钟先生，您好：

如刚才电话沟通，经您的确认，该问题目前已解决，case 将做关闭处理，感谢您这段时间的大力配合，以下为案例总结，请您知悉：

Case No：CAS-05772-J6R0H4

问题描述：

==========

用户来电反馈 V2020-L 中 Print Spooler 服务无法启动，报错代码为 0x80070057，目前有 5 台电脑涉及此问题

问题分析：

==========

经问题排查，由于 RPC 连接失败导致 print spooler 服务无法启动，删除如下位置的注册表键值（建议提前导出备份），可以解决 RPC 连接失败的问题，print spooler 服务可以正常开启。

HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Internet

问题总结：

==========

经用户确认，问题得到解决，此案例可以关闭。

以上，如您后续有任何问题，可随时与我们联系，谢谢。

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

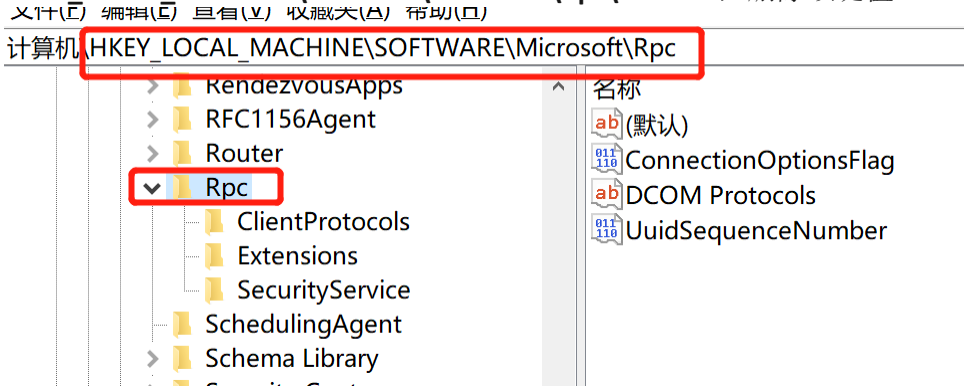
发件人: Li Qi
发送时间: 2022 年 3 月 21 日 14:02
收件人: '钟先生' <807199247@qq.com>
抄送: Case_Notification <Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-05772-J6R0H4] % 广东省第三强制隔离戒毒所用户来电反馈 V2020-L 中 Print Spooler 服务无法启动无法打印问题 % 初次响应 CMIT:0001607

钟先生，您好:

刚才电话未联系到您，经分析，该问题应为 RPC 的连接出现问题导致，请尝试删除如下注册表键值查看:

1， 按 Win+R，在运行窗口输入"regedit"，打开注册表编辑器，导航至如下位置:

HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Internet， 删除该键值



2， 尝试启动 print spooler 服务，看是否可以正常启动

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

神州网信 CMIT

发件人: Li Qi
发送时间: 2022 年 3 月 15 日 9:57
收件人: '钟先生' <807199247@qq.com>
抄送: Case_Notification <Case_Notification@cmgos.com>

主题: 回复: [案例号: CAS-05772-J6R0H4] % 广东省第三强制隔离戒毒所用户来电反馈 V2020-L 中 Print Spooler 服务无法启动无法打印问题 % 初次响应 CMIT:0001607

钟先生，您好:

请参见如下的下一步方案：

==========

1、请把如下注册表导出上传。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip

2、请在问题发生的时候，收集如下的日志：

1）printing etl

以管理权限运行以下命令开启：

logman create trace "printscan_print" -ow -o c:\printscan_print.etl -p "Microsoft-Windows-PrintService" 0xffffffffffffffff 0xff -nb 16 16 -bs 1024 -mode Circular -f bincirc -max 4096 -ets
logman update trace "printscan_print" -p {C9BF4A03-D547-4D11-8242-E03A18B5BE01} 0xffffffffffffffff 0xff -ets
logman update trace "printscan_print" -p {C9BF4A9F-D547-4D11-8242-E03A18B5BE01} 0xffffffffffffffff 0xff -ets
logman update trace "printscan_print" -p {C9BF4A9E-D547-4D11-8242-E03A18B5BE01} 0xffffffffffffffff 0xff -ets
logman update trace "printscan_print" -p {C9BF4A05-D547-4D11-8242-E03A18B5BE01} 0xffffffffffffffff 0xff -ets
logman update trace "printscan_print" -p {C9BF4A01-D547-4D11-8242-E03A18B5BE01} 0xffffffffffffffff 0xff -ets

