Hi Lianbin:

根据刚才的电话沟通，我将暂时归档此案例。
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：多台新机的定制系统在登录后，发生账户异常锁定情况

问题分析：
在 CMGE 系统下，根据安全规范配置由帐户锁定阈值为 5 次，在此情况下，在安全日志中，可以看到 iNodeSec.exe 从 13:02:41 一直到 13:03:25 短时间内，一直是在使用 user 用户名远程登录失败，大概有 3~4 千条的登录失败日志；
测试在配置 iNode 认证前，先修改帐户锁定阈值为 0 后，再配置 iNode 认证，则没有出现大量的登录失败信息。也没有出现帐户锁定情况。
暂时可以通过配置帐户锁定阈值为 0 解决此问题。

问题总结：在配置 iNode 认证之前，先配置帐户锁定阈值为 0 后，再配置 iNode 认证，测试未出现帐户锁定情况。等待用户最终测试反馈。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

神州网信 CMIT

发件人: Lianbin.Que@dell.com <Lianbin.Que@dell.com>
发送时间: 2020 年 7 月 22 日 9:02
收件人: Wei Liang <weiliang@cmgos.com>; Sherwood.Wang@dell.com; Lisa.Li@Dell.com; Sun Zhenning <sunzn@cmgos.com>
抄送: Wade.Wang1@Dell.com; Tony.Hong@dell.com; CRM Case Email <casemail@cmgos.com>; Liu Jian <liujian@cmgos.com>; Hao.Xu@Dell.com
主题: 回复: [案例号: CAS-02606-V9R5J2] % |普通事件| Dell | 多台 OPTI 7070 新机发生账户锁定情况 % 初次响应 CMIT:0001309

Hi Liang
因提取的日志过大，我们放到共享网盘中：
链接：https://pan.baidu.com/s/1Ls6ZnWpawhO6FdMOED1efQ　　提取码：ntfw

Lianbin_Que
CTE, Great China Client Technical Support
Pro Support | Pro Support Plus
office +86-592-818-8753

发件人: Wei Liang <weiliang@cmgos.com>
发送时间: 2020 年 7 月 20 日 16:19
收件人: Wang, Sherwood; Li, Lisa(TSM); Que, Lianbin; Sun Zhenning
抄送: Wang, Wade; Hong, Tony; CRM Case Email; Liu Jian; Xu, Hao
主题: 回复: [案例号: CAS-02606-V9R5J2] % |普通事件| Dell | 多台 OPTI 7070 新机发生账户锁定情况 % 初次响应 CMIT:0001309

[EXTERNAL EMAIL]

Hi Sherwood:

这里没有收到您发送的网盘链接下载地址，麻烦您再发送一次。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Sherwood.Wang@dell.com <Sherwood.Wang@dell.com>
发送时间: 2020 年 7 月 20 日 16:11
收件人: Lisa.Li@Dell.com; Wei Liang <weiliang@cmgos.com>; Lianbin.Que@dell.com; Sun Zhenning <sunzn@cmgos.com>
抄送: Wade.Wang1@Dell.com; Tony.Hong@dell.com; CRM Case Email <casemail@cmgos.com>; Liu Jian <liujian@cmgos.com>; Hao.Xu@Dell.com

主题: RE: [案例号: CAS-02606-V9R5J2] % |普通事件| Dell | 多台 OPTI 7070 新机发生账户锁定情况 % 初次响应 CMIT:0001309

Dell Customer Communication - Confidential

Hi 危工,

如电话沟通，下午 2 点多我用个人账号已经把网盘链接发给你这边。请查收。

谢谢!

