使用iMC TAM组件对设备登陆用户进行认证授权审计的典型配置

iMC 马永鸿 2021-12-29 发表

组网及说明

某局点网络比较复杂，在网设备较多，网管人员均通过telnet方式来管理设备。在整个管理过程中，有诸如账号管理、配置操作审计以及权限管理等方面的问题。鉴于此，客户有如下需求：

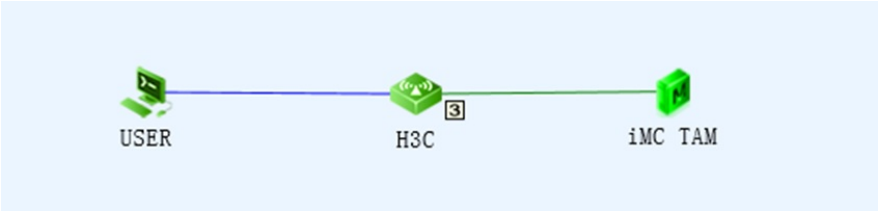
1）所有telnet/ssh账号保存在服务器，进行统一管理。

2）所有账号在现有账号权限级别的基础上，限制某些危险操作，如reset命令。

3）所有账号登陆设备的操作都有迹可循，以便在出现问题之后便于回溯。

设备上保留一全权限账号，该账号仅有相关维护组主管可知，其他账号不可以在设备上新建远程账号。

下图中，iMC TAM代表AAA服务器，H3C为网络中设备，USER为网管人员登录终端。



配置步骤

整个配置涉及到设备侧的配置和TAM服务器侧的配置。

1 TAM服务器侧配置

1） 将设备添加到iMC平台，该步骤为可选步骤。设备上配置为基本的SNMP配置，如下：

snmp-agent

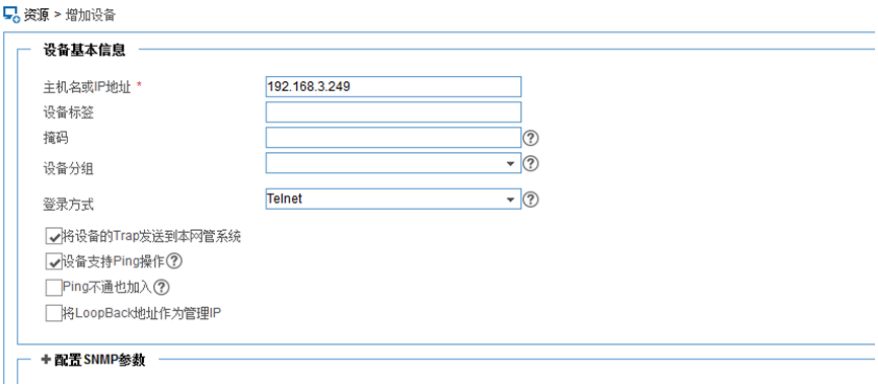
snmp-agent community read public

snmp-agent community write private

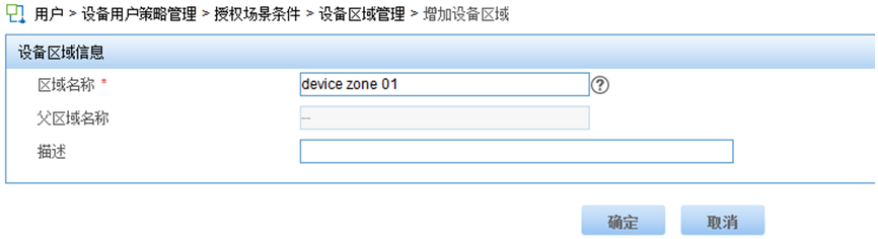
snmp-agent sys-info version all

snmp-agent target-host trap address udp-domain 192.168.3.130 params securityname public v2c

在iMC首页点击【资源】>【增加设备】，输入设备的管理IP地址以及SNMP参数之后，便可将设备成功添加到iMC平台中去，见下图：



2） 配置设备区域，操作员可以基于多种维度来划分设备区域，例如按照设备所处的层次地位划分、按照地理位置划分等。依次点击【用户】>【设备用户策略管理】>【授权场景条件】>【设备区域管理】>【增加设备区域】便可添加一设备区域，本例中以device zone 01为例，见下图：



3） 增加授权时段策略，授权时段主要用来控制网络管理员可以登陆设备进行操作的时间段。依次点击【用户】>【设备用户策略管理】>【授权场景条件】>【授权时段策略管理】>【增加授权时段策略】便可完成一个授权时段的创建。本例以authorization time-range01为例，要求只能在上班时间对网络设备进行操作，见下图：

4） 增加用户shell profile，shell profile将来会被授权策略调用。主要用来限定调用该授权策略的管理员用户的权限级别。依次点击【用户】>【设备用户策略管理】>【授权命令配置】>【shell profile配置】>【增加shell profile】,便可增加一shell profile。本文中以增加shell profile名称shell profile 1为例，规定其授权级别为3。见下图：

在整个操作过程中，需要保证设备和iMC TAM之间hwtacacs可达，如果有防火墙，请放通相关端口。

TAM侧认证、授权以及计费key必须与设备侧配置一致。