

许先生 您好：

经过您的确认，问题已经解决，我将归档此案例。

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：

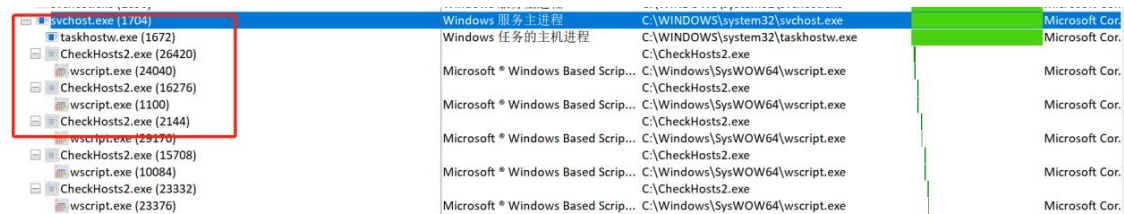
宁波分行用户反馈有设备的鼠标指针右边一直有圆圈图标显示，需要协助排查是什么原因。

问题总结：

经过排查，确认是针对 hosts 文件的审核策略变化导致的问题，重新调整相关策略后解决问题，可以归档案例。

问题排查：

在 procmon 日志中发现 checkhosts2.exe 进程反复启动停止。



The image shows a Windows Task Manager window with the 'Processes' tab selected. A red box highlights several instances of 'CheckHosts2.exe' with their respective PIDs: 26420, 24040, 16276, 1100, 2144, 29170, 15708, 10084, 23332, and 23376. To the right, a portion of the Process Monitor (Procmon) log is visible, showing a list of processes including 'svchost.exe', 'taskhostw.exe', and multiple instances of 'CheckHosts2.exe' and 'wscript.exe'.

Process Name	PID	Path	Company Name
svchost.exe	1704	C:\WINDOWS\system32\svchost.exe	Microsoft Cor.
taskhostw.exe	1672	C:\WINDOWS\system32\taskhostw.exe	Microsoft Cor.
CheckHosts2.exe	26420	C:\CheckHosts2.exe	Microsoft Cor.
wscript.exe	24040	C:\Windows\SysWOW64\wscript.exe	Microsoft Cor.
CheckHosts2.exe	16276	C:\CheckHosts2.exe	Microsoft Cor.
wscript.exe	1100	C:\Windows\SysWOW64\wscript.exe	Microsoft Cor.
CheckHosts2.exe	2144	C:\CheckHosts2.exe	Microsoft Cor.
wscript.exe	29170	C:\Windows\SysWOW64\wscript.exe	Microsoft Cor.
CheckHosts2.exe	15708	C:\CheckHosts2.exe	Microsoft Cor.
wscript.exe	10084	C:\Windows\SysWOW64\wscript.exe	Microsoft Cor.
CheckHosts2.exe	23332	C:\CheckHosts2.exe	Microsoft Cor.
wscript.exe	23376	C:\Windows\SysWOW64\wscript.exe	Microsoft Cor.

经了解，checkhosts2.exe 在计划任务中配置了检测到“安全”事件日志中出现 eventID 4663 后，触发此任务。

查看“安全”事件日志，发现一直在生成 4663 日志记录，导致了 checkhosts2.exe 一直重复启动退出。

4663 是在访问 C:\Windows\System32\drivers\etc\hosts 文件时产生的审核日志。

级别	日期和时间	来源	事件 ID	任务类别
信息	2022/11/4 15:51:46	Micros...	4663	File Syst...

事件 4663, Microsoft Windows security auditing.	
常规	详细信息
对象名:	C:\Windows\System32\drivers\etc\hosts
句柄 ID:	0x340
资源属性:	S:AI
进程信息:	
进程 ID:	0x3e14
进程名:	C:\Windows\SysWOW64\wscript.exe
访问请求信息:	
访问:	ReadData (或 ListDirectory)
访问掩码:	0x1

checkhosts2.exe 封装了 vbs 脚本，它运行时会调用 wscript.exe，事件日志显示此时的 4663 事件是读取（ReadData）hosts 文件产生的。

