



A2020-G(二代) 访问资产报错问题处理案例

堡垒机

李熙

2021-12-24 发表

组网及说明

暂无

问题描述

堡垒机之前访问该linux资产没问题，后续将资产内核从7.6升级到7.9，openssh版本从7.4到8.8后，访问资产提示如下报错， **linux permission denied , please try again**

```
[root@nginx pam.d]# ssh -U  
OpenSSH_8.8p1, OpenSSL 1.0.2k-fips 26 Jan 2017  
[root@nginx pam.d]# _
```

```
[root@nginx pam.d]# cat /etc/redhat-release  
CentOS Linux release 7.9.2009 (Core)  
[root@nginx pam.d]#
```

过程分析

1、root账号的权限足够，内网终端通过root账号直接ssh到服务器没问题，**pc直接通过root账号ssh登录设备没问题**；仅通过堡垒机ssh登录该linux系统才会出问题。

2、对应的端口均放通，具体端口如下：

PC客户端到堡垒机 443/22/3389/5899

堡垒机到应用发布服务器 3389/5156

堡垒机到目标资产服务器/设备等 按需放通，21/22/23等

应用发布服务器需要访问目标资产 80/443/1521/3306/1433等

3、从抓包来看，堡垒机连接centOS时提供的服务器主机密钥算法只有ssh-rsa和ssh-dss两种：

```
SSH Protocol
├─ SSH Version 2
│   ├── Packet Length: 620
│   ├── Padding Length: 10
│   └─ Key Exchange (method:ecdh-sha2-nistp256)
│       ├── Message Code: Key Exchange Init (20)
│       └─ Algorithms
│           ├── Cookie: f73e84071ee70364b6efe43b50fc97b6
│           ├── kex_algorithms length: 164
│           ├── kex_algorithms string: ecdh-sha2-nistp256,ecdh-sha2-nistp384,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,d
│           ├── server_host_key_algorithms length: 15
│           └─ server_host_key_algorithms string: ssh-rsa,ssh-dss
│               └─ encryption_algorithms_client_to_server length: 109
```

Openssh 8.8是今年九月底新发布的版本，在发行说明里面提到了对ssh算法进行了调整，“当连接到尚未升级或没有密切跟踪SSH协议改进的旧版本时，可能会由于不兼容导致连接失败

解决方法

需要升级堡垒机版本至E6112P18或更新版本支持新的算法。

