张先生 您好:

感谢您的电话接听。

麻烦您测试开启 UWF 功能且**不进行文件排除配置**时，是否也会出现 DLP 安全策略缓慢情况。

测试后请您**以管理员权限**打开 cmd 命令行，执行以下命令收集日志。

msinfo32 /nfo C:\SYSSUM.NFO /categories +systemsummary

将生成的日志 **C:\SYSSUM.NFO** 和系统日志文件夹 **C:\Windows\System32\winevt\Logs** 压缩后通过 CDUC 系统上传。

日志上传方法：

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：nonghangabc

密码：nonghangabc

注意：添加文件，点击上传后，跳转到新的页面点击保存。

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: 2023 年 3 月 1 日 11:18
收件人: '张辉银' <zhanghuiyinjgcq@abchina.com>
抄送: '赵晶晶' <zhaojingjing@abchina.com>; PR_Case_Notification <PR_Case_Notification@cmgos.com>; Liu Wei <liuwei@cmgos.com>
主题: 回复: [案例号：CAS-07964-V4N3T4] % 农业银行用户反馈 CMGE 系统下开启 UWF 保护机制导致安全策略执行变慢问题 % 初次响应 CMIT:0001963

张先生 您好:

感谢您的回复，日志已经收到，有任何进展会及时与您联系沟通。

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: Wei Liang
发送时间: 2023 年 2 月 27 日 15:16
收件人: '张辉银' <zhanghuiyinjgcq@abchina.com>
抄送: '赵晶晶' <zhaojingjing@abchina.com>; PR_Case_Notification <PR_Case_Notification@cmgos.com>; Liu Wei <liuwei@cmgos.com>
主题: 回复: [案例号：CAS-07964-V4N3T4] % 农业银行用户反馈 CMGE 系统下开启 UWF 保护机制导致安全策略执行变慢问题 % 初次响应 CMIT:0001963

张先生 您好:

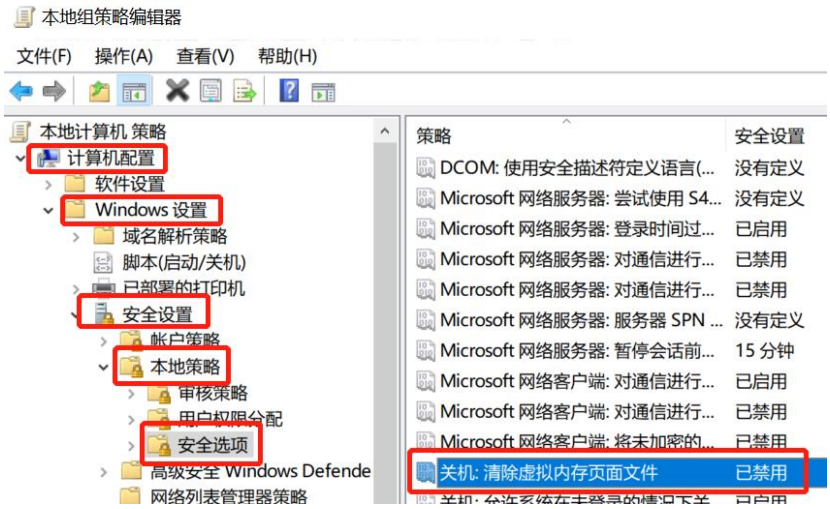
针对您的环境中配置 boot logging 无法抓取对应日志的情况，重新修改了新的日志收集方法，具体操作如下:

1）以**管理员权限打开 cmd 命令行**，运行以下命令禁用 UWF，并重启系统生效。

uwfmgr filter disable

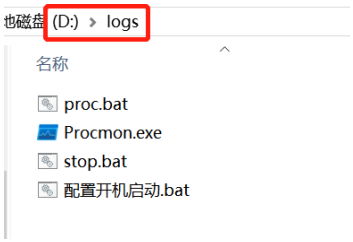
2）重启系统关闭 UWF 后，运行 gpedit.msc 打开本地组策略编辑器，定位到:

“计算机配置”-“Windows 设置”-“安全设置”-“本地策略”-“安全选项”中的策略**“关机:清除虚拟内存页面文件”**设置为**“已禁用”**



3）从以下链接下载 **proc.zip** 文件，将其解压，保存到 **D:\logs**目录，其中包含以下几个文件。

https://cduc.cmgos.com/download.php?id=823&token=gRWlHRZMNjHWUVbaAGLd2NjL4L3GYwmX



4）运行**配置开机启动.bat**，将 proc.bat 脚本配置为**“用户登录后自动运行”**，脚本会自动退出。

5）**以管理员权限**打开 cmd 命令行，运行以下命令**启用 uwf**，并重启系统生效。

uwfmgr filter enable

6）重启计算机并登录，出现 cmd 命令行运行可能会弹出**“用户帐户控制”**提示，选择**“是”**同意运行。

7）确认 **DLP 安全策略经过较长时间生效**后，运行 **D:\logs\stop.bat** 脚本停止日志抓取，将 **D:\logs**目录下 **uwf 开头的文件以及文件夹**压缩后通过 CDUC 上传。

8）**再次禁用 UWF 功能**后，重启计算机再次运行 proc.bat，策略生效后，运行 D:\logs\stop.bat 脚本停止日志抓取，此时**获取 DLP 安全策略快速生效的 proc 和 wpr 日志**（D:\logs\目录下新的 uwf 开头的文件以及文件夹）压缩后上传。

注意：每次重启都会生成新的 uwf 文件，将旧的 uwf 文件覆盖。**在运行 stop.bat 停止后，及时复制对应的 uwf 文件和文件夹并压缩。**

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: 2023 年 2 月 23 日 17:19
收件人: '赵晶晶' <zhaojingjing@abchina.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>; Liu Wei <liuwei@cmgos.com>
主题: 回复: [案例号：CAS-07964-V4N3T4]％ 农业银行用户反馈 CMGE 系统下开启 UWF 保护机制导致安全策略执行变慢问题 ％初次响应 CMIT:0001963

赵女士 您好:

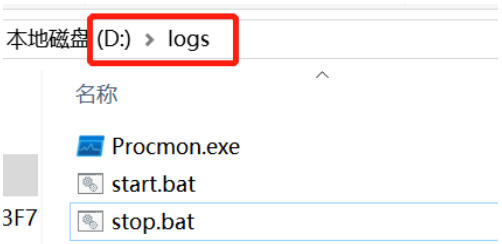
与您的同事张先生沟通确认，按照以下操作再次抓取新的 procmon 日志和 wpr etl 日志，具体操作如下：

1）以**管理员权限打开 cmd 命令行**，运行以下命令禁用 UWF，并**重启系统生效。**

uwfmgr filter disable

2）**重启系统关闭 UWF** 后，从以下链接下载 **wpr 日志.zip** 文件，将其解压，保存到 **D:\logs** 目录（相关文件已经更新，**请清空原先的 D:\logs\目录**），其中包含以下几个文件。

https://cduc.cmgos.com/download.php?id=817&token=52WfMHzqXOXTtNZqSYyIBKHA6faj17mW



3）**右键以管理员权限**运行 **start.bat**，将配置开机自动抓取 procmon 日志和 wpr etl 日志。

4）**以管理员权限**打开 cmd 命令行，运行以下命令**启用 uwf**，并**重启系统生效。**

uwfmgr filter enable

5）重启计算机并登录，确认 **DLP 安全策略经过较长时间生效**后，**右键以管理员权限**运行 **D:\logs\stop.bat** 脚本停止日志收集，将 **D:\logs**目录下 uwf.pml 和 uwf.etl 的文件和 uwf.etl.文件夹压缩后通过 CDUC 上传。

6）**再次禁用 UWF 功能**后，重启计算机确认策略生效后，右键以管理员权限运行 D:\logs\stop.bat 脚本停止日志收集，此时**获取 DLP 安全策略快速生效的日志**（D:\logs\目录下新的 uwf.pml 和 uwf.etl 的文件和 uwf.etl.文件夹）压缩后上传。