查看 hosts 文件的具体审核配置情况（PO-ICBC-HostFileMonitorPolicy）：

文件系统

C:\WINDOWS\SYSTEM32\DRIVERS\ETC\HOSTS

入选的 GPO

PO-ICBC-HostFileMonitorPolicy

配置这个文件或文件夹，然后: 向所有子文件夹和文件传播继承权限

所有者

权限

类型	名称	权限	应用于
允许	BUILTIN\Administrators	完全控制	此文件夹、子文件夹和文件
允许	CREATOR OWNER	完全控制	仅子文件夹和文件
允许	NT AUTHORITY\SYSTEM	完全控制	此文件夹、子文件夹和文件
允许	BUILTIN\Users	读取和执行	此文件夹、子文件夹和文件
允许	APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	读取和执行	此文件夹、子文件夹和文件

允许可继承的权限从父对象传播到此对象以及所有子对象

已禁用

正在审核

类型	名称	访问	应用于
成功	Everyone	读取和执行	此文件夹、子文件夹和文件
成功	Everyone	创建文件/写入数据,写入属性,写入扩展属性	此文件夹、子文件夹和文件

允许可继承的审核项目从父对象传播到此对象以及所有子对象

已启用

开启了“读取和执行”审核配置，这使得 checkhosts2.exe 运行时生成 4663 事件，而计划任务发现有 4663 事件，会触发再次执行 checkhosts2.exe，导致 checkhosts2.exe 循环启动。

对比以前 checkhosts.exe 的计划任务对 hosts 文件的审核配置如下：

文件系统

C:\WINDOWS\SYSTEM32\DRIVERS\ETC\HOSTS

入选的 GPO

PO-ICBC-HostFileMonitorPolicy

配置这个文件或文件夹，然后：向所有子文件夹和文件传播继承权限

所有者

权限

类型	名称	权限	应用于
允许	BUILTIN\Administrators	完全控制	此文件夹、子文件夹和文件
允许	CREATOR OWNER	完全控制	仅子文件夹和文件
允许	NT AUTHORITY\SYSTEM	完全控制	此文件夹、子文件夹和文件
允许	BUILTIN\Users	读取和执行	此文件夹、子文件夹和文件
允许	APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	读取和执行	此文件夹、子文件夹和文件

允许可继承的权限从父对象传播到此对象以及所有子对象

已禁用

正在审核

类型	名称	访问	应用于
成功	Everyone	创建文件/写入数据,写入属性,写入扩展属性	此文件夹、子文件夹和文件

允许可继承的审核项目从父对象传播到此对象以及所有子对象

已启用

在测试环境中按照用户环境配置 hosts 文件审核，验证是否复现问题，如果关闭“读取和执行”审核策略，是否可以解决问题。

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](mailto:weiliang@cmgos.com)



发件人: Wei Liang  
发送时间: 2022 年 11 月 7 日 10:39  
收件人: '许翔' <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>; 'xiongqiang@nb.icbc.com.cn' <[xiongqiang@nb.icbc.com.cn](mailto:xiongqiang@nb.icbc.com.cn)>; '8655919@qq.com' <[8655919@qq.com](mailto:8655919@qq.com)>  
抄送: ICBC\_Notification <[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>  
主题: 回复: [案例号: CAS-07510-L4F4N9 ] % |P2|ICBC|反馈宁波分行用户鼠标图标问题 % 初次响应 CMIT:0001948

许先生 您好:

感谢您的电话接听。

经了解，checkhosts2.exe 在计划任务中配置了检测到“安全”事件日志中出现 eventID 4663 后，触发此任务。

查看“安全”事件日志，发现一直在生成 4663 日志记录，导致了 checkhosts2.exe 一直重复启动退出。

4663 是在访问 C:\Windows\System32\drivers\etc\hosts 文件时产生的审核日志。



checkhosts2.exe 封装了 vbs 脚本，它运行时会调用 wscript.exe，事件日志显示此时的 4663 事件是读取（ReadData）hosts 文件产生的。

查看 hosts 文件的具体审核配置情况（PO-ICBC-HostFileMonitorPolicy）：

文件系统

C:\WINDOWS\SYSTEM32\DRIVERS\ETC\HOSTS

入选的 GPO

PO-ICBC-HostFileMonitorPolicy

配置这个文件或文件夹，然后：向所有子文件夹和文件传播继承权限

所有者

权限

类型	名称	权限	应用于
允许	BUILTIN\Administrators	完全控制	此文件夹、子文件夹和文件
允许	CREATOR OWNER	完全控制	仅子文件夹和文件
允许	NT AUTHORITY\SYSTEM	完全控制	此文件夹、子文件夹和文件
允许	BUILTIN\Users	读取和执行	此文件夹、子文件夹和文件
允许	APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	读取和执行	此文件夹、子文件夹和文件

