您好!

重新抓取了几个日志，验证可以打开，请协助看下，感谢。

Centerm | 聚力金融，智领未来

潘家铭 | 福建升腾资讯有限公司

智能终端事业部 | 软件工程师

18059769998

panjiaming@centerm.com

福州市高新区新港大道 33 号星网锐捷科技园 A 楼 19F

发件人： panjiaming@centerm.com
发送时间： 2022-09-21 16:02
收件人： Jia Wei
抄送： PR_Case_Notification; Li Qi
主题： Re: 回复: [案例号: CAS-06797-L5Q7B6] % |普通事件|Centerm|系统组策略丢失导致 Admin 权限丢失问题 % 初次响应 CMIT:0001343

您好!

用故障镜像 软重启时，随机抓取了几次重启前的 进程监控日志，帮看看是否能找到操作组策略文件的进程，感谢。

Centerm | 聚力金融，智领未来

潘家铭 | 福建升腾资讯有限公司

智能终端事业部 | 软件工程师

18059769998

panjiaming@centerm.com

福州市高新区新港大道 33 号星网锐捷科技园 A 楼 19F

发件人： Jia Wei
发送时间： 2022-09-19 14:37
收件人： panjiaming@centerm.com
抄送： PR_Case_Notification; Li Qi
主题： 回复: 回复: [案例号: CAS-06797-L5Q7B6] % |普通事件|Centerm|系统组策略丢失导致 Admin 权限丢失问题 % 初次响应 CMIT:0001343

潘先生，您好

请查看是否可以从如下链接下载：

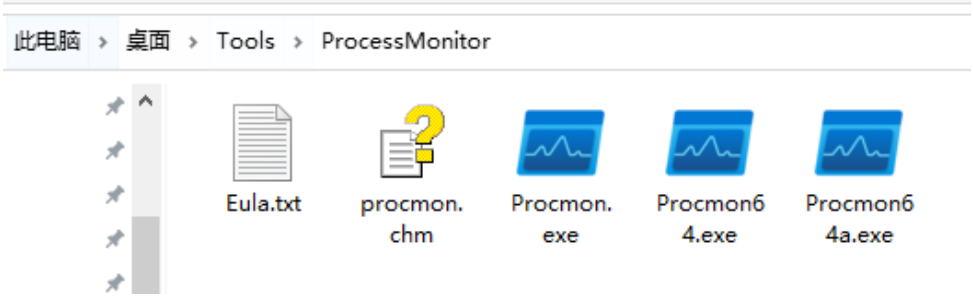
https://cduc.cmgos.com/download.php?id=655&token=RqIh67w3x7G6pmFjzreeJcoAQ73nHjfj

纯净版系统未能复现您的问题，而出现问题的计算机有很多三方软件，所以建议您可以按照如下操作抓取日志。

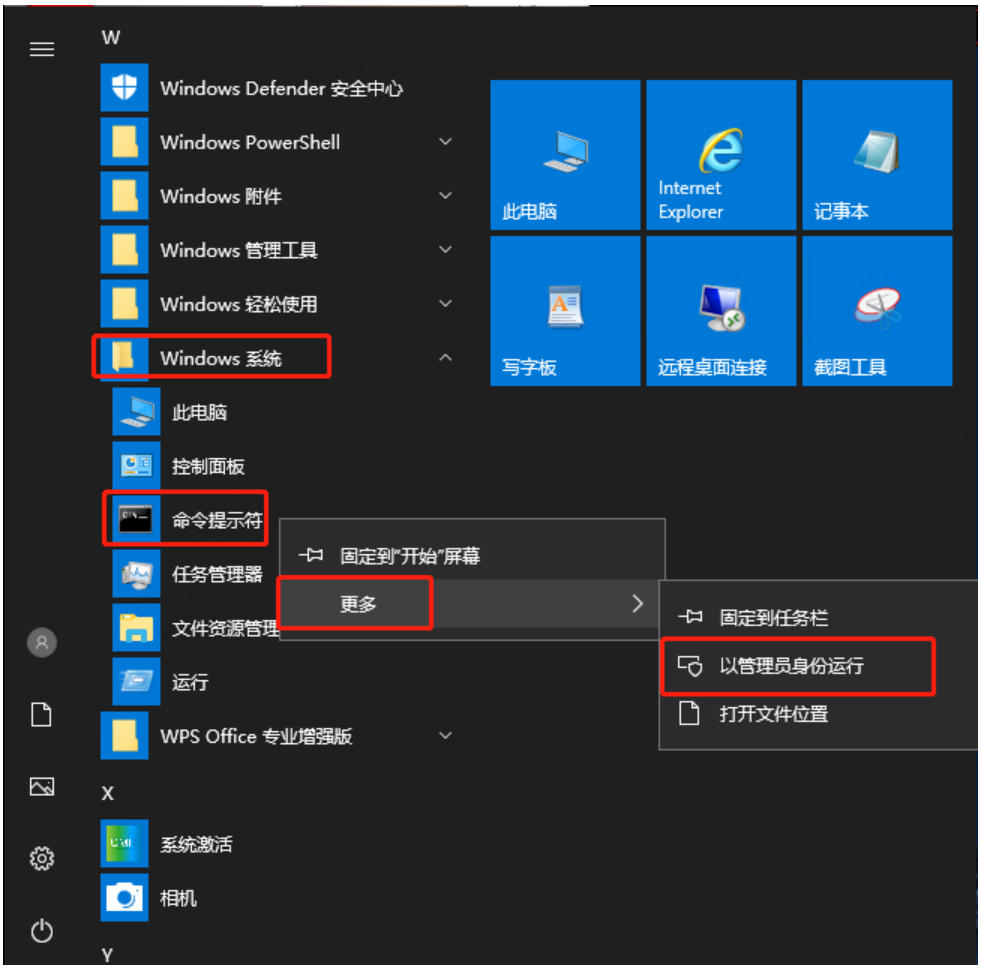
且此问题现象不固定复现，目前只能尝试抓取关机过程的日志信息，尽量帮您排查 registry.pol 文件损坏的原因。

