

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
Copyright (c) 2004-2015 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
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

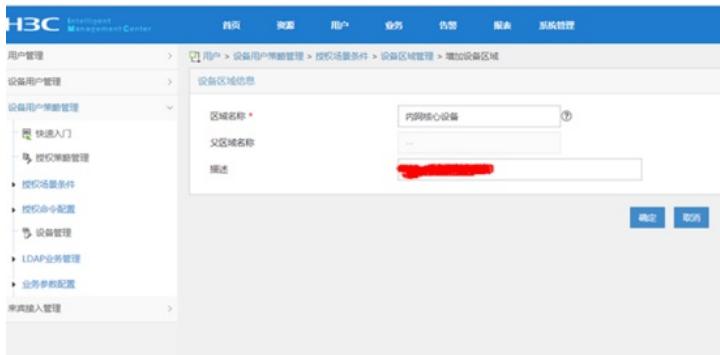
配置“授权场景条件”



添加“设备区域管理”



设置“区域名称”



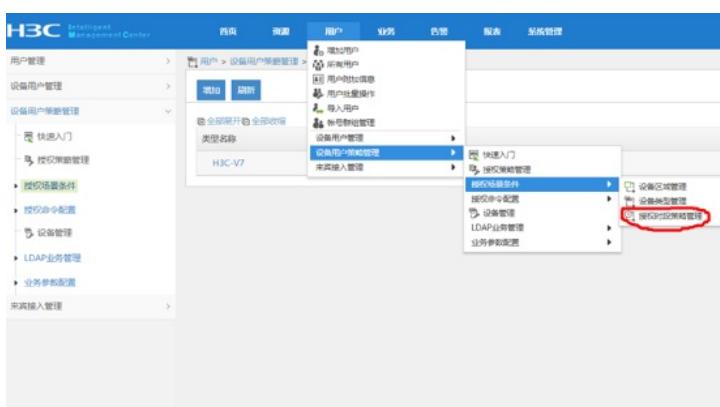
设置“设备类型管理”



增加



设置“授权时段策略管理”

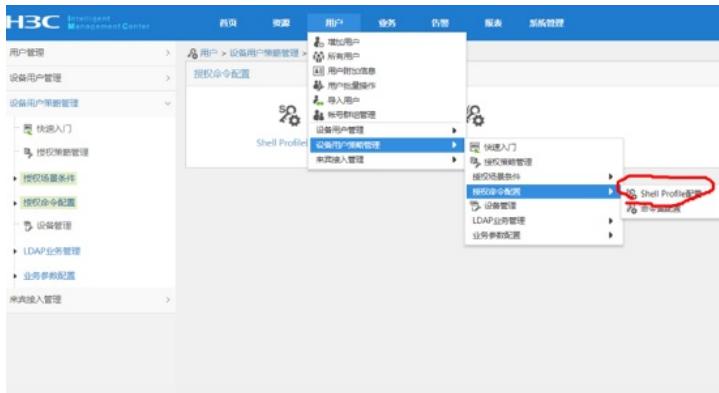


增加，设置“授权时段策略名称”、“生效时间”、“失效时间”

设置“授权时段管理”-“授权时间段配置”

授权时段名称 *: 工作时间
 生效时间 *: 2019-10-30 00:00
 失效时间 *: 2018-01-01 00:00
 描述:
 授权时段信息
 增加
 指定时段类型: 插入开始时间: 插入结束时间:
 日为周期: 00:00:00 24:00:00
 共有1条记录。
 确定 取消

设置“授权命令配置”-“shell profile配置”

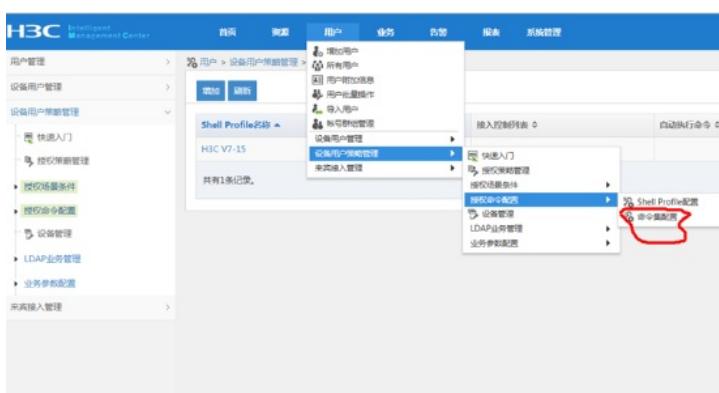


设置“shell profile名称”-“授权级别”

