

ECS运维指南 之Windows系统诊断

云运维工程师从入门到精通

作者:棋玉



- 阿里云工程师多年云上ECS运维经验
- 图文详解33个windows常见问题案例
- 排查要点及最佳解决方案分享





云服务技术大学
云产品干货高频分享



云服务技术课堂
和大牛零距离沟通



阿里云开发者“藏经阁”
海量免费电子书下载

I 目录

第一章 windows 启动问题排查	5
windows 启动失败常用排查方案	5
安装补丁后服务器启动卡住	8
重启卡在“正在应用计算机设置”？6步排查搞定	13
Windows 控制台登录不能切换用户	16
启动报错 “An operating system wasn’t found”	20
windows 重置密码不生效	22
启动报错 “No bootable device”	25
第二章 windows 激活问题排查	27
激活常用排查方案	27
window 机器 ping 不通 KMS 服务器	30
windows 激活报错 0xC004F074	31
windows 激活报错 0x80070020 或 0x80041010	33
第三章 远程 / 网络相关问题排查	36
windows 远程问题的 3 个排查方案	36
windows 网络状态显示 X，看不到网卡信息	44
Windows 网卡驱动丢失，手动安装驱动	48

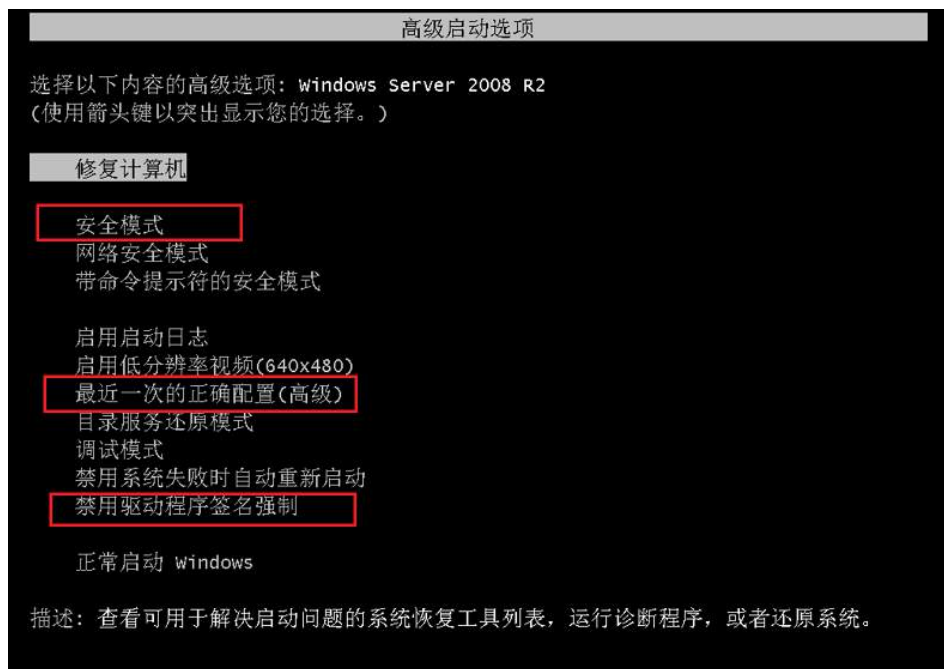
第四章 windows 更新问题排查	51
windows 更新常用的 5 个排查方案	51
查找更新时报错？2 个方案解决	55
“此更新不适用于你的计算机”的 3 个排查方法	57
更新安装报错的 3 个实战分析	59
第五章 windows 服务问题排查	64
服务启动失败？2 步轻松搞定	64
服务启动报错“不能在本地计算机启动”	67
服务启动失败“系统找不到指定文件”	72
如何手动恢复服务	74
第六章 windows 性能问题排查	78
占用内存高 – 分页数 / 未分页	78
内存占用高 –AWE	81
explorer.exe 占用 cpu 或者内存高	83
C 盘空间占满？主要是这 2 个原因	84
第七章 windows 系统相关问题排查	87
如何追踪 Windows 进程自动异常退出	87
进程 crash 报错 1000	90
windows 桌面显示黑屏或者蓝屏	92
windows 异常问题 – 怀疑中毒	96
Windows 数据恢复 – 动态盘显示无效	101
WMI 异常问题要如何重置？	109
提示权限有问题？3 步修改注册表搞定	111

第一章 windows 启动问题排查

windows 启动失败常用排查方案

简介: 本文分享几个 windows 启动失败常用排查方案。

1. 开机按 F8 分别尝试“安全模式”“最近一次的正确配置(高级)”“禁用驱动程序签名强制”。



2. 把系统盘挂载到其他实例进行排查，挂载步骤请参考 https://help.aliyun.com/document_detail/146752.html。系统盘空间不足的话，先清理出空间再继续（一定要找到正确的系统盘！！！需要找到源实例的系统盘比如 D 盘）。



