Experience case of S5500-EI DOT1X authentication failure

Switches 孟普 2020-08-21 Published

Network Topology

A client reported an iNode dot1x dial exception.The specific phenomenon is that you can go online successfully, but it will automatically go offline after 1 to 2 minutes

Configuration Steps

1. By analyzing the configuration of IMC, the server is used to issue security ACL to each user. During the issue of security ACL, an exception occurs, which can be seen from device debug.

```
*May 17 13:46:42:939 2000 N-12F-SW-S5500-52C-EI PORTAL/7/PORTAL_DEBUG: Processing SET_POLICY user index 71 IP 10.2.33.11, add new ACL rule failed!
*May 17 13:46:42:949 2000 N-12F-SW-S5500-52C-EI RDS/7/DEBUG: Send attribute list:
*May 17 13:46:42:950 2000 N-12F-SW-S5500-52C-EI RDS/7/DEBUG:
[H3C-26 Connect_ID             ] [6 ] [290817]
[H3C-20 Command                ] [6 ] [4]
[H3C-24 Control_Identifier     ] [6 ] [1]
[H3C-25 Result_Code            ] [6 ] [1]
[44 Acct-Session-Id            ] [18] [1000417134631010]
*May 17 13:46:42:951 2000 N-12F-SW-S5500-52C-EI RDS/7/DEBUG: Send:IP=[10.2.2.1],PortNum=[9033],UserIndex=[71],ID=[207],Code=[20],Length=[68]
*May 17 13:46:42:952 2000 N-12F-SW-S5500-52C-EI RDS/7/DEBUG:
 14 cf 00 44 b9 96 e9 01 8f b2 5c af 2b 7e b1 77
 b5 15 b8 a7 2c 12 31 30 30 30 34 31 37 31 33 34
 36 33 31 30 31 30 1a 1e 00 00 07 db 1a 06 00 04
 70 01 14 06 00 00 00 04 18 06 00 00 00 01 19 06
 00 00 00 01
```

Of course, there is also a corresponding process on IMC:

```
2017-05-18 16:56:30 [策略服务器] [调试 (0)] [50] [AclDatagramManager::sendACLToGeneralDevice]
The ACL update control response message was received from 10.2.253.12.1812
Acct-Session-Id       (44): [str] [1000417134631010]
Command            (HW-20): [int] [4]
Connect_Id         (HW-26): [int] [290817]
Control_Identifier (HW-24): [int] [1]
Result_Code        (HW-25): [int] [1]
2017-05-18 16:56:30 [策略服务器] [错误 (141348)] [50]
[AclDatagramManager::sendACLToGeneralDevice] There was an error in the ACL update control response received from 10.2.253.12:1812
2017-05-18 16:56:30 [策略服务器] [错误 (141561)] [50] [AsyncUserEventProcessor::openAccess] 用户"OnlineUser<nxxzx07@gxgt, 10.2.33.11, null, 9C:EB:E8:08:BD:61, MF17mEAh>" The ACL security permission failed to open
```

IMC sends the security ACL to the switch through session Control message, which can be seen from the debug information.

When a message is sent, the switch can receive and also reply a response message. However, there is an attribute "[h3c-25 Result_Code] [6] [1]" in the response message. Since the value of this attribute is 1, the server determines that the response message is abnormal. The result is that the security ACL fails to be issued and the client goes offline. The IMC side confirms that the normal value of this property is 0.

2、 Check the printing information on the equipment:

```
%May 17 13:46:26:239 2000 N-12F-SW-S5500-52C-EI PORTAL/4/PORTAL_ACL_FAILURE: The input parameters are wrong。
```

It can be seen from the printing information that there is a problem with the configuration of ACL. By looking at the ACL configured by the customer on the device, we found that there was a rule matching the source. The security ACL does not allow the configuration of the matching source:

```
acl number 3002
description securityacl
```

```
rule 0 deny tcp destination-port eq telnet
rule 1 permit ip source 10.2.31.0 0.0.0.255
rule 3 deny tcp destination-port eq 445
rule 5 permit ip
```

After modifying the security ACL on the spot, the problem still exists, and the debug information is collected again to continue the analysis.