抓取 ProcessMonitor 日志

1）下载附件 ProcessMonitor.zip，将内容解压至 C:\根目录，如下图所示：



2）按下图以管理员身份运行命令提示符 cmd。



3）逐一运行以下的命令开启 Process Monitor Log:

Cd C:\ProcessMonitor

procmon /backingfile C:\logfile.pml /NoFilter /AcceptEula /Minimized /Quiet

4）执行单次重启，例如运行：

shutdown -r -t 30

5）系统重启后进入系统，将 **C:\ logfile.pml** 文件压缩后反馈。

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: panjiaming@centerm.com <panjiaming@centerm.com>
发送时间: 2022 年 9 月 19 日 9:44
收件人: Jia Wei <jiawei@cmgos.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>; Li Qi <liqi@cmgos.com>
主题: Re: 回复: [案例号: CAS-06797-L5Q7B6] % |普通事件|Centerm|系统组策略丢失导致 Admin 权限丢失问题 % 初次响应 CMIT:0001343

您好!

这个有没有什么优化的方式方法，能够减少这种故障率的?

Centerm | 聚力金融，智领未来

潘家铭 | 福建升腾资讯有限公司
智能终端事业部 | 软件工程师
18059769998
panjiaming@centerm.com
福州市高新区新港大道 33 号星网锐捷科技园 A 楼 19F

发件人: Jia Wei
发送时间: 2022-09-16 14:38
收件人: panjiaming@centerm.com
抄送: PR_Case_Notification; Li Qi
主题: 回复: 回复: [案例号: CAS-06797-L5Q7B6] % |普通事件|Centerm|系统组策略丢失导致 Admin 权限丢失问题 % 初次响应 CMIT:0001343

潘先生，您好

很高兴与您电话沟通。根据目前的日志分析，怀疑此问题与**系统意外关闭有关。**

- 目前您上传的日志共涉及 3 台计算机，通过脚本重启计算机并在事件日志中计数。
- 根据脚本内容推断重启频率为 30 秒重启 1 次，根据 User32 筛选可以看到两次重启之间实际上大概间隔 1 分 15 秒 – 1 分 30 秒左右。

