

知 某局点U-Center 2.0 纳管的华为设备ssh探测失败

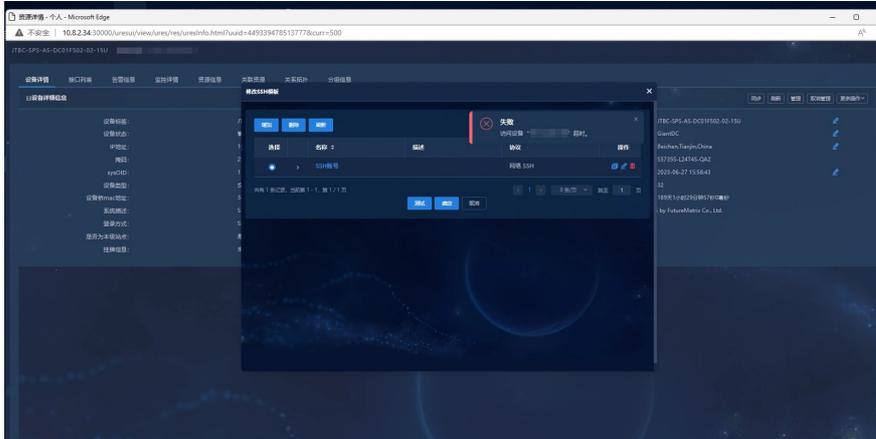
U-Center 2.0 小熊猫没有熊猫眼 2023-06-28 发表

组网及说明

不涉及

告警信息

版本信息: network 0711H04, 用snmp参数纳管华为设备S5735S-L24T4S-QA2成功, 但是配置的ssh参数探测失败, 报错访问设备超时。



问题描述

我司设备ssh探测均成功，只有华为设备探测产生超时报错，需要进一步排查设备ssh探测超时原因

过程分析

- (1) 经与客户确认，排查设备参数，账号名密码配置正确，且设备通过服务器后台能够登录设备，ss h -p port 账号名@IP;
- (2) 由于前台探测是通过产品自己内置脚本的方式实现的，后台服务器能够登录设备不代表探测功能就一定出了问题；
- (3) 通过在后台抓取探测报文，发现问题出现在客户端和服务器的ssh连接过程中的key exchange过程（密钥协商过程从客户端和服务器相互发出Key Exchange Init请求开始，主要是告诉对方自己支持的相关加密算法列表、MAC算法列表等。）