Regards,

Sherwood Wang, PMP®

End User Computing Deployment Services (终端部署服务), Greater China

Dell Technologies | Services

Office: +86 592 818 5884 **Cell**: +86 180 3008 5632

Know more about EUC Deployment Services, visit us at Dell site

---

From: Li, Lisa(TSM) <Lisa_Li10@Dell.com>
Sent: Monday, July 20, 2020 4:05 PM
To: Wei Liang; Que, Lianbin; Wang, Sherwood; Sun Zhenning
Cc: Wang, Wade; Hong, Tony; CRM Case Email; Liu Jian; Xu, Hao
Subject: RE: [案例号: CAS-02606-V9R5J2] % |普通事件| Dell | 多台 OPTI 7070 新机发生账户锁定情况 % 初次响应 CMIT:0001309

Dell Customer Communication - Confidential

@Sun Zhenning
危良提到的开启高级审核模式， 明天收集日志时供参考。

@Wang, Sherwood
上传镜像的方法如下， 还请协助提供镜像。

1．将附件文件拷贝并解压到本地，运行 sftp 客户端软件（如 FileZilla）

您可以通过此连接下载 filezilla 客户端软件，https://filezilla-project.org/download.php

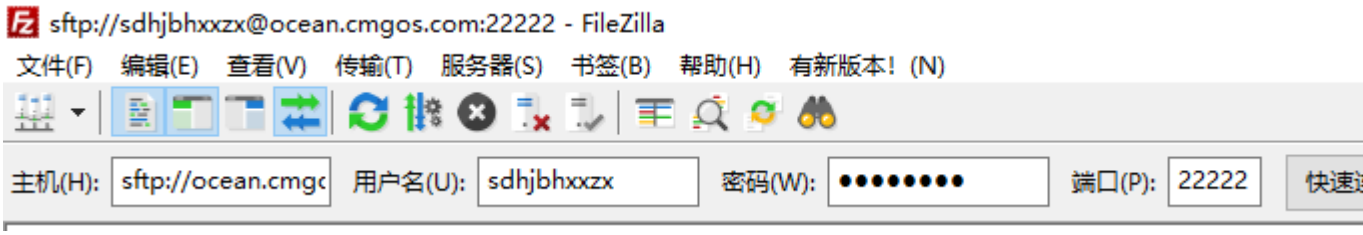
2．输入服务器\用户名\密码

外网登陆地址：sftp://ocean.cmgos.com:22222

用户名：sdhjbhxxzx

密码：J63NA32d

端口：22222



3．连接到 SFTP 文件服务器后，在提示框选择"确定"，进入 SFTP 服务器的 upload 路径下，再右键点击镜像文件-上传，等待上传完成。

Best Regards,
Lisa

From: Wei Liang <weiliang@cmgos.com>
Sent: 2020 年 7 月 20 日 15:55
To: Que, Lianbin
Cc: Wang, Wade; Sun Zhenning; Hong, Tony; Li, Lisa(TSM); CRM Case Email; Liu Jian
Subject: 回复: [案例号: CAS-02606-V9R5J2] % |普通事件| Dell | 多台 OPTI 7070 新机发生账户锁定情况 % 初次响应 CMIT:0001309

[EXTERNAL EMAIL]

Hi lianbin:

您可以通过此连接下载 filezilla 客户端软件，https://filezilla-project.org/download.php
开启高级审核模式在开箱登录修改密码后，开始配置即可。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2020 年 7 月 20 日 15:10
收件人: 'Lianbin.Que@dell.com' <Lianbin.Que@dell.com>
抄送: Wade.Wang1@Dell.com; Sun Zhenning <sunzn@cmgos.com>; Tony.Hong@dell.com; Lisa.Li@Dell.com; CRM Case Email <casemail@cmgos.com>; Liu Jian <liujian@cmgos.com>
主题: 回复: [案例号：CAS-02606-V9R5J2] % |普通事件| Dell | 多台 OPTI 7070 新机发生账户锁定情况 % 初次响应 CMIT:0001309

Hi lianbin:

Sftp 客户端软件 filezilla 请您查收。
开启高级审核模式在开箱登录修改密码后，开始配置即可。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Lianbin.Que@dell.com <Lianbin.Que@dell.com>
发送时间: 2020 年 7 月 20 日 15:05
收件人: Wei Liang <weiliang@cmgos.com>
抄送: Wade.Wang1@Dell.com; Sun Zhenning <sunzn@cmgos.com>;

Tony.Hong@dell.com; Lisa.Li@Dell.com; CRM Case Email <casemail@cmgos.com>; Liu Jian <liujian@cmgos.com>
主题: 回复: [案例号: CAS-02606-V9R5J2] % |普通事件| Dell | 多台 OPTI 7070 新机发生账户锁定情况 % 初次响应 CMIT:0001309