允许可继承的权限从父对象传播到此对象以及所有子对象

已禁用

正在审核

类型	名称	访问	应用于
成功	Everyone	读取和执行	此文件夹、子文件夹和文件
成功	Everyone	创建文件/写入数据,写入属性,写入扩展属性	此文件夹、子文件夹和文件

允许可继承的审核项目从父对象传播到此对象以及所有子对象

已启用

确实开启了“读取和执行”审核配置，这使得 checkhosts2.exe 运行时生成 4663 事件，而计划任务发现有 4663 事件，会触发再次执行 checkhosts2.exe，导致 checkhosts2.exe 循环启动。

对比以前 checkhosts.exe 的计划任务对 hosts 文件的审核配置如下：

文件系统

C:\WINDOWS\SYSTEM32\DRIVERS\ETC\HOSTS

入造的 GPO

PO-ICBC-HostFileMonitorPolicy

配置这个文件或文件夹，然后：向所有子文件夹和文件传播继承权限

所有者

权限			
类型	名称	权限	应用于
允许	BUILTIN\Administrators	完全控制	此文件夹、子文件夹和文件
允许	CREATOR OWNER	完全控制	仅子文件夹和文件
允许	NT AUTHORITY\SYSTEM	完全控制	此文件夹、子文件夹和文件
允许	BUILTIN\Users	读取和执行	此文件夹、子文件夹和文件
允许	APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	读取和执行	此文件夹、子文件夹和文件
允许可继承的权限从父对象传播到此对象以及所有子对象		已禁用	

正在审核

类型	名称	访问	应用于
成功	Everyone	创建文件/写入数据,写入属性,写入扩展属性	此文件夹、子文件夹和文件
允许可继承的审核项目从父对象传播到此对象以及所有子对象		已启用	

您可以在测试环境中按照用户环境配置 hosts 文件审核，验证是否复现问题，如果关闭“读取和执行”审核策略，是否可以解决问题。

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](mailto:weiliang@cmgos.com)



发件人: Wei Liang  
发送时间: 2022 年 11 月 7 日 10:13  
收件人: '许翔' <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>; 'xiongqiang@nb.icbc.com.cn' <[xiongqiang@nb.icbc.com.cn](mailto:xiongqiang@nb.icbc.com.cn)>; '8655919@qq.com' <[8655919@qq.com](mailto:8655919@qq.com)>  
抄送: ICBC\_Notification <[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>  
主题: 回复: [案例号: CAS-07510-L4F4N9 ] % |P2|ICBC|反馈宁波分行用户鼠标图标问题 %  
初次响应 CMIT:0001948

许先生 您好:

感谢您的电话接听。

再次对比查看 **hosts 文件**相关的组策略对比设置，此组策略名称为：**PO-ICBC-HostFileMonitorPolicy**

出现问题的设备的组策略配置：

文件系统

C:\WINDOWS\SYSTEM32\DRIVERS\ETC\HOSTS			
入选的 GPO		PO-ICBC-HostFileMonitorPolicy	
配置这个文件或文件夹，然后: 向所有子文件夹和文件传播继承权限			
所有者			
权限			
类型	名称	权限	应用于
允许	BUILTIN\Administrators	完全控制	此文件夹、子文件夹和文件
允许	CREATOR OWNER	完全控制	仅子文件夹和文件
允许	NT AUTHORITY\SYSTEM	完全控制	此文件夹、子文件夹和文件
允许	BUILTIN\Users	读取和执行	此文件夹、子文件夹和文件
允许	APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	读取和执行	此文件夹、子文件夹和文件
允许可继承的权限从父对象传播到此对象以及所有子对象		已禁用	
正在审核			
类型	名称	访问	应用于
成功	Everyone	读取和执行	此文件夹、子文件夹和文件
成功	Everyone	创建文件/写入数据,写入属性,写入扩展属性	此文件夹、子文件夹和文件
允许可继承的审核项目从父对象传播到此对象以及所有子对象		已启用	