3. 替换系统注册表（建议替换 system 和 software），替换后重复 1,2 步骤

把系统盘挂载到其他实例，挂载步骤请参考 https://help.aliyun.com/document_detail/146752.html。

2008 之后系统

服务器备份注册表路径为：Windows\System32\config\RegBack。

名称	修改日期	类型	大小
DEFAULT	2018/9/8 14:55	文件	252 KB
DEFAULT.LOG1	2018/5/25 14:53	LOG1 文件	0 KB
DEFAULT.LOG2	2018/5/25 14:53	LOG2 文件	0 KB
SAM	2018/9/8 14:55	文件	24 KB
SAM.LOG1	2018/5/25 14:53	LOG1 文件	0 KB
SAM.LOG2	2018/5/25 14:53	LOG2 文件	0 KB
SECURITY	2018/9/8 14:55	文件	32 KB
SECURITY.LOG1	2018/5/25 14:53	LOG1 文件	0 KB
SECURITY.LOG2	2018/5/25 14:53	LOG2 文件	0 KB
SOFTWARE	2018/8/28 18:29	文件	80,876 KB
SOFTWARE.LOG1	2018/5/25 14:53	LOG1 文件	0 KB
SOFTWARE.LOG2	2018/5/25 14:53	LOG2 文件	0 KB
SYSTEM	2018/9/8 14:55	文件	16,720 KB
SYSTEM.LOG1	2018/5/25 14:53	LOG1 文件	0 KB
SYSTEM.LOG2	2018/5/25 14:53	LOG2 文件	0 KB

替换步骤:

1. 把系统盘挂载到其他实例，找到源实例的系统盘，假设为 D 盘，将 D:\windows\system32\config\system 重命名为 system.old(万一重启仍然有问题，我们可以将该文件重命名成 system 进行恢复)
2. D:\Windows\System32\config\RegBack\system 拷贝至 D:\windows\system32\config

注：备份注册表可能比较旧，让客户确认一下应用和数据情况。

2003 系统

服务器备份注册表路径在 WINDOWS\repair。

名称	大小	类型	修改日期	属性
default	228 KB	文件	2018-5-29 22:39	A
ntuser.dat	228 KB	DAT 文件	2018-5-29 22:32	A
san	24 KB	文件	2018-5-29 22:39	A
secsetup.inf	790 KB	安装信息	2018-5-29 22:32	A
security	36 KB	文件	2018-5-29 22:39	A
setup.log	267 KB	文本文档	2018-5-29 22:32	A
software	15,220 KB	文件	2018-5-29 22:39	A
system	1,240 KB	文件	2018-5-29 22:39	A

替换步骤:

1. 把系统盘挂载到其他实例，找到源实例的系统盘，假设为 D 盘，将 D:\windows\system32\config\system 重命名为 system.old(万一重启仍然有问题，我们可以将该文件重命名成 system 进行恢复)。
2. D:\WINDOWS\repair\system 拷贝至 D:\windows\system32\config。