注意：生成的日志文件比较大，每次重启都会生成新的 uwf 文件，将旧的 uwf 文件覆盖。**在运行 stop.bat 停止日志收集后，及时复制对应的 uwf 文件并压缩。**

日志上传方法：

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：nonghangabc

密码：nonghangabc

注意：添加文件，点击上传后，跳转到新的页面点击保存。

修改 uwfs.sys 驱动在 fltmc 中的高度方法：

1）以**管理员权限打开 cmd 命令行**，运行以下命令禁用 UWF，并**重启系统生效。**

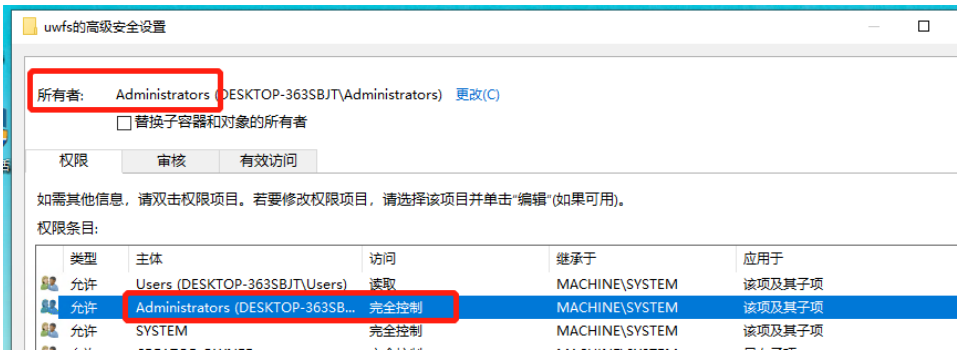
uwfmgr filter disable

2）运行 regedit 打开注册表编辑器，定位到：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\uwfs\Instances\uwfs

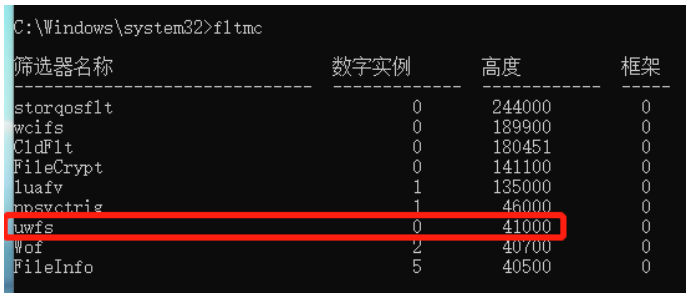
3）在注册表编辑器界面，修改右侧的 **Altitude 键值**设置为 41000 并保存（也可以根据 fltmc 查询显示的高度设置合适的数值）。

如果修改 Altitude 键值提示没有权限，右键点击 **uwfs** 选择**权限**，选择**高级**，更改所有者为 **administrators**，并设置为**完全控制权限**，并保存，然后再修改 Altitude 键值。



4）再次右键点击 **uwfs** 选择**权限**，选择**高级**，添加一个**主体 everyone**，类型为**拒绝**，点击**显示高级权限**，只勾选**设置权限**和**删除**，并保存确认。

5）开启 UWF 功能，重启计算机生效，以管理员权限打开 cmd 命令行，执行 **fltmc** 验证 uwfs 的高度情况。



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: 2023 年 2 月 13 日 15:11
收件人: '赵晶晶' <zhaojingjing@abchina.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>; Liu Wei <liuwei@cmgos.com>
主题: 回复: [案例号：CAS-07964-V4N3T4] % 农业银行用户反馈 CMGE 系统下开启 UWF 保护机制导致安全策略执行变慢问题 % 初次响应 CMIT:0001963

赵女士 您好:

与您的同事张先生沟通确认无法提供对应的软件给神州网信进行测试复现问题，而且也无法将您那边的测试机系统转换成虚拟机提供给神州网信。

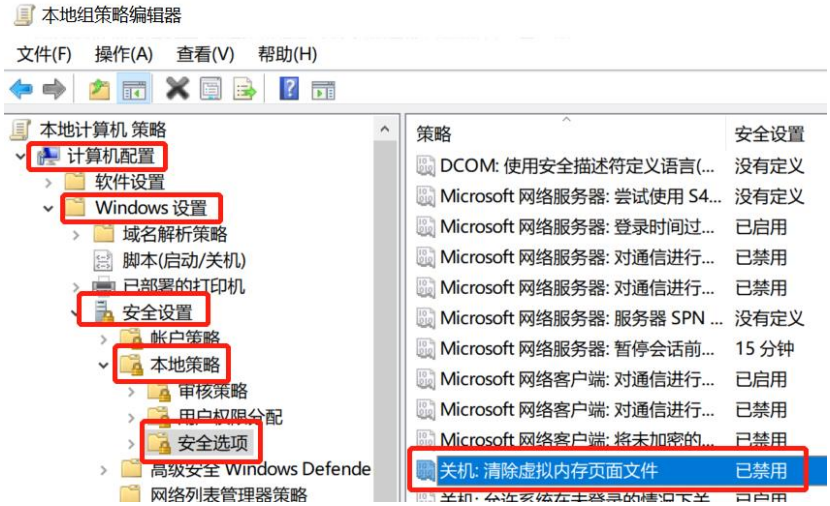
经过测试，请最终用户按照以下操作抓取登录系统后的 procmon 日志用于分析问题，具体操作如下:

1）以**管理员权限打开 cmd 命令行**，运行以下命令禁用 UWF，并重启系统生效。

uwfmgr filter disable

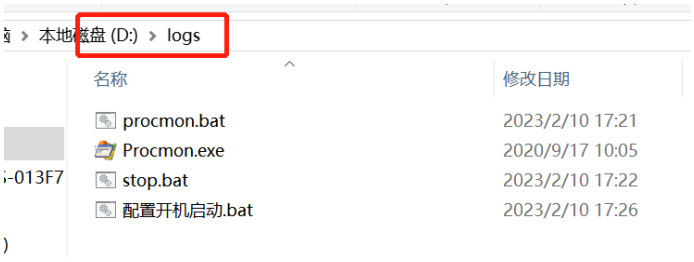
2）重启系统关闭 UWF 后，运行 gpedit.msc 打开本地组策略编辑器，定位到:

“计算机配置”-“Windows 设置”-“安全设置”-“本地策略”-“安全选项”中的策略**“关机:清除虚拟内存页面文件”**设置为**“已禁用”**



3）从以下链接下载 **procmon 日志.zip** 文件，将其解压，保存到 **D:\logs**目录，其中包含以下几个文件。

https://cduc.cmgos.com/download.php?id=796&token=TCxhNVeripbljbrIpHiHKlWFoAX0aEen



4）**右键以管理员权限**运行**配置开机启动.bat**，将 procmon.bat 脚本配置为**“用户登录后自动运行”**，脚本会自动退出。

5）**以管理员权限**打开 cmd 命令行，运行以下命令**启用 uwf**，并重启系统生效。

```
uwfmgr filter enable
```

6）重启计算机并登录，出现 cmd 命令行运行 procmon.exe 可能会弹出**“用户帐户控制”**提示，选择**“是”**同意运行。

7）确认 **DLP 安全策略经过较长时间生效**后，**右键以管理员权限**运行 **D:\logs\stop.bat** 脚本停止 procmon，将 **D:\logs**目录下 uwf 开头的文件压缩后通过 CDUC 上传。

8）**再次禁用 UWF 功能**后，重启计算机再次运行 procmon.exe，策略生效后，右键以管理员权限运行 D:\logs\stop.bat 脚本停止 procmon，此时**获取 DLP 安全策略快速生效的 procmon 日志**（D:\logs\目录下新的 uwf 开头的文件）压缩后上传。

注意：每次重启都会生成新的 uwf 文件，将旧的 uwf 文件覆盖。**在运行 stop.bat 停止 procmon 后，及时复制对应的 uwf 文件并压缩。**