未配置 checkhosts2.exe 应用前的组策略配置：

文件系统

C:\WINDOWS\SYSTEM32\DRIVERS\ETC\HOSTS			
入选的 GPO		PO-ICBC-HostFileMonitorPolicy	
配置这个文件或文件夹，然后: 向所有子文件夹和文件传播继承权限			
所有者			
权限			
类型	名称	权限	应用于
允许	BUILTIN\Administrators	完全控制	此文件夹、子文件夹和文件
允许	CREATOR OWNER	完全控制	仅子文件夹和文件
允许	NT AUTHORITY\SYSTEM	完全控制	此文件夹、子文件夹和文件
允许	BUILTIN\Users	读取和执行	此文件夹、子文件夹和文件
允许	APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES	读取和执行	此文件夹、子文件夹和文件
允许可继承的权限从父对象传播到此对象以及所有子对象		已禁用	
正在审核			
类型	名称	访问	应用于
成功	Everyone	创建文件/写入数据,写入属性,写入扩展属性	此文件夹、子文件夹和文件
允许可继承的审核项目从父对象传播到此对象以及所有子对象		已启用	

您这边可以测试 checkhosts2.exe 反复运行是否与 hosts 文件的审核配置有关。

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](mailto:weiliang@cmgos.com)



发件人: Wei Liang

发送时间: 2022 年 11 月 4 日 18:24

收件人: '许翔' <[win10sup@cdc.icbc.com.cn](mailto:win10sup@cdc.icbc.com.cn)>; 'xiongqiang@nb.icbc.com.cn'

<[xiongqiang@nb.icbc.com.cn](mailto:xiongqiang@nb.icbc.com.cn)>; '8655919@qq.com' <[8655919@qq.com](mailto:8655919@qq.com)>

抄送: ICBC\_Notification <[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>

主题: 回复: [案例号: CAS-07510-L4F4N9 ] % |P2|ICBC|反馈宁波分行用户鼠标图标问题 %  
初次响应 CMIT:0001948

许先生 您好:

感谢您的电话接听。

查看抓取的 procmon 日志, 发现 checkhosts2.exe 与 pcit.exe 一直在不停地启动退出,

checkhosts2.exe 是由计划任务执行的, 怀疑鼠标图标问题与此有关。

svchost.exe (1704)	Windows 服务主进程	C:\WINDOWS\system32\svchost.exe	Microsoft Cor...
taskhostw.exe (1672)	Windows 任务的主机进程	C:\WINDOWS\system32\taskhostw.exe	Microsoft Cor...
CheckHosts2.exe (26420)		C:\CheckHosts2.exe	
wscript.exe (24040)	Microsoft * Windows Based Scri...	C:\WINDOWS\SysWOW64\wscript.exe	Microsoft Cor...
CheckHosts2.exe (16276)		C:\CheckHosts2.exe	
wscript.exe (1100)	Microsoft * Windows Based Scri...	C:\WINDOWS\SysWOW64\wscript.exe	Microsoft Cor...
CheckHosts2.exe (2144)		C:\CheckHosts2.exe	
wscript.exe (29170)	Microsoft * Windows Based Scri...	C:\WINDOWS\SysWOW64\wscript.exe	Microsoft Cor...
CheckHosts2.exe (15708)		C:\CheckHosts2.exe	
wscript.exe (10084)	Microsoft * Windows Based Scri...	C:\WINDOWS\SysWOW64\wscript.exe	Microsoft Cor...
CheckHosts2.exe (23332)		C:\CheckHosts2.exe	
wscript.exe (23376)	Microsoft * Windows Based Scri...	C:\WINDOWS\SysWOW64\wscript.exe	Microsoft Cor...
scclient.exe (29088)	scclient.exe (29088)	C:\WINDOWS\SysWOW64\Pclient\app\scclient...	
kvoop.exe (9064)		C:\WINDOWS\SysWOW64\Pclient\app\hplib\kv...	
kvoop.exe (27684)		C:\WINDOWS\SysWOW64\Pclient\app\hplib\kv...	
pcit_x64.exe (23104)		C:\WINDOWS\SysWOW64\Pclient\appx64\pcit_...	
pcit_x64.exe (27428)		C:\WINDOWS\SysWOW64\Pclient\appx64\pcit_...	
pcit_x64.exe (18892)		C:\WINDOWS\SysWOW64\Pclient\appx64\pcit_...	
pcit.exe (12640)		C:\WINDOWS\SysWOW64\Pclient\app\pcit.exe	
pcit.exe (18560)		C:\WINDOWS\SysWOW64\Pclient\app\pcit.exe	
pcit_x64.exe (9208)		C:\WINDOWS\SysWOW64\Pclient\appx64\pcit_...	
pcit.exe (24720)		C:\WINDOWS\SysWOW64\Pclient\app\pcit.exe	
pcit.exe (21188)		C:\WINDOWS\SysWOW64\Pclient\app\pcit.exe	
pcit.exe (23660)		C:\WINDOWS\SysWOW64\Pclient\app\pcit.exe	
pcit.exe (17112)		C:\WINDOWS\SysWOW64\Pclient\app\pcit.exe	
pcit.exe (20988)		C:\WINDOWS\SysWOW64\Pclient\app\pcit.exe	

