## 环境

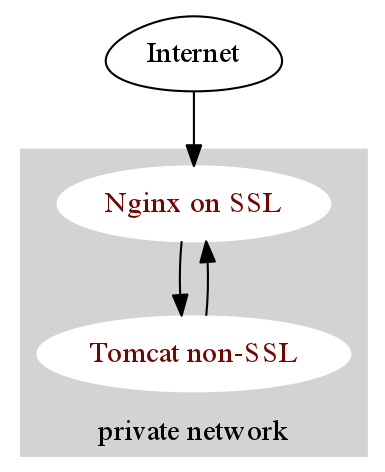
宿主机环境: windows 旗舰版 64

服务器OS version(VM 虚拟机): centos7 64-bit

Java version: java1.8.0 64-bit

nginx version: nginx-1.11.6

概述: 配置的方案是浏览器和 Nginx 之间走的 HTTPS 通讯，而 Nginx 到 Tomcat 通过 proxy\_pass 走的是普通 HTTP 连接。



1. nginx安装与配置
   1. 环境准备

**安装gcc-c++**

# yum install gcc-c++

**安装pcre**

为了支持rewrite功能，需要安装pcre命令如下，如果已经安装，则跳过此步

# yun install pcre\*

**安装openssl**

为了支持ssl，需要安装openssl。可以使用openssl version查看是否已经安装，如果已经安装则可跳过此步骤

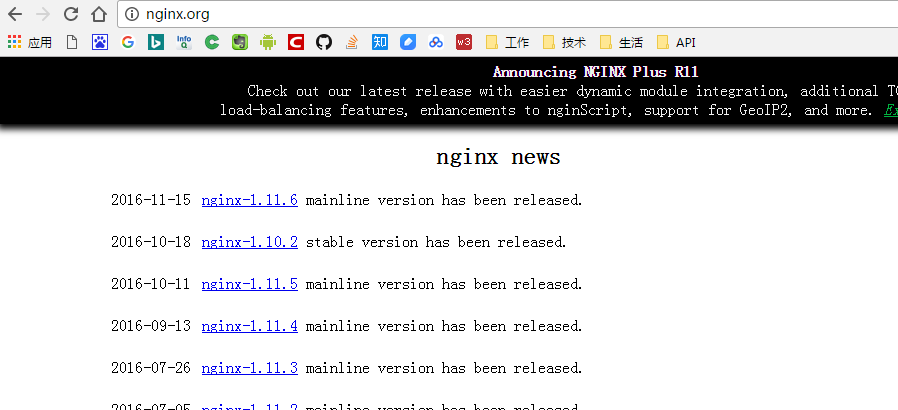
# yun install openssl\*

**安装gzip**

# yum install zlib zlib-devel

* 1. Nginx下载与配置

到<http://nginx.org/>上下载需要的版本，本文档中下载的是当前的最新版



下载完成后上传至centos，本文档将nginx放置在centos的 /home目录下。cd到/home目录下,使用命令

# tar –zxvf nginx-1.11.6.tar.gz

解压nginx后，进入nginx

# cd nginx-1.11.6

开始配置

# ./configure /usr/local/nginx-1.7.0 --with-http\_ssl\_module --with-http\_spdy\_module --with-http\_stub\_status\_module --with-pcre

以上命令需要在同一行执行。正常情况下会正常自动配置完，但如果遇到需要–with-openssl=<path>的错误。此处的path值并不指的是openssl的安装路径，此处需要的是openssl的源码

解决方法:

# cd /home

# wget <http://www.openssl.org/source/openssl-0.9.8y.tar.gz>

# tar xzvf openssl-0.9.8y.tar.gz

配置openssl

# cd openssl-0.9.8y

# ./config –prefix=/usr/local/openssl

编译安装:

# make && make install

再次进入nginx安装目录

./configure –with-http\_stub\_status\_module –with-http\_ssl\_module –with-openssl=/home/openssl-0.9.8y

没有错误的话使用下面命令进行安装

# make && make install

安装完成后使用

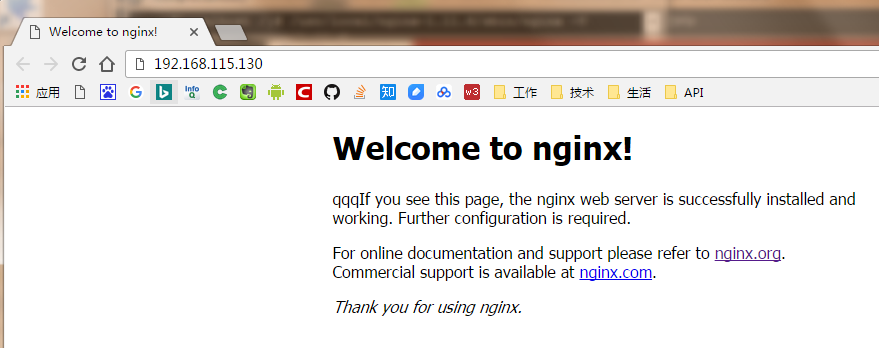
# /usr/local/nginx-1.11.6/sbin/nginx 可以启动nginx

