曹先生,您好!

案例总结：

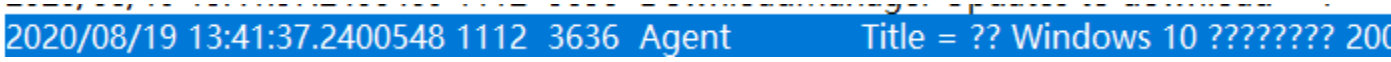
很高兴与您沟通，根据沟通的结果，我将暂时归档此问题。**案例归档后您会收到调查问卷的邮件，希望可以对我们的服务进行评价。**
工单的归档并不会影响我们为您提供技术支持服务，如果您的问题复现，或有新的问题出现，您也可以致电我们的技术支持热线 4008180055。

案例描述：
1）WindowsUpdate.log 乱码
2）Windows 更新时间间隔不为 22 小时
3）Windows 从非 CMGE 更新源下载更新

案例进展：
1）WindowsUpdate.log 乱码
使用 PowerShell 中 Get-WindowsUpdateLog 命令 在转换.etl 日志文件对 utf-8 字符集转换时，中文编码处理有误导致生成的日志文件中出现乱码。具体出现在 etl 日志文件转换 csv 文件时出现。

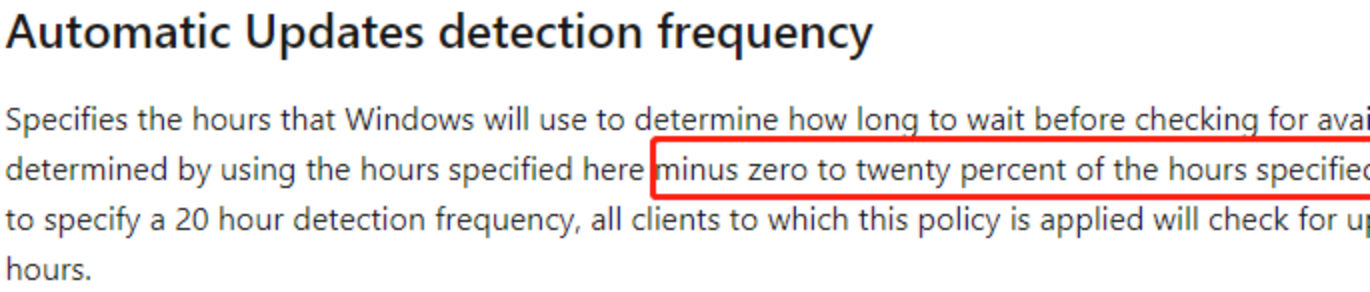
- 临时解决方案：此方法暂只能将中文乱码：靠转换为?。开始 -> 设置 -> 时间和语言 -> 语言 -> 管理语言设置 -> 管理页面 -> 更改系统区域设置 -> 勾选 Beta 版：使用 Unicode UTF-8 提供全球语言支持。

- 更改设置后重启计算机，收集 WindowsUpdate.log 里面的中文乱码消失。



2）Windows 更新时间间隔不为 22 小时

- 首先，组策略编辑器中，计算机配置 -> 管理模板 -> Windows 组件 -> Windows 更新 -> 自动更新检测频率。如果时“未配置”则默认检测间隔为 22 小时。但是关于间隔时间有一条重要的解释：准确的时间是由所指定时间的 0-20%所决定的。例如指定了检查频率是 20 小时，那么检查更新时间会在 16-20 小时之间，因为 20 x 20% = 4。如果是默认 22 小时，那么**检测时间就是在 22-(22 x 20%)=17.6 小时至 22 小时之间进行**。



- 对比发现 14:03 最后检查更新时间，按照规则，应该在第二天 7:39 - 12:03 之间扫描。WindowsUpdate.log 发现在第二天 10:02 确实进行了扫描行为，符合规则。
  但此次扫描却没有成功，经过对比查看 log，关键信息如下：

```
2020/08/13 10:02:06.9745658 11156 7376   ComApi                    * END
*     Federated Search failed to process service registration, hr=0x8024500C
(cV = oq2qbdxF+UWoaq3N.0.3.1.1.0)
```

报错代码 hr=0x8024500C 直接导致了扫描失败。针对此代码有分析文章指出：本地 WSUS 服务器想要推送 Windows 更新给客户端，而不是使用 Windowsupdate.microsoft.com
而以下的 solution 部分，也是关于关闭 Dual Scan 功能的操作。所以此次扫描失败也是由于 Dual Scan 的影响造成的。