经了解, checkhosts2.exe 在计划任务中是检测到“安全”事件日志中出现 eventID 4663 后, 会触发此任务。查看“安全”事件日志, 发现一直在生成 4663 日志记录, 导致了 cheskhosht2.exe 一直重复启动退出。

4663 是在访问 C:\Windows\System32\drivers\etc\hosts 文件时产生的审核日志。

级别	日期和时间	来源	事件 ID	任务类别
① 信息	2022/11/4 14:52:44	Microsoft Windows ...	4663	File System
① 信息	2022/11/4 14:52:43	Microsoft Windows ...	4663	File System
① 信息	2022/11/4 14:52:42	Microsoft Windows ...	4663	File System
① 信息	2022/11/4 14:52:41	Microsoft Windows ...	4663	File System

事件 4663, Microsoft Windows security auditing

常规 详细信息

对象服务器: Security

对象类型: File

对象名: C:\Windows\System32\drivers\etc\hosts

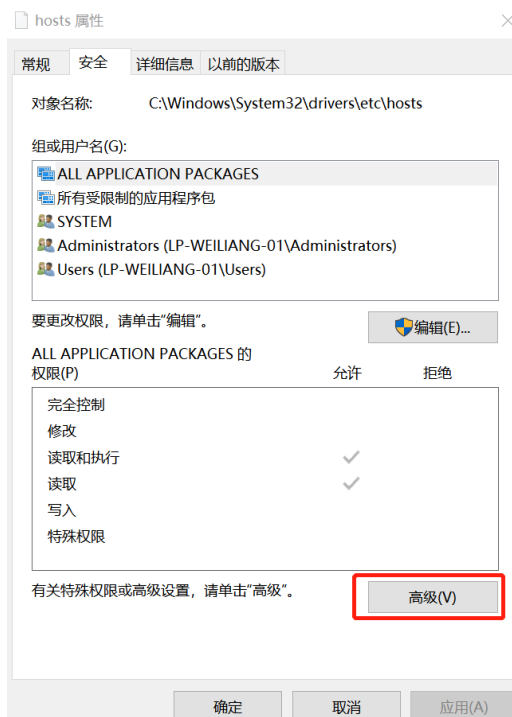
句柄 ID: 0x35c

资源属性: S:AI

### 下一步建议：

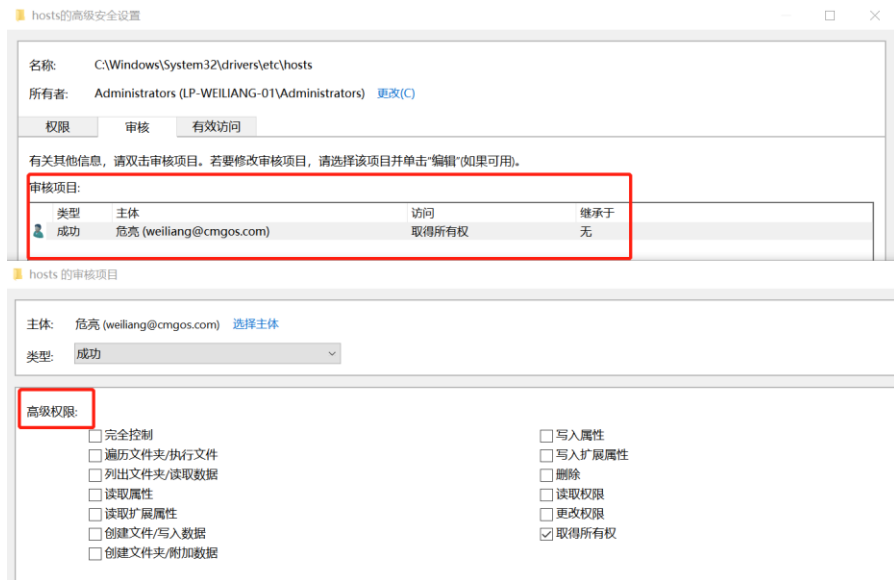
排查出问题的设备上的 hosts 文件审核配置情况，与未出现问题的设备上的审核配置对比有什么区别，查看文件审核配置如图所示：

