许先生 您好：

经过您的同意，我将暂时归档此案例。

工单的归档并不会影响我们为您提供技术支持服务，如您有其他问题，您可以致电技术支持热线 4008180055。

案例总结：

问题定义：

无线网络突然断网，断网后手工重连时卡在正在连接状态，此时整个操作系统会出现各种无法响应的问题，需要分析原因。

问题总结：

更新网卡驱动并优化 CheckHosts 任务调度后，未再次出现问题，暂时归档案例。

日志分析及建议：

从 dump 中的情况看，有以下几个问题：

1）有进程等待在 smb 上，在等待访问 CheckHosts.exe 应用。

2）RPCSS 服务中有多个线程等待在 DCOM Launch 服务，但是三方驱动 krnlmgr.sys 注册了 PspCallProcessNotifyRoutines，所以一直等待在它上面。经过确认 krnlmgr.sys 是 TMS 的驱动，无法回退或者临时卸载。

测试建议：

1）在本地修改一些对象的审核策略，减少 4663 事件的生成，**具体操作如下：**

a）以**管理员权限**运行 gpedit.msc，打开**本地组策略编辑器**，定位到：

“本地计算机策略”-“计算机配置”-“Windows 设置”-“安全设置”-“高级审核策略”-“系统审核策略-本地组策略对象”-“对象访问”，

b）修改**“审核内核对象”**和**“审核注册表”**为**“未配置”**状态。

2）从设备官网下载更新有线网卡和无线网卡驱动。

以上，如您后续有任何问题，可随时与我们联系，谢谢。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2022 年 9 月 30 日 10:00
收件人: 'Windows Server 技术支持' <windowsserversupport@sdc.icbc.com.cn>; 'hy1198809722@163.com' <hy1198809722@163.com>; 'qiyq@sdc.icbc.com.cn' <qiyq@sdc.icbc.com.cn>
抄送: 'win10sup@sdc.icbc.com.cn' <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: 回复: 回复: 回复:【外来邮件，注意核实】回复: [案例号：CAS-06619-Z0Z8H9] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001372

戚先生 & 黄先生 你们好:

来信是想了解近期是否再次出现多个应用无法打开、系统卡死等问题。如果出现相关问题，可以**通过手动生成 dump，并记录出现问题时运行了哪个应用发现无法打开**后，通过许先生@'Windows Server 技术支持' 将此 dump 提供给我们进一步分析。

如果针对当前案件还有需要我们帮助的地方, 欢迎随时联系我们。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2022 年 9 月 23 日 16:24
收件人: 'Windows Server 技术支持' <windowsserversupport@sdc.icbc.com.cn>; 'hy1198809722@163.com' <hy1198809722@163.com>
抄送: 'win10sup@sdc.icbc.com.cn' <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>; 'qiyq@sdc.icbc.com.cn' <qiyq@sdc.icbc.com.cn>
主题: 回复: 回复: 回复: 回复:【外来邮件，注意核实】回复: [案例号: CAS-06619-Z0Z8H9] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001372

黄先生 您好:

下午给您的电话没有接通。

来信是想询问您调整相关配置并更新有线和无线网卡驱动后，近期是否再次出现多个应用无法打开、系统卡死等问题。

如果针对当前案件还有需要我们帮助的地方, 欢迎随时联系我们。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2022 年 9 月 18 日 12:05
收件人: 'Windows Server 技术支持' <windowsserversupport@sdc.icbc.com.cn>
抄送: win10sup@sdc.icbc.com.cn; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: 回复: 回复: 回复:【外来邮件，注意核实】回复: [案例号: CAS-06619-Z0Z8H9] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001372

许先生 您好:

调整对象审核策略**不会影响**审计 hosts 文件。

开启对象访问策略后，当符合审核条件时会生成 4663 事件，但是**对象访问审核策略有很多类别，如审核内核对象、审核注册表、审核文件系统等。**

而**审计 hosts 文件是属于审核文件系统类别**，我们只是调整**关闭了审核内核对象和审核注册表**，减少多余的 4663 事件生成，并**不会影响到审核文件系统**的 4663 事件，不会影响审计 hosts 文件。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Windows Server 技术支持 <windowsserversupport@sdc.icbc.com.cn>
发送时间: 2022 年 9 月 17 日 17:41
收件人: Wei Liang <weiliang@cmgos.com>
主题: 回复: 回复: 回复: 回复:【外来邮件，注意核实】回复: [案例号: CAS-06619-Z0Z8H9] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001372

危老师，这个方案会不会影响我们审计 hosts 文件呢。后面我们进行了 4663 触发的优化，也改成本地运行 checkhosts 脚本。

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

中国工商银行软件开发中心（珠海）
许 翔
系统一部

电话：17606669571

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

-----原始邮件-----

发件人: "Wei Liang" <weiliang@cmgos.com>
发送时间: 2022-09-16 19:19:58
收件人: "hy1198809722@163.com" <hy1198809722@163.com>
抄送: "win10 技术支持" <win10 技术支持.软件开发中心系统一部@工商银行.icbc>,"ICBC_Notification" <icbc_notification@cmgos.com>,"qiyq@sdc.icbc.com.cn" <戚云琪.杭州研发部杭州开发一部@工商银行.icbc>,"Windows Server 技术支持" <windowsserver 技术支持.软件开发中心系统一部@工商银行.icbc>
主题: 回复: 回复: 回复:【外来邮件，注意核实】回复: [案例号: CAS-06619-Z0Z8H9] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001372

黄先生 您好:

感谢您的电话接听。

从 dump 中的情况看，有以下几个问题:

1）有进程等待在 smb 上，在等待访问 CheckHosts.exe 应用。

2）RPCSS 服务中有多个线程等待在 DCOM Launch 服务，但是三方驱动 krnlmgr.sys 注册了 PspCallProcessNotifyRoutines，所以一直等待在它上面。经过确认 krnlmgr.sys 是 TMS 的驱动，无法回退或者临时卸载。

下一步建议：

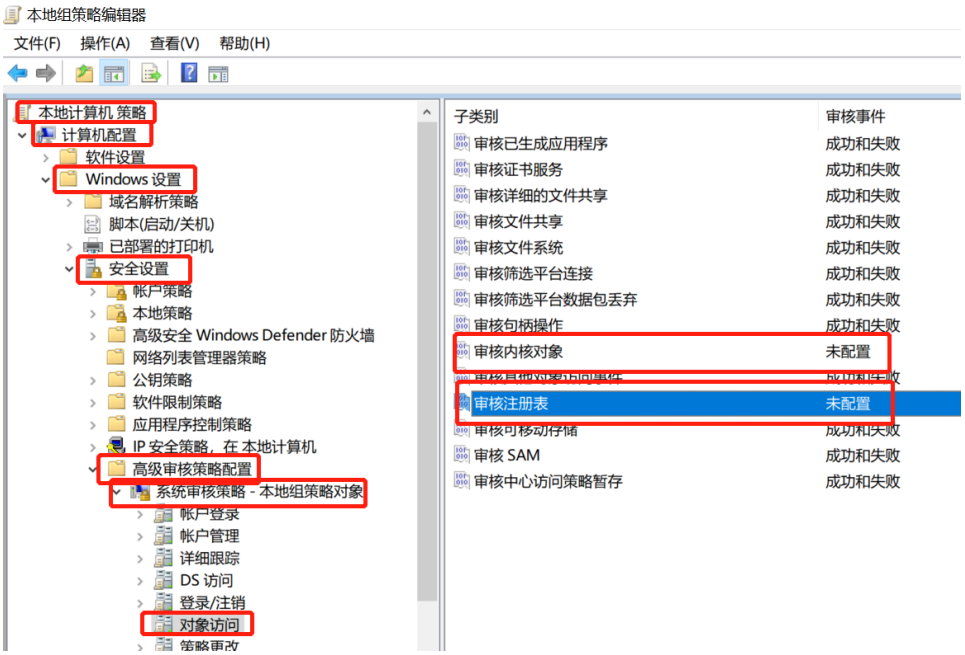
结合 T490s 设备也出现了类似问题，请进行以下配置修改相关设置并更新有线和无线网卡驱动，再观察是否再次复现问题。

1、在本地修改一些对象的审核策略，减少 4663 事件的生成，**具体操作如下：**

a）以**管理员权限**运行 gpedit.msc，打开**本地组策略编辑器**，定位到：

“本地计算机策略”-“计算机配置”-“Windows 设置”-“安全设置”-“高级审核策略”-“系统审核策略-本地组策略对象”-“对象访问”，

b）修改**“审核内核对象”**和**“审核注册表”**为**“未配置”**状态。



2、更新有线网卡和无线网卡驱动，可以访问以下链接从联想官网下载对应的驱动：

有线网卡驱动：

https://think.lenovo.com.cn/support/driver/driverdetail.aspx?DEditid=98449&docTypeID=DOC_TYPE_DRIVER&driverID=undefined&treeid=3114897&args=%3Fcategoryid%3D3114897%26CODEName%3D20T1%26SearchType%3D1%26wherePage%3D%25202%26SearchNodeCC%3DThinkPad%2520t14s%26needmt%3D20T1%26osid%3D42

无线网卡驱动：

https://think.lenovo.com.cn/support/driver/driverdetail.aspx?DEditid=96868&docTypeID=DOC_TYPE_DRIVER&driverID=undefined&treeid=3114897&args=%3Fcategoryid%3D3114897%26CODEName%3D20T1%26SearchType%3D1%26wherePage%3D%25202%26SearchNodeCC%3DThinkPad%2520t14s%26needmt%3D20T1%26osid%3D42

3、暂时卸载禁用 ThinkVantage Active Protection System 驱动，打开注册表编辑器，定位到：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services**ApsX64**，将 start 键值修改为 **4**

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services**ApsHM64**，将 start 键值修改为 **4**

禁用 ApsX64 和 ApsHM64 驱动，重启计算机生效。

dump 具体分析：

有进程等待在 smb 上

```
0: kd> !mex.t ffffd703034c8040
Process                 Thread                          CID       UserTime KernelTime ContextSwitches Wait Reason       Time State
System (ffffd702fea5e300) ffffd703034c8040  (E|K|W|R|V) 4.1b0            0  1m:50.109          406376 Executive    26m:00.156 Waiting

WaitBlockList:
    Object                Name                            Type              Other Waiters
    ffffd7034adfdd90(SmXc)    @\0  <TRUNCATED 28686 CHARS> NotificationEvent            0
    ffffd70313ada180(
Irp List:
    IRP              File                                                                                  Driver
    ffffd7034461c010 \KFZXBADM191.Intranet.ICBC.COM.CN\SYSVOL\INTRANET.ICBC.COM.CN\SCRIPTS\CHECKHOSTS.EXE mrxsmb

Priority:
    Current Base Decrement ForegroundBoost IO Page
    9       8    0         16              0  5

 # Child-SP         Return           Call Site
 0 fffff3059a67f970 fffff8001890c5d7 nt!KiSwapContext+0x76
 1 fffff3059a67fab0 fffff8001890c149 nt!KiSwapThread+0x297
 2 fffff3059a67fb70 fffff80018909e12 nt!KiCommitThreadWait+0x549
 3 fffff3059a67fc10 fffff80018f56af1 nt!KeWaitForMultipleObjects+0x582
 4 fffff3059a67fce0 fffff800278011b3 nt!FsRtlCancellableWaitForMultipleObjects+0x91
 5 fffff3059a67fd50 fffff8002789aefe mrxsmb!SmbCeWaitForCompletionAndFinalizeExchangeEx+0x1a3
 6 fffff3059a67fe20 fffff80027817512 mrxsmb20!MRxSmb2Create+0xc6e
 7 fffff3059a67ff50 fffff80018a595ee mrxsmb!SmbpShellCreateWithNewStack+0x22
 8 fffff3059a67ff80 fffff80018a595ac nt!KxSwitchKernelStackCallout+0x2e
 9 fffff305924ce570 fffff800188d0626 nt!KiSwitchKernelStackContinue
```

