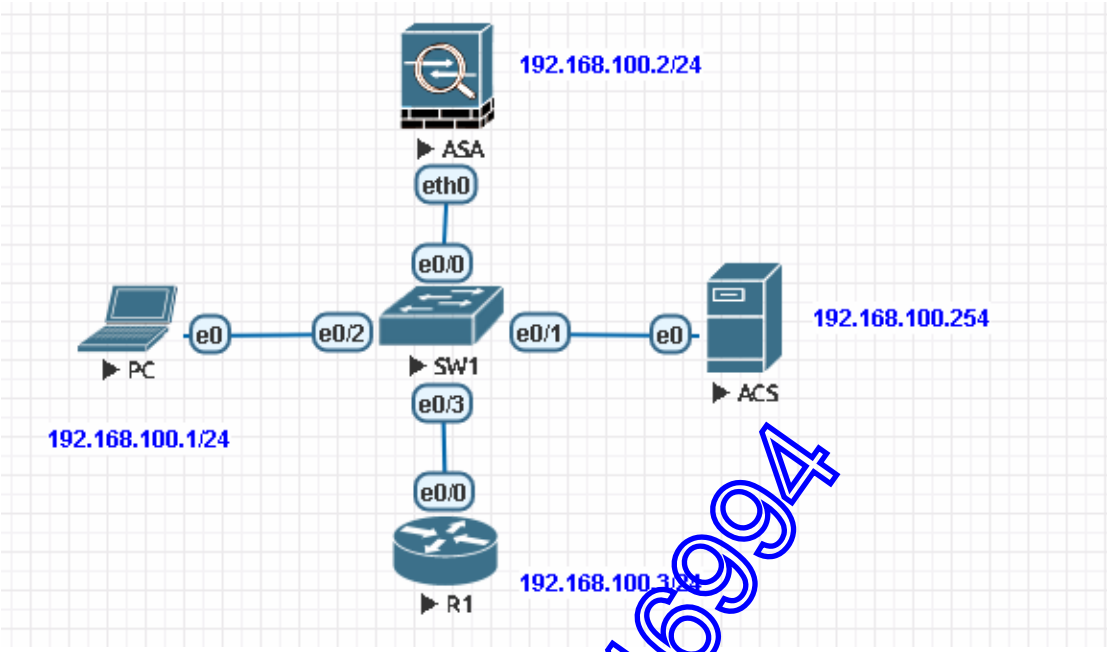
ASA 中的命令行和 Shell 授权

一、拓扑



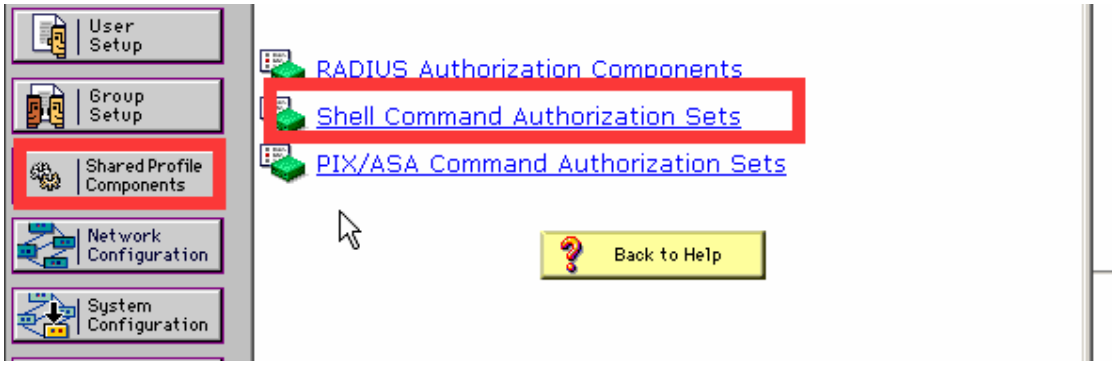
二、配置

1.ASA 中的配置

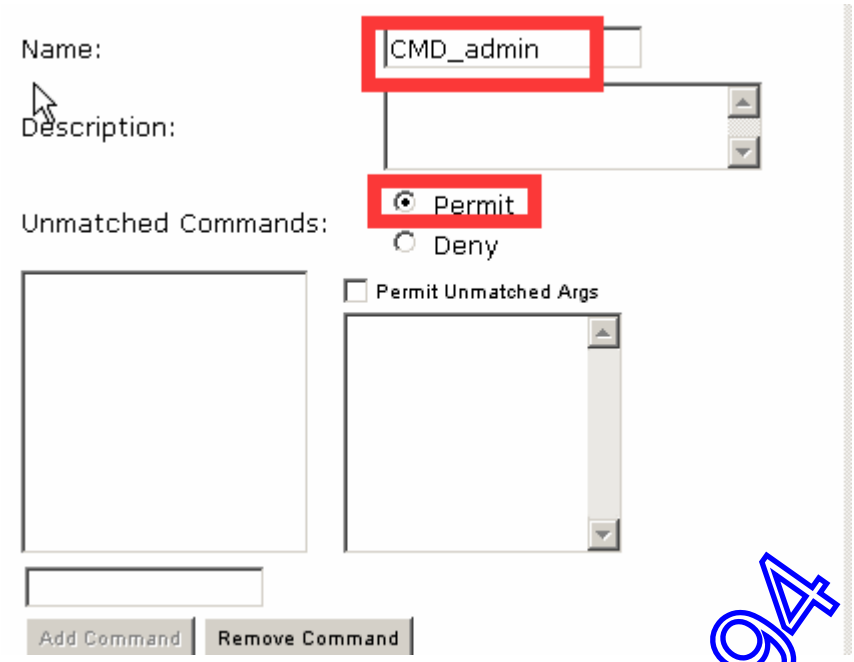
```
ASA# show run aaa
aaa authentication telnet console 3A LOCAL
aaa authentication enable console 3A LOCAL
aaa authentication serial console 3A LOCAL
aaa authorization command 3A LOCAL
aaa authorization exec authentication-server
ASA# show run telnet
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 5
ASA#
```

