ACG1000系列AD域单点登录典型配置举例

赵崇帅 2018-03-01 发表

HostA 、HostB 均为内网用户，属于192.168.1.0/24网段,通过NAT的方式访问Internet
GE2接口 ip： 192.168.1.1
内网存在AD域服务器、已加入AD域的PC，如图1示

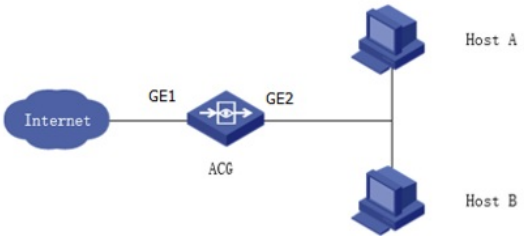


图1

1. 登录Web网关

按照组网图组网，如图2

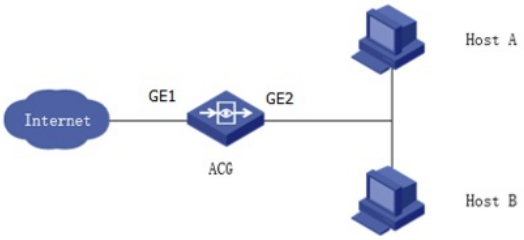


图2

2. 配置认证策略

在导航栏中选择"用户管理 > 认证策略 "，进入认证策略的显示页面，如图3所示

图 3

配置源接口为GE2，认证方式为单点登录，登录失败的用户选择动作为不需要认证，自动上线
配置时间对象为always。如图4所示

图 4认证策略界面

3 单点登录配置

在导航栏中选择"用户管理 >认证设置>单点登录

启用单点登录

配置会话密钥，如:123456，如图5

图 5单点登录配置界面

4. 单点登录脚本

下载域单点登录程序，并解压，如图6所示

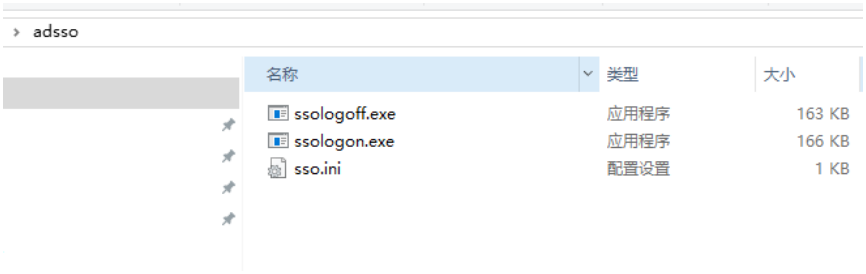


图 6单点登录配置脚本

5. 配置sso.ini

修改Gwip 为GE2 接口IP， 修改seessionKey 为之前配置的密码

```
[SSOCtrl]
EnableHeartBeat = 1
EnableCopyStartup = 1
HeartBeatInterval = 30
LogPath = C:\

[GW1]
GWIP = 192.168.1.1
Port = 6622
SessionKey = 123456
```

