

吴先生, 您好!

很高兴与您电话沟通, 根据沟通的结果, 我将暂时归档此问题。**案例归档后您会收到调查问卷的邮件, 希望可以对我们的服务进行评价。**

工单的归档并不会影响我们为您提供技术支持服务, 如果您的问题复现, 或有新的问题出现, 您也可以致电我们的技术支持热线 4008180055。

案例总结:

案例描述:

工行吉林分行出现蓝屏。在开机过程中蓝屏, 重启后进入系统修复过程但无法进入系统。用户使用半个月左右正常, 后 TMS 进行客户端和策略升级后出现此现象。

案例分析:

- 目前启动失败问题是由于系统启动相关组件损坏导致, 从操作系统层面将, 日志中记录的启动相关的系统文件损坏并不是第一现场, 所以无法捕捉到造成组件损坏的第三方软件或驱动。
- 为了尽可能修复 No Boot 问题, 从问题现象和 Log 分析出发反复 Troubleshooting, 但尝试的方法暂无法成功修复此问题。
- 除了暂未重装的 2 台问题机器, 其余计算机重装后问题不再复现, 暂无复现此问题的测试环境。

案例进展及建议操作:

- 鉴于上述问题, 继续修复 No Boot 问题对于定位是谁造成了系统组件损坏帮助不大, 且耗时较长。
- 建议后续在可以复现问题的测试环境进行对比测试, 逐一安装三方软件并更新策略、观察, 以便更准确地定位具体问题原因。
- 如果定位到三方程序, 则建议查看其记录的 Log 信息确认具体行为。

贾伟 Jia Wei
神州网信技术有限公司
服务支持电话: 400-818-0055

电子邮箱: jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei

发送时间: 2022 年 2 月 9 日 10:32

收件人: '飞行小子' <7840160@qq.com>

抄送: ICBC_Notification <ICBC_Notification@cmgos.com>; '吴毓杰' <win10sup@sdicbc.com.cn>

主题: 回复: 回复: [案例号: CAS-05611-L7D0Q4] % |P2|ICBC|工商银行吉林分行反馈蓝屏问题 % 初次响应 CMIT:0001303

孙先生, 您好

很高兴与您电话沟通, 根据之前的沟通结果, 目前此问题的关注点如下:

- 目前启动失败问题是由于系统启动相关组件损坏导致, 从操作系统层面将, 日志中记录的启动相关的系统文件损坏并不是第一现场, 所以无法捕捉到造成组件损坏的第三方软件或驱动。
- 为了尽可能修复 No Boot 问题, 从问题现象和 Log 分析出发反复 Troubleshooting, 但尝试的方法暂无法成功修复此问题。
- 除了暂未重装的 2 台问题机器, 其余计算机重装后问题不再复现, 暂无复现此问题的测试环境。

建议操作:

- 鉴于上述问题, 继续修复 No Boot 问题对于定位是谁造成了系统组件损坏帮助不大, 且耗时较长。
- 建议后续在可以复现问题的测试环境进行对比测试, 逐一安装三方软件并更新策略、观察, 以便更准确地定位具体问题原因。
- 如果定位到三方程序, 则建议查看其记录的 Log 信息确认具体行为。

贾伟 Jia Wei
神州网信技术有限公司
服务支持电话: 400-818-0055
电子邮箱: jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: 飞行小子 <7840160@qq.com>

发送时间: 2022 年 1 月 28 日 16:36

收件人: Jia Wei <jiawei@cmgos.com>

主题: 回复: [案例号: CAS-05611-L7D0Q4] % |P2||CBC|工商银行吉林分行反馈蓝屏问题
% 初次响应 CMIT:0001303

第一台运行命令结果:

管理员: X:\windows\system32\cmd.exe

Microsoft Windows [版本 10.0.17763.107]

(c) 2018 Microsoft Corporation。保留所有权利。

X:\Sources>sfc.exe /scannow /offbootdir=c:\ /offwindir=c:\

开始系统扫描。此过程将需要一些时间。

Windows 资源保护找到了损坏文件，但其中有一些文件无法修复。对于联机修复，位于 windir\Logs\CBS\CBS.log 的 CBS 日志文件有详细信息。例如 C:\Windows\Logs\CBS\CBS.log。对于脱机修复，/OFFLOGFILE 标记提供的日志文件中有详细信息。

X:\Sources>

C:\ 管理员: X:\windows\system32\cmd.exe

Windows 资源保护找到了损坏文件，但其中有一些文件无法修复。对于联机修复，位于 windir\Log\CBS\CBS.log 的 CBS 日志有详细信息。例如 C:\Windows\Log\CBS\CBS.log。对于脱机 /OFFLOGFILE 标记提供的日志文件中有详细信息。

X:\Sources>chkdsk c:
文件系统的类型是 NTFS。
卷标是 Windows。

警告！未指定 /F 参数。
将在只读模式下运行 CHKDSK。

阶段 1: 检查基本文件系统结构...
已处理 561152 个文件记录。
文件验证完成。
已处理 19649 个大型文件记录。
已处理 0 个错误的文件记录。

阶段 2: 检查文件名链接...
已处理 355 个重新解析记录。
已处理 677136 个索引项。
索引验证完成。
已扫描到 0 个未索引文件。
已将 0 个未编制索引的文件恢复到回收箱。
已处理 355 个重新解析记录。

阶段 3: 检查安全描述符...
安全描述符验证完成。
已处理 57993 个数据文件。
CHKDSK 正在验证 Usn 日志...
已处理 40119648 个 USN 字节。
Usn 日志验证完成。

Windows 已扫描文件系统并且没有发现问题。
无需采取进一步操作。

----- 原始邮件 -----

发件人：“Jia Wei” <jiawei@cmgos.com>;

发送时间： 2022 年 1 月 28 日(星期五) 下午 4:04

收件人：“飞行小子”<7840160@qq.com>;

抄送：“ICBC_Notification”<ICBC_Notification@cmgos.com>;“吴毓杰”<win10sup@sdicbc.com.cn>;

主题： 回复：回复：回复：[案例号：CAS-05611-L7D0Q4] % |P2| ICBC|工商银行吉林分行反馈蓝屏问题 %
初次响应 CMIT:0001303

孙先生，您好

0xc000000f 报错可以尝试通过如下方式修复，首先使用 PE 盘启动（如果有 CMGE 系统盘，可以引导启动后同时按下 Shift+F10 启动命令提示符）：