RPCSS 服务中有很多进程在等待 Dcom Launch 服务

```
0: kd> !mex.lt ffffd70309f6b440
Process           PID Thread             Id State              Time Reason      Waiting On
================= === ================ ==== ======= ============== ========== ==========================================================================
svchost.exe (-p)  560 ffffd70309e03080  564 Waiting       8m:28.859 UserRequest
svchost.exe (-p)  560 ffffd70309f61640  570 Waiting          2s.718 WrQueue
svchost.exe (-p)  560 ffffd70309e5b240  578 Waiting         13s.625 UserRequest
svchost.exe (-p)  560 ffffd70309f64240  57c Waiting       8m:28.625 WrQueue
svchost.exe (-p)  560 ffffd7030a521080  834 Waiting 4d.09:43:19.109 UserRequest
svchost.exe (-p)  560 ffffd703113e5080 19f0 Waiting         28s.000 UserRequest
svchost.exe (-p)  560 ffffd703111c5080 4264 Waiting         28s.000 UserRequest
svchost.exe (-p)  560 ffffd7033fa45080 43cc Waiting      23m:52.218 WrLpcReply  Thread: ffffd70341e03080 in svchost.exe (-p) (0n1228)
svchost.exe (-p)  560 ffffd7034fe55080 4d44 Waiting       5m:23.062 WrLpcReply  Thread: ffffd7033a7d4080 in svchost.exe (-p) (0n1228)
svchost.exe (-p)  560 ffffd7034fe9b080 400c Waiting          50s.484 WrQueue
svchost.exe (-p)  560 ffffd7033e346080 1b2c Waiting       7m:05.968 WrLpcReply  Thread: ffffd7031ef4c040 in svchost.exe (-p) (0n1228)
svchost.exe (-p)  560 ffffd7033e355080  5d8 Waiting       6m:34.921 UserRequest Mutex: ffffd7030f348ba0 Owning Thread: ffffd7033e346080 (svchost
svchost.exe (-p)  560 ffffd7031ef3e080  a84 Waiting       8m:24.437 WrLpcReply  Thread: ffffd703238cf080 in svchost.exe (-p) (0n1228)
svchost.exe (-p)  560 ffffd7034584d080  ca0 Waiting       4m:55.781 UserRequest Mutex: ffffd7030f348ba0 Owning Thread: ffffd7033e346080 (svchost
svchost.exe (-p)  560 ffffd70334bae040 2ebc Waiting       1m:04.656 WrLpcReply  Thread: ffffd703479cf080 in svchost.exe (-p) (0n1228)
svchost.exe (-p)  560 ffffd7034bae0080 2ce0 Waiting           343ms WrQueue

Thread Count: 16
```

三方驱动 krnlmgr 注册在 PspCallProcessNotifyRoutines 上，一直在等待，从 krnlmgr 的函数名称 krnlmgr!IsProtectFile 可能是在对文件做一些检查操作。

```
0: kd> !mex.t ffffd7031ef4c040
Process                           Thread                           CID       TEB              UserTime KernelTime ContextSwitches
svchost.exe (-p) (ffffd70309e0f3c0) ffffd7031ef4c040 (E|K|W|R|V) 4cc.408c  000000886243c000        0       16ms             1,46

WaitBlockList:
    Object                Type              Other Waiters
    ffffd7031e1ff3f0(mnti) NotificationEvent             0

 # Child-SP         Return           Call Site
 0 fffff30599cde640 fffff8001890c5d7 nt!KiSwapContext+0x76
 1 fffff30599cde780 fffff8001890c149 nt!KiSwapThread+0x297
 2 fffff30599cde840 fffff8001890aed0 nt!KiCommitThreadWait+0x549
 3 fffff30599cde8e0 fffff8001ea77a7d nt!KeWaitForSingleObject+0x520
 4 fffff30599cde9b0 fffff8001ea76aee krnlmgr!QueryProcInformaionById+0x279d
 5 fffff30599cdea00 fffff8001ea75c35 krnlmgr!QueryProcInformaionById+0x180e
 6 fffff30599cdea90 fffff8001ea8f3e2 krnlmgr!QueryProcInformaionById+0x955
 7 fffff30599cdeb20 fffff80018e9df6d krnlmgr!IsProtectFile+0xfcf2
 8 fffff30599cdeb60 fffff80018ea15fa nt!PspCallProcessNotifyRoutines+0x249
 9 fffff30599cdec30 fffff80018e78a8e nt!PspInsertThread+0x04a
 a fffff30599cdecf0 fffff80018a67005 nt!NtCreateUserProcess+0x88e
 b fffff30599cdf990 00007ffa2c9f1244 nt!KiSystemServiceCopyEnd+0x25
 c 0000008862c7cbf8 00007ffa297f8842 ntdll!NtCreateUserProcess+0x14
 d 0000008862c7cc00 00007ffa297f53d3 KERNELBASE!CreateProcessInternalW+0x1f12
```

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2022 年 9 月 9 日 11:21
收件人: 'qiyq@sdc.icbc.com.cn' <qiyq@sdc.icbc.com.cn>; 'Windows Server 技术支持' <windowsserversupport@sdc.icbc.com.cn>
抄送: 'win10 升级支持' <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: 回复: 回复:【外来邮件，注意核实】回复: [案例号：CAS-06619-Z0Z8H9] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001372

戚先生、许先生 你们好：

感谢电话接听。

针对 T490s 这台设备，戚先生您确认近期未复现问题，我们再持续观察一段时间此设备的运行情况。

T14s 这台设备最近的 dump 文件已经收到，请许先生 @'Windows Server 技术支持' 与用户沟通此次出现问题时的场景，如问题的具体现象，在进行什么操作时出现问题等，这对我们的问题排查很有帮助。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2022 年 9 月 1 日 17:36
收件人: 'qiyq@sdc.icbc.com.cn' <qiyq@sdc.icbc.com.cn>; 'Windows Server 技术支持' <windowsserversupport@sdc.icbc.com.cn>
抄送: 'win10 升级支持' <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: 回复: 回复:【外来邮件，注意核实】回复: [案例号: CAS-06619-Z0Z8H9] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001372

戚先生、许先生 你们好:

感谢电话接听。

针对 T490s 这台设备，请您尝试以下操作，再观察后续情况。

1）尝试更新网卡驱动到最新版本。您可以通过以下链接从联想官网下载最新的网卡驱动更新。

https://think.lenovo.com.cn/support/driver/driverdetail.aspx?DEditid=97931&docTypeID=DOC_TYPE_DRIVER&driverID=undefined&treeid=13850&args=%3Fcategoryid%3D13850%26CODEName%3DThinkPad%2520T490s%26SearchType%3D0%26wherePage%3D2

2）暂时卸载禁用 ThinkVantage Active Protection System 驱动，打开注册表编辑器，定位到:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services**ApsX64**，将 start 键值修改为 **4**

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services**ApsHM64**，将 start 键值修改为 **4**

禁用 ApsX64 和 ApsHM64 驱动，重启计算机生效。

3）如果想追踪 DNS cache 的行为，请将以下命令**保存到文本文档中并保存为 bat** 文件，以**管理员权限运行并重启计算机**生效。它会在内存中记录 DNS cache 的行为，可以在下次生成 dump 时分析。

```
logman create trace "autosession\minio_dns" -ow -o c:\minio_dns.etl -p "Microsoft-Windows-DNS-Client" 0xffffffffffffffff 0xff -nb 400 400 -bs 1024 -mode BufferOnly -max 1024 -ets
logman update trace "autosession\minio_dns" -p {1540FF4C-3FD7-4BBA-9938-1D1BF31573A7} 0xffffffffffffffff 0xff -ets
logman update trace "autosession\minio_dns" -p {609151DD-04F5-4DA7-974C-FC6947EAA323} 0xffffffffffffffff 0xff -ets
logman update trace "autosession\minio_dns" -p {9CA335ED-C0A6-4B4D-B084-9C9B5143AFF0} 0xffffffffffffffff 0xff -ets
logman update trace "autosession\minio_dns" -p {F230B1D5-7DFD-4DA7-A3A3-7E87B4B00EBF} 0xffffffffffffffff 0xff -ets
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\minio_dns /v FileMax /t REG_DWORD /d 2 /f
```

针对 T14s 设备，确认近期是否再次出现问题。并进行以下操作，观察是否规避问题。

1）以管理员权限运行如下 cmd 命令，

```
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters /v IoTimeoutForCAShare /t REG_DWORD /d 1 /f
```

2）**重启计算机生效**，并观察是否能规避问题。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.

服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

神州网信 CMIT

发件人: Wei Liang
发送时间: 2022 年 8 月 31 日 17:58
收件人: 'qiyq@sdc.icbc.com.cn' <qiyq@sdc.icbc.com.cn>; 'Windows Server 技术支持' <windowsserversupport@sdc.icbc.com.cn>
抄送: 'win10 升级支持' <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: 回复: 回复:【外来邮件，注意核实】回复: [案例号：CAS-06619-Z0Z8H9] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001372

戚先生、许先生 你们好：

查看提供的 0807、0822 两次在锁屏界面卡死的 dump 文件，查看对应的 winlogon 进程在处理 unlocking，但是有一个等待链，最终等待在 dnscache 服务上，在尝试解析内网某个域名。

在 dump 中查看网络情况，显示无线网卡和 VPN 的虚拟网卡都处于连接状态。不过从 dump 中无法查询到本地网络以及 VPN 的连通情况。

0822 的 dump 中显示有 apsx64.sys 驱动挂起了磁盘的写操作，经查询这个驱动是 ThinkVantage Active Protection System 的驱动，这个驱动是 2018 年年底的。

昨天获取的另一台设备 T14s 的 memory.dmp 显示在连接共享时无法解析连接到对应的共享目录，最后出现了问题。这台设备出现问题时没有网络连接，怀疑这个问题可能与持久处理（Persistent Handlers）有关。

下一步建议：

针对戚先生的 T490s 设备：

1）尝试更新网卡驱动到最新版本。
2）暂时卸载禁用 ThinkVantage Active Protection System 驱动或者更新到最新版。

3）如果想追踪 DNS cache 的行为，请将以下命令**保存到文本文档中并保存为 bat** 文件，以**管理员权限运行并重启计算机**生效。它会在内存中记录 DNS cache 的行为，可以在下次生成 dump 时分析。

```
logman create trace "autosession\minio_dns" -ow -o c:\minio_dns.etl -p "Microsoft-Windows-DNS-Client" 0xffffffffffffffff 0xff -nb 400 400 -bs 1024 -mode BufferOnly -max 1024 -ets
logman update trace "autosession\minio_dns" -p {1540FF4C-3FD7-4BBA-9938-1D1BF31573A7} 0xffffffffffffffff 0xff -ets
logman update trace "autosession\minio_dns" -p {609151DD-04F5-4DA7-974C-FC6947EAA323} 0xffffffffffffffff 0xff -ets
logman update trace "autosession\minio_dns" -p {9CA335ED-C0A6-4B4D-B084-9C9B5143AFF0} 0xffffffffffffffff 0xff -ets
logman update trace "autosession\minio_dns" -p {F230B1D5-7DFD-4DA7-A3A3-7E87B4B00EBF} 0xffffffffffffffff 0xff -ets
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\minio_dns /v FileMax /t REG_DWORD /d 2 /f
```

针对另一台 T14s 设备：

1）以管理员权限运行如下 cmd 命令，

```
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters /v IoTimeoutForCAShare /t REG_DWORD /d 1 /f
```

