

Lianbin.Que 先生, 您好:

感谢您的回复, 经您的同意, 由于目前用户暂不需要提供后续支持工作, 此 case 将暂做关闭处理, 以下为案例总结, 请您知悉:

Case No: CAS-02920-F4R0M4

问题描述:

=====

用户反馈多台电脑在加域后开机时都会出现开机慢的问题。

问题分析:

=====

经过对用户收取日志的初步分析, 可以看到在系统登录过程中, LogonUI 不停在尝试读取 HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers 的键值, 怀疑是因为权限问题 (此操作需要 system 账户权限), 无法完成此操作, 提示“NO MORE ENTRIES”。因此导致登录时间过长。基于上述描述, 初步怀疑与系统在登录过程中第三方软件需要调用 U 盾类安全识别软件有关, 请在用户现场着重排查此类软件。具体排查思路可参见之前邮件。

问题总结:

=====

经用户确认, 认可当前分析结论, 不需要后续支持, case 将暂做关闭处理。

以上, 如您后续有任何问题, 可随时与我们联系, 谢谢。

李琦 Li Qi

神州网信技术有限公司

C&M Information Technologies Co., Ltd.

服务电话: 4008180055

电子邮箱 Email: liqi@cmgos.com



发件人: Que, Lianbin <Lianbin.Que@dell.com>

发送时间: 2020 年 9 月 17 日 16:21

收件人: Li Qi <liqi@cmgos.com>; 307654849@qq.com

抄送: CRM Case Email <casemail@cmgos.com>; Liu Jian <liujian@cmgos.com>; Hua, Vincent <Vincent.Hua@dell.com>; Wei, Laob <Laob.Wei@dell.com>; Hu, Bill <Bill.Hu@dell.com>; Wang, Wade <Wade.Wang1@Dell.com>

主题: 回复: 回复: [案例号: CAS-02920-F4R0M4] % |普通事件|Dell|多台机器加域后开机变慢的问题 % 初次响应 CMIT:0001998

Hi Qi

客户对于能找到问题原因表示认可和感谢!

客户表示进一步的排查方案暂时无需进一步操作了, 可以先结案, 谢谢!

Lianbin_Que

CTE, Great China Client Technical Support

Pro Support | Pro Support Plus

office +86-592-818-8753

发件人: Li Qi <liqi@cmgos.com>

发送时间: 2020 年 9 月 16 日 14:23

收件人: Que, Lianbin; 307654849@qq.com

抄送: CRM Case Email; Liu Jian; Hua, Vincent; Wei, Laob; Hu, Bill; Wang, Wade

主题: 回复: 回复: [案例号: CAS-02920-F4R0M4] % |普通事件|Dell|多台机器加域后开机变慢的问题 % 初次响应 CMIT:0001998

[EXTERNAL EMAIL]

Lianbin.Que 先生, 您好:

如上午电话沟通, 经过对用户收取日志的初步分析, 可以看到在系统登录过程中, LogonUI 不停在尝试读取 HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers 的键值, 怀疑是因为权限问题(此操作需要 system 账户权限), 无法完成此操作, 提示“NO MORE ENTRIES”。因此导致登录时间过长。以下为相关日志信息:

用户终端日志:

9/21/21, 2258996	svchost.exe	3296	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000031
9/21/21, 2259155	svchost.exe	3296	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	NO MORE ENTRIES	Index: 0. Lengt...	0.000017
9/21/21, 2259234	svchost.exe	3296	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000010
9/21/21, 2259155	LogonUI.exe	1332	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000048
9/21/21, 2259158	LogonUI.exe	1332	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	NO MORE ENTRIES	Index: 0. Lengt...	0.000021
9/21/21, 2259187	LogonUI.exe	1332	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000011
9/21/21, 2259098	svchost.exe	3296	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000034
9/21/21, 2259258	svchost.exe	3296	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	NO MORE ENTRIES	Index: 0. Lengt...	0.000021
9/21/21, 2259637	svchost.exe	3296	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000007
9/21/21, 2302078	LogonUI.exe	1332	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000034
9/21/21, 2302180	LogonUI.exe	1332	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	NO MORE ENTRIES	Index: 0. Lengt...	0.000017
9/21/21, 2302269	LogonUI.exe	1332	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000010
9/21/21, 2303498	svchost.exe	3296	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000031
9/21/21, 2303872	svchost.exe	3296	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	NO MORE ENTRIES	Index: 0. Lengt...	0.000020
9/21/21, 2303754	svchost.exe	3296	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000007
9/21/21, 2308280	LogonUI.exe	1332	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000044
9/21/21, 2308406	LogonUI.exe	1332	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	NO MORE ENTRIES	Index: 0. Lengt...	0.000014
9/21/21, 2308493	LogonUI.exe	1332	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000010
9/21/21, 2309256	svchost.exe	3296	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000031
9/21/21, 2309420	svchost.exe	3296	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	NO MORE ENTRIES	Index: 0. Lengt...	0.000020
9/21/21, 2309502	svchost.exe	3296	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000010
9/21/21, 2313912	svchost.exe	3296	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000027
9/21/21, 2314069	svchost.exe	3296	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	NO MORE ENTRIES	Index: 0. Lengt...	0.000017
9/21/21, 2314147	svchost.exe	3296	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000007
9/21/21, 2314496	LogonUI.exe	1332	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000047
9/21/21, 2314649	LogonUI.exe	1332	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	NO MORE ENTRIES	Index: 0. Lengt...	0.000024
9/21/21, 2314755	LogonUI.exe	1332	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000010
9/21/21, 2318520	svchost.exe	3296	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000031
9/21/21, 2318994	svchost.exe	3296	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	NO MORE ENTRIES	Index: 0. Lengt...	0.000021
9/21/21, 2319080	svchost.exe	3296	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000013
9/21/21, 2320513	LogonUI.exe	1332	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000038
9/21/21, 2320823	LogonUI.exe	1332	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	NO MORE ENTRIES	Index: 0. Lengt...	0.000023
9/21/21, 2320715	LogonUI.exe	1332	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000010
9/21/21, 2323773	svchost.exe	3296	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000031
9/21/21, 2323930	svchost.exe	3296	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	NO MORE ENTRIES	Index: 0. Lengt...	0.000017
9/21/21, 2324003	svchost.exe	3296	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000007
9/21/21, 2327422	LogonUI.exe	1332	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	NO MORE ENTRIES	Index: 0. Lengt...	0.000027
9/21/21, 2327533	LogonUI.exe	1332	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	NO MORE ENTRIES	Index: 0. Lengt...	0.000023
9/21/21, 2327678	svchost.exe	3296	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000010
9/21/21, 2328599	svchost.exe	3296	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000028
9/21/21, 2328750	svchost.exe	3296	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	NO MORE ENTRIES	Index: 0. Lengt...	0.000017
9/21/21, 2328823	svchost.exe	3296	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000010
9/21/21, 2334013	LogonUI.exe	1332	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000036
9/21/21, 2334047	svchost.exe	3296	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000055
9/21/21, 2334100	LogonUI.exe	1332	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	NO MORE ENTRIES	Index: 0. Lengt...	0.000027
9/21/21, 2334245	LogonUI.exe	1332	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000010
9/21/21, 2334259	svchost.exe	3296	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	NO MORE ENTRIES	Index: 0. Lengt...	0.000020
9/21/21, 2334344	svchost.exe	3296	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000010
9/21/21, 2339184	svchost.exe	3296	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000031
9/21/21, 2339341	svchost.exe	3296	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	NO MORE ENTRIES	Index: 0. Lengt...	0.000021
9/21/21, 2339430	svchost.exe	3296	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000007
9/21/21, 2339689	LogonUI.exe	1332	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000045
9/21/21, 2339805	svchost.exe	1332	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	NO MORE ENTRIES	Index: 0. Lengt...	0.000024
9/21/21, 2339884	LogonUI.exe	1332	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\Calais\Readers	SUCCESS	Desired Access:...	0.000010

操作权限：

PID: 1332 Architecture: 64-bit
Parent PID: 1020 Virtualized: False
Session ID: 1 Integrity: System
User: NT AUTHORITY\SYSTEM
Auth ID: 00000000.00000000
Started: 2020/9/11 9:20:06 Ended: 2020/9/11 9:22:08

Call stack:

Event	Process	Stack
Frame	Module	Location
K 0	ntoskrnl.exe	ntoskrnl.exe + 0x5a6dad 0x7fff
K 1	ntoskrnl.exe	ntoskrnl.exe + 0x4ac491 0x7fff
K 2	ntoskrnl.exe	ntoskrnl.exe + 0x1bb143 0x7fff
U 3	stdll.dll	RtlCaptureStackContext + 0x11d4 0x7fff
U 4	KernelBase.dll	KernelBase.dll + 0x31b68 0x7fff
U 5	KernelBase.dll	KernelBase.dll + 0x2fda 0x7fff
U 6	WinSCard.dll	SCardWriteCacheW + 0x2e4e 0x7fff
U 7	WinSCard.dll	SCardWriteCacheW + 0x426d 0x7fff
U 8	WinSCard.dll	SCardWriteCacheW + 0x5335 0x7fff
U 9	WinSCard.dll	SCardAccess + 0x38a3 0x7fff
U 10	SmartcardCredentialProvider.dll	DllCanUnloadNow + 0x6a96f 0x7fff
U 11	SmartcardCredentialProvider.dll	DllCanUnloadNow + 0x6a679 0x7fff
U 12	kernel32.dll	MultiByteToWideChar + 0x4 0x7fff
U 13	stdll.dll	SetDefaultHardErrorPort + 0x1 0x7fff

Module Properties

Module: WinSCard.dll

Path: C:\Windows\System32\WinSCard.dll

Description: Microsoft 智能卡 API

Version: 10.0.17134.1 (WinBuild.160101.0800)

Company: Microsoft Corporation

Timestamp: 1971/8/27 10:05:44

Close Save...

Next Highlighted Copy All Close

正常登录终端日志：

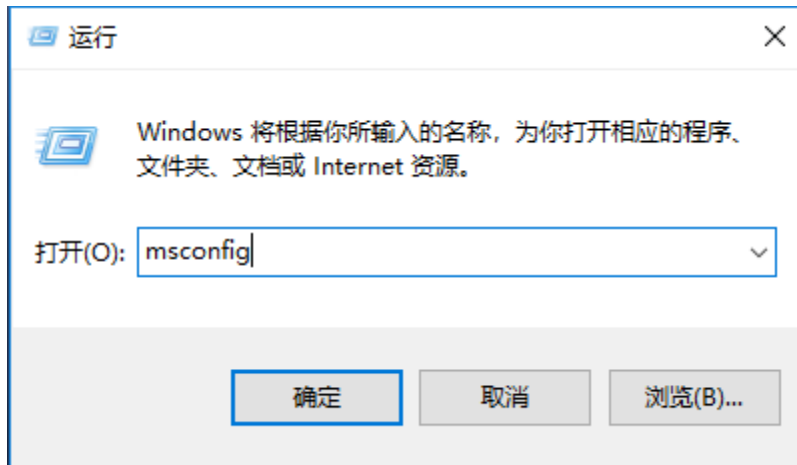
Tim...	Process Name	PID	Operation	Path	Result	Detail
10:5...	smss.exe	328	RegCreateKey	HKLM\SOFTWARE\Microsoft\Cryptography\Certs\Readers	SUCCESS	Desired Acces...
10:5...	smss.exe	328	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\Certs\Readers	SUCCESS	