一、检测系统盘是否受损（灰色部分请替换成实际系统盘盘符）

chkdsk C:

```

X:\Sources>chkdsk C
文件系统的类型是 NTFS。

警告！未指定 /F 参数。
将在只读模式下运行 CHKDSK。

阶段 1: 检查基本文件系统结构...
已处理 173824 个文件记录。
文件验证完成。
已处理 2972 个大型文件记录。
已处理 0 个错误的文件记录。

阶段 2: 检查文件名链接...
已处理 88 个重新解析记录。
已处理 224066 个索引项。
索引验证完成。
已扫描到 0 个未索引文件。
已将 0 个未编制索引的文件恢复到回收箱。
已处理 88 个重新解析记录。

阶段 3: 检查安全描述符...
安全描述符验证完成。
已处理 25122 个数据文件。
CHKDSK 正在验证 Usn 日志...
已处理 39974744 个 USN 字节。
Usn 日志验证完成。

Windows 已扫描文件系统并且没有发现问题。
无需采取进一步操作。

总共有 41312255 KB 磁盘空间。
145460 个文件中有 11491032 KB。
25123 个索引 96340 KB。
坏扇区 0 KB。
系统正在使用 270851 KB。
日志文件占用了 55232 KB。
磁盘上 29454032 KB 可用。

每个分配单元中有 4096 字节。
磁盘上共有 10328063 个分配单元。
磁盘上有 7363508 个可用的分配单元。
无法将记录的消息传输到状态为 50 的事件日志。

```

二、使用命令尝试修复这两台计算机（灰色部分请替换成实际系统盘盘符），是否可以进入系统。

```
sfc.exe /scannow /offbootdir=C:\ /offwindir=C:\windows
```

```

X:\Sources>sfc.exe /scannow /offbootdir=C:\ /offwindir=C:\windows
开始系统扫描。此过程将需要一些时间。

```

贾伟 Jia Wei

神州网信技术有限公司

服务支持电话： 400-818-0055

电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei

发送时间: 2022 年 1 月 28 日 13:19

收件人: '飞行小子' <7840160@qq.com>; '吴毓杰' <win10sup@cdc.icbc.com.cn>

抄送: ICBC_Notification <ICBC_Notification@cmgos.com>

主题: 回复: 回复: 回复: [案例号: CAS-05611-L7D0Q4] % |P2|ICBC|工商银行吉林分行反馈蓝屏问题 % 初次响应 CMIT:0001303

孙先生，您好

针对第一台机器，替换文件之后不再出现蓝屏，而出现“自动修复”界面，由此可见替换文件后系统行为发生了变化，可以尝试如下**建议操作：一、关闭自动修复**的方法尝试找到报错信息。



- @吴毓杰很高兴与您电话沟通，目前最终用户表示除了暂未重装的 2 台问题机器，其余计算机重装后问题不再复现。
- 关于 No boot 问题，日志中记录的启动相关的系统文件损坏并不是第一现场，目前从系统日志分析只能针对现有的问题现象尽可能修复。
- 建议后续在可以复现问题的测试环境进行对比测试，以便更准确地定位具体原因。

建议操作：

一、第一台机器，关闭“自动修复”，尝试看到报错信息

1) 首先使用 PE 盘启动（如果有 CMGE 系统盘，可以引导启动后同时按下 Shift+F10 启动命令提示符），为 System 隐藏卷分配盘符

```
diskpart
```

```
list vol
```

```
select vol 3（根据实际卷情况，选择 FAT32 格式，100M 左右的已隐藏卷，此卷为系统卷）
```

```
assign letter=Z
```

```
exit
```

```

Microsoft Windows [版本 10.0.17763.107]
(c) 2018 Microsoft Corporation。保留所有权利。

X:\Sources>diskpart

Microsoft DiskPart 版本 10.0.17763.1

Copyright (C) Microsoft Corporation.
在计算机上: MINWINPC

DISKPART> list vol

   卷 ###      LTR  标签          FS      类型        大小      状态      信息
-----
卷 0          D    WIN10_CMGE  UDF     DVD-ROM    4517 MB   正常
卷 1          恢复      NTFS     磁盘分区  499 MB    正常
卷 2          C        NTFS     磁盘分区  39 GB     正常
卷 3          FAT32    磁盘分区  99 MB     正常      已隐藏

DISKPART> select vol 3

卷 3 是所选卷。

DISKPART> assign letter=Z

DiskPart 成功地分配了驱动器号或装载点。

DISKPART> exit

退出 DiskPart...

```

2) 禁用自动修复，且打开高级选项

```
bcdedit /store Z:\EFI\Microsoft\Boot\BCD /set {default} recoveryenabled no
```

```

X:\Sources>bcdedit /store Z:\EFI\Microsoft\Boot\BCD /set {default} recoveryenabled no
操作成功完成。

```

3) 重启计算机，拍照反馈截图。

二、使用命令尝试修复这两台计算机（灰色部分请替换成实际系统盘盘符），是否可以进入系统。

```
sfc.exe /scannow /offbootdir=C:\ /offwindir=C:\windows
```

```
X:\Sources>sfc.exe /scannow /offbootdir=C:\ /offwindir=C:\windows  
开始系统扫描。此过程将需要一些时间。
```

贾伟 Jia Wei
神州网信技术有限公司
服务支持电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: 飞行小子 <7840160@qq.com>

发送时间: 2022 年 1 月 28 日 9:03

收件人: Jia Wei <jiawei@cmgos.com>

主题: 回复: 回复: [案例号: CAS-05611-L7D0Q4] % |P2|ICBC|工商银行吉林分行反馈蓝屏问题 % 初次响应 CMIT:0001303

上封邮件中二、如何禁用驱动程序强制签名,

操作结果与邮件表述有差异:

启动设置

按一个数字以从下列选项中进行选择:

使用数字键或功能键 F1-F9。

- 1) 启用调试
- 2) 启用启动日志记录
- 3) 启用低分辨率视频
- 4) 启用安全模式
- 5) 启用带网络连接的安全模式
- 6) 启用带命令提示符的安全模式
- 7) 禁用驱动程序强制签名
- 8) 禁用预先启动反恶意软件保护
- 9) 禁用失败后自动重新启动

按 Enter 以返回到操作系统

如果在此界面按下 F10 再按 F1，即可进入恢复环境

因为无 F10 选项，所以未成功进入恢复环境，请帮助……

----- 原始邮件 -----

发件人: "Jia Wei" <jiawei@cmgos.com>;

发送时间: 2022 年 1 月 27 日(星期四) 下午 2:29

收件人: "飞行小子" <7840160@qq.com>;

抄送: "ICBC_Notification" <ICBC_Notification@cmgos.com>; "吴毓杰" <win10sup@sdicbc.com.cn>;