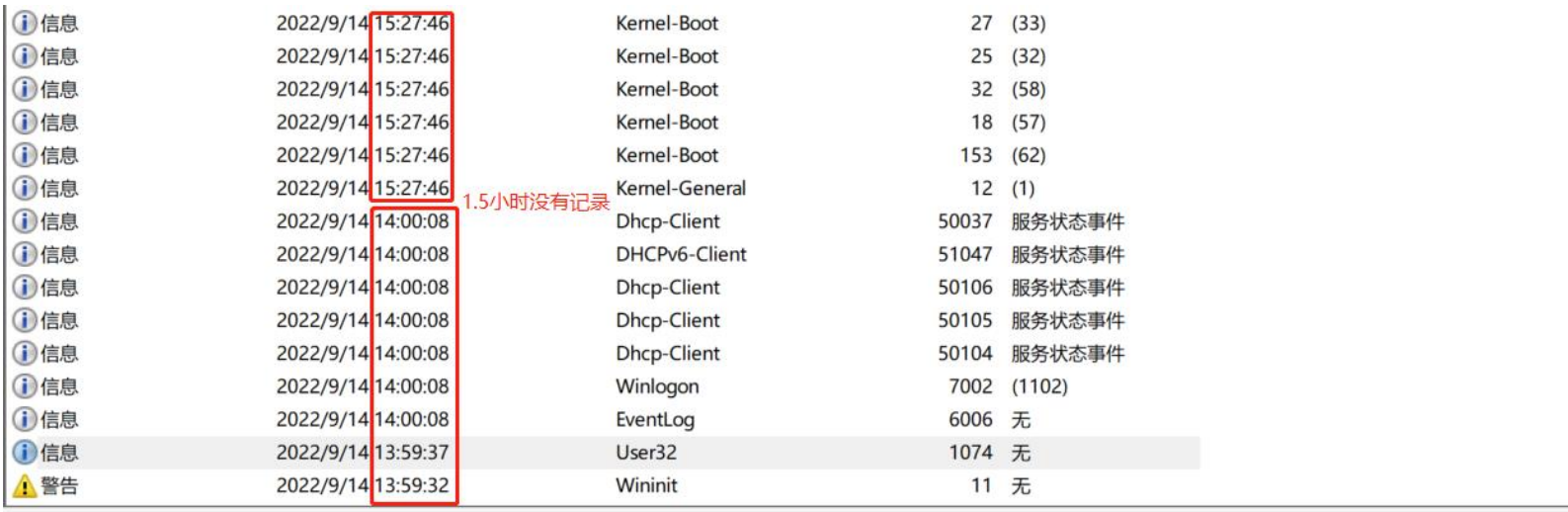
计算机 1：CMGE2022091501

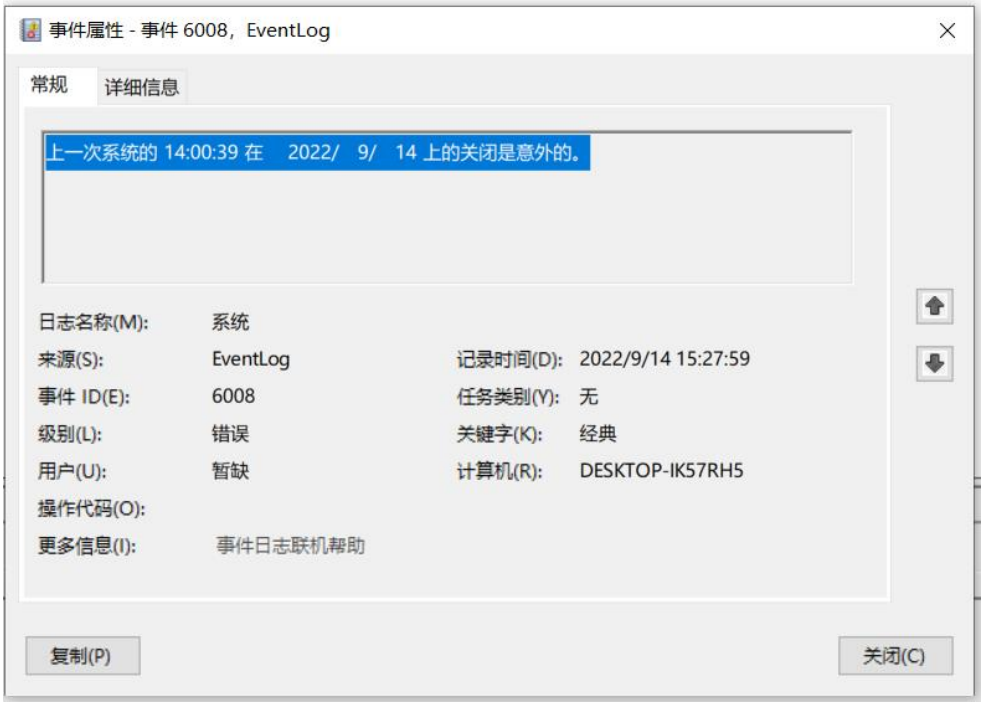
此机器的日志未能覆盖实际发生问题的时间点。

计算机 2：CMGE2022091502

通过事件日志，可发现

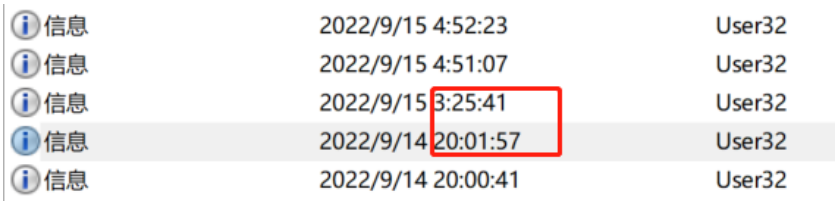
1. 此机器在通过脚本重启计数（Reboot Num）33 后就一直不变了。
2. 第 31 次重启后，至下一次计算机启动，期间有 1.5 小时左右没有任何记录
3. 且在 15:27 分左右报出错误 EventID 6008: **上一次系统的 14:00:39 在 2022/9/14 上的关闭是意外的**。



