

组网及说明

本案例使用S5110 V5平台的交换机配置hwtacacs，与IMC TAM联动，实现设备的安全管理。

IMC版本为PLAT 7.3 E0506P03

S5110的版本信息如下：

H3C Comware Platform Software

Comware Software, Version 5.20.99, Release 1114

Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.

H3C S5110-52P uptime is 66 weeks, 4 days, 19 hours, 55 minutes

H3C S5110-52P

128M bytes DRAM

32M bytes Flash Memory

Config Register points to Flash

Hardware Version is Ver.A

Bootrom Version is 121

[SubSlot 0] 48GE+4SFP Hardware Version is Ver.A

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

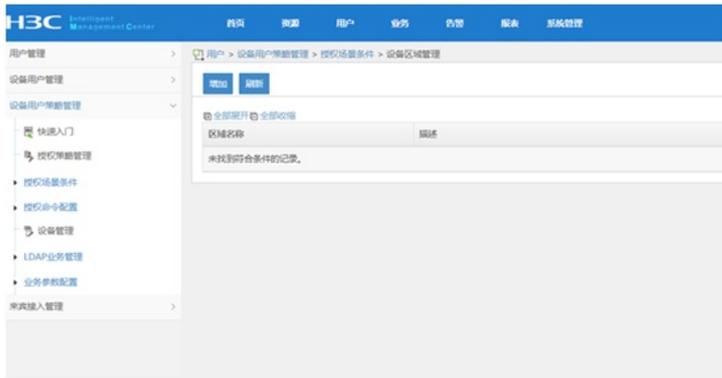
5、S5110部署hwtacacs

配置关键点

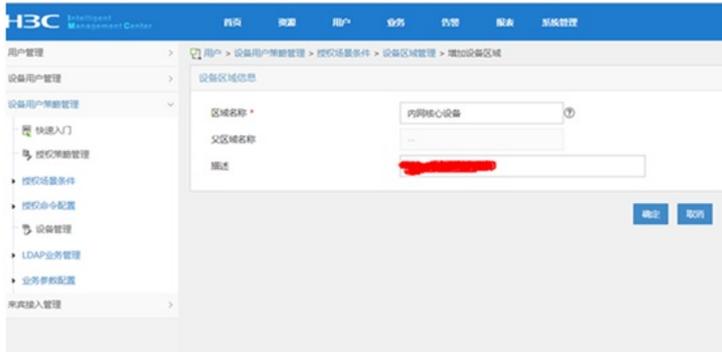
IMC侧配置：



添加“设备区域管理”



设置“区域名称”



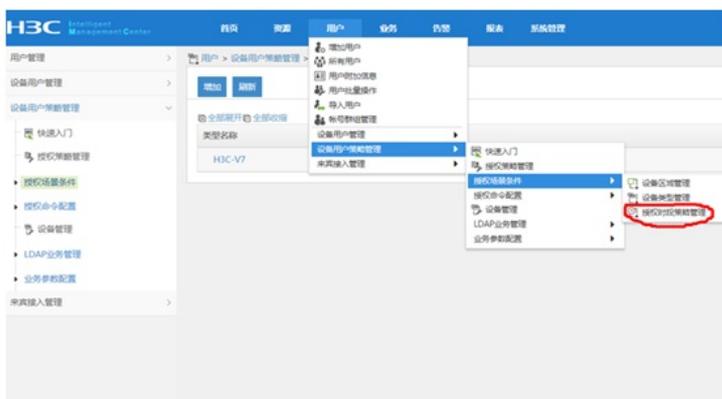
设置“设备类型管理”



