Hi, 宏发：

如刚才电话沟通，鉴于当前问题分析已告知用户，最近并未上传更多问题，经您的同意，此 case 将暂做归档处理，以下为案例总结，请您知悉：

Case No：CAS-06804-R3Z5V3

问题描述：

==========

用户反馈开机自动修复，蓝屏等问题，需要协助排查。

问题分析：

==========

根据用户所上传日志分析，已找到出现问题之原因，所涉问题电脑均已修复完成。

问题总结：

==========

经用户确认，近期未再复现更多问题，此 case 做归档处理。

以上为此问题的案例总结，如有任何问题，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

神州网信
CMIT

发件人: Li Qi
发送时间: 2022 年 9 月 29 日 14:36
收件人: 'Hongfa HF3 Ou' <ouhf3@lenovo.com>
抄送: Liu Jian <liujian@cmgos.com>; 'Hepeng HP14 Wang' <wanghp14@lenovo.com>; PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [External] [案例号: CAS-06804-R3Z5V3] % |普通事件|lenovo|天津农行-大港支行 M930s 开机进入自动修复、蓝屏 % 初次响应 CMIT:0001358

Hi，All:

如上午会议沟通，此次在天津农行现场处理的 5 台问题电脑的故障分析汇总如下表:

问题电脑 SN	故障内容	问题定位	解决方案
M70P84CP	自动修复问题	文件丢失 fvevol.sys	替换 fvevol.sys
M70JWXH9	自动修复问题	system 注册表文件损坏，后发现硬盘坏道	更换硬盘
M70P84CH	自动修复问题，定位问题为: 0xc000000f	引导分区文件损坏，并且源文件损坏，无法修复	重装系统
M70P84BG	开机启动阶段黑屏	System32 文件夹下文件丢失	替换同补丁版本机器的 system32 文件夹
M70P84CQ	蓝屏 critical service failed	上一次关机异常	开启高级启动，禁用驱动强制签名

此外，上述 5 台电脑从事件日志中均能发现意外关机的 6008 事件日志记录，与用户描述的使用行为相符。

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 9 月 27 日 14:01
收件人: 'Hongfa HF3 Ou' <ouhf3@lenovo.com>
抄送: Liu Jian <liujian@cmgos.com>; 'Hepeng HP14 Wang' <wanghp14@lenovo.com>;

PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [External] [案例号: CAS-06804-R3Z5V3] % |普通事件|lenovo|天津农行-大港支行 M930s 开机进入自动修复、蓝屏 % 初次响应 CMIT:0001358

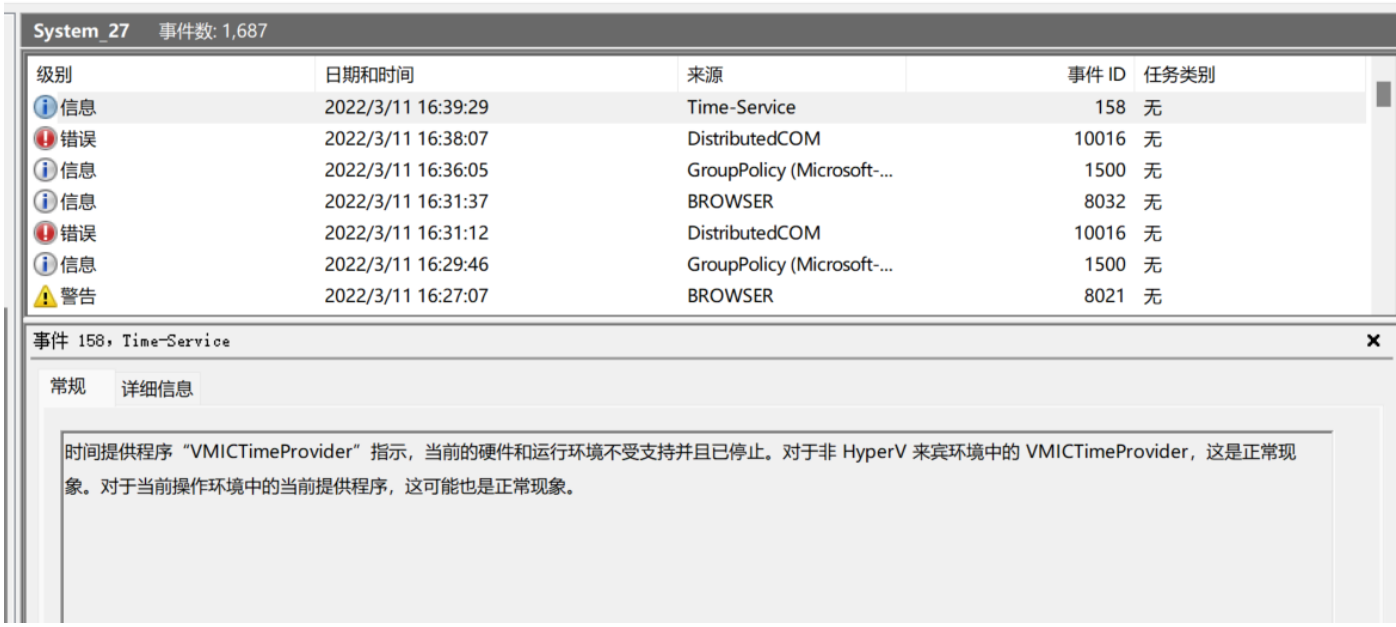
藕工，您好:

最后一台的 7f 蓝屏问题的电脑从操作系统层面尝试了很多方法，均无法完成修复。由于该问题出现在 load os 之前，所以其实可操作的修复动作十分有限。

目前以经验判断，该问题大概率为引导分区问题，即系统分区的 BCD 文件配置；并且由于相应的 rebuild 操作失败，因此怀疑在执行过程中所使用的源文件也存在问题。

当前该问题的解决方式：可通知用户方使用 PE 备份数据后，重装系统。

另外说明一点，查看该机器的系统日志，自 22 年 3 月 11 日之后便没有更多日志信息，怀疑在 3 月后该机器并未使用，不确定是否在当时已经出现此问题，供参考，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 9 月 22 日 18:05
收件人: 'Hongfa HF3 Ou' <ouhf3@lenovo.com>
抄送: Liu Jian <liujian@cmgos.com>; 'Hepeng HP14 Wang' <wanghp14@lenovo.com>; PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [External] [案例号: CAS-06804-R3Z5V3] % |普通事件|lenovo|天津农行-大港支行 M930s 开机进入自动修复、蓝屏 % 初次响应 CMIT:0001358

藕工，您好:

很抱歉更新晚了，自上次现场收取的两台问题未解决的电脑的 P2V 分析起来比较复杂。目前刚刚完成其中一台电脑的日志分析。请参见下方内容:

故障电脑:

问题 SN	故障现象
M70P84BG	黑屏

问题原因:

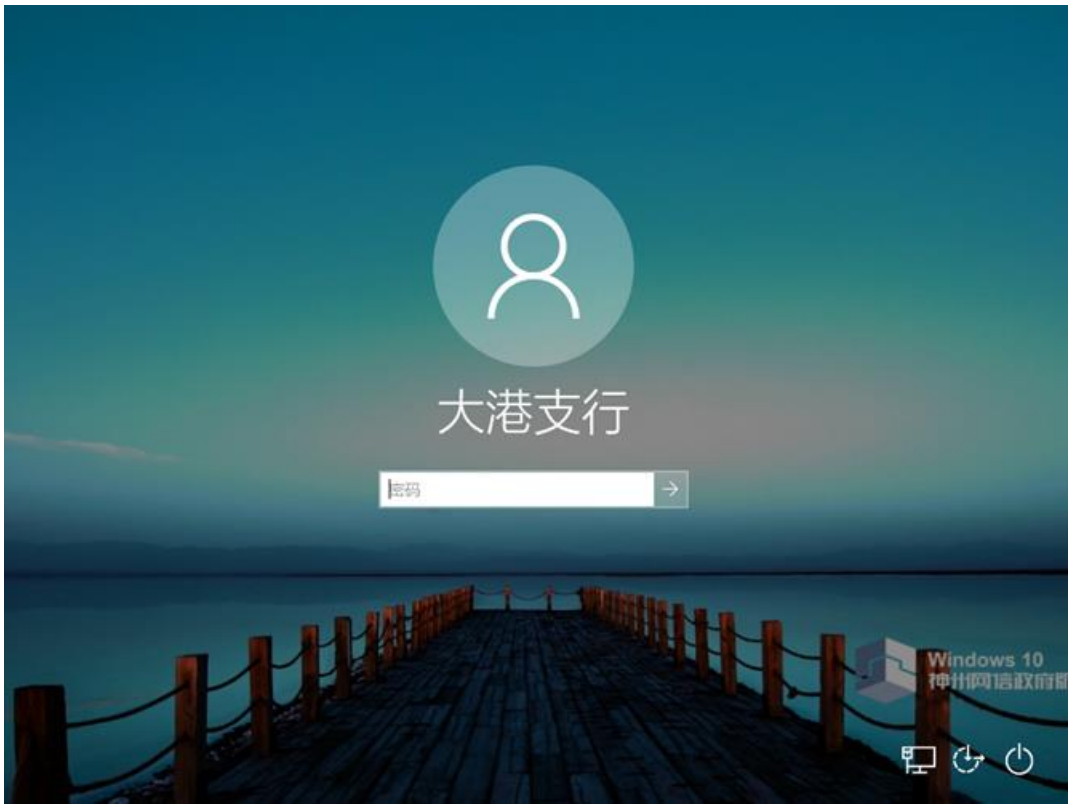
由于 c:\windows\system32 下面驱动文件丢失导致
其中黑屏的直接原因是因为 winlogon 没有启动 userinit, userinit 没有启动 explorer.exe 导致。
进一步 winlogon 的 ETL trace，可以看到 winlogon 在 RequestCredentials 的时候失败了，并且反复循环在重试。

[0]03E0.03E4::09/21/2022-13:37:18.261 [core]StateFn: DisplayLegalNotice/Exit
[0]03E0.**0784**::09/21/2022-13:37:18.261 [core]StateFn: Request_Logon_Credz/Execute
[0]03E0.**0784**::09/21/2022-13:37:18.261 [core]Logon dialog timeout is 30000.
[0]03E0.**0784**::09/21/2022-13:37:18.263 [core]RequestCredentials failed, status = -2147418113
[0]03E0.03E4::09/21/2022-13:37:18.263 [core]StateFn: Request_Logon_Credz/Exit
[0]03E0.03E4::09/21/2022-13:37:18.263 [core]StateFn: Welcome_Return/Enter
[0]03E0.**0784**::09/21/2022-13:37:18.263 [core]StateFn: Welcome/Execute
[0]03E0.03E4::09/21/2022-13:37:18.269 [core]StateFn: Welcome/Exit
[0]03E0.**0784**::09/21/2022-13:37:18.269 [core]StateFn: DisplayLegalNotice/Execute
[0]03E0.03E4::09/21/2022-13:37:18.269 [core]StateFn: DisplayLegalNotice/Exit
[0]03E0.**0784**::09/21/2022-13:37:18.269 [core]StateFn: Request_Logon_Credz/Execute
[0]03E0.**0784**::09/21/2022-13:37:18.270 [core]Logon dialog timeout is 30000.
[0]03E0.**0784**::09/21/2022-13:37:18.272 [core]RequestCredentials failed, status = -2147418113
[0]03E0.03E4::09/21/2022-13:37:18.272 [core]StateFn: Request_Logon_Credz/Exit
[0]03E0.03E4::09/21/2022-13:37:18.272 [core]StateFn: Welcome_Return/Enter
[0]03E0.**0784**::09/21/2022-13:37:18.272 [core]StateFn: Welcome/Execute
[0]03E0.03E4::09/21/2022-13:37:18.279 [core]StateFn: Welcome/Exit
[0]03E0.**0784**::09/21/2022-13:37:18.279 [core]StateFn: DisplayLegalNotice/Execute
[0]03E0.03E4::09/21/2022-13:37:18.279 [core]StateFn: DisplayLegalNotice/Exit
[0]03E0.**0784**::09/21/2022-13:37:18.279 [core]StateFn: Request_Logon_Credz/Execute
[0]03E0.**0784**::09/21/2022-13:37:18.280 [core]Logon dialog timeout is 30000.

[0]03E0.**0784**::09/21/2022-13:37:18.281 [core]RequestCredentials failed, status = -2147418113
[0]03E0.03E4::09/21/2022-13:37:18.281 [core]StateFn: Request_Logon_Credz/Exit
[0]03E0.03E4::09/21/2022-13:37:18.281 [core]StateFn: Welcome_Return/Enter
[0]03E0.**0784**::09/21/2022-13:37:18.282 [core]StateFn: Welcome/Execute
至于反复循环重试的原因是由于系统的很多服务都启动失败了。失败的原因是 0x0000007e = ERROR_MOD_NOT_FOUND。这个原因是由于有驱动 missing 导致的。

Service Name Display Name State Start State Start Error Win32 Exit Start Type
=========== =========== ======= ============ ========== ========== ==========
CertPropSvc CertPropSvc STOPPED SC_START_FAIL 0x0000007e = ERROR_MOD_NOT_FOUND Demand
DsmSvc DsmSvc STOPPED SC_START_FAIL 0x0000007e = ERROR_MOD_NOT_FOUND Demand
NcbService NcbService STOPPED SC_START_FAIL 0x0000007e = ERROR_MOD_NOT_FOUND Demand
ProfSvc ProfSvc STOPPED SC_START_FAIL 0x0000007e = ERROR_MOD_NOT_FOUND Auto
SessionEnv SessionEnv STOPPED SC_START_FAIL 0x0000007e = ERROR_MOD_NOT_FOUND Demand
UserManager UserManager STOPPED SC_START_FAIL 0x0000042c = ERROR_SERVICE_DEPENDENCY_FAIL 0x0000042c = ERROR_SERVICE_DEPENDENCY_FAIL Auto

查看服务启动的过程，共发现丢失 3 个组件:
\Device\HarddiskVolume3\Windows\System32\WinSCard.dll
\Device\HarddiskVolume3\Windows\System32\OLEAUT32.dll
\Device\HarddiskVolume3\Windows\System32\devicesetupmanager.dll
将上述文件从正常电脑拷贝之后，问题发生变化，出现其他的报错问题，如 dwm winlogon 的 crash 问题，再次抓取上述日志后发现仍然有文件丢失。根据经验判断，system32 下应有很多驱动文件丢失的情况出现，因此若解决此问题，需要如下步骤:
找到一台安装相同操作系统的电脑，将 system32 下的驱动文件全部拷贝至该电脑相同路径，则可以正常启动该电脑。



