nmcli connection add type con-name eth1 ifname eth1

//添加网卡

**Nginx服务器**

安装

yum -y install gcc pcre-devel openssl-devel

//安装依赖包

useradd -s /sbin/nologin nginx

//创建nginx用户

yum list | grep pcre

包名-devel多为红帽的依赖包

带@的为已经装进系统里的,不带@则为未安装的包

解压配置安装起服务

tar -xf nginx-1.10.3.tar.gz

cd nginx-1.10.3

./configure \

>--prefix=/usr/local/nginx \ //指定安装路径

>--user=nginx \ //指定nginx用户

>--group=niginx \ //指定nginx用户组

>--with-http\_ssl\_module //启用加密功能模块

make && make install

//使用nginx的意义,如果用root登录,nginx被攻破时对方将获得root权限

/usr/local/nginx/sbin/nginx //启动服务

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

/usr/local/nginx/sbin/nginx -s reload //重新加载配置nginx必须开启

/usr/local/nginx/sbin/nginx -V //查看版本信息和配置信息

ln -s /usr/local/nginx/sbin/nginx /sbin/

//将nginx文件的软链接放如$PATH下可以,方便后期直接使用

**netstat命令**

-a //显示所有端口信息

-n //以数字格式显示端口号

-t //显示TCP链接的端口

-u //显示UDP链接的端口

-l //显示服务正在监听的端口信息

-p //显示监听端口的服务名称是什么

netstat -anptu | grep nginx

//查看nginx的端口信息

ss -anptu | grep 80

//查看80端口被哪个程序占用,并显示进程号,kill -9 强制杀死

//ss获取socket统计信息，ss比netstat效率更高

nginx需要关闭防火墙和selinux

**升级nginx**

升级前必须先停止nginx服务

升级时，配置文件和html等文件不需要改变，需要新版本的nginx按照老版本的配置文件编译后，将nginx文件复制到/usr/local/sbin/下，复制前先备份原有版本文件，老版本的配置文件可以通过nginx -V查看

mv /usr/local/nginx/sbin/nginx /usr/local/nginx/sbin/nginxold

//备份老版本文件

cp objs/nginx /usr/local/nginx/sbin/

//将objs目录下的nginx拷贝到原有目录中

make upgrade

//升级

nginx -v

//查看版本信息

//make upgrade是一个脚本,只是杀死nginx进程并再次启用,时间消耗短

//如果先停止服务,再重新复制nginx文件,消耗时间过长

//但make upgrade不是100%成功

客户端访问测试

curl http://192.168.1.100

//在终端中以文字形式显示页面html信息

**用户认证**

配置文件位置

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

在server\_name下方添加

auth\_basic "Input Password"; //认证提示信息

auth\_basic\_user\_file "/usr/local/nginx/pass"; //认证密码文件

nginx.conf文件中每一行后必须有分号;

加密需要httpd-tools文件支持

yum -y install httpd-tools

htpasswd -c /usr/local/nginx/pass tom //创建密码文件

htpasswd /usr/local/nginx/pass jerry //追加用户不需要写-c

//-c将覆盖原有的所有密码文件,相当重新创建pass文件

重启nginx服务

nginx -s reload

访问时需要输入用户名密码才能访问

**基于域名的虚拟主机**

nginx服务的根目录位于/usr/local/nginx下

配置文件位置

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

server {

listen 80; //监听端口

server\_name www.b.com; //域名

auth\_basic "Input Password"; //认证提示信息

auth\_basic\_user\_file "/usr/local/nginx/pass"; //认证密码文件

location / {

root www; //指定网站根路径

index index.html index.htm;

}

}

创建根目录及首页文件

mkdir /usr/local/nginx/www

echo 'www' > /usr/local/nginx/www/index.html

重启服务

客户端访问测试

配置本地域名解析hosts文件

192.168.4.5 www.b.com

**SSL虚拟主机**

加密算法

对称加密:AES,DES.用于单机数据加密,如压缩加密

非对称加密:RSA,DSA,用于网络数据加密

信息摘要:MD5,sha256(哈希值),用于校对数据完整性,数据秒传

配置SSL虚拟主机

生成私钥

cd /usr/local/nginx/conf

openssl genrsa > cert.key //生成私钥

openssl req -new -x509 -key cert.key > cert.pem

//生成证书

在配置文件/var/local/nginx/conf/nginx.conf最下面

去掉server前的注释

在server\_name下添加

ssl\_certificate cert.pem; //这里是证书文件

ssl\_certificate\_key cert.key; //这里是私钥文件

//此两行默认已存在

重启nginx服务

添加hosts,客户端访问测试