iMC 张轩玮 2019-07-29 发表

组网及说明

1 配置需求及说明

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: ad min/admin, HWTACACS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HWTACACS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

HWTACACS服务器IP为10.88.142.178,设备IP地址为10.88.142.102。



配置步骤

- 1.1 配置HWTACACS服务器 (IMC)
- 1.1.1 增加设备
- (1) 选择"用户"页签。
- (2) 单击导航树中的"设备用户策略管理 > 设备管理"菜单项,进入"设备管理"页面

🕞 用户 > 设备用户策略管	理 > 设备管理					📩 加入收藏 ② 帮助
查询设备						
设备IP地址 从			至			
设备区域		2. 6	设备类型		P. (Í
设备名称						查询 重置
增加 批量导入 報	移设备 批量修改 批	星删除 与平台设备同	步 批量导出			
设备名称 ≎	设备IP地址 ▲	设备型号	设备区域	设备类型	详细信息	修改
未找到符合条件的记录						
共有0条记录,当前第	0 - 0 , 第 1/1 页。				« < >	> >> 50 ▼

(3) 单击<增加>按钮,进入"增加设备"页面。

🕞 用户 > 设备用户策略管理 >	设备管理 >	增加设备				②帮助
设备配置						
共享密钥 *			0			
确认共享密钥 *			?			
认证端口 *	49		0			
设备区域			21. 🔟			
设备类型			Ē1 🔟			
单一连接 *	不支持	-				
Watchdog报文 *	不支持	•				
描述						
设备管理						
选择 ▼ 手工増加	全部清除	💡 提示:TAM不支持IP	v6地址。			
设备名称		设备IP地址		设备型号	删除	
未找到符合条件的记录。						
共有0条记录。						
			确定	取消		

(4) 配置设备参数如下:

共享密钥/确认共享密钥:此处的配置必须与设备命令行配置的共享密钥保持一致。本例采用"fine"作为 共享密钥。

认证端口:此处必须与设备命令行配置的端口保持一致。本例采用缺省值 49。其他参数,保持缺省值 。

(5) 配置设备,手工增加:在设备管理区域,单击<手工增加>按钮,在弹出的下拉列表中选择"批量增加"项,弹出手工增加设备窗口。

● 手工増加设备 - Google Chrome					
① 不安全 10.88	.142.178:8080/imc/tam/devmng/manualAddOne.jsf				
手工增加设备					
设备名称类型	FQDN Sysname				
设备名称	获取IP地址				
设备IP地址*	10.88.142.102				
	确定 取消				
]			

(6) 单击<确定>按钮,增加设备成功,返回增加设备页面。

🕞 用户 > 设备用户策略管理	■ > 设备管理 > 増加设备	设备管理 > 增加设备 (?				
设备配置						
共享密钥 *		φ				
确认共享密钥 *		0				
认证端口 *	49	C				
设备区域		2. 6				
设备类型						
单一连接*	不支持	•				
Watchdog报文 *	不支持	•				
描述						
设备管理						
选择 ▼ 手工増加	全部清除 号提示: TAM不支	持IPv6地址。				
设备名称	设备IP地址	设备型号	删除			
	10.88.142.102		â			
共有1条记录。						
		确定 取消				

(7) 单击<确定>按钮,增加设备完毕,进入"增加设备结果"页面。

1.1.2 增加启用认证的授权策略

- (1) 选择"用户"页签。
- (2) 单击导航树中的"设备用户策略管理 > 授权策略管理"菜单项,进入"授权策略管理"页面。
- (3) 单击<增加>按钮,进入"增加授权策略"页面。

➡ 用户 > 设备用户策略管理 > 授权策略管理					
<u> 靖加</u>					
策略名称 ▲	描述	修改	删除		
未找到符合条件的记录。					
共有0条记录。					

(4) 修改"接入授权信息"的缺省记录。点击"修改"图标,弹出"修改接入授权信息"窗口,将"Shell Profile"修改为"使用设备的缺省设置",将"授权命令集"设置为"不限"。

,用户 > 设备用户策略管	理 > 授权策略管理 > 増加授	反策略					?
授权策略信息							
基本信息							
授权策略名 *	test	Ø					
描述							
启用RSA							
接入授权信息							
増加							
设备区域	设备类型	授权时段	Shell Profile	授权命令集	优先级	修改	删除
不限	不限	不限	拒绝	禁止使用		P	
						-	
		确定	取消				

