贾老师，给的日志是手动执行过脚本的，按照正常用户登录时间应该是早上 8 点 30 左右登录桌面，我让分行老师再收集一下从未执行过脚本的日志。

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆
中国工商银行软件开发中心（珠海）
许 翔
系统一部
电话：17606669571
☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

-----原始邮件-----

发件人: "Jia Wei" <jiawei@cmgos.com>
发送时间: 2023-05-25 09:54:35
收件人: "win10 技术支持" <win10 技术支持.软件开发中心系统一部@工商银行.icbc>
抄送: "ICBC_Notification" <icbc_notification@cmgos.com>
主题: 【外来邮件，注意核实】回复: [案例号: CAS-08988-G5D5Y2] % |P2|ICBC| 系统未加载登录脚本问题 % 初次响应 CMIT:0001309

许先生，您好

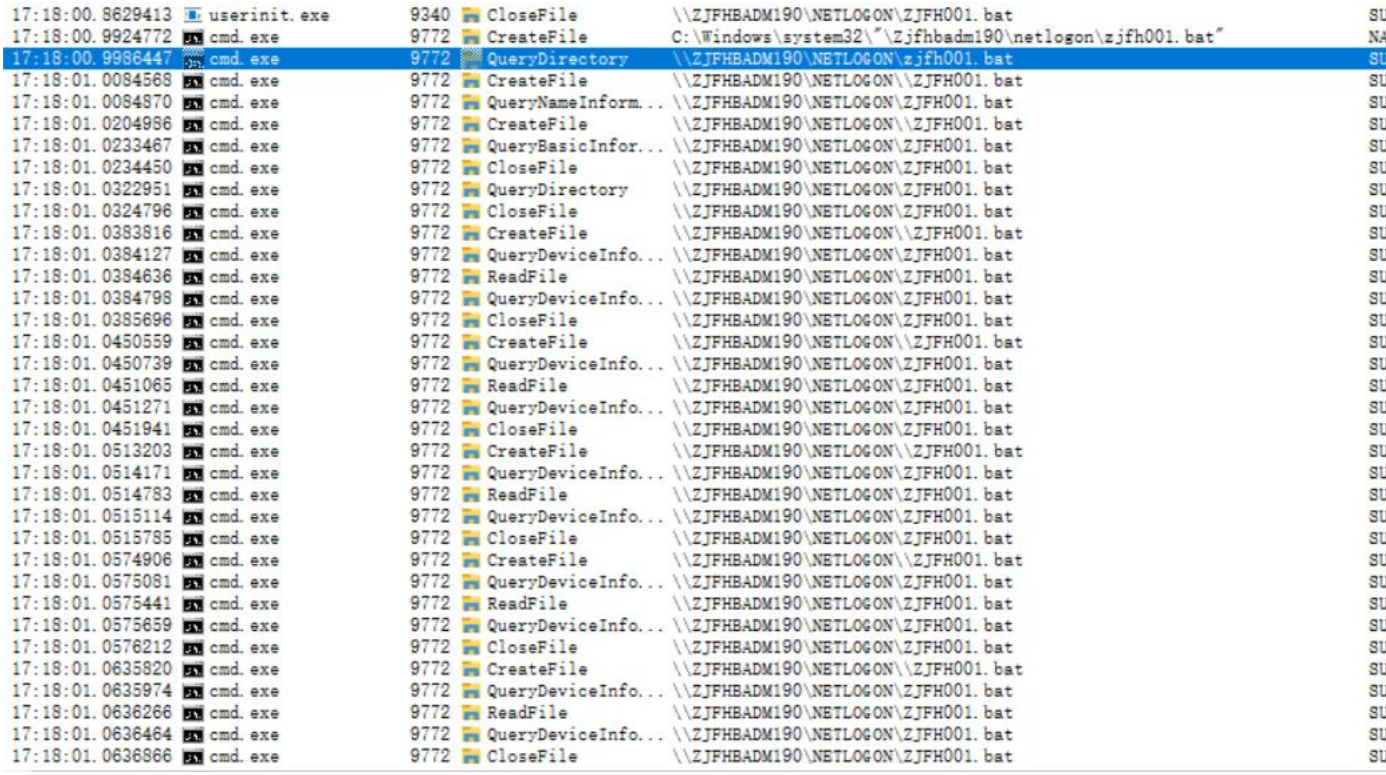
日志分析：

经过和本地测试环境日志对比，目前有如下发现

1）当前用户（**zjhz-weiq02**）登录过程中成功从\\ZJFHBADM190\NETLOGON 执行了脚本 zjfh001.bat；

2）未发现执行 **bjfh001.bat** 的记录

根据当前日志，客户端执行登录脚本正常。



17:18:00.8629413	userinit.exe	9340	CloseFile	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:00.9924772	cmd.exe	9772	CreateFile	C:\Windows\system32\"\Zjfhbadm190\netlogon\zjfh001.bat"	NA
17:18:00.9986447	cmd.exe	9772	QueryDirectory	\\ZJFHBADM190\NETLOGON\zjfh001.bat	SU
17:18:01.0084568	cmd.exe	9772	CreateFile	\\ZJFHBADM190\NETLOGON\\ZJFH001.bat	SU
17:18:01.0084870	cmd.exe	9772	QueryNameInform...	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0204986	cmd.exe	9772	CreateFile	\\ZJFHBADM190\NETLOGON\\ZJFH001.bat	SU
17:18:01.0233467	cmd.exe	9772	QueryBasicInfor...	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0234450	cmd.exe	9772	CloseFile	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0322951	cmd.exe	9772	QueryDirectory	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0324796	cmd.exe	9772	CloseFile	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0383816	cmd.exe	9772	CreateFile	\\ZJFHBADM190\NETLOGON\\ZJFH001.bat	SU
17:18:01.0384127	cmd.exe	9772	QueryDeviceInfo...	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0384636	cmd.exe	9772	ReadFile	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0384798	cmd.exe	9772	QueryDeviceInfo...	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0385696	cmd.exe	9772	CloseFile	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0450559	cmd.exe	9772	CreateFile	\\ZJFHBADM190\NETLOGON\\ZJFH001.bat	SU
