

知

某局点iMC PLAT 所在Windows系统因为中了挖矿病毒导致iMC连接数据库异常

PLAT

李树兵

2020-06-30 发表

组网及说明

略。

问题描述

某局点反馈会随机出现iMC 的智能部署监控代理会出现连接数据库异常，在连接数据库的详细信息里面提示如下报错：

com.microsoft.sqlserver.jdbc.SQLServerException: 通过端口 1433 连接到主机 127.0.0.1 的 TCP/IP 连接失败。错误:"No buffer space available (maximum connections reached?): connect。请验证连接属性。确保 SQL Server 的实例正在主机上运行，且在此端口接受 TCP/IP 连接，还要确保防火墙没有阻止到此端口的 TCP 连接。”。

at com.microsoft.sqlserver.jdbc.SQLServerException.makeFromDriverError(SQLServerException.java:190)

at

com.microsoft.sqlserver.jdbc.SQLServerException.ConvertConnectExceptionToSQLServerException(SQLServerException.java:241)

at com.microsoft.sqlserver.jdbc.SocketFinder.findSocket(IOBuffer.java:2243)

at com.microsoft.sqlserver.jdbc.TDSCchannel.open(IOBuffer.java:491)

at com.microsoft.sqlserver.jdbc.TDSCchannel.open(IOBuffer.java:491)

```
1 com.microsoft.sqlserver.jdbc.SQLServerException: 通过端口 1433 连接到主机 127.0.0.1 的 TCP/IP 连接失败。错误:"No buffer space available (maximum connections reached?): connect。
2 请验证连接属性。确保 SQL Server 的实例正在主机上运行，且在此端口接受 TCP/IP 连接，还要确保防火墙没有阻止到此端口的 TCP 连接。"。
3
4 at com.microsoft.sqlserver.jdbc.SQLServerException.makeFromDriverError(SQLServerException.java:190)
5 at com.microsoft.sqlserver.jdbc.SQLServerException.ConvertConnectExceptionToSQLServerException(SQLServerException.java:241)
6 at com.microsoft.sqlserver.jdbc.SocketFinder.findSocket(IOBuffer.java:2243)
7 at com.microsoft.sqlserver.jdbc.TDSCchannel.open(IOBuffer.java:491)
8 at com.microsoft.sqlserver.jdbc.SQLServerConnection.connectHelper(SQLServerConnection.java:1309)
9 at com.microsoft.sqlserver.jdbc.SQLServerConnection.login(SQLServerConnection.java:991)
10 at com.microsoft.sqlserver.jdbc.SQLServerDriver.connect(SQLServerDriver.java:1012)
11 at java.sql.DriverManager.getConnection(DriverManager.java:582)
12 at java.sql.DriverManager.getConnection(DriverManager.java:154)
13 at com.h3c.imc.deploy.dma.EnvPanel.a(EnvPanel.java:1144)
14 at com.h3c.imc.deploy.dma.EnvPanel.F(EnvPanel.java:1097)
15 at com.h3c.imc.deploy.dma.EnvPanel.a(EnvPanel.java:128)
16 at com.h3c.imc.deploy.dma.az.run(EnvPanel.java:627)
17
```

```
1 com.microsoft.sqlserver.jdbc.SQLServerException: 通过端口 1433 连接到主机 127.0.0.1 的 TCP/IP 连接失败。错误:"No buffer space available (maximum connections reached?): connect。
2 请验证连接属性。确保 SQL Server 的实例正在主机上运行，且在此端口接受 TCP/IP 连接，还要确保防火墙没有阻止到此端口的 TCP 连接。"。
3
4 at com.microsoft.sqlserver.jdbc.SQLServerException.makeFromDriverError(SQLServerException.java:190)
5 at com.microsoft.sqlserver.jdbc.SQLServerException.ConvertConnectExceptionToSQLServerException(SQLServerException.java:241)
6 at com.microsoft.sqlserver.jdbc.SocketFinder.findSocket(IOBuffer.java:2243)
7 at com.microsoft.sqlserver.jdbc.TDSCchannel.open(IOBuffer.java:491)
8 at com.microsoft.sqlserver.jdbc.SQLServerConnection.connectHelper(SQLServerConnection.java:1309)
9 at com.microsoft.sqlserver.jdbc.SQLServerConnection.login(SQLServerConnection.java:991)
10 at com.microsoft.sqlserver.jdbc.SQLServerDriver.connect(SQLServerDriver.java:1012)
11 at java.sql.DriverManager.getConnection(DriverManager.java:582)
12 at java.sql.DriverManager.getConnection(DriverManager.java:154)
13 at com.h3c.imc.deploy.dma.EnvPanel.a(EnvPanel.java:1144)
14 at com.h3c.imc.deploy.dma.EnvPanel.F(EnvPanel.java:1097)
15 at com.h3c.imc.deploy.dma.EnvPanel.a(EnvPanel.java:128)
16 at com.h3c.imc.deploy.dma.az.run(EnvPanel.java:627)
17
```