设置“命令集配置”

Shell Profile名称*: H3C V7-15
 插入控制列表: 15 分钟
 授权级别: 分钟
 间隔时长: 分钟
 会话时长: 分钟
 自动执行命令: 自定义属性
 插入: 确定 取消

设置“命令集配置”



设置“命令集名称”、“缺省授权方式”

The screenshot shows the '命令集配置' (Command Set Configuration) page. In the '基本信息' (Basic Information) section, the command set name is 'H3C V7' and the privilege level is '允许' (Allow). In the '命令信息' (Command Information) section, there is one entry: '权限' (Privilege) is '命令行' (Command Line), and '允许' (Allow) is 'interface'. At the bottom right, there are '确定' (Confirm) and '取消' (Cancel) buttons.

配置“设备管理”

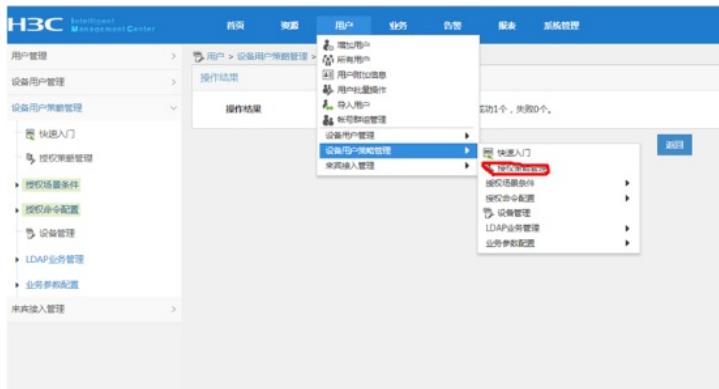
The screenshot shows a context menu being used to assign permissions. A right-clicked item has a submenu where '设备管理' (Device Management) is highlighted and circled in red. Other options in the submenu include '快速入门' (Quick Start), '授权策略管理' (Authorization Policy Management), '授权条件管理' (Authorization Condition Management), '命令行管理' (Command Line Management), '业务参数配置' (Business Parameter Configuration), and '业务参数配置' (Business Parameter Configuration).

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”

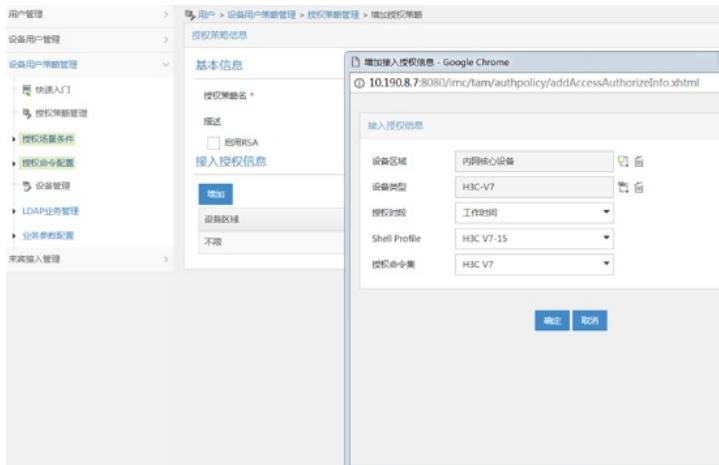
The screenshot shows the '增加设备' (Add Device) page. The '共享密钥' (Shared Key) field contains '*****', and the '确认共享密钥' (Confirm Shared Key) field also contains '*****'. The '认证端口' (Authentication Port) is set to '49'. The '设备区域' (Device Area) is '内网核心设备' (Intranet Core Equipment), and the '设备类型' (Device Type) is 'H3C-V7'. The '单一连接' (Single Connection) dropdown is set to '不支持' (Not Supported). The 'Watchdog校验' (Watchdog Check) dropdown is also set to '不支持' (Not Supported). Below the form, the '设备管理' (Device Management) section shows a table with one row of data.