注：备份注册表可能比较旧，替换后需要确认一下应用和数据情况。

卸载系统盘，挂回源实例 (https://help.aliyun.com/document_detail/146752.html)，启动机器，可以正常进入系统。

安装补丁后服务器启动卡住

简介：两个案例透彻排查安装补丁后服务器启动卡住的情况。

症状 1

安装补丁后服务器卡在“请等候 windows modules installer”界面。



排查

1. 此类问题一般都是由于补丁安装配置太久，可以尝试进入安全模式或者将系统盘挂载到其他实例看一下。

2. 目前 ecs 已支持系统盘卸载功能，可以把系统盘挂载到其他实例进行排查，挂载步骤请参考。

https://help.aliyun.com/document_detail/146752.html

3. 挂载后，发现原来实例系统盘剩余空间只有 6MB，清理磁盘空间后成功启动（一定要找到正确的系统盘！！！需要改到源实例的系统盘比如 D 盘）。

注：补丁安装并没有规定的磁盘可用空间大小，因为补丁大小不一样，不过一般建议至少保留 5G 以上剩余空间。



症状 2

服务器卡在“配置 windows update 失败 还原更改 请勿关闭计算机”界面。

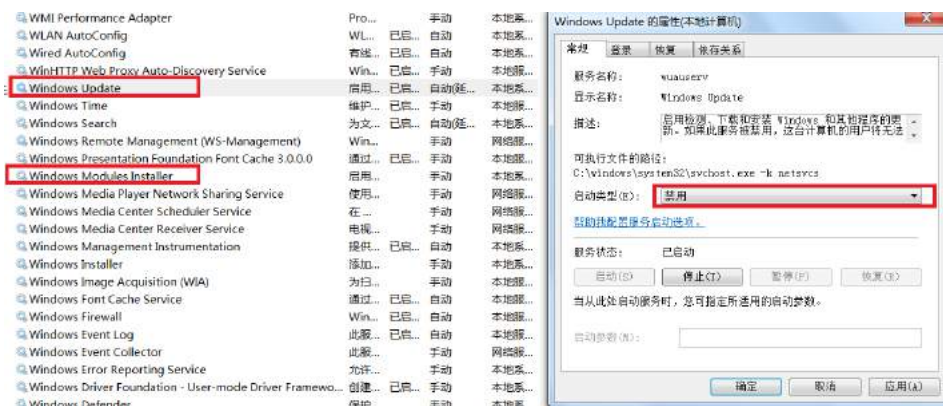


排查

1. 此类问题都是由于补丁安装失败，在回滚过程中遇到了报错，导致不停地重启不停地回滚。

2. 临时解决方案：

进入安全模式，将 windows update 和 Windows Modules Installer 服务禁用。

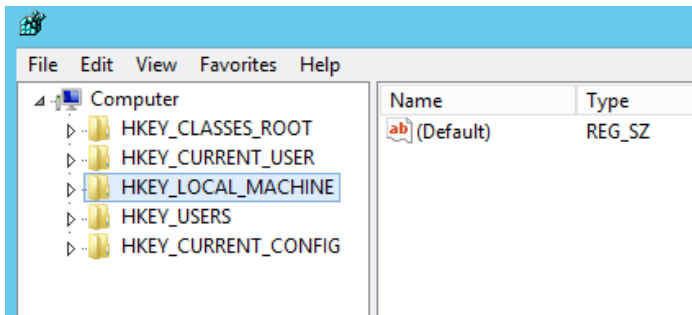