at

com.microsoft.sqlserver.jdbc.SQLServerConnection.connectHelper(SQLServerConnection.java:1309)

at com.microsoft.sqlserver.jdbc.SQLServerConnection.login(SQLServerConnection.java:991)

at com.microsoft.sqlserver.jdbc.SQLServerConnection.connect(SQLServerConnection.java:827)

at com.microsoft.sqlserver.jdbc.SQLServerDriver.connect(SQLServerDriver.java:1012)

at java.sql.DriverManager.getConnection(DriverManager.java:582)

at java.sql.DriverManager.getConnection(DriverManager.java:154)

at com.h3c.imc.deploy.dma.EnvPanel.a(EnvPanel.java:1144)

at com.h3c.imc.deploy.dma.EnvPanel.F(EnvPanel.java:1097)

at com.h3c.imc.deploy.dma.EnvPanel.a(EnvPanel.java:128)

at com.h3c.imc.deploy.dma.az.run(EnvPanel.java:627)

过程分析

根据数据库连接失败的提示可以明显看到时因为iMC通过端口 1433 连接到主机 127.0.0.1 的 TCP/IP 连接失败。错误:"No buffer space available (maximum connections reached?): connect。请验证连接属性。确保 SQL Server 的实例正在主机上运行，且在此端口接受 TCP/IP 连接，还要确保防火墙没有阻止到此端口的 TCP 连接。”。

此种情况很多情况下是因为socket句柄连接过多导致，可以通过如下反复排查：

1、下载 <https://docs.microsoft.com/zh-cn/sysinternals/downloads/handle>

运行Handle.exe -a afd > result.txt

收集result.txt

文件下载和分析方法，可以参考此案例：<https://zhiliao.h3c.com/Theme/details/93574>

2、在收集的result文件中可以看到Syste64.exe程序占了1023条数据，占据了大部分的连接

```

146
147 Sysste64.exe pid: 22992 type: File 11D8: \Device\Afd
148
149 Sysste64.exe pid: 22992 type: File 11DC: \Device\Afd
150
151 Sysste64.exe pid: 22992 type: File 11E0: \Device\Afd
152
153 Sysste64.exe pid: 22992 type: File 11E4: \Device\Afd
154
155 Sysste64.exe pid: 22992 type: File 11E8: \Device\Afd
156
157 Sysste64.exe pid: 22992 type: File 11EC: \Device\Afd
158
159 Sysste64.exe pid: 22992 type: File 11F0: \Device\Afd
160
161 Sysste64.exe pid: 22992 type: File 11F4: \Device\Afd
162
163 Sysste64.exe pid: 22992 type: File 11F8: \Device\Afd
164
165 Sysste64.exe pid: 22992 type: File 11FC: \Device\Afd
166
167 Sysste64.exe pid: 22992 type: File 1200: \Device\Afd
168
169 Sysste64.exe pid: 22992 type: File 1204: \Device\Afd
170
171 Sysste64.exe pid: 22992 type: File 1208: \Device\Afd
172
173 Sysste64.exe pid: 22992 type: File 120C: \Device\Afd
174
175 Sysste64.exe pid: 22992 type: File 1210: \Device\Afd
176
177 Sysste64.exe pid: 22992 type: File 1214: \Device\Afd
178
179 Sysste64.exe pid: 22992 type: File 1218: \Device\Afd

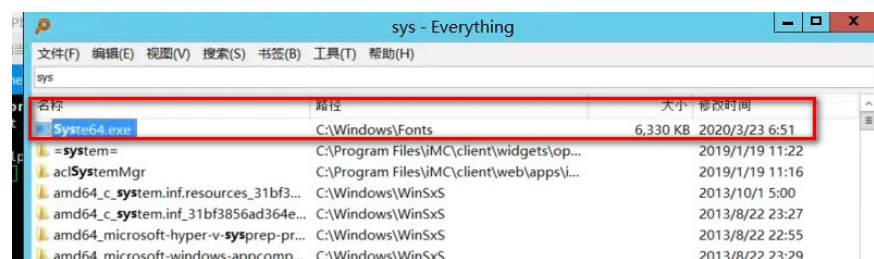
```

```

! result - 1,023 hits
search "Sysste64" (1023 hits in 1 file)
D:\客户问题收集\6.29 imc连接数据库问题\result.txt (1023 hits)
Line 2657: Sysste64.exe pid: 22992 type: File 15C: \Device\Afd
Line 2659: Sysste64.exe pid: 22992 type: File 164: \Device\Afd
Line 2661: Sysste64.exe pid: 22992 type: File 168: \Device\Afd
Line 2663: Sysste64.exe pid: 22992 type: File 1A0: \Device\Afd
Line 2665: Sysste64.exe pid: 22992 type: File 1C8: \Device\Afd
Line 2667: Sysste64.exe pid: 22992 type: File 1E8: \Device\Afd
Line 2669: Sysste64.exe pid: 22992 type: File 1EC: \Device\Afd
Line 2671: Sysste64.exe pid: 22992 type: File 1F0: \Device\Afd
Line 2673: Sysste64.exe pid: 22992 type: File 1F4: \Device\Afd
Line 2675: Sysste64.exe pid: 22992 type: File 1F8: \Device\Afd
Line 2677: Sysste64.exe pid: 22992 type: File 1FC: \Device\Afd
Line 2679: Sysste64.exe pid: 22992 type: File 200: \Device\Afd
Line 2681: Sysste64.exe pid: 22992 type: File 204: \Device\Afd
Line 2683: Sysste64.exe pid: 22992 type: File 208: \Device\Afd
Line 2685: Sysste64.exe pid: 22992 type: File 20C: \Device\Afd
Line 2687: Sysste64.exe pid: 22992 type: File 210: \Device\Afd