Dell Customer Communication - Confidential

Hi Liang
我们这未收到相关附件，请帮忙再次确定下.
==========
1．将附件文件拷贝并解压到本地，运行 sftp 客户端软件（如 FileZilla）
2．输入服务器\用户名\密码

下面这个设置操作是什么时候操作？开箱后更改密码后或什么操作前？
可以开启高级审核策略获取更详细的审核信息，操作方法如下：

Lianbin_Que
CTE, Great China Client Technical Support
Pro Support | Pro Support Plus
office +86-592-818-8753

发件人: Wei Liang <weiliang@cmgos.com>
发送时间: 2020 年 7 月 20 日 14:36
收件人: Que, Lianbin
抄送: Wang, Wade; Sun Zhenning; Hong, Tony; Li, Lisa(TSM); CRM Case Email; Liu Jian
主题: 回复: [案例号: CAS-02606-V9R5J2] % |普通事件| Dell | 多台 OPTI 7070 新机发生账户锁定情况 % 初次响应 CMIT:0001309

[EXTERNAL EMAIL]

Hi lianbin:

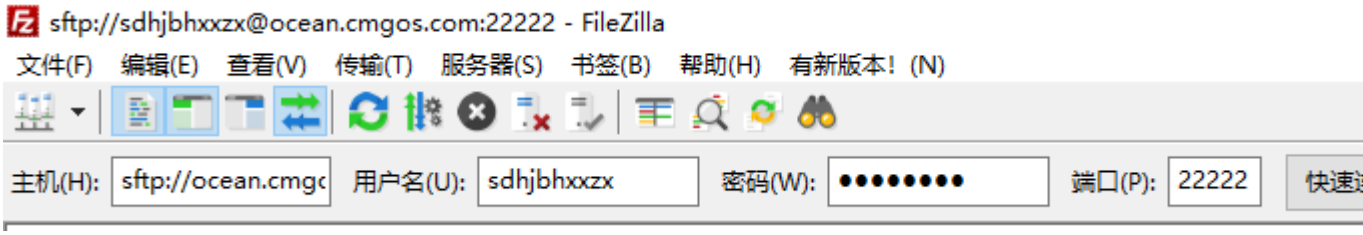
根据上午的沟通情况，可以使用 sftp 上传定制镜像，以下为操作步骤:
==========
1．将附件文件拷贝并解压到本地，运行 sftp 客户端软件（如 FileZilla）
2．输入服务器\用户名\密码