2）**重启计算机生效**，并观察是否能规避问题。

具体分析：

查看 winlogon 情况，正在处理 unlocking，但是有等待链：

winlogon->UserManager->lsass->Dnscache

```
0: kd> !mex.t ffffb30fa2091080
Process                           Thread                          CID       TEB              UserTime KernelTime ContextSwitches Wait
winlogon.exe (ffffb30f9fe8d100) ffffb30fa2091080 (E|K|W|R|V) 128.5a0   000000453e8ff000     172ms      5s.750           14277 WrLpcR

WaitBlockList:
    Object           Type      Other Waiters Info
    ffffb30fa20916c8 Semaphore             0 Limit: 1

Priority:
    Current Base Decrement ForegroundBoost IO Page
    13      13   0         0               0  5

LPC Msg          ServerProcess                                 ServerThread
ffffca0b5ffd3720 svchost.exe (UserManager)(ffffb30fa28b7080) ffffb30fc7432080

 # Child-SP          Return           Call Site
 0 ffffc584704c7350 fffff8065d7245d7 nt!KiSwapContext+0x76
 1 ffffc584704c7490 fffff8065d724149 nt!KiSwapThread+0x297
 2 ffffc584704c7550 fffff8065d722ed0 nt!KiCommitThreadWait+0x549
 3 ffffc584704c75f0 fffff8065d6fc632 nt!KeWaitForSingleObject+0x520
 4 ffffc584704c76c0 fffff8065dc9f286 nt!AlpcpSignalAndWait+0x222
 5 ffffc584704c7760 fffff8065dc9ed95 nt!AlpcpReceiveSynchronousReply+0x56
 6 ffffc584704c77c0 fffff8065dc9d1c2 nt!AlpcpProcessSynchronousRequest+0x3a5
 7 ffffc584704c78d0 fffff8065d87f005 nt!NtAlpcSendWaitReceivePort+0x1e2
 8 ffffc584704c7990 00007ff9c6f00b24 nt!KiSystemServiceCopyEnd+0x25
 9 000000453ecfe758 00007ff9c44ac542 ntdll!NtAlpcSendWaitReceivePort+0x14
 a 000000453ecfe760 00007ff9c44a9a91 RPCRT4!LRPC_BASE_CCALL::DoSendReceive+0x112
 b 000000453ecfe810 00007ff9c4559169 RPCRT4!LRPC_CCALL::SendReceive+0x51
 c 000000453ecfe860 00007ff9c4557a51 RPCRT4!NdrpClientCall3+0xdf9
 d 000000453ecfec10 00007ff9b4e31667 RPCRT4!NdrClientCall3+0xf1
 e 000000453ecfefa0 00007ff9b4e3145b usermgrcli!<lambda_b79cc596b12b90f9c2d70da39ec59573>::operator()+0x1d7
 f 000000453ecff130 00007ff9b4e3142a usermgrcli!DoRpcCall<<lambda_b79cc596b12b90f9c2d70da39ec59573> >+0x1f
10 000000453ecff170 00007ff62453ce05 usermgrcli!UMgrLogonUser+0xfa
11 000000453ecff2a0 00007ff6245132d4 winlogon!AuthenticateUser+0x555
12 000000453ecff880 00007ff62452387b winlogon!WLGeneric_Unlocking_Execute+0x1d4
13 000000453ecffaf0 00007ff9c6ecbb10 winlogon!StateMachineWorkerCallback+0x4b
14 000000453ecffb20 00007ff9c6e76964 ntdll!TppWorkpExecuteCallback+0x130
15 000000453ecffb70 00007ff9c6527974 ntdll!TppWorkerThread+0x644
16 000000453ecffe60 00007ff9c6eba2f1 KERNEL32!BaseThreadInitThunk+0x14
17 000000453ecffe90 0000000000000000 ntdll!RtlUserThreadStart+0x21

0: kd> !mex.t ffffb30fc7432080
Process                          Thread                          CID       TEB              UserTime KernelTime ContextSwitches Wa
svchost.exe (UserManager) (ffffb30fa28b7080) ffffb30fc7432080 (E|K|W|R|V) be4.2100  000000a5f2dbf000     16ms       31ms             525 Wr

WaitBlockList:
    Object           Type      Other Waiters Info
    ffffb30fc74326c8 Semaphore             0 Limit: 1

Priority:
    Current Base Decrement ForegroundBoost IO Page
    13      8    0         0               0  5

LPC Msg          ServerProcess                ServerThread
ffffca0b67fae040 lsass.exe(ffffb30f9feb44c0) ffffb30fc7897080

 # Child-SP          Return           Call Site
 0 ffffc584721a7350 fffff8065d7245d7 nt!KiSwapContext+0x76
 1 ffffc584721a7490 fffff8065d724149 nt!KiSwapThread+0x297
 2 ffffc584721a7550 fffff8065d722ed0 nt!KiCommitThreadWait+0x549
 3 ffffc584721a75f0 fffff8065d6fc632 nt!KeWaitForSingleObject+0x520
 4 ffffc584721a76c0 fffff8065dc9f286 nt!AlpcpSignalAndWait+0x222
 5 ffffc584721a7760 fffff8065dc9ed95 nt!AlpcpReceiveSynchronousReply+0x56
 6 ffffc584721a77c0 fffff8065dc9d1c2 nt!AlpcpProcessSynchronousRequest+0x3a5
 7 ffffc584721a78d0 fffff8065d87f005 nt!NtAlpcSendWaitReceivePort+0x1e2
 8 ffffc584721a7990 00007ff9c6f00b24 nt!KiSystemServiceCopyEnd+0x25
 9 000000a5f327df08 00007ff9c44ac542 ntdll!NtAlpcSendWaitReceivePort+0x14
 a 000000a5f327df10 00007ff9c44a9a91 RPCRT4!LRPC_BASE_CCALL::DoSendReceive+0x112
 b 000000a5f327dfc0 00007ff9c4559169 RPCRT4!LRPC_CCALL::SendReceive+0x51
```

```
0: kd> !mex.t ffffb30fc7897080
Process                 Thread                  CID       TEB              UserTime KernelTime ContextSwit
lsass.exe (ffffb30f9feb44c0) ffffb30fc7897080 (E|K|W|R|V) 408.3b40  000000f6ba5ca000   4s.891     1s.047           1

WaitBlockList:
    Object           Type      Other Waiters Info
    ffffb30fc78976c8 Semaphore             0 Limit: 1

Priority:
    Current Base Decrement ForegroundBoost IO Page
    13      9    0         0               0  5

LPC Msg          ServerProcess                          ServerThread
ffffca0b5eb62690 svchost.exe (Dnscache)(ffffb30fa220f080) ffffb30fc76d5080

 # Child-SP          Return           Call Site
 0 ffffc5847733a350 fffff8065d7245d7 nt!KiSwapContext+0x76
 1 ffffc5847733a490 fffff8065d724149 nt!KiSwapThread+0x297
 2 ffffc5847733a550 fffff8065d722ed0 nt!KiCommitThreadWait+0x549
 3 ffffc5847733a5f0 fffff8065d6fc632 nt!KeWaitForSingleObject+0x520
 4 ffffc5847733a6c0 fffff8065dc9f286 nt!AlpcpSignalAndWait+0x222
 5 ffffc5847733a760 fffff8065dc9ed95 nt!AlpcpReceiveSynchronousReply+0x56
 6 ffffc5847733a7c0 fffff8065dc9d1c2 nt!AlpcpProcessSynchronousRequest+0x3a5
 7 ffffc5847733a8d0 fffff8065d87f005 nt!NtAlpcSendWaitReceivePort+0x1e2
 8 ffffc5847733a990 00007ff9c6f00b24 nt!KiSystemServiceCopyEnd+0x25
 9 000000f680478fc8 00007ff9c44a983f ntdll!NtAlpcSendWaitReceivePort+0x14
 a 000000f680478fd0 00007ff9c4559169 RPCRT4!LRPC_BASE_CCALL::SendReceive+0x12f
 b 000000f6804790a0 00007ff9c4557a51 RPCRT4!NdrpClientCall3+0xdf9
 c 000000f680479450 00007ff9c237f006 RPCRT4!NdrClientCall3+0xf1
 d 000000f6804797e0 00007ff9c237c8fc DNSAPI!Rpc_ResolverQuery+0xf6
 e 000000f6804798f0 00007ff9c237c0fe DNSAPI!Query_PrivateExW+0x79c
 f 000000f68047a130 00007ff9c2612c66 DNSAPI!DnsQueryEx+0x16e
10 000000f68047a2b0 00007ff9c2612a39 mswsock!SaBlob_Query+0xaa
11 000000f68047a380 00007ff9c2612217 mswsock!Rnr_DoDnsLookup+0x1c5
12 000000f68047a430 00007ff9c633918f mswsock!Dns_NSPLookupServiceNext+0x1d7
13 000000f68047a7a0 00007ff9c6339053 WS2_32!NSQUERY::LookupServiceNext+0xeb
14 000000f68047a8a0 00007ff9c6338d4a WS2_32!WSALookupServiceNextW+0xd3
15 000000f68047a8f0 00007ff9c6336590 WS2_32!QueryDnsForFamily+0x1ae
16 000000f68047b2a0 00007ff9c63341d6 WS2_32!QueryDns+0x170
17 000000f68047b360 00007ff9c6333956 WS2_32!LookupAddressForName+0x122
18 000000f68047b470 00007ff9c24e79c1 WS2_32!GetAddrInfoW+0x226
19 000000f68047b610 00007ff9c24b674d netlogon!NetpSrvNextEx+0x1ffc1
```

查看 lsass 通过 DNS 查询域名 **gyjdbadm192.intranet.icbc.com.cn**

```
0: kd> .frame /r 0x16; !mex.x
16 000000f6`8047b2a0 00007ff9`c63341d6 WS2_32!QueryDns+0x170
rax=0000000000000000 rbx=0000000000000000 rcx=0000000000000000
rdx=0000000000000000 rsi=0000000000000003 rdi=000000f68047b3e0
rip=00007ff9c6336590 rsp=000000f68047b2a0 rbp=00000214046a5a20
 r8=0000000000000000  r9=0000000000000000 r10=0000000000000000
r11=0000000000000000 r12=0000000000206003 r13=00000214046a5a20
r14=000000f68047b3c8 r15=000000f68047b3cc
iopl=0         nv up di pl nz na pe nc
cs=0000  ss=0000  ds=0000  es=0000  fs=0000  gs=0000             efl=00000000
WS2_32!QueryDns+0x170:
00007ff9`c6336590 8bd8            mov     ebx,eax
0: kd> db 00000214046a5a20
00000214`046a5a20  67 00 79 00 6a 00 64 00-62 00 61 00 64 00 6d 00  g.y.j.d.b.a.d.m.
00000214`046a5a30  31 00 39 00 32 00 2e 00-69 00 6e 00 74 00 72 00  1.9.2...i.n.t.r.
00000214`046a5a40  61 00 6e 00 65 00 74 00-2e 00 69 00 63 00 62 00  a.n.e.t...i.c.b.
00000214`046a5a50  63 00 2e 00 63 00 6f 00-6d 00 2e 00 63 00 6e 00  c...c.o.m...c.n.
00000214`046a5a60  00 00 00 00 00 00 00 00-00 00 71 00 00 00 0c 00  ..........q.....
00000214`046a5a70  00 51 55 04 14 02 00 00-20 78 cb 03 14 02 00 00  .QU..... x......
00000214`046a5a80  c0 92 79 04 14 02 00 00-00 00 00 00 00 00 00 00  ..y.............
00000214`046a5a90  57 55 31 1e 00 00 00 00-00 00 00 00 a5 99 2d 11  WU1...........-.
```

查看此时设备的网络状况，无线网卡和 VPN 都处于连接状态：

```
MINIPORT

    Intel(R) Wireless-AC 9560 160MHz

    Ndis handle         ffffb30f9af611a0
    Ndis API version    v6.60
    Adapter context     ffffb30fc78a5050
    Driver              ffffb30f9830aa90 - Netwtw08  v2.1
    Network interface   ffffb30f9a18d8a0

    Media type          802.3
    Physical medium     Native802.11
    Device instance     PCI\VEN_8086&DEV_9DF0&SUBSYS_00348086&REV_30\3&11583659&2&A3
    Device object       ffffb30f9af61050    More information
    MAC address         94-e6-f7-49-a8-f4

STATE

    Miniport            Running
    Device PnP          Started             Show state history
    Datapath            Normal
    Interface           Up
    Media               Connected
    Power               D0
    References          0x22                Show detail
    Total resets        0

MINIPORT

    Sangfor SSL VPN CS Support System VNIC

    Ndis handle         ffffb30f9ad031a0
    Ndis API version    v5.0
    Adapter context     ffffb30f9e904010
    Driver              ffffb30f9ac52a40 - SangforVnic  v0.257
    Network interface   ffffb30f9a19f8a0

    Media type          802.3
    Physical medium     NdisPhysicalMediumUnspecified
    Device instance     ROOT\NET\0000
    Device object       ffffb30f9ad03050    More information
    MAC address         00-ff-a1-4a-73-81

STATE

    Miniport            Running
    Device PnP          Started             Show state history
    Datapath            Normal
    Interface           Up
    Media               Connected
    Power               D0
    References          0x10                Show detail
    Total resets        0
    Pending OID         None
```