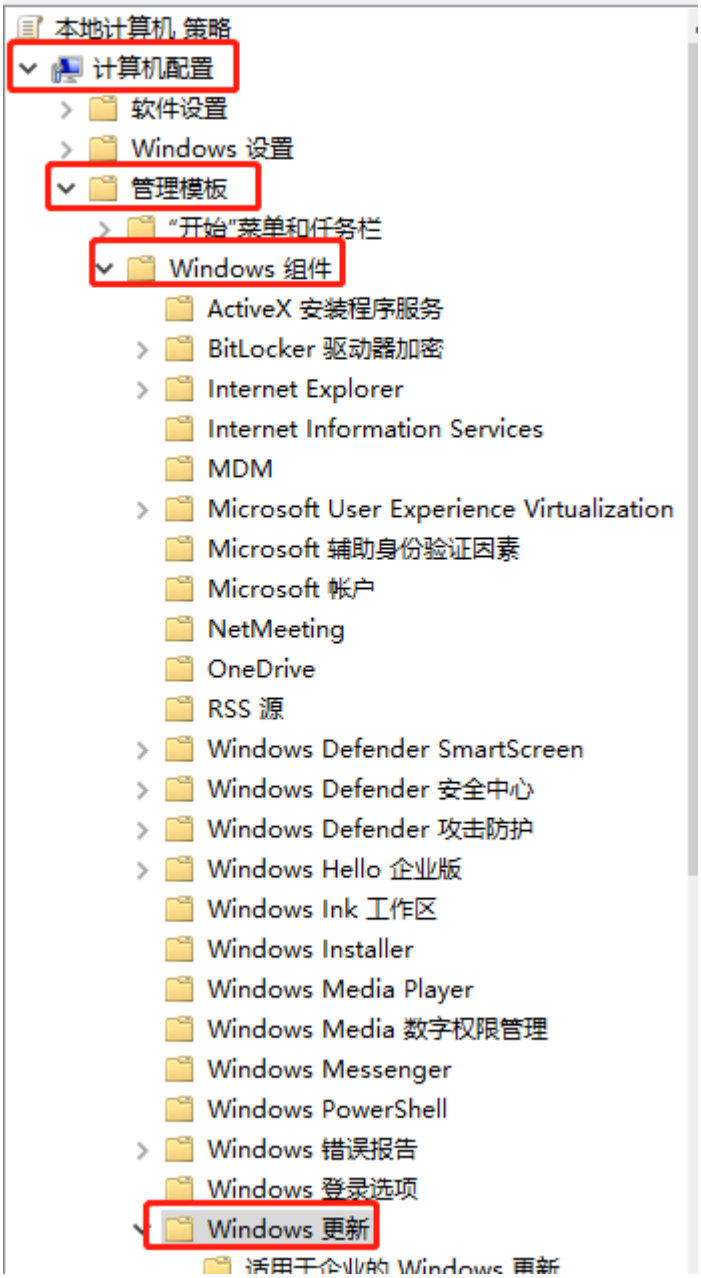
3）Windows 从非 CMGE 更新源下载更新
查看发现默认更新源变为 MS 的 Windows Update。

```
Name                  : DCat Flighting Prod
ContentValidationCert : {}
ExpirationDate        :
IsManaged             : False
IsRegisteredWithAU    : False
IssueDate             : 1601/1/1 0:00:00
OffersWindowsUpdates  : True
RedirectUrls          : System.__ComObject
ServiceID             : 8b24b027-1dee-babb-9a95-3517dfb9c552
IsScanPackageService  : False
CanRegisterWithAU     : False
ServiceUrl            : https://fe3.delivery.mp.microsoft.com/
SetupPrefix           : wu
IsDefaultAUService    : False

Name                  : Windows Store (DCat Prod)
ContentValidationCert : {}
ExpirationDate        :
IsManaged             : False
IsRegisteredWithAU    : False
IssueDate             : 1601/1/1 0:00:00
OffersWindowsUpdates  : False
RedirectUrls          : System.__ComObject
ServiceID             : 855e8a7c-ecb4-4ca3-b045-1dfa50104289
IsScanPackageService  : False
CanRegisterWithAU     : True
ServiceUrl            : https://fe3.delivery.mp.microsoft.com/
SetupPrefix           : ws
IsDefaultAUService    : False

Name                  : Windows Update
ContentValidationCert : {}
ExpirationDate        :
IsManaged             : False
IsRegisteredWithAU    : True
IssueDate             : 1601/1/1 0:00:00
OffersWindowsUpdates  : True
RedirectUrls          : System.__ComObject
ServiceID             : 9482f4b4-e343-43b6-b170-9a65bc822c77
IsScanPackageService  : False
CanRegisterWithAU     : True
ServiceUrl            : https://fe2.update.microsoft.com/v6/
SetupPrefix           : wu
IsDefaultAUService    : True
```

- 建议操作：

用如下组策略设置

启用“不要连接任何 Windows 更新 Internet 位置”
启用“配置自动更新”
启用“允许来自 Intranet Microsoft 更新服务位置的签名更新”



