S7503E hwtacacs典型组网配置案例（IMC部署TAM作为tacacs服务器）

Tacacs 韦家宁 2020-04-08 发表

组网及说明

本案例使用H3C S7503E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
S7503E交换机的版本如下：
H3C Comware Software, Version 7.1.070, Release 7557P03
Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.
H3C S7503E-M uptime is 17 weeks, 3 days, 6 hours, 56 minutes
Last reboot reason : Cold reboot

Boot image: flash:/S7500E-CMW710-BOOT-R7557P03.bin
Boot image version: 7.1.070, Release 7557P03
Compiled Nov 07 2017 16:00:00
System image: flash:/S7500E-CMW710-SYSTEM-R7557P03.bin
System image version: 7.1.070, Release 7557P03
Compiled Nov 07 2017 16:00:00

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

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
5、S7503E交换机配置hwtacacs

配置关键点

IMC侧配置：
配置“授权场景条件”

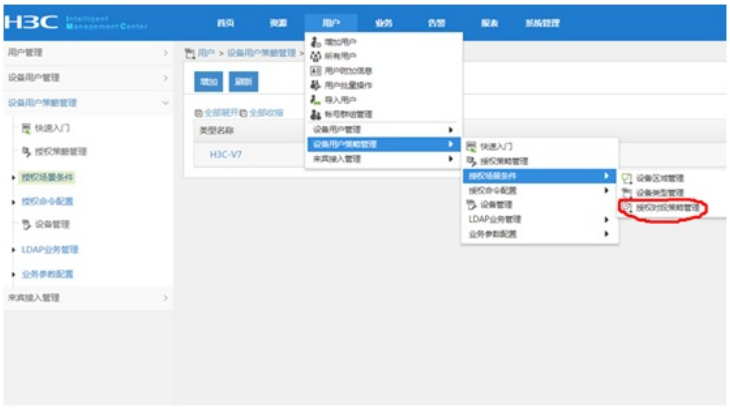
添加“设备区域管理”

设置“区域名称”

设置“设备类型管理”

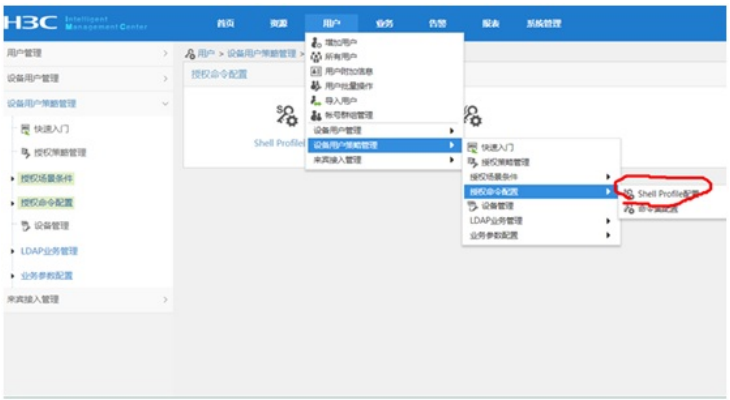
增加

设置“授权时段策略管理”

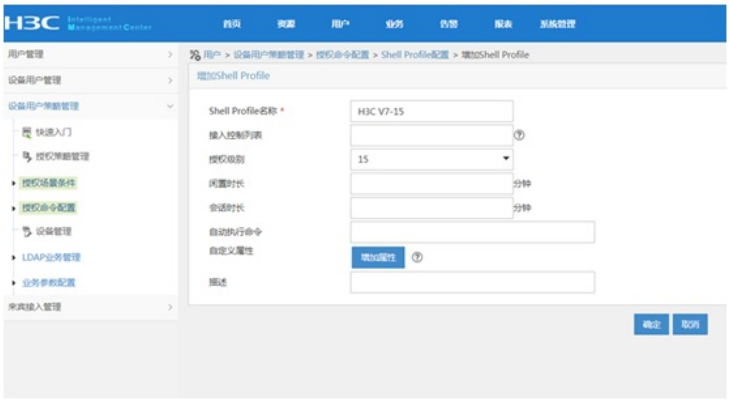


增加，设置“授权时段策略名称”、“生效时间”、“失效时间”

