某局点 S5130S-52S-HI 替换v5设备dot1x认证不通过经验案例

802.1X 关萌 2017-07-26 发表

用户使用我司S5130S-52S-HI替换v5一台交换机，替换后dot1x无法正常认证通过，用户认证时刚上线就会下线。用户的配置是使用v5设备的配置信息，收集了配置和调试信息进行分析。

用户反馈的debug信息如下，对用户收集的调试信息进行详细分析，发现用户收集的调试信息中，认证流程是正常的，有如下提示

*Jan 1 01:56:16:466 2013 H3C RADIUS/7/EVENT:
Reply SocketFd recieved EPOLLIN event.
*Jan 1 01:56:16:466 2013 H3C RADIUS/7/EVENT:
Received reply packet succuessfully.
*Jan 1 01:56:16:466 2013 H3C RADIUS/7/EVENT:
Found request context, dstIP: 198.1.1.98, dstPort: 1812, VPN instance: --(public), socketFd: 66, pktID: 209.
*Jan 1 01:56:16:467 2013 H3C RADIUS/7/EVENT:
The reply packet is valid.
*Jan 1 01:56:16:467 2013 H3C RADIUS/7/EVENT:
Decoded reply packet successfully.
*Jan 1 01:56:16:467 2013 H3C RADIUS/7/PACKET:
User-Name="\006\007aGFbHBlRNXMqTUljQN4eiyKJmQ= xxx"
Service-Type=Framed-User
State=0x474e385844784338
Termination-Action=Default
Session-Timeout=86401
Acct-Interim-Interval=1200
H3c-Server-String=[]
EAP-Message=0x03020004
Message-Authenticator=0x4d73cfd34e3bf578aa9a6272e430d313
*Jan 1 01:56:16:470 2013 H3C RADIUS/7/PACKET:
02 d1 00 bf a5 f4 fa c9 de a8 20 bf 0e 5b 66 01
80 36 b1 13 01 2a 06 07 61 47 46 62 48 42 6c 52
4e 58 4d 71 54 55 6c 6a 4a 51 4e 34 65 69 79 4b
4a 6d 51 3d 20 20 6d 61 69 6e 6f 66 66 69 06 06
00 00 00 02 18 0a 47 4e 38 58 44 78 43 38 1d 06
00 00 00 00 1b 06 00 01 51 81 55 06 00 00 04 b0
1a 47 00 00 63 a2 3d 41 36 06 00 00 00 00 37 06
00 00 00 00 38 06 00 00 00 00 3a 06 00 00 00 00
42 06 00 00 00 00 4a 06 00 00 00 00 43 11 56 37
30 30 52 30 30 33 42 30 33 44 30 30 34 3d 0a 47
4e 38 58 44 78 43 38 4f 06 03 02 00 04 50 12 4d
73 cf d3 4e 3b f5 78 aa 9a 62 72 e4 30 d3 13
*Jan 1 01:56:16:470 2013 H3C RADIUS/7/EVENT:
PAM_RADIUS: Processing RADIUS authentication.
%Jan 1 01:56:16:472 2013 H3C DOT1X/6/DOT1X_LOGIN_SUCC: -IfName=GigabitEthernet1/0/16-MACAddr=0023-245f-3b24-VLANID=508-Username=mainoffi; User passed 802.1X authentication and came online.
*Jan 1 01:56:16:470 2013 H3C RADIUS/7/EVENT:
PAM_RADIUS: Fetched authentication reply-data successfully, resultCode: 0
*Jan 1 01:56:16:471 2013 H3C DOT1X/7/PACKET:
Transmitted a packet on interface GigabitEthernet1/0/16.
Destination Mac Address=0023-245f-3b24
Source Mac Address=1cab-34a7-cc73
VLAN ID=508
Mac Frame Type=888e
Protocol Version ID=1
Packet Type=0
Packet Length=69
-----Packet Body-----
Code=10
Identifier=2