贾伟 Jia Wei
神州网信技术有限公司
服务电话： 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: 2020 年 8 月 19 日 17:45
收件人: Cao Yang <caoyang@cmgos.com>
抄送: CRM Case Email <casemail@cmgos.com>; Yin Xin <yinxin@cmgos.com>; Shi Guannan <shign@cmgos.com>
主题: 回复: [案例号: CAS-02786-P2R1R6] % WindowsUpdate 自动更新异常&Log 日志显示中文“靠” % 初次响应 CMIT:0001650

Hi Cao Yang,

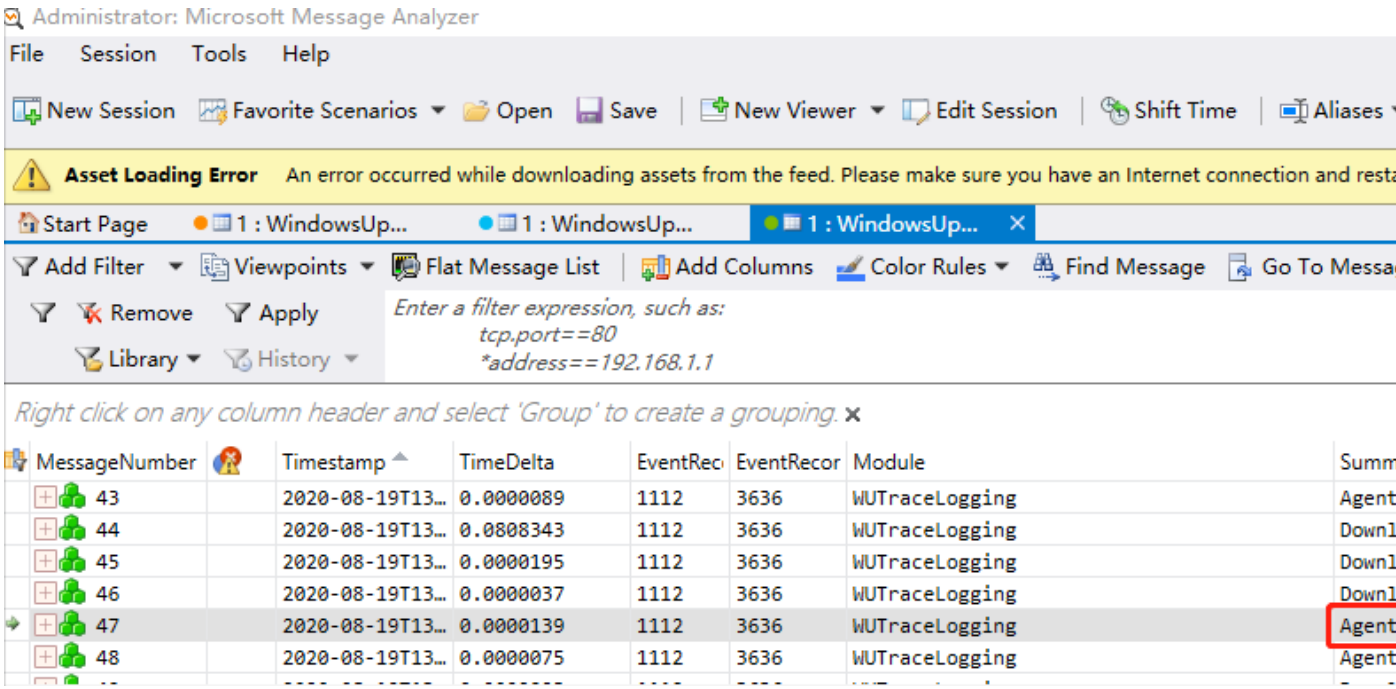
WindowsUpdate.log 乱码问题的具体解释：使用 PowerShell 中 Get-WindowsUpdateLog 命令 在转换.etl 日志文件对 utf-8 字符集转换时，中文编码处理有误导致生成的日志文件中出现乱码。

生成 Windowsupdate.log 过程

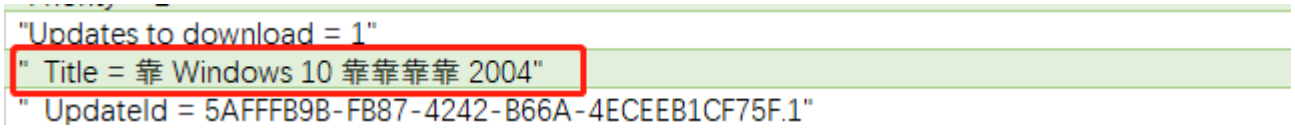
1）使用 C:\Users\User\AppData\Local\Temp\WindowsUpdateLog\tracerpt.exe，将 etl 文件，分别转换成若干 wuetl.CSV.tmp.00X

