S6520X hwtacacs典型组网配置案例（IMC部署TAM作为tacacs服务器）

Tacacs 韦家宁 2020-04-09 发表

组网及说明

本案例使用S6520X交换机部署hwtacacs，与IMC TAM进行联动，达到设备安全管理的效果。
IMC版本为PLAT 7.3 E0506P03
S6520版本信息如下：
H3C Comware Software, Version 7.1.070, Release 1110P02
Copyright (c) 2004-2018 New H3C Technologies Co., Ltd. All rights reserved.
H3C S6520X-54QC-EI uptime is 24 weeks, 1 day, 21 hours, 29 minutes
Last reboot reason : Cold reboot

Boot image: flash:/s6520x-cmw710-boot-r1110p02.bin
Boot image version: 7.1.070, Release 1110P02
Compiled Aug 14 2018 11:00:00
System image: flash:/s6520x-cmw710-system-r1110p02.bin
System image version: 7.1.070, Release 1110P02
Compiled Aug 14 2018 11:00:00

Slot 1:
Uptime is 24 weeks,1 day,21 hours,29 minutes
S6520X-54QC-EI with 2 Processors
BOARD TYPE: S6520X-54QC-EI
DRAM: 2048M bytes
FLASH: 1024M bytes
PCB 1 Version: VER.A
Bootrom Version: 105
CPLD 1 Version: 001
CPLD 2 Version: 003
Release Version: H3C S6520X-54QC-EI-1110P02
Patch Version : None
Reboot Cause : ColdReboot
[SubSlot 0] 48SFP Plus + 2QSFP Plus
[SubSlot 1] 1/2.5/5G BASE-T
[SubSlot 2] 1/2.5/5G BASE-T

Slot 2:
Uptime is 24 weeks,1 day,20 hours,16 minutes
S6520X-54QC-EI with 2 Processors
BOARD TYPE: S6520X-54QC-EI
DRAM: 2048M bytes
FLASH: 1024M bytes
PCB 1 Version: VER.A
Bootrom Version: 105
CPLD 1 Version: 001
CPLD 2 Version: 003
Release Version: H3C S6520X-54QC-EI-1110P02
Patch Version : None
Reboot Cause : IRFMergeReboot
[SubSlot 0] 48SFP Plus + 2QSFP Plus
[SubSlot 1] 1/2.5/5G BASE-T
[SubSlot 2] 1/2.5/5G BASE-T

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

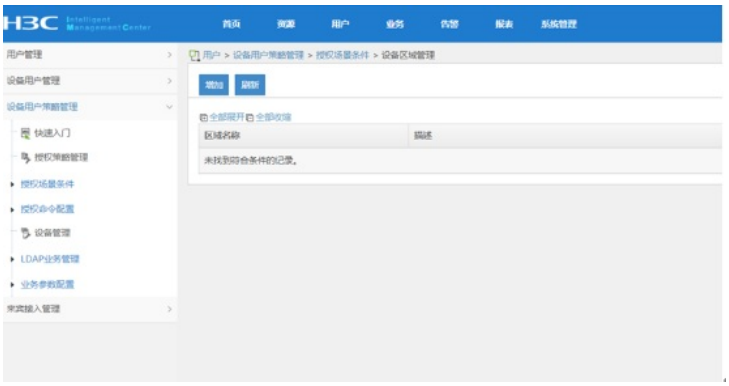
5、S6520X交换机部署hwtacacs

配置关键点

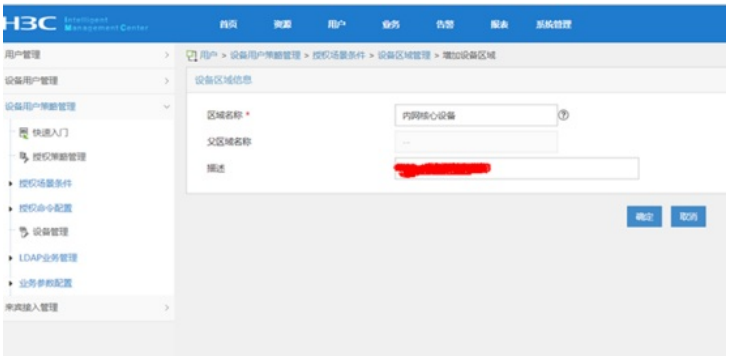
IMC侧配置：

配置“授权场景条件”