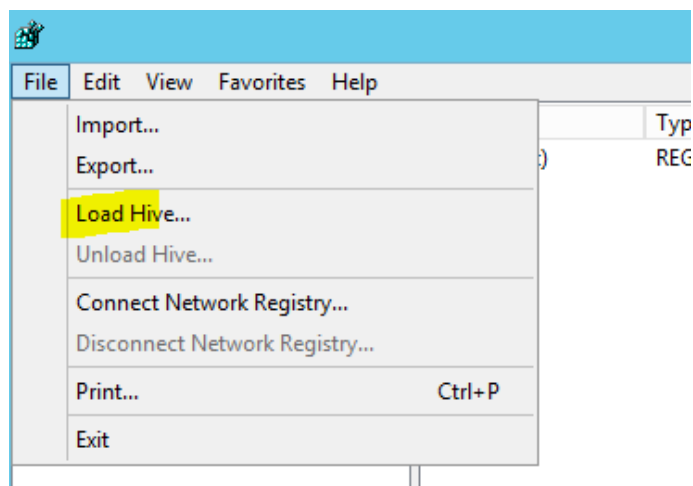
如果安全模式进不去，可以把系统盘挂载到其他实例进行排查，挂载步骤请参考

https://help.aliyun.com/document_detail/146752.html，修改注册表禁用服务。

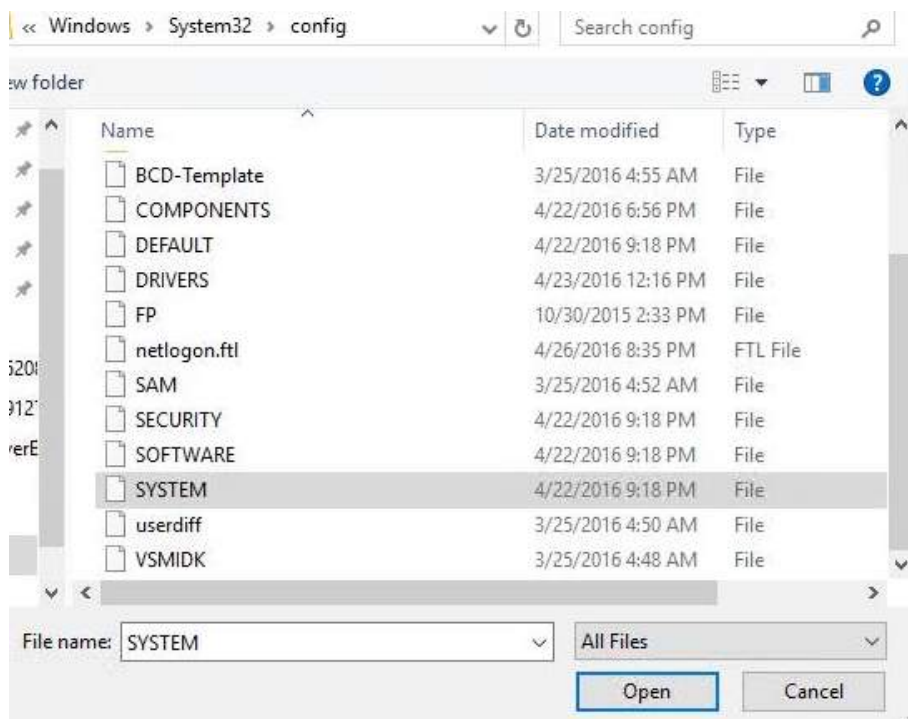
1. cmd 命令行输入 regedit。

2. 找到 HKEY_LOCAL_MACHINE, 然后点击 file, 选择 Load Hive。

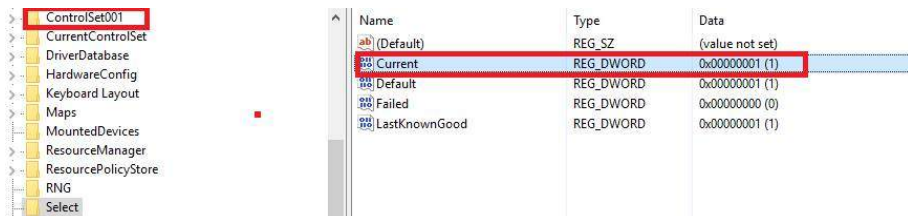




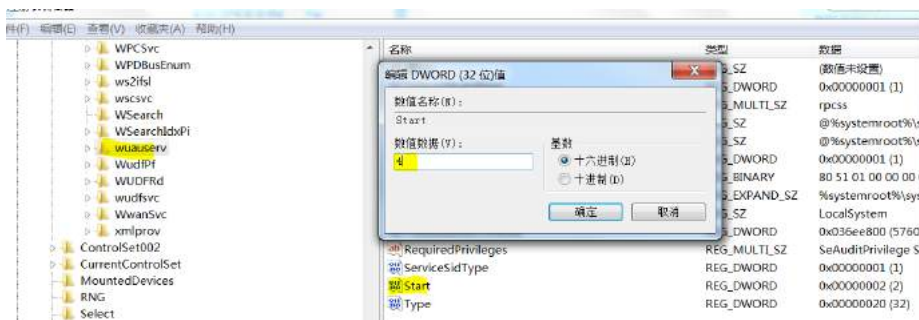
3. 找到系统盘（一定要找到正确的系统盘！！！默认加载的是当前实例的 C 盘，需要改到源实例的系统盘比如 D 盘），并加载 `windows\system32\config\system`，任意命名（例如 test）。



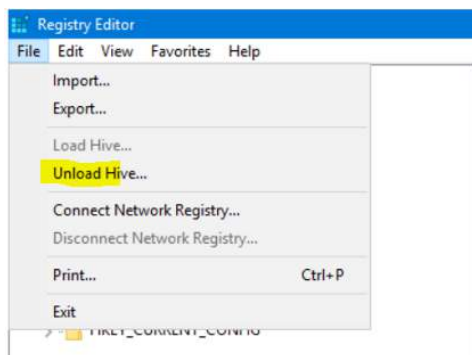
4. 展开 test，查看 select 项，current 值为 1，则我们应该去找 ControlSet001。



5. 展开 ControlSet001，展开 services，找到 TrustedInstaller 和 wuauserv，将 start 值改为 4。



6. 回到 test 项，先选中 test，再选择 file，点击 Unload Hive。



7. 卸载系统盘，挂回源实例 (https://help.aliyun.com/document_detail/146752.html)，启动机器，可以正常进入系统。