如下图，网管侧作为客户端在密钥及算法交换时支持的算法如红框中的部分，但是交换机侧配置的算法为rsa-sha2-512和rsa-sha2-256，两者协商不到相同的算法导致连接失败，故导致报错连接超时。

```
Packet 28: 2023-06-27 17:43:55.114300
  28 2023-06-27 17:43:55.114300
  31 2023-06-27 17:43:55.120746
  32 2023-06-27 17:43:55.120843
  33 2023-06-27 17:43:55.124808
  34 2023-06-27 17:43:55.124808
  35 2023-06-27 17:43:55.125106
  36 2023-06-27 17:43:55.132176
  37 2023-06-27 17:43:55.133188
  38 2023-06-27 17:43:55.133188
  39 2023-06-27 17:43:55.133415
  40 2023-06-27 17:43:55.139338
  41 2023-06-27 17:43:55.141180
  42 2023-06-27 17:43:55.145499

  Padding Length: 4
  * Key Exchange
  Message Code: Key Exchange Init (28)
  Algorithms
  Cookie: 15f66c3f2f78014602842640941b
  key_algorithm string: curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,rsa-sha2-512,rsa-sha2-256,rsa-sha2-2048,rsa-sha2-1024
  server_host_key_algorithms string: ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-rsa,ssh-dss
  encryption_algorithm_client_to_server string: aes256-ctr,aes128-ctr,rijndael-cbc@lysator.liu.se,aes192-ctr,aes128-ctr,aes128-cbc,chaCha20-poly1305@openssh.com,blowfish-ctr,blowfish-cbc,des-ctr,des-cbc,arcfour256
  encryption_algorithm_server_to_client string: aes256-ctr,aes128-ctr,rijndael-cbc@lysator.liu.se,aes192-ctr,aes128-ctr,aes128-cbc,chaCha20-poly1305@openssh.com,blowfish-ctr,blowfish-cbc,des-ctr,des-cbc,arcfour256
  mac_algorithm_client_to_server string: hmac-sha2-256,hmac-sha1,hmac-sha1-96,hmac-md5,hmac-md5-96,hmac-sha2-256-eta@openssh.com,hmac-sha1-eta@openssh.com,hmac-md5-eta@openssh.com
  mac_algorithm_server_to_client string: hmac-sha2-256,hmac-sha1,hmac-sha1-96,hmac-md5,hmac-md5-96,hmac-sha2-256-eta@openssh.com,hmac-sha1-eta@openssh.com,hmac-md5-eta@openssh.com
  mac_algorithm_server_to_client string: hmac-sha2-256,hmac-sha1,hmac-sha1-96,hmac-md5,hmac-md5-96,hmac-sha2-256-eta@openssh.com,hmac-sha1-eta@openssh.com,hmac-md5-eta@openssh.com
  compression_algorithm_client_to_server string: none,zlib
  compression_algorithm_server_to_client string: none,zlib
```

```
Packet 28: 2023-06-27 17:43:55.114300
  28 2023-06-27 17:43:55.120746
  31 2023-06-27 17:43:55.120746
  32 2023-06-27 17:43:55.120843
  33 2023-06-27 17:43:55.124808
  34 2023-06-27 17:43:55.124808
  35 2023-06-27 17:43:55.125106
  36 2023-06-27 17:43:55.132176
  37 2023-06-27 17:43:55.133188
  38 2023-06-27 17:43:55.133188
  39 2023-06-27 17:43:55.133415
  40 2023-06-27 17:43:55.139338
  41 2023-06-27 17:43:55.141180
  42 2023-06-27 17:43:55.145499

  Padding Length: 4
  * Key Exchange
  Message Code: Key Exchange Init (28)
  Algorithms
  Cookie: feb036e5e573f4880c3123548717
  key_algorithm string: diffie-hellman-group14-sha1,diffie-hellman-group15-sha1,diffie-hellman-group-exchange-sha256
  server_host_key_algorithms string: ssh-ed25519,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-rsa,ssh-dss
  encryption_algorithm_client_to_server string: aes256-ctr,aes128-ctr,rijndael-cbc@lysator.liu.se,aes192-ctr,aes128-ctr,aes128-cbc,chaCha20-poly1305@openssh.com,blowfish-ctr,blowfish-cbc,des-ctr,des-cbc,arcfour256
  encryption_algorithm_server_to_client string: aes256-ctr,aes128-ctr,rijndael-cbc@lysator.liu.se,aes192-ctr,aes128-ctr,aes128-cbc,chaCha20-poly1305@openssh.com,blowfish-ctr,blowfish-cbc,des-ctr,des-cbc,arcfour256
  mac_algorithm_client_to_server string: hmac-sha2-256,hmac-sha1,hmac-sha1-96,hmac-md5,hmac-md5-96,hmac-sha2-256-eta@openssh.com,hmac-sha1-eta@openssh.com,hmac-md5-eta@openssh.com
  mac_algorithm_server_to_client string: hmac-sha2-256,hmac-sha1,hmac-sha1-96,hmac-md5,hmac-md5-96,hmac-sha2-256-eta@openssh.com,hmac-sha1-eta@openssh.com,hmac-md5-eta@openssh.com
  compression_algorithm_client_to_server string: none,zlib
  compression_algorithm_server_to_client string: none,zlib
```

解决方法

经了解，交换机侧可以配置其他密钥及加密算法，可通过配置与网管侧相同的算法进行ssh连接，修改后，探测成功。

