**Morning：**

1. Web服务器分类

1）Unix和Linux平台：

与PHP、Python、Perl语言组合：

Apache（旧项目）、Nginx（性能、并发量更优）

Tengine（淘宝引擎、基于Nginx优化而成）、Lighttped

与java语言组合：

Tomcat、IBM WebSphere、Jboss

2）Windows平台；

微软公司的IIS(Internet Information Server)

1. 构建Nginx服务器

**-Nginx源码包安装**

1. tar -xf nginx-1.10.3.tar.gz && cd nginx-1.10.3.tar.gz
2. yum安装gcc、pcre-devel（兼容perl版本的正则，与shell有区别）、openssl-devel（加密网站）

#红帽光盘内，以devel结尾的都是依赖包

2）useradd -s /sbin/nologin nginx（建立普通用户，用于启服务）

#计算机安全机制(权限)-->用户，为了保护web服务器的安全

1. ./configure \ #指定安装目录、功能模块等（检测gcc）

> --prefix=/usr/local/nginx \ #安装目录

> --user=nginx \ #账户名

> --group=nginx \ #组名称

> --with-http\_ssl\_module #安装模块，支持加密功能

#所有的模块放在源码包解压目录的./scr下

#./configure结束后多了一个./objs，里面放置了主程序、安装模块等

#--with-模块名、--without-模块名，分别表示安装/不安装模块

#现代化软件都是模块化（可自定义安装、也有默认模块）

1. make && make install #编译、安装
2. 查看安装结果ls /usr/local/nginx/

conf 配置文件 html网页 logs日志 sbin主程序

1. 建立nginx主程序快捷方式

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

**-Nginx命令的用法**

nginx #启动服务

nginx -s stop #关闭服务

nginx -s reload #不关服务，重新加载配置文件

nginx -V #查看软件信息，包括版本、安装信息等

netstat -alnptu #查看系统中启动的端口信息

-a显示所有端口的信息 -n以数字格式显示端口号

-t显示TCP连接的端口 -u显示UDP连接的端口

-l只显示**服务**正在监听的端口信息，如httpd启动后，会一直监听80端口

-p显示监听端口的服务名称是什么（也就是程序名称）

**-设置防火墙与SELinux**

**-测试首页文件**

curl <http://192.168.4.5> #Linux命令行网页，用于验证

**Afternoon：**

1. 升级Nginx服务器

**-编译新版本Nginx软件**

1. 解包、进入目录
2. ./config（指定信息与旧版一致）
3. make（不需install）

**-替换老版本主程序**

1）备份旧版主程序

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

2）拷贝新版本

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

1. 将运行的nginx程序切换成新版本

方法1：make upgrade #升级，但脚本有可能出错

方法2：killall nginx && /usr/local/nginx/sbin/nginx #杀死后重启

1. 查看程序版本

/usr/local/nginx/sbin/nginx -v

**-客户端访问测试**

curl <http://192.168.4.5>

1. Nginx主配置文件框架

默认路径/usr/local/nginx/conf/nginx.conf

#######################################

2 user nobody; #进程所有者

3 worker\_processes 1; #启动进程数量

程序(grogram) 存在硬盘

进程(process) 读到内存；多进程可以提高并发量，但独占内存

线程(thread) 在进程下启n个线程，共享该进程所占内存

5 error\_log logs/error.log; #日志文件

9 pid logs/nginx.pid; #pid文件

13 worker\_connections 1024; #单个进程最大并发量

#######################################

全局配置（用户名、日志、进程）

http{

server{

listen 80; #定义网页端口

server\_name localhost; #域名

root html; #网页根目录（允许绝对/相对路径）

}

server{

listen 80;

server\_name www.xyz.com;

location / { #发布目录

root “/usr/local/nginx/www”;

index index.html index.htm; #默认首页文件名

}

}

}

注意：保证{}成对出现，必须分号结尾，否则服务无法正常启动/停止。

1. 网站用户认证

作用：为了控制外部的访问，如：公司内部的监控、boss系统等

1. 修改Nginx主配置文件

server{

...

