operation 01

=============================================

**一，nginx基本应用**

**Nginx（"engine x"）**

**是俄罗斯人编写的HTTP服务工具**

**1，环境准备**

yum -y install vim //安装vim编辑器

yum list | grep bash //查询名字和bash有关的软件包

yum -y install bash-completion //安装支持tab键的软件包

装好之后，使用exit退出，重新登录才生效

Yum -y install net-tools //安装网络相关软件包

yum -y install psmisc //安装支持killall命令的软件

yum -y install gcc make //安装编译工具

yum -y install pcre-devel //安装可以让nginx支持正则的软件包

yum -y install openssl-devel //安装可以让nginx支持安装加密网站

的软件包

然后将lnmp\_soft.tar.gz 传入虚拟机的root家目录

scp /linux-soft/2/lnmp\_soft.tar.gz 192.168.2.5:

cd //到家目录

tar -xf lnmp\_soft.tar.gz //释放tar包

cd lnmp\_soft/

tar -xf nginx-1.17.6.tar.gz //释放nginx

cd nginx-1.17.6/ //进入nginx目录

./configure --prefix=/usr/local/nginx --user=nginx --with-http\_ssl\_module

//配置，--prefix是指定安装路径，--user是指定用户

--with-http\_ssl\_module是安全网站模块

make //编译

make install //安装

-------------------------------------------------------------

ls /usr/local/nginx/ //安装好之后查看目录

**conf 存放配置文件 sbin 存放主程序**

**html 存放网站页面 logs 存放日志**

------------------------------------------------------------

**开启服务并测试**

cd /usr/local/nginx

useradd nginx -s /sbin/nologin //创建用户

/usr/local/nginx/sbin/nginx //开启服务

sbin/nginx //使用相对路径开启服务也可以

sbin/nginx -V //查看nginx版本以及安装时带了哪些参数和模块

systemctl stop firewalld //关闭防火墙

使用真机的火狐浏览器打开192.168.2.5要看到nginx默认页面

sbin/nginx -s stop //关闭服务

sbin/nginx -s reload //重加载配置文件

**2，测试网站页面：**

echo "nginx-test~~~" > html/index.html //修改默认页

echo "abc-test~~~" > html/abc.html //创建新页面

<http://192.168.2.5> //打开浏览器访问默认页

<http://192.168.2.5/abc.html> //访问新页面

echo "我爱linux~~~" > html/abc.html

vim conf/nginx.conf //修改配置文件

charset utf-8; //第39行，添加utf-8支持中文

sbin/nginx -s reload //重加载配置

火狐访问192.168.2.5/abc.html //如果无效，可以

按ctrl+f5强制刷新

测试成品网站页面：

cd /root/lnmp\_soft

yum -y install unzip //安装解压缩工具

unzip www\_template.zip //解压缩网站模板

cp -r www\_template/\* /usr/local/nginx/html //拷贝网站模板文件

到nginx的网页目录

cp：是否覆盖"/usr/local/nginx/html/index.html"？ y

然后使用火狐访问192.168.2.5

--------------------------------------------------------------------------------

**二，为nginx增加网站认证功能**

修改nginx配置文件，在40、41行添加两句

vim conf/nginx.conf

auth\_basic "password"; //网页弹出的提示信息,此信息可能会根据

不同浏览器显示效果不一，有的浏览器甚至不显示，但不影响认证功能

auth\_basic\_user\_file "/usr/local/nginx/pass"; //存放网站账户的文件

sbin/nginx -s reload //重加载配置，检验之前配置，没有任何信息即可

yum -y install httpd-tools //之后安装软件包

htpasswd -c pass tom //创建pass文件，里面创建tom账户，之后

会要求输入两次密码

然后用火狐浏览器访问192.168.2.5，可以看到输入用户名密码的对话框、

输入用户名tom以及密码即可

htpasswd pass jerry //追加一个账户，名字是jerry

如果要反复测试网站认证功能，需要清空浏览器的历史记录

--------------------------------------------------------------------------------------