Length=17664
*Jan 1 01:56:16:471 2013 H3C DOT1X/7/EVENT: Sent server string notification packet: UserMAC=0
023-245f-3b24, VLANID=508, Interface=GigabitEthernet1/0/16.
*Jan 1 01:56:16:471 2013 H3C DOT1X/7/EVENT: Received authentication response with code 0: Us
erMAC=0023-245f-3b24, VLANID=508, Interface=GigabitEthernet1/0/16.
*Jan 1 01:56:16:472 2013 H3C DOT1X/7/EVENT: BE is in Success state: UserMAC=0023-245f-3b2
4, VLANID=508, Interface=GigabitEthernet1/0/16.
*Jan 1 01:56:16:473 2013 H3C PORTSEC/7/EVENT: Received an authentication success message f
rom user: AuthenType=2, UserMAC=0023-245f-3b24, VLANID=508,
Interface=GigabitEthernet1/0/16.
*Jan 1 01:56:16:473 2013 H3C DOT1X/7/PACKET:
Transmitted a packet on interface GigabitEthernet1/0/16.
Destination Mac Address=0023-245f-3b24
Source Mac Address=1cab-34a7-cc73
VLAN ID=508
Mac Frame Type=888e
Protocol Version ID=1
Packet Type=0
Packet Length=4
-----Packet Body-----
Code=3
Identifier=2
Length=1024
*Jan 1 01:56:16:474 2013 H3C DOT1X/7/EVENT: PAE is in Authenticated state: UserMAC=0023-24
5f-3b24, VLANID=508, Interface=GigabitEthernet1/0/16.
*Jan 1 01:56:16:474 2013 H3C DOT1X/7/EVENT: Sent authorization request: UserMAC=0023-245f-
3b24, VLANID=508, Interface=GigabitEthernet1/0/16.
*Jan 1 01:56:16:475 2013 H3C DOT1X/7/EVENT: AAA processed authorization request: Result= Fail
ure, UserMAC=0023-245f-3b24, VLANID=508, Interface=GigabitEthernet1/0/16.
*Jan 1 01:56:16:476 2013 H3C RADIUS/7/EVENT:
Sent reply message successfully.
*Jan 1 01:56:16:476 2013 H3C DOT1X/7/PACKET:
Transmitted a packet on interface GigabitEthernet1/0/16.
Destination Mac Address=0023-245f-3b24
Source Mac Address=1cab-34a7-cc73
VLAN ID=508
Mac Frame Type=888e
Protocol Version ID=1
Packet Type=0
Packet Length=4
-----Packet Body-----
Code=4
Identifier=2
Length=1024
*Jan 1 01:56:16:477 2013 H3C DOT1X/7/EVENT: PAE is in Aborting state: UserMAC=0023-245f-3b
24, VLANID=508, Interface=GigabitEthernet1/0/16.
*Jan 1 01:56:16:477 2013 H3C DOT1X/7/EVENT: BE is in Initialize state: UserMAC=0023-245f-3b24
, VLANID=508, Interface=GigabitEthernet1/0/16.
*Jan 1 01:56:16:477 2013 H3C DOT1X/7/EVENT: PAE is in Disconnect state: UserMAC=0023-245f-
3b24, VLANID=508, Interface=GigabitEthernet1/0/16.
*Jan 1 01:56:16:478 2013 H3C DOT1X/7/EVENT: BE is in Idle state: UserMAC=0023-245f-3b24, VL
ANID=508, Interface=GigabitEthernet1/0/16.
%Jan 1 01:56:16:478 2013 H3C DOT1X/6/DOT1X_LOGOFF: -IfName=GigabitEthernet1/0/16-MACA
ddr=0023-245f-3b24-VLANID=508-Username=mainoffi-ErrCode=0; 802.1X user was logged off.
*Jan 1 01:56:16:478 2013 H3C DOT1X/7/EVENT: Interface GigabitEthernet1/0/16 received Set the p
ort authorization status to unauthorized event.
*Jan 1 01:56:16:479 2013 H3C PORTSEC/7/EVENT: Received a session-end message from user: A
uthenType=2, UserMAC=0023-245f-3b24, VLANID=508, Interface=GigabitEthernet1/0/16.
*Jan 1 01:56:16:479 2013 H3C PORTSEC/7/EVENT: Processing session-end message and attempti
ng to release the session: AuthenType=2, UserMAC=0023-245f-3b24, VLANID=508,
Interface=GigabitEthernet1/0/16.
*Jan 1 01:56:16:480 2013 H3C PORTSEC/7/EVENT: 802.1X [0023-245f-3b24:VLAN508:GE1/0/16]
Processing session-end msg, and attempt to free the session.
*Jan 1 01:56:16:481 2013 H3C PORTSEC/7/EVENT: Session deleted: UserMAC=0023-245f-3b24, V

LANID=508, Interface=GigabitEthernet1/0/16.

对用户反馈过来了调试信息分析过程如下。从调试信息中筛选到如下关键信息
*Jan 1 01:56:16:473 2013 BOTS_N_BGL_F5_5130-A PORTSEC/7/EVENT: Received an authenticat ion success message from user: AuthenType=2, UserMAC=0023-245f-3b24, VLANID=508, Interface =GigabitEthernet1/0/16.
从以上信息可以看出，用户dot1x认证已经通过了radius认证，应该可以正常上线，说明认证之前是没问题的。继续分析debug信息，发现信息中有授权失败的提示信息。
*Jan 1 01:56:16:474 2013 BOTS_N_BGL_F5_5130-A DOT1X/7/EVENT: Sent authorization request: UserMAC=0023-245f-3b24, VLANID=508, Interface=GigabitEthernet1/0/16.
*Jan 1 01:56:16:475 2013 BOTS_N_BGL_F5_5130-A DOT1X/7/EVENT: AAA processed authorization request: Result= Failure, UserMAC=0023-245f-3b24, VLANID=508, Interface=GigabitEt hernet1/0/16.
从以上信息可以看出应该是授权过程中出了问题。进一步检查配置，发现用户在domain域下没有配置授权指向AAA服务器，配置如下：
#
domain h3c
 authentication lan-access radius-scheme h3c
 accounting lan-access radius-scheme h3c
#
查看v5配置如下，确实没有授权配置
#
domain h3c
 authentication radius-scheme h3c
 accounting radius-scheme h3c
domain system
#

在domain域中下发授权使用AAA方案后测试，问题解决
#
domain h3c
 authentication lan-access radius-scheme h3c
 authorization lan-access radius-scheme h3c
 accounting lan-access radius-scheme h3c
#

在使用v7设备做802.1x认证时需要配置授权服务器。当设备替换时，如果不仅仅需要做配置翻译，还要对新设备的配置手册进行确认，是否有些必配项需要配置