基于上述描述，初步怀疑与系统在登录过程中第三方软件需要调用 U 盾类安全识别软件有关，请在用户现场着重排查此类软件。可根据实际现场环境选择尝试以下几种方式：

- 1，了解用户终端是否安装此类软件，并收集名称，版本等信息。
- 2，使用 clean boot 方法登录，看是否问题复现

以下为进入 clean boot 的方法：

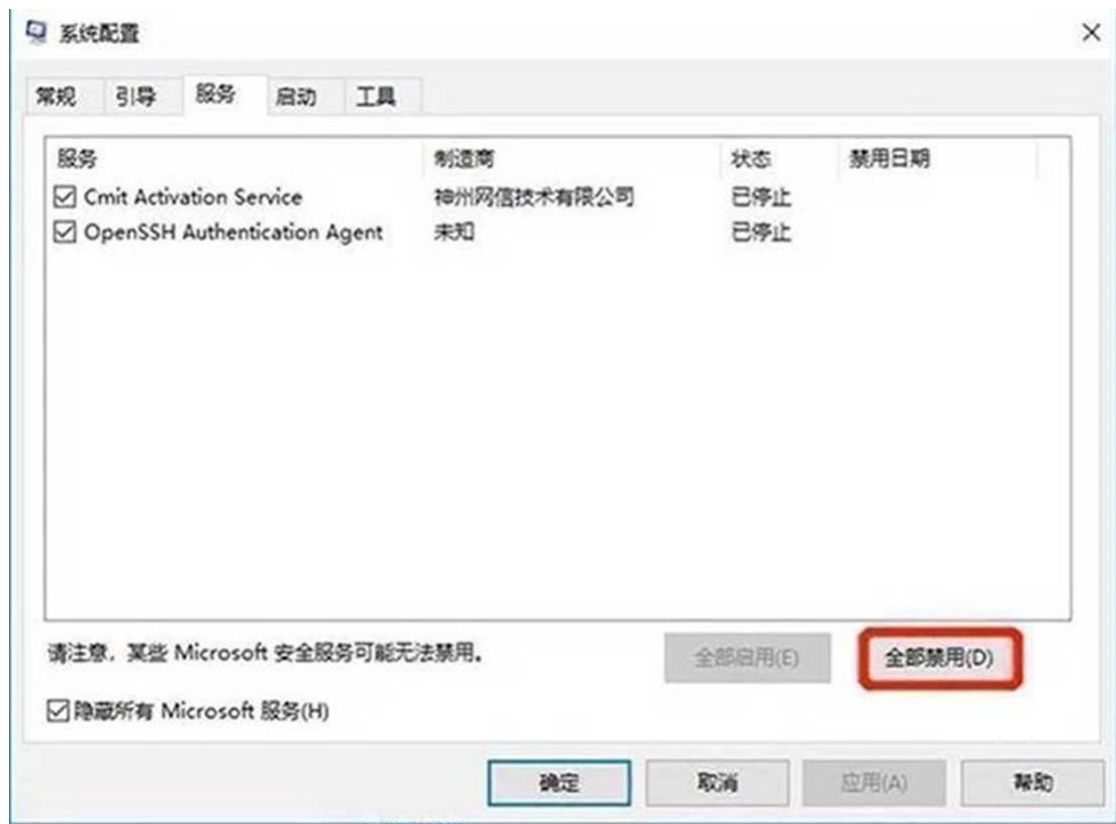
- 在运行栏内输入 msconfig，调出系统配置，在“常规”下选择“有选择的启动”，勾选加载系统服务和加载启动项
- 在“服务”选项下，勾选“隐藏所有 Microsoft 服务”，再点击“全部禁用”-确定，重启进入 Clean boot
- 步骤操作：
- 在运行栏内输入 msconfig，调出系统配置



- 在“常规”选项下选择“有选择的启动”，勾选加载系统服务和加载启动项



- 在“服务”选项下，勾选“隐藏所有 Microsoft 服务”，再点击“全部禁用”-确定



- 重启进入 Clean boot

- 3, 检查用户终端驱动是否安装最新, 卸载 U 盾类第三方软件后查看是否问题复现。
- 4, 使用测试电脑仅安装入域必备软件后 (如 TMS), 成功入域, 看是否问题复现。如未复现问题, 再逐步安装 DSP, 亚信, 趋势等安控软件及用户所需的第三方软件, 进一步 narrow down 问题。

接下来, 我会进一步排查收集日志, 如有新的发现, 我会第一时间和您更新, 另外, 如果方便的话, 请联系用户使用 Enable Boot Logging 的方法收集用户未入域状态的登录 procmon 日志, 用于对比分析。

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co., Ltd.
服务电话: 4008180055
电子邮箱 Email: liqi@cmgos.com



发件人: Que, Lianbin <Lianbin.Que@dell.com>

发送时间: 2020 年 9 月 16 日 9:38

收件人: Li Qi <liqi@cmgos.com>; 307654849@qq.com

抄送: CRM Case Email <casemail@cmgos.com>; Liu Jian <liujian@cmgos.com>; Hua, Vincent <Vincent.Hua@dell.com>; Wei, Laob <Laob.Wei@dell.com>; Hu, Bill <Bill.Hu@dell.com>; Wang, Wade <Wade.Wang1@Dell.com>

主题: 回复: 回复: [案例号: CAS-02920-F4R0M4] % |普通事件|Dell|多台机器加域后开机变慢的问题 % 初次响应 CMIT:0001998

Dell Customer Communication - Confidential

Hi Qi

收集的信息比较大, 有 176MB, 无法直接邮件发送.

