

组网及说明

本案例使用S5820交换机部署hwtacacs，与IMC TAM联动，达到设备安全管理的效果。

IMC版本为PLAT 7.3 E0506P03

S5820的版本信息如下：

H3C Comware Software, Version 7.1.045, Release 2418P06

Copyright (c) 2004-2015 Hangzhou H3C Tech. Co., Ltd. All rights reserved.

H3C S5820V2-48S uptime is 233 weeks, 5 days, 23 hours, 47 minutes

Last reboot reason : USER reboot

Boot image: flash:/s5820v2_5830v2-cmw710-boot-r2418p06.bin

Boot image version: 7.1.045, Release 2418P06

Compiled Aug 07 2015 15:40:53

System image: flash:/s5820v2_5830v2-cmw710-system-r2418p06.bin

System image version: 7.1.045, Release 2418P06

Compiled Aug 07 2015 15:40:53

特别说明：

- 1、要部署hwtacacs的设备已经在IMC进行了纳管。
- 2、要部署hwtacacs的设备已经和IMC网络互通。
- 3、要部署hwtacacs的设备需要提前开启远程管理的功能，并创建用户及赋予权限，待设备和服务器都部署完tacacs后，需要使用服务器上的tacacs账号对设备进行远程登陆管理，当tacacs服务器挂掉了，才可以使用设备的本地用户远程登陆管理。

配置步骤

1、授权场景条件：

设备区域管理、设备类型管理、授权时段策略管理

2、授权命令配置：

Shell profile配置、命令集配置

3、设备管理：

配置共享密钥、绑定设备区域、绑定设备类型

4、添加用户名、密码

5、S5820部署hwtacacs

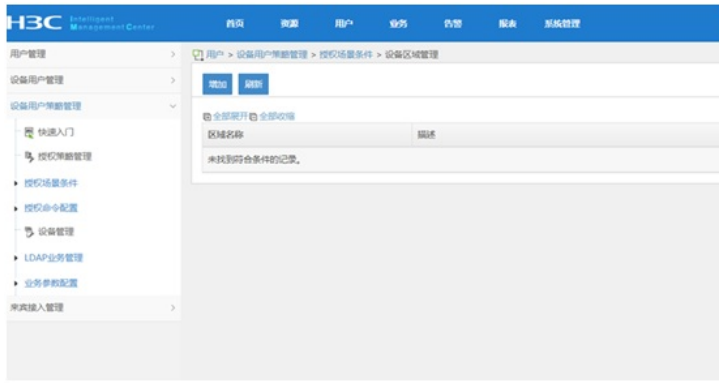
配置关键点

IMC侧配置如下：

配置“授权场景条件”



添加“设备区域管理”



设置“区域名称”



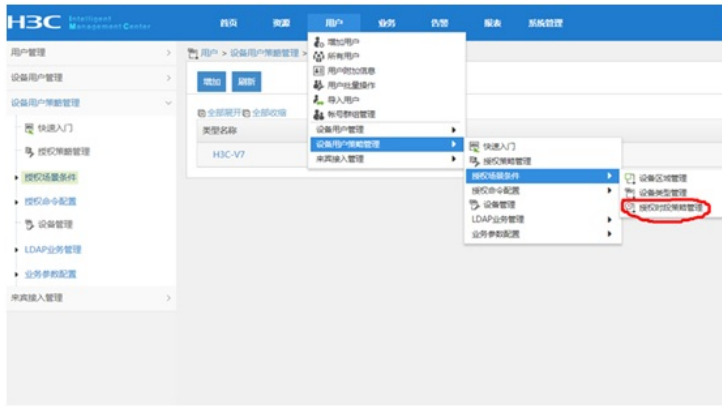
设置“设备类型管理”



增加



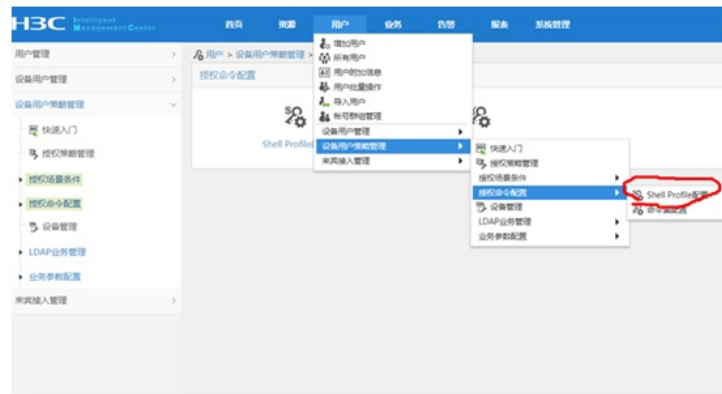
设置“授权时段策略管理”