如图7所示

图 7脚本配置界面

6. 登录AD域控

进入组策略：AD域服务器“运行”输入gpmc.msc

选择Default Domian Policy

选择“用户配置”——“脚本（登录/注销）”-登录，如图8

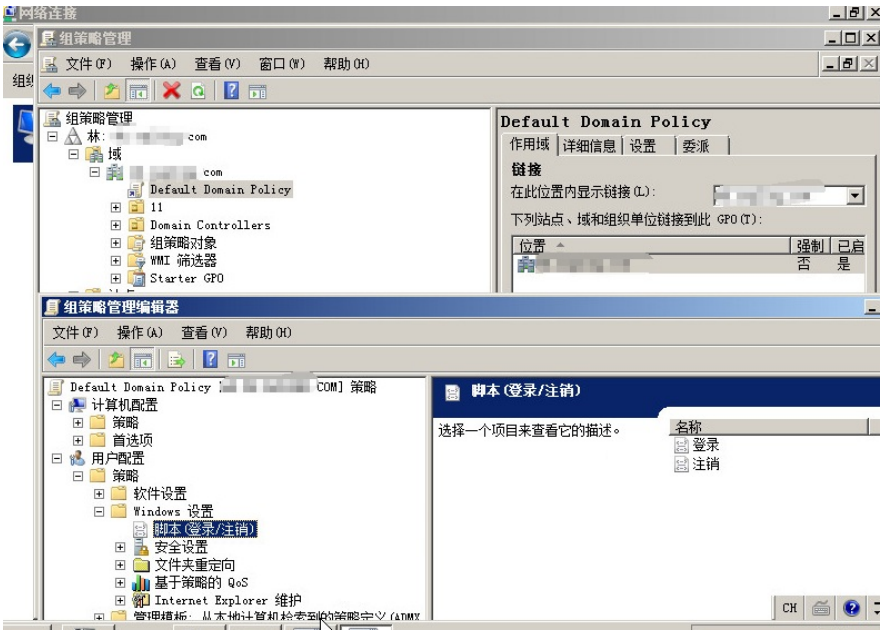


图 8组策略配置界面

7. 导入登录脚本

如图9所示

图 9组策略配置界面

将配置文件及脚本导入到启动目录，如图10

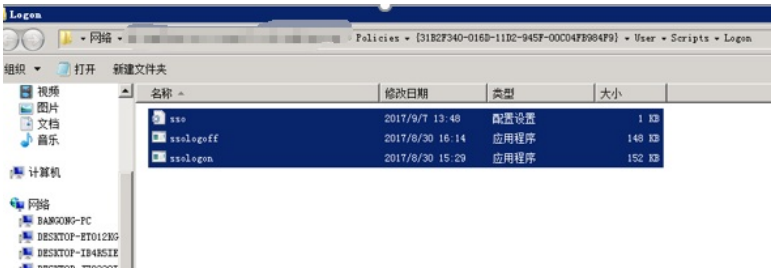


图 10组策略脚本配置界面

8. 导入注销脚本

如图11所示

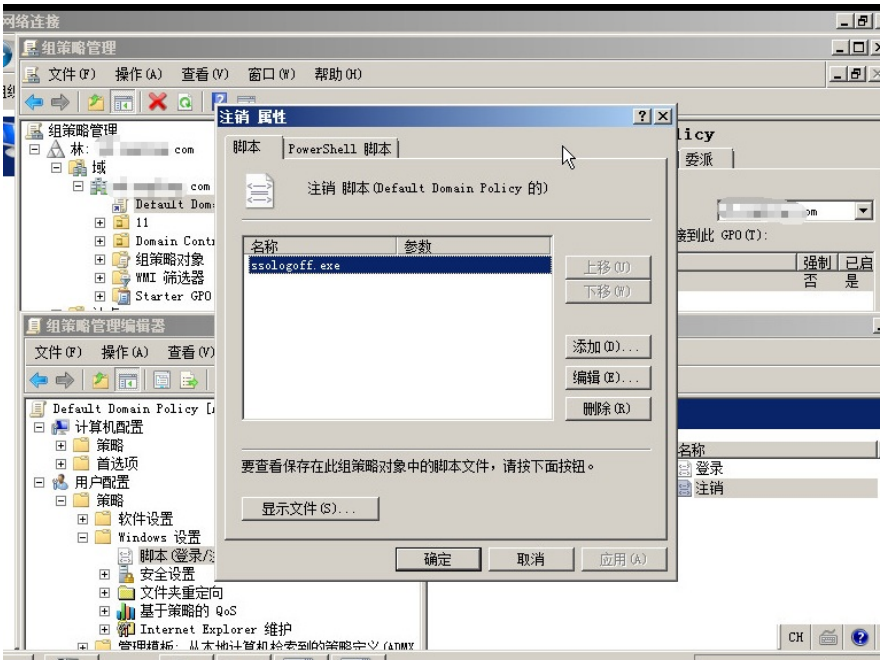
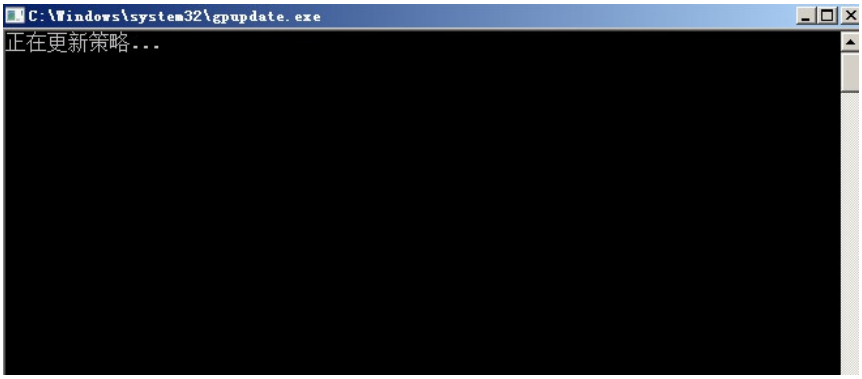


图 11组策略脚本配置界面

9. 组策略更新

通过组策略下发给域用户,域控中， 运行-gpupdate.exe



如图12所示

图 12组策略更新界面

10 验证效果

如图13所示

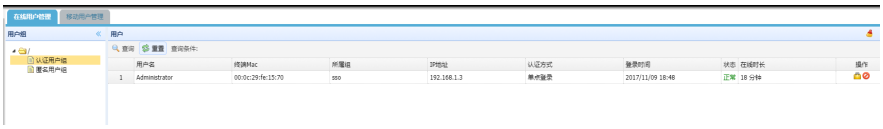


图 13在线用户状态界面

11 配置文件

!user-group

!

!

!

!user-policy

!

user-policy ge2 any any any always sso-no-authen-ip 1

!zone

!

!user-sso

!

user-adsso session-key kTgxl5p34DqlzzT+XZ0R14cv6Qal7urj9YogDjQGHYyVxSLYlpmOxTPwro4b0aN

需将启动脚本放置安全类软件白名单。

不同用户登录同一台域内测试pc，在线用户只显示一个账号，在线用户只识别第一次登录的账号，避免频繁出现账号切换，目前设备是基于IP来识别用户的，无法实现两个IP一样账号不一样的用户同时在线。

单点登录用户不支持HA主备：

HA主备单点登录配置支持HA同步，但在线用户不支持HA同步，如果发生HA切换，存在以下两种情形：

1、单点登录失败的用户，不需要认证,自动上线

新的主设备收到用户心跳报文后（默认30s发一次心跳报文），用户会重新上线，但是如果上网流量产生在心跳报文之前，则以IP做为用户名直接上线

2、单点登录失败的用户，继续匹配后续策略

新的主设备收到用户心跳报文后（默认30s发一次心跳报文），用户会重新上线，但是如果上网流量产生在心跳报文之前，则会继续匹配设备上的后续认证策略，如果没有后续认证策略，则会丢弃在收到下个心跳报文之前的30s内的所有报文，后续收到心跳报文后则会重新上线。