主题: 回复: [案例号: CAS-05611-L7D0Q4] % |P2|ICBC|工商银行吉林分行反馈蓝屏问题 % 初次响应
CMIT:0001303

孙先生，您好

如果上封邮件中二、**如何禁用驱动程序强制签名，进入恢复模式**的操作完成后，需要恢复正常启动模式，可参考如下步骤：

```
diskpart
```

```
list vol
```

```
select vol 3（根据实际卷情况，选择 FAT32 格式，100M 左右的已隐藏卷，此卷为系统卷）
```

```
assign letter=Z
```

```
exit
```

```
bcdedit /store Z:\EFI\Microsoft\Boot\BCD /set {default} advancedoptions off
```

X:\Sources>diskpart

Microsoft DiskPart 版本 10.0.17763.1

Copyright (C) Microsoft Corporation.
在计算机上: MINWINPC

DISKPART> list vol

卷 ###	LTR	标签	FS	类型	大小	状态	信息
卷 0	D	WIN10_CMGE	UDF	DVD-ROM	4517 MB	正常	
卷 1		恢复	NTFS	磁盘分区	499 MB	正常	
卷 2	C		NTFS	磁盘分区	126 GB	正常	
卷 3			FAT32	磁盘分区	100 MB	正常	已隐藏

DISKPART> select vol 3

卷 3 是所选卷。

DISKPART> assign letter=Z

DiskPart 成功地分配了驱动器号或装载点。

DISKPART> exit

退出 DiskPart...

X:\Sources>bcdedit /store Z:\EFI\Microsoft\Boot\BCD /set {default} advancedoptions off
操作成功完成。

贾伟 Jia Wei

神州网信技术有限公司

服务支持电话: 400-818-0055

电子邮箱: jiawei@cmgos.com

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei

发送时间: 2022 年 1 月 27 日 11:27

收件人: '飞行小子' <7840160@qq.com>

抄送: ICBC_Notification <ICBC_Notification@cmgos.com>; '吴毓杰' <win10sup@sdicbc.com.cn>

主题: 回复: 回复: 回复: [案例号: CAS-05611-L7D0Q4] % |P2|ICBC|工商银行吉林分行反馈蓝屏问题 % 初次响应 CMIT:0001303

孙先生, 您好

很高兴与您电话沟通。您可以参考如下内容进行操作。

一、下载、制作系统安装 U 盘。

- 1) 神州网信政府版 V2020-L 系统 iso 文件可通过如下链接下载, 有效期 30 天。(注意: 此版本镜像为纯净版系统, 非 ICBC 定制版, 不可用于系统安装)

<https://download.cmgos.com/api/dynamic/download/ea67255589674635e866cec159e39318>

- 2) 您可以参考附件 pdf 文件, 制作安装 U 盘。

二、如何禁用驱动程序强制签名, 进入恢复模式

- 1) 首先使用 PE 盘启动 (如果有 CMGE 系统盘, 可以引导启动后同时按下 Shift+F10 启动命令提示符), 为 System 隐藏卷分配盘符

```
diskpart
```

```
list vol
```

```
select vol 3 (根据实际卷情况, 选择 FAT32 格式, 100M 左右的已隐藏卷, 此卷为系统卷)
```

```
assign letter=Z
```

```
exit
```

```

Microsoft Windows [版本 10.0.17763.107]
(c) 2018 Microsoft Corporation。保留所有权利。

X:\Sources>diskpart

Microsoft DiskPart 版本 10.0.17763.1

Copyright (C) Microsoft Corporation.
在计算机上: MINWINPC

DISKPART> list vol

卷 ###      LTR  标签          FS      类型          大小      状态      信息
-----
卷 0        D    WIN10_CMGE   UDF     DVD-ROM      4517 MB   正常
卷 1        恢复  NTFS        磁盘分区  499 MB     正常
卷 2        C    NTFS        磁盘分区  39 GB      正常
卷 3        FAT32 磁盘分区    99 MB     正常      已隐藏

DISKPART> select vol 3

卷 3 是所选卷。

DISKPART> assign letter=Z

DiskPart 成功地分配了驱动器号或装载点。

DISKPART> exit

退出 DiskPart...

```

2) 禁用自动修复，且打开高级选项

```
bcdedit /store Z:\EFI\Microsoft\Boot\BCD /set {default} advancedoptions on
```

```
bcdedit /store Z:\EFI\Microsoft\Boot\BCD /set {default} recoveryenabled no
```

```
bcdedit /store S:\EFI\Microsoft\Boot\BCD /enum active (确认图中所示的 recoveryenabled =
No, advancedoptions = Yes)
```

```
X:\Sources\bcdedit /store Z:\EFI\Microsoft\Boot\BCD /set {default} advancedoptions on
操作成功完成。
```

```
X:\Sources\bcdedit /store Z:\EFI\Microsoft\Boot\BCD /set {default} recoveryenabled no
操作成功完成。
```

```
X:\Sources\bcdedit /store Z:\EFI\Microsoft\Boot\BCD /enum active
```

Windows 启动管理器

```
-----
标识符          {bootmgr}
device          partition=Z:
path            \EFI\Microsoft\Boot\bootmgfw.efi
description     Windows Boot Manager
locale          zh-CN
inherit         {globalsettings}
default         {default}
resumeobject    {1c0e16fc-9362-11ea-bd32-00155d240b75}
displayorder    {default}
toolsdisplayorder {memdiag}
timeout         30
```

Windows 启动加载器


```
-----
标识符          {default}
device          partition=C:
path            \Windows\system32\winload.efi
description     Windows 10
locale          zh-CN
inherit         {bootloadersettings}
recoverysequence {1c0e16fe-9362-11ea-bd32-00155d240b75}
displaymessageoverride Recovery
recoveryenabled  No
advancedoptions Yes
isolatedcontext  Yes
allowedinmemorysettings 0x15000075
osdevice        partition=C:
systemroot      \Windows
resumeobject    {1c0e16fc-9362-11ea-bd32-00155d240b75}
nx              OptIn
bootmenupolicy   Standard
```

重启计算机，即可进入启动设置，选择 7 可以禁用驱动程序强制签名

启动设置

按一个数字以从下列选项中进行选择:

使用数字键或功能键 F1-F9。

- 1) 启用调试
- 2) 启用启动日志记录
- 3) 启用低分辨率视频
- 4) 启用安全模式
- 5) 启用带网络连接的安全模式
- 6) 启用带命令提示符的安全模式
-  7) 禁用驱动程序强制签名
- 8) 禁用预先启动反恶意软件保护
- 9) 禁用失败后自动重新启动

按 F10 以查看更多选项

按 Enter 以返回到操作系统

如果在此界面按下 F10 再按 F1，即可进入恢复环境

启动设置

按一个数字以从下列选项中进行选择:

使用数字键或功能键 F1-F9。

1) 启动恢复环境

按 F10 以查看更多选项

按 Enter 以返回到操作系统

贾伟 Jia Wei

神州网信技术有限公司

服务支持电话: 400-818-0055

电子邮箱: jiawei@cmgos.com

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: 飞行小子 <7840160@qq.com>

发送时间: 2022 年 1 月 27 日 9:24

收件人: Jia Wei <jiawei@cmgos.com>

主题: 回复: 回复: [案例号: CAS-05611-L7D0Q4] % |P2|ICBC|工商银行吉林分行反馈蓝屏问题 % 初次响应 CMIT:0001303

老师, 您好

第一台遇到问题: CMGE 系统启动 U 盘或光盘, 在哪里能够得到?

