How To Create a SSL Certificate on nginx for CentOS 6

AUTHOR: ETEL SVERDLOV
PUBLISHED: JUN 8, 2012
UPDATED: JUN 10, 2014
SUBSCRIBE
TAGGED IN: CENTOS, NGINX
DIFFICULTY: BEGINNER

About Self-Signed Certificates

A SSL certificate is a way to encrypt a site's information and create a more secure connection. Additionally, the certificate can show the virtual private server's identification information to site visitors. Certificate Authorities can issue SSL certificates that verify the server's details while a self-signed certificate has no 3rd party corroboration.

Intro

Make sure that nginx is installed on your VPS. If it is not, you can quickly install it with 2 steps.

Install the EPEL repository:

```
su -c 'rpm -Uvh http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm'
```

Install nginx

```
yum install nginx
```

Step One—Create a Directory for the Certificate

The SSL certificate has 2 parts main parts: the certificate itself and the public key. To make all of the relevant files easy to access, we should create a directory to store them in:

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

We will perform the next few steps within the directory:

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

Step Two—Create the Server Key and Certificate Signing Request

Start by creating the private server key. During this process, you will be asked to enter a specific passphrase. Be sure to note this phrase carefully, if you forget it or lose it, you will not be able to access the certificate.

```
sudo openssl genrsa -des3 -out server.key 1024
```

Follow up by creating a certificate signing request:

```
sudo openssl req -new -key server.key -out server.csr
```

This command will prompt terminal to display a lists of fields that need to be filled in.

The most important line is "Common Name". Enter your official domain name here or, if you don't have one yet, your site's IP address. Leave the challenge password and optional company name blank.

```
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.
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) [AU]:US
State or Province Name (full name) [Some-State]:New York
Locality Name (eg, city) []:NYC
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Awesome Inc
Organizational Unit Name (eg, section) []:Dept of Merriment
Common Name (e.g. server FQDN or YOUR name) []:example.com
Email Address []:webmaster@awesomeinc.com
```

Step Three—Remove the Passphrase

We are almost finished creating the certificate. However, it would serve us to remove the passphrase. Although having the passphrase in place does provide heightened security, the issue starts when one tries to reload nginx. In the event that nginx crashes or needs to reboot, you will always have to re-enter your passphrase to get your entire web server back online.

Use this command to remove the passphrase:

```
sudo cp server.key server.key.org
sudo openssl rsa -in server.key.org -out server.key
```

Step Four— Sign your SSL Certificate

Your certificate is all but done, and you just have to sign it. Keep in mind that you can specify how long the certificate should remain valid by changing the 365 to the number of days you prefer. As it stands, this certificate will expire after one year.

```
sudo openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

You are now done making your certificate.

Step Five—Set Up the Certificate

Open up the SSL config file:

```
vi /etc/nginx/conf.d/ssl.conf
```

Uncomment within the section under the line HTTPS Server. Match your config to the information below, replacing the example.com in the "server_name" line with your domain name or IP address. If you are just looking to test your certificate, the default root there will work.

```
# HTTPS server
```

```
server {
    listen       443;
    server_name example.com;

    ssl on;
    ssl_certificate /etc/nginx/ssl/server.crt;
    ssl_certificate_key /etc/nginx/ssl/server.key;
}
```

Then restart nginx:

```
/etc/init.d/nginx restart
```

Visit https://youraddress.

You will see your self-signed certificate on that page!

Resources

- http://wiki.nginx.org/HttpSslModule#Generate_Certificates

By Etel Sverdlov

Tagged In: CentOS, NGINX

Related Tutorials

How To Set Up Nginx Server Blocks on CentOS 7

How To Stream Videos With Nginx and JWPlayer on CentOS 6

How To Set Up nginx Virtual Hosts (Server Blocks) on CentOS 6

How To Install and Update WordPress with Version Control on CentOS 7

How To Create an SSL Certificate on Apache for CentOS 7

15 Comments

You must be logged in to comment. Log In

Leave a comment...

SUBMIT COMMENT

Notify me of replies to my comment

dewsworld *September 23, 2013*

♡ Brower warn me that the connection is untrusted. let me know what did I miss!

kamaln7 STAFF *September 24, 2013*

♡ @dewsworld: This article walks you through creating a self-signed certificate (Step Four— Sign your SSL Certificate). If you want to get rid of that warning, you will have to purchase an SSL cert from a trusted provider such as Comodo/DigiCert/Verisign to name a few or any of their resellers. You will have to provide them the CSR which you can get by running