注释: /usr/local/nginx-1.11.6是本文档的nginx安装目录

测试是否成功

在浏览器访问虚拟机ip地址本文档中的虚拟机地址是192.168.115.130

正常情况应该显示



如果访问不了，可以使用命令查看nginx进程是存在，若存在可以试着关闭centos防火墙试试。

**配置Https**

创建https证书，https证书可以自己颁发也可以去网站申请，有免费和收费的，此处使用自己颁发的证书

进入nginx的conf目录，以方便把证书放在此目录下

创建服务器私钥

# openssl genrsa -des3 -out server.key 1024 #根据提示输入证书口令

创建签名请求的证书（CSR）：

# openssl req -new -key server.key -out server.csr #输入上面设置的口令

#根据提示输入相应的信息

Country Name (2 letter code) [XX]:cn #国家

State or Province Name (full name) []:zhejiang #省份

Locality Name (eg, city) [Default City]:hangzhou #城市

Organization Name (eg, company) [Default Company Ltd]:osyunwei #公司

Organizational Unit Name (eg, section) []:sys #部门

Common Name (eg, your name or your server's hostname) []:osyunwei #主机名称

Email Address []:[email protected] #邮箱

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:123456 #证书请求密钥，CA读取证书的时候需要输入密码

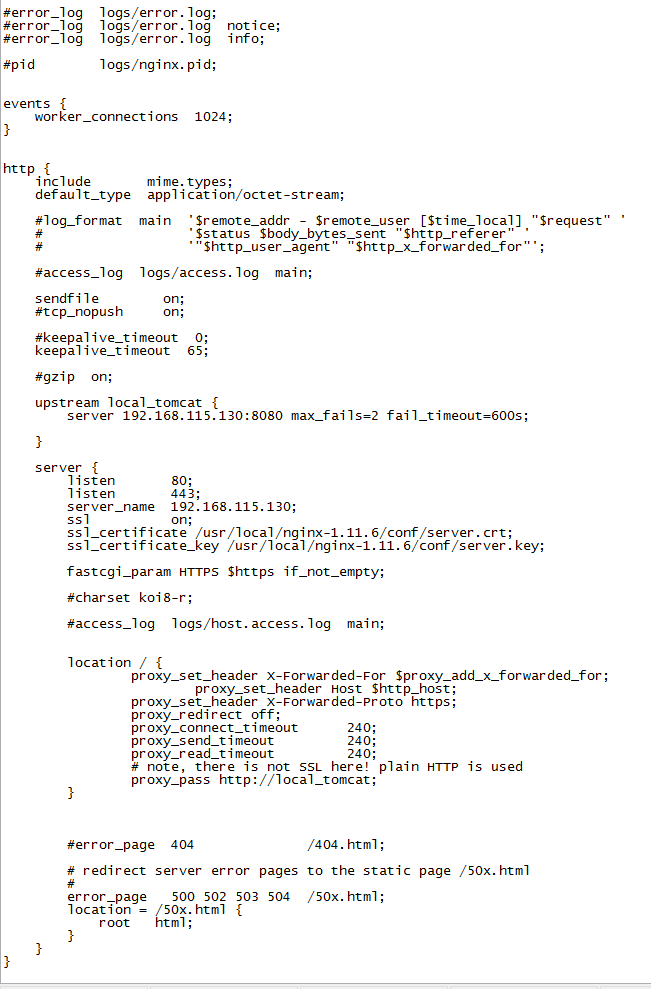
An optional company name []:osyunwei #公司名称，CA读取证书的时候需要输入密码

# openssl rsa -in server.key -out server\_nopassword.key #对key进行解密

# openssl x509 -req -days 365 -in server.csr -signkey server\_nopassword.key –out server.crt

**编辑nginx配置文件 加载ssl证书**

内容如下



**其中最为关键的就是 ssl\_certificate 和 ssl\_certificate\_key 这两项配置，其他的按正常配置。不过多了一个 proxy\_set\_header X-Forwarded-Proto https; 配置。**

