认证授权和访问控制

ip访问控制：

目录控制语句以<Directory 目录名>开头；以</Directory>结束。
先允许后拒绝，默认拒绝所有：Order allow,deny
先拒绝后允许，默认允许所有：Order deny,allow

AllowOverride None：不允许覆盖，即不允许从根目录向子目录覆盖。即默认情况下拒绝从根目录下向子目录访问，如果要看根目录下的一个子目录，必须先打开子目录的访问权限。

Order allow，deny：访问控制的顺序，先匹配允许，再匹配拒绝，默认拒绝。
Allow from all：表示允许任何地址访问。
Allow from 172.18.49.0/24
Deny from 172.18.49.102

用户身份认证授权

主要参数
Authtype 是认证类型 Basic apache自带的基本认证
Authname 认证名字，是提示你输入密码的对话框的提示语
Authuserfile 是存放认证用户的文件
require user 用户名 允许指定的一个或多个用户访问，如果认证文件里面还有其他用户，还是不能访问
require valid-user 所有认证文件里面的用户都可以访问
require group 组名 授权给一个组，较少用

```
vim /etc/httpd/conf/httpd.conf
-----------------------------------------
<VitrualHost 172.18.211.100>
   Document Root /www/wg
   <Directory /www/wg>认证的目录
   AuthType Basic   认证的方法：密码
   AuthName Password! 登录框的提示
   AuthUserFile /etc/httpd/webpasswd 验证的文件
   require user tom 认证的要求
   </Directory>
</VitrualHost>
-----------------------------------------
```

htpasswd -c /etc/httpd/webpasswd tom 创建/etc/httpd/webpasswd并且将tom加入验证文件，为tom设置密码
htpasswd /etc/httpd/webpasswd jack 将jack加入验证文件，为jack设置密码

源码包安装httpd

一、配yum

1.挂光驱 mount /dev/sr0 /media
2.vim /etc/yum.repo.d/wg.repo

```
-----------------------------
[local]
name = wg
baseurl = file:///media  软件路径
gpgcheck = 0 不做软件包验证
```

enable =1 启用

二、安装FTP服务器上传httpd源码包

yum -y install vsftpd
getenforce 0 设置SELinnux为警告模式
useradd tom -s /sbin/nologin 创建用户tom，限制tom不能登录到系统
上传httpd源码包

三、安装编译软件gcc make

yum -y instabll gcc make

四、编译安装

tar -xvf httpd..... 解包
cd httpd....
./configure &&make &&make install 编译安装源码包

五、测试

源码包安装默认
网站根目录 /usr/local/apache2/htdocs/
主页 index.html
主配置文件 /usr/local/apache2/conf/httpd.conf
启动服务 /usr/local/apache2/bin/apachectl start

六、配置虚拟主机（同前）

配置DNS 实现正确解析www.wg.com www.rg.com
配置基于域名的虚拟主机，方法同前

Https
1.安装Apache
2.安装mod_ssl模块
Yum -y install httpd.* mod_ssl.*
3.创建网站 直接用虚拟主机配置站点
/var/www/wg 下创建index.html
4.创建保存证书的文件夹
Mkdir /etc/httpd/.sslkey 权限400 chmod -R 400 /etc/httpd/.sslkey
Openssl genrsa -out server.key 1024 生成私钥
Openssl req -new -x509 -key server.key -out server.crt 生成公钥
设置信息
注意主机名项用访问站点时的主机名
修改Apache主配置文件监听端口443
<VirtualHost 192.168.0.1:443>
……
SSLEngine on开启证书引擎
SSLCertificateFile /etc/httpd/.sslkey /server.crt
SSLCertificateKeyFile /etc/httpd/.sslkey /server.key
指明公钥私钥文件
</VirtualHost>
重启Apache
5.测试
默认不信任 会有警告 但是可以访问

不出现警告
1.删除刚建立的密钥对

4.创建证书
Openssl genrsa -des3 -out ca.key 1024 生成ca的私钥
Openssl req -new -x509 -key ca.key -out ca.crt 生成ca的公钥

Openssl genrsa -des3 -out server.key 1024 生成私钥
Req -new -key server.key -out server.csr 生成公钥请求文件

通过ca颁发请求文件
颁发的脚本sign. sh
./sign.sh server.csr

生成server. crt文件

修改配置文件
打开引擎
指明密钥

启动Apache 输入私钥密码

测试 依然会有警告

将ca. crt复制到windows下
双击 安装证书
运行--mmc(控制台)-查看 添加管理单元--证书
受信任的根证书颁发机构 中有刚导入的证书
再访问 该证书是由已信任机构颁发

设置客户端有证书才能访问
Apache配置文件添加
SSLVerifyClient require 有证书才能浏览
SSLverifyDepth 1
重启服务

再访问测试 不能访问

Openssl pkcs12 -export -in server.crt -inkey server.key -out client.p12 -name "client" 生成客户端能使用的证书
输入私钥密码

将生成clieny.p12证书复制到windows 双击 安装
访问测试 成功 有证书