查看系统资源!locks 的情况，两个线程都有 apsx64 介入了磁盘的写操作。

```
0: kd> !mex.t ffffb30f988c1040
Process                 Thread                  CID       UserTime KernelTime ContextSwitches Wait Reason Time State
System (ffffb30f98281080) ffffb30f988c1040 (E|K|W|R|V) 4.d4             0       63ms            2373 Executive      0 Waiting

WaitBlockList:
    Object                Type              Other Waiters
    ffffb30f9a39d080(PFXM) NotificationEvent            0

Irp List:
    IRP              File Driver
    ffffb30fc5f6f970      Disk

Priority:
    Current Base Decrement ForegroundBoost IO Page
    15      15   0         0               0  5

 # Child-SP         Return           Call Site                                                Source
 0 ffffc58476e7ece0 fffff8065d7245d7 nt!KiSwapContext+0x76
 1 ffffc58476e7ee20 fffff8065d724149 nt!KiSwapThread+0x297
 2 ffffc58476e7eee0 fffff8065d722ed0 nt!KiCommitThreadWait+0x549
 3 ffffc58476e7ef80 fffff8065d6f6a7e nt!KeWaitForSingleObject+0x520
 4 ffffc58476e7f050 fffff8065d6f6984 nt!PopFxActivateComponent+0xbe
 5 ffffc58476e7f0e0 fffff80663509e8e nt!PoFxActivateComponent+0x44
 6 ffffc58476e7f110 fffff806635096b9 storport!RaidStartIoPacket+0x54e
 7 ffffc58476e7f220 fffff8066350945a storport!RaUnitScsiIrp+0x219
 8 ffffc58476e7f2c0 fffff8065d730d79 storport!RaDriverScsiIrp+0x5a
 9 ffffc58476e7f300 fffff806635b59f5 nt!IofCallDriver+0x59
 a ffffc58476e7f340 fffff80662eb1c4e EhStorClass!FilterDeviceEvtWdmIoctlIrpPreprocess+0x265
 b (Inline)         ---------------- Wdf01000!PreprocessIrp+0x2e                              minkernel\wdf\framework\shared\c
 c (Inline)         ---------------- Wdf01000!DispatchWorker+0x179                            minkernel\wdf\framework\shared\c
 d (Inline)         ---------------- Wdf01000!FxDevice::Dispatch+0x197                        minkernel\wdf\framework\shared\c
 e ffffc58476e7f390 fffff8065d730d79 Wdf01000!FxDevice::DispatchWithLock+0x1ee               minkernel\wdf\framework\shared\c
 f ffffc58476e7f3f0 fffff806645e8b9f nt!IofCallDriver+0x59
10 ffffc58476e7f430 fffff8065d730d79 devmgr+0x18b9f
11 ffffc58476e7f480 fffff80664567658 nt!IofCallDriver+0x59
12 ffffc58476e7f4c0 fffff806645669e9 CLASSPNP!SubmitTransferPacket+0x2c8
13 ffffc58476e7f500 fffff806645667b3 CLASSPNP!ServiceTransferRequest+0x209
14 ffffc58476e7f590 fffff80664561404 CLASSPNP!ClassReadWrite+0x2d3
15 ffffc58476e7f5e0 fffff8065d730d79 CLASSPNP!ClassGlobalDispatch+0x24
16 ffffc58476e7f610 fffff80663311c94 nt!IofCallDriver+0x59
17 ffffc58476e7f650 fffff80663311f21 partmgr!PmWrite+0x174
18 ffffc58476e7f6d0 fffff8065d730d79 partmgr!PmGlobalDispatch+0x21
19 ffffc58476e7f700 fffff80664bc3da2 nt!IofCallDriver+0x59
1a ffffc58476e7f740 fffff80664bc223d ApsX64+0x3da2
1b ffffc58476e7f770 fffff80664bc1070 ApsX64+0x223d
```


```
18 ffffc58476e7f6d0 fffff8065d730d79 partmgr!PmGlobalDispatch+0x21
19 ffffc58476e7f700 fffff80664bc3da2 nt!IofCallDriver+0x59
1a ffffc58476e7f740 fffff80664bc223d ApsX64+0x3da2
1b ffffc58476e7f770 fffff80664bc1070 ApsX64+0x223d
1c ffffc58476e7f800 fffff8065d730d79 ApsX64+0x1070
1d ffffc58476e7f830 fffff80663311a8d nt!IofCallDriver+0x59
1e ffffc58476e7f870 fffff8066331189e partmgr!PartitionIo+0x1dd
1f ffffc58476e7f920 fffff80663311f21 partmgr!PartitionWrite+0x1e
20 ffffc58476e7f950 fffff8065d730d79 partmgr!PmGlobalDispatch+0x21
21 ffffc58476e7f980 fffff80663401af9 nt!IofCallDriver+0x59
22 ffffc58476e7f9c0 fffff8065d730d79 volmgr!VmReadWrite+0xf9
23 ffffc58476e7fa00 fffff80664b03a23 nt!IofCallDriver+0x59
24 ffffc58476e7fa40 fffff80664b0305c fvevol!FveFilterRundownReadWrite+0x953
25 ffffc58476e7fb40 fffff8065d730d79 fvevol!FveFilterRundownWrite+0x4c
26 ffffc58476e7fbe0 fffff80664503ca3 nt!IofCallDriver+0x59
27 ffffc58476e7fc20 fffff80664504e48 iorate!IoRateIssueAndRecordIo+0x7f
28 ffffc58476e7fc60 fffff80664505020 iorate!IoRateProcessIrpWrapper+0x180
29 ffffc58476e7fd70 fffff8065d730d79 iorate!IoRateDispatchReadWrite+0x80
2a ffffc58476e7fdb0 fffff80664401033 nt!IofCallDriver+0x59
2b ffffc58476e7fdf0 fffff8065d730d79 volume!VolumePassThrough+0x23
2c ffffc58476e7fe20 fffff806644114e9 nt!IofCallDriver+0x59
2d ffffc58476e7fe60 fffff806644113b3 volsnap!VolsnapWriteFilter+0x119
2e ffffc58476e7fee0 fffff8065d730d79 volsnap!VolSnapWrite+0x13
2f ffffc58476e7ff10 fffff806637e038c nt!IofCallDriver+0x59
30 ffffc58476e7ff50 fffff8065d8715ee Ntfs!NtfsStorageDriverCallout+0x1c
31 ffffc58476e7ff80 fffff8065d8715ac nt!KxSwitchKernelStackCallout+0x2e
32 ffffc5846fbf1ba0 fffff8065d6e8636 nt!KiSwitchKernelStackContinue
33 ffffc5846fbf1bc0 fffff8065d6e837c nt!KiExpandKernelStackAndCalloutOnStackSegment+0x256
34 ffffc5846fbf1c50 fffff8065d6e81f3 nt!KiExpandKernelStackAndCalloutSwitchStack+0xdc
35 ffffc5846fbf1cc0 fffff8065d6e81ad nt!KeExpandKernelStackAndCalloutInternal+0x33
36 ffffc5846fbf1d30 fffff806637c61d9 nt!KeExpandKernelStackAndCalloutEx+0x1d
37 ffffc5846fbf1d70 fffff806637c4f9d Ntfs!NtfsMultipleAsync+0xe9
38 ffffc5846fbf1de0 fffff806637d277c Ntfs!NtfsNonCachedIo+0x3dd
39 ffffc5846fbf2070 fffff806637d1aad Ntfs!NtfsCommonWrite+0xa3c
3a ffffc5846fbf22a0 fffff8065d730d79 Ntfs!NtfsFsdWrite+0x1ed
3b ffffc5846fbf2360 fffff80662e3624e nt!IofCallDriver+0x59
3c ffffc5846fbf23a0 fffff80662e34a66 FLTMGR!FltpLegacyProcessingAfterPreCallbacksCompleted+0x28e
3d ffffc5846fbf2410 fffff8065d730d79 FLTMGR!FltpDispatch+0xb6
3e ffffc5846fbf2470 fffff8065dcd66c1 nt!IofCallDriver+0x59
3f ffffc5846fbf24b0 fffff8065dc693ed nt!IopSynchronousServiceTail+0x1b1
40 ffffc5846fbf2560 fffff8065d87f005 nt!NtWriteFile+0x8bd
41 ffffc5846fbf2670 fffff8065d871b20 nt!KiSystemServiceCopyEnd+0x25
42 ffffc5846fbf2878 fffff8065dc3bf69 nt!KiServiceLinkage
43 ffffc5846fbf2880 fffff8065dc3b9f8 nt!EtwpFlushBufferToLogfile+0x81
44 ffffc5846fbf28f0 fffff8065dcad751 nt!EtwpFlushBuffer+0x94
```


对应的 apsx64 驱动是 2018 年的:

```
0: kd> lmvm apsx64
Browse full module list
start             end                 module name
fffff806`64bc0000 fffff806`64bea000   ApsX64     (no symbols)
    Loaded symbol image file: ApsX64.sys
    Image path: \SystemRoot\System32\drivers\ApsX64.sys
    Image name: ApsX64.sys
    Browse all global symbols  functions  data
    Timestamp:        Wed Dec 19 13:31:01 2018 (5C19D795)
    CheckSum:         0002C99A
    ImageSize:        0002A000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:

Unable to enumerate user-mode unloaded modules, NTSTATUS 0xC0000147
```

针对 T14s 的 dump 分析：

Explorer 进程在等待访问网络共享资源：

```
0: kd> !mex.t ffff808d72899080
Process                 Thread                  CID       TEB              UserTime KernelTime ContextSwitches Wait
explorer.exe (ffff808d727e8080) ffff808d72899080 (E|K|W|R|V) 2888.2afc 00000000005ca000    313ms      734ms           14844 Execut

WaitBlockList:
    Object                Type              Other Waiters
    ffff808d736ddd90(SmXc) NotificationEvent            0

Irp List:
    IRP              File                                                                  Driver
    ffff808d748a39a0 \122.248.14.41\杭州基地共享软件\06办公工具软件\无线及VPN客户端\OTP VPN安装介质及文档                mrxsmb
    ffff808d77d469a0 \122.248.14.41\杭州基地共享软件\06办公工具软件\无线及VPN客户端\OTP VPN安装介质及文档\OTP VPN介质 FltMgr
    ffff808d730d4010 \Windows\bcastdvr                                                     Ntfs

Priority:
    Current Base Decrement ForegroundBoost IO Page
    11      8    0         48              0  5

 # Child-SP         Return           Call Site
 0 ffff928d6f4e7930 fffff8016a68d5d7 nt!KiSwapContext+0x76
 1 ffff928d6f4e7a70 fffff8016a68d149 nt!KiSwapThread+0x297
 2 ffff928d6f4e7b30 fffff8016a68bed0 nt!KiCommitThreadWait+0x549
 3 ffff928d6f4e7bd0 fffff8016acd7b2b nt!KeWaitForSingleObject+0x520
 4 ffff928d6f4e7ca0 fffff8016acd7457 nt!FsRtlCancellableWaitForMultipleObjects+0xcb
 5 ffff928d6f4e7d10 fffff80173771095 nt!FsRtlCancellableWaitForSingleObject+0x27
 6 ffff928d6f4e7d50 fffff80172f9af16 mrxsmb!SmbCeWaitForCompletionAndFinalizeExchangeEx+0x85
 7 ffff928d6f4e7e20 fffff80173787512 mrxsmb20!MRxSmb2Create+0xc86
 8 ffff928d6f4e7f50 fffff8016a7da5ee mrxsmb!SmbpShellCreateWithNewStack+0x22
 9 ffff928d6f4e7f80 fffff8016a7da5ac nt!KxSwitchKernelStackCallout+0x2e
 a ffff928d702057e0 fffff8016a651636 nt!KiSwitchKernelStackContinue
 b ffff928d70205800 fffff8016a65137c nt!KiExpandKernelStackAndCalloutOnStackSegment+0x256
 c ffff928d70205890 fffff8016a6511f3 nt!KiExpandKernelStackAndCalloutSwitchStack+0xdc
 d ffff928d70205900 fffff8016a744e15 nt!KeExpandKernelStackAndCalloutInternal+0x33
 e ffff928d70205970 fffff801737874d5 nt!KeExpandKernelStackAndCallout+0x15
```

而且有一个线程一直在重连网络资源：

```
0: kd> !mex.t ffff808d77bf0040
Process                 Thread                  CID      UserTime KernelTime ContextSwitches Wait Reason    Time State
System (ffff808d62a9a300) ffff808d77bf0040 (E|K|W|R|V) 4.2e20          0      203ms            6621 Executive   31s.281 Waiting

WaitBlockList:
    Object                Type              Other Waiters
    ffff808d6f3c3eb8(SmXc) NotificationEvent            0

Priority:
    Current Base Decrement ForegroundBoost IO Page
    12      12   0         0               0  5

 # Child-SP         Return           Call Site
 0 ffff928d6fcff030 fffff8016a68d5d7 nt!KiSwapContext+0x76
 1 ffff928d6fcff170 fffff8016a68d149 nt!KiSwapThread+0x297
 2 ffff928d6fcff230 fffff8016a68bed0 nt!KiCommitThreadWait+0x549
 3 ffff928d6fcff2d0 fffff8016acd7b2b nt!KeWaitForSingleObject+0x520
 4 ffff928d6fcff3a0 fffff8016acd7457 nt!FsRtlCancellableWaitForMultipleObjects+0xcb
 5 ffff928d6fcff410 fffff80173771095 nt!FsRtlCancellableWaitForSingleObject+0x27
 6 ffff928d6fcff450 fffff80172fb0755 mrxsmb!SmbCeWaitForCompletionAndFinalizeExchangeEx+0x85
 7 ffff928d6fcff520 fffff80172fae7d5 mrxsmb20!Smb2ValidateAndReconnectSrvOpen+0x101
 8 ffff928d6fcff580 fffff8017378c2c5 mrxsmb20!MRxSmb2ProbeAndReconnectSrvOpen+0x9bd5
 9 ffff928d6fcff5b0 fffff801720dca11 mrxsmb!SmbShellProbeAndReconnectSrvOpen+0x35
 a ffff928d6fcff5e0 fffff801720dba1c rdbss!RxReconnectSrvOpen+0xa1
 b ffff928d6fcff610 fffff8017210d436 rdbss!RxSelectAndSwitchPagingFileObject+0xf4
 c ffff928d6fcff770 fffff8017210ca5f rdbss!RxScavengeRelatedClosePendingFobxs+0x526
```

此时出现问题时，没有网络连接：

```
MINIPORT

    Intel(R) Wi-Fi 6 AX201 160MHz

    Ndis handle         ffff808d68c101a0
    Ndis API version    v6.60
    Adapter context     ffff808d697ca050
    Driver              ffff808d68a96020 - Netwtw10  v2.1
    Network interface   ffff808d6493f8a0

    Media type          802.3
    Physical medium     Native802.11
    Device instance     PCI\VEN_8086&DEV_02F0&SUBSYS_00708086&REV_00\3&11583659&2&A3
    Device object       ffff808d68c10050    More information
    MAC address         4c-79-6e-b6-02-ec


STATE

    Miniport            Running
    Device PnP          Started             Show state history
    Datapath            DIVERTED BECAUSE MEDIA DISCONNECTED
    NBL status          NDIS STATUS MEDIA DISCONNECTED
    Operational status  DOWN
    Operational flags   DOWN NOT CONNECTED
    Admin status        ADMIN UP
    Media               MediaDisconnected
    Miniport media      Connected
    Power               D0
    References          0n25                Show detail
    Total resets        0
    Pending OID         None
```