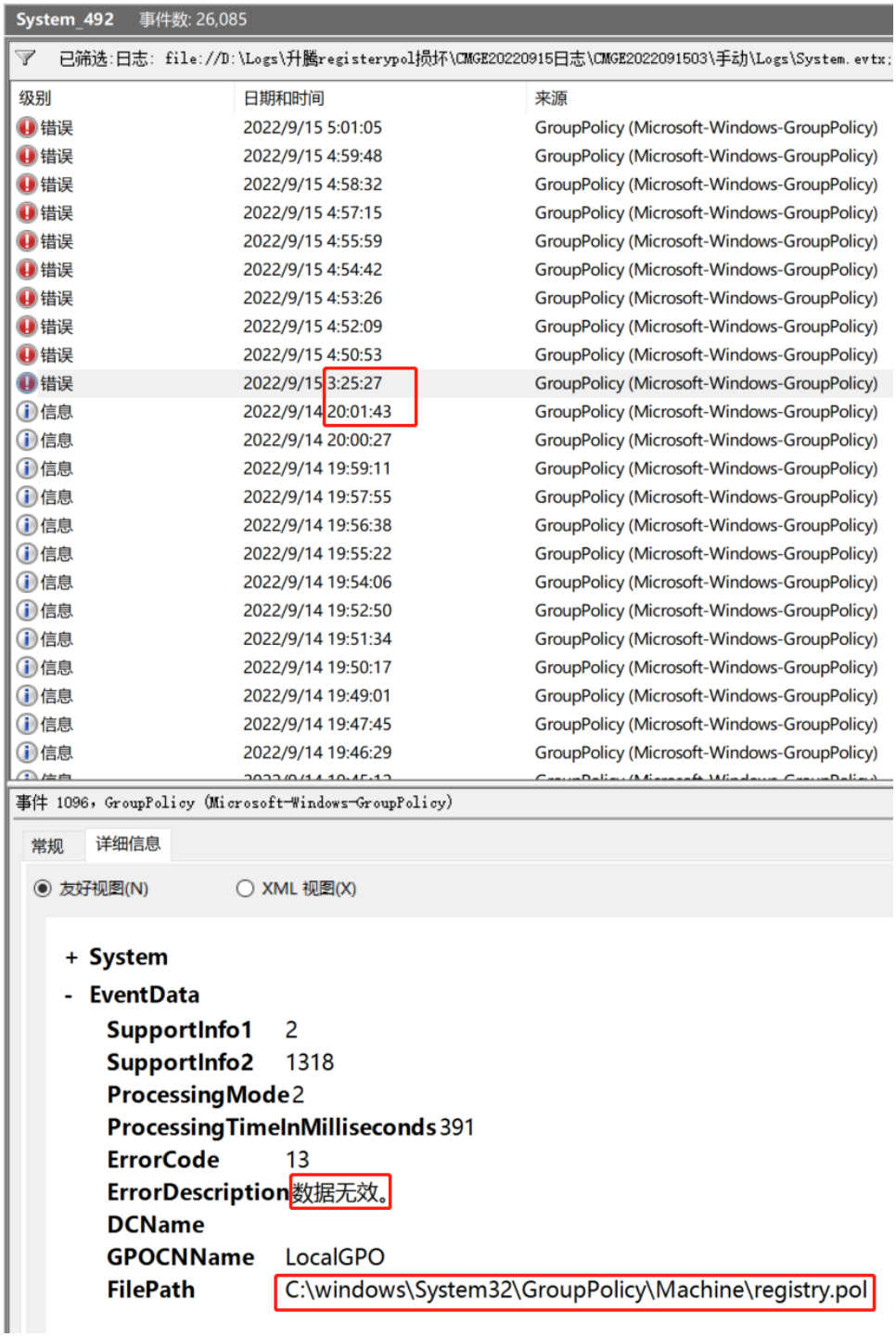


计算机 3：CMGE2022091503

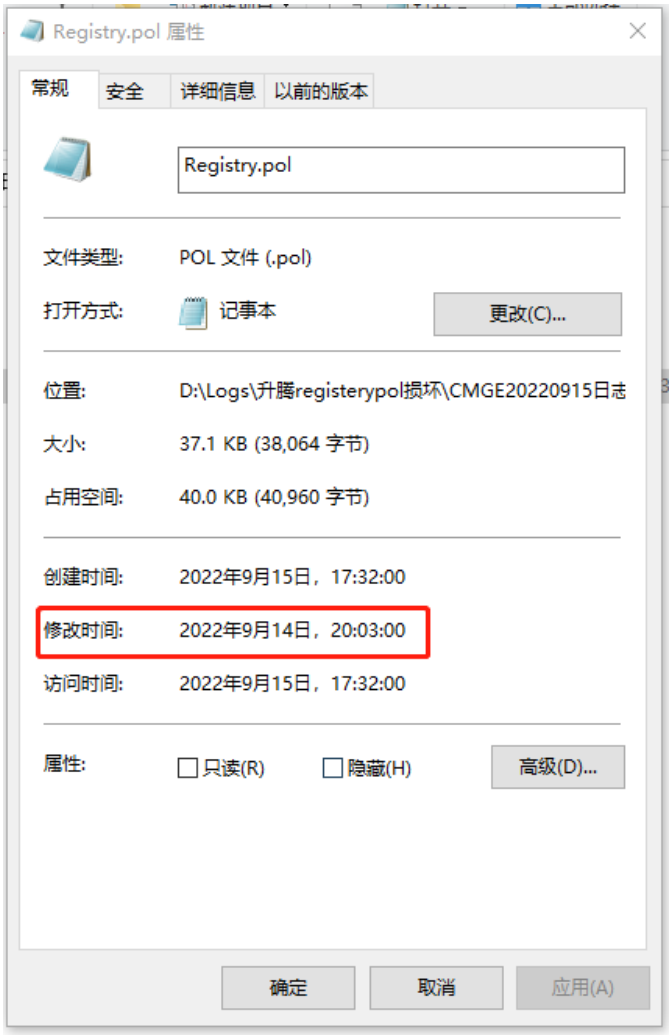
1. 此机器在通过脚本重启计数（Reboot Num）69 后就一直不变了。
2. 第 67 次重启后，至下一次计算机启动（68），期间有 7.5 小时左右没有任何记录



3. Registry.pol 在此时间点后损坏;



4. 最后一次重启的时间点为 9-14 20:02，与 Registry.pol 文件最后的修改时间相吻合。



5. 虽然没有 6008 的报错信息，但是怀疑此现象为系统意外关闭导致。

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: panjiaming@centerm.com <panjiaming@centerm.com>
发送时间: 2022 年 9 月 15 日 15:53
收件人: Jia Wei <jiawei@cmgos.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>; Li Qi <liqi@cmgos.com>

主题: Re: 回复: [案例号: CAS-06797-L5Q7B6] % |普通事件|Centerm|系统组策略丢失导致 Admin 权限丢失问题 % 初次响应 CMIT:0001343

您好!

故障现象是在产线做软重启测试时出现的，我们的测试方法大致就是 往开机启动项里，添加重启脚本（如附件）

这个脚本会往注册表里写重启次数，也能够读取，然后重启到 100 次后，会走下一个测试流程。

目前这些故障机都是出现在百次重启之内。

不好意思，刚刚正好不在位子上，有需要这下可以再打我电话。

