

知 S5500 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

本案例采用S5500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

S5500版本信息：

H3C Comware Platform Software

Comware Software, Version 5.20, Release 5206

Copyright (c) 2004-2013 Hangzhou H3C Tech. Co., Ltd. All rights reserved.

H3C S5500-58C-HI uptime is 90 weeks, 5 days, 6 hours, 42 minutes

H3C S5500-58C-HI with 2 Processors

1024M bytes SDRAM

4096K bytes Nor Flash Memory

512M bytes Nand Flash Memory

Hardware Version is REV.C

CPLD Version is 003

Bootrom Version is 211

[SubSlot 0] 48GE+4SFP+2SFP PLUS Hardware Version is REV.C

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、S5500部署hwtacacs

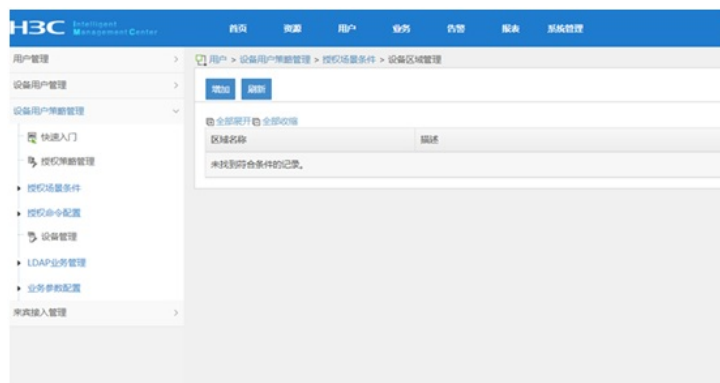
配置关键点

IMC侧配置如下：

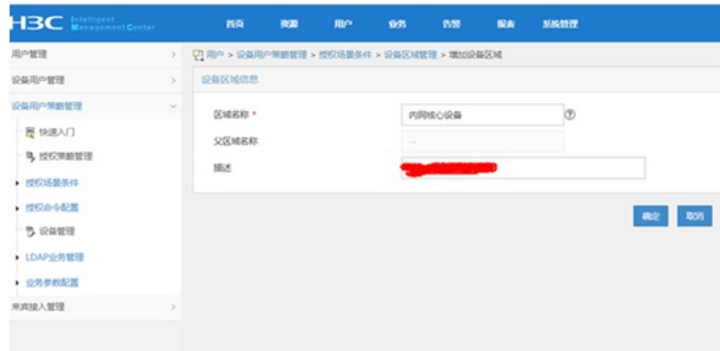
配置“授权场景条件”



添加“设备区域管理”



设置“区域名称”



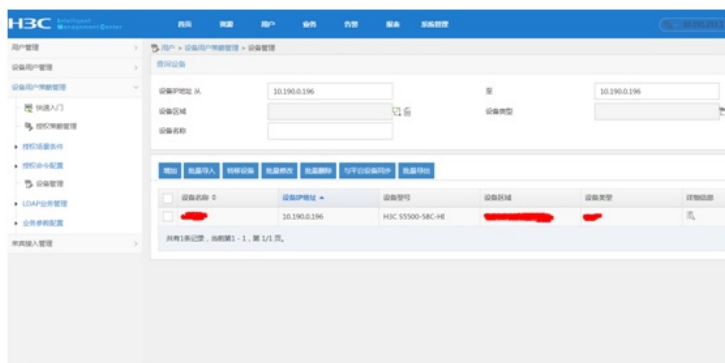
设置“设备类型管理”



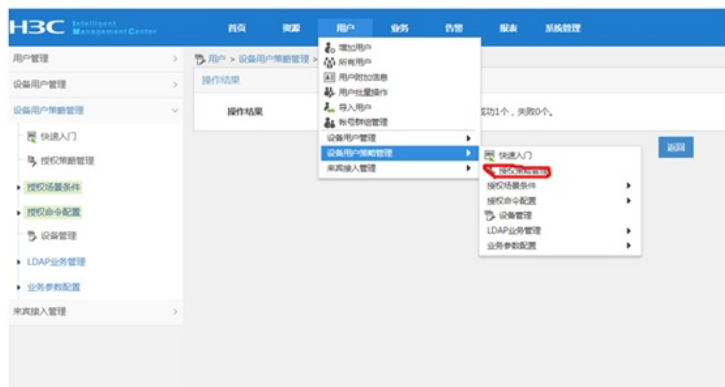
增加



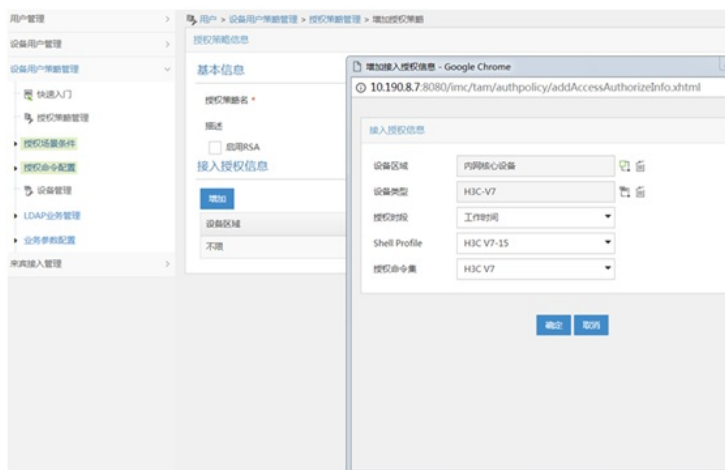
设置“授权时段策略管理”



