一. httpd是什么

httpd是一个开源软件，且一般用作web服务器来使用。目前最流行的web服务器软件叫做httpd，

在早期的http server就叫做apache，到了http server 2.0以后就改名为httpd了。

所以有时候听到apache服务器和httpd服务器其实都是指得是一个意思。

二. httpd的安装及设置

1. 安装httpd服务器

sudo yum install httpd httpd-tools httpd-manual -y

2. 对配置文件做语法检查

httpd -t

3. 查看版本

httpd -V

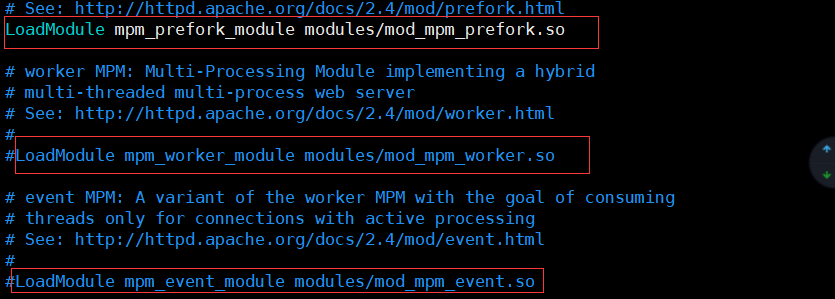
4. 修改模式

编辑文件/etc/httpd/conf.modules.d/00-mpm.conf，根据需要启用相应的行

LoadModule mpm\_prefork\_module modules/mod\_mpm\_prefork.so

# LoadModule mpm\_worker\_module modules/mod\_mpm\_worker.so

#LoadModule mpm\_event\_module modules/mod\_mpm\_event.so



5. 查看80端口是否有监听

netstat -ntlp

6. 配置文件

1). 主配置文件

/etc/httpd/conf/httpd.conf

2). 其他配置文件

/etc/httpd/conf.d/的所有配置文件

7. 设置局域网网页和共享

PPP1

PPP2

#注意，这些配置有些在虚拟主机下不能生效，应该在真实主机上运行

apache 常用设置指令

ServerRoot "/etc/httpd"

PidFile run/httpd.pid

Timeout 60

KeepAlive On

MaxKeepAliveRequests 100

KeepAliveTimeout 15

Listen 80

#Listen 12.34.56.78:80

Include conf.d/\*.conf <-- 把 $ServerRoot/conf.d/下面所有的.conf文件都包含进来

User apache <-- httpd进程的用户身份

Group apache <-- httpd进程的组身份

ServerAdmin root@localhost <-- 管理员邮箱

DocumentRoot "/var/www/html" <-- 网站根目录

DirectoryIndex index.html <-- 设置默认主页文件



AccessFileName .htaccess <-- 访问控制文件的名字

ErrorLog logs/error\_log <-- 错误日志的存放位置

LogLevel warn <-- 日志等级

访问控制:(PPP3)

Order allow,deny

Allow from all

allow 和 deny 如何结合？

类似于层叠样式表 css.

指令的容器：

Directory: 针对文件系统上的一个目录

Files: 针对指定的文件，可以是全局的，也可以是在某个Directory下

Location: 针对网址的控制

PPP1. 设置简单的网页

1. sudo iptables -F

sudo setenforce 0

2. 在 /var/www/html里面创建一个文件index.html， 添加内容

3. 重启服务

sudo systemctl restart httpd

4. 127.0.0.1 / 192.168.0.\*

PPP2. 自定义httpd根目录

1. 备份主配置文件

2. 编辑原配置文件

3. 在文件中修改

DocumentRoot "/www"

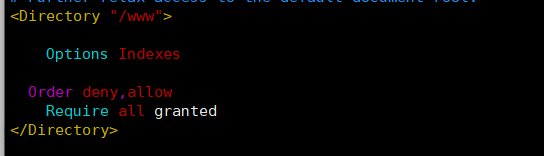
<Directory "/www">

Options Indexes

Order deny,allow

Require all granted

</Directory>



4. 创建目录， 修改所有者

5. 创建一个文件index.html， 添加内容

6. 重启服务

7. 127.0.0.1 / 192.168.0.\*

PPP3 httpd文件共享

1. 把网站家目录设置为/www

2. 清空/www文件夹下面的东西

3. 允许列出网站根目录里面的内容

4. 不允许列出网站根目录下面的子目录secret 里面的内容

5. 不允许访问所有目录下的.jpg 文件，但是images 目录除外

6. 在/www目录下面创建1\_root.jpg 2\_root.jpg 3\_root.jpg 4\_root.jpg

7. 在/www/images目录下面创建1\_image.jpg 2\_image.jpg 3\_image.jpg 4\_image.jpg

8. 在/www/secret目录下创建一些文件

参考配置

DocumentRoot "/www"