上面的 3 个认证：serail、enable、serial 必须配置

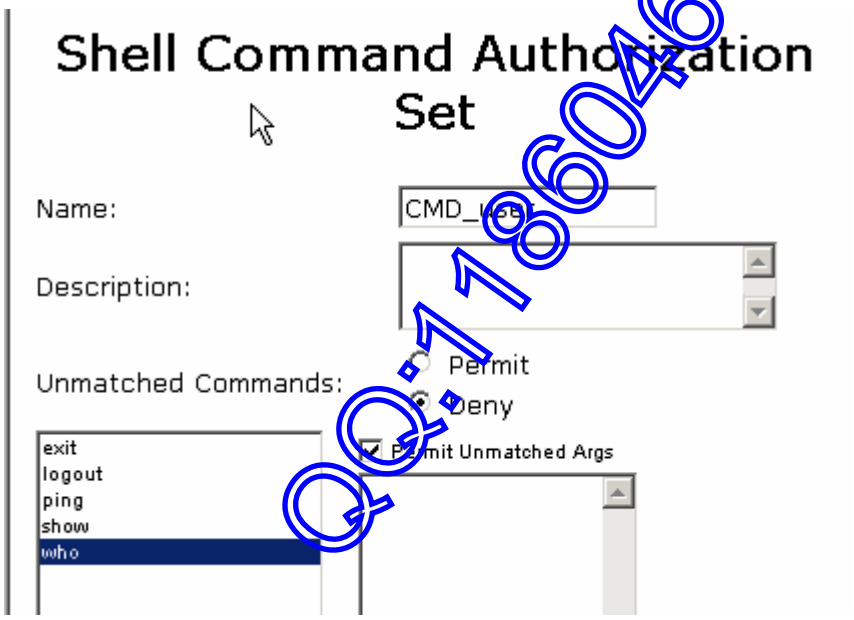
2.ACS4.2 中的 shell 配置



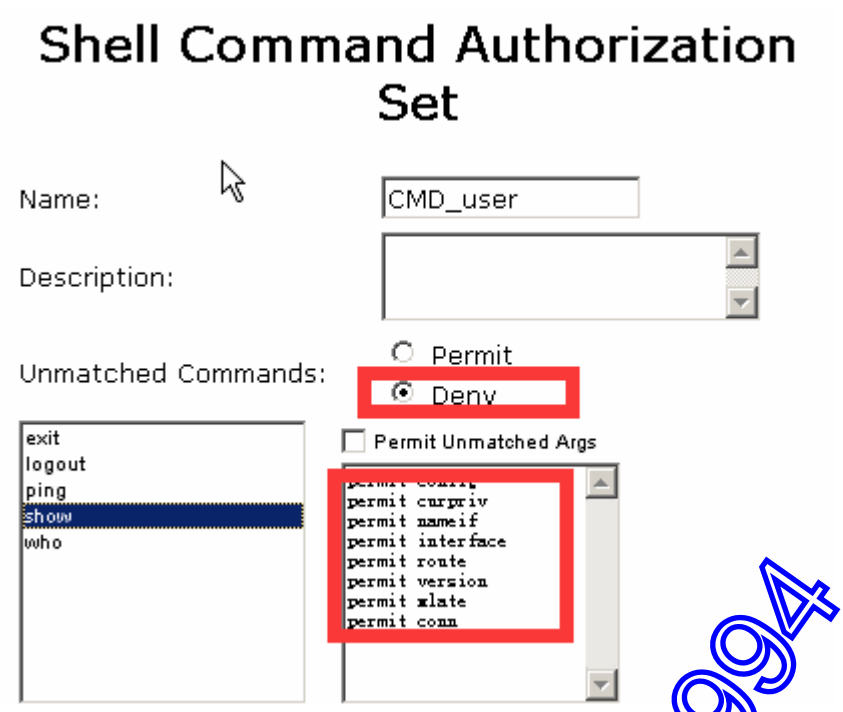
①管理员的命令行



②普通用户的命令行