重启卡在“正在应用计算机设置”？6步排查搞定

简介：分享一个配置开机脚本后服务器启动卡在“正在应用计算机设置”的案例。

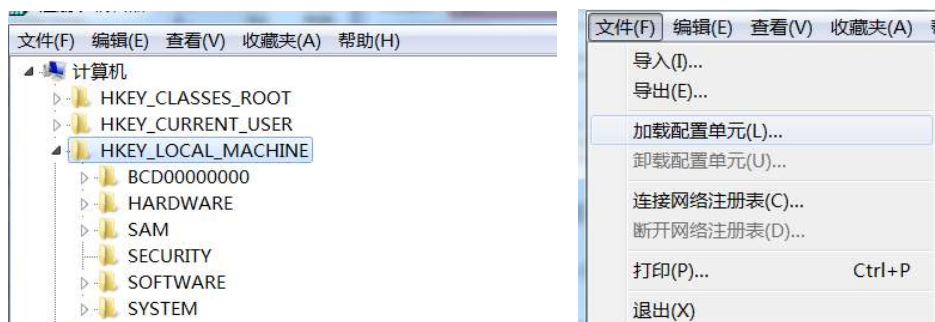
问题现象

客户表示新配置了启动脚本，之后重启卡在“正在应用计算机设置”。

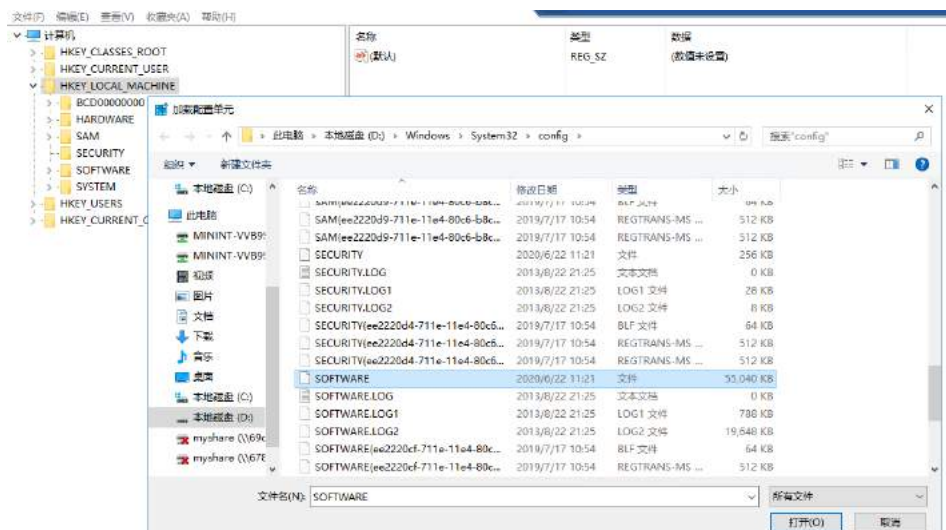


排查

1. 问题发生在配置启动脚本后，那我们可以首先尝试将启动脚本禁用。
2. 把系统盘挂载到其他实例，挂载步骤请参考 https://help.aliyun.com/document_detail/146752.html，修改注册表禁用启动脚本。
3. cmd 命令行输入 regedit，找到 HKEY_LOCAL_MACHINE，然后点击文件，选择加载配置单元。



4. 找到系统盘，并加载 `windows\system32\config\software` (注：一定要找到正确的系统盘！！默认加载的是当前实例的 C 盘，需要改到源实例的系统盘比如 D 盘)，任意命名（例如 test）。



5. 启动脚本注册表路径如下：

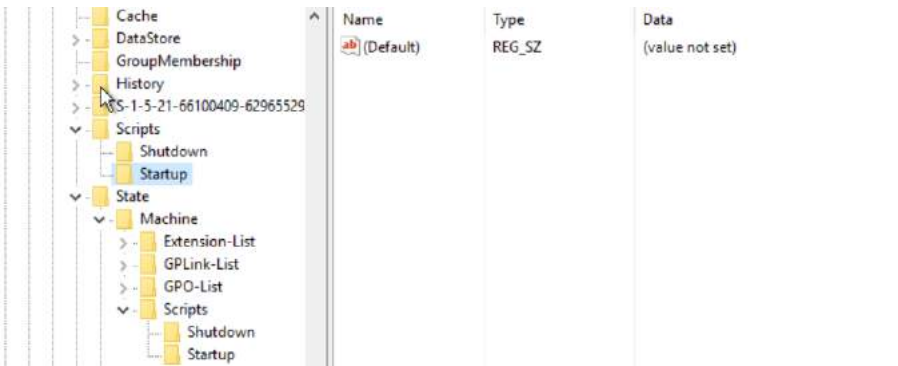
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\GroupPolicy\Scripts\startup`

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\GroupPolicy\State\Machine\Scripts\Startup`