<Files ~ "\.jpg$">

Order allow,deny

Require all denied

</Files>

<Directory "/www">

Options Indexes

Order deny,allow

Require all granted

</Directory>

<Directory "/www/secret">

Options -Indexes

</Directory>

<Directory "/www/images">

<Files ~ "\.jpg$">

Order deny,allow

Require all granted

</Files>

</Directory>



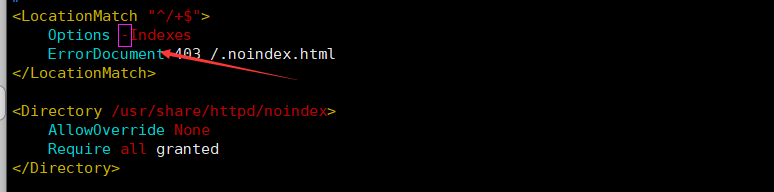
ps: /etc/httpd/conf.d/welcome.conf

<LocationMatch "^/+$">

Options Indexes <-- 把 - 去掉

ErrorDocument 403 /.noindex.html

</LocationMatch>



创建文件

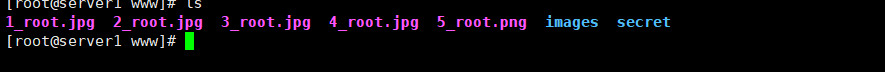
touch /www/{1\_root.jpg,2\_root.jpg,3\_root.jpg,4\_root.jpg,5\_root.png}

mkdir /www/images/

touch /www/images/{1\_image.jpg,2\_image.jpg,3\_image.jpg,4\_image.jpg}

mkdir /www/secret/

touch /www/secret/{1.txt,2.txt}



输入url访问：http://192.168.224.11



会发现相对应的文件看不了。.jpg结尾的看不了，其他的可以看

三. 对目录的访问进行密码控制(PPP4)

1. 创建访问控制文件

需要控制哪个目录及其子目录，就在Directory 指令里指定哪个目录

<Directory "/var/www/html/secret">

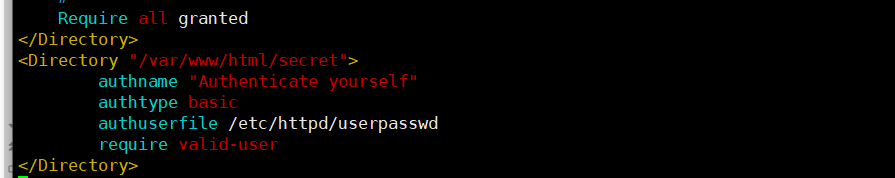
authname "Authenticate yourself"

authtype basic #基于Basic认证

authuserfile /etc/httpd/userpasswd #指定账号文件

require valid-user #指定允许登录的用户，valid-user表示账号文件内的所有用户

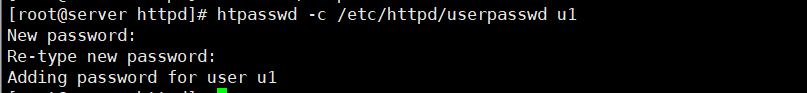
</Directory>



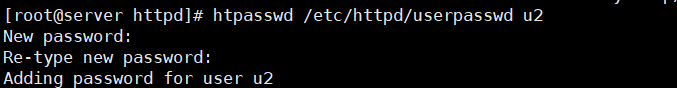
2. 创建账户文件

htpasswd -c /etc/httpd/userpasswd u1 <-- 创建该文件并添加用户u1

htpasswd /etc/httpd/userpasswd u2 <-- 添加用户u2



密码2 和22





3. 重启httpd服务

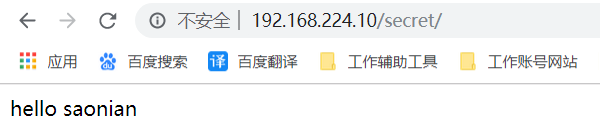
如果一个目录使用密码控制访问，那么在通过网页浏览器列出该目录的父目录时，看不到该目录，也就是说，该目录被隐藏了。但是可以通过直接输入url来访问。

