S3110 hwtacacs典型组网配置案例（IMC部署TAM作为tacacs服务器）

Tacacs 韦家宁 2020-05-20 发表

组网及说明

本案例使用S3110交换机部署hwtacacs，与IMC TAM进行联动，达到安全管理设备的效果。
IMC版本为PLAT 7.3 E0506P03

S3110版本信息如下：
H3C Comware Platform Software
Comware Software, Version 5.20.99, Release 1106

H3C S3110-26TP uptime is 0 week, 0 day, 2 hours, 50 minutes

H3C S3110-26TP
128M bytes DRAM
32M bytes Flash Memory
Config Register points to Flash

Hardware Version is REV.A
Bootrom Version is 110
[SubSlot 0] 24FE+2GE Combo Hardware Version is REV.A

配置步骤

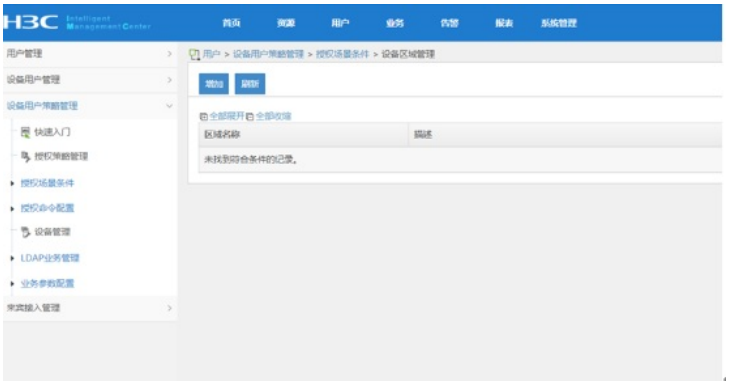
IMC TAM部署有如下要点：
1、授权场景条件：
设备区域管理、设备类型管理、授权时段策略管理
2、授权命令配置：
Shell profile配置、命令集配置
3、设备管理：
配置共享密钥、绑定设备区域、绑定设备类型
4、添加用户名、密码

交换机部署hwtacacs

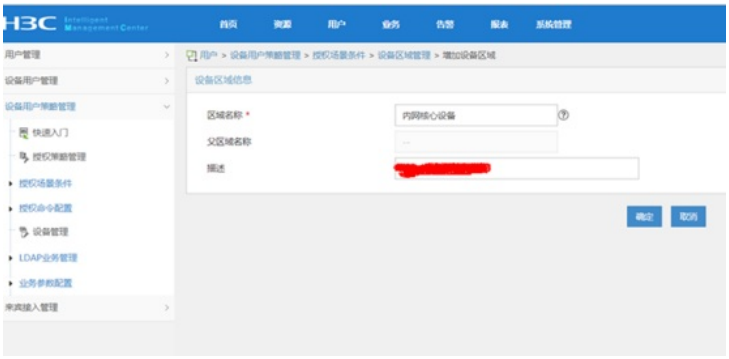
配置关键点

配置“授权场景条件”

添加“设备区域管理”



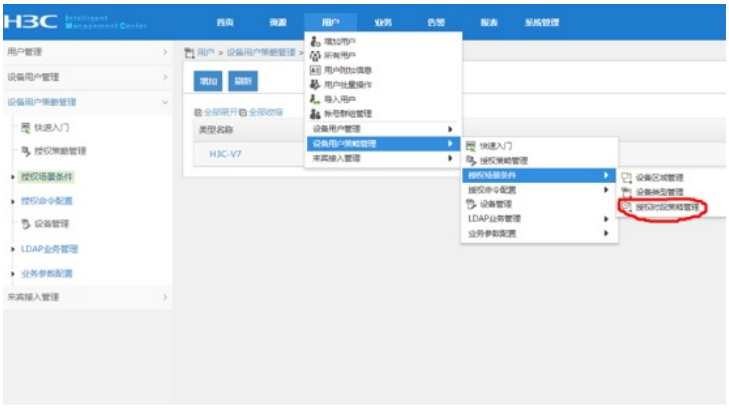
设置“区域名称”



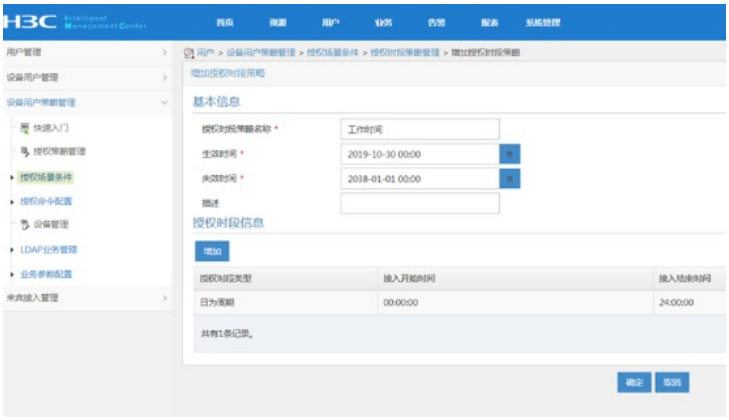
设置“设备类型管理”

