最小化安装的系统，通常需要安装的软件包：

yum -y install net-tools 支持ifconfig的安装包

yum -y install vim 支持vim编辑器的安装包

yum -y install bash-completion 支持tab键补全命令的安装包，安装完毕之后，需要退出账户从新登陆

yum -y install NetworkManager 支持nmcli的安装包

nmcli connection modify eth0 connection.autoconnect yes

练习一：部署nginx

1. 把lnmp\_soft.tar.gz传入虚拟机root家目录，然后释放tar包 tar -xf lnmp\_soft.tar.gz
2. 把nginx-1.12.2.tar.gz拷贝到/opt，然后释放

cp lnmp\_soft/nginx-1.12.2.tar.gz /opt

cd /opt

tar -xf nginx-1.12.2.tar.gz

1. 安装依赖工具

yum -y install gcc pcre-devel openssl-devel

gcc是编译工具，pcre-devel是让nginx支持正则表达式，openssl-devel是让nginx支持https（加密）网站

1. 编译安装nginx 并测试

cd nginx-1.12.2/

./configure --with-http\_ssl\_module 编译时添加加密模块

make

make install

cd /usr/local/nginx/ 前往安装目录，查看

conf 存放配置文件

html 存放网页文件

logs 存放日志

sbin 存放主程序

sbin/nginx -V 查看nginx版本，以及安装的模块等信息

sbin/nginx 启动服务

sbin/nginx -s stop 关闭服务

sbin/nginx -s reload 重置服务（重新读取配置文件）

netstat -ntulp | grep :80 查询80端口被谁占用

systemctl stop firewalld 关闭防火墙

使用浏览器访问 192.168.2.5

1. 测试页面

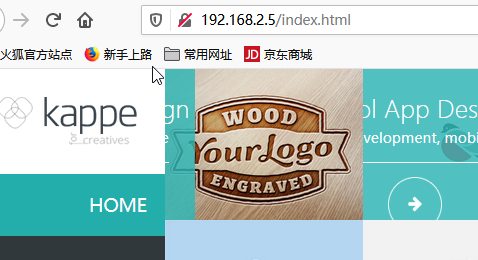
cd ~/lnmp\_soft

yum -y install unzip 安装解压缩zip的工具

unzip www\_template.zip 解压缩网页模板文件

cp -r www\_template/\* /usr/local/nginx/html/ 拷贝模板目录中所有文件到nginx的html目录中，是否覆盖默认页，输入y

再次使用浏览器访问服务器查看页面，看到下图则成功



另外，后期测试页面可以使用精简方式

rm -rf /usr/local/nginx/html/\* 先删除模板页面

cd /usr/local/nginx/

echo "proxy\_nginx\_test\_你好" > html/index.html

vim conf/nginx.conf 修改主配置文件

charset utf-8; 在第40行添加支持中文的配置

sbin/nginx -s reload 重置服务

然后从新使用浏览器访问服务器，可以使用ctrl+F5强制刷新

练习二：使用nginx实现账户认证

1. 修改主配置文件 ，在38、39行添加以下内容

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

auth\_basic "password" ; 提示信息

auth\_basic\_user\_file "/usr/local/nginx/pass"; 网站用户信息的存放文件路径

yum -y install httpd-tools 安装可以生成认证文件的工具

htpasswd -c /usr/local/nginx/pass tom 创建认证文件，并添加tom账户，需要输入2次密码

sbin/nginx -s reload 重置nginx服务

使用浏览器访问网站时发现需要输入用户名和密码

如果再次测试该功能时，可能需要清除浏览器的缓存

htpasswd /usr/local/nginx/pass jerry 追加账户，不能添加-c选项，否则是覆盖

sbin/nginx -s reload 重置nginx服务

练习三：使用nginx配置虚拟主机

在httpd中配置虚拟机主机的格式：

<virtualhost \*:80>

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

documentroot /var/www/html

</virtualhost>

在nginx中配置虚拟主机的格式：

http {

server {

listen 80;

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

root html;

index index.html index.htm;

}

server {

listen 80;

server\_name www.b.com;

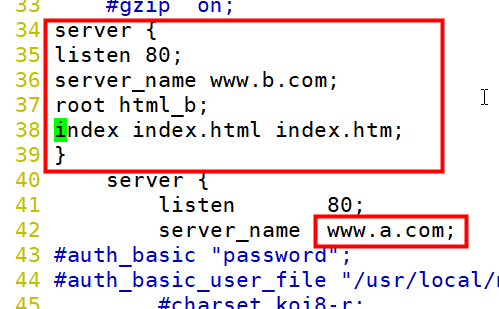
root html\_b;

index index.html index.htm;