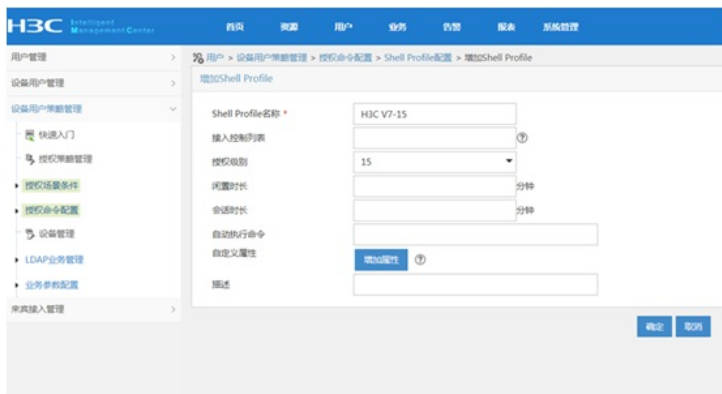
增加，设置“授权时段策略名称”、“生效时间”、“失效时间”



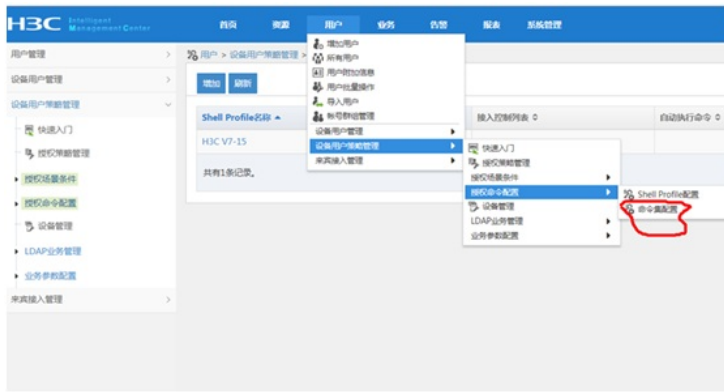
设置“授权命令配置”-“shell profile配置”



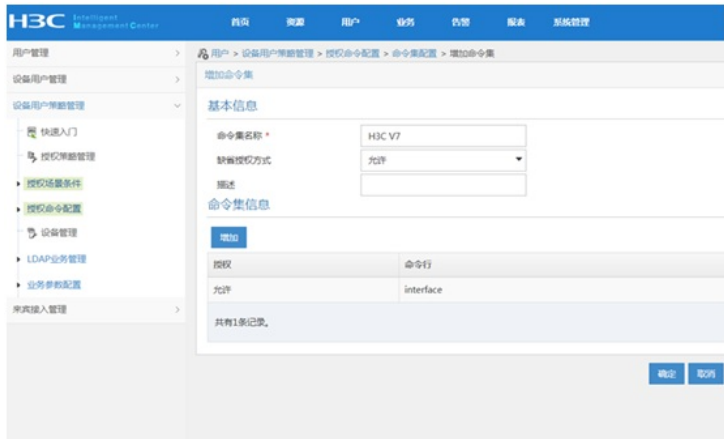
设置“shell profile名称”-“授权级别”



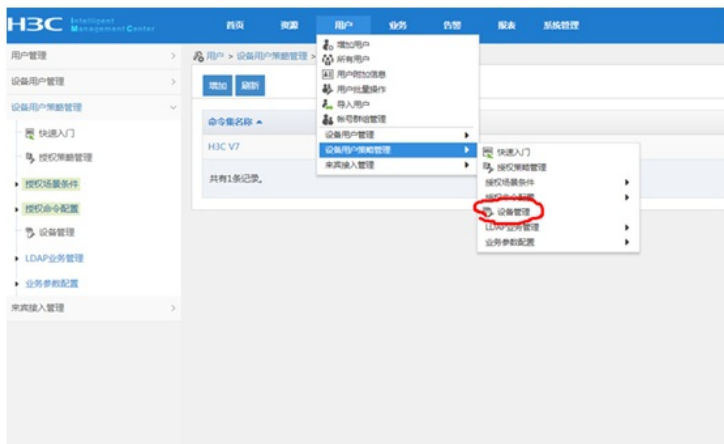
设置“命令集配置”



