WX18H/25H/30H/35H/55H系列管理用户认证典型配置案例（RADIUS服务器）

AAA 章宁 2019-09-18 发表

组网及说明

1 配置需求或说明

1.1 适用场合。

适用于设备管理员登录设备时需要进行身份验证的场合。

1.2 配置需求及实现的效果

配置前需确保终端、设备、服务器相互连通。

设备管理员以Telnet 方式登录设备时，需要进行外置3A服务器进行身份验证,输入账户密码：aaa@device/aaa，radius服务器进行验证，只有验证通过后才能登录到设备进行操作。

IMC作为radius服务器，该实验中以iMC为例（使用iMC版本为：iMC PLAT 7.3(E0605)、iMC EIA 7.3(E0504)）。

2 组网图

Radius服务器IP为192.168.1.218，设备IP地址为192.168.30.100。

1 配置需求或说明

1.1 适用场合。

适用于设备管理员登录设备时需要进行身份验证的场合。

1.2 配置需求及实现的效果

配置前需确保终端、设备、服务器相互连通。

设备管理员以Telnet 方式登录设备时，需要进行外置3A服务器进行身份验证,输入账户密码：aaa@device/aaa，radius服务器进行验证，只有验证通过后才能登录到设备进行操作。

IMC作为radius服务器，该实验中以iMC为例（使用iMC版本为：iMC PLAT 7.3(E0605)、iMC EIA 7.3(E0504)）。

2 组网图

Radius服务器IP为192.168.1.218，设备IP地址为192.168.30.100。

配置步骤

3 配置步骤

3.1 配置RADIUS服务器（IMC）

3.1.1 增加接入设备

将需要管理的设备增加为 UAM 中的接入设备。

增加接入设备的方法如下：

(1) 选择“用户”页签。

(2) 单击导航树中的“接入策略管理> 接入设备管理 > 接入设备配置”菜单项，进入接入设备配置页面。

(3) 单击<增加>按钮，进入增加接入设备页面。

(4)　配置以下参数：

认证端口：输入认证端口，与设备上的配置保持一致，默认为 1812。

计费端口：输入计费端口，与设备上的配置保持一致，默认为 1813。

业务类型：本例选择“设备管理业务”，该类型适用于用户登录到设备进行管理的场景。

接入设备类型：在下拉框中选择设备的厂商和类型。下拉框中包含了Standard、UAM 系统预定义和管理员自定义的厂商和类型。

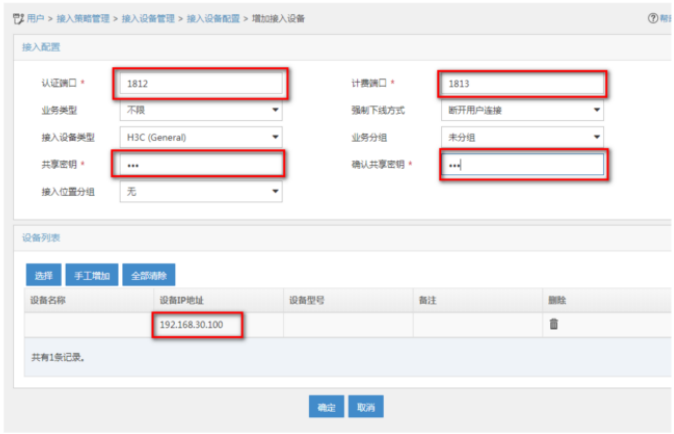
接入设备分组：该参数在用户登录设备进行管理的场景不起作用，保持缺省值即可。

共享密钥：输入共享密钥，与设备命令行中的配置保持一致，共享秘钥为123。

确认共享密钥：再次输入共享密钥。

业务分组：在下拉框中选择设备所属的业务分组。

设备列表：单击<手工增加>按钮，手工增加接入设备。如图3-3 所示。此处设置的IP地址必须与接入设备上nas-ip的配置一致。如果设备上未配置nas-ip，则使用设备与iMC相连的接口的IP。