外网登陆地址：sftp://ocean.cmgos.com:22222

用户名：sdhjbhxxzx

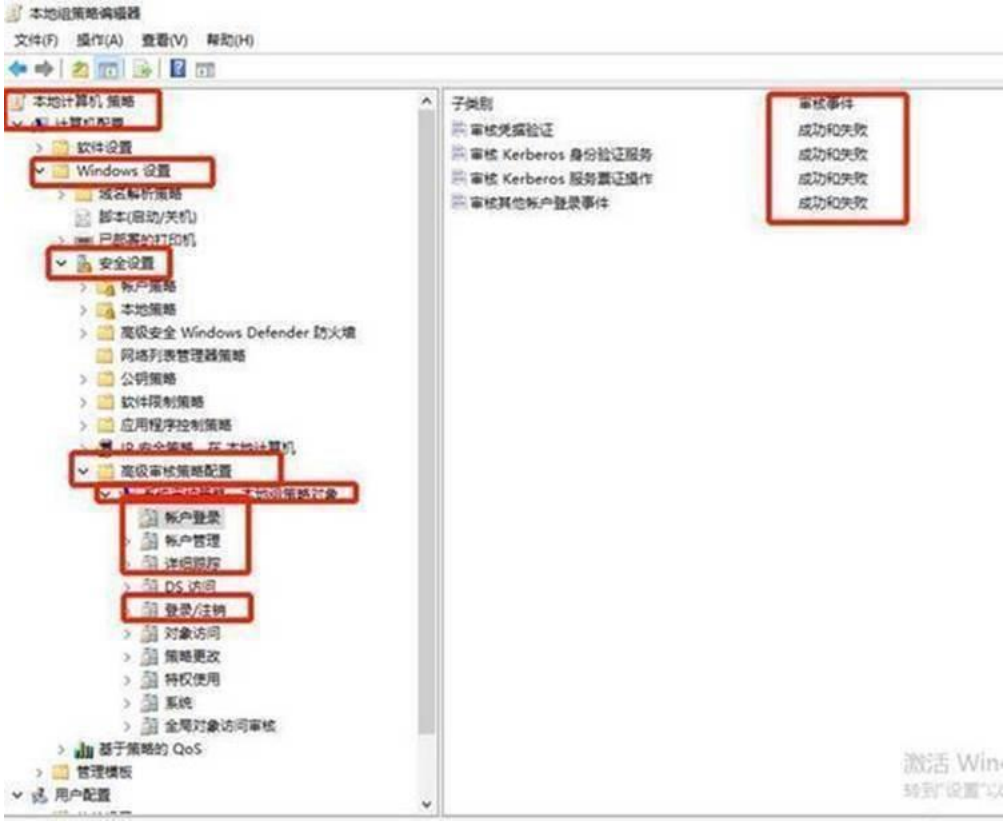
密码：J63NA32d

端口：22222

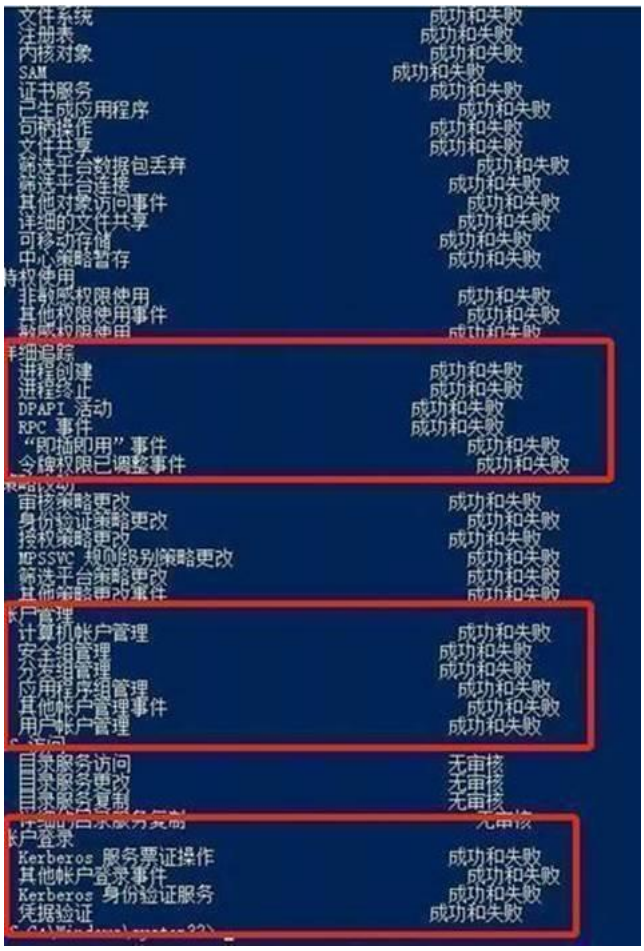


3．连接到 SFTP 文件服务器后，在提示框选择“确定”，进入 SFTP 服务器的 upload 路径下，再右键点击镜像文件-上传，等待上传完成。

可以开启高级审核策略获取更详细的审核信息，操作方法如下：
gpedit.msc 打开本地组策略，定位到
本地计算机策略-计算机配置-Windows 设置-安全设置-高级审核策略配置-“系统审核策略-本地组策略对象”
选定“帐户登录”、“帐户管理”、“详细跟踪”、“登录/注销”这几项中的所有类别的审核事件都配置为“成功和失败”。



使用管理员方式打开 cmd 命令行，运行 gpupdate /force 更新组策略
在 cmd 命令行中运行 auditpol /get /category:* 查看配置是否生效。