mkdir /var/www/html/secret/

echo "hello saonian" > /var/www/html/secret/index.html

输入url访问 <http://192.168.224.10/secret/>





PPP4. 用密码来保护 /www/books 路径

1. 书写配置

<Directory "/www/books">

Options Indexes FollowSymLinks

order allow,deny

allow from all

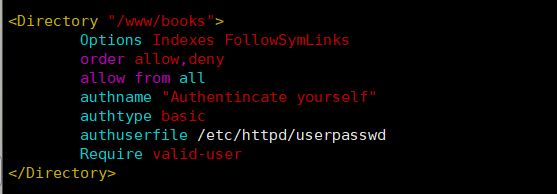
authname "Authenticate yourself"

authtype basic

authuserfile /etc/httpd/userpasswd

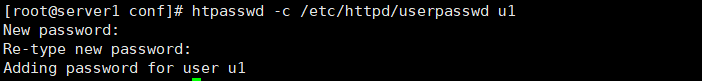
Require valid-user

</Directory>



2. 创建用户

htpasswd -c /etc/httpd/userpasswd u1

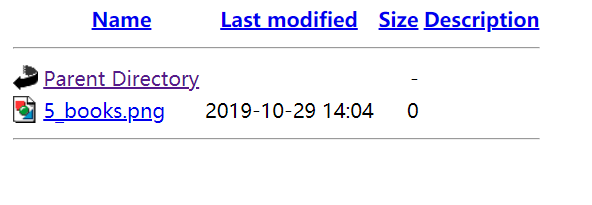


3. 重启 httpd 服务

mkdir /www/books

touch /www/books/{1\_root.jpg,2\_root.jpg,3\_root.jpg,4\_books.jpg,5\_books.png}

然后输入url访问：



只能访问.png的，因为jpg的不能访问

四. 基于域名的虚拟主机(PPP5)操练虚拟主机的配置

1. 配置两个虚拟主机，名字分别是:

web1.abc.com

web2.abc.com

2. 文档根目录分别如下，要求其中的index.html文件显示不同的内容

/www/web1

/www/web2

3. 通过DNS服务器解析两个域名

参考步骤：

0. 本方案基于以下假设：

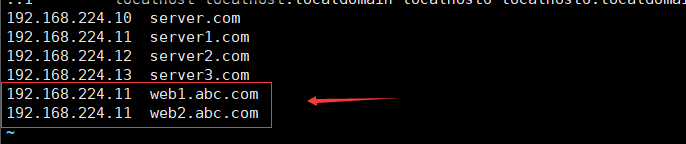
虚拟主机 web1.abc.com 的文档根目录：/www/web1

虚拟主机 web2.abc.com 的文档根目录：/www/web2

1. 配置DNS，设定以下的域名与IP的映射：

127.0.0.1 web1.abc.com

127.0.0.1 web2.abc.com



2. 在客户端配置 /etc/resolv.conf 文件，然后测试DNS可以正常解析，并且主机能够连通：

# vi /etc/resolve.conf, 删除里面原有内容，添加以下一行

nameserver 192.168.224.2

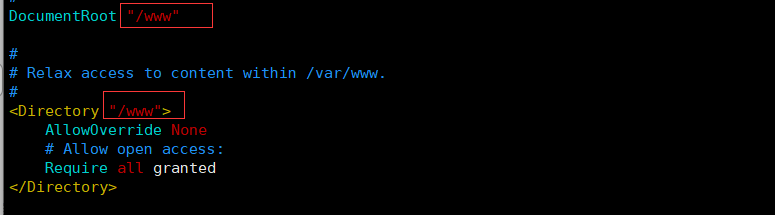
# ping web1.abc.com

# ping web1.abc.com

编辑主配置文件修改根目录

vim /etc/httpd/conf/httpd.conf

DocumentRoot "/www"