第二台遇到问题: 高级启动选项如何才能进入? BIOS secure boot 开关我检查了。

----- 原始邮件 -----

发件人: "Jia Wei" <jiawei@cmgos.com>;

发送时间: 2022 年 1 月 25 日(星期二) 晚上 11:33

收件人: "飞行小子" <7840160@qq.com>;

抄送: "ICBC_Notification" <ICBC_Notification@cmgos.com>; "吴毓杰" <win10sup@sdic.icbc.com.cn>;

主题: 回复: [案例号: CAS-05611-L7D0Q4] % |P2|ICBC|工商银行吉林分行反馈蓝屏问题 % 初次响应 CMIT:0001303

孙先生, 您好

TMS 第一台 Dump 中, 可以看到系统关键进 csrss.exe 程退出导致启动蓝屏, 而目前怀疑原因是加载 C:\Windows\system32\winsrv.DLL 的时候失败造成。

TMS 第二台 Dump 中, 蓝屏代码是 c000021a, 具体是 smss 进程启动过程有错误。根据以往案件经验, 这个阶段在启动一些系统必备的驱动, 会校验驱动签名文件等。所以问题可能是驱动签名丢失导致的。

建议操作:

针对第一台, 可以使用 CMGE 系统启动 U 盘或光盘启动后, 同时按下 Shift+F3 调出命令提示符。

- 1) 查看这个文件的时间戳、大小等信息, 和同版本级别系统的是否有差异

a) 在命令提示符中，运行如下命令（注意使用“\\”）：

```
wmic datafile where Name="C:\\Windows\\System32\\winsrv.dll" get  
Name,Version,FileSize,CreationDate
```

```
X:\windows\system32>wmic datafile where Name="C:\\Windows\\System32\\winsrv.dll"  
CreationDate      FileSize  Name      Version  
20180915152847.686314+480  66048    c:\\windows\\system32\\winsrv.dll  10.0.17763.
```

b) 在其他 Version 信息与此版本完全相同的、可以正常运行的机器上，以管理员身份运行命令提示符，重复上述操作，确认 CreateDate、FileSize 是否有差异。

2) 如果上述方法确认无差异，可以尝试将正常机器同版本的这个文件拷贝过来进行替换，看是否可以正常启动

a) 同样在 PE 下的命令提示符中，运行如下命令（加粗部分盘符需要按实际情况替换）：

```
Xcopy Z:\winsrv.dll C:\Windows\System32\winsrv.dll
```

```
X:\Sources>xcopy Z:\winsrv.dll C:\Windows\System32\winsrv.dll  
覆盖 C:\Windows\System32\winsrv.dll (Y:是/N:否/A:全部)?Y  
Z:\winsrv.dll  
复制了 1 个文件
```

针对第二台，建议进入恢复模式

1) 在高级启动选项中选择“禁用强制驱动签名”看能否进入系统。具体操作可参考附件《禁用驱动程序强制签名》。

2) 如果后续能进入系统，可以将 C:\Windows\System32\winevt\Logs\Microsoft-Windows-CodeIntegrity%4Operational.evtx 事件日志文件回传，以便进一步排查问题。

3) 如果无法进入系统, 可以使用 CMGE 系统 U 盘启动, 同时按下 Shift+F10 调出命令行窗口, 运行如下命令拷贝此文件 (粗体部分需要替换 U 盘或其他移动介质的实际盘符):

```
Xcopy C:\Windows\System32\winevt\Logs\Microsoft-Windows-CodeIntegrity%4Operational.evtx Z:\
```

```
X:\sources>xcopy C:\Windows\System32\winevt\Logs\Microsoft-Windows-CodeIntegrity%4Operational.evtx Z:\
C:\Windows\System32\winevt\Logs\Microsoft-Windows-CodeIntegrity%4Operational.evtx
复制了 1 个文件
```

Dump 分析:

第一台:

//系统蓝屏发生在刚启动的时候, 蓝屏代码是 0xEF, 即关键进程 csrss.exe 退出

Dump Name: MEMORY.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 = 0xfffff802`13ab5000 PsLoadedModuleList = 0xfffff802`13ecb4d0

Debug session time: Mon Jan 24 15:34:58.897 2022 (UTC + 8:00)

System Uptime: 0 days 0:00:12.859

SystemManufacturer = LENOVO

SystemProductName = 11CWS0BW00

Processor: Intel(R) Core(TM) i5-10500 CPU @ 3.10GHz

Critical Object Termination Bugcheck: EF

Kernel Complete Dump File: Full address space is available.

CRITICAL_PROCESS_DIED (ef)

Arg1: fffffac0dd7cf1080: Process: csrss.exe

Arg2: 0: Process died

Arg3: 0

Arg4: 0

//Crash 的线程如下

0: kd> !mex.t ffffac0dd7a82080

Process	Thread	CID	UserTime	KernelTime	ContextSwitches	Wait Reason	Time State
csrss.exe	(ffffac0dd7cf1080)	ffffac0dd7a82080	3f0.3ec	0s	0s	83	
WrPageIn	0s	Running on CPU 0					

#	Child-SP	Return	Call Site
0	ffffbc01042ea838	fffff8021433dc4d	nt!KeBugCheckEx+0x0
1	ffffbc01042ea840	fffff802142385e3	nt!PspCatchCriticalBreak+0xfd
2	ffffbc01042ea8e0	fffff802140a0ecc	nt!PspTerminateAllThreads+0x197da7
3	ffffbc01042ea950	fffff802140a0fc9	nt!PspTerminateProcess+0xe0
4	ffffbc01042ea990	fffff80213c7e305	nt!NtTerminateProcess+0xa9
5	ffffbc01042eaa00	00007ffcd37bff74	nt!KiSystemServiceCopyEnd+0x25
6	0000003b4f79fc08	00007ff6ef22177b	ntdll!ZwTerminateProcess+0x14
7	0000003b4f79fc10	00007ff6ef221311	csrss!main+0x42b
8	0000003b4f79fc50	00007ff6ef221026	csrss!NtProcessStartup_AfterSecurityCookieInitialized+0x2e1
9	0000003b4f79fce0	00007ffcd377a2ff	csrss!NtProcessStartup+0x16
a	0000003b4f79fd10	0000000000000000	ntdll!RtlUserThreadStart+0x2f