等待问题复现后收集系统日志和安全日志。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Lianbin.Que@dell.com <Lianbin.Que@dell.com>
发送时间: 2020 年 7 月 20 日 10:26
收件人: Wei Liang <weiliang@cmgos.com>

抄送: Wade.Wang1@Dell.com; Sun Zhenning <sunzn@cmgos.com>; Tony.Hong@dell.com; Lisa.Li@Dell.com; CRM Case Email <casemail@cmgos.com>; Liu Jian <liujian@cmgos.com>
主题: 回复: [案例号: CAS-02606-V9R5J2] % |普通事件| Dell | 多台 OPTI 7070 新机发生账户锁定情况 % 初次响应 CMIT:0001309

Dell Customer Communication - Confidential

Hi Liang
目前我们考虑跟客户进一步了解和获取信息，你看是否方便电话联系沟通，谢谢!

Lianbin_Que
CTE, Great China Client Technical Support
Pro Support | Pro Support Plus
office +86-592-818-8753

发件人: Que, Lianbin
发送时间: 2020 年 7 月 20 日 9:03
收件人: 'Wei Liang'
抄送: Wang, Wade; Sun Zhenning; Hong, Tony; Li, Lisa(TSM); CRM Case Email; Liu Jian
主题: 回复: [案例号: CAS-02606-V9R5J2] % |普通事件| Dell | 多台 OPTI 7070 新机发生账户锁定情况 % 初次响应 CMIT:0001309

Dell Customer Communication - Confidential

Hi Liang
目前客户反馈的信息如下，今天预计有 DELL 工程师上门，是否还需要进一步确定信息或直接联系沟通，谢谢

1．iNode 配置与本地帐户用户名和密码的关联情况：

1） iNode 客户端是否需要配置本机的用户名和密码？不需要。

2）本地帐户修改密码后，iNode 是否也需要同步修改配置帐户密码？不需要

2．第一次开箱配置以及 iNode 是否能在不联网的状态下配置？使用 iNode 认证需要内部网络环境，iNode 账号在公司的 LDAP 上。

3．确认 iNode 配置策略中的安全配置有没有与用户登录相关的配置？请再解释下问题本身，我怕理解有误。

4．在确定 iNode 配置完成并重启后系统用户正常使用，如果再次出现帐户锁定问题，能否配合收集对应的系统日志、安全日志等。可以。

5．是否有条件不通过 iNode 进行后台软件推送或补丁更新？iNode 并不负责打补丁，它只是将补丁服务器的地址写到用户主机的注册表中，并检测用户是不是按要求安装了最新的补丁，这是 iNode 的主要工作，也是我们使用该软件的初衷。

Lianbin_Que
CTE, Great China Client Technical Support
Pro Support | Pro Support Plus
office +86-592-818-8753