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 9 月 13 日 10:06
收件人: 'Hongfa HF3 Ou' <ouhf3@lenovo.com>
抄送: Liu Jian <liujian@cmgos.com>; Hepeng HP14 Wang <wanghp14@lenovo.com>; PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [External] [案例号: CAS-06804-R3Z5V3] % |普通事件|lenovo|天津农行-大港支行 M930s 开机进入自动修复、蓝屏 % 初次响应 CMIT:0001358

藕工，您好:

您上传的两个 dump 已分析完毕，请参见下面的分析说明:

1. MEMORY1.DMP 中系统是于 9/6 0:53 发生了 0xa 的蓝屏， call stack 中显示系统在做时钟转换相关的操作，由于读取了 IRQL 比较高的地址触发的，但是由于地址已经无效，无法追溯过去的行为。
2. MEMORY2.DMP 中系统于 9/6 23:03 发生了 0x3b 的蓝屏，call stack 中显示系统底层在做查找对象名的操作，call 到了 filter manager 进行 IO cpmpletion 和验证文件名，最后被捕获到异常触发了蓝屏。第 13 帧中有 FLMonDrv.sys 这个组件在操作，之后 filter manager 在验证文件名的时候便发生了异常，FLMonDrv.sys 是三方软件，时间戳是 2021 年 7 月的，建议升级或者找厂商看一下。

====dump analysis====

//Memory1.dmp 中系统是于 9/6 0:53 发生了 0xa 的蓝屏，是由于读取了 IRQL 比较高的地址触发的：

```
Windows 10 Kernel Version 17763 MP (12 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS
Edition build lab: 17763.1.amd64fre.rs5_release.180914-1434
Debug session time: Tue Sep  6 00:53:14.810 2022 (UTC + 8:00)
System Uptime: 0 days 0:13:39.775
SystemManufacturer = LENOVO
SystemProductName = 11CXCTO1WW
Processor: Intel(R) Core(TM) i5-10500 CPU @ 3.10GHz

IRQL_NOT_LESS_OR_EQUAL (a)
An attempt was made to access a pageable (or completely invalid) address at an
interrupt request level (IRQL) that is too high.  This is usually caused by
drivers using improper addresses.
If a kernel debugger is available get the stack backtrace.
Arguments:
Arg1: fffff80002b5932c, memory referenced
Arg2: 00000000000000ff, IRQL
Arg3: 000000000000006e, bitfield :
        bit 0 : value 0 = read operation, 1 = write operation
        bit 3 : value 0 = not an execute operation, 1 = execute operation (only
on chips which support this level of status)
Arg4: fffff800016ea1cb, address which referenced memory
```

//call stack 中显示系统在做时钟转换相关的操作，访问了无效地址而发生了 pagefault：

```
Process               AttachedProcess          Thread           CID       U
serTime KernelTime ContextSwitches Wait Reason Time State
Idle (fffff80001b739c0) System (ffffd68d8c6a3300) ffff9b0097ea1300
0.0            0s 12m:58.656         276235 Executive   15ms Running on CPU
8

# Call
Site
                                  Info
0 nt!KeBugCheckEx+0x0
1 nt!KiBugCheckDispatch+0x69
2
nt!KiPageFault+0x454
                                        TrapFrame @ ffffd40cd429f470
```

```
3 nt!KiCheckForTimerExpiration+0x13b
4 nt!KeAccumulateTicks+0x30
5 nt!PpmIdleExecuteTransition+0x893
6 nt!PoIdle+0x33f
7 nt!KiIdleLoop+0x2c

This thread is crashing
```

//Bugcheck 参数 1 和参数 4 中的地址已经无效了：

```
8: kd> !pool fffff80002b5932c
Pool page fffff80002b5932c region is Unknown
fffff80002b59000 is not a valid large pool allocation, checking large session
pool...

8: kd> !pool fffff800016ea1cb
Pool page fffff800016ea1cb region is Unknown
fffff800016ea000 is not a valid large pool allocation, checking large session
pool...
```

//第 4 帧中系统在做计时相关的操作，但是部分时钟参数已经无法解析了：

```
8: kd> .frame /r 0x4;.echo;!mex.x
04 ffffd40c`d429f680 fffff800`016e8af3     nt!KeAccumulateTicks+0x30
rax=ffffffffffffffff rbx=ffff9b0097e91180 rcx=00000001e8a22be0
rdx=000000000000ccf1 rsi=000000000000ccf1 rdi=000000000000ccf1
rip=fffff800016e9cc0 rsp=ffffd40cd429f680 rbp=0000000000000000
r8=000000000000ccf1  r9=0000000000000000 r10=fffff8000208ab00
r11=0000000000000000 r12=ffffd68d923310f0 r13=0000000000000000
r14=00000001e8b92b00 r15=00000001e8b6e047
iopl=0         nv up di ng nz na po nc
cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00000086
nt!KeAccumulateTicks+0x30:
fffff800`016e9cc0   89b3742e0000      mov       dword    ptr    [rbx+2E74h],esi
ds:002b:ffff9b00`97e93ff4=0000ccf1

@rbx              Prcb = 0xffff9b00`97e91180
@edi              LastTick = 0xccf1
<unavailable>     CurrentTick = <value unavailable>
@ebp              PreviousIrql = 0x00 ''
ffffd40c`d429f700 ProcessorMode = 0n0 ''
<unavailable>     Slot = <value unavailable>
@r14b             DpcStackCaptured = 0x00 ''
@esi              TickPeriods = 0xccf1
<unavailable>     MaximumDpcQueueDepth = <value unavailable>
<unavailable>     Thread = <value unavailable>
<unavailable>     BugcheckCycleTime = <value unavailable>
<unavailable>     Next = <value unavailable>
```

//Memory2.dmp 中系统于 9/6 23:03 发生了 0x3b 的蓝屏：

```
Dump Name: MEMORY2.dmp
Windows 10 Kernel Version 17763 MP (12 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS
Edition build lab: 17763.1.amd64fre.rs5_release.180914-1434
Kernel base = 0xfffff807`0f618000 PsLoadedModuleList = 0xfffff807`0fa325d0
```

```
Debug session time: Tue Sep  6 23:03:18.827 2022 (UTC + 8:00)
System Uptime: 0 days 0:00:25.828
SystemManufacturer = LENOVO
SystemProductName = 11CXCTO1WW
Processor: Intel(R) Core(TM) i5-10500 CPU @ 3.10GHz

SYSTEM_SERVICE_EXCEPTION (3b)
An exception happened while executing a system service routine.
Arguments:
Arg1: 0000000080000003, Exception code that caused the BugCheck
Arg2: fffff8070f7d77c8, Address of the instruction which caused the BugCheck
Arg3: ffffda8f2f65e110, Address of the context record for the exception that
caused the BugCheck
Arg4: 0000000000000000, zero.
```