添加“设备区域管理”



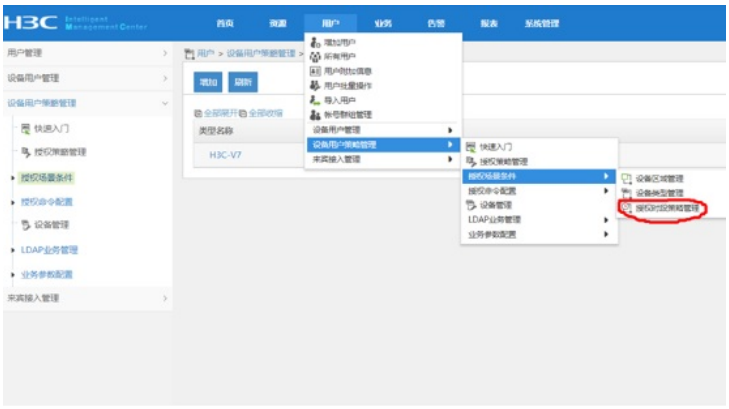
设置“区域名称”



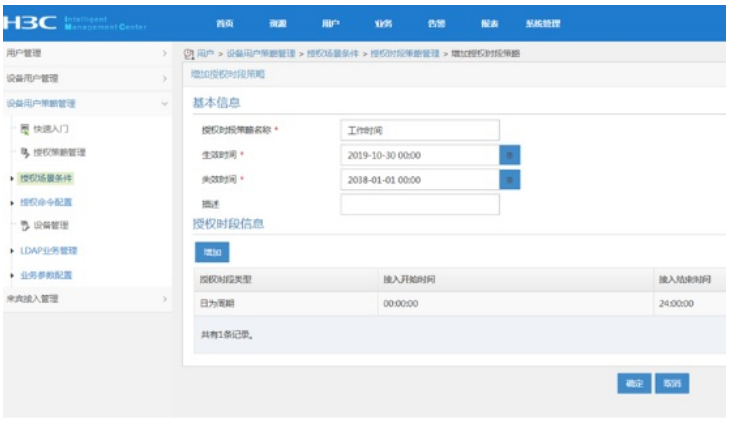
设置“设备类型管理”

增加

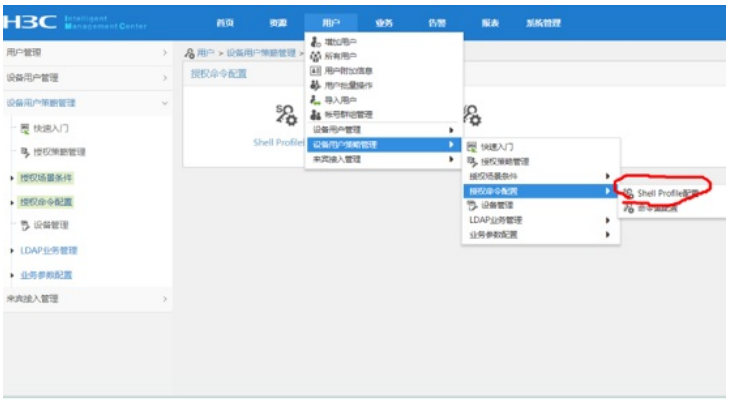
设置“授权时段策略管理”



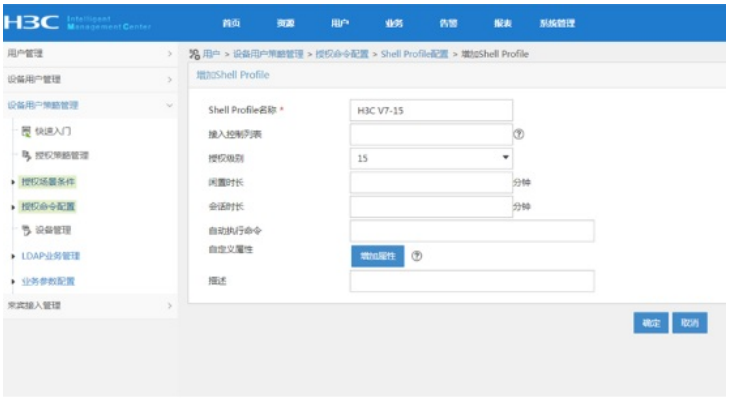
增加，设置“授权时段策略名称”、“生效时间”、“失效时间”