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2022 年 8 月 30 日 17:27

收件人: 'Windows Server 技术支持' <windowsserversupport@sdc.icbc.com.cn>
抄送: 'win10 升级支持' <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: 回复: 回复:【外来邮件，注意核实】回复: [案例号: CAS-06619-Z0Z8H9] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001372

许先生 您好:

感谢您的电话接听。

最新上传的断开 wifi 后出现系统卡死问题的 dump 已经收到，请您帮忙了解以下情况:

1）用户在什么情况下发现了系统卡死的问题？如做了什么操作时出现了系统卡死问题。

2）出现问题时用户做了哪些操作确认了系统处于卡死状态？如打开应用，或者点击哪个图标发现应用没有响应等。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话: 400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2022 年 8 月 29 日 17:11
收件人: 'Windows Server 技术支持' <windowsserversupport@sdc.icbc.com.cn>
抄送: win10 升级支持 <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: 回复: 回复:【外来邮件，注意核实】回复: [案例号: CAS-06619-Z0Z8H9] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001372

许先生 您好:

感谢您的回复。

日志正在下载，有任何进展会及时与您沟通。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Windows Server 技术支持 <windowsserversupport@sdc.icbc.com.cn>
发送时间: 2022 年 8 月 29 日 17:09
收件人: Wei Liang <weiliang@cmgos.com>
抄送: win10 升级支持 <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: 回复: 回复:【外来邮件，注意核实】回复: [案例号：CAS-06619-Z0Z8H9] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001372

wifi 卡死日志已上传请协助分析。上传路径：ftp-wfif 卡死目录。

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

中国工商银行软件开发中心（珠海）
许 翔
系统一部
电话：17606669571

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

-----原始邮件-----

发件人: "Wei Liang" <weiliang@cmgos.com>
发送时间: 2022-08-25 16:16:01
收件人: "戚云琪" <戚云琪.软件开发中心杭州开发一部@工商银行.icbc>,"Windows Server 技术支持" <windowsserver 技术支持.软件开发中心系

统一部@工商银行.icbc>
抄送: "win10 升级支持" <win10 技术支持.软件开发中心系统一部@工商银行.icbc>,"ICBC_Notification" <icbc_notification@cmgos.com>
主题: 回复: 回复:【外来邮件，注意核实】回复: [案例号: CAS-06619-Z0Z8H9] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001372

戚先生 您好:

感谢您的电话接听。

麻烦您上传最新的出现问题时的 dump 日志给我们进一步排查问题。

请许先生 @'Windows Server 技术支持' 帮忙把 dump 日志压缩后上传到 CDUC 或 sftp 服务器。

如果针对当前案件还有需要我们帮助的地方, 欢迎随时联系我们。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话: 400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2022 年 8 月 18 日 15:39
收件人: 'qiyq@sdc.icbc.com.cn' <qiyq@sdc.icbc.com.cn>; 'Windows Server 技术支持' <windowsserversupport@sdc.icbc.com.cn>
抄送: 'win10 升级支持' <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: 回复:【外来邮件，注意核实】回复: [案例号: CAS-06619-Z0Z8H9] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001372

戚先生 您好:

感谢您的电话接听。

请您按照上一封邮件在本机配置审核策略，减少 4663 事件，再观察是否能缓解您的问题。

如果针对当前案件还有需要我们帮助的地方, 欢迎随时联系我们。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2022 年 8 月 11 日 16:28
收件人: 'qiyq@sdc.icbc.com.cn' <qiyq@sdc.icbc.com.cn>; 'Windows Server 技术支持' <windowsserversupport@sdc.icbc.com.cn>
抄送: 'win10 升级支持' <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: 回复:【外来邮件，注意核实】回复: [案例号：CAS-06619-Z0Z8H9] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001372

戚先生 您好:

感谢您的电话接听。

根据上一封邮件的描述和 dump 分析过程，怀疑您的问题与 checkhosts.exe 进程有关，您也确认出现问题时无法打开任务管理器结束 checkhosts.exe 进程。

而 checkhosts.exe 应用是通过域控推送的计划任务执行的，本地计算机无法管理此计划任务。

此计划任务的触发条件是在**“安全”**日志中出现 eventid 为 4663 的事件时，会运行 checkhosts.exe 程序。

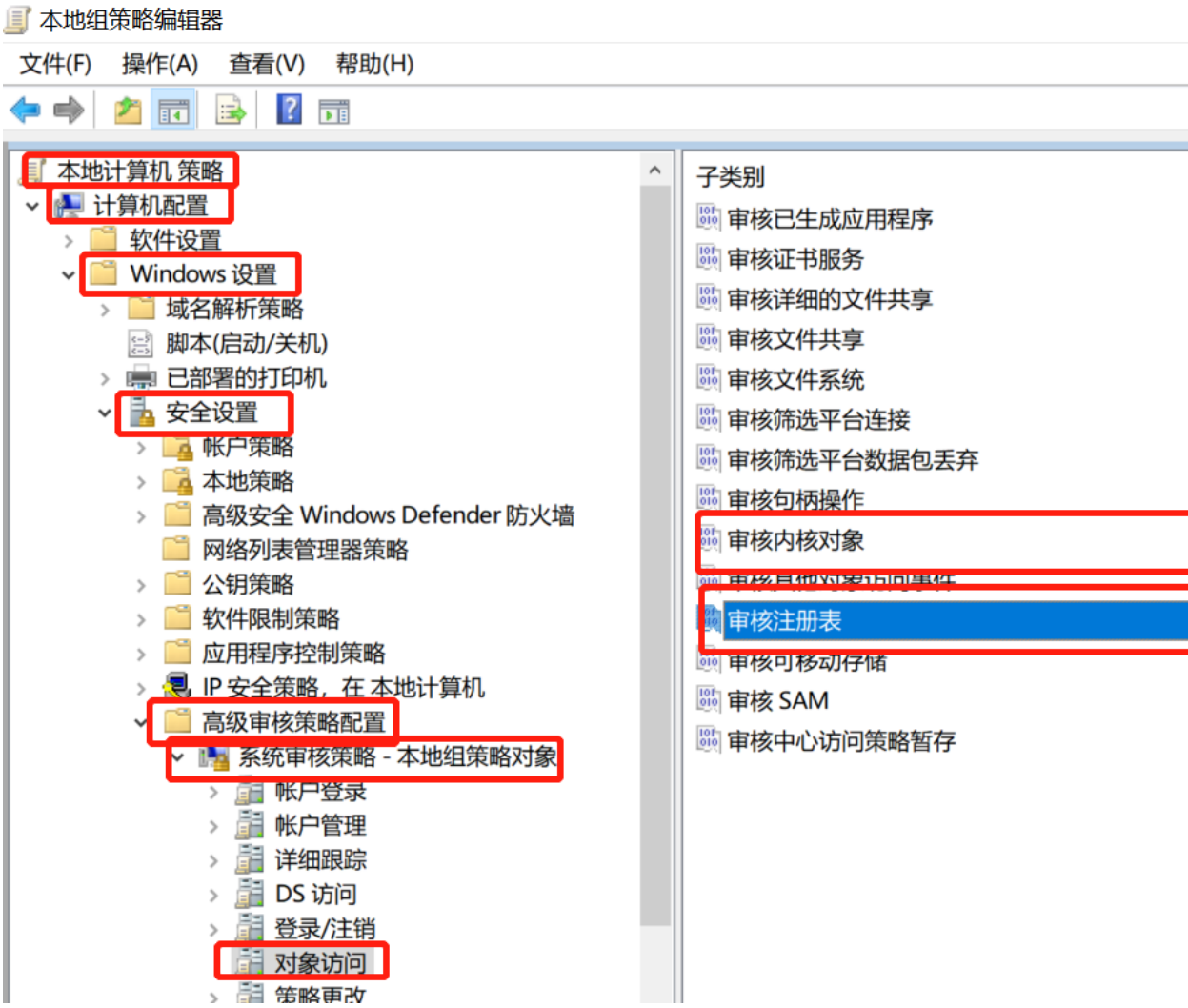
操作		替换
任务		
	名称	CheckHostsFile
	作者	INTRANET\icbc-ad-adm01
	描述	
	只在用户登录时运行	S4U
	UserId	NT AUTHORITY\System
	使用最高权限运行	HighestAvailable
	隐藏	否
	配置	1.2
	已启用	是
触发器		
1. 发生事件时		
	已启用	是
	订阅	<QueryList><Query Id="0" Path="Security"><Select Path="Security">*[System[Provider[@Name='Microsoft-Windows-Security-Auditing'] and EventID=4663]]</Select></Query></QueryList>
操作		
1. 启动程序		
	程序/脚本	\\intranet.icbc.com.cn\sysvol\Intranet.ICBC.COM.CN\Scripts\CheckHosts.exe

为缓解 checkhosts.exe 应用对这个问题的影响，我们通过在本地修改一些对象的审核策略，减少 4663 事件的生成。

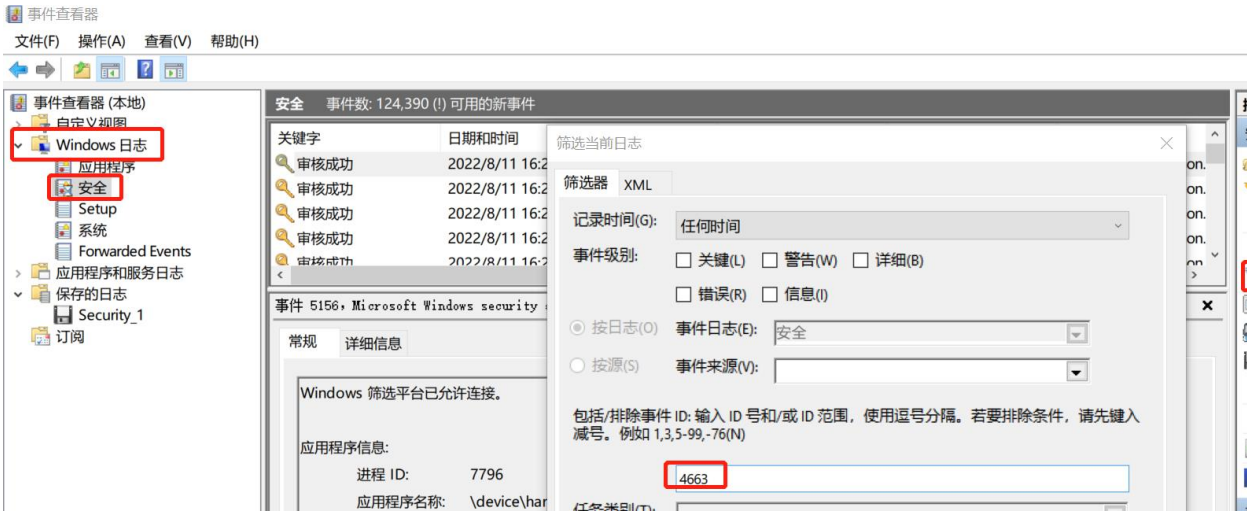
具体操作如下：

1）以**管理员权限**运行 gpedit.msc，打开**本地组策略编辑器**，定位到：**“本地计算机策略”-“计算机配置”-“Windows 设置”-“安全设置”-“高级审核策略”-“系统审核策略-本地组策略对象”-“对象访问”**，

2）修改**“审核内核对象”**和**“审核注册表”**为**“未配置”**状态。



3）打开事件查看器，定位到**“Windows 日志”**-**“安全”**列表，筛选当前日志，查询 4663 事件记录，是否不再增加 **registry** 和 **kernel object** 的任务类别的事件日志。



调整后，请您**重启计算机**，再观察对您的问题是否有缓解。

也请许先生 @'Windows Server 技术支持' 帮忙关注域控上的 checkhosts 功能调整。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2022 年 8 月 3 日 17:42
收件人: 'Windows Server 技术支持' <windowsserversupport@sdc.icbc.com.cn>; 'qiyq@sdc.icbc.com.cn' <qiyq@sdc.icbc.com.cn>
抄送: 'win10 升级支持' <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: 回复:【外来邮件，注意核实】回复: [案例号：CAS-06619-Z0Z8H9] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001372

戚先生 您好:

感谢您的电话接听。

在 dump 中可以查看 control.exe 线程情况，发现最后等在一个 system thread ffffd08d5afe1080 的 LPC message

```
0: kd> !mex.p ffffd08d52a53080
Name        Address                 Ses PID          Parent         PEB              Create Time                Mods Handle
=========== ======================= === ============ ============== ================ ========================== ==== ======
control.exe ffffd08d52a53080 (E|K|O)   1 a8c (0n2700) 2960 (0n10592) 0000007f0fc31000 07/26/2022 04:45:09.583 下午    77

Command Line: "C:\WINDOWS\system32\control.exe"netconnections\0

Memory Details:

    VM   Peak Commit Size PP Quota  NPP Quota
    ==== ==== =========== ========= =========
    2 TB 2 TB     4.68 MB 251.27 KB  24.03 KB

Show LPC Port information for process

Show Threads: Unique Stacks    !mex.listthreads (!lt) ffffd08d52a53080    !process ffffd08d52a53080 7

0: kd> !mex.lt ffffd08d52a53080
Process     PID Thread             Id State        Time Reason      Waiting On
=========== === ================ ==== ======= ======== =========== ==========================================================
control.exe a8c ffffd08d56b93080 2d34 Waiting 2m:48.828 UserRequest
control.exe a8c ffffd08d57ede080 2b08 Waiting 2m:48.828 WrQueue
control.exe a8c ffffd08d57883080  6dc Waiting 2m:48.828 WrQueue
control.exe a8c ffffd08d598f3080 38fc Waiting 2m:48.828 WrQueue
control.exe a8c ffffd08d5af95080 39ac Waiting 2m:48.828 UserRequest
control.exe a8c ffffd08d57edf080 2cb0 Waiting 2m:48.828 WrLpcReply  Thread: ffffd08d5afe1080 in svchost.exe (-p) (0n1364)

Thread Count: 6
```

查看此线程情况，它等待在一个 LPC Message Queued 上（Port OLEF8EDEB0B95C61425A313EB461A13），但是没有线程 handle 在此端口上。

```
0: kd> !mex.t ffffd08d5afe1080
Process                          Thread                         CID       TEB              UserTi
svchost.exe (-p) (ffffd08d52781240) ffffd08d5afe1080 (E|K|W|R|V) 554.1c54  00000034fc92e000

WaitBlockList:
    Object           Type      Other Waiters Info
    ffffd08d5afe16c8 Semaphore             0 Limit: 1

Priority:
    Current Base Decrement ForegroundBoost IO Page
    9       8    0         16              0  5

LPC Msg          ServerProcess                  ServerThread
ffff95874fcd1cb0 control.exe(ffffd08d52a53080) Message Queued
```

```
0: kd> !kdexts.alpc /p ffffd08d76311500
Port  ffffd08d76311500
  Type                    : ALPC_CONNECTION_PORT
  CommunicationInfo       : ffff95873b4d1980
    ConnectionPort        : ffffd08d76311500 (OLEF8EDEB0B95C61425A313EB461A13)
    ClientCommunicationPort : 0000000000000000
    ServerCommunicationPort : 0000000000000000
  OwnerProcess            : ffffd08d52a53080 (control.exe)
  SequenceNo              : 0x00000001 (1)
  CompletionPort          : ffffd08d719c87c0
  CompletionList          : 0000000000000000
```

尝试查询死锁情况，发现有两个锁信息

```
0: kd> !locks
**** DUMP OF ALL RESOURCE OBJECTS ****
KD: Scanning for held locks.....................................

Resource @ 0xffffd08d58bfb600    Exclusively owned
    Contention Count = 1000
    Threads: ffffd08d5d132280-01<*>
KD: Scanning for held locks.....................................

Resource @ 0xffffd08d5bd23d98    Shared 1 owning threads
    Contention Count = 12
    Threads: ffffd08d488d1140-01<*>
KD: Scanning for held locks.....................................
46543 total locks, 2 locks currently held
```

查看对应的线程情况，指向了去访问 UNC 地址上的文件 checkhosts.exe，之后一直等在 io 上，等待了 12mins

```
0: kd> !mex.t ffffd08d488d1140
Process                 AttachedProcess                     Thread                      CID
System (ffffd08d4888a300) CheckHosts.exe *32 (ffffd08d4f320080) ffffd08d488d1140 (E|K|W|R|V) 4.24

WaitBlockList:
    Object                Type              Other Waiters
    ffffd08d5bbdeb10(RxIr) NotificationEvent            0

Irp List:
    IRP                   File
    ffffd08d749f8010      \KFZXBADM191.Intranet.ICBC.COM.CN\sysvol\Intranet.ICBC.COM.CN\Scripts\CheckHo

Priority:
    Current Base Decrement ForegroundBoost IO Page
    9       8    0         16              0  5

 # Child-SP          Return           Call Site
```

另一个进程也是一直在等待 SMB 响应

```
0: kd> !mex.t ffffd08d5d132280
Process                 Thread                        CID       UserTime KernelTime ContextSwitch
System (ffffd08d4888a300) ffffd08d5d132280 (E|K|W|R|V) 4.45e0           0     2s.266          1491

WaitBlockList:
    Object                Name                              Type              Other Waiters
    ffffd08d5cafbce0(SmXc)    @\0  <TRUNCATED 22102 CHARS> NotificationEvent             0

Priority:
    Current Base Decrement ForegroundBoost IO Page
    12      12   0         0               0  5

 # Child-SP          Return           Call Site
 0 ffff900a76d60040 fffff80571f265d7 nt!KiSwapContext+0x76
 1 ffff900a76d60180 fffff80571f26149 nt!KiSwapThread+0x297
 2 ffff900a76d60240 fffff80571f24ed0 nt!KiCommitThreadWait+0x549
 3 ffff900a76d602e0 fffff80572570b2b nt!KeWaitForSingleObject+0x520
 4 ffff900a76d603b0 fffff80572570457 nt!FsRtlCancellableWaitForMultipleObjects+0xcb
 5 ffff900a76d60420 fffff8057e531095 nt!FsRtlCancellableWaitForSingleObject+0x27
 6 ffff900a76d60460 fffff8057a7e49c7 mrxsmb!SmbCeWaitForCompletionAndFinalizeExchangeEx+0x85
 7 ffff900a76d60530 fffff8057e53c778 mrxsmb20!MRxSmb2Close+0x2f7
 8 ffff900a76d60630 fffff8057989bef8 mrxsmb!SmbShellCloseSrvOpen+0x38
 9 ffff900a76d60670 fffff8057989bc57 rdbss!RxCloseAssociatedSrvOpen+0x170
 a ffff900a76d606d0 fffff8057989bb0b rdbss!RxFinalizeNetFobx+0xa7
 b ffff900a76d60720 fffff8057989d926 rdbss!RxFcbScavengeRelatedFobxs+0x16b
 c ffff900a76d60790 fffff8057989ca7f rdbss!RxScavengeRelatedFobxs+0x376
 d ffff900a76d60970 fffff8057989dc6a rdbss!RxScavengerFinalizeEntries+0x63
 e ffff900a76d609b0 fffff80579864d7f rdbss!RxScavengerTimerRoutine+0x8a
 f ffff900a76d60a10 fffff80571ee3f2a rdbss!RxpProcessWorkItem+0x8f
10 ffff900a76d60a70 fffff80571fd63a5 nt!ExpWorkerThread+0x16a
```

下一步建议：

怀疑系统出现很多应用无法响应可能与 checkhosts.exe 进程有关，请您再次出现问题时，尝试通过任务管理器**结束所有 checkhosts.exe 进程**，观察系统运行情况。

如果无法结束 checkhosts.exe 进程或者此操作无法使系统恢复正常，请您再次通过键盘触发 fulldump，并提供给我们进行对比分析。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2022 年 8 月 1 日 17:50
收件人: 'Windows Server 技术支持' <windowsserversupport@sdc.icbc.com.cn>; 'qiyq@sdc.icbc.com.cn' <qiyq@sdc.icbc.com.cn>
抄送: 'win10 升级支持' <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: 回复:【外来邮件，注意核实】回复: [案例号：CAS-06619-Z0Z8H9] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001372

戚先生 您好:

感谢您的电话接听。

我这边正在尝试从 dump 中查找 control.exe 进程未能正常响应请求的原因，需要一点时间进一步排查。

在排查期间如果再次出现同样问题，麻烦您再次通过手动触发 dump 方式收集蓝屏 dump，并提供给我们对比分析。

麻烦许先生 @'Windows Server 技术支持' 帮忙上传 7 月 22 日的蓝屏 dump 到 sftp 服务器，后续如有新的 dump，也请帮忙上传。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2022 年 7 月 26 日 11:12
收件人: 'Windows Server 技术支持' <windowsserversupport@sdc.icbc.com.cn>
抄送: 'win10 升级支持' <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>; 'qiyq@sdc.icbc.com.cn' <qiyq@sdc.icbc.com.cn>
主题: 回复: 回复:【外来邮件，注意核实】回复: [案例号：CAS-06619-Z0Z8H9] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001372

许先生 您好:

感谢您的电话接听。

请您与最终用户沟通，先删除 C:\Windows\目录下的旧的 memory.dmp 文件，确保**系统盘可用空间大于当前设备物理内存容量**。

下载附件，将 txt 文件后缀改为.bat，在**手动触发 fulldump.bat** 上点击右键，**选择以管理员身份运行，**注意**保存个人数据，**因为运行完成后，需要按任意键重启设备使配置生效。

在下一次出现问题时，直接通过键盘组合键**左 shift +右 shift 按住不放，连按两次波浪号键“~”**（Esc 下方），手动触发蓝屏自动重启，生成 memory.dmp。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2022 年 7 月 21 日 17:42
收件人: 'qiyq@sdc.icbc.com.cn' <qiyq@sdc.icbc.com.cn>
抄送: 'Windows Server 技术支持' <windowsserversupport@sdc.icbc.com.cn>; 'win10 升级支持' <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: 回复:【外来邮件，注意核实】回复: [案例号：CAS-06619-Z0Z8H9] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001372

戚先生 您好:

感谢您的电话接听。

请您先删除 C:\Windows\目录下的旧的 memory.dmp 文件，确保系统盘可用空间大于当前设备物理内存容量。

在下一次出现问题时，直接通过键盘组合键**左 shift +右 shift 按住不放，连按两次波浪号键“~”**（Esc 下方），手动触发蓝屏自动重启，生成 memory.dmp。

如果针对当前案例还有需要我们帮助的地方, 欢迎随时联系我们。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2022 年 7 月 18 日 17:11
收件人: 'qiyq@sdc.icbc.com.cn' <qiyq@sdc.icbc.com.cn>
抄送: 'Windows Server 技术支持' <windowsserversupport@sdc.icbc.com.cn>; 'win10 升级支持' <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: 回复:【外来邮件，注意核实】回复: [案例号：CAS-06619-Z0Z8H9] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001372

戚先生 您好:

感谢您的电话接听。

在出现问题的时候，您可以按照上一封邮件操作收集相关日志提供给我们进一步分析。由于近期您这边未出现此问题，我会间隔一周左右与您联系沟通问题进展。

如果针对当前案例还有需要我们帮助的地方, 欢迎随时联系我们。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2022 年 7 月 14 日 16:33
收件人: 'qiyq@sdc.icbc.com.cn' <qiyq@sdc.icbc.com.cn>
抄送: 'Windows Server 技术支持' <windowsserversupport@sdc.icbc.com.cn>; 'win10 升级支持' <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: 回复:【外来邮件，注意核实】回复: [案例号: CAS-06619-Z0Z8H9] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001372

戚先生 您好:

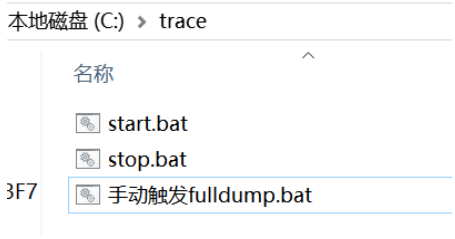
上一封邮件您没有收到，重新再次发送。

请您按照以下方式操作，尝试收集相关日志。

1）在 C 盘创建 trace 文件夹，即 **C:\trace** 文件夹。

2）通过以下链接下载压缩包 **trace.zip**，解压到 **C:\trace** 文件夹，**将 txt 后缀改为 bat**，如图所示。

https://cduc.cmgos.com/download.php?id=476&token=gzCCERt9InYZhRMQGw9VfrvRSZcSBnqA



3）在**手动触发 fulldump.bat** 上点击右键，**选择以管理员身份运行，**注意**保存个人数据，**因为运行完成后，需要按任意键重启设备使配置生效。

4）按任意键重启（如需稍后重启，键入 Ctrl+C）。

5）重启后，打开 **C:\trace** 目录，在 start.bat 上点击右键，选择**以管理员身份运行**。此时设备不要重启，**设备重启后需要重新以管理员权限运行 start.bat**。

6）等待复现问题后，打开 C:\trace 文件夹，在 stop.bat 上点击右键，选择**以管理员身份运行**，运行结束后会在 **C:\trace** 文件夹生成 **trace.etl 文件和相关目录。**

7）再按下键盘 **左 shift +右 shift 按住不放，连按两次波浪号键“~”**（Esc 下方），触发蓝屏。

8）等待蓝屏信息收集完毕，设备自动重启进入系统后，收集 Dump 文件 C:\Window\Memory.DMP 并**压缩文件**上传。

9）将 **C:\trace 文件夹压缩打包**上传。

日志上传：

为了更安全、快速地传输数据，您可以在 Filezilla 上使用以下账户信息登入神州网信网站。

- Filezilla client 端下载 URL：https://filezilla-project.org/download.php?type=client
- 登陆地址：sftp://ocean.cmgos.com
- 用户名为：ICBC（区分大小写）