尝试上传之前你同事给的链接一直提示错误, 你看是否可以从腾讯微云上下来帮分析, 谢谢!

文件链接: <https://share.weiyun.com/VfbZjVMF>



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 9 月 15 日 12:50

收件人: Li Qi; 307654849@qq.com

抄送: CRM Case Email; Liu Jian; Hua, Vincent; Wei, Laob; Hu, Bill; Wang, Wade

主题: 回复: 回复: [案例号: CAS-02920-F4R0M4] % |普通事件|Dell|多台机器加域后开机变慢的问题 % 初次响应 CMIT:0001998

Dell Customer Communication - Confidential

Hi Qi

我们还在获取信息确定, 确定收集好信息后发送你邮箱, 谢谢!

Lianbin_Que

CTE, Great China Client Technical Support

发件人: Li Qi <liqi@cmgos.com>
发送时间: 2020 年 9 月 15 日 11:31
收件人: Que, Lianbin; 307654849@qq.com
抄送: CRM Case Email; Liu Jian; Hua, Vincent; Wei, Laob; Hu, Bill; Wang, Wade
主题: 回复: 回复: [案例号: CAS-02920-F4R0M4] % |普通事件|Dell|多台机器加域后开机变慢的问题 % 初次响应 CMIT:0001998

[EXTERNAL EMAIL]

Lianbin.Que 先生, 您好:

循例问一下, 目前用户最近是否仍有此问题, 成功收集日志过程中是否出现问题, 盼复, 谢谢

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co., Ltd.
服务电话: 4008180055
电子邮箱 Email: liqi@cmgos.com



发件人: Que, Lianbin <Lianbin.Que@dell.com>
发送时间: 2020 年 9 月 9 日 16:22
收件人: Li Qi <liqi@cmgos.com>; 307654849@qq.com
抄送: CRM Case Email <casemail@cmgos.com>; Liu Jian <liujian@cmgos.com>; Hua, Vincent <Vincent.Hua@dell.com>; Wei, Laob <Laob.Wei@dell.com>; Hu, Bill <Bill.Hu@dell.com>; Wang, Wade <Wade.Wang1@Dell.com>
主题: 回复: 回复: [案例号: CAS-02920-F4R0M4] % |普通事件|Dell|多台机器加域后开机变慢的问题 % 初次响应 CMIT:0001998

Dell Customer Communication - Confidential

Hi Qi
好的, 感谢解答.

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

发件人: Li Qi <liqi@cmgos.com>
发送时间: 2020 年 9 月 9 日 16:18
收件人: Que, Lianbin; 307654849@qq.com
抄送: CRM Case Email; Liu Jian; Hua, Vincent; Wei, Laob; Hu, Bill; Wang, Wade
主题: 回复: 回复: [案例号: CAS-02920-F4R0M4] % |普通事件|Dell|多台机器加域后开机变慢的问题 % 初次响应 CMIT:0001998

[EXTERNAL EMAIL]

Hi:

不会的。Procmon 抓取的是开机阶段的程序运行过程，都是即时数据，停止捕获后就不再抓取了。CMGEDataCollector 是抓取用户现有的事件日志等信息。这两个工具在我们之前对工行的其他问题 debug 时也经常用到，没有安全问题，请放心使用，使用之后如有顾虑，直接删除即可，谢谢

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co., Ltd.
服务电话: 4008180055
电子邮箱 Email: liqi@cmgos.com



发件人: Que, Lianbin <Lianbin.Que@ dell.com>
发送时间: 2020 年 9 月 9 日 16:14
收件人: Li Qi <liqi@cmgos.com>; 307654849@qq.com
抄送: CRM Case Email <casemail@cmgos.com>; Liu Jian <liujian@cmgos.com>; Hua, Vincent <Vincent.Hua@ dell.com>; Wei, Laob <Laob.Wei@ dell.com>; Hu, Bill <Bill.Hu@ dell.com>; Wang, Wade <Wade.Wang1@ Dell.com>
主题: 回复: 回复: [案例号: CAS-02920-F4R0M4] % |普通事件|Dell|多台机器加域后开机变慢的问题 % 初次响应 CMIT:0001998