- 1) 查看 hosts 文件的“属性”，在“安全”页选择“高级”。



- 2) 在打开的页面中选择“审核”，查看具体的配置情况，注意要打开具体的审核项目并选择“高级权限”查看具体配置。





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](mailto:weiliang@cmgos.com)



发件人: Wei Liang  
发送时间: 2022 年 11 月 4 日 17:25  
收件人: '许翔' <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>; 'xiongqiang@nb.icbc.com.cn' <[xiongqiang@nb.icbc.com.cn](mailto:xiongqiang@nb.icbc.com.cn)>; '8655919@qq.com' <[8655919@qq.com](mailto:8655919@qq.com)>  
抄送: ICBC\_Notification <[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>  
主题: 回复: [案例号: CAS-07510-L4F4N9 ] % |P2|ICBC|反馈宁波分行用户鼠标图标问题 %  
初次响应 CMIT:0001948

熊先生 您好:

您发送的鼠标图标问题的邮件已经收到, 正在下载相关日志, 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](mailto:weiliang@cmgos.com)



---

**发件人:** Wei Liang  
**发送时间:** 2022 年 11 月 4 日 14:30  
**收件人:** 许翔 <[win10sup@cdc.icbc.com.cn](mailto:win10sup@cdc.icbc.com.cn)>; 'xiongqiang@nb.icbc.com.cn' <[xiongqiang@nb.icbc.com.cn](mailto:xiongqiang@nb.icbc.com.cn)>; '8655919@qq.com' <[8655919@qq.com](mailto:8655919@qq.com)>  
**抄送:** ICBC\_Notification <[ICBC\\_Notification@cmgos.com](mailto:ICBC_Notification@cmgos.com)>  
**主题:** 回复: [案例号: CAS-07510-L4F4N9 ] % |P2|ICBC|反馈宁波分行用户鼠标图标问题 %  
初次响应 CMIT:0001948

熊先生 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:**

宁波分行用户反馈有设备的鼠标指针右边一直有圆圈图标显示, 需要协助排查是什么原因。

**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。

## 排查建议：

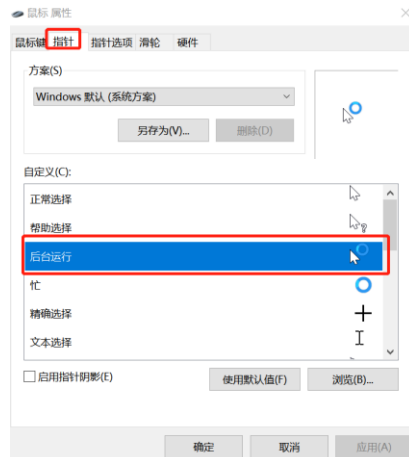
从以下链接下载收集日志所需的工具：

<https://cdac.cmgos.com/download.php?id=733&token=8vCL7U8G5hz8g9YaArusZo3K4CTIQ5RT>

1) 请确认设备上的鼠标属性配置情况，打开“控制面板”-“硬件和声音”类别中的“鼠标”项。



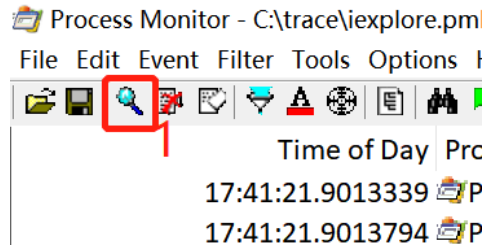
2) 确认 **鼠标属性** 的 **指针** 图标显示情况默认如下图所示。从此图中可以知道鼠标带圆圈图标表示后台运行。