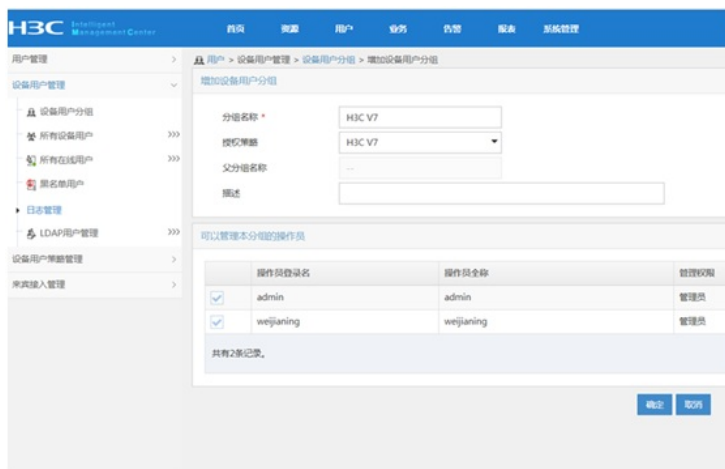
配置“授权管理”



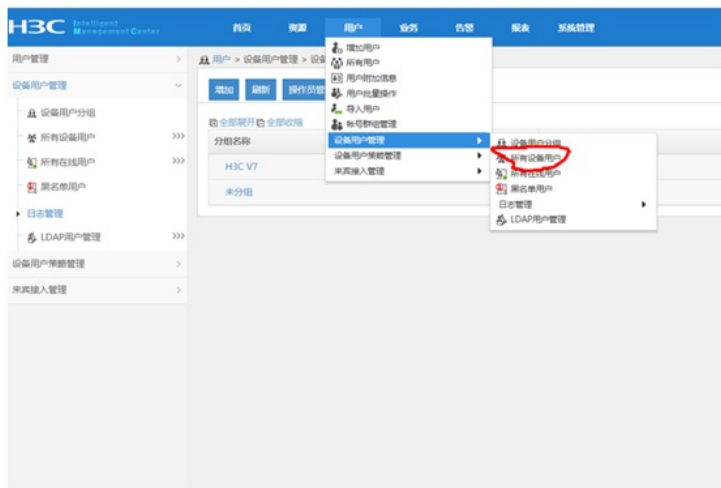
绑定“设备区域”-“设备类型”-“授权时段”-“shell profile”-“授权命令集”



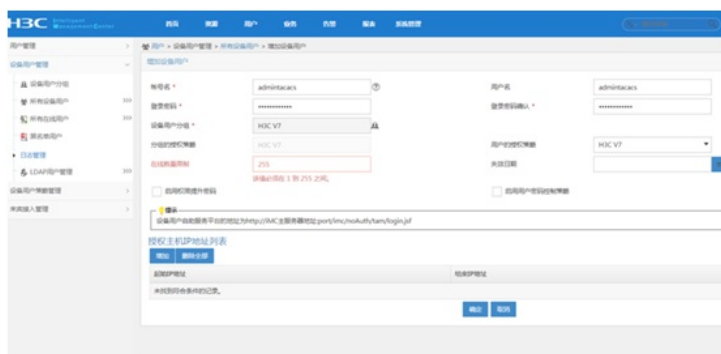
配置“用户设备分组”，设置“分组名称”-“授权策略”



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”



S5500 hwtacacs部署如下:

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

nas-ip 10.190.0.196

key authentication cipher \$c\$3\$cfGkloFkI4gPycbjPGJU0ycuqcn6cajnIItsRBo=

key authorization cipher \$c\$3\$xaEme+UbBnijKlztJvElrByux984yGlf/x/deG8=

key accounting cipher \$c\$3\$owN6PJUawje2DzODvLdR9UMecnfMTB9aYWFirTc=

user-name-format without-domain

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

access-limit disable

state active

idle-cut disable

self-service-url disable

3、部署默认domain:

domain default enable tamdm

4、查看hwtacacs显示信息:

dis hwtacacs

HWTACACS scheme name : shebeiguanli

Primary Authen Server:

IP: 10.190.8.7 Port: 49 State: Active

VPN instance : Not configured

Encryption Key : Not configured

Primary Author Server:

IP: 10.190.8.7 Port: 49 State: Active

VPN instance : Not configured
Encryption Key : Not configured
Primary Account Server:
IP: 10.190.8.7 Port: 49 State: Active
VPN instance : Not configured
Encryption Key : Not configured
NAS IP address : 10.190.0.196
Authentication key : *****
Authorization key : *****
Accounting key : *****
VPN instance : Not configured
Quiet interval(min) : 5
Realtime accounting interval(min) : 12
Response timeout interval(sec) : 5
Retransmission times of stop-accounting packet : 100
Username format : without-domain
Data flow unit : Byte
Packet unit : one

Total 1 HWTACACS scheme(s).

、查看domain显示信息:

dis domain

0 Domain : system

State : Active
Access-limit : Disabled
Accounting method : Required
Default authentication scheme : local
Default authorization scheme : local
Default accounting scheme : local
Domain User Template:
Idle-cut : Disabled
Self-service : Disabled
Authorization attributes:

1 Domain : tamdm

State : Active
Access-limit : Disabled
Accounting method : Required
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
Command accounting scheme : hwtacacs:shebeiguanli
Domain User Template:
Idle-cut : Disabled
Self-service : Disabled
Authorization attributes:

Default Domain Name: tamdm

Total 2 domain(s).

至此，S5500 hwtacacs典型组网配置案例已完成！