使用

# /usr/local/nginx/sbin/nginx –s reload实现nginx的重启

此时在浏览器输入<https://192.168.115.130可访问既nginx>部分配置https成功

Tomcat配置

最主要的配置来自 Tomcat，下面是我测试环境中的完整 server.xml：

<?xml version='1.0' encoding='utf-8'?>

<Server port="8005" shutdown="SHUTDOWN">

<Service name="Catalina">

<Connector port="8080" protocol="HTTP/1.1"

connectionTimeout="20000"

redirectPort="443"

proxyPort="443"/>

<Engine name="Catalina" defaultHost="localhost">

<Host name="localhost" appBase="webapps"

unpackWARs="true" autoDeploy="true">

<Valve className="org.apache.catalina.valves.RemoteIpValve"

remoteIpHeader="x-forwarded-for"

remoteIpProxiesHeader="x-forwarded-by"

protocolHeader="x-forwarded-proto"

/>

<Context path="" docBase="/home/apache-tomcat-8.5.8/webapps/docs" reloadable="false"/>

</Host>

</Engine>

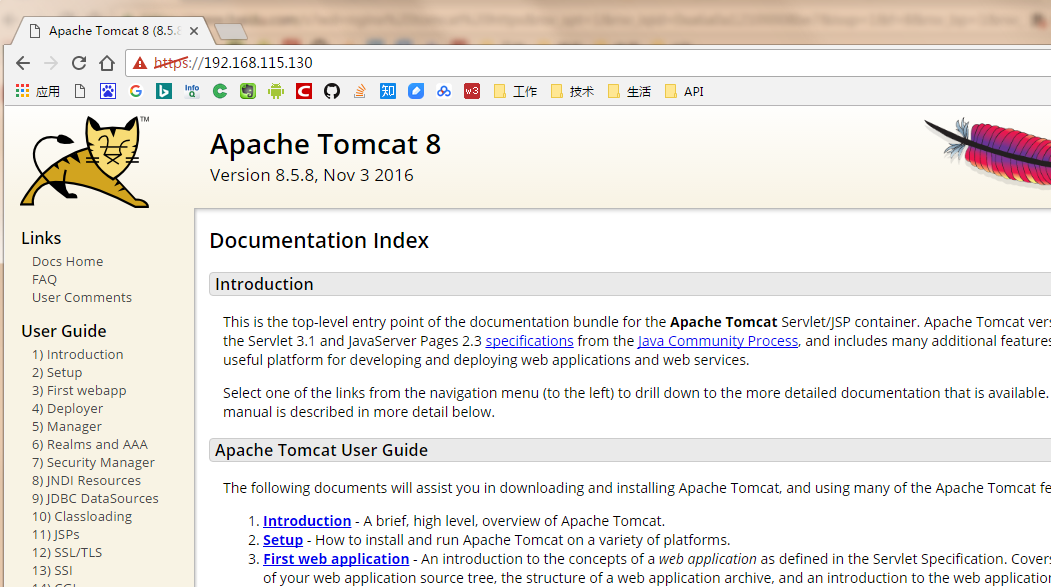
</Service>

</Server>

上述的配置中没有什么特别的，但是特别特别注意的是必须有 **proxyPort="443"**，这是整篇文章的关键，当然 redirectPort 也必须是 443。同时 **<Value>** 节点的配置也非常重要，否则你在 Tomcat 中的应用在读取 getScheme() 方法以及在 web.xml 中配置的一些安全策略会不起作用。

使用./startup.sh启动tomcat

正常此时访问<https://192.168.115.130>将出现如下图



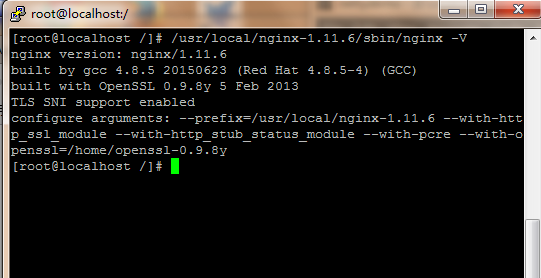
注释：

1、使用<Context >标签随意部署了一个tomcat自带的一个项目所以上图会显示tomcat启动完成时访问localhost:8080这样熟悉的界面

2、因为是自己颁发的证书，所以浏览器不认识，多个横线

Note:

1. 当然你也可以在centos命令行中使用wget直接获取nginx。
2. Nginx默认是没有编译Https模块的，需要自己手动编译，如果已经安装nignx，可以使用nginx –V查看当前nginx是否支持https



如果configure arguments中包含—with-http\_ssl\_module，则当前nginx已经支持https

注释: /usr/local/nginx-1.11.6是本文中的nginx的安装位置

参考资料

<http://www.oschina.net/question/12_213459>

<http://www.centoscn.com/nginx/2014/0506/2916.html>

<http://www.jb51.net/article/89313.htm>