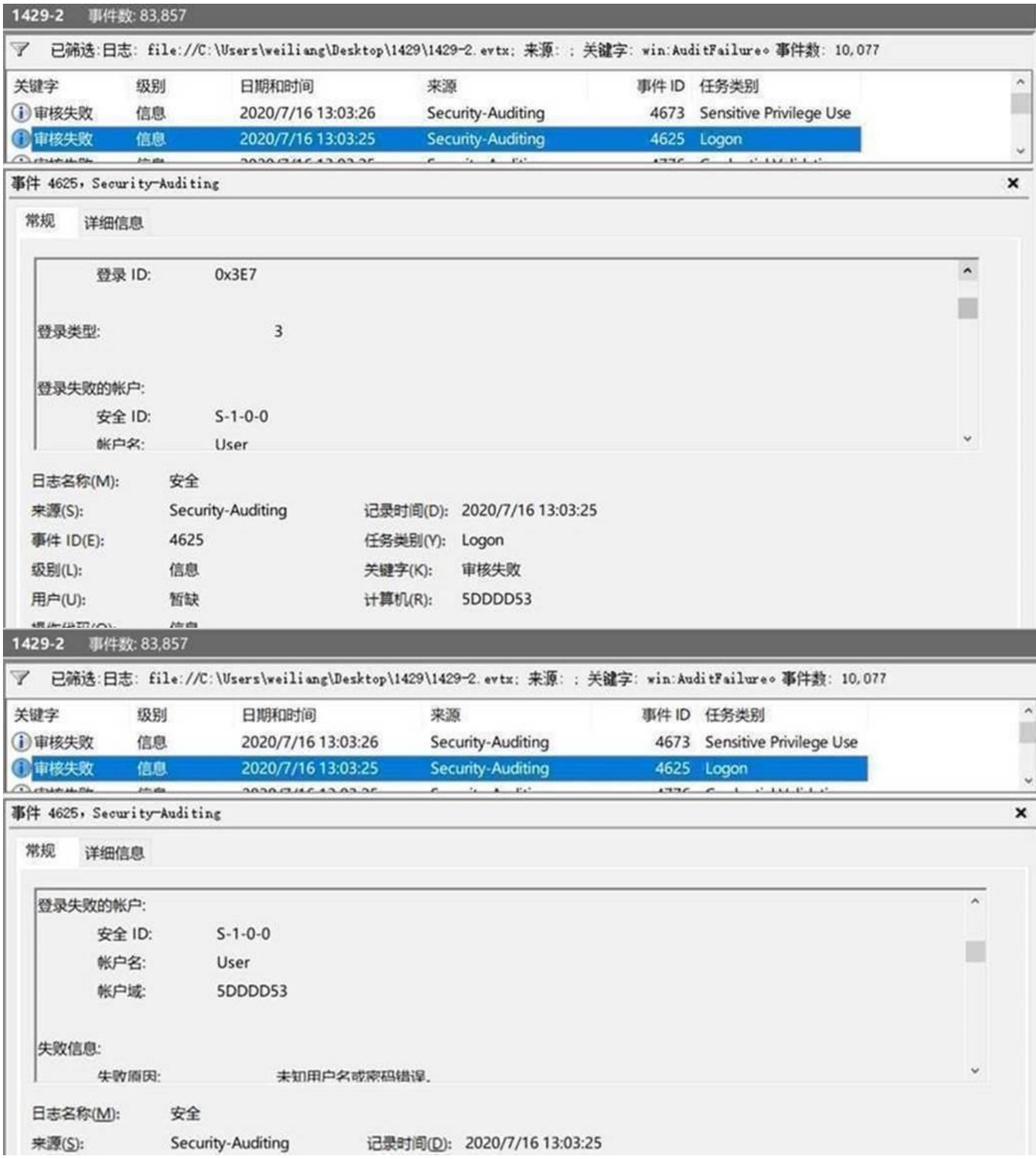
发件人: Wei Liang <weiliang@cmgos.com>
发送时间: 2020 年 7 月 17 日 16:27
收件人: Que, Lianbin
抄送: Wang, Wade; Sun Zhenning; Hong, Tony; Li, Lisa(TSM); CRM Case Email; Liu Jian
主题: 回复: [案例号: CAS-02606-V9R5J2] % |普通事件| Dell | 多台 OPTI 7070 新机发生账户锁定情况 % 初次响应 CMIT:0001309

