## **Setup Nginx in front of Jenkins server:**

1. Create SSL certificate, in this case we have created self-signed certificate. Move the certificate and key on Jenkins host machine.

****

1. Modify and share the nginx.conf file over Jenkins host machine. (In this case dev-jenkins-01.dt.vmware.com) ([conf file source](https://www.digitalocean.com/community/tutorials/how-to-configure-jenkins-with-ssl-using-an-nginx-reverse-proxy))

#user nobody;

worker\_processes 1;

#error\_log logs/error.log;

#error\_log logs/error.log notice;

#error\_log logs/error.log info;

#pid logs/nginx.pid;

events {

worker\_connections 1024;

}

http {

include mime.types;

default\_type application/octet-stream;

#log\_format main '$remote\_addr - $remote\_user [$time\_local] "$request" '

# '$status $body\_bytes\_sent "$http\_referer" '

# '"$http\_user\_agent" "$http\_x\_forwarded\_for"';

#access\_log logs/access.log main;

sendfile on;

#tcp\_nopush on;

#keepalive\_timeout 0;

keepalive\_timeout 65;

#gzip on;

server {

**listen 80;**

**return 301 https://$host$request\_uri;**

#charset koi8-r;

#access\_log logs/host.access.log main;

location / {

root html;

index index.html index.htm;

}

#error\_page 404 /404.html;

# redirect server error pages to the static page /50x.html

#

error\_page 500 502 503 504 /50x.html;

location = /50x.html {

root html;

}

# proxy the PHP scripts to Apache listening on 127.0.0.1:80

#

#location ~ \.php$ {

# proxy\_pass http://127.0.0.1;

#}

# pass the PHP scripts to FastCGI server listening on 127.0.0.1:9000

#

#location ~ \.php$ {

# root html;

# fastcgi\_pass 127.0.0.1:9000;

# fastcgi\_index index.php;

# fastcgi\_param SCRIPT\_FILENAME /scripts$fastcgi\_script\_name;

# include fastcgi\_params;

#}

# deny access to .htaccess files, if Apache's document root

# concurs with nginx's one

#

#location ~ /\.ht {

# deny all;

#}

}

server {

**listen 443 ssl;**

**server\_name dev-jenkins-01.dt.vmware.com;**

**ssl\_certificate           /usr/share/nginx/nginx-signed.crt;**

**ssl\_certificate\_key       /usr/share/nginx/nginx-signed.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;

    access\_log            /var/log/nginx/jenkins.access.log;

    location / {

**proxy\_set\_header        Host $host:443;**

      proxy\_set\_header        X-Real-IP $remote\_addr;

      proxy\_set\_header        X-Forwarded-For $proxy\_add\_x\_forwarded\_for;

      proxy\_set\_header        X-Forwarded-Proto $scheme;

      # Fix the “It appears that your reverse proxy set up is broken" error.

**proxy\_pass          http://dev-jenkins-01.dt.vmware.com:12345;**

      proxy\_read\_timeout  90;

**proxy\_redirect      http://dev-jenkins-01.dt.vmware.com:12345 https://dev-jenkins-01.dt.vmware.com:443;**

    }

  }

        include servers/\*;

}

1. Build nginx docker image using Dockerfile, save as Dockerfile.txt



1. Start nginx docker container



1. Change the Jenkins URL in Manage Jenkins -> Configure System to <https://dev-jenkins-01.dt.vmware.com/>
2. Test the Jenkins SSL connection using url <https://dev-jenkins-01.dt.vmware.com/login?from=%2F>