The screenshot shows the '搜索设备' (Search Device) page. The search criteria are: '开始IP地址从' (Start IP Address From) is '10.190.232.67', '至' (To) is '10.190.232.67', '设备区域' (Device Area) is '任意' (Any), and '设备名称' (Device Name) is empty. Below the search bar, there are several buttons: '搜索' (Search), '批量导入' (Batch Import), '批量导出' (Batch Export), '批量修改' (Batch Modify), '批量删除' (Batch Delete), '为手工添加' (For Manual Addition), and '全局清除' (Global Clear). The main table lists one device entry: '设备名称' (Device Name) is '10.190.232.67', '设备IP地址' (Device IP Address) is '10.190.232.67', '设备型号' (Device Model) is 'ICMP', '设备区域' (Device Area) is 'H3C-V7', and '设备类型' (Device Type) is 'H3C-V7'. A note at the bottom states '共有1条记录，当前第1 - 1, 共1/1页' (1 record found, page 1 of 1).

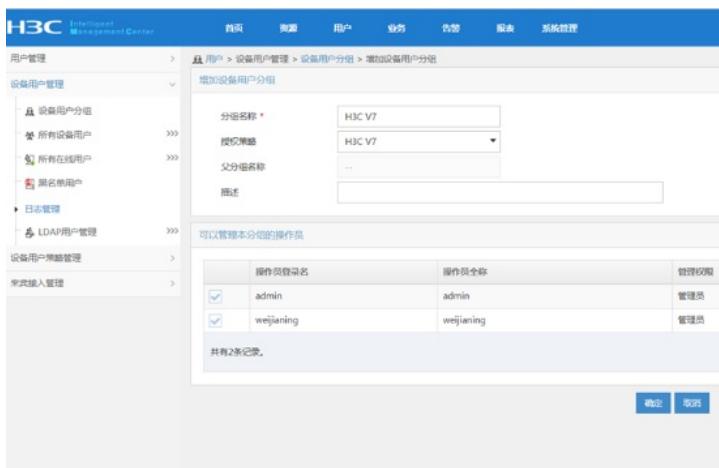
配置“授权管理”



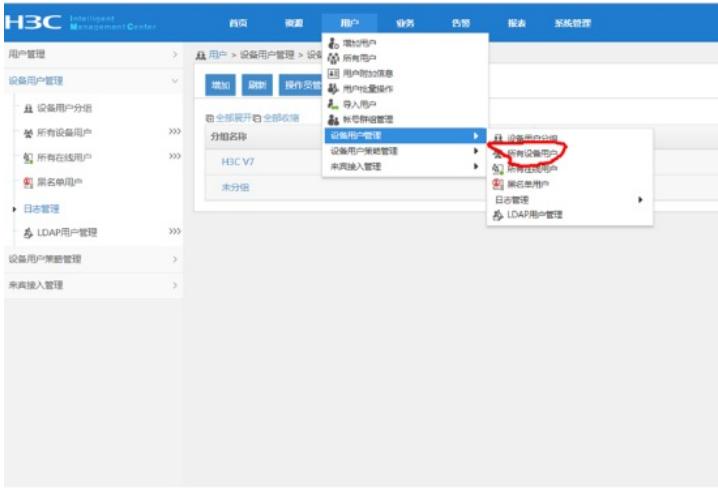
绑定“设备区域”-“设备类型”-“授权时段”-“shell profile”-“授权命令集”



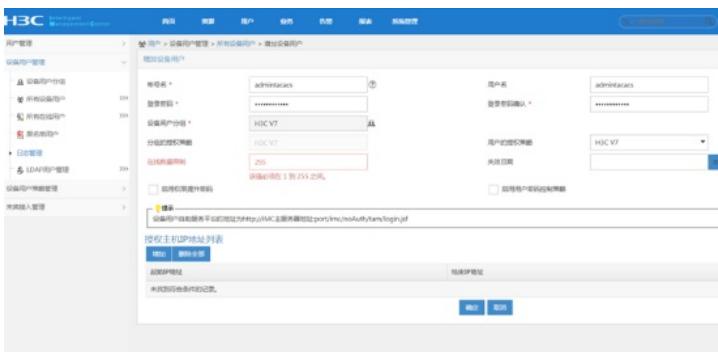
配置“用户设备分组”，设置“分组名称”-“授权策略”



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 nnhtacacs
key authorization nnhtacacs
key accounting nnhtacacs
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！