}

}

1，修改nginx主配置文件，可以注释之前的用户认证配置，然后按下图添加虚拟主机[www.b.com](http://www.b.com)，另外将默认虚拟主机的域名改为[www.a.com](http://www.a.com)



1. 修改完配置之后，在nginx默认的安装路径创建html\_b目录

mkdir /usr/local/nginx/html\_b 创建b网站的目录

cd /usr/local/nginx

echo proxy\_web\_b > html\_b/index.html 创建b网站的默认页面

sbin/nginx -s reload 重置nginx服务

1. 打算使用哪台主机做客户机测试，就去修改哪台主机的hosts文件，添加a网站和b网站的域名解析

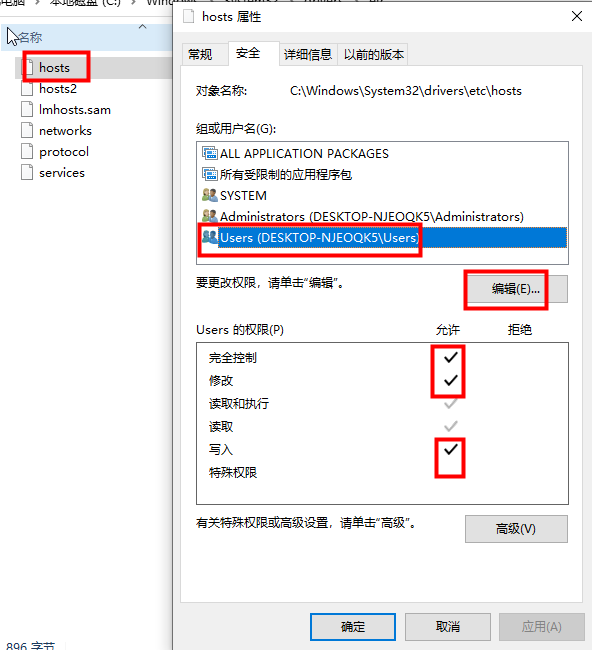
vim /etc/hosts

192.168.2.5 [www.a.com](http://www.a.com) [www.b.com](http://www.b.com) 最后一行追加

如果修改Windows的hosts文件，最后一行写入与上述一致内容即可，改完即可使用浏览器尝试a与b网站的访问

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

修改时，可能需要用 右键>属性>安全,设置users的权限为完全控制



练习四：创建加密网站

http 80 不加密

https 443 加密

加密算法一般分为对称算法、非对称算法、信息摘要。

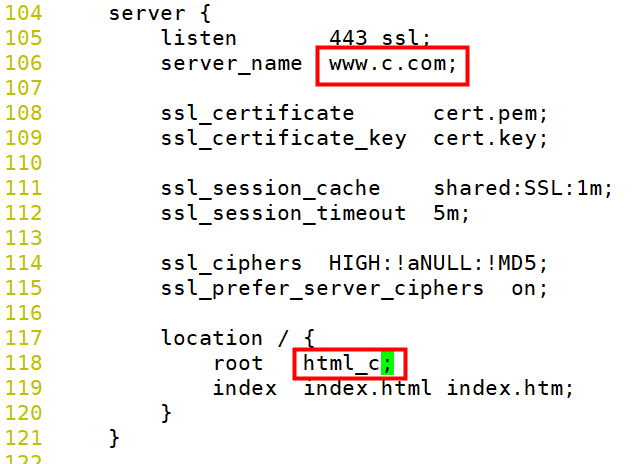
对称算法有：AES、DES，主要应用在单机数据加密。

非对称算法有：RSA、DSA，主要应用在网络数据加密。

信息摘要：MD5、sha256，主要应用在数据完整性校验。

非对称算法使用公钥加密，私钥解密

1. 修改主配置文件，在大概106行左右的位置删除安全加密网站模板的#，可以使用 :104,121s/#//



2，创建c网站的页面

cd /usr/local/nginx

mkdir html\_c

echo proxy\_web\_c > html\_c/index.html

3，创建私钥和公钥

cd conf/

openssl genrsa > cert.key 生成私钥

openssl req -x509 -key cert.key > cert.pem 根据私钥生成公钥，过程中会询问公司，国家，部门等信息，随意填写即可

cd .. 返回上级目录

sbin/nginx -s reload 重置nginx服务

4，测试

再修改hosts文件添加 [www.c.com](http://www.c.com)即可

192.168.2.5 [www.a.com](http://www.a.com) [www.b.com](http://www.b.com) [www.c.com](http://www.c.com)

最后使用火狐浏览器访问<https://www.c.com>

看到风险提示可以选择高级> 确认安全例外即可



如果使用linux系统的命令行测试，首先在hosts文件添加c网站的域名

vim /etc/hosts

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

curl -k <https://www.c.com>