设置“授权命令配置”-“shell profile配置”

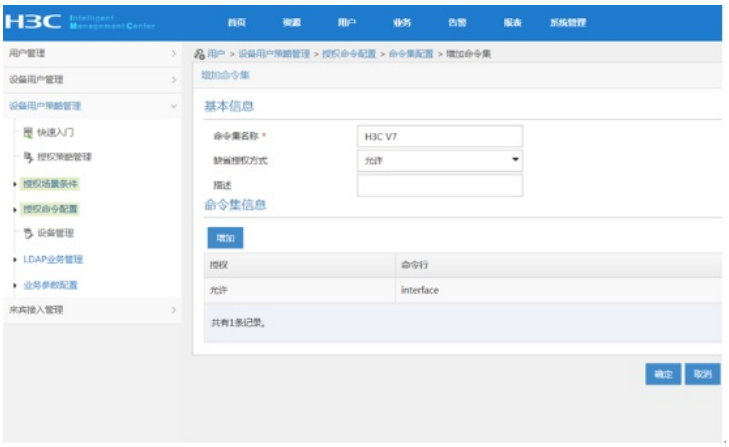


设置“shell profile名称”-“授权级别”

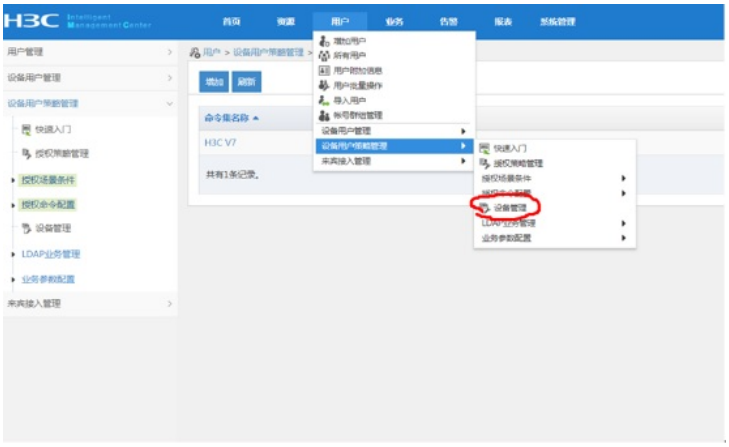


设置“命令集配置”

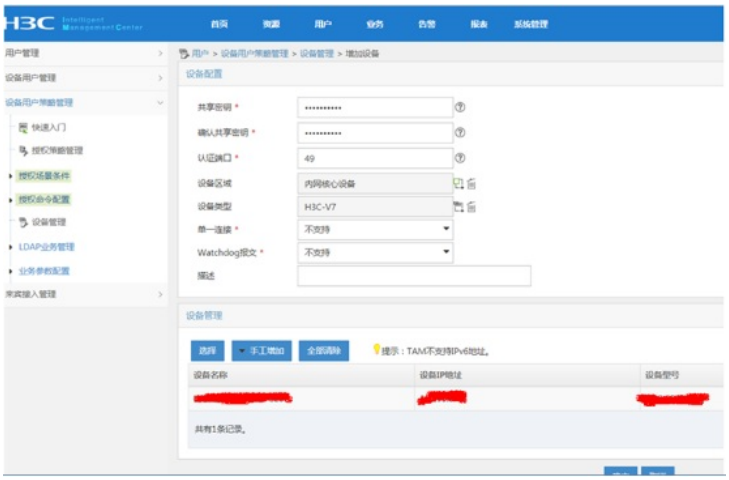
设置“命令集名称”、“缺省授权方式”