Centerm | 聚力金融，智领未来

潘家铭 | 福建升腾资讯有限公司

智能终端软件部 | 软件工程师

18059769998

panjiaming@centerm.com

福州市金山大道 618 号橘园洲星网锐捷科技园 21 号楼 3 层

发件人: Jia Wei
发送时间: 2022-09-15 15:44
收件人: panjiaming@centerm.com
抄送: PR_Case_Notification; Li Qi
主题: 回复: Re: [案例号: CAS-06797-L5Q7B6] % |普通事件|Centerm|系统组策略丢失导致 Admin 权限丢失问题 % 初次响应 CMIT:0001343

潘先生，您好

刚刚电话未能联系到您，我公司的日志上传网址可能无法上传过大的文件。您在案例描述中提到的 ftp 服务器可以提供，我可以按照您提供的方式下载。

另外我看到日志中每隔 1 分钟左右系统会自动重启，这具体是通过什么方式实现的？如果是脚本文件可以反馈给我。

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: panjiaming@centerm.com <panjiaming@centerm.com>
发送时间: 2022 年 9 月 15 日 15:40
收件人: Jia Wei <jiawei@cmgos.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>; Li Qi <liqi@cmgos.com>
主题: Re: Re: [案例号: CAS-06797-L5Q7B6] % |普通事件|Centerm|系统组策略丢失导致 Admin 权限丢失问题 % 初次响应 CMIT:0001343

您好!