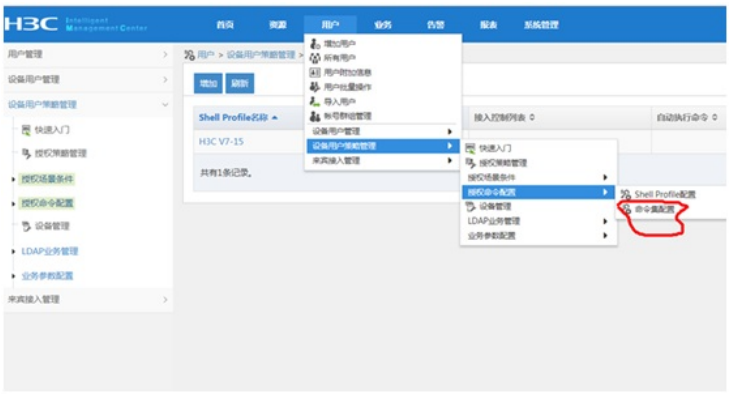
设置“授权命令配置”-“shell profile配置”



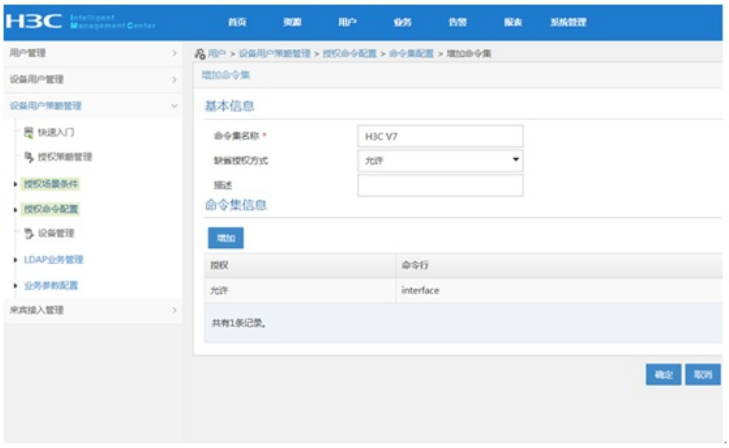
设置“shell profile名称”-“授权级别”



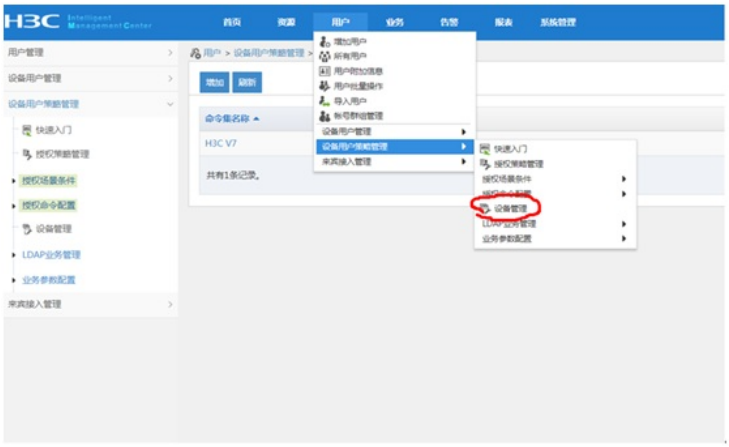
设置“命令集配置”



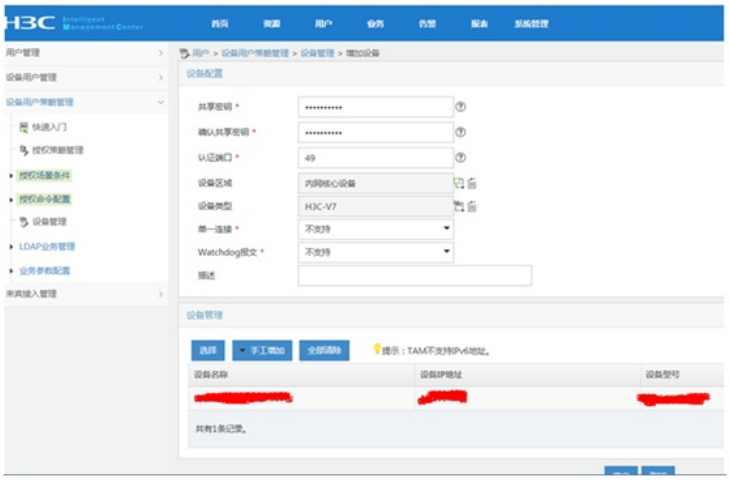
设置“命令集名称”、“缺省授权方式”

