

Cloud VPS Servers

Generate a self-signed SSL certificate - Nginx,CentOS

Following article describes how to generate and install a self-signed SSL certificate for a domain.

Requirements

- [Bytehouse Cloud Product](#)
- [Basic Server Setup](#)
- [Nginx](#)

Self signed SSL

As the name indicates, they are certificates that is signed by the same entity whose identity it certifies. Since self signed SSL certificates are not validated/trusted by any Certificate Authority, its usage in production environment is not recommended. However its a favourable choice in development environment since self signed SSL certificates are free and can be created/deployed very easily.

How to

- Login to your server and switch to root by executing sudo su.
- Create a directory to store SSL certificates

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

- Execute the below command to generate self signed certificate

```
root@your-server-$ openssl req -x509 -nodes -days 365 -newkey r
sa:2048 -keyout /etc/nginx/ssl/self.key -out /etc/nginx/ssl/self
.crt
```

- Enter the required information during the prompt.

```
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/etc/nginx/ssl/self.key'
-----
You are about to be asked to enter information
that will be incorporated
into your certificate request.
What you are about to enter is what is called
a Distinguished Name or a DN.
```

Cloud VPS Servers

There are quite a few fields but you can leave some blank

For some fields there will be a default value, If you enter '.', the field will be left blank.

```
Country Name (2 letter code) [XX]:
State or Province Name (full name) []:
Locality Name (eg, city) [Default City]:
Organization Name (eg, company) [Default Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:
Email Address []:
```

- SSL key and certificate will be generated in the location /etc/nginx/ssl.

```
root@your-server-~$ pwd
/etc/nginx/ssl
root@your-server-~$ ls
self.crt  self.key
```

Nginx

- Edit nginx configuration file

```
root@your-server-~$ vi /etc/nginx/conf.d/default.conf
```

- Edit the following parameters

```
listen          443 ssl;
server_name     yourdomain.com;
ssl_certificate  /etc/nginx/ssl/self.crt;
ssl_certificate_key /etc/nginx/ssl/self.key;
```

- Restart nginx service

```
root@your-server-~$ service nginx restart
Stopping nginx: [
OK ]
Starting nginx: [ OK
]
```

Cloud VPS Servers

Verify that your site is loading with self signed certificate.

`https://yourdomain.com`

While accessing the site, you will be presented with a warning message. This happens due to the self signed certificate we installed. You can continue to the website by accepting the connection.

Your site is now using a self signed SSL certificate.

Bytehouse offers [different types of SSL certificates](#). For production environments, you can [purchase an SSL certificate](#) from your Bytehouse account.

Unique solution ID: #1343

Author: Bytehouse Technical Support

Last update: 2016-07-07 02:31