

知 ADCampus解决方案如何查看共享密钥是否一致？

ADCampus解决方案 网络蝎子精 2019-08-04 发表

问题描述

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 $c$$$1qLi2/p8qkwwubRfgrgsd5tkHLE12xQ  
radius session-control client ip 192.168.10.102 vpn-instance vpn-default key cipher $c$$$3m3Lb8nZ7Evd10be2o/xadpwf+f1ni5T0
```

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。

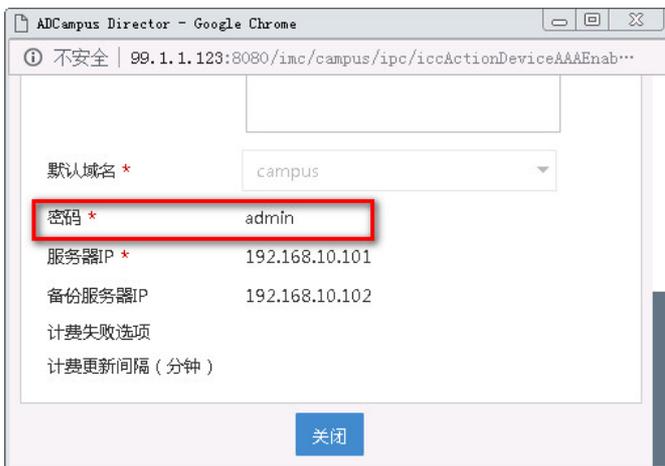
(1) 在“业务--通用组--设备组”路径下，点击“Leaf设备组”的组策略，如下图所示：



(2) 在弹框中点击“AAA认证配置”的“动作参数配置”，如下图所示：

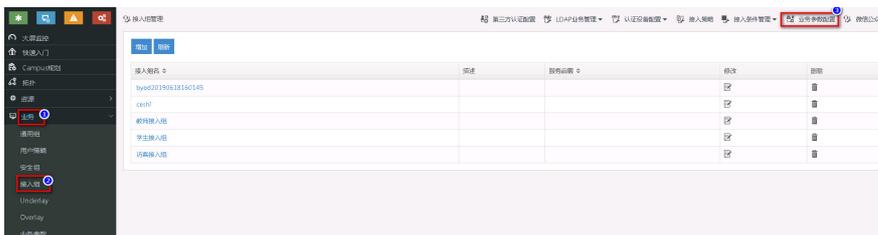
名称	描述	动作参数配置	可恢复	修改	删除
leaf					
AAA认证配置	全局使能AAA认证，域名及认证服务器等相关配置	是	是		
使能DHCP Snooping	全局使能DHCP Snooping	是	是		
有线MAC Portal Free ACL3001	配置有线设备ACL3001，配置MAC Portal认证相关规则。	是	是		
802.1X配置	全局使能802.1X	是	是		
使能MAC认证	全局使能MAC认证	是	是		
开启MAC迁移	开启允许MAC迁移功能	是	是		

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

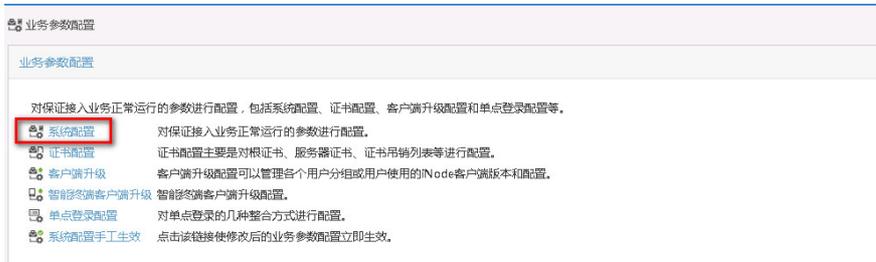


2、需要查明radius客户端侧配置的共享密钥。

(1) 在“业务--接入组”路径下，点击“业务参数配置”，如下图所示：



(2) 点击“业务参数配置”页面下的“系统配置”，如下图所示：



(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：



(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：



(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：



(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：

认证点设备配置 认证点设备管理

认证点设备查询 高级查询

设备IP地址从 至

设备名称 认证点设备类型

缺省配置

<input checked="" type="checkbox"/>	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
<input checked="" type="checkbox"/>	Leaf-19	192.168.10.4	H3C S5560X-30C-EI	Leaf				...

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：

修改认证点设备

接入配置

认证端口 * 计费端口 *

业务类型

认证点设备类型 接入位置分组

共享密钥 *

设备列表

设备名称	设备IP地址	设备型号	备注
Leaf-19	192.168.10.4	H3C S5560X-30C-EI	

共有1条记录。

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。