2）将若干 wuetl.CSV.tmp.00X 合并为 WindowsUpdate.log

首先使用 Microsoft Message Analyzer 查看 etl 文件，发现 etl 文件的 Windows Update Patch 名称正确。



再将 wuetl.CSV.tmp.00X 去后缀变成 wuetl.CSV 后，查看名称就出现乱码了



由此可见问题出现在 etl 文件转 CSV.temp 文件过程中。

贾伟 Jia Wei
神州网信技术有限公司
服务电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

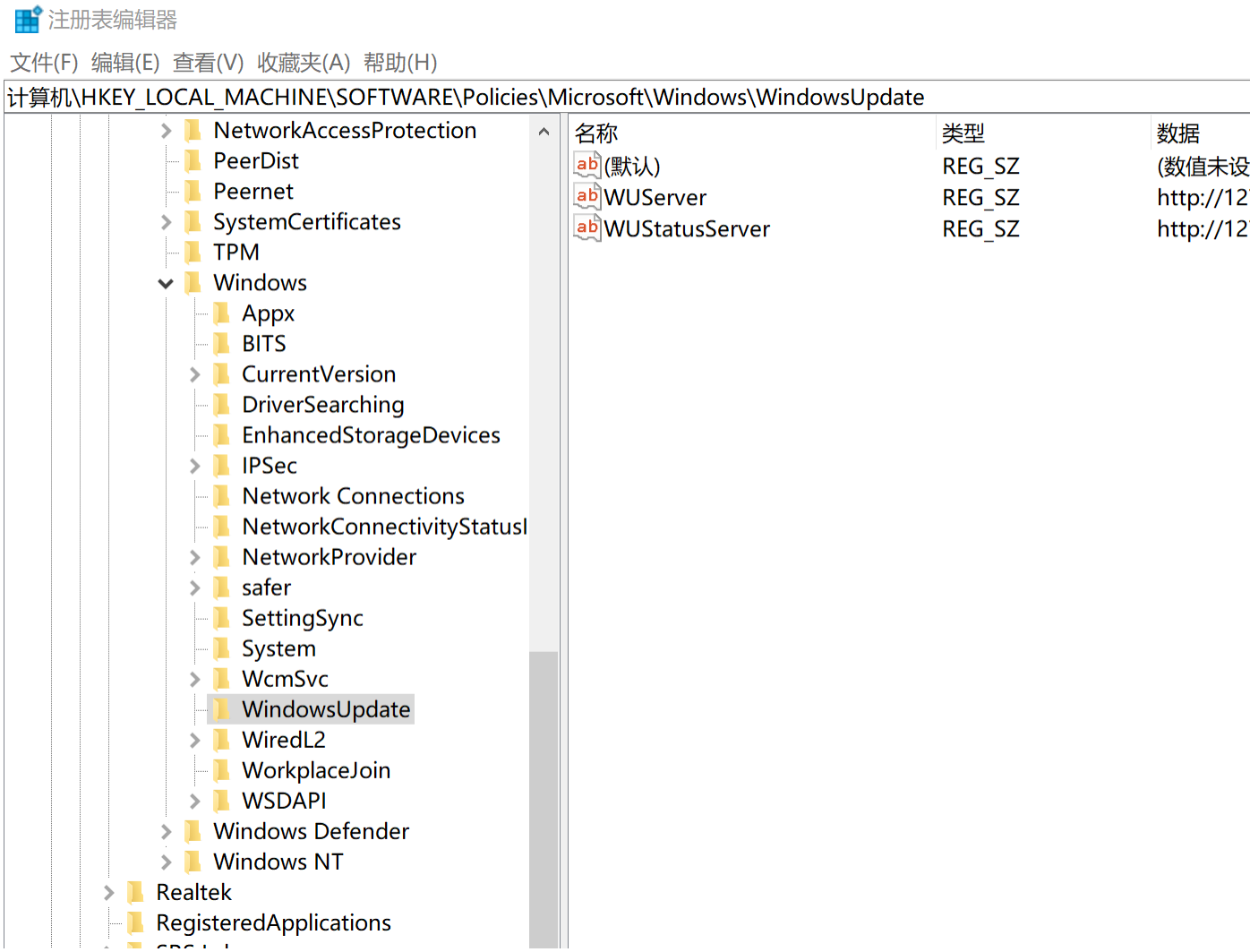
C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Cao Yang <caoyang@cmgos.com>
发送时间: 2020 年 8 月 19 日 13:53
收件人: Jia Wei <jiawei@cmgos.com>
抄送: CRM Case Email <casemail@cmgos.com>; Yin Xin <yinxin@cmgos.com>; Shi