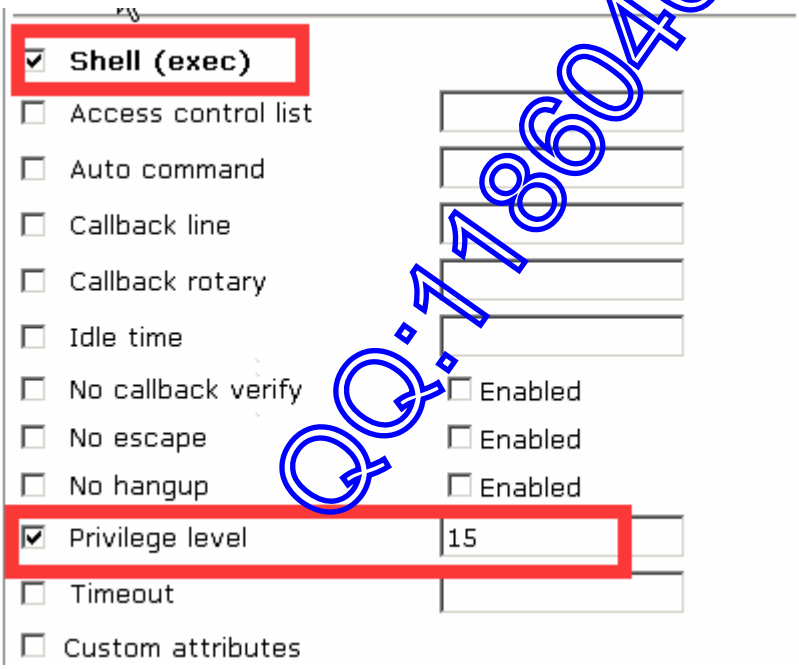


其中 show 命令为

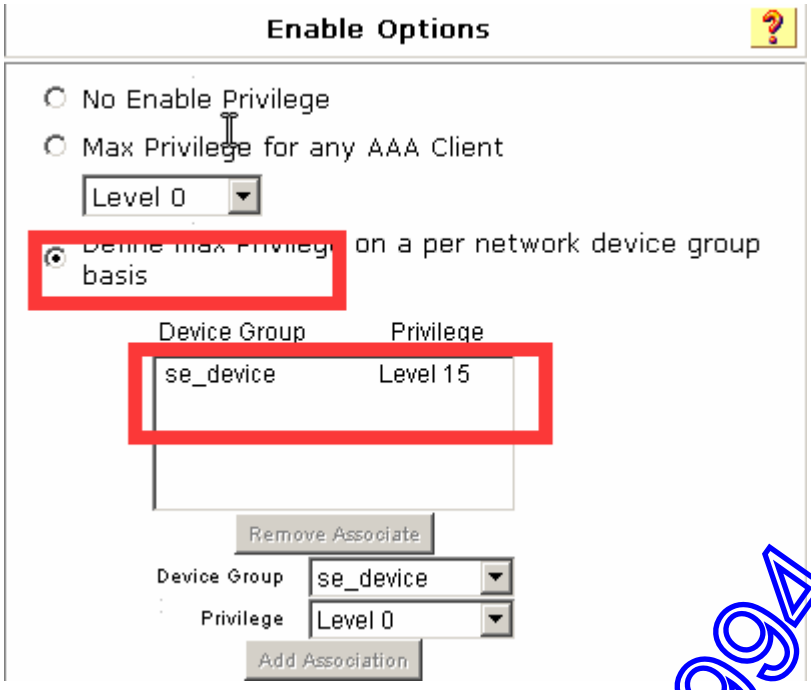


3.建立各个用户组

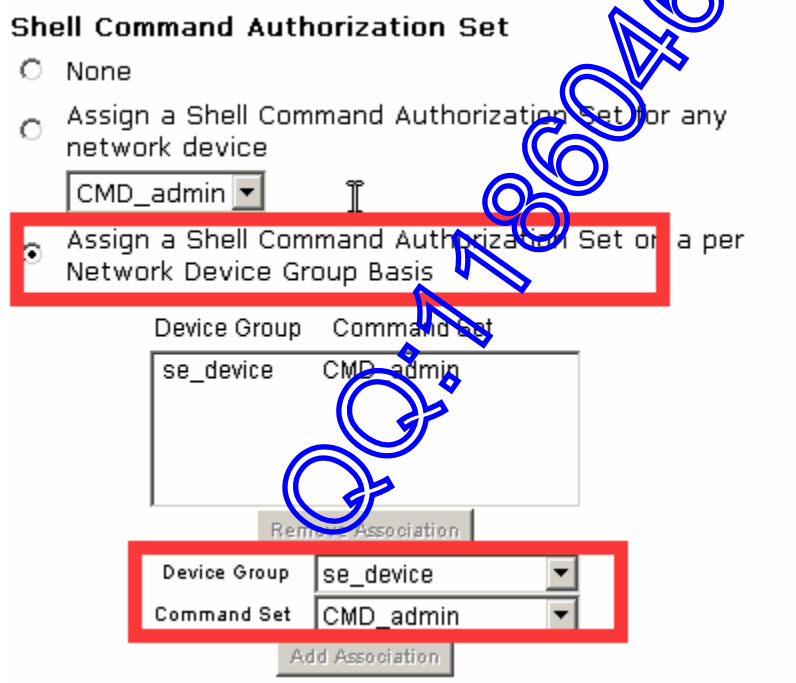