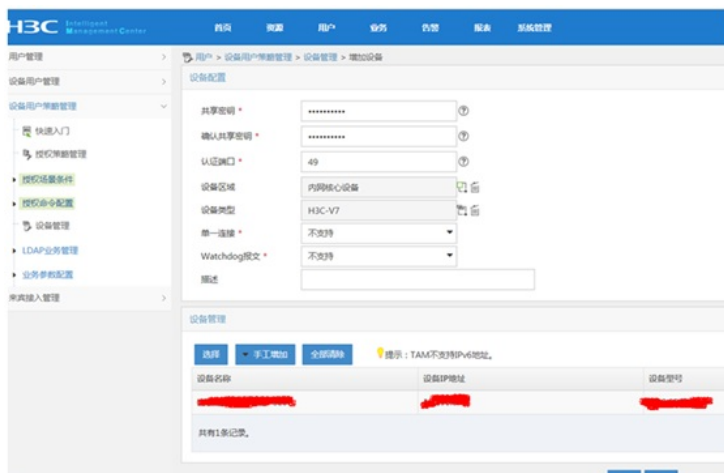
设置“命令集名称”、“缺省授权方式”

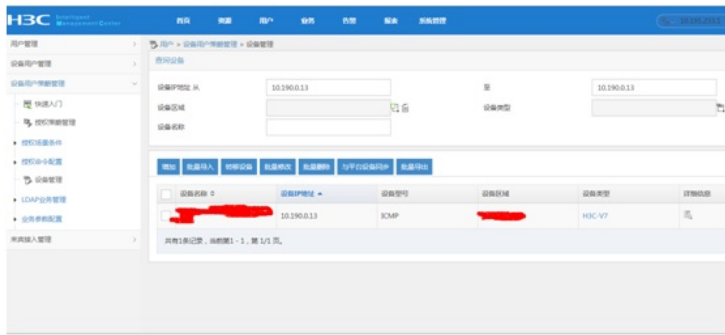


配置“设备管理”

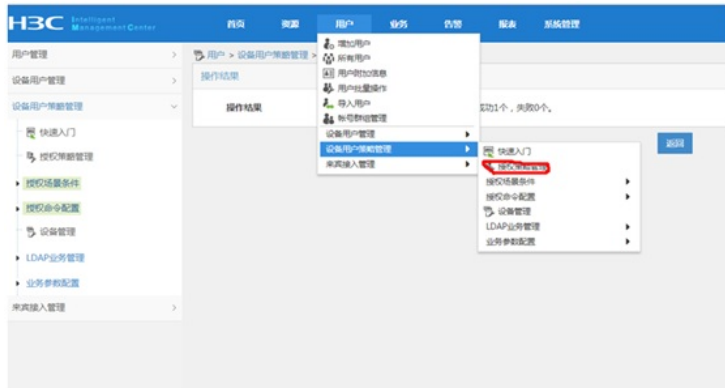


增加设备，设置“共享密钥”、“确认共享密钥”，绑定“设备区域”、“设备类型”

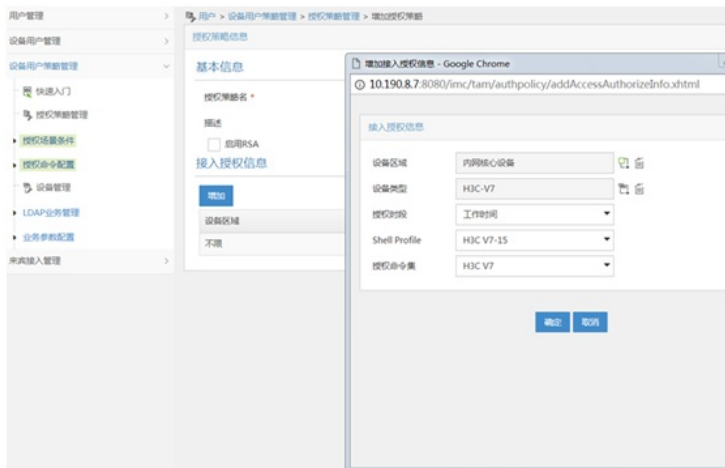




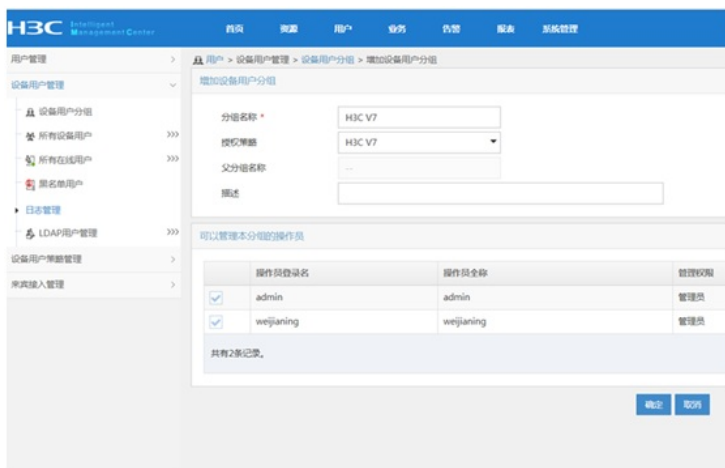
配置“授权管理”