This thread is crashing

//当前进程的 environment 如下，已经加载了 4 个 dll，正常应该会继续加载 C:\Windows\system32\winsrv.DLL，所以怀疑是当前机器中此 dll 有问题

当前问题计算机的 DLL 加载情况：

0: kd> !peb

PEB at 0000003b4f99e000

InheritedAddressSpace: No

ReadImageFileExecOptions: No

BeingDebugged: No

ImageBaseAddress: 00007ff6ef220000

NtGlobalFlag: 0

NtGlobalFlag2: 0

Ldr 00007ffcd38853a0

Ldr.Initialized: Yes

Ldr.InInitializationOrderModuleList: 000001ce4d003760 . 000001ce4d005340

Ldr.InLoadOrderModuleList: 000001ce4d0038d0 . 000001ce4d005320

Ldr.InMemoryOrderModuleList: 000001ce4d0038e0 . 000001ce4d005330

Base	Time Stamp	Module
------	------------	--------

7ff6ef220000	a6477453	May 27 12:51:31 2058 C:\Windows\system32\csrss.exe
--------------	----------	--

7ffcd3720000	65420ea4	Nov 01 16:39:00 2023 C:\Windows\SYSTEM32\ntdll.dll
--------------	----------	--

7ffccf870000	931a7c76	Mar 16 23:49:10 2048 C:\Windows\SYSTEM32\CSRSSRV.dll
--------------	----------	--

7ffccf850000	87ef4d75	Apr 09 05:58:13 2042 C:\Windows\system32\basesrv.DLL
--------------	----------	--

SubSystemData: 0000000000000000

ProcessHeap: 000001ce4ce90000

ProcessParameters: 000001ce4d002dc0

正常计算机的 DLL 加载情况:

16.kd> !peb

PEB at 0000008653f36000

InheritedAddressSpace: No

ReadImageFileExecOptions: No

BeingDebugged: No

ImageBaseAddress: 00007ff74a5a0000

NtGlobalFlag: 0

NtGlobalFlag2: 0

Ldr 00007ffdd77753a0

Ldr.Initialized: Yes

Ldr.InInitializationOrderModuleList: 000002397aec1ed0 . 000002397aecbdc0

Ldr.InLoadOrderModuleList: 000002397aec2040 . 000002397aecbda0

Ldr.InMemoryOrderModuleList: 000002397aec2050 . 000002397aecbdb0

Base	Time Stamp	Module
------	------------	--------

7ff74a5a0000	a6477453	May 27 12:51:31 2058 C:\Windows\system32\csrss.exe
--------------	----------	--

7ffdd7610000	3c398a4b	Jan 07 19:45:15 2002 C:\Windows\SYSTEM32\ntdll.dll
--------------	----------	--

7ffdd35c0000	931a7c76	Mar 16 23:49:10 2048 C:\Windows\SYSTEM32\CSRSSRV.dll
--------------	----------	--

7ffdd35a0000	87ef4d75	Apr 09 05:58:13 2042 C:\Windows\system32\basesrv.DLL
--------------	----------	--

7ffdd3580000	88510fe0	Jun 22 09:37:36 2042 C:\Windows\system32\winsrv.DLL
--------------	----------	---

7ffdd39c0000	ad1c2e55	Jan 12 23:27:17 2062
--------------	----------	----------------------

C:\Windows\System32\kernelbase.dll

7ffdd5fa0000	6fc57844	Jun 04 04:19:16 2029 C:\Windows\System32\kernel32.dll
--------------	----------	---

7ffdd3560000	949f3cf4	Jan 05 20:49:56 2049 C:\Windows\SYSTEM32\winsrvext.dll
--------------	----------	--

7ffdd5310000 316731a3 Apr 07 11:08:19 1996 C:\Windows\System32\USER32.dll
7ffdd4800000 ff141dbb Aug 12 16:20:11 2105 C:\Windows\System32\win32u.dll
7ffdd4c20000 b9f6192c Nov 12 10:34:20 2068 C:\Windows\System32\GDI32.dll
7ffdd43b0000 db59761c Aug 13 18:34:04 2086 C:\Windows\System32\gdi32full.dll
7ffdd37f0000 448f33c2 Jun 14 05:53:06 2006 C:\Windows\System32\msvc_p_win.dll
7ffdd38c0000 48ac8393 Aug 21 04:50:27 2008 C:\Windows\System32\ucrtbase.dll
7ffdd4c50000 56e03de8 Mar 09 23:14:48 2016 C:\Windows\System32\combase.dll
7ffdd48d0000 8280105a May 19 23:14:34 2039 C:\Windows\System32\RPCRT4.dll
7ffdd36b0000 6313481e Sep 03 20:27:10 2022
C:\Windows\System32\bcryptPrimitives.dll
7ffdd47b0000 ca7e64ca Aug 27 17:09:30 2077 C:\Windows\System32\cfgmgr32.dll
7ffdd3550000 9e6eabdd Mar 25 20:04:45 2054 C:\Windows\system32\sxsrv.DLL
7ffdd33e0000 c10f722d Aug 21 22:22:37 2072 C:\Windows\system32\sxs.dll
SubSystemData: 0000000000000000
ProcessHeap: 000002397aec0000
ProcessParameters: 000002397aec1540
CurrentDirectory: 'C:\Windows\system32\
WindowTitle: '< Name not readable >'
ImageFile: 'C:\Windows\system32\csrss.exe'

第二台:

//系统蓝屏发生在刚启动的时候, 蓝屏代码是 c000021a, 第二个参数是
0xc0000034(**STATUS_OBJECT_NAME_NOT_FOUND**)
Dump Name: MEMORY.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 = 0xfffff801`2f404000 PsLoadedModuleList = 0xfffff801`2f81a4d0
Debug session time: Mon Jan 24 14:28:05.992 2022 (UTC + 8:00)
System Uptime: 0 days 0:00:12.955
SystemManufacturer = LENOVO
SystemProductName = 11CWS0BW00
Processor: Intel(R) Core(TM) i5-10500 CPU @ 3.10GHz
Bugcheck: C000021A (FFFF928F85020060, FFFFFFFFC0000034, 0, 1A100010000)
Kernel Complete Dump File: Full address space is available.