Dell Customer Communication - Confidential

Hi Qi

我理解是这 2 个附件是可以直接运行的程序，无需安装，后面收集完后直接删除即可？因 ICBC 有安全方面的要求，所以会在系统底层留下相关记录吗？有彻底删除的步骤吗？

Lianbin_Que

CTE, Great China Client Technical Support

Pro Support | Pro Support Plus

office +86-592-818-8753

发件人: Li Qi <liqi@cmgos.com>

发送时间: 2020 年 9 月 9 日 16:10

收件人: 307654849@qq.com; Que, Lianbin

抄送: CRM Case Email; Liu Jian

主题: 回复: 回复: [案例号: CAS-02920-F4R0M4] % |普通事件|Dell|多台机器加域后开机变慢的问题 % 初次响应 CMIT:0001998

[EXTERNAL EMAIL]

Hi

抱歉回复晚了, 可以的。用户收集完数据删除工具就可以了。工具本身应该不需要安装。

李琦 Li Qi

神州网信技术有限公司

C&M Information Technologies Co., Ltd.

服务电话: 4008180055

电子邮箱 Email: liqi@cmgos.com



神州网信
CMIT

发件人: 307654849@qq.com <307654849@qq.com>

发送时间: 2020 年 9 月 9 日 16:05

收件人: Li Qi <liqi@cmgos.com>; lianbin_que <lianbin_que@dell.com>

主题: 回复: [案例号: CAS-02920-F4R0M4] % |普通事件|Dell|多台机器加域后开机变慢的问题 % 初次响应 CMIT:0001998

Hi Qi

你提供的工具收集完信息后可以马上卸载吗?



307654849

邮箱 307654849@qq.com

签名由 网易邮箱大师 定制

在 2020 年 09 月 08 日 16:43, 307654849@qq.com 写道:

Hi Qi

客户愿意配合测试和收集信息，只是新 ICBC 银行限制
和安全性要求，收集完后工具是否可以卸载？



307654849

[邮箱 307654849@qq.com](mailto:307654849@qq.com)

签名由 网易邮箱大师 定制

在 2020 年 09 月 08 日 15:50, 307654849@qq.com 写道:

邮件收到，我这确定后回复，谢谢



307654849

[邮箱 307654849@qq.com](mailto:307654849@qq.com)

签名由 网易邮箱大师 定制

在
2
0
2
0
年
0
9
月
0
8

日

1

5

:

0

0

,

L

i

Q

i

写

道

:

L

i

a

n

b

i

n

.

Q

u

e

先

生

,

您

好

:

请

查

收

之

前

邮

件
内
容
，
谢
谢

李
琦
L
i
Q
i
神
州
网
信
技
术
有
限
公
司
C
&
M
I
n
f
o
r
m
a
t
i
o
n
T
e
c
h

n
o
l
o
g
i
e
s
C
o
.
,
L
t
d
.
服
务
电
话
:
4
0
0
0
8
1
8
0
0
5
5
电
子
邮
箱
E
m
a
i
l
:
1iq

liqi@cmgo.com



神州网信
CMIT

发件人：L i Q i 发送时间：2 0 2 0 年 9 月 8 日 1 1 : 0

6 收件人: L i a n b i n . Q u e < L i a n b i n : Q u e @ d e l ! : c o m > 抄送: C R

M
C
a
s
e
E
m
a
i
l
<
casemail@ccmpos.com
>
; L
i
u
J
i
a
n
<
liui

[i
a
n
@
c
m
g
o
s
:
c
o
m](mailto:ian@cmgos.com)
> 主题:
: 回复:
: [案例号:
:
C
A
S
-
0
2
9
2
0
-
F
4
R
0
M
4