登录脚本：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVer-
sion\Group Policy\State\{GUID}\Scripts\Logon
```

将下面的子项全部删除。



6. 卸载系统盘，挂回源实例 (https://help.aliyun.com/document_detail/146752.html), 启动机器，可以正常进入系统。

Windows 控制台登录不能切换用户

简介：客户将原来的用户禁用了，新建了一个用户，但是控制台登录的时候无法切换到新的用户。

客户还把允许远程禁止了，因此无法通过远程登录。

背景

客户将原来的用户禁用了，新建了一个用户，但是控制台登录的时候无法切换到新的用户。

客户还把允许远程禁止了，因此无法通过远程登录。



解决方案

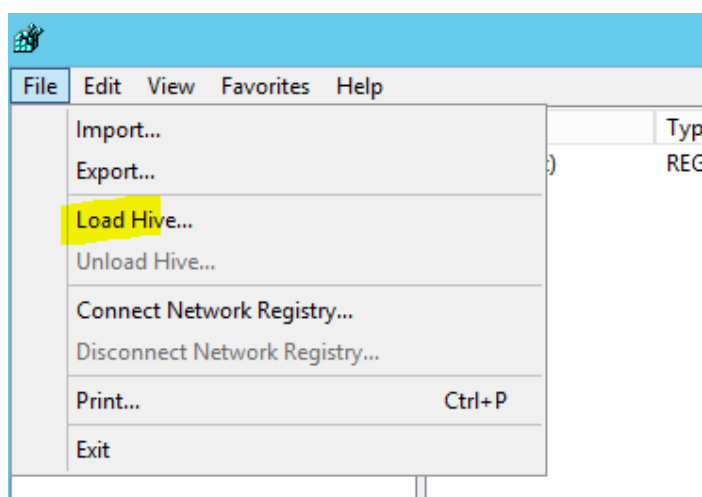
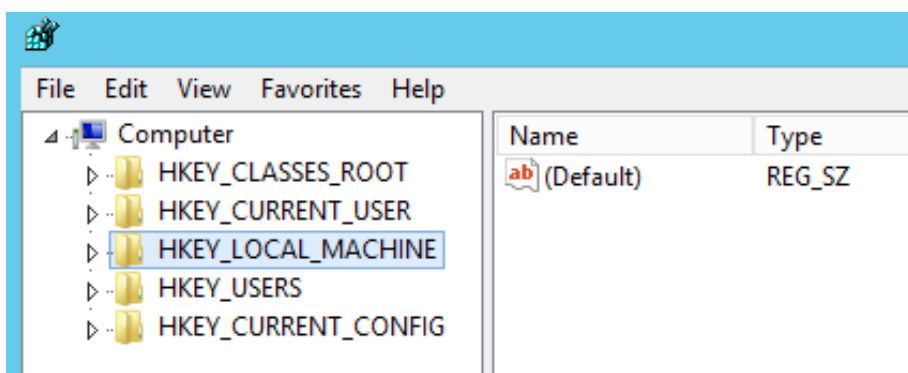
1. 把系统盘挂载到其他实例，挂载步骤请参考 https://help.aliyun.com/document_detail/146752.html。
2. 更改以下组策略对应的注册表。

组策略：计算机配置 \ Windows 设置 \ 安全设置 \ 本地策略 \ 安全选项 \ 交互式登录：不显示最后的用户名。

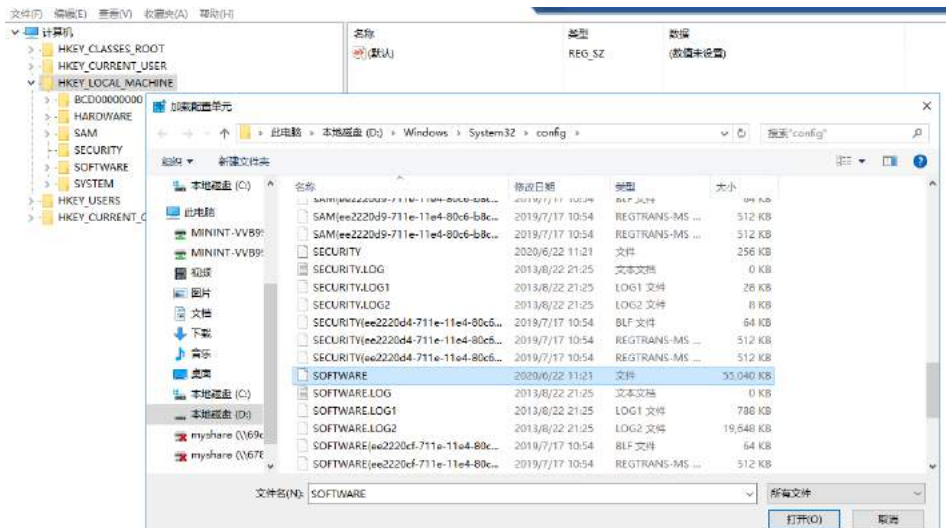
注册表：`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\dontdisplaylastusername`

具体步骤如下

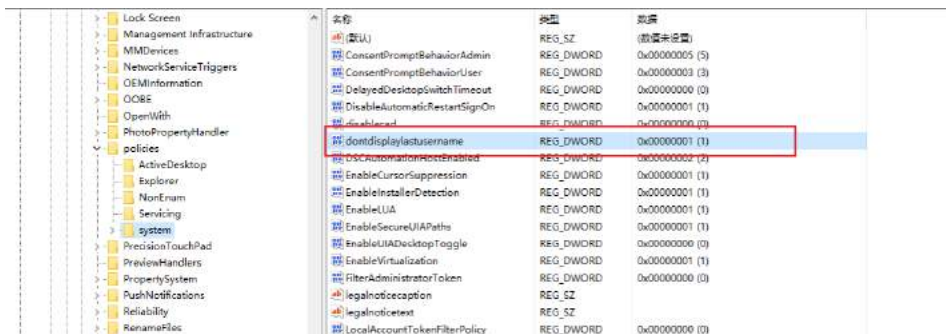
- a. cmd 命令行输入 regedit，找到 HKEY_LOCAL_MACHINE，然后点击 file，选择 Load Hive。



- b. 找到系统盘，并加载 `windows\system32\config\software` (注：一定要找到正确的系统盘！！默认加载的是当前实例的 C 盘，需要改到源实例的系统盘比如 D 盘)，任意命名（例如 test）。



- c. 找到 `HKEY_LOCAL_MACHINE\test\Microsoft\Windows\CurrentVersion\policies\system\dontdisplaylastusername`，改为 1。



3. 卸载系统盘，挂回源实例 (https://help.aliyun.com/document_detail/146752.html), 启动机器，看到登录界面用户名是空的，这样就可以手动输入用户名和密码进行登录。



启动报错 “An operating system wasn't found”

简介：分享一个启动报错 “An operating system wasn't found” 的案例。

问题现象

启动报错 “An operating system wasn't found”。

```
SeaBIOS (version 8c24b4c)
Machine UUID da5a44fe-85f9-4a92-8f0b-f2748271e1a3

iPXE (http://ipxe.org) 00:03.0 C980 PCI2.10 PnP PMM+BFF91490+BFEF1490 C980

Booting from Hard Disk...