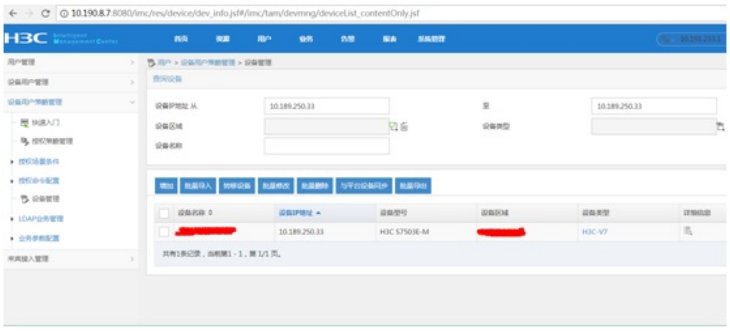


配置“设备管理”

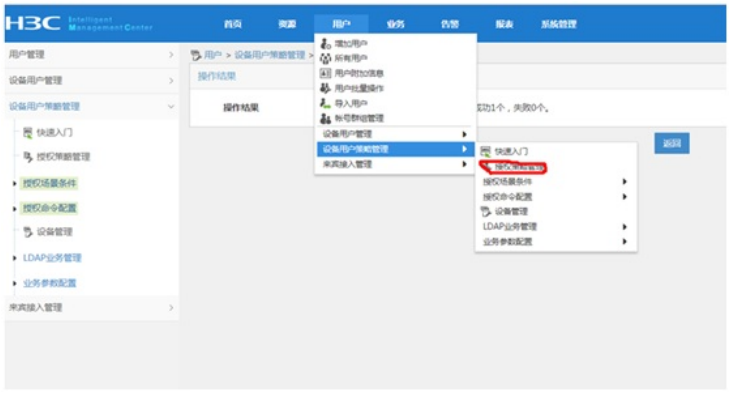


增加设备，设置“共享密钥”、“确认共享密钥”，绑定“设备区域”、“设备类型”

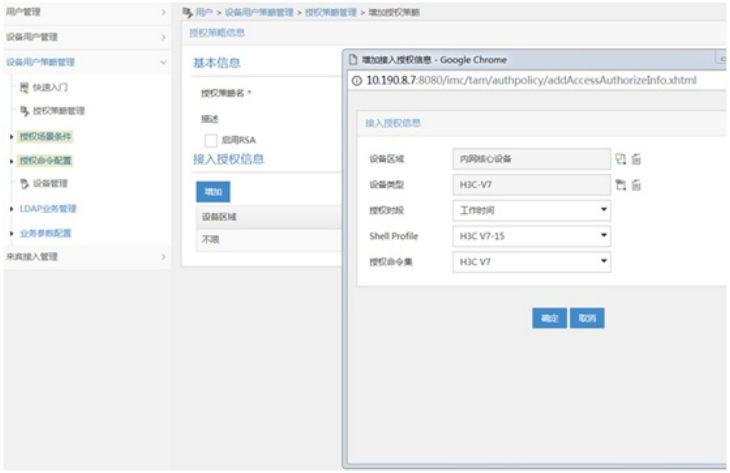




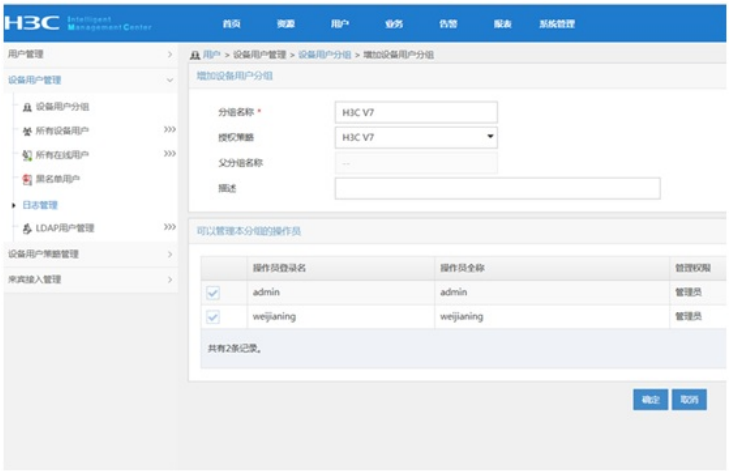
配置“授权管理”



