ssl\_protocols TLSv1 TLSv1.1 TLSv1.2;

ssl\_ciphers HIGH:!aNULL:!eNULL:!EXPORT:!CAMELLIA:!DES:!MD5:!PSK:!RC4;

ssl\_prefer\_server\_ciphers on;

}

}