Guannan <shign@cmgos.com>
主题: 回复: [案例号: CAS-02786-P2R1R6] % WindowsUpdate 自动更新异常&Log 日志显示中文“靠” % 初次响应 CMIT:0001650

我的机器只能到
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate，没有 AU

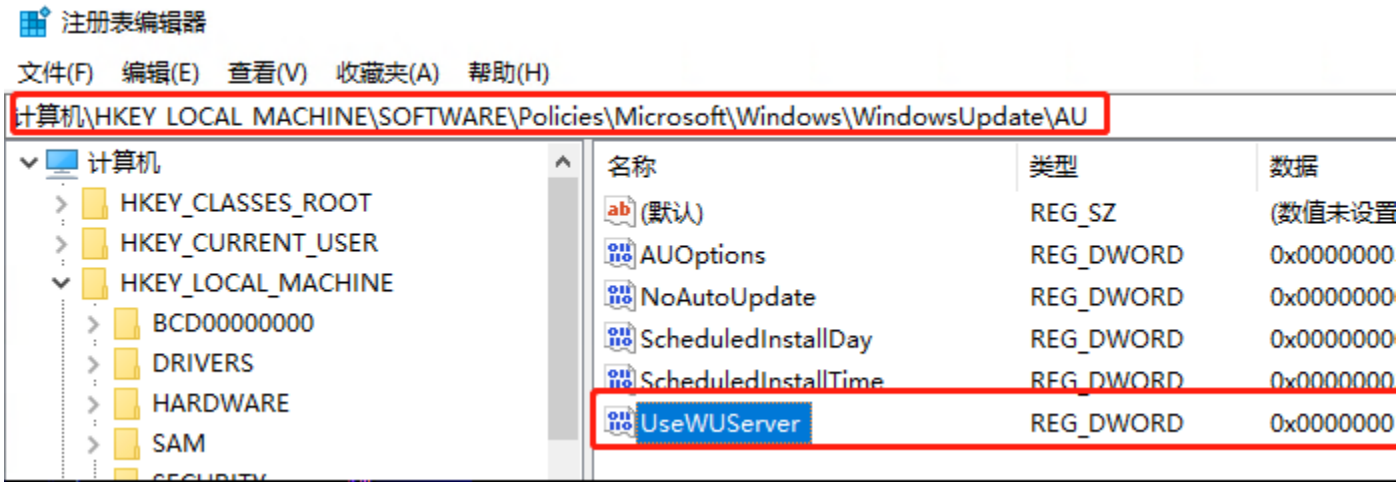
截图



发件人: Jia Wei <jiawei@cmgos.com>
发送时间: 2020 年 8 月 19 日 11:51
收件人: Cao Yang <caoyang@cmgos.com>
抄送: CRM Case Email <casemail@cmgos.com>; Yin Xin <yinxin@cmgos.com>; Shi Guannan <shign@cmgos.com>
主题: 回复: [案例号: CAS-02786-P2R1R6] % WindowsUpdate 自动更新异常&Log 日志显示中文“靠” % 初次响应 CMIT:0001650

Hi Cao Yang

- 查看一下 **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU，UseWUServer** 如果是 0，则从 WU 下载更新，可以设置为 1-禁用。这样可以将你的更新服务指回 WSUS。



- 另外，可以在虚拟机的 CMGE 上，使用附件的 2 种方式复现从 MS 下载更新的现象。

贾伟 Jia Wei
神州网信技术有限公司
服务电话： 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: Cao Yang <caoyang@cmgos.com>
发送时间: 2020 年 8 月 18 日 17:01
收件人: Jia Wei <jiawei@cmgos.com>

抄送: CRM Case Email <casemail@cmgos.com>; Yin Xin <yinxin@cmgos.com>; Shi Guannan <shign@cmgos.com>
主题: 回复: [案例号: CAS-02786-P2R1R6] % WindowsUpdate 自动更新异常&Log 日志显示中文“靠” % 初次响应 CMIT:0001650

测试了一下，虚拟机中单独把“不要连接任何 Windows 更新 Internet 位置”启用，更新未复现我现在这台机器的问题。

另外，Loop 上周把我机器接研发环境的 Guannan

发件人: Cao Yang
发送时间: 2020 年 8 月 17 日 15:01
收件人: Jia Wei <jiawei@cmgos.com>
抄送: CRM Case Email <casemail@cmgos.com>; Yin Xin <yinxin@cmgos.com>
主题: 回复: [案例号: CAS-02786-P2R1R6] % WindowsUpdate 自动更新异常&Log 日志显示中文“靠” % 初次响应 CMIT:0001650

再补充一个可能性，这台机器以前印象中没出现过 windows update 中更新驱动的事情，上周五出现更新驱动的事情后，今天才出现让更新 windows 1909。另外我本人也未手动操作过组策略的更改。所以组策略的异常应该不是很久之前就被改了的，应该就发生在近期。