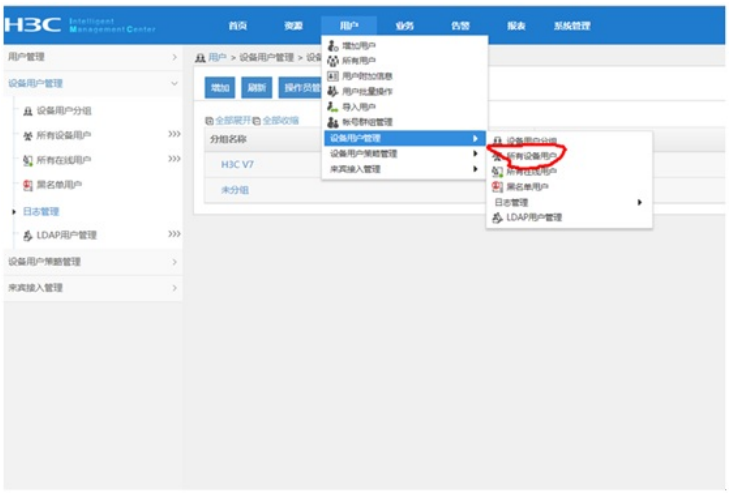
绑定“设备区域”-“设备类型”-“授权时段”-“shell profile”-“授权命令集”



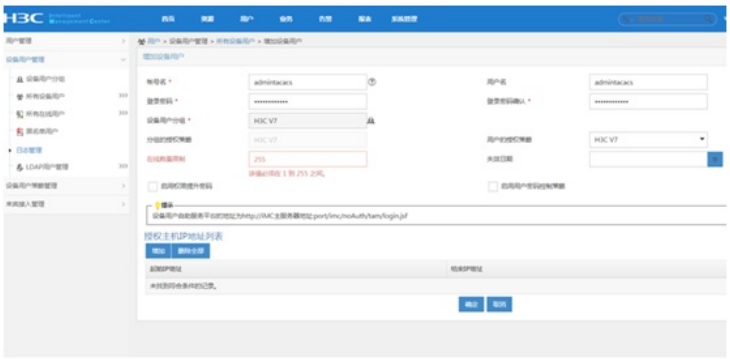
配置“用户设备分组”，设置“分组名称”-“授权策略”



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”



S7503E tacacs部署：

1、部署hwtacacs方案

```
hwtacacs scheme shebeiguanli
 primary authentication 10.190.8.7  //指定认证服务器
 primary authorization 10.190.8.7  //指定授权服务器
 primary accounting 10.190.8.7  //指定计费服务器
 key authentication cipher $c$3$Rq1CZthv4iRJXyN2WzfKFHBiuzEQakm36IGE3F4=  //指定认证密钥
 key authorization cipher $c$3$YgH9b/imd5MVywPEEuFTuOAuB7CEfBGxGBAsfgU=
 key accounting cipher $c$3$64W4CnmoC5VSSl/8ApDbghZ3MtCSrbSbHxp6YGM=
 user-name-format without-domain
 nas-ip 10.189.250.33  //指定nas ip为本机
 vpn-instance XXWG34
```

2、配置domain

```
domain tamdm
 authentication login hwtacacs-scheme shebeiguanli local  //配置认证登录的方式调用hwtacacs方案
 authorization login hwtacacs-scheme shebeiguanli local //配置授权登录的方式调用hwtacacs方案

 accounting login hwtacacs-scheme shebeiguanli local //配置计费登录的方式调用hwtacacs方案

 authorization command hwtacacs-scheme shebeiguanli local  //配置授权命令集调用hwtacacs方案

 accounting command hwtacacs-scheme shebeiguanli //配置认计费命令集调用hwtacacs方案

#
 domain default enable tamdm  //配置tamdm为默认domain

dis domain tamdm  //查看tamdm域的信息

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
```

dis hwtacacs scheme //查看hwtacacs的显示信息：

```
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                         : XXWG34
  NAS IP Address                       : 10.189.250.33
  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
------------------------------------------------------------------------
```

至此，S7503E hwtacacs典型组网配置案例已完成！