**operation 运维 day 01**

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

**回顾：**

() 正则 保留 $( ) 获取命令的执行结果

$(( )) 运算 if(){ } for(){ }

$[ ] 运算 [条件测试]

a=10

echo ${a}XXX 变量名容易混淆时

${变量名称:} 截取

${变量名称/} 替换

${变量名称#} 掐头

${变量名称%} 去尾

${变量名称:-} 定义初值

awk BEGIN{ }{ }END{ }

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

**Nginx（"engine x"）**

**是俄罗斯人编写的十分轻量级的HTTP服务器**

**是一个高性能的HTTP和反向代理服务器，同时也是一个IMAP/POP3/SMTP 代理服务器**

**官方网站：http://nginx.org/**

**下面使用proxy主机配置nginx：**

**1，准备工作**

ip add show //查看ip

**安装常用工具：**

yum -y install bash-completion //安装支持tab键的工具包，安装完毕之后，要退出终端重新登录才生效

yum -y install vim //安装vim编辑器

yum provides XXX //查xxx工具来自哪个软件包

yum -y install net-tools //安装网络相关工具，比如ifconfig查询ip地址

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

nmcli connection modify ens33 connection.autoconnect yes //网卡开机自启

**2，Nginx环境搭建：**

1，找到lnmp\_soft.tar.gz，拷贝到虚拟机的root家目录，并释放到原地

2，释放lnmp\_soft目录中的nginx-1.17.6.tar.gz

yum -y install gcc //安装编译工具

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

yum -y install openssl-devel //让nginx搭建基于ssl（安全加密）

的网站

**3.编译安装**

./configure --with-http\_ssl\_module //配置，添加安全模块

make //编译

make install //安装

/usr/local/nginx/sbin/nginx //开启服务

./configure --help | grep http\_ssl //另外，可以用该方式搜索与http\_ssl有关的模块，--help可以看配置nginx时的配置选项与模块

cd /usr/local/nginx //进入nginx安装目录

ls //查看

**Nginx中的主要目录:**

**conf 存放配置文件**

**html 存放网页文件**

**sbin 存放主程序**

**logs 存放日志**

**4，使用nginx服务：**

/usr/local/nginx/sbin/nginx -V //查看版本已经添加的功能模块

/usr/local/nginx/sbin/nginx //开启

/usr/local/nginx/sbin/nginx -s stop //关闭

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

systemctl stop firewalld //关闭防火墙

[root@proxy nginx]# cd ~/lnmp\_soft/

[root@proxy lnmp\_soft]# yum -y install unzip //安装解压缩工具

unzip www\_template.zip //解压缩网页模板文件

cp -r www\_template/\* /usr/local/nginx/html/ 拷贝网站模板的文件到nginx的页面目录，会询问是否覆盖index.html，回答y然后使用浏览器访问192.168.2.5可以看到该网站