17:18:01.0450739	cmd.exe	9772	QueryDeviceInfo...	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0451065	cmd.exe	9772	ReadFile	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0451271	cmd.exe	9772	QueryDeviceInfo...	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0451941	cmd.exe	9772	CloseFile	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0513203	cmd.exe	9772	CreateFile	\\ZJFHBADM190\NETLOGON\\ZJFH001.bat	SU
17:18:01.0514171	cmd.exe	9772	QueryDeviceInfo...	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0514783	cmd.exe	9772	ReadFile	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0515114	cmd.exe	9772	QueryDeviceInfo...	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0515785	cmd.exe	9772	CloseFile	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0574906	cmd.exe	9772	CreateFile	\\ZJFHBADM190\NETLOGON\\ZJFH001.bat	SU
17:18:01.0575081	cmd.exe	9772	QueryDeviceInfo...	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0575441	cmd.exe	9772	ReadFile	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0575659	cmd.exe	9772	QueryDeviceInfo...	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0576212	cmd.exe	9772	CloseFile	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0635820	cmd.exe	9772	CreateFile	\\ZJFHBADM190\NETLOGON\\ZJFH001.bat	SU
17:18:01.0635974	cmd.exe	9772	QueryDeviceInfo...	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0636266	cmd.exe	9772	ReadFile	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0636464	cmd.exe	9772	QueryDeviceInfo...	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU
17:18:01.0636866	cmd.exe	9772	CloseFile	\\ZJFHBADM190\NETLOGON\ZJFH001.bat	SU

请确认

1）目前域控设置的脚本文件是 **zjfh001.bat** 还是 **bjfh001.bat**

2）如果需要执行多个开机 bat 文件，建议使用 GPO 推送至对应 Groups

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: 2023 年 5 月 23 日 15:04
收件人: 许翔 <win10sup@sdc.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>

主题: 回复: [案例号: CAS-08988-G5D5Y2] % |P2|ICBC|系统未加载登录脚本问题 % 初次响应 CMIT:0001309

许先生，您好

很高兴与您电话沟通，目前还需要收集如下日志进一步分析。

问题定义:

部分用户的 win10 政府版 1809 在开机时，未加载域账户启动时需运行的登录脚本，请协助分析问题原因。

问题范围:

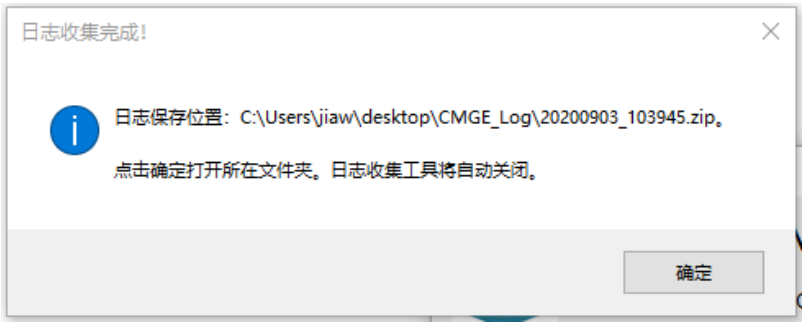
我们将协助您分析处理上述问题，并对定义的问题给予最大的技术支持。

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。

一、工具收集

1）在V2020-L和出现问题V2022-L的计算机上，分别下载附件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。



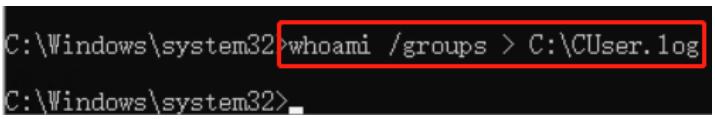
2）收集完毕后将在当前用户桌面生产CMGE_Log。点击确定，将直接打开文件夹并定为压缩文件。