①管理员组



还必须给管理员组设置 enable 下的最大权限

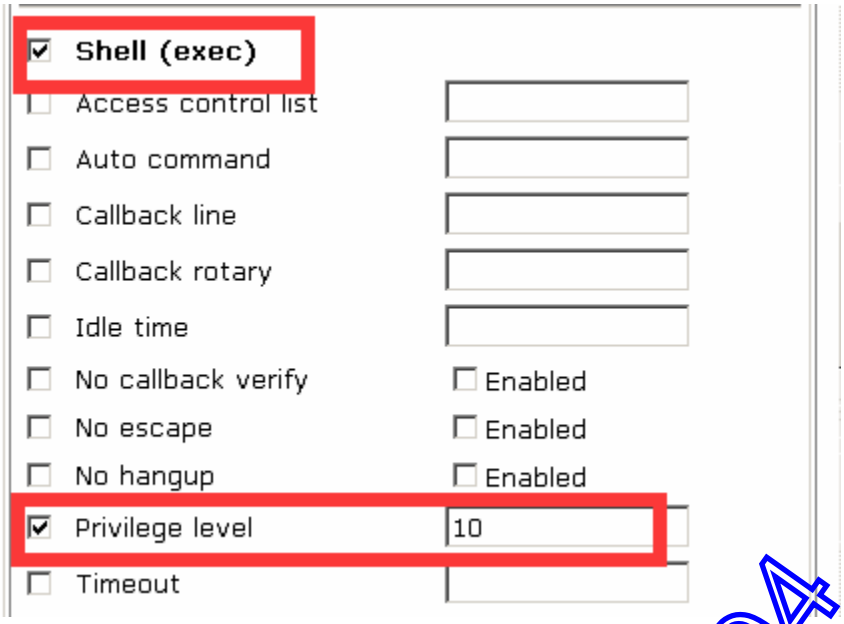


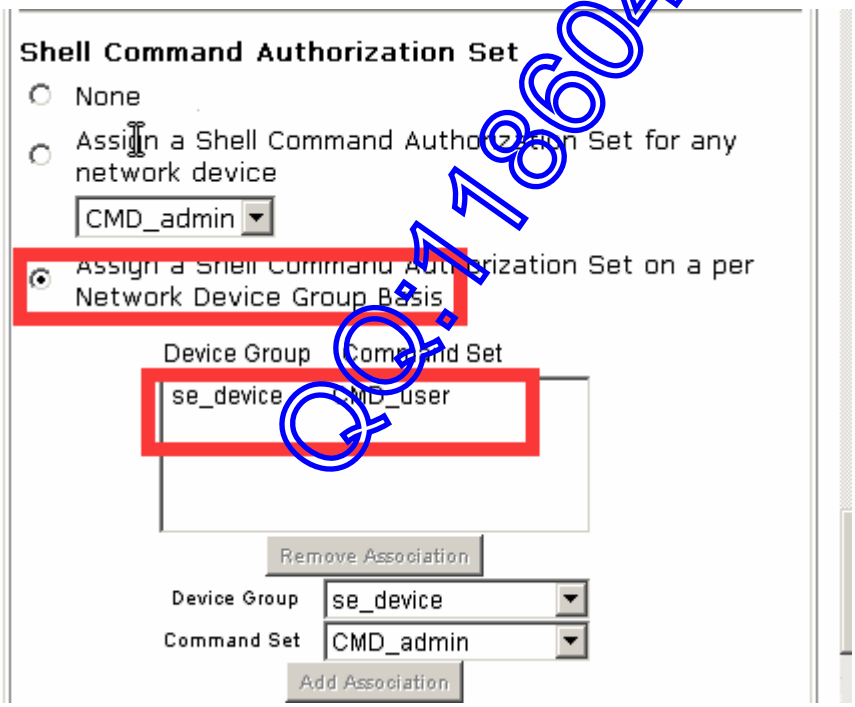
这里用到了 NDG 组，即在 enable 下，该组用户最大可使用 15 级的命令。