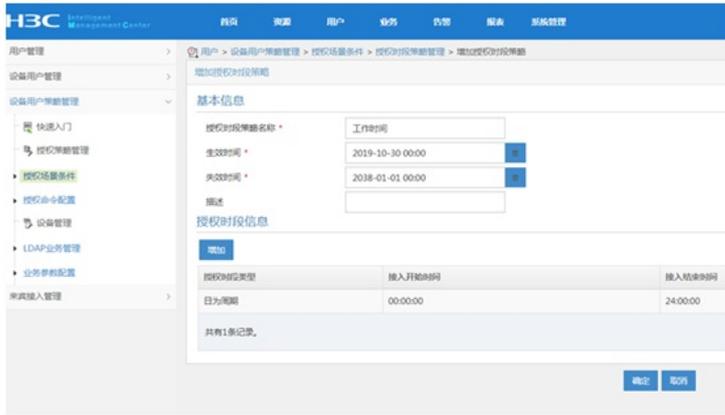
增加



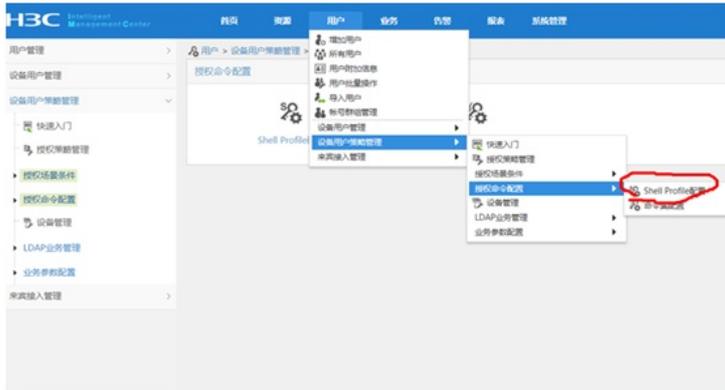
设置“授权时段策略管理”



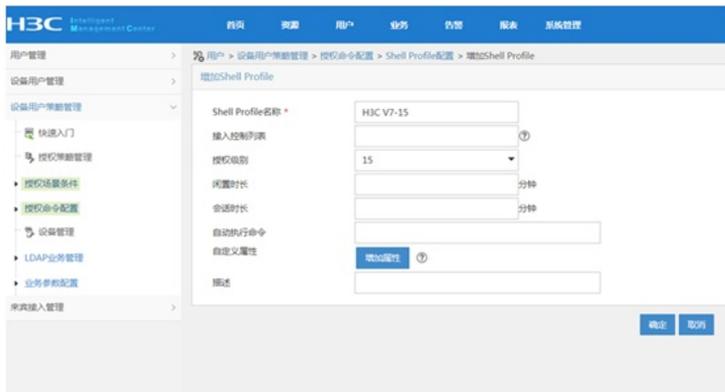
增加，设置“授权时段策略名称”、“生效时间”、“失效时间”



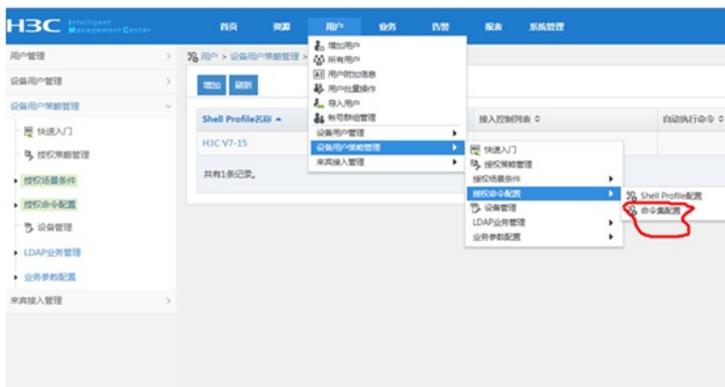
设置“授权命令配置”-“shell profile配置”



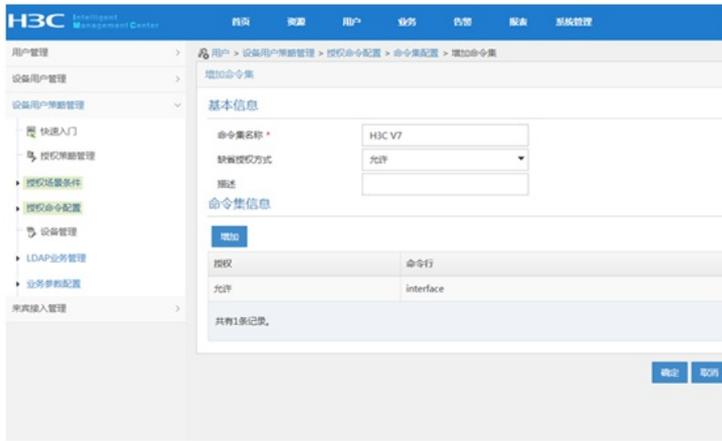
设置“shell profile名称”-“授权级别”



