某局点S5048V5-EI设备配置802.1x认证结合锐捷服务器RG-SAM系统不能主动将认证账户踢下线

802.1X 刘倩 2023-01-29 发表

组网及说明

组网不涉及

告警信息

告警不涉及

问题描述

客户使用5048PV5-EI设备结合锐捷的radius服务器RG-SAM对接做802.1x认证，现在可以通过有线SA客户端认证，但RG-SAM系统不能把认证账户踢下线。

过程分析

在radius服务器上主动将认证客户端踢下线需要服务器发送DM报文，DM（Disconnect Message）是指用户下线报文，即由RADIUS服务器主动发起的强制用户下线的报文。

1. 管理员在RADIUS服务器上强制用户下线，RADIUS服务器向设备发送DM-Request报文，请求用户下线。
2. 设备收到DM-Request报文后，与设备上的用户信息匹配来识别用户。如果匹配成功，则通知用户下线；如果匹配失败，则用户保持在线。
3. 设备回应DM-ACK/NAK报文。

- 如果用户成功下线，设备给RADIUS服务器回应DM-ACK报文。
- 如果用户未下线，设备给RADIUS服务器回应DM-NAK报文。

抓包来看，认证点收到DM请求报文后，没有回复ACK报文。现网没有配置DAE功能，不支持处理DM报文，导致无法主动踢掉认证账户

解决方法

需要开启DAE功能。DAE（Dynamic Authorization Extensions，动态授权扩展）协议是RFC 5176中定义的RADIUS协议的一个扩展，它用于强制认证用户下线，或者更改在线用户授权信息。DAE采用客户端/服务器通信模式，由DAE客户端和DAE服务器组成。

· DAE客户端：用于发起DAE请求，通常驻留在一个RADIUS服务器上，也可以为一个单独的实体。

· DAE服务器：用于接收并响应DAE客户端的DAE请求，通常为一个NAS（Network Access Server，网络接入服务器）设备。

DAE报文包括以下两种类型：

· DMs（Disconnect Messages）：用于强制用户下线。DAE客户端通过向NAS设备发送DM请求报文，请求NAS设备按照指定的匹配条件强制用户下线。

· COA（Change of Authorization）Messages：用于更改用户授权信息。DAE客户端通过向NAS设备发送COA请求报文，请求NAS设备按照指定的匹配条件更改用户授权信息。

在设备上开启RADIUS DAE服务后，设备将作为RADIUS DAE服务器在指定的UDP端口监听指定的RADIUS DAE客户端发送的DAE请求消息，然后根据请求消息进行用户授权信息的修改、断开用户连接、关闭/重启用户接入端口或重认证用户，并向RADIUS DAE客户端发送DAE应答消息。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 开启RADIUS DAE服务，并进入RADIUS DAE服务器视图。

radius dynamic-author server

缺省情况下，RADIUS DAE服务处于关闭状态。

(3) 指定RADIUS DAE客户端。

client { **ip** *ipv4-address* | **ipv6** *ipv6-address* } [**key** { **cipher** | **simple** } *string* | **vendor-id** 2011 **version** { 1.0 | 1.1 } | **vpn-instance** *vpn-instance-name*] *

缺省情况下，未指定RADIUS DAE客户端。

(4) （可选）指定RADIUS DAE服务端口。

port *port-number*

缺省情况下，RADIUS DAE服务端口为3799。