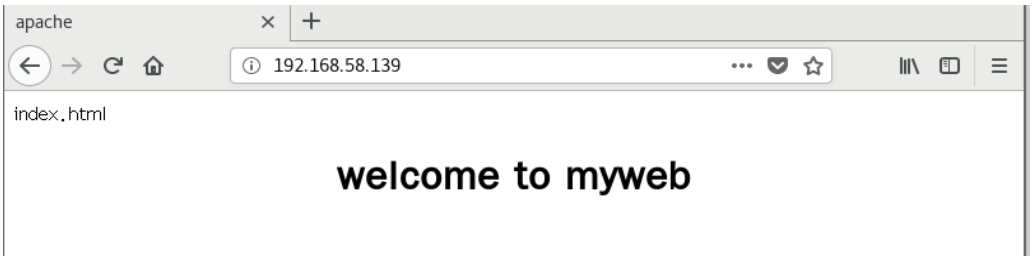
项目 2-搭建并配置 Apache 服务器指导书（2-5）

任务 9：假设某企业搭建了一个 Apache 服务器，IP 地址可设置为 DHCP 自动获取。现需要创建一个虚拟目录“/httest”，要求使用.htaccess 文件配置用户身份认证，让用户必须输入用户名（smile）和相应认证密码才能访问，即浏览器会弹出认证窗口，提示输入用户名和密码才能访问，如何完成配置呢？

准备工作：

可恢复到快照 1 状态。



实训配置步骤

1.创建一个虚拟目录“/httest”,物理路径为“/virdir/test”，让用户输入用户名和相应认证密码才能访问。

1.1 首先创建物理路径目录/virdir/test,并在此目录下创建一个内容为“Require valid_users’s web”的名字为 index.html 的文档。

```
[root@192 ~]# mkdir -p /virdir/test
[root@192 ~]# echo "Require valid_users's web">/virdir/test/index.html
```

1.2 在/virdir/test 目录下创建一个用户 smile 和相应认证密码，可以相同的方法继续添加其他用户，但之后添加用户不能使用-c 选项，否则会覆盖之前的用户。

知识点：在/usr/bin 目录下，有一个 htpasswd 可执行文件，它就是用来创建.htaccess 文件身份认证使用的密码，语法格式为：

htpasswd　[-bcD] [-mdps]　密码文件名字　用户名

说明：密码文件推荐使用.htpasswd,因为 apache 默认系统对“.ht”开头的文件默认不允许外部读取，安全系数会高一些。

参数：

- -b：用批处理方式创建用户。htpasswd 不会提示输入用户密码，不过由于要在命令行输入可见的密码，因此并不是很安全。
- -c：新创建（create）一个密码文件。
- -D：删除一个用户。
- -m：采用 MD5 编码加密。
- -d：采用 CRYPT 编码加密，这是预设的方式。
- -p：采用明文格式的密码。因为安全的原因，目前不推荐使用。
- -s：采用 SHA 编码加密。

```
[root@192 ~]# cd /virdir/test
[root@192 test]# /usr/bin/htpasswd -c /usr/local/.htpasswd smile
New password:
Re-type new password:
Adding password for user smile
```

2.**设置**/virdir/test 目录，允许采用.htaccess 进行用户身份认证，在/etc/httpd/conf/httpd.conf **主配置文件中加入以下内容**

说明：.htaccess 文件是一个访问控制文件，用来配置相应目录的访问方法。默认的配置是不会读取相应目录下的.htaccess 文件来进行访问控制的，这是用为 AllowOverride 中的配置为 none。

```
Alias /httest "/virdir/test"
<Directory "/virdir/test">
Options indexes Multiviews FollowSymLinks     #允许列目录
AllowOverride AuthConfig                      #启用用户身份认证
```

```
Order deny,allow                    #先检查禁止设定，没有禁止的全部允许
Allow from all                      #允许所有用户访问
Authname Test_Zone                  #定义的认证名称，与后面的.htaccess 文件中的一致
</Directory>
```

同时修改网站默认目录：

#DocumentRoot "/var/www/html"

DocumentRoot "/virdir/test/"