3. 编辑httpd的子配置文件 /etc/httpd/conf.d/vir.conf，添加以下内容：

<VirtualHost \*:80>

DocumentRoot /www/web1

ServerName web1.abc.com

<Location />

options Indexes

order deny,allow

allow from all

</Location>

</VirtualHost>

<VirtualHost \*:80>

DocumentRoot /www/web2

ServerName web2.abc.com

<Location />

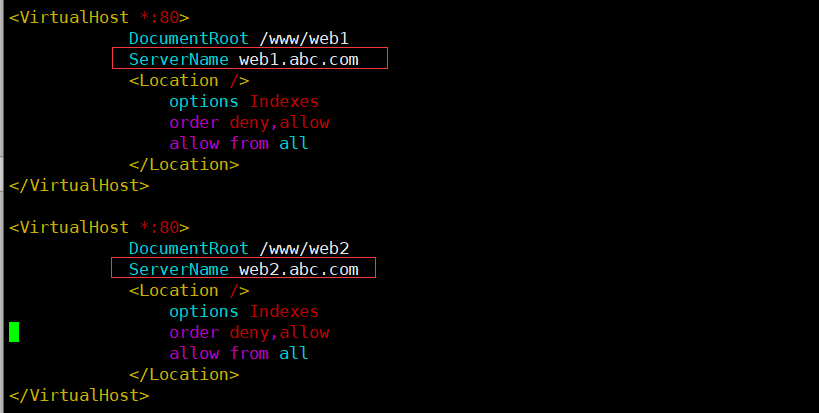
options Indexes

order deny,allow

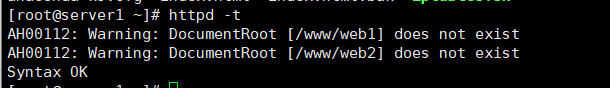
allow from all

</Location>

</VirtualHost>



报下面的错误是因为没有创建相关目录，创建好就可以了。



4. 在两个虚拟主机的文档根目录下创建 index.html文件，内容分别如下：

mkdir /www/{web1,web2} -p

# /www/web1/index.html

<h2>Web1</h2>

# /www/web2/index.html

<h2>Web2</h2>

1. 重启httpd服务器



sudo systemctl restart httpd

6. 在客户端，分别打开以下网址，查看内容是否不同：

http://web1.abc.com

http://web2.abc.com

别名：把URL映射到文件系统路径

Alias URL-path file-path|directory-path

例子：把系统上面的目录/external/software 映射到URL http://192.168.224.10/software

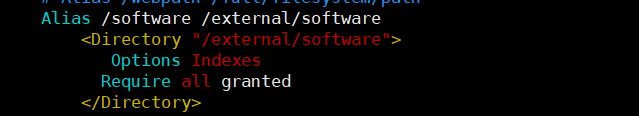
Alias /software /external/software

<Directory "/external/software">

Options Indexes

Require all granted

</Directory>



重启httpd

mkdir /external/software/ -p

echo "nihoa alias" > /external/software/index.html

然后浏览器访问<http://192.168.224.10/software/>这里面的文件，

就相当于访问/external/software/index.html 这里的了

五. 配置https

1. 安装模块和工具

sudo yum install mod\_ssl openssl -y

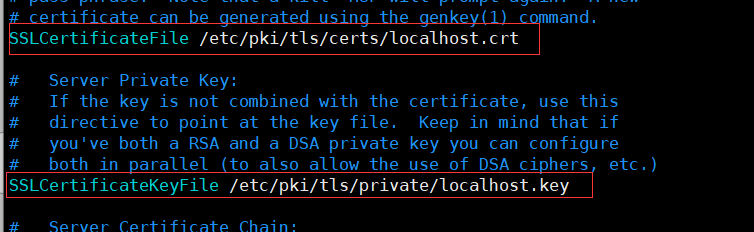
2. 写配置

vi /etc/httpd/conf.d/ssl.conf

以下配置项用于指定私钥和证书（公钥）

SSLCertificateFile /etc/pki/tls/certs/localhost.crt

SSLCertificateKeyFile /etc/pki/tls/private/localhost.key



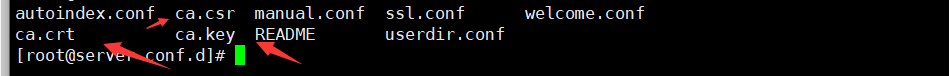
3. 预备证书和key

openssl genrsa -out ca.key 2048

openssl req -new -key ca.key -out ca.csr

一直回车

openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt



4. 将ca.crt移动并重命名为/etc/pki/tls/certs/localhost.crt，

ca.key移动并重命名为/etc/pki/tls/private/localhost.key

5. https的端口为443，应在httpd.conf里，将该网站监听的端口改为443

6. 重启服务

sudo systemctl restart httpd

PPP6. 综合实验

要求：

1. 关闭iptables，关闭SELinux

2. 把文件系统目录 /www 设为网站根目录

3. 把网站默认主页名称设为 index.html

4. 网站根目录允许列目录功能(Indexes)

5. 在网站根目录下面创建文件 main.do, 内容为 "main page" （不包含双引号）

6. 在网站根目录下面创建一个目录 special，只允许IP 为192.168.0.223 和 本机127.0.0.1 访问