- 密码：2qfs52ninbFB
- 端口：22222

登录之后，上传到**/upload/杭州断开 wifi 卡死**文件夹

如果无法访问此 sftp 服务器，请许翔 @Windows Server 技术支持 帮忙上传对应日志。

==========

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。

危亮 Wei Liang

神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

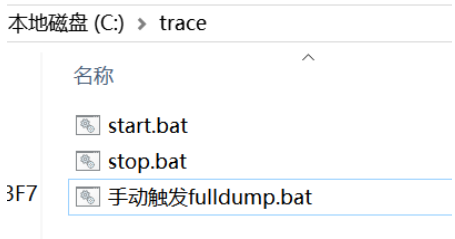
发件人: Wei Liang
发送时间: 2022 年 7 月 12 日 17:16
收件人: 'qiyq@sdc.icbc.com.cn' <qiyq@sdc.icbc.com.cn>
抄送: 'Windows Server 技术支持' <windowsserversupport@sdc.icbc.com.cn>; win10 升级支持 <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: 回复:【外来邮件，注意核实】回复: [案例号：CAS-06619-Z0Z8H9] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001372

戚先生 您好:

感谢您的电话接听。请您按照以下方式操作，尝试收集相关日志。

1）在 C 盘创建 trace 文件夹，即 **C:\trace** 文件夹。

2）将附件中的压缩包 **trace.zip** 下载，解压到 **C:\trace** 文件夹，**将 txt 后缀改为 bat**，如图所示。



3）在**手动触发 fulldump.bat** 上点击右键，**选择以管理员身份运行，**注意**保存个人数据，**因为运行完成后，需要按任意键重启设备使配置生效。

4）按任意键重启（如需稍后重启，键入 Ctrl+C）。

5）重启后，打开 **C:\trace** 目录，在 start.bat 上点击右键，选择**以管理员身份运行**。此时设备不要重启，**设备重启后需要重新以管理员权限运行 start.bat**。

6）等待复现问题后，打开 C:\trace 文件夹，在 stop.bat 上点击右键，选择**以管理员身份运行**，运行结束后会在 **C:\trace** 文件夹生成 **trace.etl 文件和相关目录。**

7）再按下键盘 **左 shift +右 shift 按住不放，连按两次波浪号键“~”**（Esc 下方），触发蓝屏。

8）等待蓝屏信息收集完毕，设备自动重启进入系统后，收集 Dump 文件 C:\Window\Memory.DMP 并**压缩文件**上传。

9）将 **C:\trace 文件夹压缩打包**上传。

日志上传：

为了更安全、快速地传输数据，您可以在 Filezilla 上使用以下账户信息登入神州网信网站。

- Filezilla client 端下载 URL：https://filezilla-project.org/download.php?type=client
- 登陆地址：sftp://ocean.cmgos.com
- 用户名为：ICBC（区分大小写）

- 密码：2qfs52ninbFB
- 端口：22222

登录之后，上传到**/upload/杭州断开 wifi 卡死**文件夹

如果无法访问此 sftp 服务器，请许翔 @Windows Server 技术支持 帮忙上传对应日志。

==========

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。

危亮 Wei Liang

神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Windows Server 技术支持 <windowsserversupport@sdc.icbc.com.cn>
发送时间: 2022 年 7 月 11 日 17:13
收件人: Wei Liang <weiliang@cmgos.com>
抄送: Windows Server 技术支持 <windowsserversupport@sdc.icbc.com.cn>; win10 升级支持 <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复:【外来邮件，注意核实】回复: [案例号: CAS-06619-Z0Z8H9] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001372

wifi 卡死联系人：戚云琪 联系电话：17682348418

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

中国工商银行软件开发中心（珠海）
许 翔
系统一部
电话：17606669571

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

-----原始邮件-----

发件人: "Wei Liang" <weiliang@cmgos.com>
发送时间: 2022-07-11 17:08:17
收件人: "Windows Server 技术支持" <windowsserver 技术支持.软件开发中心系统一部@工商银行.icbc>
抄送: "win10 升级支持" <win10 升级支持.软件开发中心系统一部@工商银行.icbc>,"ICBC_Notification" <icbc_notification@cmgos.com>
主题: 【外来邮件，注意核实】回复: [案例号: CAS-06619-Z0Z8H9] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001372

许先生 您好:

来信是想了解最终用户针对此问题的日志收集情况如何，请尝试按照 **2022 年 6 月 29 日 15:43 的邮件操作**获取相关日志。
在问题处理过程中如有需要我们帮助的地方，欢迎随时联系我们。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2022 年 7 月 7 日 17:49
收件人: '许翔' <windowsserversupport@sdc.icbc.com.cn>
抄送: 'win10sup@sdc.icbc.com.cn' <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号：CAS-06464-Y6X9J7] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001066

许先生 您好:

经过您的确认，这个问题是偶发现象比较难以复现，我这边也尝试以前的系统日志中是否有线索。也请您与用户沟通，尝试按照 **2022 年 6 月 29 日 15:43 的邮件操作**获取相关日志。
在问题处理过程中如有需要我们帮助的地方，欢迎随时联系我们。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055

电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2022 年 7 月 5 日 17:36
收件人: '许翔' <windowsserversupport@sdc.icbc.com.cn>
抄送: 'win10sup@sdc.icbc.com.cn' <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号: CAS-06464-Y6X9J7] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001066

许先生 您好:

感谢您的电话接听。

您提供的问题视频经确认是已经出现问题后的现象，我们需要抓取此问题的复现过程中的日志。

请您与用户确认，这个问题的详细复现步骤，并按照 **2022 年 6 月 29 日 15:43 的邮件操作** 获取相关日志。

在问题处理过程中如有需要我们帮助的地方，欢迎随时联系我们。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2022 年 7 月 1 日 17:13
收件人: '许翔' <windowsserversupport@sdc.icbc.com.cn>

抄送: 'win10sup@sdc.icbc.com.cn' <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号: CAS-06464-Y6X9J7] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001066

许先生 您好:

感谢您的电话接听。

请您与最终用户沟通，提供**出现系统卡死问题的操作视频，并按照上一封邮件说明复现问题，收集对应日志。**

在问题处理过程中如有需要我们帮助的地方，欢迎随时联系我们。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2022 年 6 月 29 日 15:43
收件人: '许翔' <windowsserversupport@sdc.icbc.com.cn>
抄送: 'win10sup@sdc.icbc.com.cn' <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号: CAS-06464-Y6X9J7] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001066

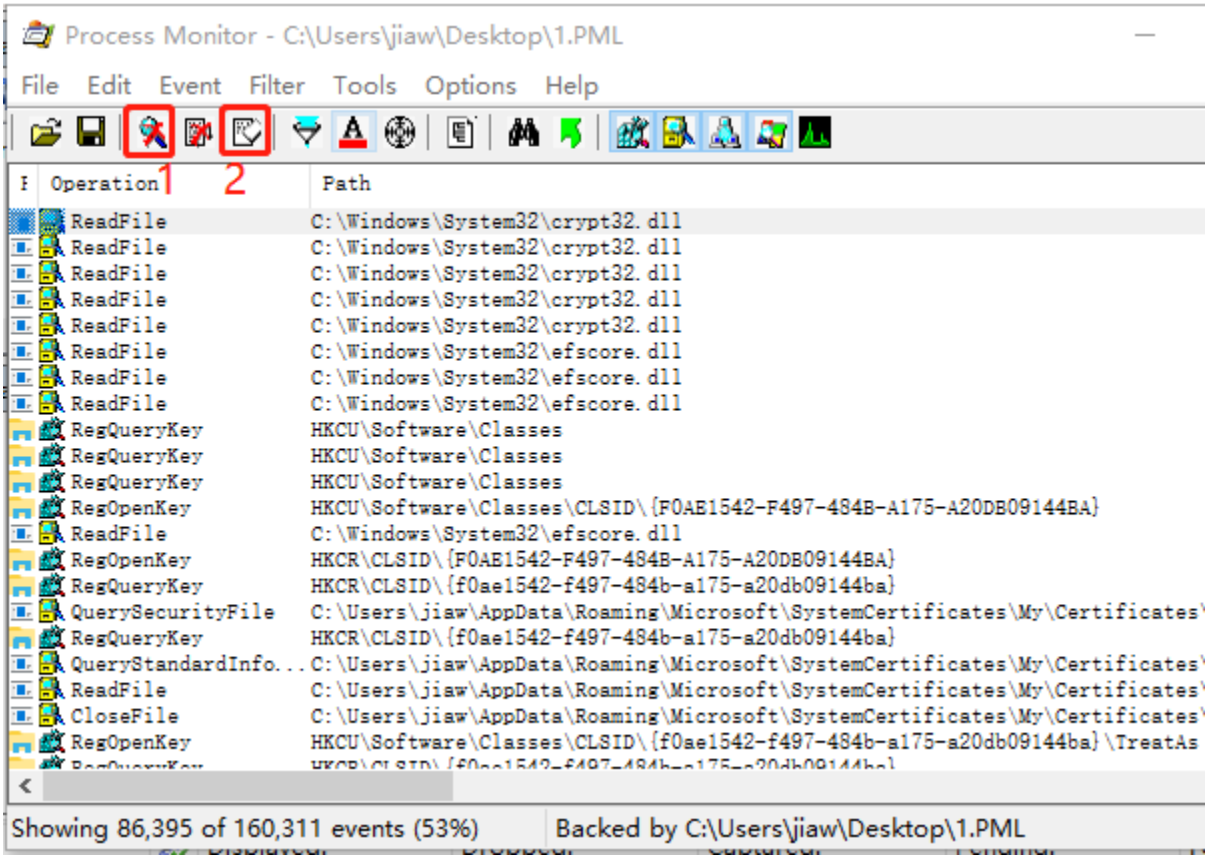
许先生 您好:

根据您提供的信息，由于安全管控策略，不允许启动到 WINPE 环境，无法复制 pagefile.sys 文件。

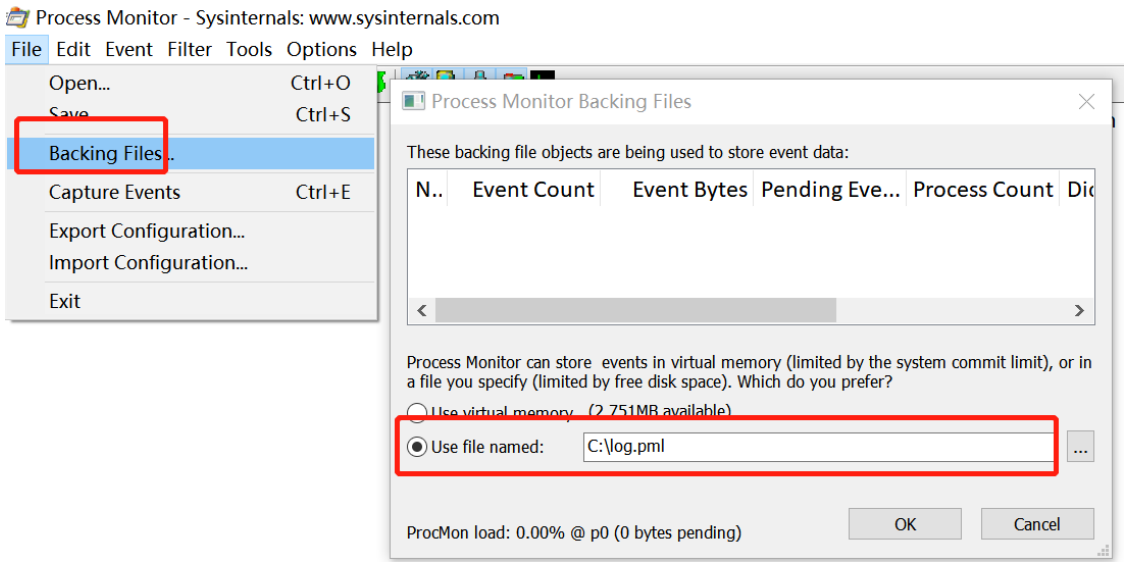
请您与用户沟通提供**出现系统卡死问题的操作视频**，并收集相关日志，具体操作如下:

Procmon 日志：

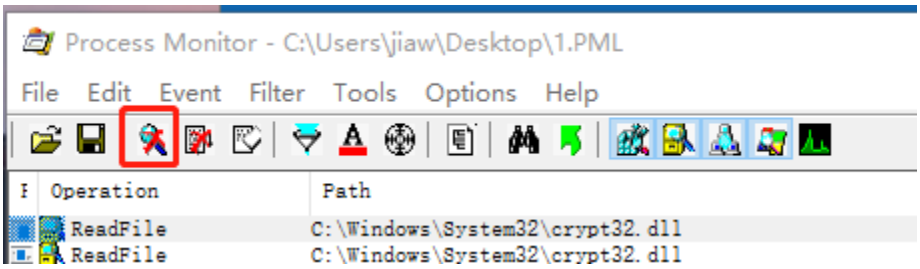
（1）下载附件中的 Procmon.zip，解压后**双击 procmon.exe 运行**，点击 Accept 后，到达此页面，会有有大量条目出现，先后点击 1，2 暂停抓取并清除当前条目。当前已经是可抓取状态；