//call stack 中显示系统底层在做查找对象名的操作，call 到了 filter manager 完成 IO 和验证文件名，最后被捕获到异常触发了蓝屏：

```
Process                          Thread           CID       UserTime  KernelTime
ContextSwitches Wait Reason Time State
svchost.exe                 (ffffdb8fff4f7080)               ffffdb8104d440c0
8ac.8b0         0s       16ms               4 Executive     0s Running on CPU 8

#                                                                          Call
Site
             Info
0 nt!KeBugCheckEx+0x0
 1 nt!KiBugCheckDispatch+0x69
 2 nt!KiSystemServiceHandler+0x7c
 3 nt!RtlpExecuteHandlerForException+0xf
4 nt!RtlDispatchException+0x430
 5 nt!KiDispatchException+0x144
 6 nt!KiExceptionDispatch+0xc2
 7
nt!KiDebugServiceTrap+0x30d
                 TrapFrame @ ffffda8f2f65e970
8 nt!DebugPrompt+0x18
 9 nt!DbgPrompt+0x35
 a FLTMGR!FltpvPrintErrors+0x183
 b FLTMGR!FltpvValidateFileNameOptions+0x4c
c FLTMGR!FltvGetFileNameInformation+0x33
d FLMonDrv+0x1fb2
 e FLTMGR!FltvPostOperation+0xb5
 f FLTMGR!FltpPerformPostCallbacks+0x32e
10 FLTMGR!FltpProcessIoCompletion+0x8
11 FLTMGR!FltpPassThroughCompletionWorker+0x73
12 FLTMGR!FltpLegacyProcessingAfterPreCallbacksCompleted+0x301
13 FLTMGR!FltpCreate+0x2f9
14 nt!IopfCallDriver+0x56
15 nt!IovCallDriver+0x275
16 nt!IofCallDriver+0x12eadf
17 nt!IoCallDriverWithTracing+0x34
18 nt!IopParseDevice+0x632
19 nt!ObpLookupObjectName+0x719
1a nt!ObOpenObjectByNameEx+0x1df
```

```
1b nt!IopCreateFile+0x822
1c nt!NtOpenFile+0x58
1d nt!KiSystemServiceCopyEnd+0x25
1e 0x7fff3d00fdc4

This thread is crashing
```

//参数 1 代表系统发生了异常断点，但是参数 4 的地址已经无法解析了：

```
8: kd> dx KiBugCheckDriver
KiBugCheckDriver : 0x0 [Type: _UNICODE_STRING *]
8: kd> !error 0000000080000003
Error code: (HRESULT) 0x80000003 (2147483651) - ?????????
```

A breakpoint or ASSERT was encountered when no kernel debugger was attached to the system.

```
Running: !pool 0xffffda8f2f65e110 2
Pool page ffffda8f2f65e110 region is Unknown
ffffda8f2f65e000 is not a valid large pool allocation, checking large session
pool...
ffffda8f2f65e000 is not valid pool. Checking for freed (or corrupt) pool
Address ffffda8f2f65e000 could not be read. It may be a freed, invalid or paged
out page
```

//第 19 帧和第 13 帧中涉及到了对象是 rpcss.dll，以及 FltMgr, Ntfs 设备：

```
8: kd> .frame /r 0x19;.echo;!mex.x
19 ffffda8f`2f65f550 fffff807`0fc5f82f     nt!ObpLookupObjectName+0x719
rax=0000000000000002 rbx=fffff8070fc8c850 rcx=fffff802629b1c58
rdx=ffffda8f2f65001f rsi=ffffdb8ffdc9ba00 rdi=00000000000000ba
rip=fffff8070fc61229 rsp=ffffda8f2f65f550 rbp=ffffda8f2f65f650
r8=ffffda8f2f65eb90  r9=0000000000000002 r10=ffffda8f2f65e970
r11=0000000000000000 r12=ffffdb810165aae0 r13=0000000000000840
r14=ffffdb8ffdc9ba30 r15=ffffdb810165aca0
iopl=0         nv up ei ng nz na pe nc
cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00000282
nt!ObpLookupObjectName+0x719:
fffff807`0fc61229 8bf8            mov     edi,eax

<unavailable>     RootDirectoryHandle = <value unavailable>
ffffda8f`2f65f728          ObjectName          =          0xffffda8f`2f65f7b8
"\Device\HarddiskVolume3\Windows\system32\rpcss.dll"

8: kd> .frame /r 0x13;.echo;!mex.x
13 ffffda8f`2f65f220 fffff807`0f788c2a     FLTMGR!FltpCreate+0x2f9
rax=0000000000000002 rbx=0000000000000000 rcx=fffff802629b1c58
rdx=ffffda8f2f65001f rsi=fffff802629b9060 rdi=ffffdb8ff5eec6c0
rip=fffff802629cd559 rsp=ffffda8f2f65f220 rbp=ffffda8f2f65f2a0
r14=ffffdb81099d4b40 r15=0000000000400000
iopl=0         nv up ei ng nz na pe nc
cs=0010  ss=0018  ds=002b  es=002b  fs=0053  gs=002b             efl=00000282
FLTMGR!FltpCreate+0x2f9:
fffff802`629cd559    4c8b642478        mov        r12,qword    ptr    [rsp+78h]
ss:0018:ffffda8f`2f65f298=ffffdb81099d4fb8
```

```
@rdi                 DeviceObject     =     0xffffdb8f`f5eec6c0     Device     for
"\FileSystem\FltMgr"
@r14               Irp = 0xffffdb81`099d4b40
@r12               irpSp = 0xffffdb81`099d4f70 IRP_MJ_CREATE / 0x0 for Device for
"\FileSystem\FltMgr"
ffffda8f`2f65f260 icc = struct _IRP_CALL_CTRL
@bl                fullProcessing = 0x00 ''
@eax               status = 0n2
@r13                         fileObject           =           0xffffdb81`06354570
"\Windows\System32\rpcss.dll" - Device for "\FileSystem\Ntfs"
@r15d              isFltMgrGeneratedCreate = 0x00 ''
```

//第 13 帧中有 FLMonDrv.sys 这个组件在操作，之后 filter manager 在验证文件名的时候便发生了异常，FLMonDrv.sys 是三方软件，时间戳是 2021 年 7 月的，建议升级或者找厂商看一下：

```
start             end                 module name
fffff802`66ef0000 fffff802`66f04000   FLMonDrv
    Loaded symbol image file: FLMonDrv.sys
    Image path: \SystemRoot\system32\DRIVERS\FLMonDrv.sys
    Image name: FLMonDrv.sys
    Timestamp:        Tue Jul 27 14:36:16 2021 (60FFA960)
    CheckSum:         0001666C
    ImageSize:        00014000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
```


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: Hongfa HF3 Ou <ouhf3@lenovo.com>
发送时间: 2022 年 9 月 8 日 14:01
收件人: Li Qi <liqi@cmgos.com>
抄送: Liu Jian <liujian@cmgos.com>; Hepeng HP14 Wang <wanghp14@lenovo.com>
主题: 回复: [External] [案例号: CAS-06804-R3Z5V3]％ |普通事件|lenovo|天津农行-大港支行 M930s 开机进入自动修复、蓝屏 ％初次响应 CMIT:0001358

Hi，李工
我们拿回来用户的 ghost 镜像在研发实验室通过“非正常关机的方式”复现到了蓝屏。

以下是 dump 文件：
链接：https://pan.baidu.com/s/1LCfOgOHYQxk2EUwsHxTPfw?pwd=xcco
提取码：xcco