WINLOGON_FATAL_ERROR (c000021a)
The Winlogon process terminated unexpectedly.
Arguments:
Arg1: ffff928f85020060, String that identifies the problem.
Arg2: ffffffff00000034, Error Code.
Arg3: 0000000000000000
Arg4: 000001a100010000

```
3: kd> !err ffffffff00000034
0xc0000034 = STATUS_OBJECT_NAME_NOT_FOUND
Object Name not found.
```

//Crash 的线程如下，但这里不是第一现场，而是系统进程触发 GracefulShutdown:

```
3: kd> !mex.t ffffa30b389bb080
Process           AttachedProcess      Thread      CID      UserTime KernelTime
ContextSwitches Wait Reason Time State
System (ffffa30b2dcb9300) smss.exe (ffffa30b384d4040) ffffa30b389bb080
4.368      0s      16ms      769 Executive  0s Running on CPU 3
```

```
# Call Site
0 nt!KeBugCheckEx+0x0
1 nt!PopGracefulShutdown+0x29a
2 nt!PopTransitionSystemPowerStateEx+0x1192
3 nt!NtSetSystemPowerState+0x4c
4 nt!KiSystemServiceCopyEnd+0x25
5 nt!KiServiceLinkage+0x0
6 nt!PopIssueActionRequest+0x9c2eb
7 nt!PopPolicyWorkerAction+0x69
8 nt!PopPolicyWorkerThread+0x8f
9 nt!ExpWorkerThread+0x16a
a nt!PspSystemThreadStartup+0x55
b nt!KiStartSystemThread+0x1c
```

This thread is crashing

//问题发生在 smss 启动过程中，这里进程检测到错误，然后 Terminate;

```
3: kd> !mex.t ffffa30b384d7080
Process           Thread      CID      UserTime KernelTime ContextSwitches Wait
Reason  Time State
smss.exe (ffffa30b384d4040) ffffa30b384d7080 344.350      0s      47ms      12
Suspended 2s.421 Waiting
```

```
# Call Site
0 nt!KiSwapContext+0x76
1 nt!KiSwapThread+0x297
2 nt!KiCommitThreadWait+0x508
```


[3](#) nt!KeWaitForSingleObject+0x520
[4](#) nt!NtInitiatePowerAction+0x1a9
[5](#) nt!KiSystemServiceCopyEnd+0x25
[6](#) nt!KiServiceLinkage+0x0
[7](#) nt!PoShutdownBugCheck+0xd5
[8](#) nt!ExpSystemErrorHandler2+0x62e
[9](#) nt!ExpSystemErrorHandler+0xd8
[a](#) nt!ExpRaiseHardError+0x132
[b](#) nt!NtRaiseHardError+0x1ba
[c](#) nt!KiSystemServiceCopyEnd+0x25
[d](#) ntdll!ZwRaiseHardError+0x14
[e](#) smss!SmpTerminate+0x6d
[f](#) smss!SmpDestroyControlBlock+0xa080
[10](#) smss!SmpStopCsr+0xc845
[11](#) smss!SmpApiCallback+0x395
[12](#) ntdll!TppAlpcpExecuteCallback+0x2ec
[13](#) ntdll!TppWorkerThread+0x3c8
[14](#) ntdll!RtlUserThreadStart+0x2f

This thread has been suspended for 2s.421

//根据以往案件经验，这个阶段在启动一些系统必备的驱动，会校验驱动签名文件等。所以问题可能是驱动签名丢失导致的，建议按照建议操作部分进行操作

贾伟 Jia Wei

神州网信技术有限公司

服务支持电话： 400-818-0055

电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei

发送时间: 2022 年 1 月 24 日 14:19

收件人: '7840160@qq.com' <7840160@qq.com>

抄送: ICBC_Notification <ICBC_Notification@cmgos.com>; '吴毓杰' <win10sup@sdicbc.com.cn>

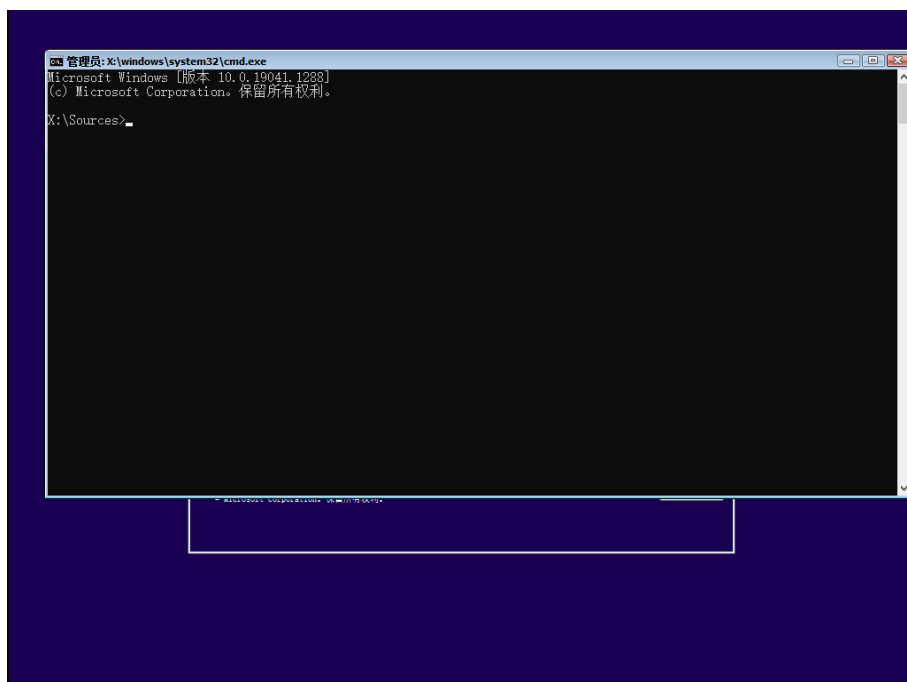
主题: 回复: [案例号: CAS-05611-L7D0Q4] % |P2|ICBC|工商银行吉林分行反馈蓝屏问题 %
初次响应 CMIT:0001303