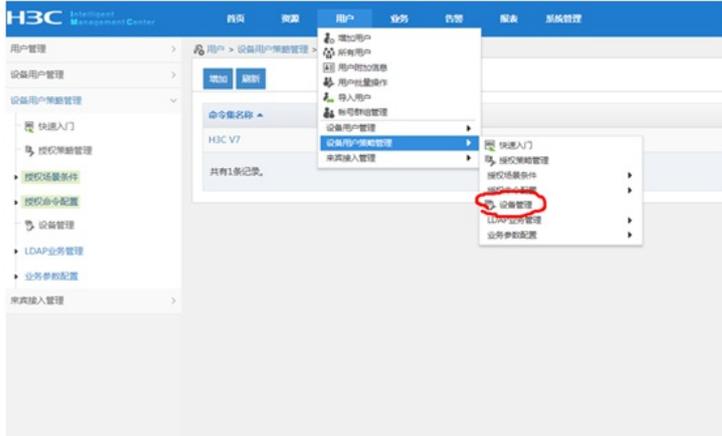
设置“命令集配置”



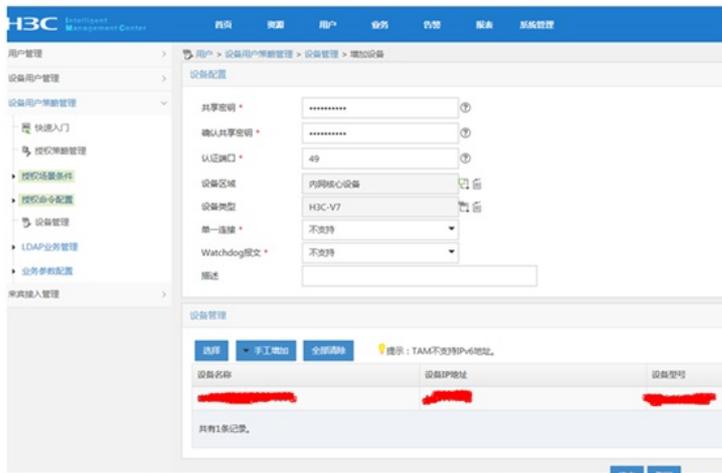
设置“命令集名称”、“缺省授权方式”



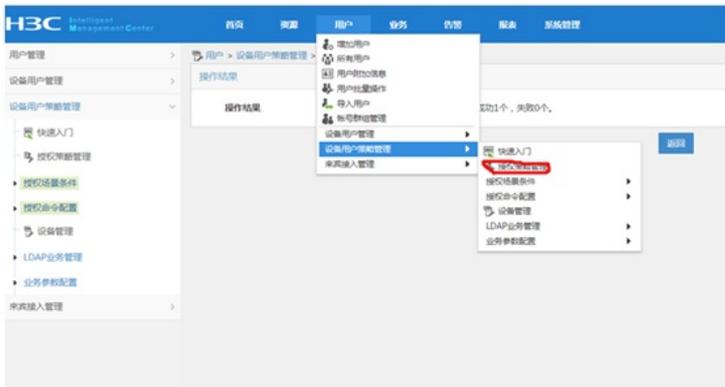
配置“设备管理”



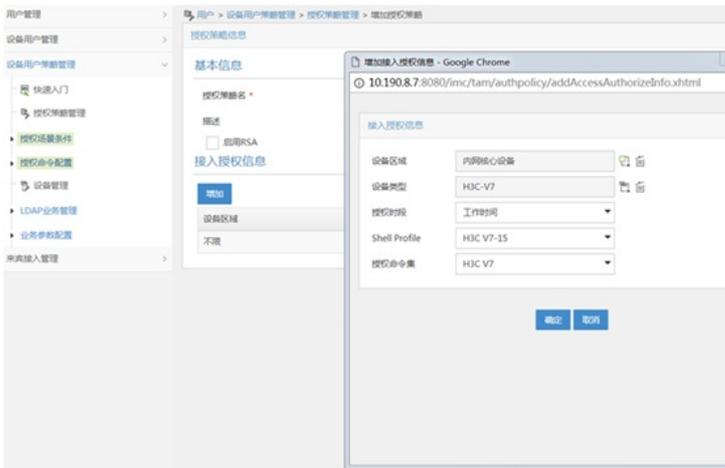
增加设备，设置“共享密钥”、“确认共享密钥”，绑定“设备区域”、“设备类型”