增加

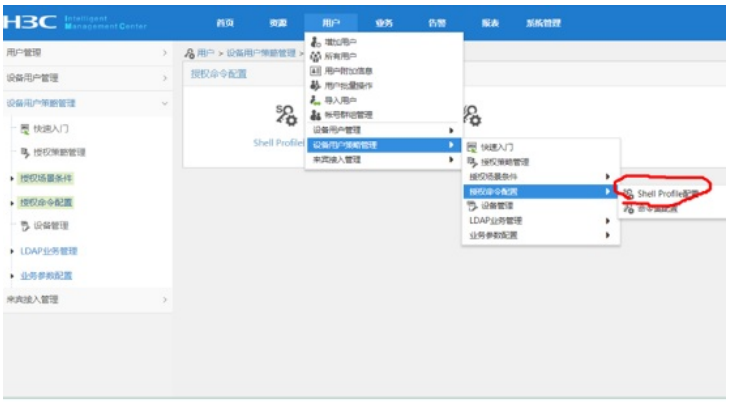
设置“授权时段策略管理”



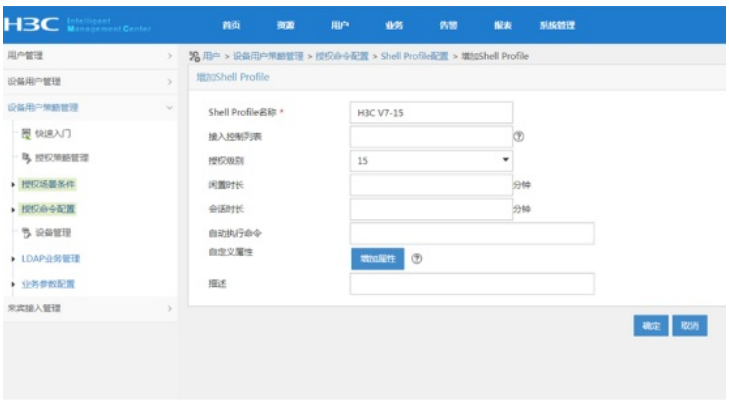
增加，设置“授权时段策略名称”、“生效时间”、“失效时间”



设置“授权命令配置”-“shell profile配置”

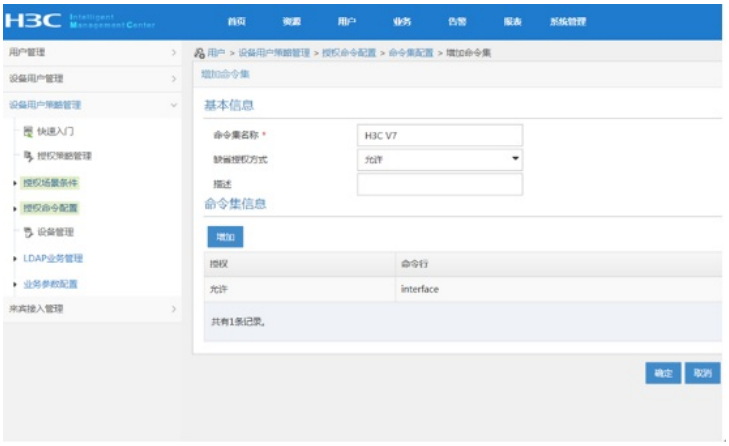


设置“shell profile名称”-“授权级别”

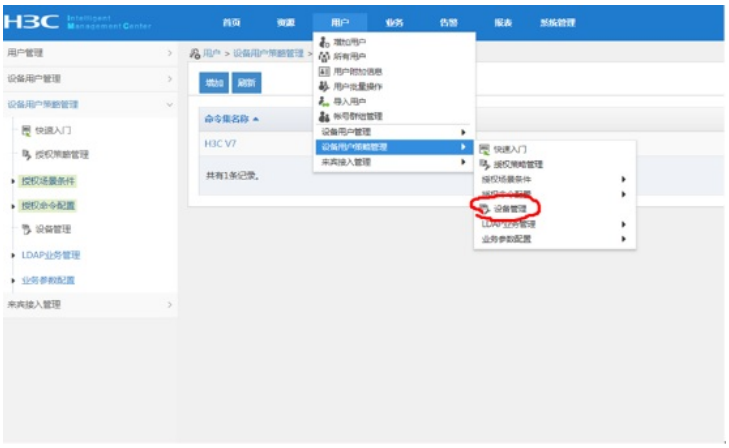


设置“命令集配置”