孙先生, 您好

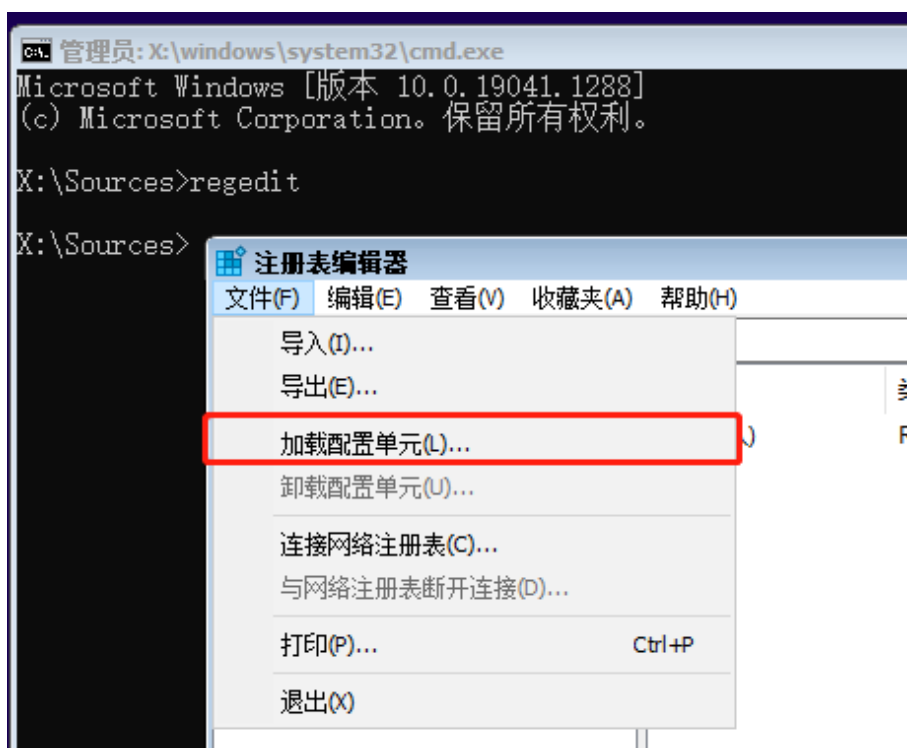
我在本地测试了离线使用注册表方法设置 FullDump, 可以参考如下方法, 如果设置后仍有问题可反馈此邮件:

建议操作:

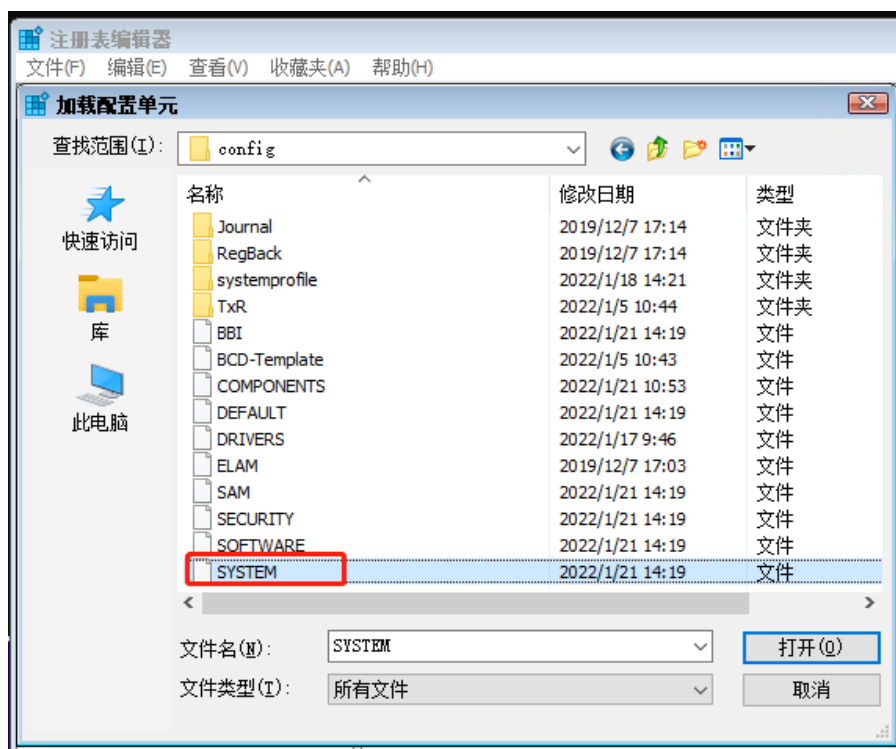
1. 以 Windows 10 神州网信政府版系统光盘或 U 盘启动, 到达安装界面后同时按下 Shift+F10, 调出命令提示符窗口;



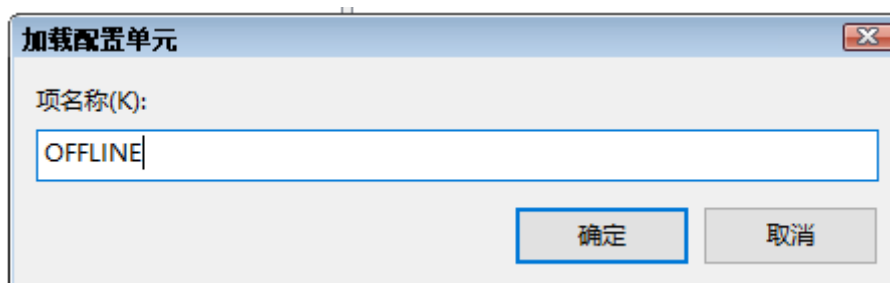
2. 运行命令 `regedit`，调出注册表编辑器；
3. 单击 `HKEY_LOCAL_MACHINE` 项，再点击文件，选择加载配置单元；



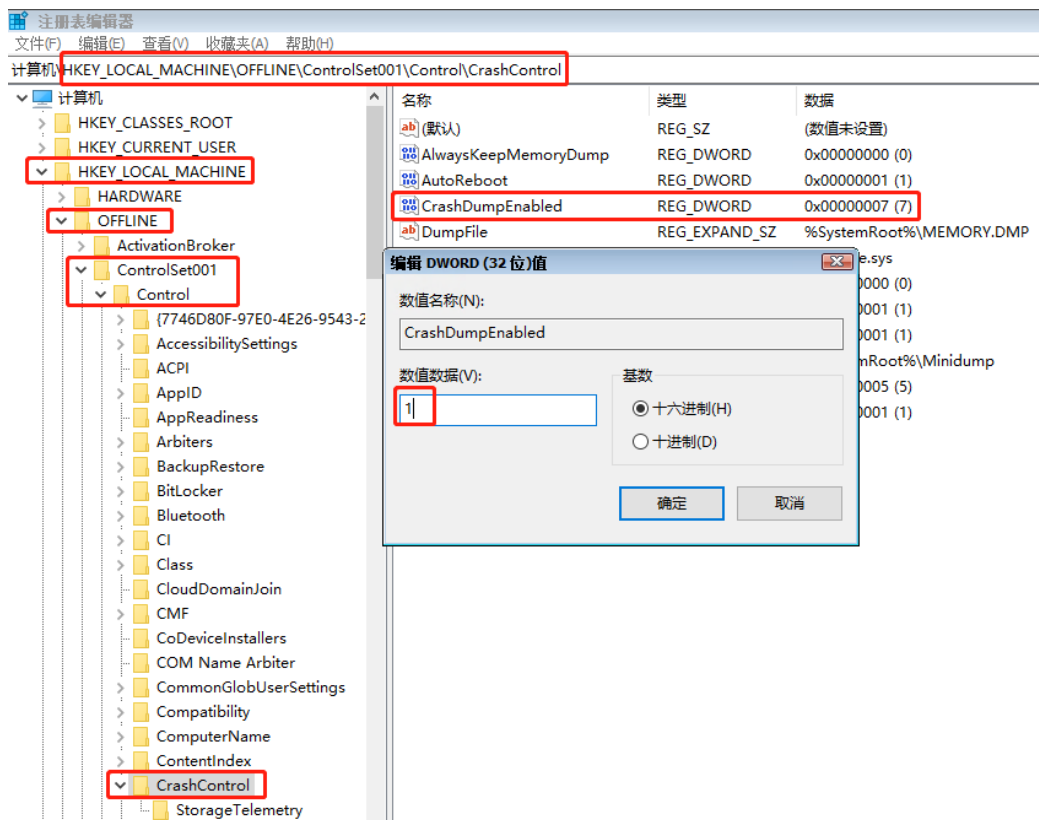
4. 点击此电脑，找到 C:\Windows\system32\config 文件夹，单击 SYSTEM 文件，打开；