2、According to the new debug information, there is no input parameter error, but the session-control message received is invalid.You can see that the user went online first and then went offline because sessctrl is invalid.

```
%May 26 08:38:13:827 2000 N-12F-SW-S5500-52C-EI PORTAL/5/PORTAL_USER_LOGON_SUCCESS: -UserName=[bzRbTklRYHQtGEkxdAMtfTlAXtI=  nxxzx06@gxgt]-IPAddr=[10.2.33.13]-IfName=[Vlan-interface25]-VlanID=[25]-MACAddr=[3c97-0ee6-5272]; User got online successfully.
*May 26 08:39:20:326 2000 N-12F-SW-S5500-52C-EI RDS/7/DEBUG:  Recv invalid sessctrl packet, drop it!Slot=0, SessSlot=1
%May 26 08:39:36:491 2000 N-12F-SW-S5500-52C-EI PORTAL/5/PORTAL_USER_LOGOFF: -UserName=[bzRbTklRYHQtGEkxdAMtfTlAXtI=  nxxzx06@gxgt]-IPAddr=[10.2.33.13]-IfName=[Vlan-interface25]-VlanID=[25]-MACAddr=[3c97-0ee6-5272]-Reason=[User Request]; User logged off.
*May 26 08:39:36:493 2000 N-12F-SW-S5500-52C-EI PORTAL/7/PORTAL_DEBUG:
Portal receive packet length:44
  Portal check packet OK
  Portal packet head:
   Type:5   SN:53015 ReqId:0    AttrNum:2  ErrCode:0  UserIP:10.2.33.13
```

Check the contents of the Session-control message and find that the connect-ID of the received message is inconsistent with the connect-ID of the actual accounting message.

Connect-id attribute value in session-Control message:

```
*May 26 08:38:19:867 2000 N-12F-SW-S5500-52C-EI RDS/7/DEBUG: Recv MSG,[MsgType=Session ctrl pkt Index = 80, ulParam3=133526112]
*May 26 08:38:19:869 2000 N-12F-SW-S5500-52C-EI RDS/7/DEBUG: Received raw session-control packet(from: 10.2.2.1 ) is:
*May 26 08:38:19:870 2000 N-12F-SW-S5500-52C-EI RDS/7/DEBUG:
 14 f2 00 50 be 94 4e f6 49 60 b0 52 08 2c 7a b2
 68 ce 3e ba
 2c 12 31 30 30 30 34 32 36 30 38 33 38 33 38 30
 31 30
 0b 06 33 30 30 32
 1a 0c 00 00 07 db 14 06 00 00 00 03
1a 0c 00 00 07 db 1a 06 00 00 00 00
         1a 0c 00 00 07 db 18 06 00 00 00 01
```

Connect-id attribute value of accounting message:

```
 [H3C-26 Connect_ID              ] [6 ] [430081]
```

Because the two values are different, the slot for the corresponding user is not found on the device, the session-control processing fails, and the iNode timeout goes offline.It can be seen that the device received a Connect-ID of 0 in the Session-control from the server, and then captured the packet on the IMC side for analysis. It was found that the device sent two vendor_specific attributes to the server, which eventually caused it to use the Session-control message in an abnormal way.

In newer versions, the switch's default acknowledgments carry two vendor-specific attributes.

Key Configuration

There are two reasons for this problem. One is the ACL configuration error, and the other is that the switch device carries two vendor_specific attributes, which causes the HW-Connection-ID of the session-ctrol message sent by EAD to be 0. After receiving the message, the device thinks it is illegal and drops the message, so the user fails to accounting and finally goes offline timed out

1. Modify the ACL mismatch source
2. Configure the device side to send only one vendor_specific property, radius view: Server-Type Extended vendor 2011.