3）将压缩文件上传。

二、用户 Groups 收集

以管理员身份运行命令提示符，运行如下命令，将 **C:\CUser.log 文件**反馈。

whoami /groups > C:\CUser.log



三、收集登录日志

配置注册表开启了三个日志 winlogon.log、netlogon.log 和 gpsvc.log

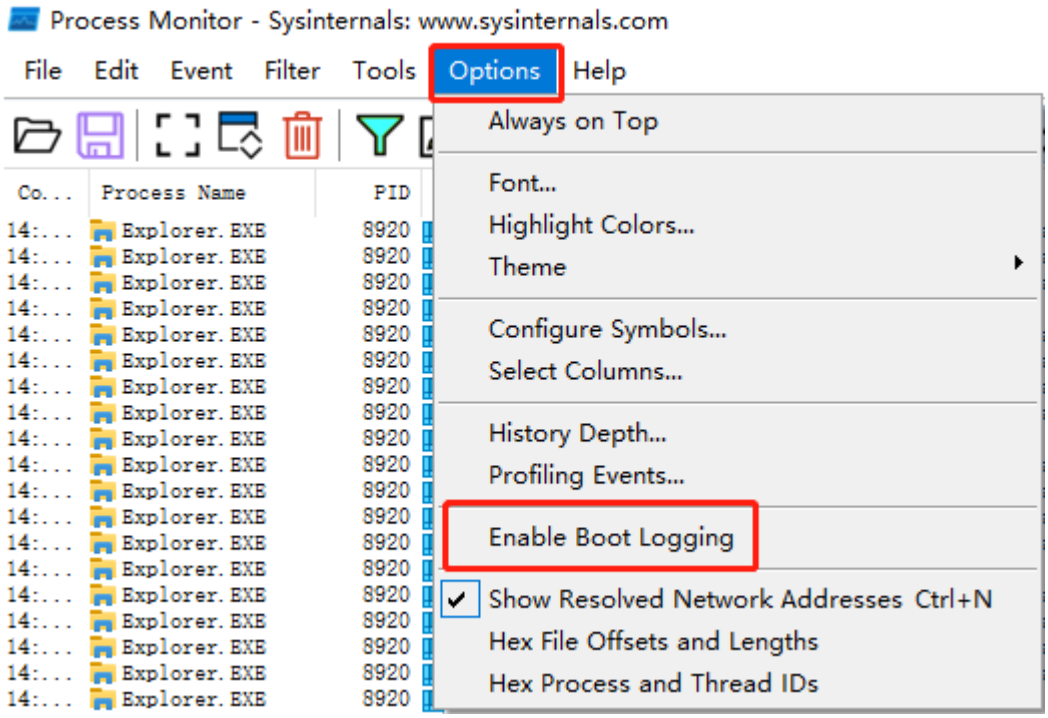
1）下载如下附件，**导入附件中的 gplog.zip 中的 gplog.reg 注册表文件**

https://cduc.cmgos.com/download.php?id=973&token=PpHfixZxEtxmXok0QEzB2dcKSPSeyheh

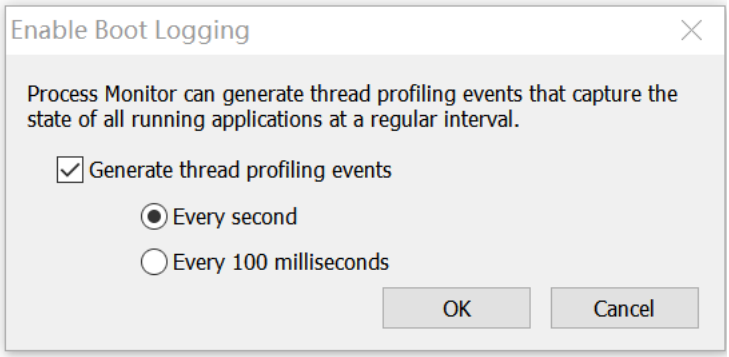
2）下载如下链接的 ProcessMonitor 工具

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

3）解压后运行 Procmon.exe，选择 **Options-Enable Boot Logging**，按照下图配置**开启 boot logging：**



4）勾选 **Generate thread profiling events**，选择 **Every second**，点击 **OK** 保存即可，然后关闭 procmon.exe。



5）**重启计算机登录域账号复现问题，再次打开 procmon.exe，**此时会提示保存 boot logging 日志。

6）将刚刚保存的**.pml 日志**、以及 **C:\Windows\security\logs**目录和 **C:\Windows\debug** 目录压缩后上传。

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: 2023 年 5 月 22 日 17:01
收件人: 许翔 <win10sup@sdc.icbc.com.cn>
抄送: Jia Wei <jiawei@cmgos.com>
主题: [案例号: CAS-08988-G5D5Y2] % |P2|ICBC|系统未加载登录脚本问题 % 初次响应 CMIT:0001309

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 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-08988-G5D5Y2 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”。