How to install ssl certs in jump server [secure connection] ?

207 Manu Chacko December 14, 2023 Tweaks & Configuration 11059

How to Create a SSL Certificate on ezeelogin jump server Apache for CentOS 6 /Centos 7/Centos 8 ?

Install Mod SSL

Create a New Directory

we need to create a new directory where we will store the server key and certificate

```
~#
```

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.

With this command, we will be both creating the self-signed SSL certificate and the server key that protects it, and placing both of them into the new directory.

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

Set up the virtual hosts to display the new certificate.

Open up the SSL config file:

Find the section that begins with <VirtualHost _default_:443> and Uncomment the DocumentRoot and ServerName line and replace example.com with your domain name or server IP address

```
#uncomment & Replace the example.com with your domain
```

Find the following three lines, and make sure that they match the extensions below:

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

Restart Apache

```
systemctl restart httpd
```

H ow to Create a SSL Certificate on jump server Apache for Ubuntu 16 /Ubuntu 18/ Ubuntu 20/ Debian9/ Debian10 ?

Install Apache2

```
root@gateway :~# apt-get install apache2
```

Create a New Directory

we need to create a new directory where we will store the server key and certificate

```
root@gateway :   ~#    mkdir /etc/certs/ssl
```

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:~# openssl req -x509 -nodes -days 365 -newkey rsa:2048
-keyout /etc/ssl/private/apache-selfsigned.key -out
/etc/ssl/certs/apache-selfsigned.crt
```

With this command, we will be both creating the self-signed SSL certificate and the server key that protects it, and placing both of them into the new directory.

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

```
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

-----
```

Modify the Default Apache SSL Virtual Host File

Next, let's modify /etc/apache2/sites-available/default-ssl.conf.he default Apache SSL Virtual Host file.

Before we go any further, let's back up the original SSL Virtual Host file:

```
root@jumphost:~# cp /etc/apache2/sites-available/default-
```

```
ssl.conf /etc/apache2/sites-available/default-ssl.conf.bak
```

Now, open the SSL Virtual Host file to make adjustments:

```

```

Find the section that begins with <VirtualHost _default_:443> and Uncomment the DocumentRoot and ServerName line and replace example.com with your domain name or server IP address,Also uncomment SSLCertificateFile, `SSLCertificateKeyFile, SSLEngine on & add the correct path of cert file & key file.`

```
                your_email@example.com

     ServerName  server_domain_or_IP

      DocumentRoot /var/www/html
```

```
 SSLEngine on

SSLCertificateFile      /etc/ssl/certs/apache-selfsigned.crt

SSLCertificateKeyFile  /etc/ssl/private/apache-selfsigned.key
```

Save & Exit the file.

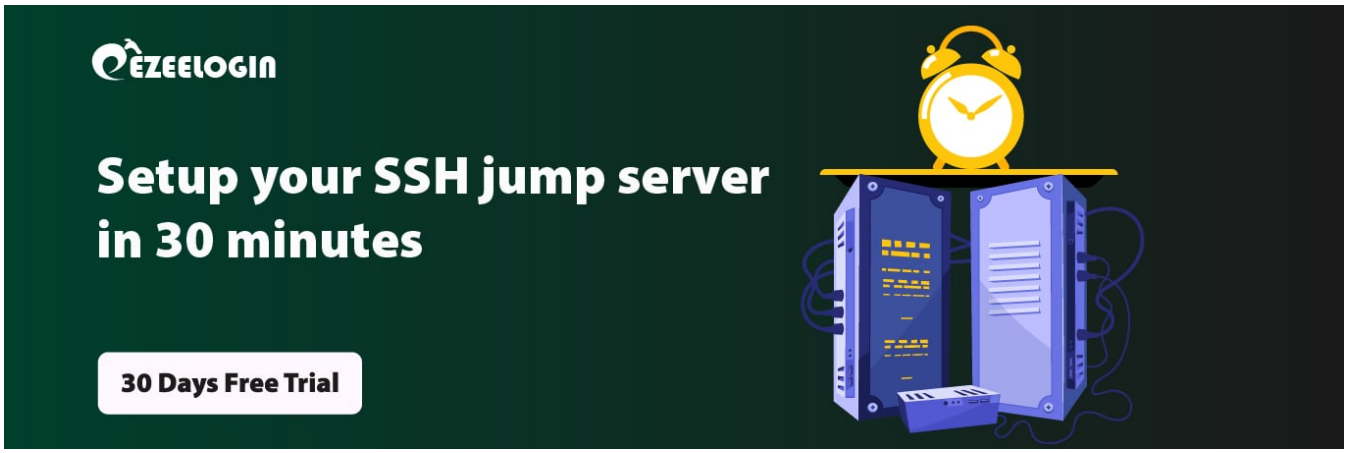
Enable the Changes in Apache

```
a2enmod ssl
root@jumphost:~# a2ensite default-ssl
```

Also enforce ssl in ezeelogin gui.

Restart Apache

```
```



Online URL:
https://www.ezeelogin.com/kb/article/how-to-install-ssl-certs-in-jump-server-secure-connection-207.html