ADCampus解决方案 网络蝎子精 2019-08-04 发表

可题描述

在ADCampus解决方案里,Leaf设备是作为radius认证的客户端,EIA组件是radius认证的服务器。为 了让终端可以认证成功,需要确保radius客户端和radius服务器的共享密钥一致。但是我们查看Leaf设 备的后台配置可以发现,radius客户端侧配置的共享密钥是密文,无法确保是否和radius服务器端侧配 置一致,如下图所示:

radius session-control enable radius session-control client ip 192.168.10.101 vpn-instance vpn-default key cipher <mark>8c\$3\$1qLi2/p8qxkwwubRfqrgsd5tkHLE12xQ</mark> radius session-control client ip 192.168.10.102 vpn-instance vpn-default key cipher <mark>8c\$3\$m3Lb8nZJEydrObeZo/xadowf+fini5JO</mark>

解决方法

为了查明radius客户端侧配置的共享密钥是否与服务器侧配置一致,有如下方法:

1、首先需要查看radius服务器侧配置的共享密钥。

(1) 在"业务--通用组--设备组"路径下,点击"Leaf设备组"的组策略,如下图所示:

× 🗔 🔺 🛤	设备组 10日18日						95 白龙义动作 ·	✿ 预留VLAN/VALAN ⊑ D	HCP
大黑絋拉									
快速入门	- ? 按示								
Campus#823	(1) 配證为Spine/Leaf/Access角色的记	备、应该只加入到对应角色设备组、不要重复加	1人其他两个很备分组。			and the s			
拓扑	(2)場面を開始を開始、受告対下及進 (3)从組内機能沿路时、会自动下及進歩	1988日1997年:3488日人出5月16人Leaf/Access设备 1988日修復訪作:如果从5pine/Leaf/Access设备	如此用用用可要下及是否和1175年6月18日。 把删除,则同时会清静安全组让将相关配	82814月,二元4484年,安全88 夏,包括私用,二层网络城,安全	2005年1月1日日本自己。1月1日 2013月1日前期日天自己。1	ALBERTS ALBERTS			
近原 >									
<u></u>	■ 自治導入投資及接口 + 増加 C	70105							
a Ria 🕗	=====================================	秋西 0	上級視問 0	東田 0	始而略	的研究表示	4932	旅程	
用户演唱	ACRIME	盛水管理	自定义权器	系统教念文	45-		8		
安全坦	Les f 2 备组	≦ ±₩	自由公務器	新纳税盘义	4)- <mark>(</mark> 3)	₹.	B		
接入坦	Spinei2698	≦ ±₩	自由公務器	系统数盘文	85-		B		
Underlay	Access设备组	≦ ™ <u>≋</u>	自由父親問	新纳税盘义	45-	₹.	B		
Overlay	具有4条记录,当新第1-4,第1/1元。							« < 1 > » 50	•
业与律数									

(2) 在弹框中点击"AAA认证配置"的"动作参数配置",如下图所示:

名称	描述	动作参数配置	可恢复	修改	删除
▼leaf				Ø	Ē
AAA认证配置	全局使能AAA认证,城名及认证服务器等相关配置	IFo,	是		
使能DHCP Snooping	全局使能DHCP Snooping	_	是		
有线MAC Portal Free ACL3001	配置有线设备ACL3001,配置MAC Portal认证相关规则。	II.,	是		
802.1X配置	全局使能802.1X	ilo,	是		
使能MAC认证	全局使能MAC认证		是		
开启MAC迁移	开启允许MAC迁移功能		是		

(3) 此时可以发现radius服务器侧配置的密码为"admin",如下图所示:

)不安全 99.1.1.	123:8080/imc/campus/ipc/iccA	ctionDeviceAAAEnab
默认域名 *	campus	~
密码 *	admin	
服务器IP *	192.168.10.101	
备份服务器IP	192.168.10.102	
计费失败选项		
计费更新间隔 (分钟	•)	
	关闭	

2、需要查明radius客户端侧配置的共享密钥。

(1) 在"业务--接入组"路径下,点击"业务参数配置",如下图所示:

I	* 🗔 🔺 👊	Q-14人把管理	AB MERNER	● LDAPARS管理・ □ LAERSNAD · □ HASH	5 HARATE - 18 5	
e	の 大麻道地					
ć	N READ	Mitton Relief				
ŧ	Campusters	遠入網名 ©	师连	副秀而殿 0	63	田府
6	\$ 拓扑	bypd20190618160145			B	0
Ľ	• 迎愿 >	ceshi			B	
4	₽ <mark>₩8</mark>	政府推入组			8	8
	通用油	学生输入组			2	8
	甩戶策略	防衛相称入損			B	8
	安全相					
	isadin 🕗					
1	Underlay					
	Overlay					
	10.000					

(2) 点击"业务参数配置"页面下的"系统配置",如下图所示:

📑 业务参数配置

业务参数配置	
对保证线入业务正常运行 管:系统强强 管: 年時强强 管: 车户端开级 E: 智能参加客户端开级 E: 智能参加客户端开级 E: 智能参加客户端开级 E: 智能参加客户端开级 E: 智能参加客户端开级	5的参数进行配置,包括系统配置、证书配置、客户满升级配置和单点管录配置等。 对保证接入业务正常运行的参数进行配置。 证书配置主要是对根证书、医务器证书、证书用特列表等进行配置。 客户端升级配置可以管理各个用户分组或用户使用的INode客户满版本和配置。 智能终满客户满升级配置。 对单点登录的几种整合方式进行配置。 点击该链接使修改后的业务参数配置立即主效。

(3) 在"系统配置"弹框中点击"系统参数配置"的"配置",如下图所示:

2. 业务参数配置		
系統配置		
模板名称	描述	配置
系统参数配置	系统是供业务相关的常用参数信息	Ø ₀
策略服务器参数配置	策略服务器及安全管理相关的参数信息	¢,
终端管理参数配置	终端管理的相关配置	0 ₀
终端老化策略配置	终端老化策略的相关配置	0 ₀
UAM运行日志参数配置	配置系统运行环境相关参数	0 ₀
用户密码控制策略配置	配置用户密码的控制策略	¢ _o
帐号自动销户任务	系统根据各个参数的设置情况,为帐号进行自动销户处理。	¢0
无线定位参数配置	配置无线定位的相关参数	¢ _o
用户通知参数配置	用户通知相关的参数信息	Ф ₀
客户端防破解配置	配置客户端管理中心	¢ _o
代理服务器检测参数	iNode客户端检测主机是否启用代理服务器的参数	O 0
用户绑定信息配置	配置用户绑定信息的自学习数量	¢ _o
预生成用户策略配置	预生成用户策略的相关配置	¢ _o

(4) 在弹框的"用户数据管理参数"一栏中,点击下拉"密钥显示方式",选择"明文(显示实际的密钥)"

,然后点击"确定"。(待后面查完radius客户端侧的共享密钥,需将该参数改为"密文(显示为******)"

) 如下图所示:

用戶數諸官理參數					
Syslog服务器(P		0	发送认证失败日志Syslog	否 •	0
UAM业务分权	允许 🔻	. (1)	接入明细保得时长(天)*	180	•
注销用户保留时长(天)*	1	0	日志保留时长(天) *	180	۲
启用IPv6	æ •	. (1)	发送继入用户认证队列满告警	* *	۲
告誓服务職IP		0	告營服务職演口	162	(?)
远程桌面连接等待时长(分钟)*	5	0	远程桌面密码输入方	各户資 *	۲
显示TopN用户分组 *	10	0	iMC配置台端口 *	8080	۲
按用户分组申请服务	禁用 ▼	• ③	按用户分组申请服务立即生效	禁用 *	0
接入帐号强制绑定IP地址和接入组	禁用 🔻	• ③	注销在线用户使用的服务	禁止 🔻	3
报修单保留时长(天)*	30	0	IP地址重复性检查	禁用 ▼	۲
MAC地址重复性检查	禁用 ▼	. (9)	MAC地址一致性检查	禁用 ▼	0
數据库异常时自动逃生	禁用 🔻				
每日短信获取密码次数(次)			按加入时长解除黑名单		
支持百万级用户	禁用 ▼				
密期显示方式	明文(显示实际的图	9月)	• 0		

(5) 在"业务--接入组"路径下,下拉并点击"认证点设备配置",如下图所示:

🕴 第三方认证配置	😢 LDAP	业务管理▼	圮 认证设备	配置 ▼	12 接入策略	▶️ 接入条件管理 ▼	🐮 业务参数配置
		UDD 认证点 II Portali	设备配置 设备配置				
		Le rortan					

(6) 在"认证点设备配置"弹框中,勾选相应的认证点设备(即radius客户端),然后点击"修改",如下图所示:

72 认证点设备配置						17 i	人证点设备管理 ▼
认证点设备查询							高级查询
设备IP地址 从 设备名称			至 认证点没备 类型			•	查询 重置
2 増加 删除 修改	【 ▼更多 刷新						同缺省配置
✓ 设备名称	设备IP地址	设备型号	设备角色	接入位置分组	备注	详细信息	操作
Leaf-19	192.168.10.4	H3C S5560X-30C-EI	Leaf			Eq.	
共有1条记录,当前:	第1 - 1 , 第 1/1 页。				« <	1 >	» 50 •

(7) 在"修改认证点设备"页面下,我们就可以看到radius客户端侧的共享密钥为"admin",如下图所示:

、配置			
认证;;;] *	1812	计费端口 * 18	13
业务类型	LAN接入业务		
认证点设备类型	H3C (General)	接入位置分组 无	•
认证点设备类型 共享密钥 *	H3C (General)	接入位置分组 无	•
认证点设备 类型 共享密钥 *	H3C (General) admin	接入位置分组 无	•
认证点设备类型 共享密钥 * 备列表	H3C (General)	接入位置分组 无	•
 认证点设备类型 共享密钥 * 备列表 投替名称 	H3C (General)	接入 位置 分组 无 设新型号	「

3、如果radius服务器侧和客户端侧的共享密钥不一致,需要修改客户端侧的共享密钥。 至此,我们就可以明确radius客户端和radius服务器的共享密钥是否配置一致了。