由于产线有交期要求，故障机只能保留到今天下班，你看看还有什么信息需要获取的。

我这边有提取了一个故障镜像，如果需要也可以一并发你，就是镜像比较大，要传一段时间。

Centerm | 聚力金融，智领未来

潘家铭 | 福建升腾资讯有限公司
智能终端软件部 | 软件工程师
18059769998
panjiaming@centerm.com
福州市金山大道 618 号橘园洲星网锐捷科技园 21 号楼 3 层

发件人： panjiaming@centerm.com
发送时间： 2022-09-15 11:11
收件人： Jia Wei
抄送： PR_Case_Notification; Li Qi
主题： Re: 回复: [案例号: CAS-06797-L5Q7B6] % |普通事件|Centerm|系统组策略丢失导致 Admin 权限丢失问题 % 初次响应 CMIT:0001343

您好!

日志已上传系统，请协助看下 确认下原因，最好能找到 3 台一些共性的特征，感谢~

Centerm | 聚力金融，智领未来

潘家铭 | 福建升腾资讯有限公司
智能终端软件部 | 软件工程师
18059769998
panjiaming@centerm.com
福州市金山大道 618 号橘园洲星网锐捷科技园 21 号楼 3 层

发件人： Jia Wei
发送时间： 2022-09-15 10:04
收件人： 潘家铭
抄送： PR_Case_Notification; Li Qi
主题： 回复: [案例号: CAS-06797-L5Q7B6] % |普通事件|Centerm|系统组策略丢失导致 Admin 权限丢失问题 % 初次响应 CMIT:0001343

潘先生，您好

很高兴与您电话沟通，您可以参考如下操作收集日志并反馈。

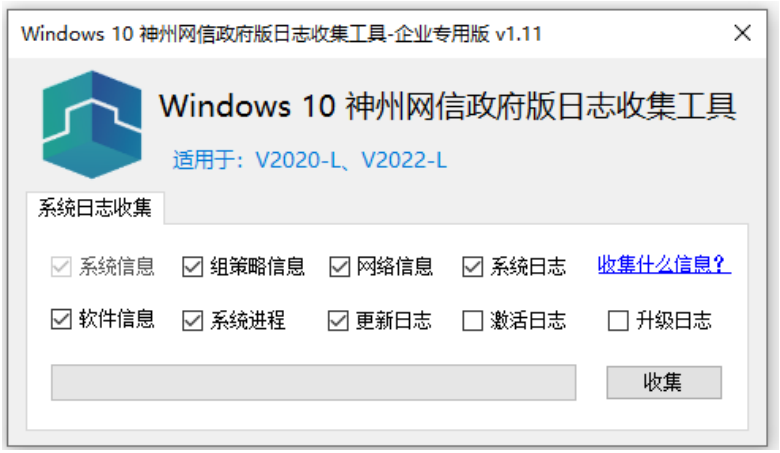
日志收集：

工具收集

l 在出现问题的计算机上，下载 zip 文件并解压到本地磁盘。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。

下载链接：

https://cduc.cmgos.com/download.php?id=644&token=TOGBo13NOJlb5eu6eioaKMT6khiA2tJA



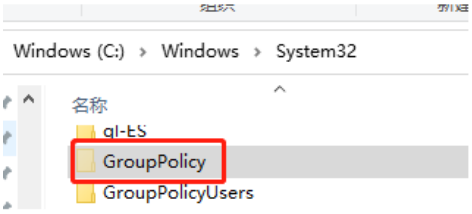
l 收集完毕后将在当前用户桌面生产 **CMGE_Log**。点击确定，将直接打开文件夹并定为压缩文件。