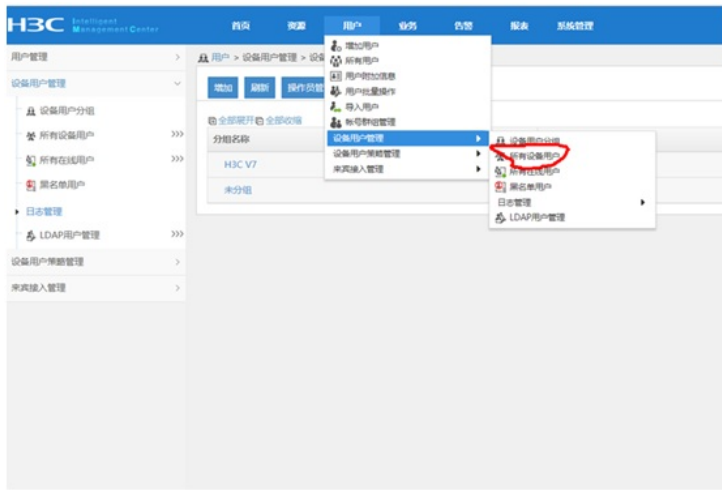
绑定“设备区域”-“设备类型”-“授权时段”-“shell profile”-“授权命令集”



配置“用户设备分组”，设置“分组名称”-“授权策略”



设置“设备用户管理”-“所有设备用户”



设置“账号名”-“登录密码”-“登录密码确认”-“设备用户分组”-“用户的授权策略”



S5820部署hwtacacs如下:

1、部署hwtacacs:

```
hwtacacs scheme shebeiguanli
primary authentication 10.190.8.7
primary authorization 10.190.8.7
primary accounting 10.190.8.7
key authentication cipher $c$3$jY/E2qCCddkGGV9+5Qu+VbPiTRm4uAEfG1K80YA=
key authorization cipher $c$3$23sT1lI6Zyu0bZzkIVMgEAh8FmTWXqcW5RQgmyM=
key accounting cipher $c$3$uKU3+jUjwC/ZwgaLBBajlNXMmBFG4ZqzPWb/oo=
user-name-format without-domain
nas-ip 10.190.0.13
```

2、部署domain:

```
domain tamdm
authentication login hwtacacs-scheme shebeiguanli local
authorization login hwtacacs-scheme shebeiguanli local
accounting login hwtacacs-scheme shebeiguanli local
authorization command hwtacacs-scheme shebeiguanli local
accounting command hwtacacs-scheme shebeiguanli
```

3、启用默认domain:

```
domain default enable tamdm
```

4、查看hwtacacs显示信息:

```
dis hwtacacs scheme
Total 1 TACACS schemes
```

```
-----
HWTACACS Scheme Name : shebeiguanli
Index : 0
Primary Auth Server:
Host name: Not Configured
IP : 10.190.8.7 Port: 49 State: Active
```

VPN Instance: Not configured
Single-connection: Disabled
Primary Author Server:
Host name: Not Configured
IP : 10.190.8.7 Port: 49 State: Active
VPN Instance: Not configured
Single-connection: Disabled
Primary Acct Server:
Host name: Not Configured
IP : 10.190.8.7 Port: 49 State: Active
VPN Instance: Not configured
Single-connection: Disabled

VPN Instance : Not configured
NAS IP Address : 10.190.0.13
Server Quiet Period(minutes) : 5
Realtime Accounting Interval(minutes) : 12
Response Timeout Interval(seconds) : 5
Username Format : without-domain

4、查看domain显示信息:

dis domain tamdm

Domain:tamdm
State: Active
login Authentication Scheme: tacacs: shebeiguanli, local
login Authorization Scheme: tacacs: shebeiguanli, local
login Accounting Scheme: tacacs: shebeiguanli, local
command Authorization Scheme: tacacs: shebeiguanli, local
command Accounting Scheme: tacacs: shebeiguanli
default Authentication Scheme: local
default Authorization Scheme: local
default Accounting Scheme: local
Authorization attributes :
Idle-cut : Disable

至此，S5820 hwtacacs典型组网配置案例已完成!