一个线索:
这台机器上周和男哥一起连过研发的批量激活内网，开机状态下连的内网，测试了批量激活后就离开了，未做其他操作。组策略的异常会否和这个原因有关，烦请确认。

发件人: Cao Yang
发送时间: 2020 年 8 月 17 日 14:28
收件人: Jia Wei <jiawei@cmgos.com>
抄送: CRM Case Email <casemail@cmgos.com>; Yin Xin <yinxin@cmgos.com>
主题: 回复: [案例号: CAS-02786-P2R1R6] % WindowsUpdate 自动更新异常&Log 日志显示中文“靠” % 初次响应 CMIT:0001650

Hi 贾工:

问题有了新的变化，今日上午又出现了一个补丁更新后要求重启，我 get 了一个 update 的 log，然后进行了机器重启。

重启系统后，我的 V2020-L 现在再进行 windows update 更新检查，发现马上就要升级成 Windows1909 了。

截图请见附件。

发件人: Jia Wei <jiawei@cmgos.com>
发送时间: 2020 年 8 月 17 日 11:43
收件人: Cao Yang <caoyang@cmgos.com>
抄送: CRM Case Email <casemail@cmgos.com>
主题: 回复: [案例号: CAS-02786-P2R1R6] % WindowsUpdate 自动更新异常&Log 日志显示中文“靠” % 初次响应 CMIT:0001650

曹先生，您好!

问题定义：1）Windows 更新出现中文乱码，2）Windows 更新出现非 CMGE 推送的补丁，3）更新之间相隔非 22 小时问题

问题范围：协助您分析并处理上述问题。

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。

案例进展：

问题 1）Windows 更新出现乱码已经进行升级处理

问题 2）Windows 更新出现非 CMGE 推送的补丁，是由于从 Microsoft 下载更新所致

问题 3）更新之间相隔非 22 小时问题。但根据 Log 分析其中一次扫描是在 22 小时内，但未体现在 Windows 更新页面，具体原因正在研究。

案例分析：

问题 1）Windows 更新出现乱码问题

Download from Microsoft: ??x64 ?Windows 10 Version 1809 ?Microsoft .NET Framework 4.8 (KB4486153)
Windows 更新显示: 适用于 x64 位 Windows 10 Version 1809 的 Microsoft.Net Framework 4.8 (KB4486153)

Download from CMGE: 2020-靠?Windows 10 Version 1809 ?08 靠靠靠靠靠?x64 靠?(KB4566424)
Windows 更新显示: 2020-适用于 Windows 10 Version 1809 的 08 累积更新，适合基于 x64 的系统 (KB4566424)

- 对比发现 CMGE 下载的补丁会显示中文乱码和?，而从 Microsoft 下载的会显示??。
- 不论是乱码还是?，都应该对应的是 Windows 更新中的中文字符部分。此问题已经升级进行处理。

问题 2）Windows 更新出现非 CMGE 推送补丁

对比 gpresult 的结果，发现出问题的计算机只开启了“指定 Intranet Microsoft 更新服务位置”的组策略，缺少了 3 项组策略设置：

- 启用“不要连接任何 Windows 更新 Internet 位置”
- 启用“配置自动更新”
- 启用“允许来自 Intranet Microsoft 更新服务位置的签名更新”

其中：如果没有启用“**不要连接任何 Windows 更新 Internet 位置**”，会启用“Dual Scan”双扫描功能。
双扫描是 Microsoft 在 1607 版本之后开始引入的，默认是开启状态。双扫描设计用来为那些希望 Microsoft WU 作为首选更新源，而其他内容由企业内的 WSUS 提供的企业用户所设计的。