5. 为配置单元命名，例如 OFFLINE；



6. 在 HKLM\OFFLINE\ControlSet001\Control\CrashControl 中，将 CrashDumpEnabled 键值改为 1；



7. 单击 OFFLINE 项，再点击文件，选择卸载配置单元；



8. 关闭所有窗口，重启计算机。

贾伟 Jia Wei

神州网信技术有限公司

服务支持电话： 400-818-0055

电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei

发送时间: 2022 年 1 月 21 日 14:06

收件人: 吴毓杰 <win10sup@sdicbc.com.cn>

抄送: ICBC_Notification <ICBC_Notification@cmgos.com>

主题: 回复: [案例号: CAS-05611-L7D0Q4] % |P2|ICBC|工商银行吉林分行反馈蓝屏问题 %
初次响应 CMIT:0001303

吴先生，您好

问题定义:

工行吉林分行出现蓝屏。在开机过程中蓝屏，重启后进入系统修复过程但无法进入系统。用户使用半个月左右正常，后 TMS 进行客户端和策略升级后出现此现象。目前有几十台机器出现此问题。

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。

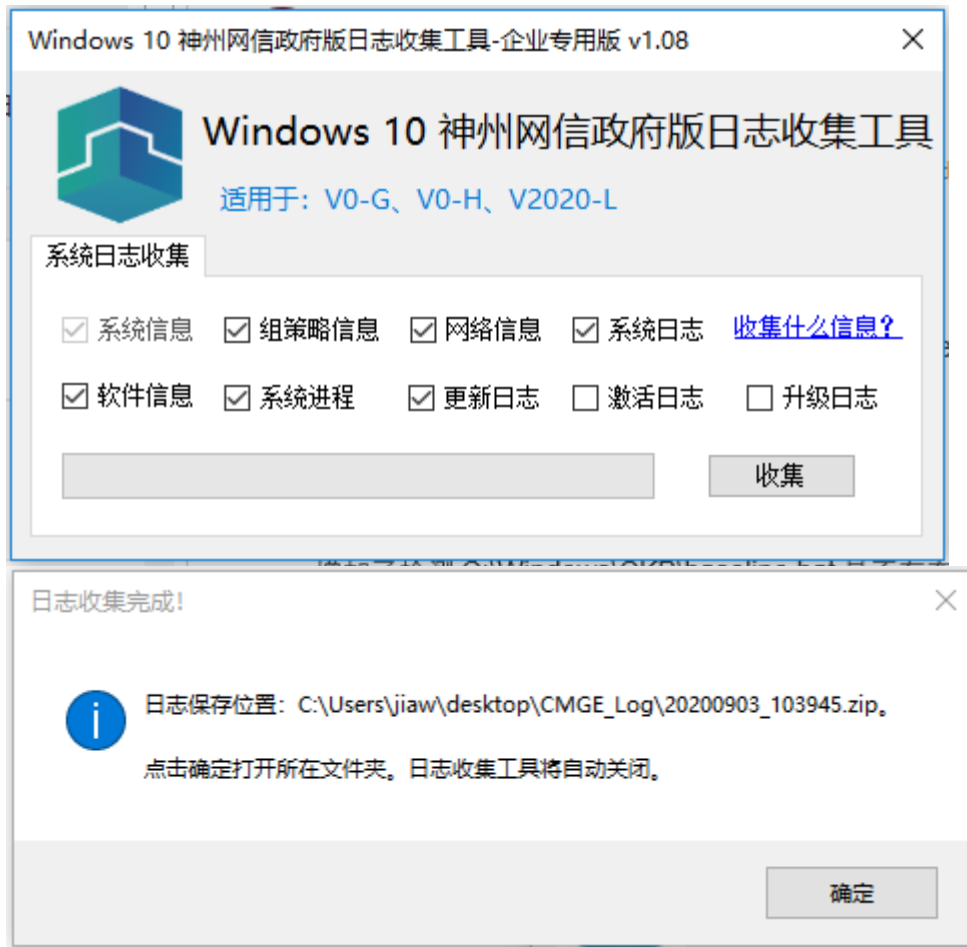
很高兴与您电话沟通，由于目前的 dump 文件不是 Full Dump，如果需要进一步分析日志请先按照如下方法，尝试设置并收集日志文件。我稍后再确认是否可以在无法进入桌面的情况下设置 Full Dump。

日志收集：

一、按照附件的《Full Dump 配置常规方案》设置 Full Dump，等待下一次关机/蓝屏后收集 C:\Windows\MEMORY.DMP，务必**压缩**后，上传。

二、工具收集

- 下载附件 zip 文件并解压到本地磁盘。之后双击运行 exe 文件，同意隐私声明后，按照下图勾选系统日志，组策略信息、网络信息、软件信息，系统进程、更新日志，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定为压缩文件。
- 将压缩文件上传。

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。

l Filezilla client 端下载 URL: <https://filezilla-project.org/download.php?type=client>

l 登陆地址: sftp://ocean.cmgos.com

l 用户名为: ICBC (区分大小写)

l 密码: 2qfs52ninbFB

l 端口：22222

登陆之后，上传至/upload/ 文件夹

=====

=====

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。

贾伟 Jia Wei

神州网信技术有限公司

服务支持电话： 400-818-0055

电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei <jiawei@cmgos.com>

发送时间: 2022 年 1 月 21 日 11:53

收件人: 吴毓杰 <win10sup@sdicbc.com.cn>

抄送: Jia Wei <jiawei@cmgos.com>

主题: [案例号: CAS-05611-L7D0Q4] % |P2|ICBC|工商银行吉林分行反馈蓝屏问题 % 初次响应 CMIT:0001303

吴毓杰 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 贾伟 。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-05611-L7D0Q4 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”。