做完上述实验之后，可以按下列方法恢复nginx为默认状态

[root@proxy nginx]# cp conf/nginx.conf.default conf/nginx.conf //恢复nginx配置文件为默认状态

cp：是否覆盖"conf/nginx.conf"？ y

----------------------------------------------------------------------------------------

**三，创建虚拟主机**

**回顾**

**httpd**

<virtualhost \*:80>

servername [www.a.com](http://www.a.com)

documentroot /var/www/html

</virtualhost>

<virtualhost \*:80>

servername www.b.com

documentroot /var/www/b

</virtualhost>

**nginx配置虚拟主机**

http {

server { //第1个虚拟主机

listen 80;

server\_name [www.a.com](http://www.a.com);

root html;

index index.html;

}

server { //第2个虚拟主机

。。。。

。。。。

}

}

**打开nginx主配置文件在34~39行添加：**

server {

listen 80; //监听端口号

server\_name www.b.com; //域名，默认的虚拟主机改成www.a.com

root html\_b; //存放网页的目录

index index.html; //默认页名字

}

sbin/nginx -s reload //之后重新加载配置文件，服务必须是开启状态

[root@proxy nginx]# mkdir html\_b //创建b网站的目录

echo "nginx-A~~~" > html/index.html //创建a网站测试页

echo "nginx-B~~~" > html\_b/index.html //创建b网站测试页

vim /etc/hosts //修改hosts文件添加ip和域名的映射关系

192.168.2.5 www.a.com www.b.com

curl www.a.com //检测a网站或b网站都可以看到页面

**另外：**

windows环境配置hosts文件

C:\Windows\System32\drivers\etc\hosts

右键---属性---安全---编辑---users---完全控制打钩

--------------------------------------------------------------------------

**四，搭建安全网站**

**对称算法 AES DES 单机数据加密 使用相同字符串加密和解密**

**非对称算法 RSA DSA 网络数据加密 利用公钥(锁)加密，私钥(钥匙)解密**

**信息摘要 md5 sha256 数据校验**

**修改配置，实现安全加密网站**

[root@proxy nginx]# vim conf/nginx.conf //修改大概103~120行

server { //此处的虚拟主机自带ssl安全加密功能，将其范围的注释取消即可

listen 443 ssl;

server\_name www.c.com; //这里修改域名

ssl\_certificate cert.pem; //证书，包含公钥

ssl\_certificate\_key cert.key; //私钥

ssl\_session\_cache shared:SSL:1m;

ssl\_session\_timeout 5m;

ssl\_ciphers HIGH:!aNULL:!MD5;

ssl\_prefer\_server\_ciphers on;

location / {

root html\_c; //这里修改页面存储目录

index index.html index.htm;

}

}

**配置文件修改好之后，再去改/etc/hosts文件添加www.c.com**

[root@proxy nginx]# mkdir html\_c //创建安全网站的目录

[root@proxy nginx]# echo "nginx-C~~~~" > html\_c/index.html //创建安全网站的页面

**创建私钥与证书**

[root@proxy nginx]# openssl genrsa > conf/cert.key //创建私钥

[root@proxy nginx]# openssl req -x509 -key conf/cert.key > conf/cert.pem

//创建证书，证书中包含公钥，生成过程会询问诸如你在哪个国家之类

的问题，可以随意回答，但要走完全过程

Country Name (2 letter code) [XX]:dc 国家名

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

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

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

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

Common Name (eg, your name or your server's hostname) []:dc 服务器名称

Email Address []:dc@dc.com 电子邮件

**启动服务并测试**

[root@proxy nginx]# sbin/nginx //服务没开的话开服务

[root@proxy nginx]# sbin/nginx -s reload //已经开了的话重加载配置

[root@proxy nginx]# curl -k https://www.c.com //检验，-k是忽略风险

nginx-C ~~~~ //看到这个内容就说明实验成功

[root@proxy nginx]# systemctl stop firewalld //如果用真机的火狐浏览器测试需要

关闭防火墙，然后输入https://www.c.com 火狐浏览器测试仅限于真机是windows，

目前真机是linux的教学环境由于配置了dns，所以解析会失败，在linux环境只要用

curl的方式成功即可