（2）点击 file—backing files，配置 log.pml 保存位置，如 **C:\log.pml**。



（3）点击以下图标开始抓取。



（4）复现 wifi 卡死问题。

当出现系统卡死，只能强制关机重启后，将第（2）步配置的 **c:\log.pml** 文件压缩后上传。

系统日志：

（1）下载附件中的 CMGELogCollector.zip，解压后运行 CMGELogCollector.exe，勾选全部选项，点击“收集”，运行几分钟后会在桌面**生成日志压缩包**，将此日志提供给我们。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

神州网信 CMIT

发件人: Wei Liang
发送时间: 2022 年 6 月 27 日 17:16
收件人: '许翔' <windowsserversupport@sdc.icbc.com.cn>
抄送: 'win10sup@sdc.icbc.com.cn' <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号：CAS-06464-Y6X9J7] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001066

许先生 您好:

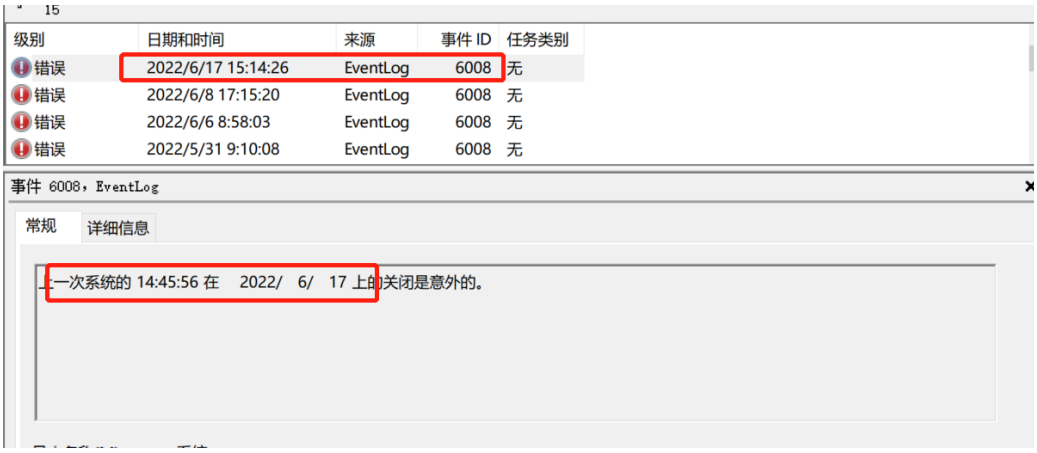
系统日志中未发现断开 wifi 系统卡死的相关线索，请您与用户沟通提供**出现系统卡死问题的操作视频，并按照上一封邮件说明复现问题，收集对应日志，**提供给我们进一步分析。
在问题处理过程中如有需要我们帮助的地方，欢迎随时联系我们。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2022 年 6 月 23 日 18:21
收件人: '许翔' <windowsserversupport@sdc.icbc.com.cn>
抄送: 'win10sup@sdc.icbc.com.cn' <win10sup@sdc.icbc.com.cn>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号：CAS-06464-Y6X9J7] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001066

许先生 您好:

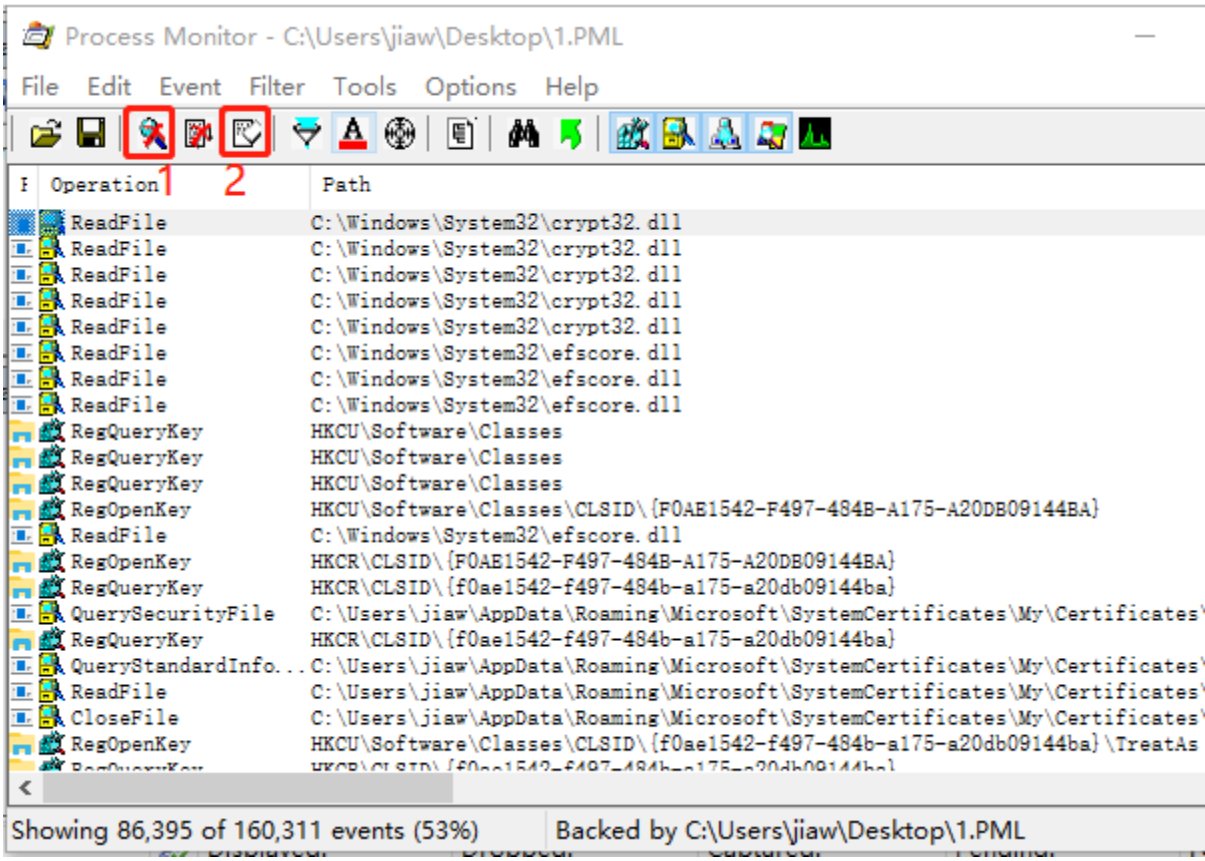
从系统日志中并未发现相关线索，只有几次意外关机的提示，不知道这些意外关机是否能和系统卡死的时间对上。



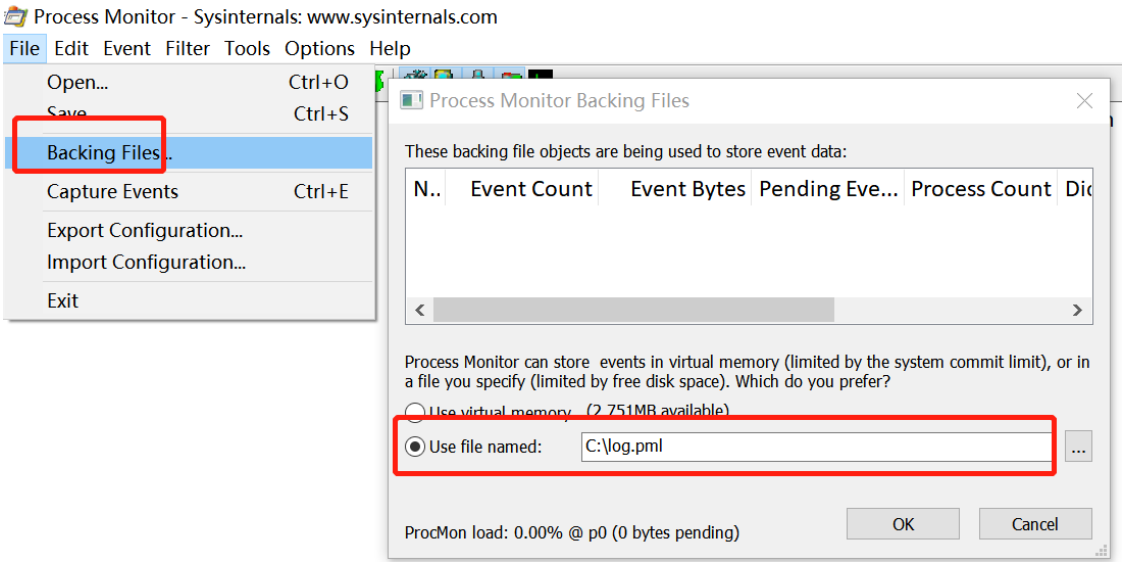
对此问题需要收集更详细的日志，并提供**出现系统卡死问题的操作视频**，具体收集相关日志操作如下:

Procmon 日志：

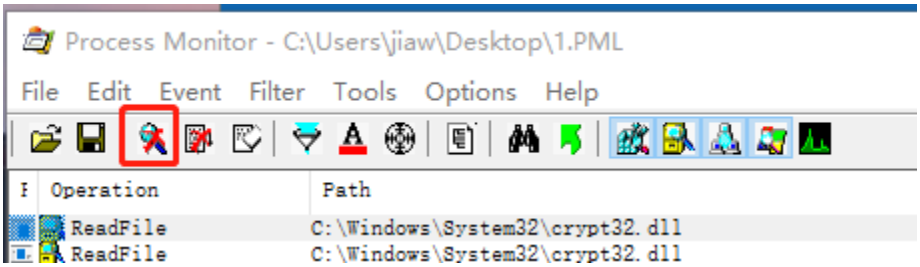
（1）下载附件中的 Procmon.zip，解压后**双击 procmon.exe 运行**，点击 Accept 后，到达此页面，会有有大量条目出现，先后点击 1，2 暂停抓取并清除当前条目。当前已经是可抓取状态；



（2）点击 file—backing files，配置 log.pml 保存位置。



（3）点击以下图标开始抓取。



（4）复现 wifi 卡死问题。

当出现系统卡死，只能强制关机时，关机后**直接使用 PE 进入 WINPE 系统**，在 WINPE 系统下复制 **C:\pagefile.sys** 文件，压缩后提供给我们。

在 WINPE 下复制了 C:\pagefile.sys 文件后，重新启动到 CMGE 系统，将第（2）步配置的 log.pml 文件压缩后上传。

系统日志：

（1）下载附件中的 CMGELogCollector.zip，解压后运行 CMGELogCollector.exe，勾选全部选项，点击“收集”，运行几分钟后会在桌面**生成日志压缩包**，将此日志提供给我们。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.

服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

神州网信 CMIT

发件人: Wei Liang
发送时间: 2022 年 6 月 21 日 17:49
收件人: 许翔 <windowsserversupport@sdc.icbc.com.cn>
抄送: win10sup@sdc.icbc.com.cn; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号: CAS-06464-Y6X9J7] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001066

许先生 您好:

感谢您的电话接听。

根据您提供的信息，我谨在此阐述我们双方针对这个问题所涉及范围界定:

问题定义:

无线网络突然断网，断网后手工重连时卡在正在连接状态，此时整个操作系统会出现各种无法响应的问题，需要分析原因。

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。

我们先分析您上传的日志，有任何进展将及时与您沟通。

也请您帮忙沟通了解出现这个问题的大概时间，并提供出现系统卡死问题的操作视频，后续可能需要抓取系统卡死问题的详细操作日志。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang <weiliang@cmgos.com>
发送时间: 2022 年 6 月 21 日 14:55
收件人: 许翔 <windowsserversupport@sdc.icbc.com.cn>
抄送: Wei Liang <weiliang@cmgos.com>
主题: [案例号：CAS-06464-Y6X9J7] % |P2|ICBC|杭州开发一部断开 wifi 系统卡死问题 % 初次响应 CMIT:0001066

许翔 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 危亮 。 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-06464-Y6X9J7 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

以上内容是一封有关向神州网信技术有限公司提交技术支持事件的邮件。

如果您希望本次回复能够被自动加入技术支持事件中,您可以选择“全部回复”。

此邮件信息仅供收件人查阅，所含任何评论、陈述或数据仅供收件人参考，若有改动，恕可能不另行通知。未经中国工商银行书面许可，请勿披露、复制、转载此邮件信息。任何第三方均不得查阅或使用此邮件信息。若您误收到本邮件，敬请及时通知发件人，并将邮件从您系统中彻底删除。发件人及中国工商银行均不对因邮件可能引发的损失负责。
This message is intended only for use of the addressees and any comment, statement or data contained herein is for the reference of the receivers only. Notification may not be sent for any revising related. Please do not disclose, copy, or distribute this e-mail without ICBC written permission. Any third party shall not read or use the content of this e-mail. If you receive this e-mail in error, please notify the sender immediately and delete this e-mail from your computer system completely.The sender and ICBC are not responsible for the loss caused possibly by e-mail.