```
cat /path/to/server.csr
```

md.imtiazmahbub *November 13, 2013*

♡ After installing ssl, I added these lines to my ssl.conf file: it's running perfectly. Did I mis-configure anything?

location / {
root /home/username/public_html;
index index.html index.htm index.php;
}
location ~ \.php$ {
root /home/username/public_html;
fastcgi_param HTTPS on;
fastcgi_pass 127.0.0.1:9000;
fastcgi_index index.php;
fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
include fastcgi_params;
}

kamaln7 STAFF *November 15, 2013*

♡ @md.imtiazmahbub: The config seems proper, are you having any issues with it?

yllorca *December 6, 2013*

♡ Hi I want to install a certificate signed by commodo using nginx for CentOS 6.
They sent me a zip with the installation files. What should I do with them?
Best Regards
Yury Llorca D

james161908 *March 6, 2014*

♡ This tutorial may work for self-signed certificates, but I'd recommend using the suggested openssl parameters to create a key for a site where security is important to you.

sudo openssl genrsa -des3 -out server.key 1024

Most Certificate Authorities will no longer accept 1024-bit keys (2048 being the minimum), and RSA keys are the default format over des3. There is no need to run openssl as root unless you're trying to protect your key by having its owner be set to root.

For further info, see http://security.stackexchange.com/questions/2557/what-ssl-key-should-i-make-for-iis-rsa-or-dh-what-bit-length-is-appropriate

kurniawanmagelang *April 6, 2014*

♡ trying to install RapidSSL on Nginx, and successfully :)

contato.tiagogomes *April 14, 2014*

♡ Hi guys,

What's the way to enable HTTPS only for the administration panel?

asb STAFF *April 15, 2014*

♡ @ Tiago,

In your server block that is listening on port 80 for normal http, set a redirect for your panel's url to the https url:

```
server {
listen 80;

# snipping every thing else just for the example

location /panel_url {
return 301 https://$server_name$request_uri;
}
}
```

Then in the server block listening on port 443, redirect https attempts back to http unless it is your panel's url.

```
server {
listen 443;

# snipping every thing else just for the example

location /panel_url {
}

location / {
return 301 http://$server_name$request_uri;
}
}
```

richardaljasteabramson *May 1, 2014*

I've got the nginx running, but the signature doesn't show up.. What may be causing this?

asb STAFF *May 1, 2014*

@Richard: I'm not entirely sure what problem you're facing. Are you able to connect to your site using https? Generally, a good place to start debugging is by checking the logs. In this case, the nginx logs are located at:

```
/var/log/nginx/error.log
```

sarah674985 *May 23, 2014*

Hello,

I followed every step the after I restarted the nginx error came up:

nginx: [emerg] SSL_CTX_use_certificate_chain_file("/etc/nginx/ssl/server.crt") failed (SSL: error:02001002:system library:fopen:No such file or directory error:20074002:BIO routines:FILE_CTRL:system lib error:140DC002:SSL routines:SSL_CTX_use_certificate_chain_file:system lib)
nginx: configuration file /etc/nginx/nginx.conf test failed

Pls help:(

kamaln7 STAFF *May 25, 2014*

@sarah: **"No such file or directory"** -- looks like `/etc/nginx/ssl/server.crt` does not exist. What's the output of

```
ls /etc/nginx/ssl
```

matthewniemerg *September 28, 2014*

What if I am running several sites on one VPS and want a separate SSL cert for each site? I realize I could easily change the name of each certificate, so that it would be with the corresponding site, but how do I set up the nginx settings?

akhilesh *October 11, 2014*

In the starting of step 5, after running `vi /etc/nginx/conf.d/ssl.conf` a new file was created as there was no such file already. Here I simply added the config info provided above.

On running `/etc/init.d/nginx restart` I am getting following error:

```
[root@wpone ssl]# /etc/init.d/nginx restart
-bash: /etc/init.d/nginx: No such file or directory
```

Please help.

SUBMIT COMMENT

Notify me of replies to my comment

Proudly Made in NY

Terms, Privacy, & Copyright
Security

D R O P L E T S L A U N C H E D