日志上传方法：

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：nonghangabc

密码：nonghangabc

注意：添加文件，点击上传后，跳转到新的页面点击保存。

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: 2023 年 2 月 3 日 14:51
收件人: '赵晶晶' <zhaojingjing@abchina.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>; Liu Wei <liuwei@cmgos.com>
主题: 回复: [案例号：CAS-07964-V4N3T4] % 农业银行用户反馈 CMGE 系统下开启 UWF 保护机制导致安全策略执行变慢问题 % 初次响应 CMIT:0001963

赵女士 您好:

昨天与您的同事张先生沟通了关于启用 UWF 功能后安全策略执行变慢问题的测试情况如下:

只安装一款安全软件并启用 UWF 功能后，都会出现安全策略生效变慢的问题，当再安装一款安全软件时，会导致安全策略生效所需时间更长。

今天联系了 DLP 厂商了解是否能提供试用版 DLP 软件进行测试，尝试复现问题，DLP 厂商表示没有供单机测试使用的 DLP 应用版本。

针对此问题只能再查找其他方法尝试在测试环境中复现问题进行排查，我这边有任何进展会及时与您联系沟通。

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: Wei Liang
发送时间: 2023 年 1 月 31 日 16:57
收件人: '赵晶晶' <zhaojingjing@abchina.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>; Liu Wei <liuwei@cmgos.com>
主题: 回复: [案例号：CAS-07964-V4N3T4] % 农业银行用户反馈 CMGE 系统下开启 UWF 保护机制导致安全策略执行变慢问题 % 初次响应 CMIT:0001963

赵女士 您好:

感谢您的电话接听。

我刚刚与您的同事张先生电话沟通了具体的测试情况，他会再次测试 DLP、天擎以及趋势安全软件的安装与否，对开启 UWF 功能后 DLP 安全策略的影响。关于此问题，如果有任何进展会及时与您联系。

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: 2023 年 1 月 29 日 15:33
收件人: '赵晶晶' <zhaojingjing@abchina.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>; Liu Wei <liuwei@cmgos.com>
主题: 回复: [案例号：CAS-07964-V4N3T4]％ 农业银行用户反馈 CMGE 系统下开启 UWF 保护机制导致安全策略执行变慢问题 ％初次响应 CMIT:0001963

赵女士 您好:

感谢您的电话接听。

请您与用户确认按照 **2023 年 1 月 18 日的邮件说明**排查应用情况，并将测试结果和收集的信息提供给我们。

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: 2023 年 1 月 20 日 11:32
收件人: '赵晶晶' <zhaojingjing@abchina.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>; Liu Wei

<liuwei@cmgos.com>
主题: 回复: [案例号: CAS-07964-V4N3T4] % 农业银行用户反馈 CMGE 系统下开启 UWF 保护机制导致安全策略执行变慢问题 % 初次响应 CMIT:0001963

赵女士 您好:

感谢您的电话接听。

您可以让最终用户按照上一封的邮件说明进行相关测试，并将测试结果和收集的信息提供给我们。

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: 2023 年 1 月 18 日 17:41
收件人: '赵晶晶' <zhaojingjing@abchina.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>; Liu Wei <liuwei@cmgos.com>
主题: 回复: [案例号: CAS-07964-V4N3T4] % 农业银行用户反馈 CMGE 系统下开启 UWF 保护机制导致安全策略执行变慢问题 % 初次响应 CMIT:0001963

赵女士 您好:

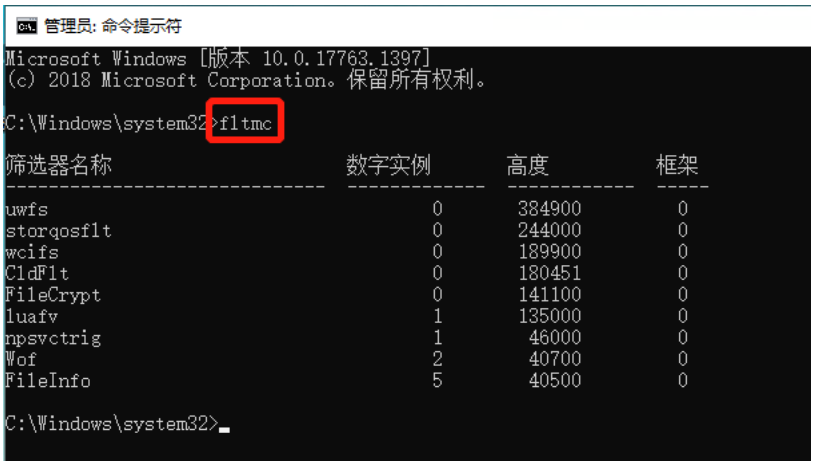
感谢您的电话接听。

根据您的反馈，调整 UWF 的覆盖设置类型后，DLP 的安全策略执行情况并没有改善。

为排除其他安全软件的影响，请您**先只安装 DLP 应用，开启 UWF，确认 DLP 安全策略执行情况，**再逐步安装天擎、趋势等安全软件，排查此问题可能与哪些安全软件有关。

有相关测试结果后，请您在复现了 DLP 的安全策略执行缓慢问题的设备上，以**管理员权限**打开 cmd 命令行，执行 **fltmc** 命令，将输出的信息提供给我们。

fltmc



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: 2023 年 1 月 16 日 16:31
收件人: '赵晶晶' <zhaojingjing@abchina.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>; Liu Wei <liuwei@cmgos.com>
主题: 回复: [案例号：CAS-07964-V4N3T4] % 农业银行用户反馈 CMGE 系统下开启 UWF 保护机制导致安全策略执行变慢问题 % 初次响应 CMIT:0001963

赵女士 您好:

感谢您的电话接听。

查看您这边设备的 UWF 覆盖设置类型为 Disk:

在测试过程中发现 UWF 覆盖设置类型为 Disk 对磁盘性能有较大影响。为**排除磁盘性能影响**，请按照以下操作配置 UWF 覆盖设置类型为 RAM，再次验证安全策略生效情况。

1）禁用 UWF 并重启计算机：

uwfmgr filter disable

2）重启计算机后，设置覆盖大小为**当前设备内存大小的一半** 4096MB，**覆盖类型为 RAM**，启用 UWF，并**重启计算机使 UWF 配置生效**。

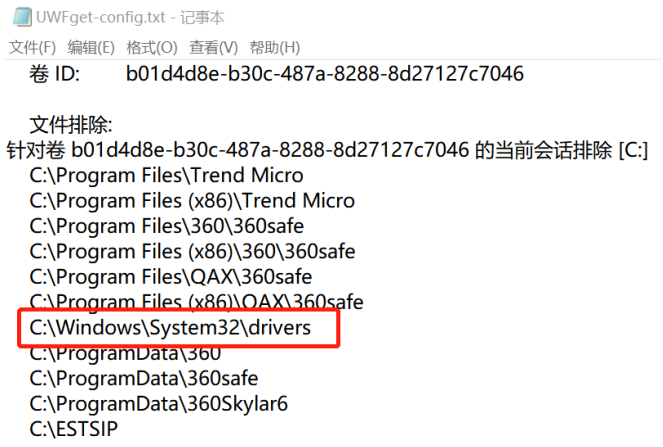
uwfmgr overlay set-size 4096

uwfmgr overlay set-type ram

uwfmgr filter enable

3）重启计算机后，验证安全策略情况。

您这边设备的 UWF 配置，建议**“文件排除”**策略**不要**包含**“C:\Windows\System32\drivers”**目录。



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: 2023 年 1 月 12 日 17:13
收件人: '赵晶晶' <zhaojingjing@abchina.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>; Liu Wei <liuwei@cmgos.com>
主题: 回复: [案例号: CAS-07964-V4N3T4] % 农业银行用户反馈 CMGE 系统下开启 UWF 保护机制导致安全策略执行变慢问题 % 初次响应 CMIT:0001963