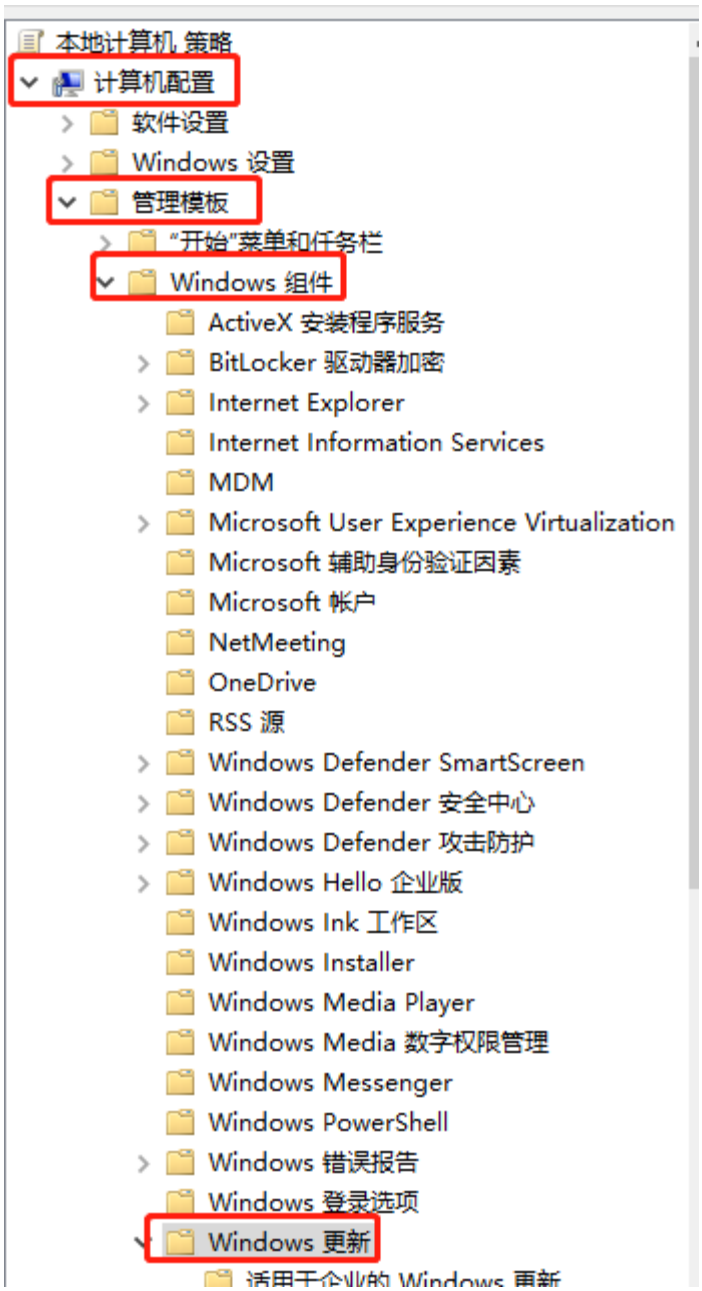
工作原理：客户端扫描 WSUS 和 WU，但只接受从 WU 扫描的结果。换句话说，任何 WUSU 中关于“Windows”家族的产品都会被忽略。

对比发现，CMGE 正常配置关闭了双扫描，只使用 WSUS 扫描更新，而问题计算机的默认扫描更新源仍为 WU（见日志对比）

建议操作:

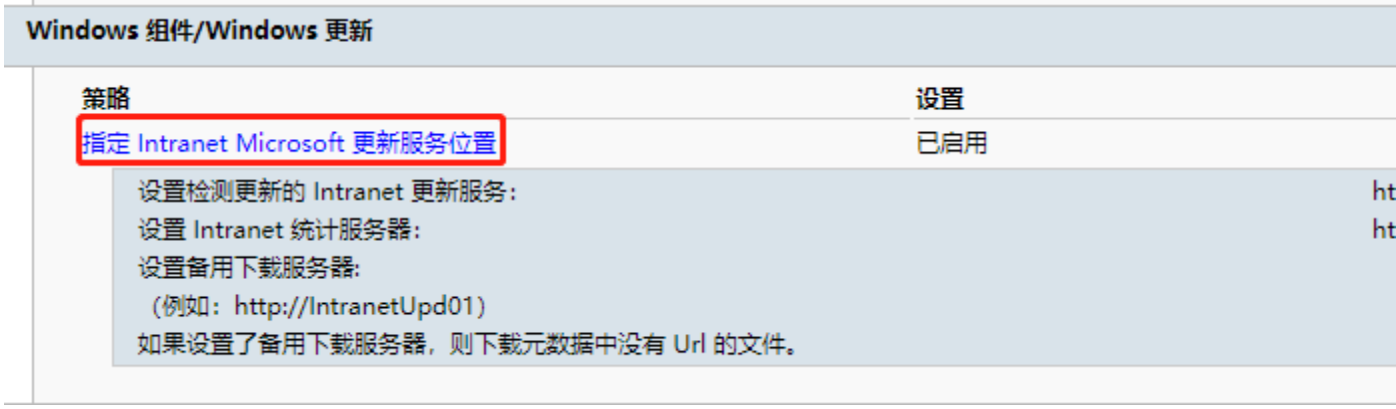
启用如下组策略设置

- 启用“不要连接任何 Windows 更新 Internet 位置”
- 启用“配置自动更新”
- 启用“允许来自 Intranet Microsoft 更新服务位置的签名更新”