```

- 3、通过查看Windows的任务管理器发现此进程时有时无，非常异常，无法确定具体什么服务和进程引起。
- 4、通过查找文件，可以看到此文件是在C盘的Windows\Fonts 目录下，这个目录是Windows存放字体的目录，一般删除是不影响IMC和系统运行的。



- 5、强制删除的时候回提示报错，提示有程序正在运行此文件，显示此文件是XMRing miner



- 6、通过此文件到网上搜索都是显示是挖矿病毒，说明Windows系统中中了挖矿病毒了。

[手动删除XmRigMiner挖矿病毒实录 - 科学-文哥 - 博客园](#)

2020年3月7日 - 另外有俩项go.exe和goo.exe不断被杀,不断重生;在任务管理器里发现了一个进程叫XmRigMiner的进程,网上说是挖矿工具,在C:/ProgramData也发现挖矿工具,于...
[博客园](#) - [百度快照](#)

[解决挖矿病毒【Xmrig_miner】CPU 100%服务器卡死问题](#)

2020年3月13日 - 【Xmrig_miner】CPU 100%服务器卡死问题,进程中找到描述中写的“Xmrig_miner”的,右键属性里面,安全禁止读写,结束掉进程,即可解决。 解决挖矿病毒【...
[www.mamicode.com/info-... - 百度快照](#)

[比特币病毒xmrigMiner入侵服务器的解决方法 - ThinkPHP框架](#)

2018年10月29日 - 服务器被比特币病毒攻击了,创建了一个xmrigMiner进程,百度了下,是比特币病毒,更准确点,是门罗币病毒。CPU持续占用超过99%,严重影响服务器运行,解决完...
[www.thinkphp.cn/code/4... - 百度快照](#)

[发现xmrig_miner,现在删了后台,有什么根治方法吗?楼里放俩图【病...](#)

回复数: 26 发帖时间: 2020年04月04日
8楼: 这类挖矿,很多由计划任务里的Powershell命令或脚本...
11楼: C盘的programdata文件夹下有两个橙色的图标,就是这两...
[百度贴吧](#) - [百度快照](#)

[...挖矿病毒xmrigcpuminer_qq_42906657的博客-CSDN博客_xmrigminer](#)

2018年9月16日 - 初步解决挖矿病毒xmrigcpuminer本人初学者,前段时间写了个爬虫,暴露了ip,服务器受到攻击,被植入了木马,后来就发现中了这个挖矿病毒。之前曾经解决过,...
[CSDN技术社区](#) - [百度快照](#)

从以上分析能确定是Windows系统可能在4月18号(病毒文件的创建时间)就被下了挖矿病毒,此病毒有时会建立很多会话,从而占用很多连接,将TCP的连接数占满,进而导致iMC连接数据库的时候因为连接数满而无法连接数据库。

解决方法

通过以上分析,要解决此问题需要消灭挖矿病毒,保证iMC正常使用。

第一步:可以参考网络上的方法尝试进行修复;

第二步:如还不能解决,可尝试先将iMC的数据通过dbman进行备份,然后安装杀毒软件进行全盘查杀(如果因为iMC本身的文件也被感染了导致文件被杀毒软件删除,进而导致iMC无法正常使用,需要重新安装iMC),如果消灭病毒之后iMC能正常使用即问题解决;

第三步:如使用全盘查杀还是不能彻底消灭病毒,在备份好iMC的数据之后,请将硬盘进行格式化,然后重新安装系统、数据库、iMC,切记安装的数据库和iMC版本和当前的一致,之后进行数据修复和license文件的导入(只是重装操作系统,不会影响license,所以使用之前的license文件重新注册即可)。