这个是前面的命令行关联。

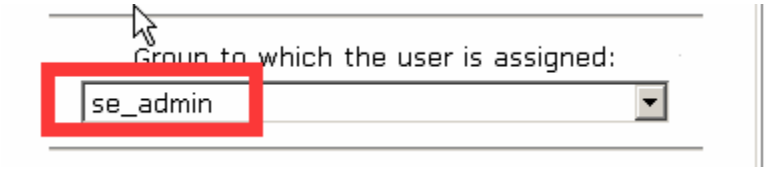
②普通用户组的设置

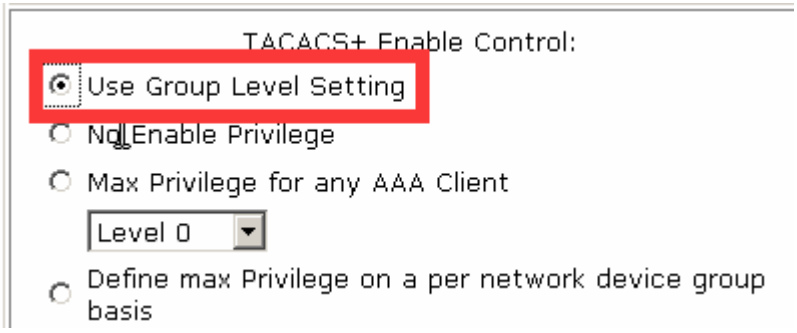


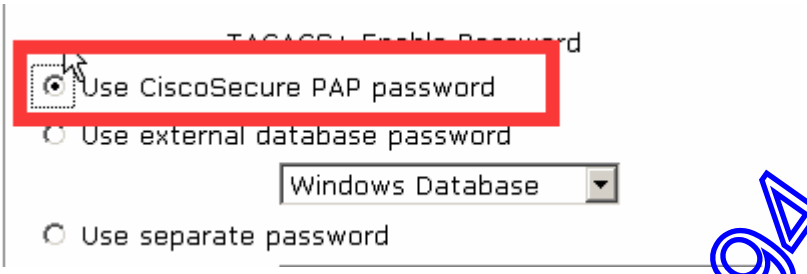


4.将用户加入到组中，并设置 enable 命令

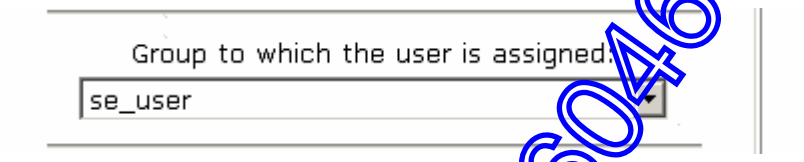
①管理员帐户

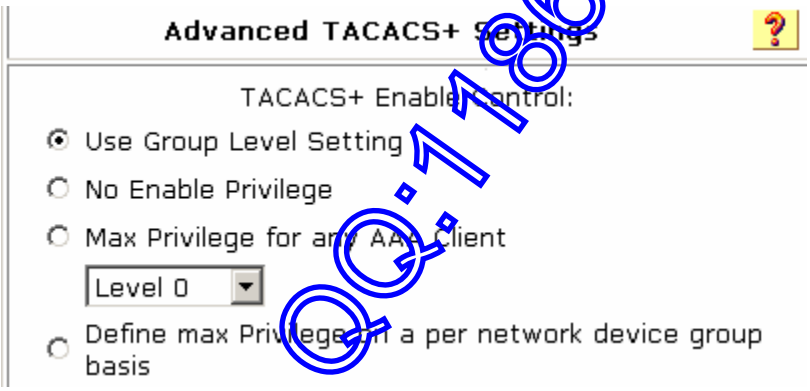


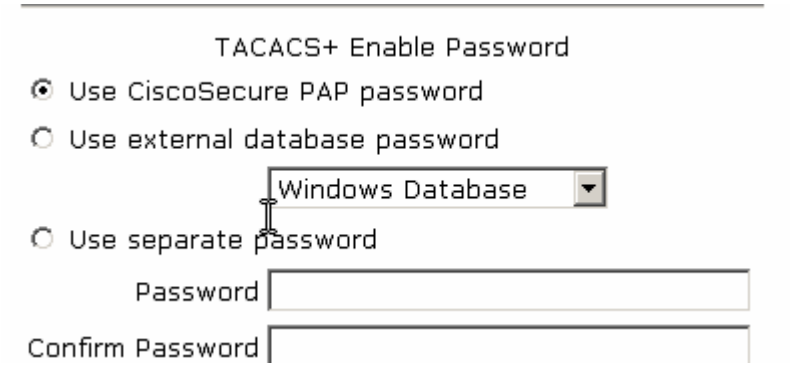




②普通用户







三、测试

1.普通用户

```
Username: user1
Password: *****
Type help or '?' for a list of available commands.
ASA> enable
Password: *****
ASA# show curpri
Username : user1
Current privilege level : 10
Current Mode/s : P_PRIV
ASA# _
```

```
ASA# ping 192.168.100.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ASA# config t
Command authorization failed
ASA# _
```

可看到其身份为 10 级，仅有可选的命令行可用。

2.管理员测试

```
User Access Verification

Username: admin
Password: *****
Type help or '?' for a list of available commands.
ASA> enable
Password: *****
ASA# show curpri
Username : admin
Current privilege level : 15
Current Mode/s : P_PRIV
ASA# _
```

显示其身份为 15 级用户。

```
ASA# confi t
ASA(config)# show run access-list
ASA(config)# show nameif
Interface              Name                    Security
Ethernet0              inside                  100
Ethernet1              outside                 0