赵女士 您好:

感谢您的电话接听。

日志已经收到，我会根据您这边的 UWF 配置情况做一些测试验证，有任何进展会及时与您联系沟通。

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: Wei Liang
发送时间: 2023 年 1 月 9 日 16:36
收件人: 赵晶晶 <zhaojingjing@abchina.com>
抄送: PR_Case_Notification <PR_Case_Notification@cmgos.com>
主题: 回复: [案例号: CAS-07964-V4N3T4] % 农业银行用户反馈 CMGE 系统下开启 UWF 保护机制导致安全策略执行变慢问题 % 初次响应 CMIT:0001963

赵女士 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:

用户反馈 CMGE 系统下开启 UWF 保护机制，发现安全软件 DLP 的安全策略生效延迟，存在数据泄露风险，需要协助分析。

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。

请帮忙提供以下信息:

1）请您提供开启了 UWF 功能的设备具体型号。

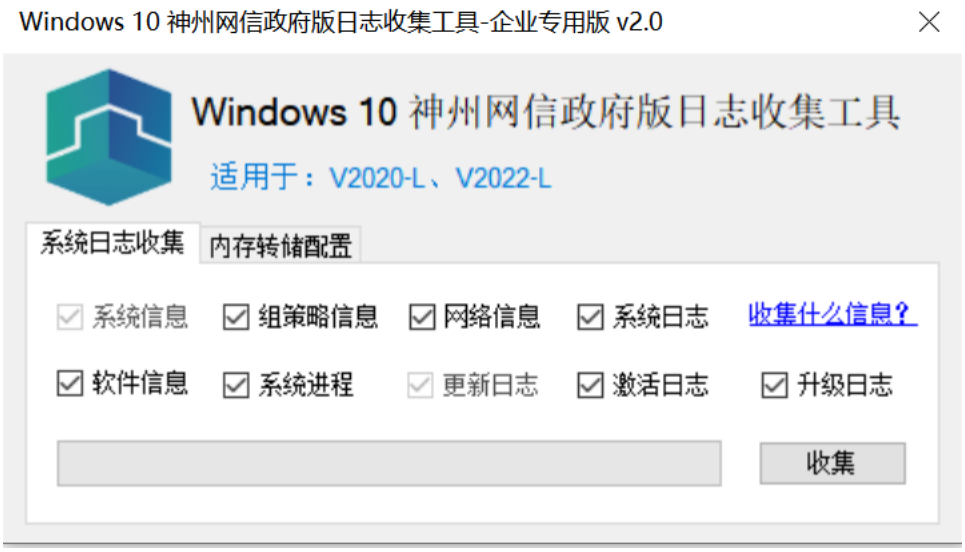
2）请您在开启了 UWF 功能的设备上以**管理员权限**打开 cmd 命令行，执行以下命令，查看 UWF 配置，将**显示的 UWF 配置内容复制保存到 txt 文档**，并通过 CDUC 上传。

uwfmgr get-config

3）通过以下链接下载日志收集工具 CMGELogCollectorV2.zip：

https://cduc.cmgos.com/download.php?id=771&token=QCEr0xQUk3ssFfnu5yuUtKrxpjOaSjSR

4）解压后运行 CMGELogCollectorV2.exe，勾选**所有选项**，点击**收集**获取对应的系统日志，将**生成的日志压缩包**通过 CDUC 上传。



日志上传方法：

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：nonghangabc

密码：nonghangabc

注意：添加文件，点击上传后，跳转到新的页面点击保存。

==========

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 <weiliang@cmgos.com>
发送时间: 2023 年 1 月 9 日 11:21
收件人: 赵晶晶 <zhaojingjing@abchina.com>
抄送: Wei Liang <weiliang@cmgos.com>
主题: [案例号：CAS-07964-V4N3T4]% 农业银行用户反馈 CMGE 系统下开启 UWF 保护机制导致安全策略执行变慢问题 % 初次响应 CMIT:0001963

赵晶晶 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-07964-V4N3T4 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