] %

| 普通事件 |

D e | |

| 多台机器加域后开机变慢的问题

% 初次响应 C M | T : 0 0 0 1

9
9
8

L
i
a
n
b
i
n
.
Q
u
e

先生，
您好：
：

由于电话未联系到您，我谨在此阐述问题涉及

的范围定义：

问题定义：用户反馈多台电脑在加域后开机时都会出现开机慢的问题。

问题范围：

协助您分析并处理上述问题。

如果您对以上的问题范围界定有任何疑问，请尽快告知。如果您有其他

任何疑问，也欢迎随时与我联系。

基于此问题，请问多台电脑是否位于同一位置？使用
c
l
e
a
n
b

oot 是否问题依旧？

以下为进入cleanboot的方法：

- 在运行栏内输入msconfig，调

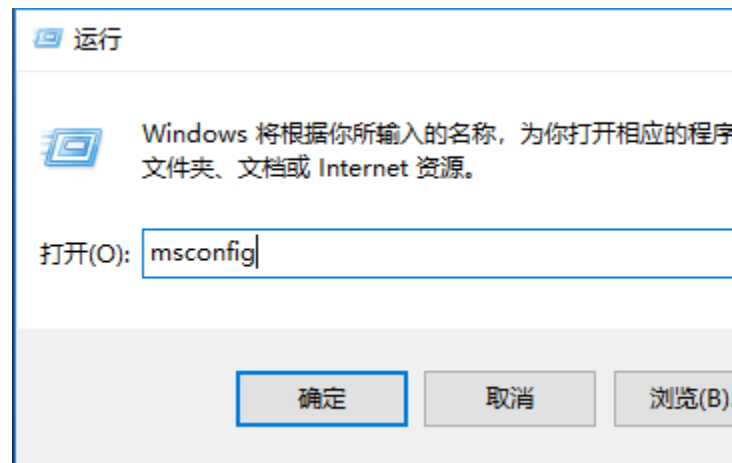
出系统配置，在“常规”下选择“有选择的启动”，勾选加载系统服务和加载启动项在“服务”选项下，勾

•

选
“ 隐藏所有 M i c r o s o f t 服务 ”
，再点击
“ 全部禁用 ”
- 确定
，重启进入 C l e a n b o o t

•

- 步骤操作：
- 在运行栏内输入 m s c o n f i g ，调出系统配置



- 在“常

规
” 选项下选择
“ 有选择的启动
”
, 勾选加载系统服务和加载启动项



- 在“服务”选项下，勾选“隐藏所有Microsoft

t
服务
”
，再
点
击
“
全
部
禁
用
”
-
确
定



- 重
启
进
入
C
I

e
a
n
b
o
o
t

如尝试上述方法后问题依旧，请帮忙收集附件工具日志，点击“收集”即可。

CMGE Log Collection Tool v1.01



神州网信CMGE日志收集工具

适用于：CMGE V0-G、V0-H、V2020-L

系统日志收集

- ☒ 系统信息 ☒ 组策略信息 ☒ 网络信息 ☒ 系统日志 [收集什么](#)
- ☒ 软件信息 ☒ 系统进程 ☒ 已安装补丁 ☐ 激活日志 ☐ 升级

收集

另外请运行附件procomn工具，收集开机登录过程日志。操作

步骤

1

)

双击

“

P

r

o

c

m

o

n

.

e

x

e

”

,

弹出

提权

窗口

点击

“

是

”

运行

P

r

o

c

e

s

s

M


o

n

i

t

or 工具。(首次运行会弹出 License Agreement 窗口，点击 Agree) ; 2) 进入

后出现
Proc Mon
窗口，此时已经处于时间捕获状态，点击
 停止捕获，再点击

清除当前

捕获的事件条目。至此准备工作完毕；
3) 点击“Option”
->“Enable Boot Log

g
i
n
g
”

，
之后
会
跳
出
窗
口

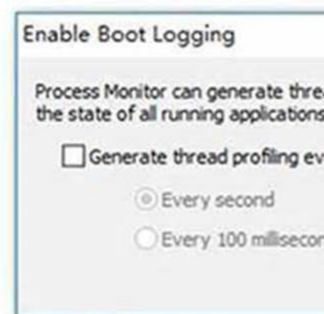
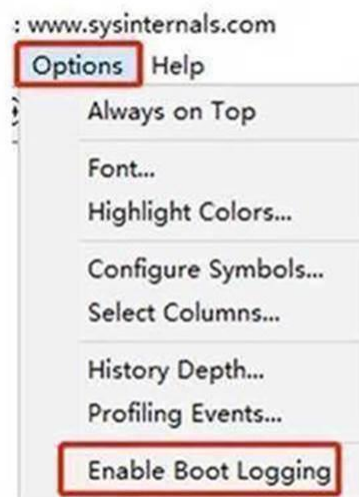
，
通常
情况
下
不
勾
选