ASA(config)#
```

一切命令都可以用。

此时关掉 ACS4.2，telnet 登录时，显示

```
User Access Verification

Username: admin
Password: *****
Type help or '?' for a list of available commands.
ASA>
ASA>
ASA>
ASA>
ASA> enable
Password:
Password: *****
ASA# confi t
ASA(config)# _
```

可看到 admin 用户登录时，验证正常。但如果输入命令时，延迟较大。
这是由于 ACS 服务器不存在时，必须做用户命令行的本地授权引发的。
※本地 15 级用户，可以在 ACS 断开时，使用所有的命令行。

```
ASA(config)# show curpriv
Username : admin
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
ASA(config)# _
```

即不会影响任何事情，但会造成 ACS 断开时，命令行操作太卡的现象。

此如果没有本地帐户 user1，则会有影响，即远程用户使用 user1 登录时，没法通过认证，所以要加上 user1 的本地帐户

ASA(config)#privilege cmd level 10 mode exec command exit
ASA(config)#privilege cmd level 10 mode exec command logout　//这两条必须加上，否则本地认证时通不出。
privilege show level 10 mode exec command configuration　//查看配置
privilege show level 10 mode exec command curpriv　　//查看权级
privilege show level 10 mode exec command interface　　//查看 IP
privilege show level 10 mode exec command nameif　　//查看 nameif
privilege show level 10 mode exec command route　　//查看路由

privilege show level 10 mode configure command interface
privilege show level 10 mode configure command nameif
privilege show level 10 mode configure command route

※在本地命令行授权中，没有搞成 ping 命令的授权。