日志对比：

问题机器 gpresult：

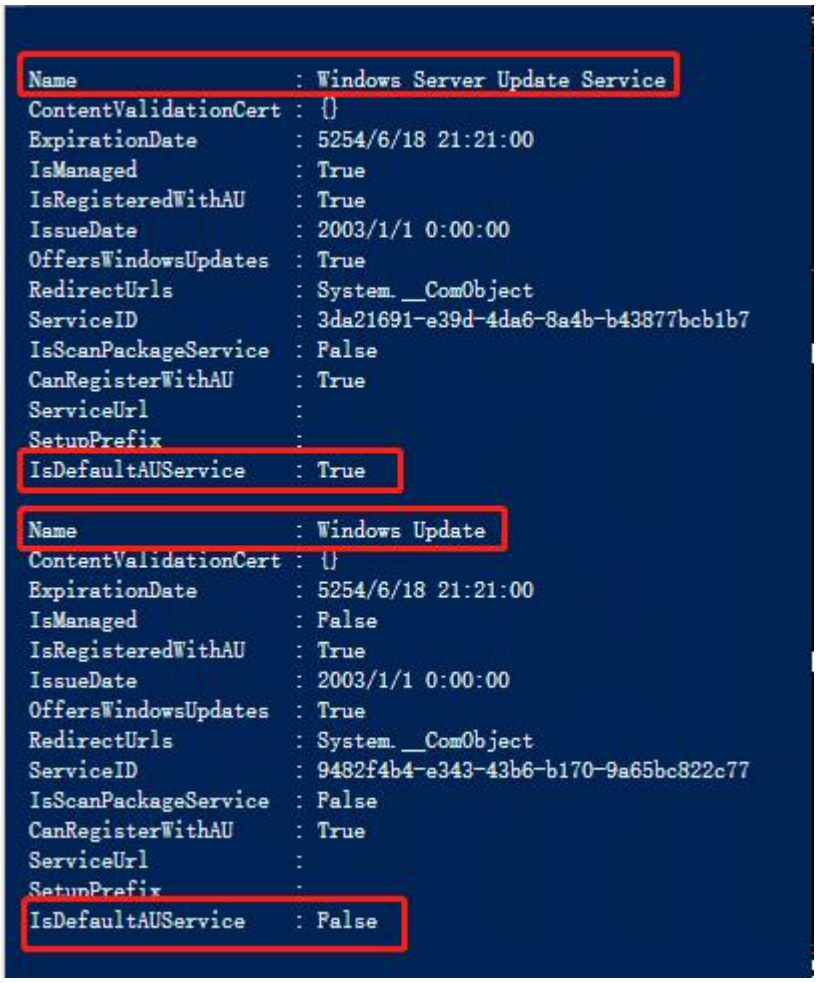


CMGE 默认 gpresult:

问题机器更新设置:

```
Name                 : DCat Flighting Prod
ContentValidationCert : {}
ExpirationDate       :
IsManaged            : False
IsRegisteredWithAU   : False
IssueDate            : 1601/1/1 0:00:00
OffersWindowsUpdates : True
RedirectUrls         : System.__ComObject
ServiceID            : 8b24b027-1dee-babb-9a95-3517dfb9c552
IsScanPackageService : False
CanRegisterWithAU    : False
ServiceUrl           : https://fe3.delivery.mp.microsoft.com/
SetupPrefix          : wu
IsDefaultAUService   : False

Name                 : Windows Store (DCat Prod)
ContentValidationCert : {}
ExpirationDate       :
IsManaged            : False
IsRegisteredWithAU   : False
IssueDate            : 1601/1/1 0:00:00
OffersWindowsUpdates : False
RedirectUrls         : System.__ComObject
ServiceID            : 855e8a7c-ecb4-4ca3-b045-1dfa50104289
IsScanPackageService : False
CanRegisterWithAU    : True
ServiceUrl           : https://fe3.delivery.mp.microsoft.com/
SetupPrefix          : ws
IsDefaultAUService   : False

Name                 : Windows Update
ContentValidationCert : {}
ExpirationDate       :
IsManaged            : False
IsRegisteredWithAU   : True
IssueDate            : 1601/1/1 0:00:00
OffersWindowsUpdates : True
RedirectUrls         : System.__ComObject
ServiceID            : 9482f4b4-e343-43b6-b170-9a65bc822c77
IsScanPackageService : False
CanRegisterWithAU    : True
ServiceUrl           : https://fe2.update.microsoft.com/v6/
SetupPrefix          : wu
IsDefaultAUService   : True
```

正常 CMGE 更新设置：



贾伟 Jia Wei
神州网信技术有限公司
服务电话： 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: 2020 年 8 月 13 日 16:55
收件人: Cao Yang <caoyang@cmgos.com>
抄送: Jia Wei <jiawei@cmgos.com>

主题: [案例号: CAS-02786-P2R1R6] % WindowsUpdate 自动更新异常&Log 日志显示中文 “靠” % 初次响应 CMIT:0001650

曹洋 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-02786-P2R1R6 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