(5)　单击<确定>按钮，完成增加接入设备。

3.1.2 增加设备管理用户

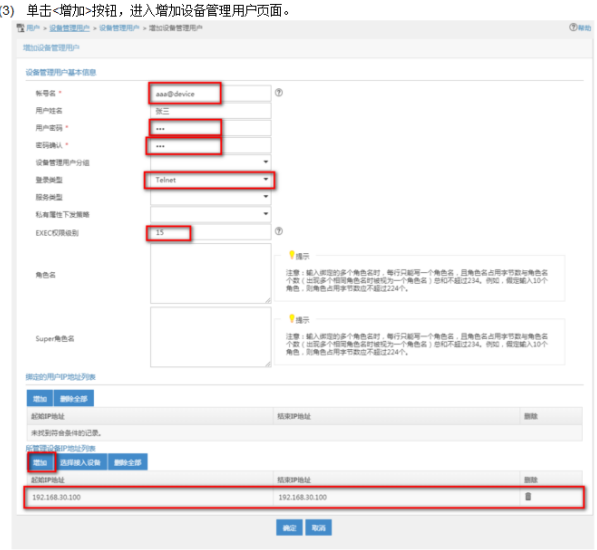
设备管理用户即可以登录并管理设备的用户。

增加设备管理用户的方法如下：

(1)　选择“用户”页签。

(2)　单击导航树中的“接入用户管理 > 设备管理用户”菜单项，进入设备管理用户页面。

(3) 单击<增加>按钮，进入增加设备管理用户页面。



(4) 配置以下参数：

帐号名：输入登录设备时使用的用户名。

用户密码：输入登录设备时使用的密码。

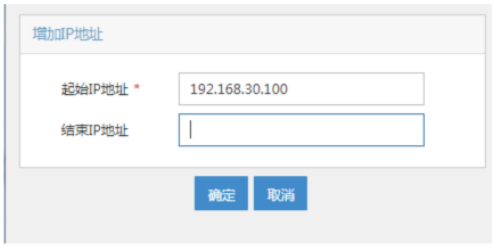
密码确认：再次输入密码。

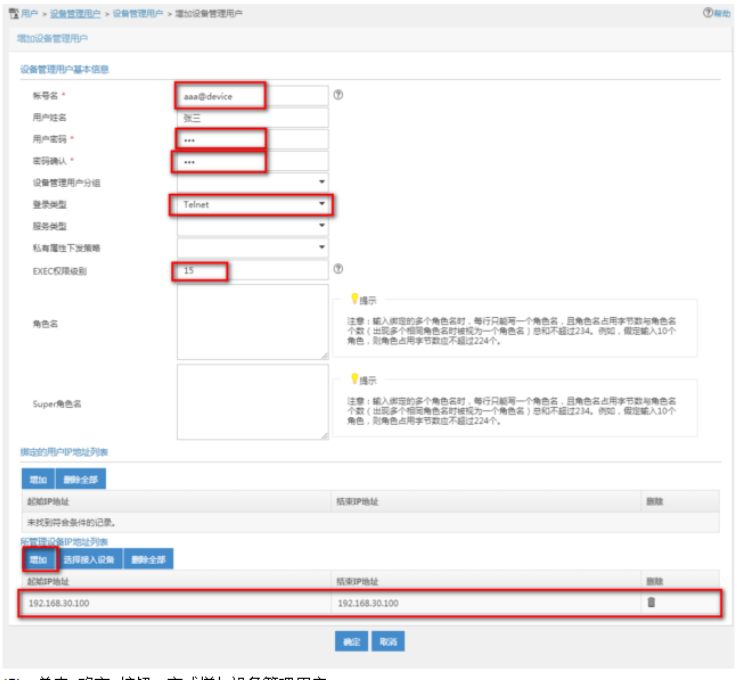
服务类型：选择服务类型，本案例选择 Telnet。

EXEC 权限级别：输入设备管理用户的管理权限等级。不同设备的管理权限等级分级不同，请以设备为准，H3C 设备的管理权限分为0-15 级。

角色名：输入绑定的角色名。该参数表示设备管理用户登录设备后被下发的角色，目前仅H3C部分设备支持。保持为空即可。

所管理设备IP地址列表：单击<增加>按钮，添加所管理设备IP地址列表，设备管理用户只能管理该IP范围内的设备，因此应包含增加接入设备时配置的IP地址。





(5)　单击<确定>按钮，完成增加设备管理用户。

3.1.3 配置接入设备

(1)　#首次登入会出现如下提示，要求输入国家码。需要配置国家码为CN，如选择其他区域可能会造成部分功能无法使用。以下标红色部分为设备自动打印部分。加粗的CN是需要手动输入的国家码。

Press ENTER to get started.

Please set your country/region code.

Input ? to get the country code list, or input q to log out.

CN

(2)　配置用户Telnet 登录时通过scheme 认证。

[H3C]line vty 0 63

[H3C-line-vty0-63]authentication-mode scheme

[H3C-line-vty0-63]quit