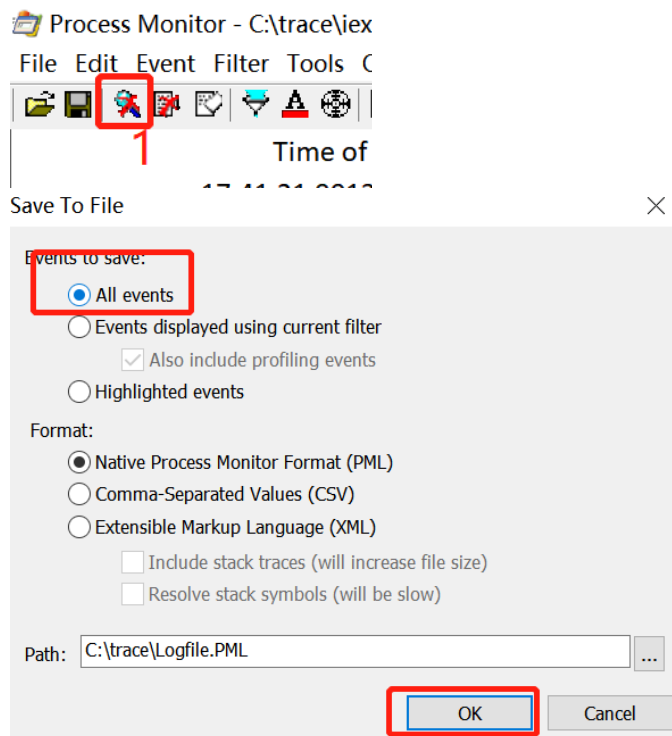
3) 打开任务管理器，切换到详细信息页面，注意观察是否有哪个应用的 PID 值在一直变化或者一直在新建应用进程，如果存在，将此应用强制结束或者卸载后，观察鼠标指针是否恢复正常。

4) 如果未发现异常的进程活动，按照以下操作收集 **procmon** 日志和 **wpr** 日志和相关系统日志。

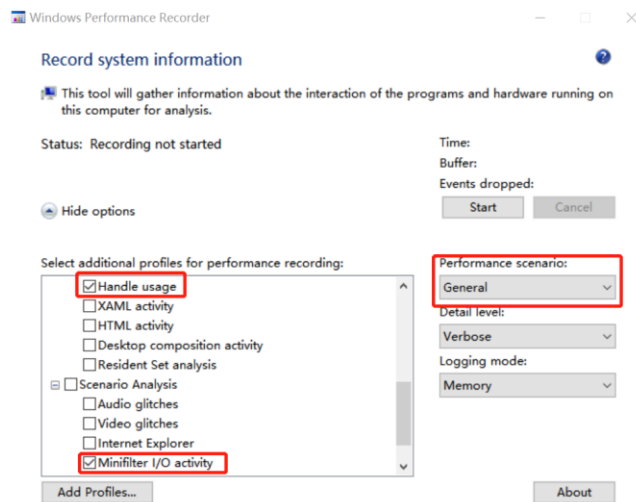
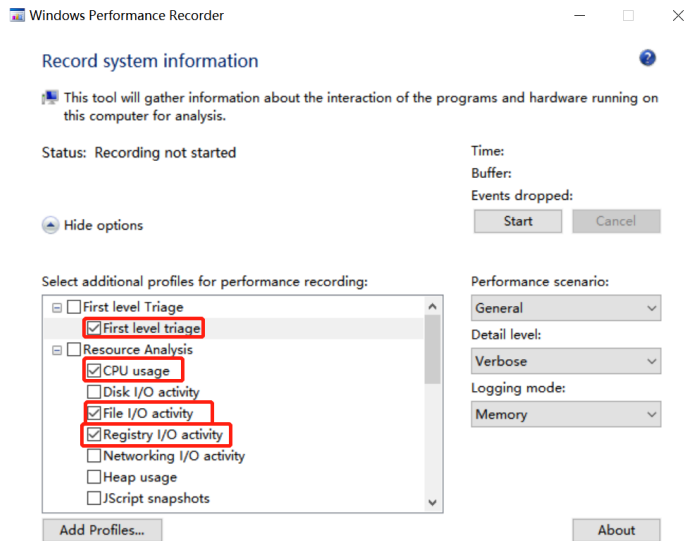
a. 运行 **procmon.exe**，点击 **accept** 后，到达如下图的界面：（图标 1 不带 x 表示处于抓取状态）