l 将压缩文件上传。

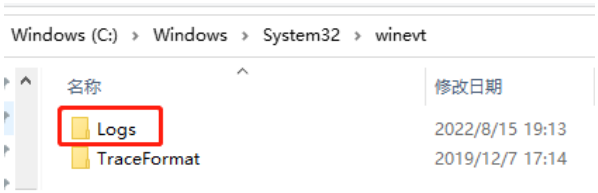
手动收集：

如果工具收集无法完成， 参考如下方法手动拷贝日志：

1）将 C:\Windows\System32\GroupPolicy 文件夹全部拷贝



2）将 C:\Windows\System32\winevt\Logs 文件夹全部拷贝



3）将上述文件夹压缩后上传。

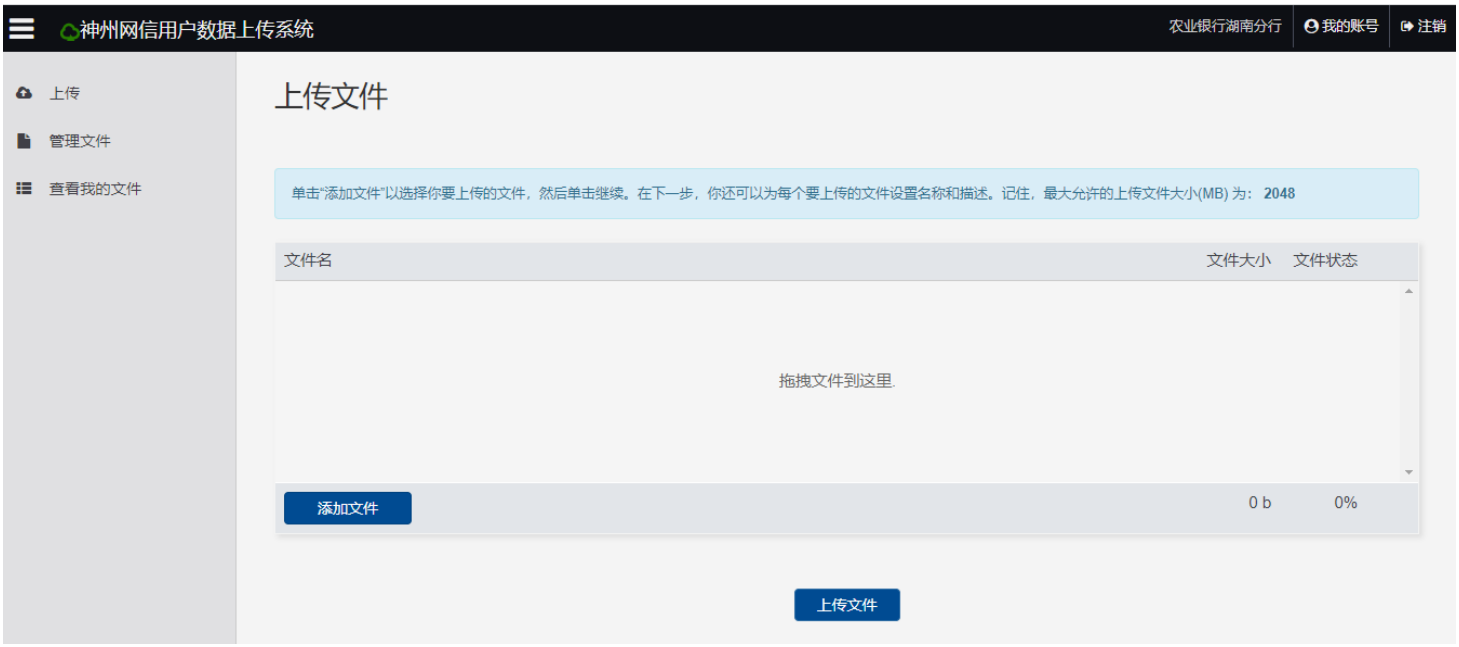
日志上传：

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

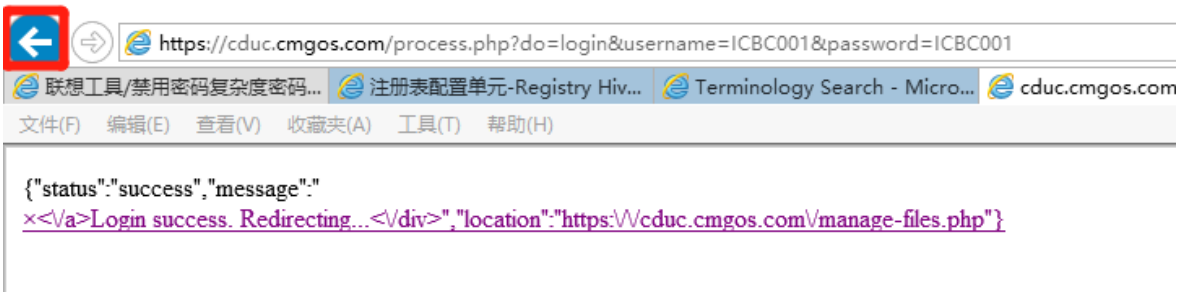
用户名：FJSTZXYXGS

密码：FJSTZXYXGS

添加文件后点击**上传文件** ,上传完毕后点击**保存**



注意，如果遇到如下所示页面，点击后退即可看到页面



==========

==========

在向 CMIT 提供日志和数据前，请阅读并接受邮件下方隐私声明。

隐私声明

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

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

神州网信保证不对外公开或向第三方提供、公开或共享您提供的数据和信息。在以下情况下，神州网信对您的数据和信息的披露将不视为违约，具体包括:

(1) 神州网信已获得您的明确授权;

(2) 根据适用法律的要求，神州网信负有披露义务的;