An operating system wasn't found. Try disconnecting any drives that don't
contain an operating system.
Press Ctrl+Alt+Del to restart
-
```

排查

1. 把系统盘挂载到其他实例进行排查，挂载步骤请参考 https://help.aliyun.com/document_detail/146752.html。
2. 发现源实例缺失 bootmgr 文件（注：一定要找到正确的系统盘！！！需要改到源实例的系统盘比如 D 盘）。

此电脑 > 本地磁盘 (D:) >

名称	修改日期	类型	大小
\$Recycle.Bin	2020/6/22 13:21	文件夹	
Boot	2020/5/14 23:46	文件夹	
Documents and Settings	2013/8/22 22:48	文件夹	
PerfLogs	2013/8/22 23:52	文件夹	
Program Files	2020/6/22 11:23	文件夹	
Program Files (x86)	2020/5/14 15:50	文件夹	
ProgramData	2020/6/22 11:20	文件夹	
Recovery	2020/6/22 11:21	文件夹	
System Volume Information	2020/5/14 7:47	文件夹	
test	2020/6/22 13:21	文件夹	
Windows	2020/6/22 11:22	文件夹	
用户	2020/5/14 15:48	文件夹	
BOOTNXT	2013/6/18 20:18	系统文件	1 KB
pagefile.sys	2020/6/22 11:21	系统文件	1,966,080...

3. 从相同版本正常机器拷贝 bootmgr 文件。

此电脑 > 本地磁盘 (D:) >

名称	修改日期	类型	大小
\$Recycle.Bin	2020/6/22 13:21	文件夹	
Boot	2020/5/14 23:46	文件夹	
Documents and Settings	2013/8/22 22:48	文件夹	
PerfLogs	2013/8/22 23:52	文件夹	
Program Files	2020/6/22 11:23	文件夹	
Program Files (x86)	2020/5/14 15:50	文件夹	
ProgramData	2020/6/22 11:20	文件夹	
Recovery	2020/6/22 11:21	文件夹	
System Volume Information	2020/5/14 7:47	文件夹	
test	2020/6/22 13:21	文件夹	
Windows	2020/6/22 14:58	文件夹	
用户	2020/5/14 15:48	文件夹	
bootmgr	2017/9/15 2:20	系统文件	381 KB
BOOTNXT	2013/6/18 20:18	系统文件	1 KB
pagefile.sys	2020/6/22 14:58	系统文件	1,966,080...

4. 卸载系统盘，挂回源实例 (https://help.aliyun.com/document_detail/146752.html)，启动机器，可以正常进入系统。

windows 重置密码不生效

简介：针对 windows 重置密码不生效问题的详细排查。

问题

控制台重置密码后重启服务器仍然不生效。

排查

1. 把系统盘挂载到其他实例进行排查，挂载步骤请参考 https://help.aliyun.com/document_detail/146752.html。
2. 控制台更改密码的日志在 `ProgramData\aliyun\vmnit\log`，查看日志没有关于更改密码的记录，怀疑是控制台更改的密码并没有被触发。
3. 查看源实例系统盘完全没有可用空间（注：一定要找到正确的系统盘！！！需要查看的是源实例的系统盘比如 D 盘），这个解释了第 2 步日志没有记录的原因。



4. 清理磁盘空间后，更改密码，重启后发现仍然不生效。
5. 再次更改密码，重启后直接进入安全模式，发现更改密码是生效了的，说明密码更改过程没有问题。

注：对于安全模式正常，直接启动异常的问题，多是跟三方有关，因为安全模式下只加载一些支撑系统能够成功启动的必要组件（有些系统组件也不会加载）。

安全模式正常重启后，再输入密码还是提示报错，基本可以确认是三方问题，一般如下排查方案：

在安全模式下：

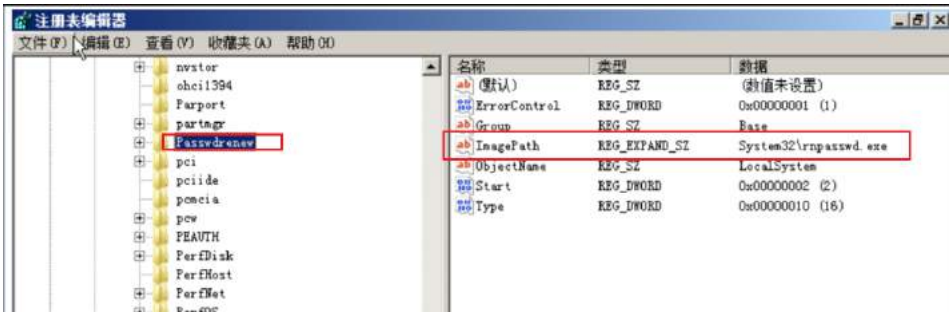
- a. 运行 msconfig，将所有非 microsoft 的服务和启动项都禁用，具体请参考如下步骤

<https://support.microsoft.com/zh-cn/help/929135/how-to-perform-a-clean-boot-in-windows>

禁用后重启发现仍然报错密码不正确，看起来还是有三方影响。

我们碰到过很多 msconfig 将三方服务和启动项禁用后仍然不行的问题，这个是因为一般三方应用除了服务外还会有三方驱动，这些驱动在系统启动过程中就会被加载，这时候就需要我们去查看对应注册表信息（驱动和服务的注册表都是 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`）。

- b. 查看注册表 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`，有一个可疑注册表项，从命名来看就是重置密码相关的，将 start 类型改成 4（4 表示禁用）。



之后重启服务器后使用密码可以正常登录了。

后续

从现有信息来看，服务器可能已经中毒或者被入侵，安全起见还是建议客户备份好数据重置系统。

启动报错 “No bootable device”

简介：三个步骤排查启动报错 “No bootable device”。

问题

启动时报错截图如下。

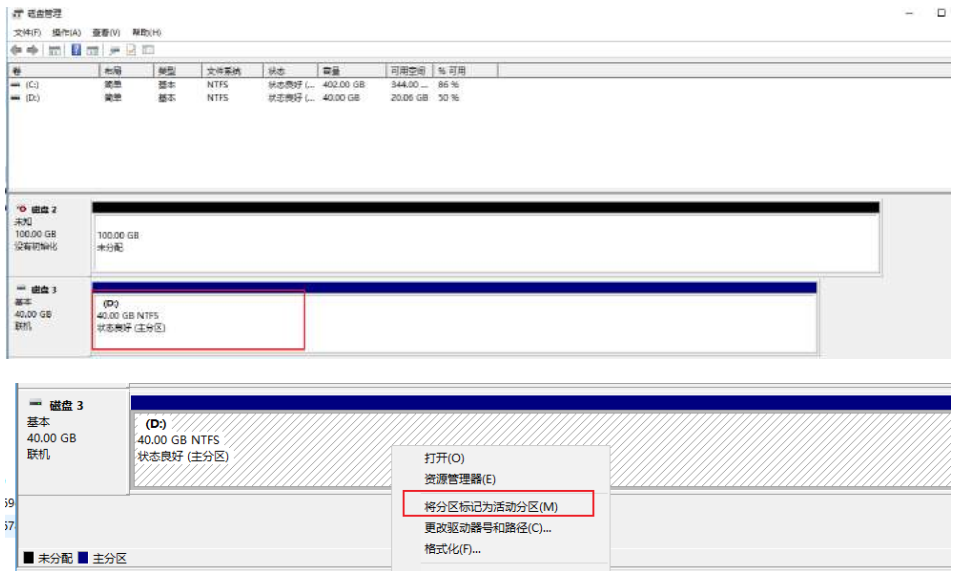