，
直接
点
击
O
K

。之后
再
看
“

E
n
a
b
l
e
B
o
o
t

Logging” 已被勾选，证明开启成功；



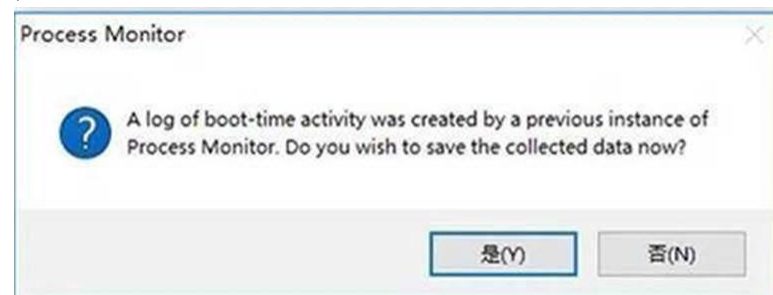
4) 此时直接重启或关机

，不用点击



开始捕获；5) 登陆进入桌面后，运行 p r o c m o n . e x e ，会弹出提示框询问是否

保存捕获的启动过程。
。 单击
“ 是
”
;

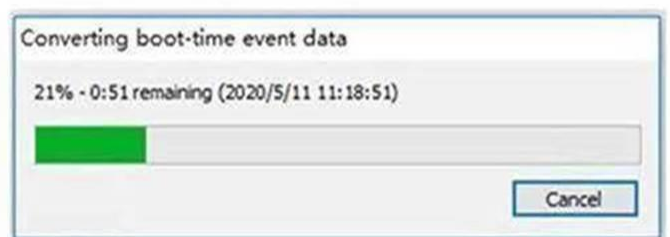


6
) 在
“ 另存为
” 窗口选择日志保存路径
, 单击

“
保存
”

，之后会有事件数据转换窗口出现。转换完毕后可以在你所指定的路径下找到日志文件；（日

志文件可能为多个，打开任意一个都可以浏览完整过程，务必全部收集)



李琦

L
i
Q
i
神州
网
信
技
术
有
限
公
司
C
&
M
I
n
f
o
r
m
a
t
i
o
n
T
e
c
h
n
o
l
o
g
i
e
s
C

O

.

,

L

t

d

.

服

务

电

话

:

4

0

0

8

1

8

0

0

5

5

电

子

邮

箱

E

m

a

i

l

:

[l](#)

[i](#)

[q](#)

[i](#)

[@](#)

[c](#)

[m](#)

[g](#)

[o](#)

[s](#)

[.](#)

[c](#)

[O
m](mailto:liqi@cmgoss.com)



神州网信
C M I T

发
件
人

:

L

i

Q

i

<

[l](mailto:liqi@cmgoss.com)

[i](mailto:liqi@cmgoss.com)

[q](mailto:liqi@cmgoss.com)

[i](mailto:liqi@cmgoss.com)

[@](mailto:liqi@cmgoss.com)

[c](mailto:liqi@cmgoss.com)

[m](mailto:liqi@cmgoss.com)

[g](mailto:liqi@cmgoss.com)

[o](mailto:liqi@cmgoss.com)

[s](mailto:liqi@cmgoss.com)

[:](mailto:liqi@cmgoss.com)

[c](mailto:liqi@cmgoss.com)

[o](mailto:liqi@cmgoss.com)

[m](mailto:liqi@cmgoss.com)

>

发

送

时

间

:

2

0

2

0

年

9

月
8
日
1
0
:
4
5
收件人:
L
i
a
n
b
i
n
.
Q
u
e
<
Liannbin@deili.co

[m](#)
> 抄送
:
L
i
Q
i
<
[!](#)
[i](#)
[g](#)
[i](#)
[@](#)
[c](#)
[m](#)
[g](#)
[o](#)
[s](#)
:
[c](#)
[o](#)
[m](#)
> 主题
:
[案例号
:

C
A
S
-
0
2
9
2
0

-
F
4
R
O
M
4

]
%

|
普
通
事
件

|
D
e

|
|

|
多
台
机
器
加
域
后
开
机
变
慢
的
问
题

%
初
次
响
应
C

M
I
T
:
0
0
0
1
9
9
8

L
i
a
n
b
i
n
.
Q
u
e

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

李
琦

。
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

C
A
S
-
0
2
9
2
0
-
F
4
R
O
M
4

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”

。