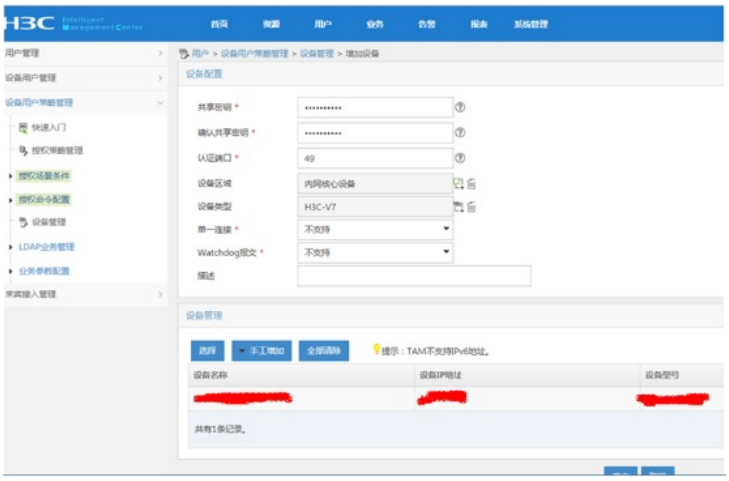
设置“命令集名称”、“缺省授权方式”



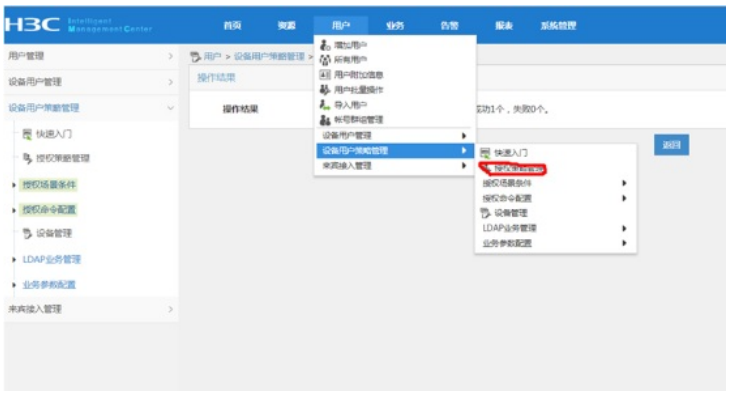
配置“设备管理”



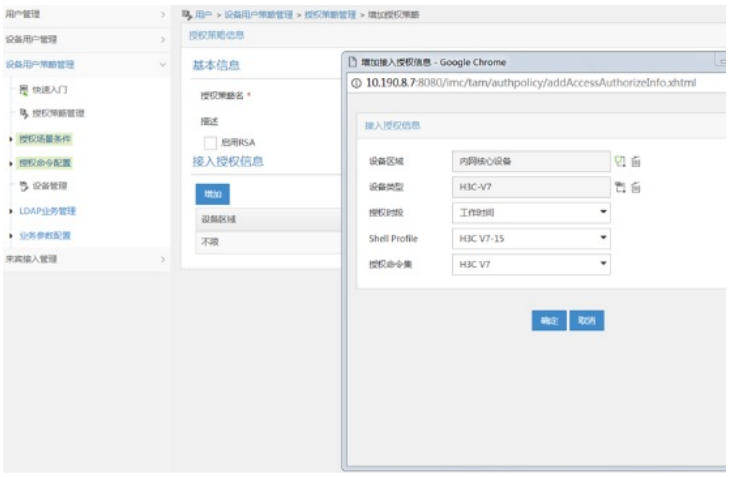
增加设备，设置“共享密钥”、“确认共享密钥”，绑定“设备区域”、“设备类型”



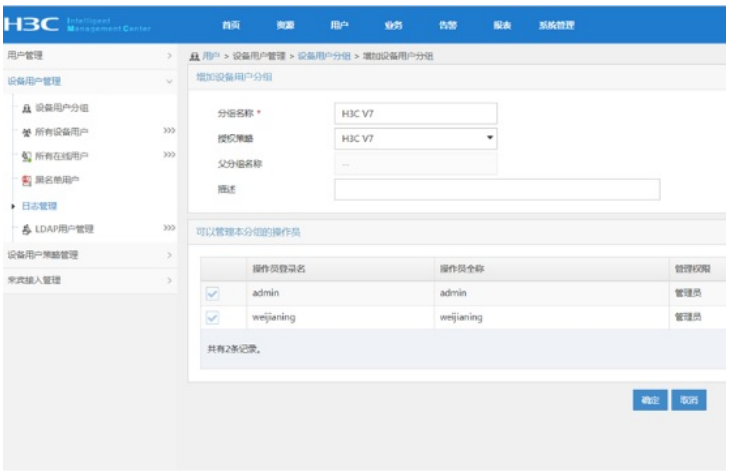
配置“授权管理”