辛苦帮忙看下 dump 吧，谢谢。

OuHongfa (藕宏发)
18910864457
CSD L2 Technical Support

发件人: Hongfa HF3 Ou
发送时间: 2022 年 8 月 19 日 16:48
收件人: Li Qi <liqi@cmgos.com>
主题: 转发: [External] [案例号: CAS-06804-R3Z5V3] % |普通事件|lenovo|天津农行-大港支行 M930s 开机进入自动修复、蓝屏 % 初次响应 CMIT:0001358

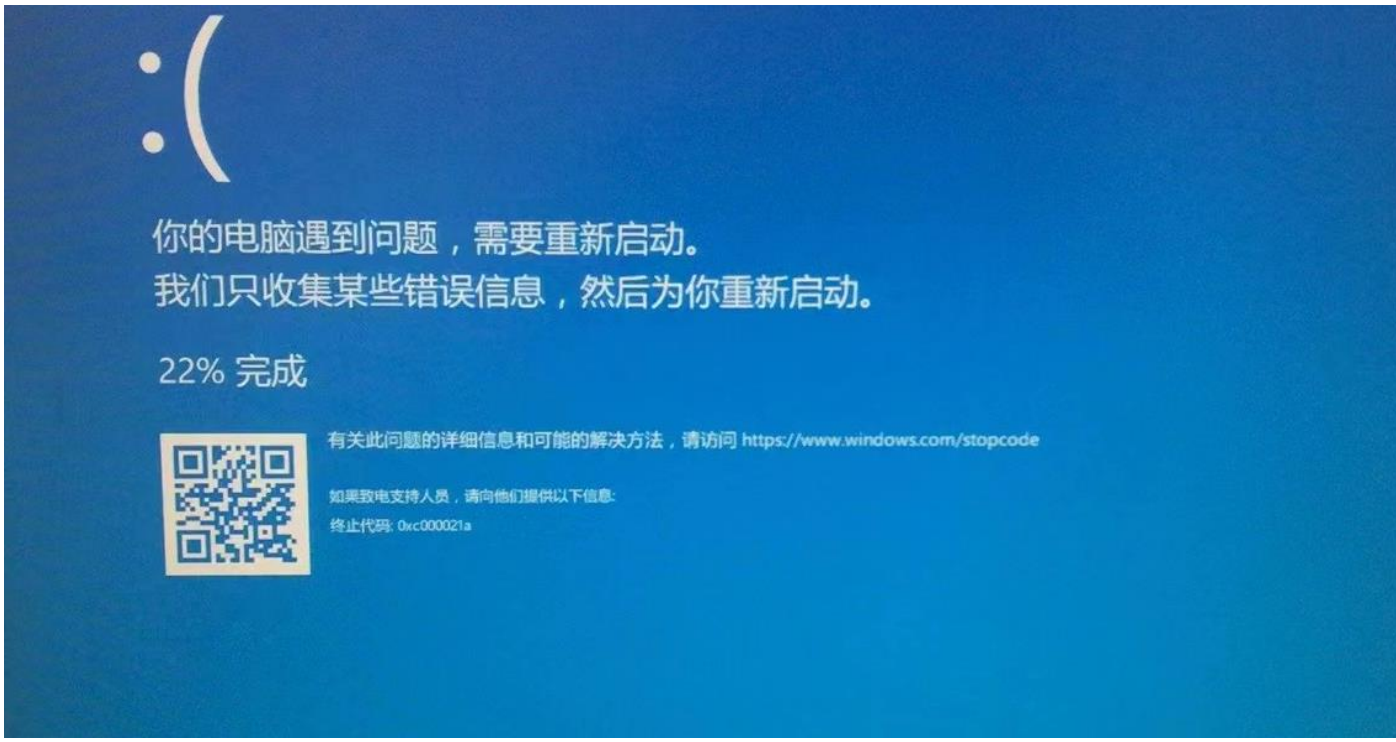
附件又被拦截了。。。

OuHongfa (藕宏发)
18910864457
CSD L2 Technical Support

发件人: Hongfa HF3 Ou
发送时间: 2022 年 8 月 18 日 14:05
收件人: XinMinA Li <lixma@lenovo.com>; Claire NH1 Yang <yangnh1@Lenovo.com>; Jing Jing4 Ye <yejing4@lenovo.com>; Joe jue1 Zhang <zhangjue1@lenovo.com>; Hepeng HP14 Wang <wanghp14@Lenovo.com>; Lingan LA1 Zhang <zhangla1@lenovo.com>; Dones YS1 Dong <dongys1@lenovo.com>; Sally YS1 Hou <houys1@lenovo.com>
主题: 回复: [External] [案例号: CAS-06804-R3Z5V3] % |普通事件|lenovo|天津农行-大港支行 M930s 开机进入自动修复、蓝屏 % 初次响应 CMIT:0001358

Hi，
前天天津农行柳滩支行上门情况：
故障现象：logo 后重启（如附件视频）
系统进不去了，PE 进入发现有 fulldump 文件，客户说之前出现过蓝屏。
dump 文件和 log 文件如下：
链接：https://pan.baidu.com/s/1RdUpcNSZ2iyGFO8378PW9Q?pwd=w25k
提取码：w25k

昨天天津农行青光支行上门情况：
故障现象：开机蓝屏（0xc000021a）



系统进不去了，PE 下发现没有 dump 文件，
log 文件如下：
链接：https://pan.baidu.com/s/1V6G_kOG_st_qcJ3T8h1CIA?pwd=brjx
提取码：brjx

OuHongfa (藕宏发)
18910864457
CSD L2 Technical Support

发件人: Hongfa HF3 Ou
发送时间: 2022 年 8 月 15 日 9:12
收件人: XinMinA Li <lixma@lenovo.com>; Claire NH1 Yang <yangnh1@Lenovo.com>; Jing Jing4 Ye <yejing4@lenovo.com>; Joe jue1 Zhang <zhangjue1@lenovo.com>; Hepeng HP14 Wang <wanghp14@Lenovo.com>; Lingan LA1 Zhang <zhangla1@lenovo.com>; Dones YS1 Dong <dongys1@lenovo.com>; Sally YS1 Hou <houys1@lenovo.com>
主题: 回复: [External] [案例号: CAS-06804-R3Z5V3]% |普通事件|lenovo|天津农行-大港支行 M930s 开机进入自动修复、蓝屏 %初次响应 CMIT:0001358

Hi，
用户的系统和软件我们 ghost 出来了，如下：
链接：https://pan.baidu.com/s/1I87tzCog2Zj3CaxZSY4BdQ?pwd=8rf9
提取码：8rf9
谢谢。

OuHongfa (藕宏发)
18910864457
CSD L2 Technical Support

发件人: XinMinA Li <lixma@lenovo.com>
发送时间: 2022 年 8 月 11 日 18:14
收件人: Claire NH1 Yang <yangnh1@lenovo.com>; Jing Jing4 Ye <yejing4@lenovo.com>; Joe jue1 Zhang <zhangjue1@lenovo.com>; Hepeng HP14 Wang <wanghp14@lenovo.com>; Hongfa HF3 Ou <ouhf3@lenovo.com>; Lingan LA1 Zhang <zhangla1@lenovo.com>; Dones YS1 Dong <dongys1@lenovo.com>; Sally YS1 Hou <houys1@lenovo.com>
主题: 回复: [External] [案例号: CAS-06804-R3Z5V3] % |普通事件|lenovo|天津农行-大港支行 M930s 开机进入自动修复、蓝屏 % 初次响应 CMIT:0001358