③ 不安全 | 10.88.142.178:8080/imc/tam/authpolicy/addAccessAuthorizeInfo.xhtml

设备区域	不限
设备类型	不限
受权时段	不限
Shell Profile	使用设备的缺省配置
受权命令集	不限

- (5) 单击<确定>按钮,完成修改接入授权信息,返回"增加授权策略"页面。
- (6) 单击<确定>按钮,授权策略增加完毕,可在授权策略列表中查看新增的授权策略。

用户 > 设备用户策略管	『理 > 授权策略管理 > 増加授格	て策略					?
受权策略信息							
基本信息							
授权策略名 *	test	?					
描述							
启用RSA							
接入授权信息							
增加							
设备区域	设备类型	授权时段	Shell Profile	授权命令集	优先级	修改	删除
不限	不限	不限	使用设备的缺省配置	不限		B	
		确定	取消				

设备用户是用户登录设备时使用的帐号,包含帐号名、密码和使用的授权策略等信息。

- (1) 选择"用户"页签。
- (2) 单击导航树中的"设备用户管理 > 所有设备用户"菜单项,进入"所有设备用户"页面。
- (3) 单击<增加>按钮,进入"增加设备用户"页面。
- (4) 输入"帐号名"、"登录密码"和"登录密码确认",并且"用户的授权策略"选择"test",其它参数保留缺
- 省值,本例登录密码为admin。

用户 > 设备用户管理 >	所有设备用户 > 增加设备用户				(? 帮助		
增加设备用户							
帐号名 *	admin	?	用户名				
登录密码 *			登录密码确认 *				
设备用户分组 *	未分组	秝					
分组的授权策略	不支持命令行访问		用户的授权策略	test 👻			
在线数量限制	1		失效日期				
启用权限提升密码	启用权限提升密码						
启用用户密码控制策	使 略						
	的地址为http://iMC主服务器地址:p	ort/imc/noAuth/t	am/login.jsf				
授权主机IP地址列表							
增加 删除全部							
起始IP地址		结束	IP地址	删除			
未找到符合条件的记录。			_				
		确定	取消				

1.2 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 配置用户Telnet 登录时通过scheme 认证。 (2) [H3C]user-interface vty 0 4 [H3C-ui-vty0-4]authentication-mode scheme [H3C-ui-vty0-4]quit (3) 创建HWTACACS方案test。IP 地址指向iMC UAM 服务器,监听端口、共享密钥fine需与iMC 中 接入设备的配置保持一致。 [H3C]hwtacacs scheme test [H3C-hwtacacs-test]primary authentication 10.88.142.178 49 [H3C-hwtacacs-test]primary authorization 10.88.142.178 49 [H3C-hwtacacs-test]primary accounting 10.88.142.178 49 [H3C-hwtacacs-test]key authorization simple fine [H3C-hwtacacs-test]key authentication simple fine [H3C-hwtacacs-test]key accounting simple fine [H3C-hwtacacs-test]user-name-format without-domain [H3C-hwtacacs-test]quit (4) 创建domain。配置域引用的 TACACS 方案。 [H3C] domain testdm [H3C-isp-testdm] authentication login hwtacacs-scheme test [H3C-isp-testdm] authorization login hwtacacs-scheme test [H3C-isp-testdm] accounting login hwtacacs-scheme test [H3C-isp-testdm]quit 配置认证方式。开启 Telnet 开关,认证方式配置为AAA。 (5) [H3C] telnet server enable [H3C] user-interface vty 0 4 [H3C-ui-vty0-4] authentication-mode scheme [H3C-ui-vty0-4] quit (6) 配置默认domain为testdm [H3C]domain default enable testdm 1.3 登录设备

(1) 以Telnet方式登录设备。

授权
login: admin Password:
(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。

授权
login: admin Password:
sbus
<pre><h3c>sys System View: return to User View with Ctrl+Z.</h3c></pre>
[H3C] display users
O AUX 0 00:08:21 Jan 07 08:44:48 1846831
10 VTY 0 00:00:22 Jan 03 06:18:08 392220 TEL + 11 VTY 1 00:00:01 Jan 07 09:05:23 1852355 TEL
Following are more details. AUX 0 :
User name: admin WTV 0
User name: admin Location: 10.88.142.189
VTY 1 :
user name: admin Location: 10.88.142.16
+ : Current operation user.
r . current operation user works in async mode. [H3C]

配置关键点