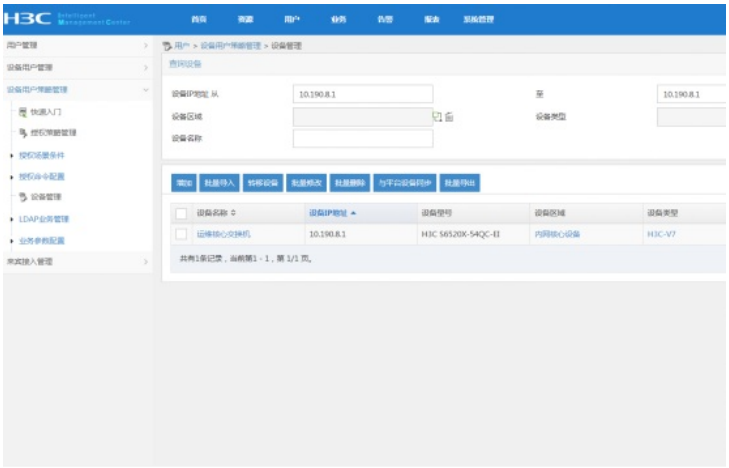


配置“设备管理”

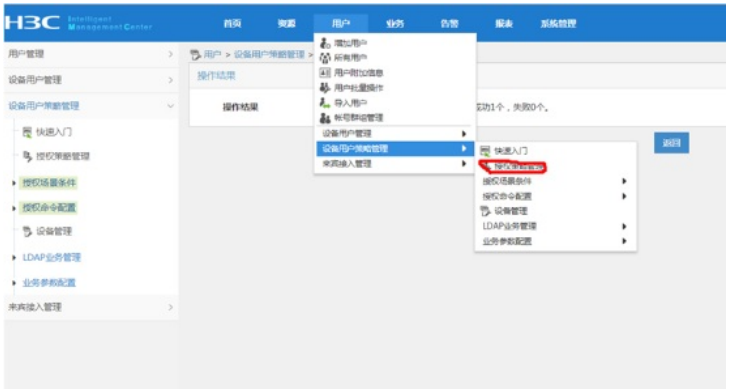


增加设备，设置“共享密钥”、“确认共享密钥”，绑定“设备区域”、“设备类型”

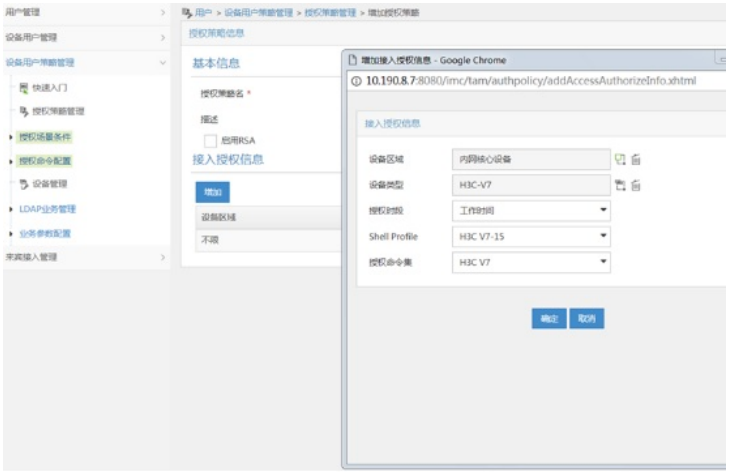




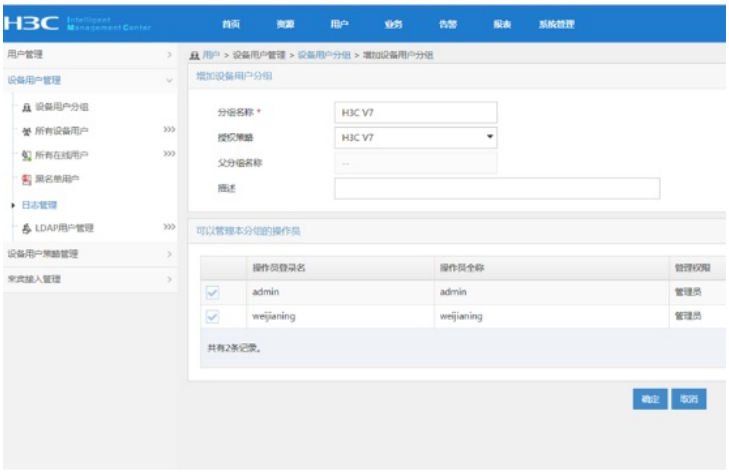
配置“授权管理”