7. 在网站根目录下面创建空文件 special/data

8. 网站里面所有（除了第9步中的目录）扩展名为.jpg, .png 的文件，禁止所有人访问

9. 在网站根目录下面创建一个目录 images，里面扩展名为 .png 的文件允许所有人访问

10. 在网站根目录下面创建以下空文件

file.jpg

file.png

file.bmp

images/file.jpg

images/file.png

11. 在文件系统上创建一个目录 /www\_admin, 用别名的方式把该目录映射成网站路径 /admin，该路径允许列目录功能

12. 在文件系统上创建空文件 /www\_admin/data

13. 在网站根目录下面创建一个目录 secret，里面的内容需要提供用户名和密码才能访问，用户名和密码都设置成 abc

14. 在文件系统上创建文件 /www/secret/data, 内容为 "secret message"（不包含双引号）

15. 在网站根目录下创建一个软连接，指向系统目录 /etc，使得可以通过网址

http://192.168.0.\*/etc/fstab 的形式来访问文件 /etc/fstab, /etc 下的其它文件不允许访问

预期效果

假设服务器IP 地址为 192.168.0.183

1. 访问http://192.168.0.183 能列出网站根目录，看到文件main.do

2. 访问http://192.168.0.183/main.do 能看到内容 "main page"（不包含双引号）

3. 只有192.168.0.220 和 192.168.0.183才能访问http://192.168.0.183/special

4. 访问http://192.168.0.183 看到的图片文件只有file.bmp

5. 访问http://192.168.0.183/images 看到的图片文件只有file.png

6. 访问http://192.168.0.183/admin/ 能看到文件列表，里面有文件data

7. 访问http://192.168.0.183/secret/data 需要用户名和密码，输入用户名abc 和密码abc 后能看到内容 "secret message"（不包含双引号）

8. 可以访问http://192.168.0.183/etc/fstab

9. 不能访问http://192.168.0.183/etc/passwd

参考配置（只包含修改/增加的部分）

DocumentRoot "/www"

<Directory "/www">

Options Indexes

AllowOverride None

Order allow,deny

Allow from all

</Directory>

DirectoryIndex index.html

<Directory "/www/special">

order deny,allow

deny from all

allow from 192.168.0.183 127.0.0.1

</Directory>

<Files ~ "\.(jpg|png)$">

order deny,allow

deny from all

</Files>

<Directory "/www/images">

<Files ~ "\.png$">

order deny,allow

allow from all

</Files>

</Directory>

Alias /admin "/www\_admin"

<Directory "/www\_admin">

Options Indexes

Order deny,allow

Allow from all

</Directory>

# 除了以下的配置之外，还需要创建用户

# 可以使用以下命令来创建用户：

# htpasswd -c /etc/httpd/userpasswd abc

#

<Directory "/www/secret">

authname "Authenticate yourself"

authtype basic

authuserfile /etc/httpd/userpasswd

require valid-user

</Directory>

<Directory "/www/etc">

Order allow,deny

Deny from all

<Files ~ "^fstab$">

order deny,allow

allow from all

</Files>

</Directory>

--------- end of 综合实验 ------------------------------------------------