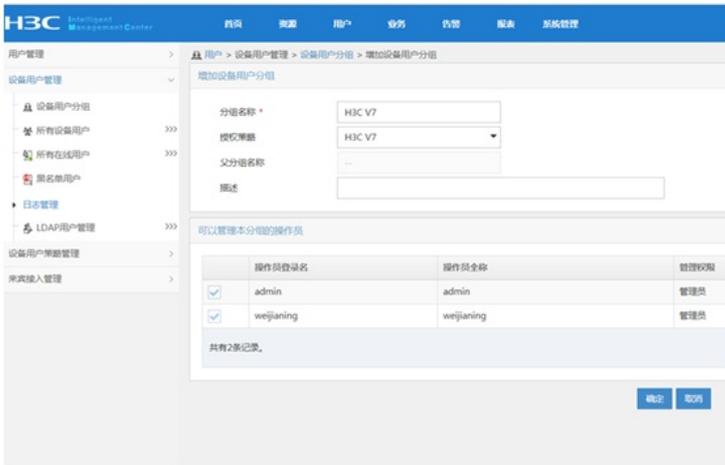
配置“授权管理”



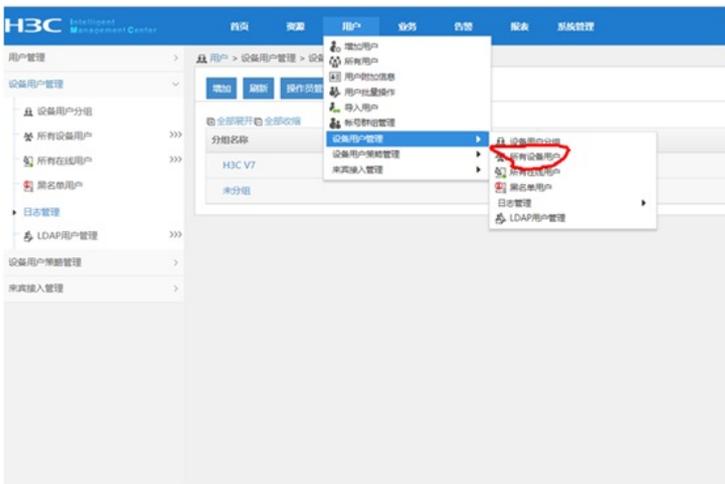
绑定“设备区域”-“设备类型”-“授权时段”-“shell profile”-“授权命令集”



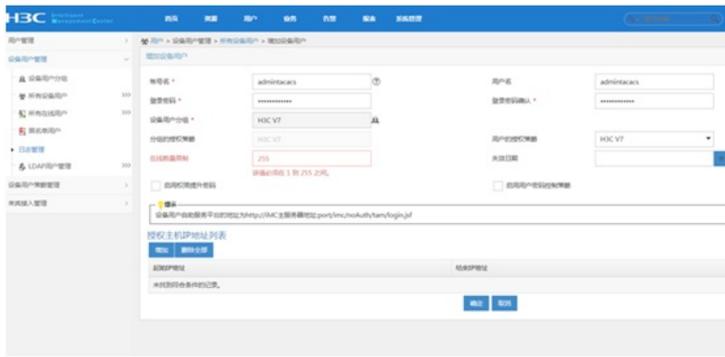
配置“用户设备分组”，设置“分组名称”-“授权策略”



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”



S5110 hwtacacs部署如下:

1、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 cipher \$c\$3\$kHqcyXRvfw1cyq1Tb1go1/TjG/qanV4VZunL0=

key authorization cipher \$c\$3\$FDnTqnTQ8f7BUMeU1912Ksm95d3HLCGKCTkDoBo=

key accounting cipher \$c\$3\$1ftl2Apw/x0+auLDgfV1ulALChfec1aOPURqUGY=

user-name-format without-domain

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

access-limit disable

state active

idle-cut disable

self-service-url disable

3、启用默认domain:

domain default enable tamdm

至此，S5110交换机（V5）hwtacacs典型组网配置案例已完成!