

于先生您好,

根据刚刚的沟通, 由于 Windows 日志中没有记录问题过程中的登录行为, 需要在问题复现后再收取此两项 Windows 日志进行分析。经您同意暂时归档此案例。

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:

-----  
问题定义: 用户反馈, 电脑使用时, 出现账号锁定, 需要排查账号锁定原因。

问题进展: 由于 Windows 日志中没有记录问题过程中的登录行为, 需要修改组策略后, 如果问题复现再收取此两项 Windows 日志进行分析, 用户后续如果再遇到类似问题会收取日志进行分析, 此案例暂时归档。

王彬彬 Wang Binbin  
神州网信技术有限公司  
C&M Information Technologies Co.,Ltd.  
热线电话: 400-818-0055  
电子邮箱 Email: [wangbb@cmgos.com](mailto:wangbb@cmgos.com)



---

发件人: 纡広傑 <[260115573@qq.com](mailto:260115573@qq.com)>

发送时间: 2020 年 7 月 24 日 8:40

收件人: Wang Binbin <[wangbb@cmgos.com](mailto:wangbb@cmgos.com)>

抄送: CRM Case Email <[casemail@cmgos.com](mailto:casemail@cmgos.com)>; Wang Wenlei <[wangwl@cmgos.com](mailto:wangwl@cmgos.com)>

主题: 回复: 回复: 回复: [案例号: CAS-02634-Q8N4M3 ] % 国网-中国电科院账户被锁定  
% 初次响应 CMIT:0001366

您好:

文件已发送, 请查收。

----- 原始邮件 -----

发件人: "Wang Binbin" <[wangbb@cmgos.com](mailto:wangbb@cmgos.com)>;

发送时间: 2020 年 7 月 23 日(星期四) 中午 1:39

收件人: "纡広傑" <[260115573@qq.com](mailto:260115573@qq.com)>;

抄送: "CRM Case Email" <[casemail@cmgos.com](mailto:casemail@cmgos.com)>; "Wang Wenlei" <[wangwl@cmgos.com](mailto:wangwl@cmgos.com)>;

主题: 回复: 回复: [案例号: CAS-02634-Q8N4M3 ] % 国网-中国电科院账户被锁定 % 初次响应  
CMIT:0001366

好的

王彬彬 Wang Binbin

神州网信技术有限公司

C&M Information Technologies Co.,Ltd.

热线电话：400-818-0055

电子邮箱 Email: [wangbb@cmgos.com](mailto:wangbb@cmgos.com)



---

发件人: 纡広傑 <[260115573@qq.com](mailto:260115573@qq.com)>

发送时间: 2020 年 7 月 23 日 13:25

收件人: Wang Binbin <[wangbb@cmgos.com](mailto:wangbb@cmgos.com)>

抄送: CRM Case Email <[casemail@cmgos.com](mailto:casemail@cmgos.com)>; Wang Wenlei <[wangwl@cmgos.com](mailto:wangwl@cmgos.com)>

主题: 回复: [案例号: CAS-02634-Q8N4M3 ] % 国网-中国电科院账户被锁定 % 初次响应  
CMIT:0001366

您好:

客户今天不在院里，明天给您发送吧，之前的包没有留存。

----- 原始邮件 -----

发件人: "纡広傑" <[260115573@qq.com](mailto:260115573@qq.com)>;

发送时间: 2020 年 7 月 22 日(星期三) 下午 5:28

收件人: "Wang Binbin" <[wangbb@cmgos.com](mailto:wangbb@cmgos.com)>;

抄送: "CRM Case Email"<[casemail@cmgos.com](mailto:casemail@cmgos.com)>; "Wang Wenlei"<[wangwl@cmgos.com](mailto:wangwl@cmgos.com)>;

主题: 回复: [案例号: CAS-02634-Q8N4M3 ] % 国网-中国电科院账户被锁定 % 初次响应 CMIT:0001366

您好:

文件已上传, 请查收

----- 原始邮件 -----

发件人: "Wang Binbin" <[wangbb@cmgos.com](mailto:wangbb@cmgos.com)>;

发送时间: 2020 年 7 月 22 日(星期三) 上午 10:49

收件人: "纡広傑"<[260115573@qq.com](mailto:260115573@qq.com)>;

抄送: "CRM Case Email"<[casemail@cmgos.com](mailto:casemail@cmgos.com)>; "Wang Wenlei"<[wangwl@cmgos.com](mailto:wangwl@cmgos.com)>;

主题: 回复: [案例号: CAS-02634-Q8N4M3 ] % 国网-中国电科院账户被锁定 % 初次响应 CMIT:0001366

于先生, 您好:

根据与您的沟通, 我谨在此阐述问题涉及的范围定义:

问题范围: 用户反馈, 电脑使用时, 出现账号锁定, 需要排查账号锁定原因。

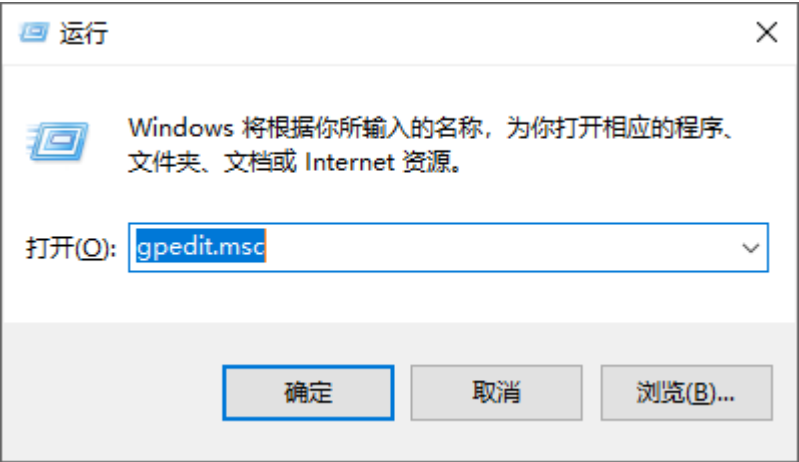
问题定义: 协助用户排查问题原因。

如您对以上问题范围定义有任何疑问请直接与我联系。

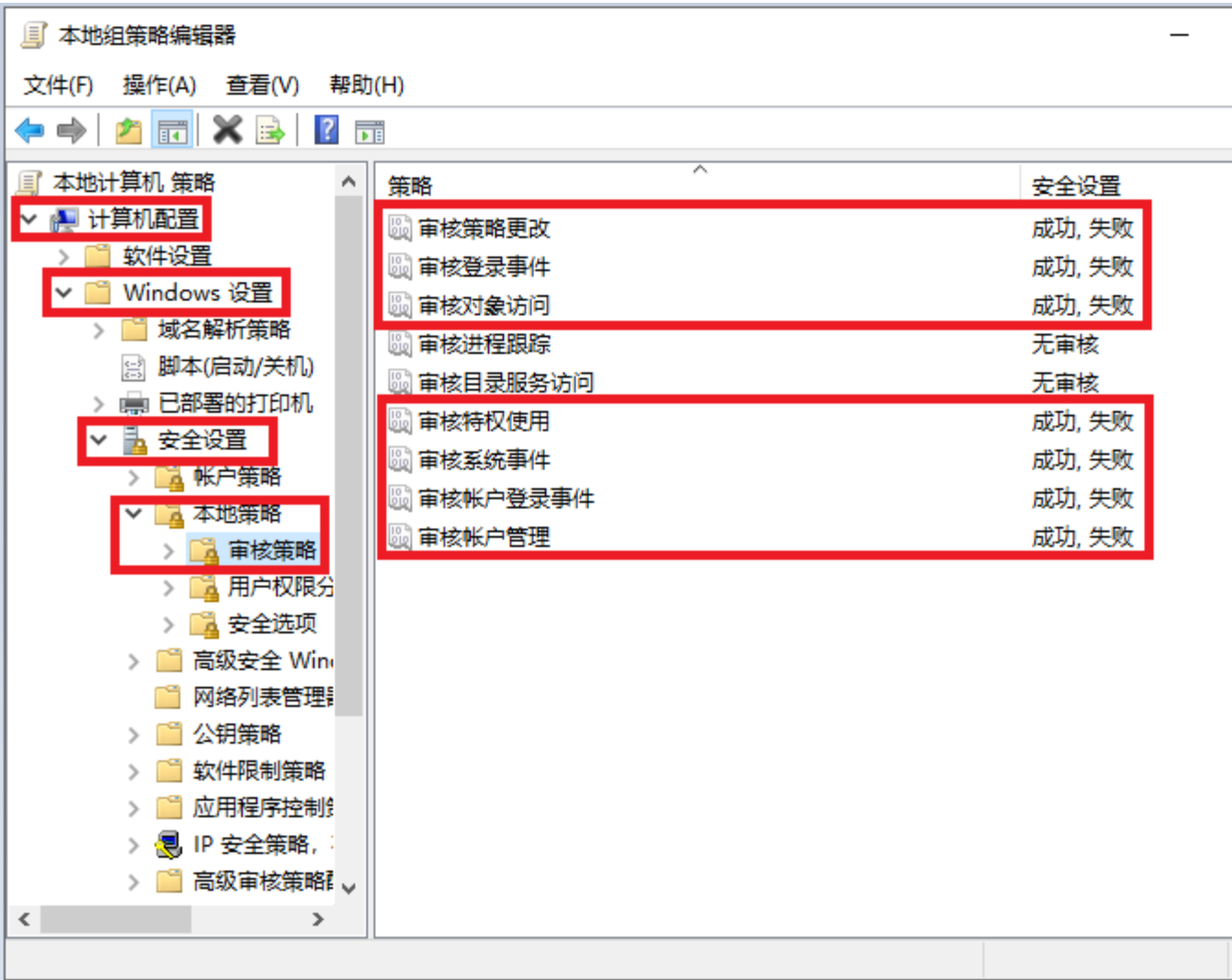
根据刚刚的电话沟通请您进行以下操作, 并收取相关信息提供给我, 我会尽快进行排查定位问题:

=====

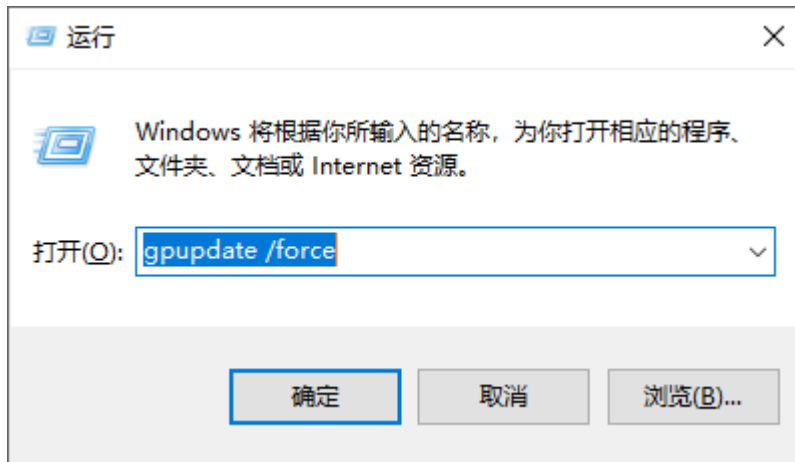
1. 键入 Windows 键+R 键调出运行栏，输入 gpedit.msc，打开本地组策略编辑器
























2. 如下图对红框内的组策略项进行设置



3. 设置完成后，退出组策略编辑器，键入 Windows 键+R 键调出运行栏，输入 gpupdate /force，更新组策略



4. 目前无法判断 Windows 日志中是否会记录问题过程中的登录行为，请您先将路径：C:\Windows\System32\winevt\Logs 下的 security.evtx 和 system.evtx 文件提供给我，如排查后确认日志中没有相关记录，需要在问题复现后再收取此两项 Windows 日志进行分析。

此电脑 > 本地磁盘 (C:) > Windows > System32 > winevt > Logs		
名称		修改日期
 Microsoft-Windows-Winsock-WS2HELP%4Operational.evtx		2019/4/2 23:12
 Microsoft-Windows-Wired-AutoConfig%4Operational.evtx		2018/10/29 19:
 Microsoft-Windows-WLAN-AutoConfig%4Operational.evtx		2019/8/9 18:40
 Microsoft-Windows-WMI-Activity%4Operational.evtx		2019/8/12 9:06
 Microsoft-Windows-WorkFolders%4Operational.evtx		2018/10/29 19:1
 Microsoft-Windows-WorkFolders%4WHC.evtx		2018/9/12 17:18
 Microsoft-Windows-Workplace Join%4Admin.evtx		2018/10/29 19:1
 Microsoft-Windows-WPD-ClassInstaller%4Operational.evtx		2018/10/29 19:1
 Microsoft-Windows-WPD-CompositeClassDriver%4Operational.evtx		2018/10/29 19:1
 Microsoft-Windows-WPD-MTPClassDriver%4Operational.evtx		2019/3/25 9:33
 Microsoft-Windows-WWAN-SVC-Events%4Operational.evtx		2018/10/29 19:1
 OAlerts.evtx		2019/8/12 10:05
 RemoteDesktopServices-RemoteFX-SessionLicensing-Admin.evtx		2018/9/29 14:18
 RemoteDesktopServices-RemoteFX-SessionLicensing-Debug.etl		2019/8/9 18:40
 RemoteDesktopServices-RemoteFX-SessionLicensing-Operational.evtx		2018/9/29 14:18
 <u>Security.evtx</u>		2019/8/12 9:36
 Setup.evtx		2019/8/2 10:00
 SMSApi.evtx		2018/10/29 19:
 Symantec Endpoint Protection Client.evtx		2019/4/12 11:30
 <u>System.evtx</u>		2019/8/12 9:05
 Windows PowerShell.evtx		2019/8/12 9:06

上传方法：

登录上传系统，使用以下账号密码登录，将收集的 2 个日志文件（security.evtx 和 system.evtx）上传此系统。

网址：cdue.comgos.com

账号：yu123

密码：123456

谢谢。

王彬彬 Wang Binbin

神州网信技术有限公司

C&M Information Technologies Co.,Ltd.

热线电话: 400-818-0055

电子邮箱 Email: [wangbb@cmgos.com](mailto:wangbb@cmgos.com)



---

发件人: Wang Binbin <[wangbb@cmgos.com](mailto:wangbb@cmgos.com)>

发送时间: 2020 年 7 月 22 日 10:30

收件人: 于先生 <[260115573@qq.com](mailto:260115573@qq.com)>

抄送: Wang Binbin <[wangbb@cmgos.com](mailto:wangbb@cmgos.com)>

主题: [案例号: CAS-02634-Q8N4M3 ] % 国网-中国电科院账户被锁定 % 初次响应  
CMIT:0001366

于先生 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 王彬彬。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-02634-Q8N4M3 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”。