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

**为nginx增加网站认证功能**

**通常情况下网站搭建好之后，只要知道ip或者域名，那么任何用户都可以访问该网站，如果仅仅想让某些用户访问就可以使用该功能**

1， 首先打开nginx主配置文件,在第42行，43行添加

vim /usr/local/nginx/conf/nginx.conf

auth\_basic "password:"; //提示信息，用户登录网站时看到的

auth\_basic\_user\_file "/usr/local/nginx/pass"; //存放用户名密码的文件路径

2，yum -y install httpd-tools //安装网站工具包，支持htpasswd命令

htpasswd -c /usr/local/nginx/pass tom //创建网站的用户与密码文件，第1个用户名为tom（可以自定义），之后输入2次密码

cat /usr/local/nginx/pass //查看pass文件

3，/usr/local/nginx/sbin/nginx -s reload //如果nginx服务已经开启，就重加载配置文件

/usr/local/nginx/sbin/nginx //如果nginx服务没开启，就开启使用火狐浏览器打开192.168.2.5发现已经需要用户名和密码认证

htpasswd /usr/local/nginx/pass abc //追加新账户，无需c选项

如果要反复测试该功能，需要清空浏览器的历史记录

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

**还原nginx配置：**

**在conf目录中存放了nginx.conf.default，这是配置文件的备份，在重新做实验或者配置文件被破坏需要还原是可以用该文件拷贝覆盖nginx.conf**

cd conf/

[root@proxy conf]#

[root@proxy conf]# cp nginx.conf.default nginx.conf

cp：是否覆盖"nginx.conf"？ y

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

**通常使用一台服务器开启一个nginx服务就可以开启一个网站，但是如果公司需要很多不同域名的网站，而每个网站的业务量不大时，不必购买多台服务器，使用一台服务器利用虚拟主机技术既可以实现。**

**回顾虚拟主机**

**在httpd中配置：**

<virtualhost \*:80>

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

Documentroot /var/www/html

</ virtualhost>

**在nginx中配置(基本框架)：**

http {

server {

listen :80; //监听端口号

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

root html; //网站页面文件存储的位置

index index.html //默认页面

}

}

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

**正式配置**

**1，修改主配置文件，在34~39行开始添加以下内容**

34 server {

35 listen 80; //监听端口

36 server\_name www.b.com; //域名

37 root b; //网页文件存放地

38 index index.html; //默认页文件名

39 }

**2，准备测试页面**

cd /usr/local/nginx

mkdir b //创建b网站的页面存放目录

echo "proxy\_nginx\_web\_b~~~~~" > b/index.html //b网站内容

echo "proxy\_nginx\_web\_a~~~~~" > html/index.html //a网站内容

vim /etc/hosts 添加域名与ip的映射关系

192.168.2.5 www.a.com www.b.com www.c.com

curl www.b.com 测试b网站

curl www.a.com 测试a网站

如果在windows环境测试域名访问网站，需要修改hosts文件，添加一样的内容（hosts文件的权限需要设置为完全控制）

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

设置hosts的权限要先右键---属性---安全---编辑---users---完全控制勾选，然后右键该文件---打开方式---选择文本方式打开在最后一行下面写入与之前linux一样的内容

192.168.2.5 www.a.com www.b.com www.c.com

然后使用火狐浏览器访问www.a.com或者www.b.com

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

**搭建基于ssl技术的安全网站**

**1，了解加密算法**

**对称加密，适合单机环境**

加密和解密是相同密码

**非对称加密，适合网络数据传递**

加密和解密分别使用公钥和私钥

证书（包含公钥），可以用来加密

私钥 ，可以用来解密

**信息摘要，数据校验**

md5sum nginx.conf //使用md5工具计算nginx配置文件随机校验值，以后可以根据该校验值判断文件是否被篡改

**2，修改主配置文件第103行左右，找安全网站的虚拟主机的配置，将所有注释去掉，可以使用:103,120s/#//**

103 server {

104 listen 443 ssl;

105 server\_name www.c.com;

106

107 ssl\_certificate cert.pem; //证书文件

108 ssl\_certificate\_key cert.key; //私钥文件

109

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

111 ssl\_session\_timeout 5m;

112

113 ssl\_ciphers HIGH:!aNULL:!MD5;

114 ssl\_prefer\_server\_ciphers on;

115

116 location / {

117 root c;

118 index index.html index.htm;

119 }

120 }

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

**3，创建私钥与证书**

cd /usr/local/nginx/conf

openssl genrsa > cert.key 创建私钥

openssl req -new -x509 -key cert.key > cert.pem 根据刚刚创建的私钥，再创建证书(包含了公钥),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 国家名称

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

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

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

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

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

Email Address []:dc@dc.com 邮件地址

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

最后测试

[root@proxy nginx]# sbin/nginx -s reload 重新加载配置

使用火狐浏览器访问https://www.c.com/ 看到提示---高级---接收风险

或者使用curl -k https://www.c.com/ 用命令行的方式访问，使用-k选项可以忽略风险提示直接看网页内容

netstat -ntulp | grep nginx //查看nginx可以看到443端口已经开放