Hi,宏发,

我在这个文档中放了个 cmd 脚本，可以用来进行相关的系统设置和收集 log，具体请参考文档中的附件部分。

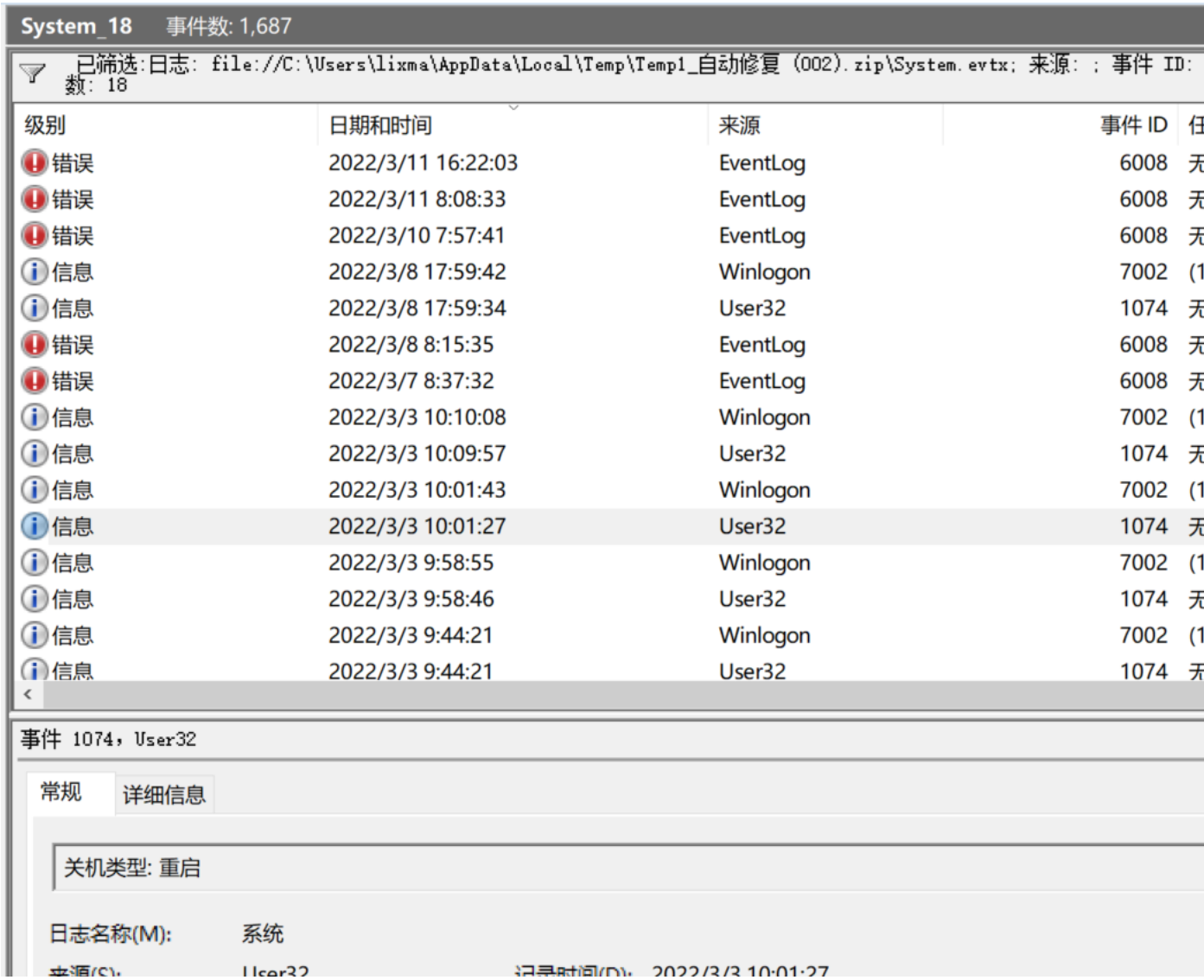
发件人: Claire NH1 Yang <yangnh1@lenovo.com>
发送时间: 2022 年 8 月 11 日 17:11
收件人: XinMinA Li <lixma@lenovo.com>; Jing Jing4 Ye <yejing4@lenovo.com>; Joe jue1 Zhang <zhangjue1@lenovo.com>; Hepeng HP14 Wang <wanghp14@lenovo.com>; Hongfa HF3 Ou <ouhf3@lenovo.com>; Lingan LA1 Zhang <zhangla1@lenovo.com>; Dones YS1 Dong <dongys1@lenovo.com>; Sally YS1 Hou <houys1@lenovo.com>
主题: 回复: [External] [案例号: CAS-06804-R3Z5V3] %|普通事件|lenovo|天津农行-大港支行 M930s 开机进入自动修复、蓝屏 % 初次响应 CMIT:0001358

+Sally thanks

发件人: XinMinA Li <lixma@lenovo.com>
发送时间: 2022 年 8 月 10 日 15:22
收件人: Jing Jing4 Ye <yejing4@lenovo.com>; Joe jue1 Zhang <zhangjue1@lenovo.com>; Hepeng HP14 Wang <wanghp14@lenovo.com>; Hongfa HF3 Ou <ouhf3@lenovo.com>; Claire NH1 Yang <yangnh1@lenovo.com>; Lingan LA1 Zhang <zhangla1@lenovo.com>; Dones YS1 Dong <dongys1@lenovo.com>
主题: 回复: [External] [案例号: CAS-06804-R3Z5V3] % |普通事件|lenovo|天津农行-大港支行 M930s 开机进入自动修复、蓝屏 % 初次响应 CMIT:0001358

Hi,

两个日志类似。几次异常关机的记录中，部分没有看到对应的用户下发关机/重启指令的事件。当然有可能这几次是不能启动到桌面的状态。
有两个 efi 文件的现象，有没有把文件抓出来？



日志名称: System
来源: Microsoft-Windows-GroupPolicy
日期: 2022/3/11 16:23:52
事件 ID: 1096
任务类别: 无
级别: 错误
关键字:
用户: S-1-5-21-3963427384-2358704765-3142656655-1002
计算机: 1408 负责人
描述:

处理组策略失败。Windows 无法应用组策略对象 LocalGPO 的基于注册表的策略设置。只有解决此事件后才会解决组策略设置。有关导致失败的文件名和路径的详细信息，请查看事件详细信息。
事件 Xml:

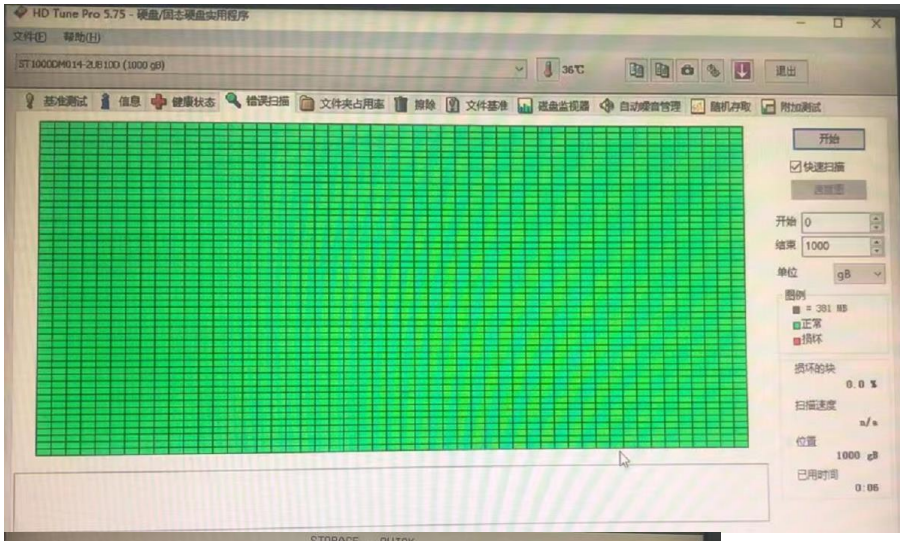
```
<Event xmlns=http://schemas.microsoft.com/win/2004/08/events/event>
 <System>
    <Provider Name="Microsoft-Windows-GroupPolicy" Guid="{aea1b4fa-97d1-45f2-a64c-4d69fffd92c9}" />
  <EventID>1096</EventID>
  <Version>0</Version>
  <Level>2</Level>
  <Task>0</Task>
  <Opcode>1</Opcode>
  <Keywords>0x8000000000000000</Keywords>
  <TimeCreated SystemTime="2022-03-11T08:23:52.4102164Z" />
  <EventRecordID>3128</EventRecordID>
  <Correlation ActivityID="{4ad62545-7411-4bac-bf00-33dd6e6dbbc4}" />
  <Execution ProcessID="2092" ThreadID="4084" />
  <Channel>System</Channel>
  <Computer>1408 负责人</Computer>
  <Security UserID="S-1-5-21-3963427384-2358704765-3142656655-1002" />
 </System>
 <EventData>
  <Data Name="SupportInfo1">2</Data>
  <Data Name="SupportInfo2">1318</Data>
  <Data Name="ProcessingMode">0</Data>
  <Data Name="ProcessingTimeInMilliseconds">31</Data>
  <Data Name="ErrorCode">32</Data>
  <Data Name="ErrorDescription">另一个程序正在使用此文件，进程无法访问。 </Data>
  <Data Name="DCName">
  </Data>
  <Data Name="GPOCNName">LocalGPO</Data>
  <Data Name="FilePath">C:\Windows\System32\GroupPolicy\User\registry.pol</Data>
 </EventData>
</Event>
```

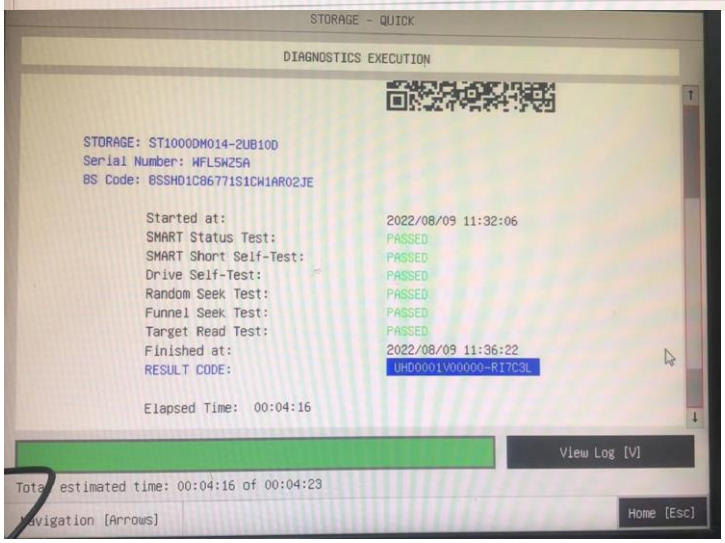
发件人: Jing Jing4 Ye <yejing4@lenovo.com>
发送时间: 2022 年 8 月 10 日 13:42
收件人: Joe jue1 Zhang <zhangjue1@lenovo.com>; Hepeng HP14 Wang <wanghp14@lenovo.com>; Hongfa HF3 Ou <ouhf3@lenovo.com>; Claire NH1 Yang <yangnh1@lenovo.com>; Lingan LA1 Zhang <zhangla1@lenovo.com>; Dones YS1 Dong <dongys1@lenovo.com>; XinMinA Li <lixma@lenovo.com>
主题: 转发: [External] [案例号: CAS-06804-R3Z5V3] % |普通事件|lenovo|天津农行-大港支行 M930s 开机进入自动修复、蓝屏 % 初次响应 CMIT:0001358

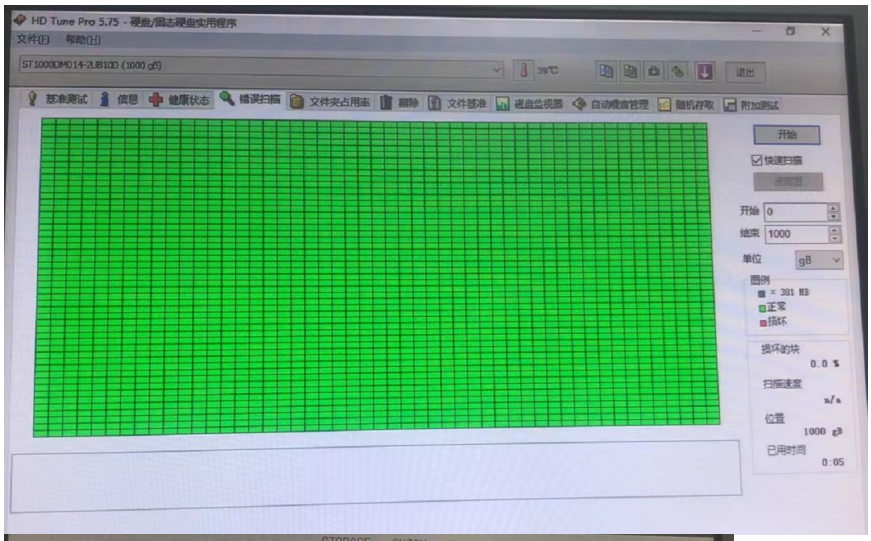
Loop @Lingan LA1 Zhang@Dones YS1 Dong

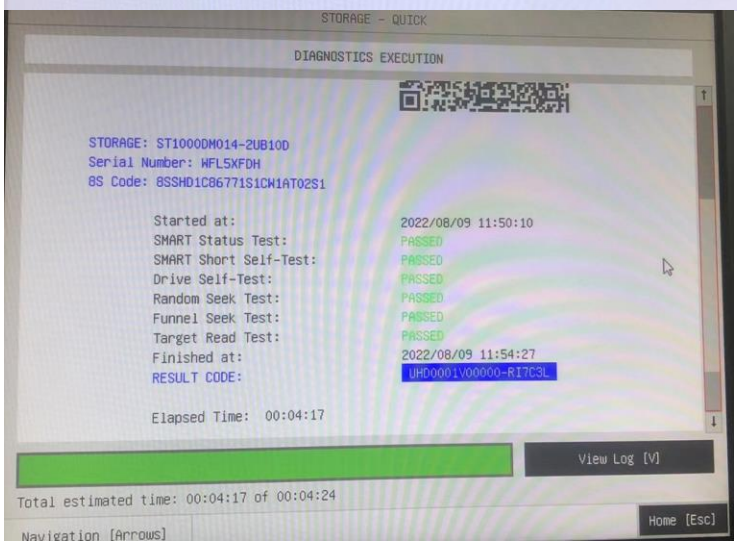
发件人: Hongfa HF3 Ou <ouhf3@lenovo.com>
发送时间: 2022 年 8 月 10 日 11:24
收件人: Li Qi <liqi@cmgos.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>; Jing Jing4 Ye <yejing4@lenovo.com>; Claire NH1 Yang <yangnh1@lenovo.com>; Joe jue1 Zhang <zhangjue1@lenovo.com>; Hepeng HP14 Wang <wanghp14@lenovo.com>
主题: 回复: [External] [案例号: CAS-06804-R3Z5V3]％ |普通事件|lenovo|天津农行-大港支行 M930s 开机进入自动修复、蓝屏 ％初次响应 CMIT:0001358