运行以下命令停止 ETL:

logman stop "printscan_print" –ets

2）winsock etl

以管理权限运行以下命令开启 TCP/IP ETL。

netsh trace start overwrite=yes maxsize=2048 tracefile=c:\minio_sockets.etl provider="Microsoft-Windows-Winsock-AFD" keywords=0x800000000000003f level=0x5 provider={EB004A05-9B1A-11D4-9123-0050047759BC} keywords=0x3ffff level=0x5 provider="Microsoft-Windows-TCPIP" keywords=0x80007fff000000ff level=0x5 provider={B40AEF77-892A-46F9-9109-438E399BB894} keywords=0xffffffffffffffff level=0xff

provider="Microsoft-Windows-WFP" keywords=0xffffffffffffffff level=0xff provider={106B464A-8043-46B1-8CB8-E92A0CD7A560} keywords=0xffffffffffffffff level=0xff

运行以下命令停止 ETL:

netsh trace stop

3）rpc etl

Start tracing:

logman create trace "base_screg" -ow -o c:\base_screg.etl -p "Service Control Manager" 0xffffffffffffffff 0xff -nb 16 16 -bs 1024 -mode Circular -f bincirc -max 4096 -ets

logman update trace "base_screg" -p "Microsoft-Windows-Services" 0xffffffffffffffff 0xff -ets

logman update trace "base_screg" -p {EBCCA1C2-AB46-4A1D-8C2A-906C2FF25F39} 0xffffffffffffffff 0xff -ets

logman update trace "base_screg" -p "Microsoft-Windows-RPC-Proxy-LBS" 0xffffffffffffffff 0xff -ets

logman update trace "base_screg" -p "Microsoft-Windows-RPC-Proxy" 0xffffffffffffffff 0xff -ets

logman update trace "base_screg" -p "Microsoft-Windows-RPC-LBS" 0xffffffffffffffff 0xff -ets

logman update trace "base_screg" -p "Microsoft-Windows-RPC" 0xffffffffffffffff 0xff -ets

logman update trace "base_screg" -p "Microsoft-Windows-RPC-Events" 0xffffffffffffffff 0xff -ets

logman update trace "base_screg" -p "Microsoft-Windows-RPCSS" 0xffffffffffffffff 0xff -ets

Stop tracing:

logman stop "base_screg" -ets

4）同一时间的 spooler 的 ttd

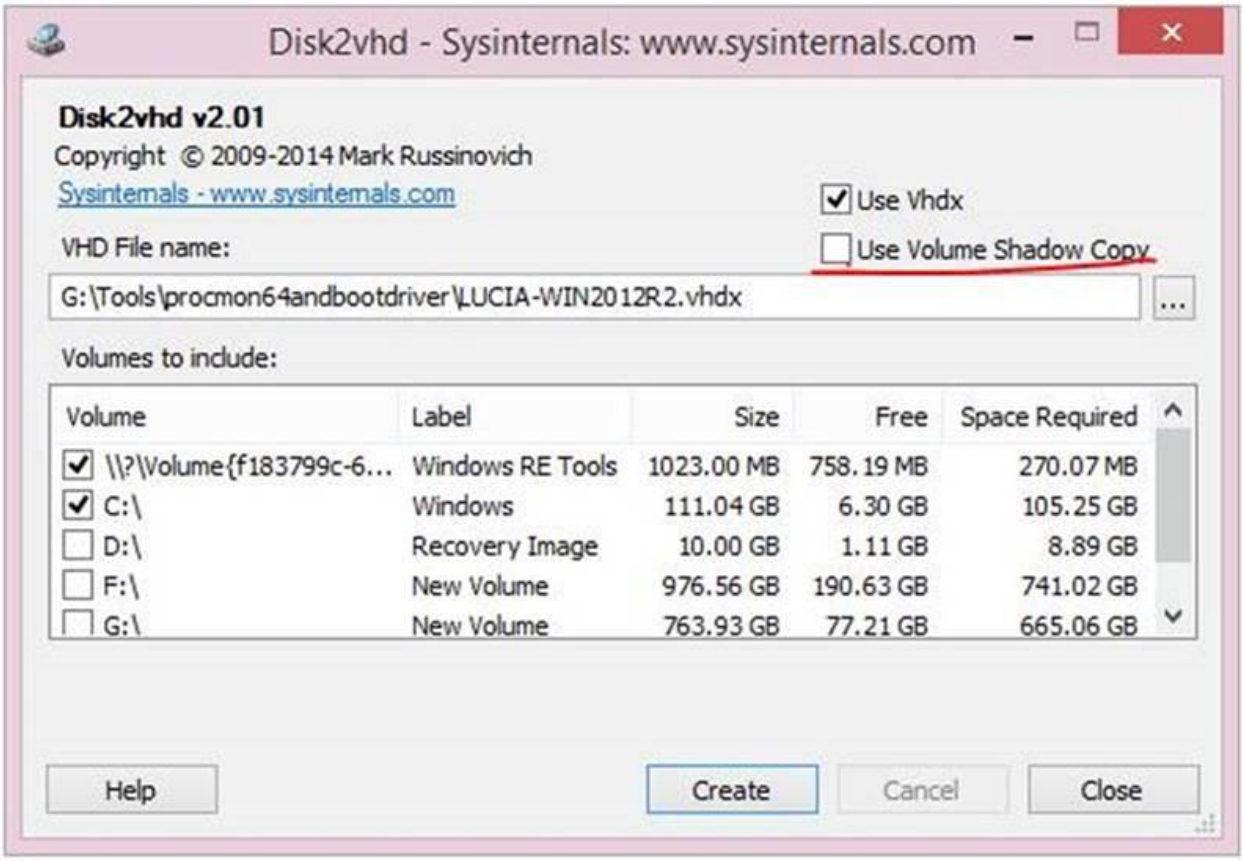
4 个日志同时开启，复现问题后，分别停止。然后上传，ttd trace、c:\base_screg.etl、c:\minio_sockets.etl、c:\printscan_print.etl。

3、如果可以 p2v，请按照如下的步骤收集 p2v 日志。

a. 下载 disk2vhd 工具保存这台机器上。附件密码为 1234
b. 复现问题的电脑，进入命令行。
c. 从命令行运行如下命令：

disk2vhd.exe

d. 取消 Use Volume Shadow Copy 勾选，选择 C 盘，然后生成 VHDX 文件。我们需要一个除 C 盘之外的盘保存这个文件。



李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

发件人: Li Qi
发送时间: 2022 年 3 月 4 日 14:02

收件人: '钟先生' <807199247@qq.com>
抄送: Case_Notification <Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-05772-J6R0H4] % 广东省第三强制隔离戒毒所用户来电反馈 V2020-L 中 Print Spooler 服务无法启动无法打印问题 % 初次响应 CMIT:0001607

Hi，钟先生：
如上午电话沟通，接下来需要针对 winsock 修复收集相关日志分析，主要步骤如下：

ttt + procmon+ etl trace
==========
1. 管理员身份运行 cmd，执行如下指令
cd /d <path of TTTracer>
tttracer.exe -initialize
logman create trace "printscan_print" -ow -o c:\printscan_print.etl -p "Microsoft-Windows-PrintService" 0xffffffffffffffff 0xff -nb 16 16 -bs 1024 -mode Circular -f bincirc -max 4096 -ets
logman update trace "printscan_print" -p {C9BF4A03-D547-4D11-8242-E03A18B5BE01} 0xffffffffffffffff 0xff -ets
logman update trace "printscan_print" -p {C9BF4A9F-D547-4D11-8242-E03A18B5BE01} 0xffffffffffffffff 0xff -ets
logman update trace "printscan_print" -p {C9BF4A9E-D547-4D11-8242-E03A18B5BE01} 0xffffffffffffffff 0xff -ets
logman update trace "printscan_print" -p {C9BF4A05-D547-4D11-8242-E03A18B5BE01} 0xffffffffffffffff 0xff -ets
logman update trace "printscan_print" -p {C9BF4A01-D547-4D11-8242-E03A18B5BE01} 0xffffffffffffffff 0xff -ets

2. 启动 TTTracer，执行如下指令
md c:\temp\
tttracer -onlaunch spoolsv.exe -parent services.exe -out c:\temp\

3. 同步抓取 procmon

4. 复现问题 (启动 spooler 服务)

5. 停止 trace，取消勾选 “tracing on” 即可，然后 tttrace 就会自动停止，并执行如下命令确认 tttracer 已停止，同时停止 etl trace
tttracer.exe -stop all tttracer.exe -delete all
logman stop "printscan_print" –ets

6. 停止 procmon 日志

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.