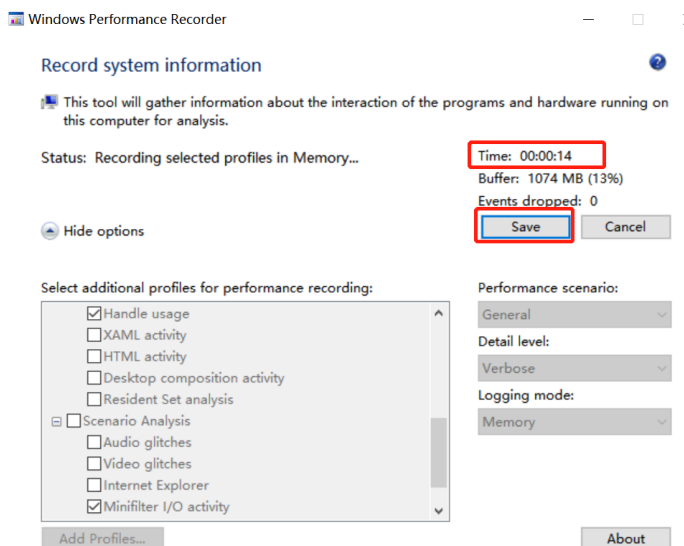
b. 在鼠标出现圆圈图标显示后，等待 20 秒钟左右，点击图标 1 停止抓取（停止抓取后图标 1 带 x），点击“File”-“save”，选择 **all events** 保存 pml 文件，将此文件压缩后上传。



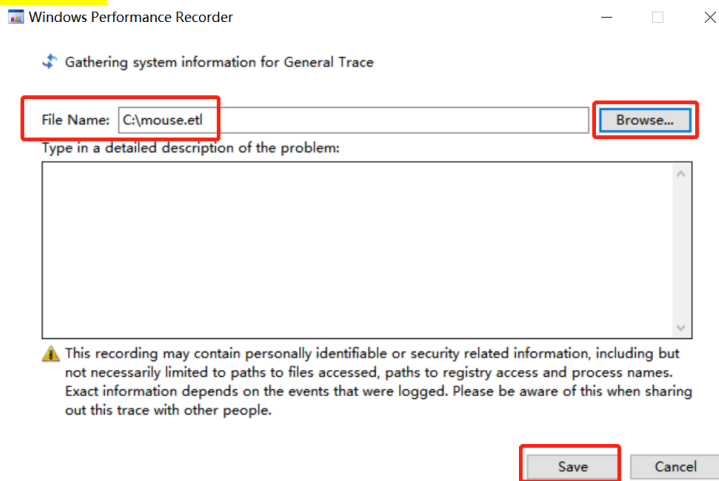
c. 打开 wpr 工具，运行 wprui.exe，出现热键提示时点击确定，在 wprui 配置界面，按照下图所示配置，即勾选“First level triage”、“CPU usage”、“File I/O activity”、“Registry I/O activity”、“Handle usage”、“Minifilter I/O activity”后，配置 Performance scenario 为 General。



- d. 配置完成后，点击“Start”开始抓取 wpr 日志，鼠标出现圆圈图标显示后，等待 20 秒钟  
(Time 显示持续时间)



e. 点击 Save 保存 wpr 日志，在 File Name 指定保存位置，点击 Save，将保存的 etl 日志压缩后上传。



f. 在设备上运行 CMGELogCollectorV2.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，将此压缩包上传。



**日志上传方法：**

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

用户名：icbcsupport

密码：icbcsupport

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](mailto:weiliang@cmgos.com)



---

发件人: Wei Liang <[weiliang@cmgos.com](mailto:weiliang@cmgos.com)>

发送时间: 2022 年 11 月 4 日 9:32

收件人: 许翔 <[win10sup@sdicbc.com.cn](mailto:win10sup@sdicbc.com.cn)>

抄送: Wei Liang <[weiliang@cmgos.com](mailto:weiliang@cmgos.com)>

主题: [案例号: CAS-07510-L4F4N9 ] % |P2|ICBC|反馈宁波分行用户鼠标图标问题 % 初次响应 CMIT:0001948

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-07510-L4F4N9 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”。