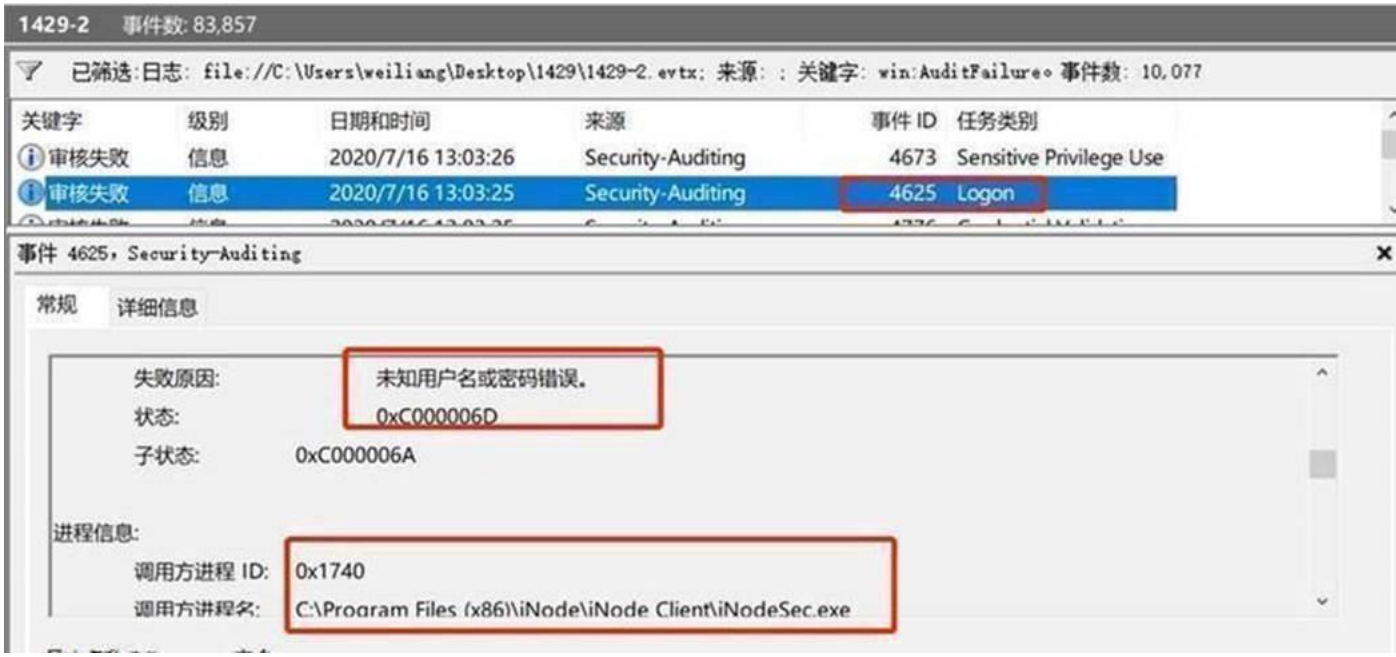
[EXTERNAL EMAIL]

Hi Lianbin :

如刚才电话沟通，我谨在此阐述问题涉及的范围定义:
问题定义：多台新机的定制系统在登录后，发生账户异常锁定情况
问题范围：协助用户分析上述问题。
如您对以上问题范围定义有任何疑问请直接与我联系。

问题分析:
通过您发送过来的系统日志，可以看到 inode 从 13:02:41 一直到 13:03:25 一直是在使用 user 用户名远程登录失败，有大量的登录失败日志:


1429-2 事件数: 83,857
已筛选:日志: file://C:\Users\weiliang\Desktop\1429\1429-2.evtx; 来源: ; 关键字: win:AuditFailure。事件数: 10,077
关键字 级别 日期和时间 来源 事件 ID 任务类别
审核失败 信息 2020/7/16 13:03:26 Security-Auditing 4673 Sensitive Privilege Use
审核失败 信息 2020/7/16 13:03:25 Security-Auditing 4625 Logon
事件 4625，Security-Auditing
常规 详细信息
登录 ID: 0x3E7
登录类型: 3
登录失败的帐户:
安全 ID: S-1-0-0
帐户名: User
日志名称(M): 安全
来源(S): Security-Auditing 记录时间(D): 2020/7/16 13:03:25
事件 ID(E): 4625 任务类别(Y): Logon
级别(L): 信息 关键字(K): 审核失败
用户(U): 暂缺 计算机(R): 5DDDD53
1429-2 事件数: 83,857
已筛选:日志: file://C:\Users\weiliang\Desktop\1429\1429-2.evtx; 来源: ; 关键字: win:AuditFailure。事件数: 10,077
关键字 级别 日期和时间 来源 事件 ID 任务类别
审核失败 信息 2020/7/16 13:03:26 Security-Auditing 4673 Sensitive Privilege Use
审核失败 信息 2020/7/16 13:03:25 Security-Auditing 4625 Logon
事件 4625，Security-Auditing
常规 详细信息
登录失败的帐户:
安全 ID: S-1-0-0
帐户名: User
帐户域: 5DDDD53
失败信息:
失败原因: 未知用户名或密码错误。
日志名称(M): 安全
来源(S): Security-Auditing 记录时间(D): 2020/7/16 13:03:25