Hi，
昨天联想服务站工程师上门大港支行，情况更新如下：
1、开机进入自动修复和蓝屏的机器硬盘检测均无坏道，健康度正常。
（每台机器均使用 hd tune 和自带 F10 检测工具测试）







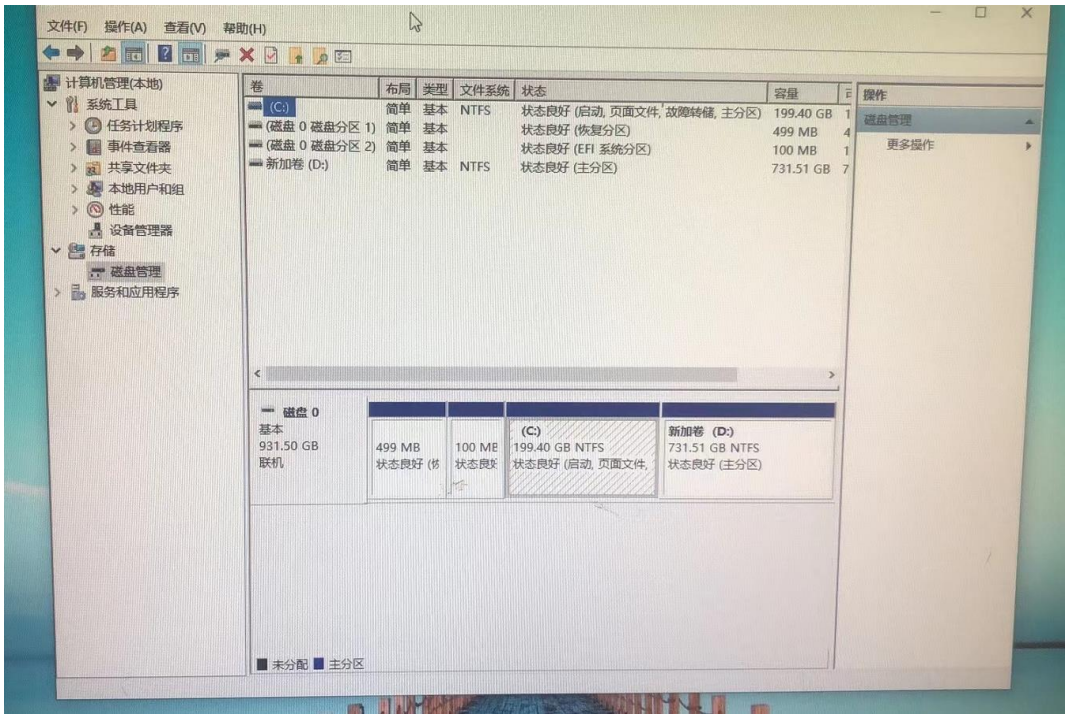


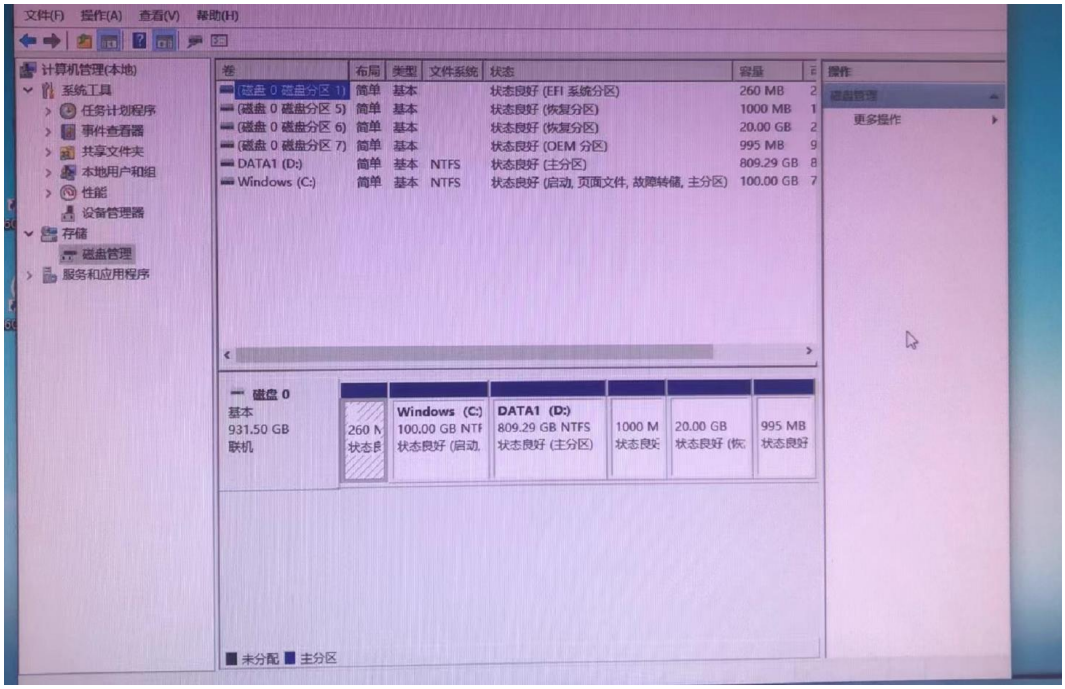
2、对应主机的故障现象和系统日志如附件，帮忙协助分析。（两台机器上均未找到 dump 文件）

3、对于自动修复的机器，使用神州网信纯净镜像标装；对于蓝屏的机器使用联想一键恢复重置系统。

两台机器系统恢复后均安装了用户软件，请用户观察使用

4、以下分别是“使用神州网信纯净镜像标装”和“使用联想一键恢复重置”后的磁盘分区情况：





谢谢。

OuHongfa (藕宏发)
18910864457
CSD L2 Technical Support

发件人: Li Qi <liqi@cmgos.com>
发送时间: 2022 年 8 月 8 日 10:45
收件人: Hongfa HF3 Ou <ouhf3@lenovo.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: [External] [案例号: CAS-06804-R3Z5V3] % |普通事件|lenovo|天津农行-大港支行 M930s 开机进入自动修复、蓝屏 % 初次响应 CMIT:0001358

藕工，您好:

如刚才电话沟通，我谨以此封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:

天津农行反馈系统开机自动进入自动修复（无法修复成功），希望可以协助调查。

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:

目前收集日志有损坏，无法解析。建议当前先进行 NTFS 磁盘的检查，排查磁盘硬件及软件问题。另针对用户当前的 no boot 问题，前期的一些调试无法明确用户实际发生问题的阶段，由于在不同的启动环节出现问题的排查思路是不一样的。因此建议收取 P2V

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