(3)　配置RADIUS scheme。IP 地址指向iMC UAM 服务器，监听端口、共享密钥需与iMC 中接入设备的配置保持一致。

[H3C]radius scheme 391

[H3C-radius-391]primary authentication 192.168.1.218 1812

[H3C-radius-391]primary accounting 192.168.1.218 1813

[H3C-radius-391]key authentication 123

[H3C-radius-391]key accounting 123

[H3C-radius-391]nas-ip 192.168.30.100

[H3C-radius-391]server-type extended

[H3C-radius-391]user-name-format with-domain

[H3C-radius-391]quit

(4)　创建domain。

设置用户登录设备时都要经过RADIUS 方案391 的认证/授权/计费。

[H3C]domain device

[H3C-isp-device]authentication login radius-scheme 391

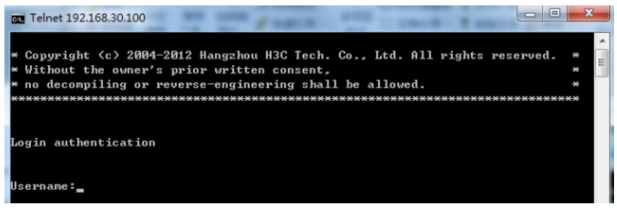
[H3C-isp-device]authorization login radius-scheme 391

[H3C-isp-device]accounting login radius-scheme 391

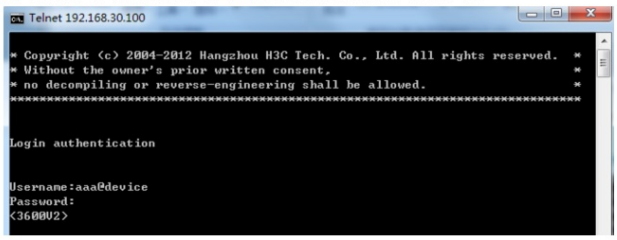
[H3C-isp-device]quit

3.2 登录设备

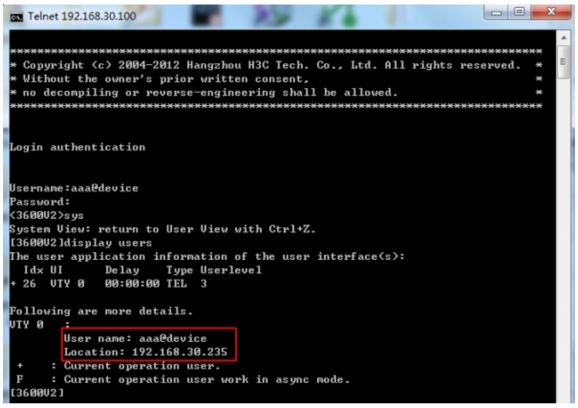
(1)　以Telnet方式登录设备。



(2) 输入用户名和密码，其中用户名与IMC配置的设备管理用户的帐号名保持一致。



(3) 登录成功后，使用display users命令查看用户的详细信息。用户IP地址再绑定的用户IP范围内，用户的权限与IMC中添加的设备管理用户配置一致。



配置关键点

无