海外局点云AP无法被云简纳管问题

绿洲平台 AP管理 谭奇伟 2024-01-16 发表

组网及说明

某海外局点，云AP —— 第三方中间设备 —— 第三方路由器 —— 公网

告警信息

无

问题描述

云AP无法被云简纳管，云AP正确进行了相关配置，云AP上设置的dns能够正确解析国际云的地址，且能ping通该地址，

注意：海外的AC和AP无法直接ping通公有云的域名（禁ping），但允许ping通公有云的IP地址。

现场反馈云AP和公网之间的设备没有FW或者阻塞云简地址或19443/443端口的设备。

过程分析

1. 在AC上通过：display dns host查看云AP上正确解析了国际云的IP地址，并有相关记录，

2. 通过display cloud-management state和dis sys int cloud-management state 查看AP和云简的状态是未连接

display system internal cloud-management state
Device module name : PROBE
Cloud module name : probeclient
Connection state : Disconnected
Module URL : N/A
Connected at : N/A
Duration : 00d 00h 00m 00s
Process state : N/A
Failure reason : N/A
Last down reason : N/A
Last down at : N/A
Last report failure reason : N/A
Last report failure at : N/A
Dropped packets after reaching buffer limit : 0
Total dropped packets : 0
Last report incomplete reason : N/A
Last report incomplete at : N/A
Buffer full count : 0

3. debug cloud-management all，查看云AP和云简建立云管道的过程：

<FLEC-KYUSYUGB-AP14>*Jan 11 18:11:22:208 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/EVENT: Successfully sent an asynchronous query request to DNS, domain name is cloudnet.h3c.com.
*Jan 11 18:11:22:243 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/EVENT: DNS parsed domain name successfully in Idle state: IP address=52.163.242.100.
*Jan 11 18:11:22:244 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/EVENT: CM tunnel state changed from Idle to Connecting.
*Jan 11 18:11:22:341 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/EVENT: TCP connected.
*Jan 11 18:11:22:342 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/EVENT: Initialized SSL.
*Jan 11 18:11:22:342 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/EVENT: SSL connection result: 2.
*Jan 11 18:11:22:342 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/EVENT: SSL connection: error: 00000000:lib(0):func(0):reason(0).
*Jan 11 18:11:22:343 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/EVENT: SSL connection (read) was not completed.
*Jan 11 18:11:22:343 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/EVENT: SSL state changed from Init to Connecting.
*Jan 11 18:11:22:343 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/TIMER: Created ssl reconnect timer 0, which will expire in 30 seconds.
*Jan 11 18:11:22:361 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/ERROR: Socket connection error: error code=104, error message=Connection reset by peer.
*Jan 11 18:11:22:361 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/EVENT: TCP connection closed because TCP callback process failed.
*Jan 11 18:11:22:363 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/TIMER: Deleted ssl reconnect ti

mer 0.
*Jan 11 18:11:22:364 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/TIMER: Deleted request Get Version info timer test.
*Jan 11 18:11:22:364 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/TIMER: Created global connection timer 0, which will expire in 10 seconds.
*Jan 11 18:11:32:408 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/EVENT: Successfully sent an asynchronous query request to DNS, domain name is cloudnet.h3c.com.
*Jan 11 18:11:32:432 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/EVENT: DNS parsed domain name successfully in Idle state: IP address=52.163.242.100.
*Jan 11 18:11:32:433 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/EVENT: CM tunnel state changed from Idle to Connecting.
*Jan 11 18:11:32:530 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/EVENT: TCP connected.
*Jan 11 18:11:32:531 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/EVENT: Initialized SSL.
*Jan 11 18:11:32:532 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/EVENT: SSL connection result: 2.
*Jan 11 18:11:32:532 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/EVENT: SSL connection: error: 00000000:lib(0):func(0):reason(0).
*Jan 11 18:11:32:532 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/EVENT: SSL connection (read) was not completed.
*Jan 11 18:11:32:532 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/EVENT: SSL state changed from Init to Connecting.
*Jan 11 18:11:32:532 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/TIMER: Created ssl reconnect timer 0, which will expire in 30 seconds.
*Jan 11 18:11:32:552 2024 FLEC-KYUSYUGB-AP14 CMTNLMGR/7/ERROR: Socket connection error: error code=104, error message=Connection reset by peer.
通过debug发现，AP尝试和云简建立TCP连接，但是连接最后被对端reset了（connection reset by peer），怀疑是云简侧的服务器reset了连接。

4. 随即联系云简侧协助排查：但云简侧根据AP的SN查询发现并没有该设备向云简发起连接建立的请求到达云简侧，同时在AP上，在AP与云简尝试建立云管道的过程中通过：dis tcp查询是否有tcp会话建立，发现一直也没有，说明AP与云简的tcp连接一直没有建立起来，但是AP的debug显示AP确实发出了请求，但是对端设备（peer）reset了这个请求，但是云简服务器却没有收到AP的tcp报文，那么这个对端设备（peer）到底是谁?

5. 尝试给AP从19443端口更换为443端口后，AP再次发起了建立云管道的请求，此时云简侧发现有一个AP的tcp建立请求到达了国际云服务器，但后续的TCP再也没有收到了，AP上查看dis tcp发现有短暂的用443端口和云简服务器建立tcp连接的过程，后续就没有了，这说明可能是中间设备或者海外运营商堵塞了443或者19443端口，更换为443端口后由于是首次AP与服务器建立会话因此没有被拦截，而该会话被中间设备监听后进行了拦截。

6. 让云AP直接绕过现场设备，直接连接公网，发现成功与云简建立的云管道，这说明就是存在中间设备拦截了19443和443端口的云AP和云简服务器之间的会话导致云管道无法建立。

解决方法

排查和放通中间设备的443和19443端口。