(3) 司法机关或行政机关基于法定程序要求神州网信提供的;

(4) 为维护社会公共利益及神州网信合法权益，在合理范围内进行披露的。

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

如果您欲提供的数据和信息中包含对您重要的保密信息以及商业秘密，在您向神州网信提供上述数据和信息前, 务必对上述数据和信息进行脱敏处理，否则请不要提供该信息给神州网信。作为一家商业软件公司，神州网信在商业可行的前提下，已为用户的数据和信息保护做了极大的努力，但是仍然不能保证现有的安全技术措施使您的数据和信息等不受任何形式的损失。您对上述情况充分知情，且不会因此追究神州网信的法律责任。

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: Li Qi <liqi@cmgos.com>
发送时间: 2022 年 8 月 9 日 10:27
收件人: 潘家铭 <panjiaming@centerm.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-06797-L5Q7B6] % |普通事件|Centerm|系统组策略丢失导致 Admin 权限丢失问题 % 初次响应 CMIT:0001343

潘先生，您好:

如刚才电话沟通，鉴于当前产线并无生产任务，无法复现该问题，经您的同意，此 case 暂做归档处理，以下为案例总结，请您知悉:

Case No：CAS-06797-L5Q7B6

问题描述：

==========

用户反馈产线部署的多台机器出现组策略文件 registry.pol 损坏的问题，需要排查问题原因及后续规避手段。

问题分析：

==========

组策略文件 registry.pol 在每次组策略更新时都会进行写入，而文件损坏一般都是因为在修改的过程中被终止导致动作未全部完成，因此造成文件失效，进而导致组策略应用失败。

解决方案:

1. 如之前案例所述，通过 LGPO 导入全新的或正常的 registry.pol 文件，重启生效
2. 重命名或移动损坏的组策略文件 registry.pol，重启后系统会自动生成新的文件

排查手段:

1. 确认产线自动化部署中，涉及组策略更新的内容有哪些？如有第三方应用的安装，在测试排查过程中，可考虑暂不安装，以排除影响。

2. 确认已损坏的 registry.pol 文件的最后修改时间，以确定问题发生的具体时间点，再根据该时间点从系统日志中筛选是否有可疑日志记录内容

问题总结：

==========

经用户确认，此 case 暂做归档处理，后续如遇相同问题，可致电 400-818-0055，或回复此邮件以重启案例。

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

发件人: Li Qi
发送时间: 2022 年 8 月 4 日 16:33
收件人: 潘家铭 <panjiaming@centerm.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-06797-L5Q7B6] % |普通事件|Centerm|系统组策略丢失导致 Admin 权限丢失问题 % 初次响应 CMIT:0001343

潘先生，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:

用户反馈产线部署的多台机器出现组策略文件 registry.pol 损坏的问题，需要排查问题原因及后续规避手段。

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：

从刚才的沟通中，我这边了解到的案例背景如下，如有问题，请您指正，谢谢：

1. 产线机器的问题复现步骤：大概重启 20-30 次左右就可能触发此问题
2. 问题机型均为同一硬件配置
3. 目前发现过此问题的机器已修复并交付，后续如再有此问题出现可配合进行测试

鉴于以上几点，请您当此问题发生时进行如下操作：

修复文件系统：

1.保存所有未保存的数据并关闭所有打开的程序单击开始，以管理员模式运行 CMD

Chkdsk X: /f

2.如果系统日志中 NTFS 55 消息定期出现，例如每天或每周，请使用/R 命令行选项运行 Chkdsk。**此选项允许 Chkdsk 定位硬盘上的坏扇区。请在此操作前备份磁盘，此修复不可逆，防止因修复命令导致数据丢失。**

Chkdsk X: /f /R

3.请确认现在磁盘状态，如果需要修复磁盘状态，都需要将**磁盘进行备份**，且修复磁盘状态并不是数据恢复。

系统日志：

下载附件中的 CMGELogCollector.zip，解压后运行 CMGELogCollector.exe，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。

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

神州网信
CMIT

发件人: Li Qi <liqi@cmgos.com>
发送时间: 2022 年 8 月 4 日 15:34
收件人: 潘家铭 <panjiaming@centerm.com>
抄送: Li Qi <liqi@cmgos.com>
主题: [案例号: CAS-06797-L5Q7B6] % |普通事件|Centerm|系统组策略丢失导致 Admin 权限丢失问题 % 初次响应 CMIT:0001343

潘家铭 先生/女士，您好!

感谢您联系神州网信技术支持中心。 我是技术支持工程师 李琦 。很高兴能有机会协助您解决该问题。 您可随时通过邮件回复以及该问题事件号码 CAS-06797-L5Q7B6 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