截图如下：

```
[root@192 test]# vim /etc/httpd/conf/httpd.conf
```

```
#DocumentRoot "/var/www/html"
DocumentRoot "/virdir/test"
#
# Relax access to content within /var/www.
#
<Directory "/var/www">
    AllowOverride None
    # Allow open access:
    Require all granted
</Directory>
Alias /httest "/virdir/test"
<Directory "/virdir/test">
Options indexes Multiviews FollowSymLinks
AllowOverride AuthConfig
Order deny,allow
Allow from all
Authname Test_Zone
</Directory>
```

注意：保存主配置文件后必须重启 httpd 服务，

执行语句：systemctl restart httpd

3.在/virdir/test 目录下新建一个.htaccess 文件：

```
[root@192 test]# touch .htaccess
[root@192 test]# vim .htaccess
```

编辑内容如下：

```
Authname "Test_Zone"                    #指令定义了要显示给用户的认证区域名称
AuthType Basic                          #认证的类型，一般为 Basic
AuthUserFile /usr/local/.htpasswd       #指令指向存储用户名和密码的.htpasswd 文件
require valid-user                      #指令意味着只有在用户名和密码匹配.htpasswd 文件中的条目时，才允许访问，
                                        也可以指定允许的个别用户。
```

```
root@192:/virdir/test
文件(F)  编辑(E)  查看(V)  搜索(S)  终端(T)  帮助(H)
Authname "Test_Zone"
AuthType Basic
AuthUserFile /usr/local/.htpasswd
require valid-user
```

