

知 某局点iMC-EIA使用mschapV2认证失败问题排查

802.1X

LDAP

iMC

罗孝晨

2020-07-01 发表

组网及说明

EIA 7.3E0505

配合AD域控进行mschapV2认证

问题描述

某局点使用iMC-EIA配合微软AD进行MSCHAPV2认证失败

过程分析

(1) 分析mschapv2日志, 通过分析ChapV2Jserver.log, 日志有如下记录:

```
[2020-06-17 00:00:00.39] [Debug] [MSChapAuth::connect]Exceptions. <jcifs.smb.SmbException: Failed to connect: 0.0.0.0<00>...>
jcifs.util.transport.TransportException
java.net.SocketException: Connection reset
    at java.net.SocketInputStream.read(SocketInputStream.java:196)
    at java.net.SocketInputStream.read(SocketInputStream.java:122)
    at jcifs.util.transport.Transport.read(Unknown Source)
    at jcifs.smb.SmbTransport.peekKey(Unknown Source)
    at jcifs.smb.SmbTransport.negotiate(Unknown Source)
    at jcifs.smb.SmbTransport.doConnect(Unknown Source)
    at jcifs.util.transport.Transport.run(Unknown Source)
    at java.lang.Thread.run(Thread.java:746)
>
    at jcifs.util.transport.Transport.run(Unknown Source)
    at java.lang.Thread.run(Thread.java:746)
>
```

从日志中可以看到EIA使用smb连接AD服务器失败

(2) 检查LDAP服务器SMB1和SMB2协议是否开启, EIA7.3E0505版本只支持SMB1协议, E0510及后续版本开始同时支持SMB1和SMB2协议。检查方法如下:

<1>登录LDAP服务器远程桌面

<2>打开Powershell,执行Get-SmbServerConfiguration | Select EnableSMB1Protocol, EnableSMB2Protocol命令, 若输出为EnableSMB1Protocol=False, 说明SMB1协议没有开启

<3>开启SMB1协议方法未, 打开PowerShell, 执行Set-SmbServerConfiguration -EnableSMB1Protocol \$true

<4>无需重启LDAP服务器

(3) 启用SMB1协议后由于iMC需要重新获取SMB1连接, 因此需要重启iMC服务器, 若服务器不能整体重启, 可以只重启mschapv2进程。

解决方法

(1) 启用SMB1协议

(2) 或者升级EIA至7.3E0510及后续版本, 支持SMB2协议