auth\_basic “Input Password:”; #认证提示字段

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

}

1. 生成密码文件，创建用户及密码

yum -y install httpd-tools #密码文件生成工具

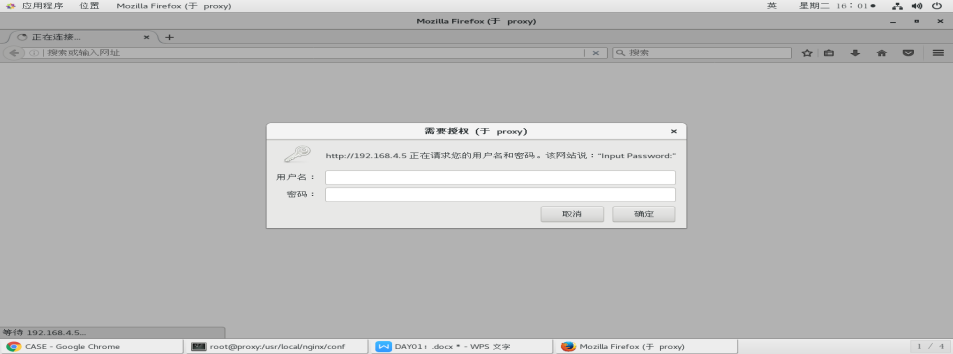
htpasswd -c /usr/local/nginx/pass tom #创建密码文件

htpasswd /usr/local/nginx/pass jerry #追加用户，无-c选项

cat /usr/local/nginx/pass #查看密码文件

1. 客户端测试

firefox http://192.168.4.5



1. 基于域名的虚拟主机

-公司常用的网站；

www.xx.com 门户

mail.xx.com 邮箱

mall.xx.com 商城

bbs.xx.com 论坛

1. 修改主配置文件的server{}标签

#charset utf-8支持中文

域名1： server\_name [www.a.com;](http://www.a.com;)

root html;

域名2： server\_name [www.b.com;](http://www.b.com;)

root www;

1. 创建网站根目录及对应首页文件

mkdir /usr/local/nginx/www

echo “www” > /usr/local/nginx/www/index.html

1. 重启nginx服务

/usr/local/nginx/sbin/nginx -s reload

1. 客户端测试：

echo “192.168.4.5 [www.a.com](http://www.a.com) www.b.com >> /etc/hosts

#修改主机映射记录

firefox http://www.a.com #显示html目录下的首页

firefox <http://www.b.com> #显示www目录下的首页

firefox 192.168.4.5 #默认显示第一个server的网页

1. 【拓展】基于端口/IP的虚拟主机

-基于端口的虚拟主机

端口1： listen 8080;

server\_name www.a.com;

端口2： listen 8000;

server\_name www.a.com;

-基于IP的虚拟主机

IP1： listen 192.168.4.5:80

server\_name www.a.com;

IP2： listen 192.168.2.5:80

server\_name www.a.com;

1. SSL虚拟主机（https）

-加密算法

对称加密：加密解密同一钥匙（适用单机加密），算法AES、DES

非对称加密：公钥(证书)加密、私钥解密（适用网络加密），RSA、DSA

CA：第三方权威机构，唯一可以承认公钥、私钥的机构。（实验环境下载CA证书是模拟权威机构、真实环境下必须到https证书申请购买）

信息摘要(HASH)：数据完整性校验，MD5、sha256

#命令行：md5sum 文件名 （生成的校验码与文件内容有关）

1. 生成私钥与证书

cd /usr/local/nginx/conf

openssl genrsa > cert.key #生成rsa私钥，配置文件默认名为cert.key

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

#生成证书，x509是证书的文件类型

Country Name (2 letter code)：CN #填写国家

Provice、City、Organization、Name、Email

#填写省份、城市、部门、姓名、邮箱

1. 修改Nginx配置文件

server {

listen 443 ssl;

server\_name www.c.com;

ssl\_certificate cert.pem; #证书文件

ssl\_certificate\_key cert.key; #私钥文件

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

ssl\_session\_timeout 5m; #请求超时5min

ssl\_ciphers HIGH:!aNULL:!MD5;

#指定为高级别加密算法，！为不使用

ssl\_prefer\_server\_ciphers on;

location / {

root html;

index index.html index.htm;

}

}

1. 重启Nginx服务，nginx -s reload
2. 客户端验证：

vim /etc/hosts

firefox https://www.c.com