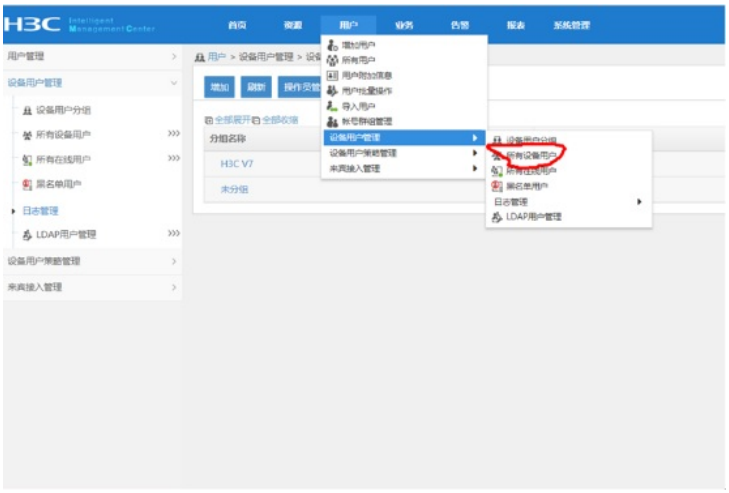
绑定“设备区域”-“设备类型”-“授权时段”-“shell profile”-“授权命令集”



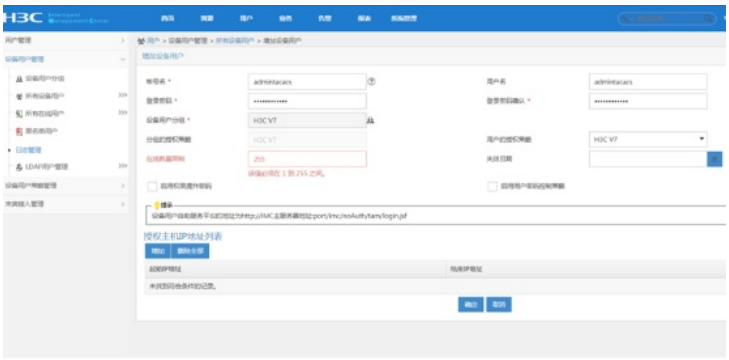
配置“用户设备分组”，设置“分组名称”-“授权策略”



设置“设备用户管理”-“所有设备用户”



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



S6520X配置如下：

1、配置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$3$RnNrR/s0ZVKz4QE76pZmc2S67dHHggjvyk46lDY=
 key authorization cipher $c$3$9Wgwwj3dGAJ6us9kQFGzpJIE3qyG17jMLMEWeqA=
 key accounting cipher $c$3$vLZwwBR6J57wvFlPg2OH8nZoGvhSf4rXYeLIFtA=
 user-name-format without-domain
 nas-ip 10.190.8.1
```

2、配置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Hwtacas显示信息
dis hwtacacs scheme
Total 1 HWTACACS 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                     : 10.190.8.1
  Server Quiet Period(minutes)       : 5
  Realtime Accounting Interval(minutes) : 12
  Stop-accounting packets buffering     : Enabled
    Retransmission times             : 100
  Response Timeout Interval(seconds)    : 5
  Username Format                    : without-domain
  Data flow unit                     : Byte
  Packet unit                        : one
```

5、查看domain显示信息
dis domain tamdm

```
Domain: tamdm
  State: Active
  Login   authentication scheme:  HWTACACS=shebeiguanli, Local
  Login   authorization  scheme:  HWTACACS=shebeiguanli, Local
  Login   accounting     scheme:  HWTACACS=shebeiguanli, Local
  Command authorization  scheme:  HWTACACS=shebeiguanli, Local
  Command accounting     scheme:  HWTACACS=shebeiguanli
  Default authentication scheme:  Local
  Default authorization  scheme:  Local
  Default accounting     scheme:  Local
  Accounting start failure action: Online
  Accounting update failure action: Online
  Accounting quota out policy: Offline
  Service type: HSI
  Session time: Exclude idle time
  Dual-stack accounting method: Merge
  Authorization attributes:
    Idle cut: Disabled
    IGMP access limit: 4
MLD access limit: 4
```

至此，S6520X交换机hwtacacs典型组网配置案例已完成！