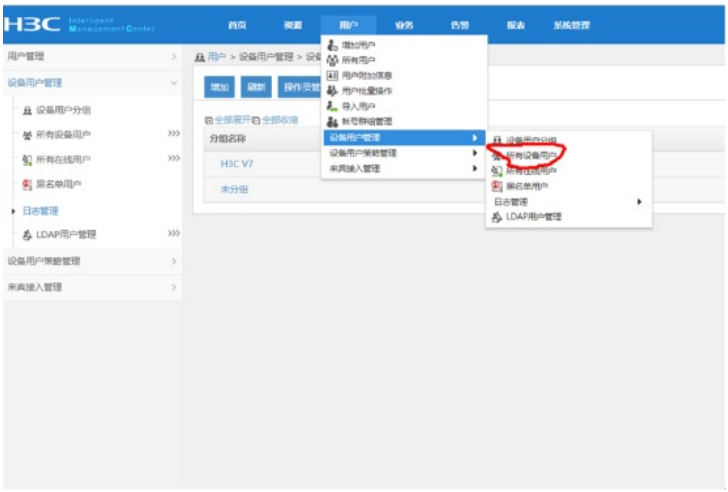
绑定“设备区域”-“设备类型”-“授权时段”-“shell profile”-“授权命令集”



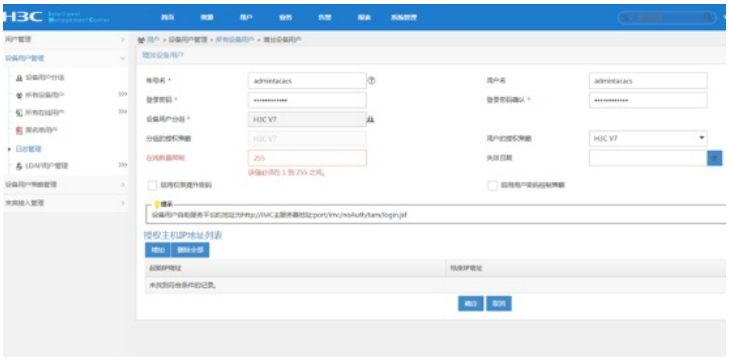
配置“用户设备分组”，设置“分组名称”-“授权策略”



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”



S3110 hwtacacs部署：

```
hwtacacs scheme shebeiguanli
 primary authentication 10.190.8.7
 primary authorization 10.190.8.7
 primary accounting 10.190.8.7
 key authentication  nnhwtacacs
 key authorization  nnhwtacacs
 key accounting  nnhwtacacs
 user-name-format without-domain
 nas-ip 10.190.232.67



 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 optional
quit

local-user admin
 service-type  terminal ssh
quit

user-interface vty 0 15
authentication-mode scheme
command accounting
command authorization
quit
```

查看hwtacacs显示信息：

dis hwtacacs

```
  ------------------------------------------------------------------------------
  HWTACACS-server template name     : shebeiguanli
  Primary-authentication-server     : 10.190.8.7:49
  Primary-authorization-server      : 10.190.8.7:49
  Primary-accounting-server         : 10.190.8.7:49
  Secondary-authentication-server   : 0.0.0.0:0
  Secondary-authorization-server    : 0.0.0.0:0
  Secondary-accounting-server       : 0.0.0.0:0
  Current-authentication-server     : 10.190.8.7:49
  Current-authorization-server      : 10.190.8.7:49
  Current-accounting-server         : 10.190.8.7:49
  Nas-IP address                    : 10.190.232.67
  key authentication                : ******
  key authorization                 : ******
  key accounting                    : ******
  Nas-IP address                    : 10.190.232.67
  Quiet-interval(min)               : 5
  Realtime-accounting-interval(min) : 12
  Response-timeout-interval(sec)    : 5
  Acct-stop-PKT retransmit times    : 100
  Username format                   : without-domain
  Data traffic-unit                 : B
  Packet traffic-unit               : one-packet
  ------------------------------------------------------------------------------
  Total 1 HWTACACS scheme(s).
```

查看domain的显示信息：

```
dis domain tamdm
   Domain: tamdm
   State: Active
   Access-limit: Disabled
   Accounting method: Optional
   Default authentication scheme      : local
   Default authorization scheme       : local
   Default accounting scheme          : local
   Login authentication scheme        : hwtacacs:shebeiguanli, local
   Login authorization scheme         : hwtacacs:shebeiguanli, local
   Login accounting scheme            : hwtacacs:shebeiguanli, local
   Command authorization scheme       : hwtacacs:shebeiguanli, local
   Domain User Template:
   Idle-cut : Disabled
   Self-service : Disabled
   Authorization attributes:
```

至此，S3110交换机hwtacacs典型组网配置案例已完成！