这应该是开箱第一次登录重置 User 用户名密码后会出现的，这需要了解用户的定制项关于 iNode 客户端的配置，iNode 客户端需要配置本机的用户名和密码吗?
iNode 配置策略中的安全配置有做哪些配置与用户登录有关?
系统日志中显示在做系统更新后，重启计算机再次登录后，就显示帐户锁定。但是在审核日志中没有发现有其他使用帐户登录的行为。

为了排查是否是由于第一次更改密码后 iNode 频繁、大量的登录错误行为造成的用户锁定情况，确认 iNode 配置与本地帐户用户名和密码的关联情况，本地帐户修改密码后，iNode 那边是不是也需要同步修改配置帐户密码?
第一次开箱配置以及配置 iNode 能不能在不联网状态下配置?
确认 iNode 配置策略中的安全配置有没有与用户登录相关的配置?
开箱重置了 User 密码并配置成功 iNode 客户端后，直接重启，确认 iNode 以及系统一切正常后，先在组策略中查询密码锁定策略，再尝试更新系统补丁，观察是否有帐户锁定的问题?

在确定 iNode 配置完成并重启后系统用户正常使用，如果再次出现帐户锁定问题，此时再收集查看对应的系统日志、安全日志等。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

神州网信
CMIT

发件人: Hong, Tony <Tony.Hong@dell.com>
发送时间: 2020 年 7 月 17 日 15:18
收件人: Li, Lisa(TSM) <Lisa.Li@Dell.com>; Que, Lianbin <Lianbin.Que@dell.com>; Wei Liang <weiliang@cmgos.com>; Sun Zhenning <sunzn@cmgos.com>
抄送: Wang, Wade <Wade.Wang1@Dell.com>
主题: 回复: [案例号: CAS-02606-V9R5J2] % |普通事件| Dell | 多台 OPTI 7070 新机发生账户锁定情况 % 初次响应 CMIT:0001309

Hi, Weiliang

您好！ 如咱们刚才所沟通，麻烦您将分析日志的发现（包含截图）及后续操作建议发给我们参考，
如有需要获取更多信息，也请一并告知，以便我们和客户沟通。

如能在下午 15:30 前发出则最好。多谢!

Tony Hong
洪育鹞
Resolution Manager, Support Resolution Team
Dell Technologies | DT Services
Office +86-592-818-6208

发件人: Li, Lisa(TSM) <Lisa_Li10@Dell.com>
发送时间: 2020 年 7 月 17 日 11:51
收件人: Que, Lianbin; Wei Liang; sunzn@cmgos.com
抄送: Hong, Tony; Wang, Wade
主题: RE: [案例号: CAS-02606-V9R5J2] % |普通事件| Dell | 多台 OPTI 7070 新机发生账户锁定情况 % 初次响应 CMIT:0001309

Loop 震宁

Best Regards,
Lisa

From: Que, Lianbin <lianbin_que@Dell.com>
Sent: 2020 年 7 月 17 日 9:48
To: Wei Liang

Cc: Hong, Tony; Wang, Wade; Li, Lisa(TSM)
Subject: 回复: [案例号: CAS-02606-V9R5J2] % |普通事件| Dell | 多台 OPTI 7070 新机发生账户锁定情况 % 初次响应 CMIT:0001309

Dell Customer Communication - Confidential

Hi Liang
此 case 有比较大的 risk，也比较紧急，请帮忙优先看下，谢谢!
我同时负责此案子的几个同事，有情况请帮忙一起 loop 这些同事，谢谢!

Lianbin_Que
CTE, Great China Client Technical Support
Pro Support | Pro Support Plus
office +86-592-818-8753

发件人: Wei Liang <weiliang@cmgos.com>
发送时间: 2020 年 7 月 17 日 9:41
收件人: Que, Lianbin
抄送: Wei Liang
主题: [案例号: CAS-02606-V9R5J2] % |普通事件| Dell | 多台 OPTI 7070 新机发生账户锁定情况 % 初次响应 CMIT:0001309

[EXTERNAL EMAIL]

Lianbin.Que 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-02606-V9R5J2 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**”。