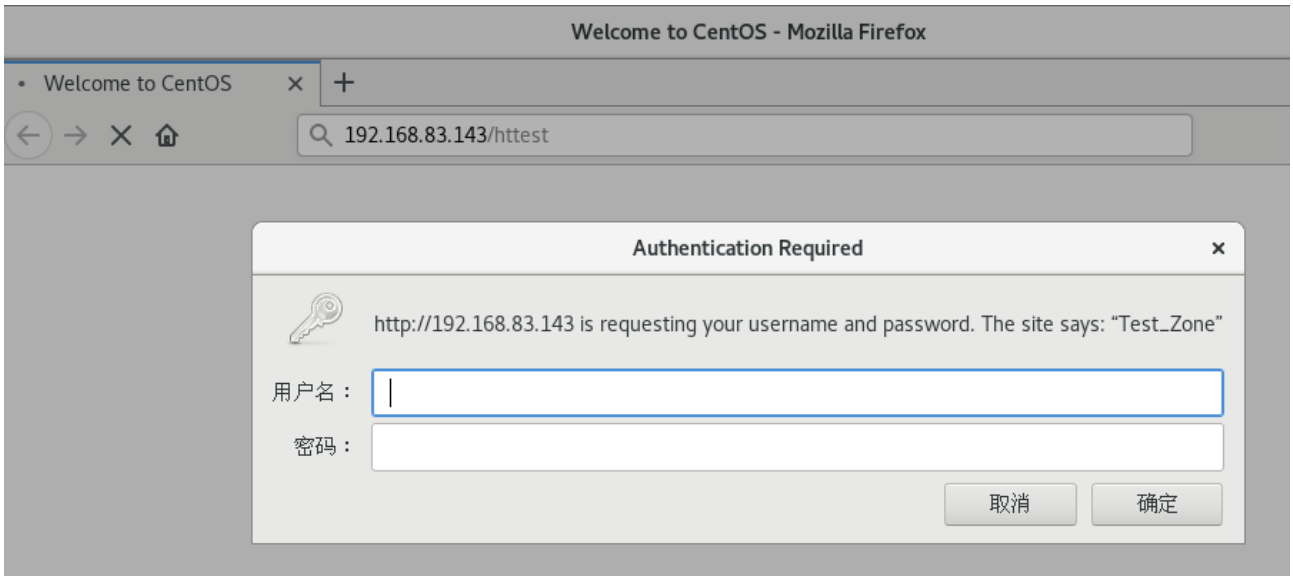
4. 设置 SELinux 允许

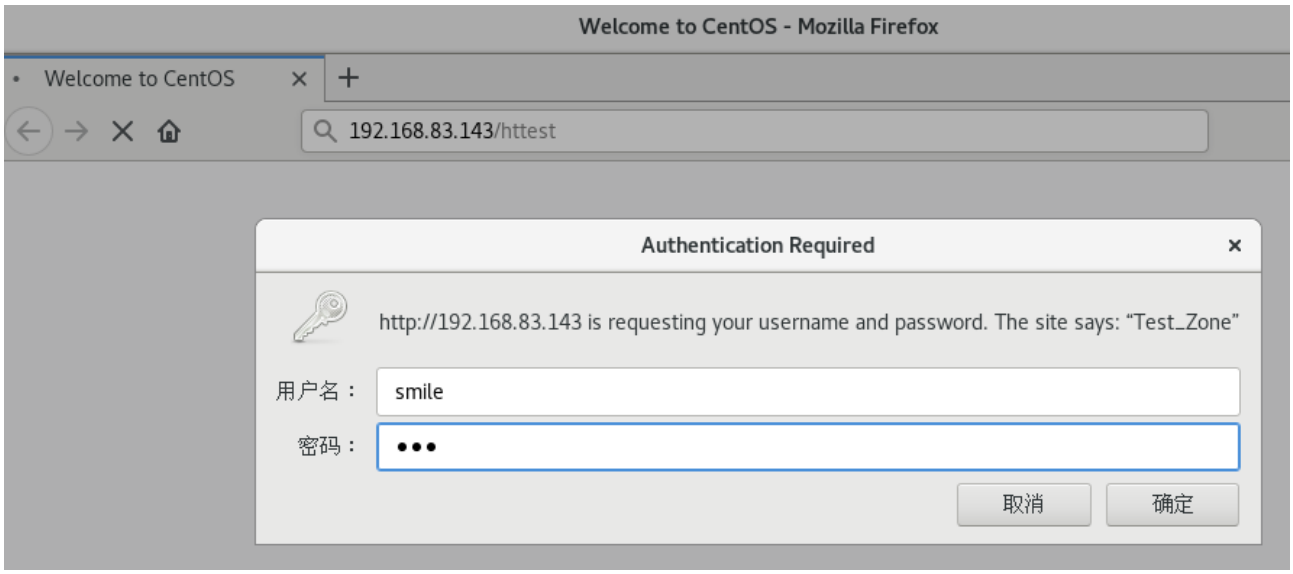
```
[root@192 test]# setenforce 0
```

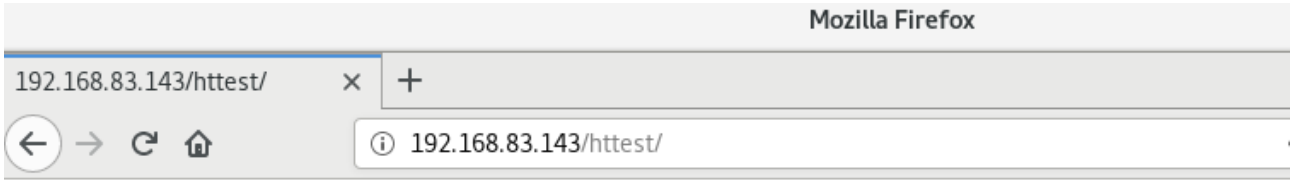
5. 测试验证

```
[root@192 test]# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.83.143  netmask 255.255.255.0  broadcast 192.168.83.255
        inet6 fe80::ad22:ea44:57a4:edd9  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:4c:84:72  txqueuelen 1000  (Ethernet)
        RX packets 582980  bytes 861701731 (821.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 113691  bytes 6974993 (6.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
```







Require valid_users's web

说明：为了服务器的性能，一般不推荐使用 AllowOverride AuthConfig 或者 AllowOverride ALL，因为这会使服务器会不断的去寻找.htaccess,从而影响服务器的效能，一般我们把一些后台管理界面或者其他特殊目录可能需要加验证这个需求。

学习网址：https://blog.csdn.net/liushu_it/article/details/18735449