服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

神州网信 CMIT

发件人: Li Qi
发送时间: 2022 年 3 月 1 日 16:09
收件人: 钟先生 <807199247@qq.com>
抄送: Case_Notification <Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-05772-J6R0H4] % 广东省第三强制隔离戒毒所用户来电反馈 V2020-L 中 Print Spooler 服务无法启动无法打印问题 % 初次响应 CMIT:0001607

钟先生，您好:

如刚才电话沟通，我将于明天上午与您联系，请您按下方步骤收取系统日志供接下来的问题排查。当前谨以此邮件阐述我们双方针对这个问题所涉及范围界定。

问题定义:

用户来电反馈 V2020-L 中 Print Spooler 服务无法启动，报错代码为 0x80070057，目前有 5 台电脑涉及此问题。

问题范围:

我们将协助您分析处理上述问题，并对定义的问题给予最大的技术支持。

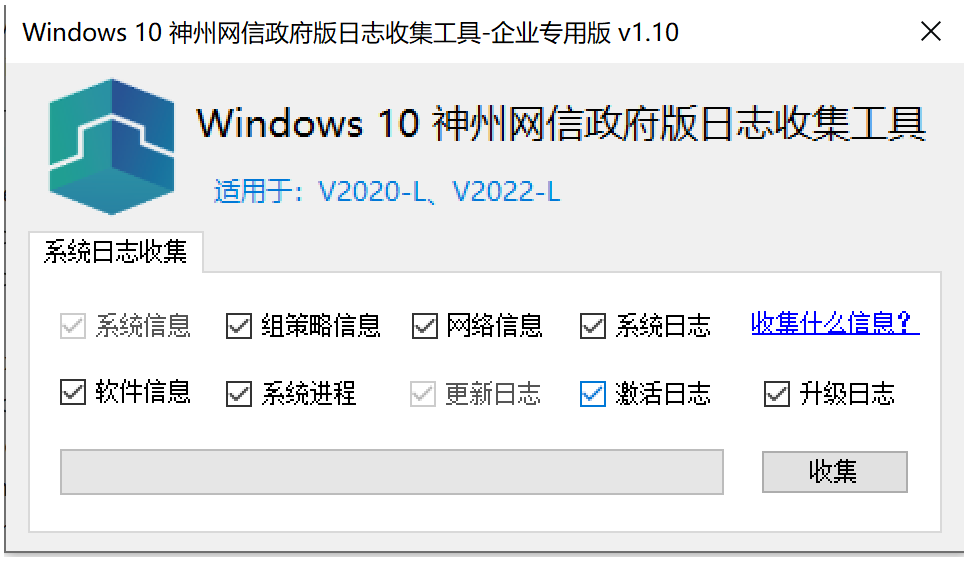
如果能及时解决问题，或问题属于产品设计的行为，或问题涉及到三方，我们将考虑关闭案例。如果存在多个问题，则我们考虑拆分案例进行分析。

接下来，我们将开始合作解决这个问题。如果您对以上的问题范围界定有任何异议，请尽快告知。如果您有其他任何疑问。也欢迎随时与我联系。

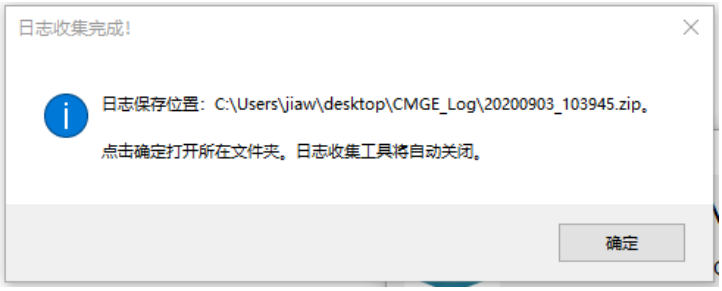
下一步动作，收集系统日志：

CMGE 系统日志:

请下载附件 CMGELogCollector.zip，解压并运行 exe 文件，同意隐私声明后，按照下图勾选，点击收集。



收集完毕后将在当前用户桌面生产 CMGE_Log。点击确定，将直接打开文件夹并保存为压缩文件。



请将保存的压缩文件上传至日志上传系统，谢谢。

日志上传：

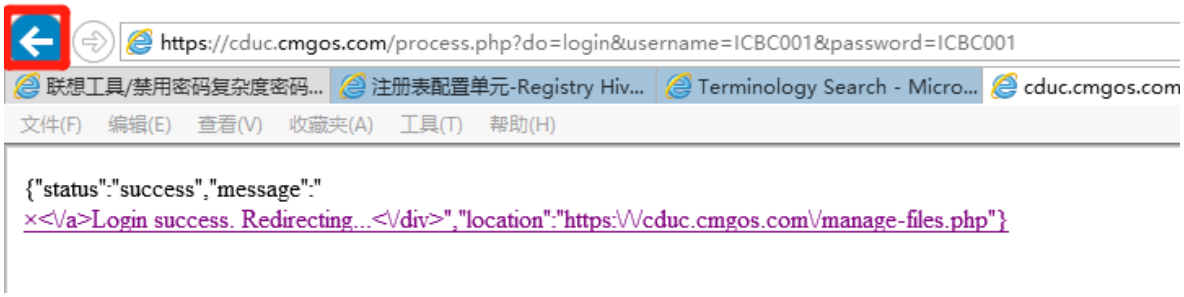
登陆 https://cduc.cmgos.com，通过数据上传系统上传您所收集的日志信息

用户名：dsqzjds001

密码：dsqzjds001

添加文件后点击上传文件 ，上传完毕后点击保存

注意，如果遇到如下所示页面，点击后退即可看到页面



==========

在向 CMIT 提供日志和数据前，请阅读并接受邮件下方隐私声明。

隐私声明

为向您提供本产品的相关技术支持及相关服务，您需要在同意本声明的前提下向神州网信提供为解决系统故障必要的数据和信息，包括但不限于与您相关的个人数据和隐私信息。通常情况下，我们仅需要如下数据以使我们的服务能够更好地满足您的需求：内存转储文件、注册表信息、组策略信息、事件日志、安装应用列表、驱动信息、网络日志或系统补丁等。

神州网信承诺将采取商业上可行及必要措施保护用户提供给神州网信的数据和信息，且仅在解决问题过程中使用。

神州网信保证不对外公开或向第三方提供、公开或共享您提供的数据和信息。

在以下情况下，神州网信对您的数据和信息的披露将不视为违约，具体包括：

(1) 神州网信已获得您的明确授权；

(2) 根据适用法律的要求，神州网信负有披露义务的；

(3) 司法机关或行政机关基于法定程序要求神州网信提供的；

(4) 为维护社会公共利益及神州网信合法权益，在合理范围内进行披露的。

(5) 为了解决您的系统故障问题，神州网信可能会与神州网信的分包商披露您提供的数据和信息。在此情况下，第三方会承担与神州网信同等的隐私保护责任的，神州网信会在合理范围内对您的信息进行披露。

如果您欲提供的数据和信息中包含对您重要的保密信息以及商业秘密，在您向神州网信提供上述数据和信息前，务必对上述数据和信息进行脱敏处理，否则请不要提供该信息给神州网信。

作为一家商业软件公司，神州网信在商业可行的前提下，已为用户的数据和信息保护做了极大的努力，但是仍然不能保证现有的安全技术措施使您的数据和信息等不受任何形式的损失。您对上述情况充分知情，且不会因此追究神州网信的法律责任。

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

神州网信
CMIT

发件人: Li Qi <liqi@cmgos.com>
发送时间: 2022 年 3 月 1 日 15:57
收件人: 钟先生 <807199247@qq.com>
抄送: Li Qi <liqi@cmgos.com>
主题: [案例号: CAS-05772-J6R0H4] % 广东省第三强制隔离戒毒所用户来电反馈 V2020-L 中 Print Spooler 服务无法启动无法打印问题 % 初次响应 CMIT:0001607

钟先生 先生/女士，您好!

感谢您联系神州网信技术支持中心。 我是技术支持工程师 李琦 。 很高兴能有机会协助您解决该问题。 您可随时通过邮件回复以及该问题事件号码 CAS-05772-J6R0H4 与我联系。

如果您有任何其他疑问，请随时与我联系。

此致,

敬礼