```
Booting from DVD/CD...
Boot failed: Could not read from CDROM (code 0003)
Booting from Hard Disk...
No bootable device.
```

排查

1. 从报错基本可以判断是识别不到启动盘。
2. 把系统盘挂载到其他实例进行排查，挂载步骤请参考 https://help.aliyun.com/document_detail/146752.html。

挂载后，发现原来实例系统盘的活动分区标志没有了（一定要找到正确的系统盘！！！需要改到源实例的系统盘比如 D 盘），右键选择“将分区标记为活动分区”。



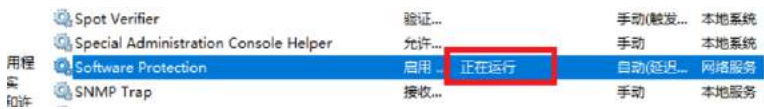
3. 卸载系统盘，挂回源实例 (https://help.aliyun.com/document_detail/146752.html), 启动机器，之后系统正常启动。

第二章 windows 激活问题排查

激活常用排查方案

简介: 分享激活常用排查方案。

- 1. 确认 software protection 服务是否正常运行，如果是运行中状态，重启服务确保能正常重启。



- 2. 能够正常 ping kms 服务器和 telnet kms 1688 端口 (确保 DNS 配置的是内网 DNS) 经典网络下是内网 10 网段地址，对应 kms.aliyun-inc.com 域名，经典网络内网 DNS: 10.143.22.116 和 10.143.22.118。

VPC 环境下是 100 网段内部服务地址，对应 kms.cloud.aliyuncs.com, vpc 内网 DNS: 100.100.2.136 和 100.100.2.138。

- 3. 确保使用的是正常的激活码 (各版本 Windows 系统产品密钥参考: <https://technet.microsoft.com/en-us/library/jj612867.aspx>)。

运行 `slmgr /upk` 卸载激活码。

运行 `slmgr /ipk < 激活码 >` 安装激活码。

```
C:\Users\Administrator>slmgr /ipk YC6KT-GKW9T-YTKYR-T4X34-R7UHC  
C:\Users\Administrator>slmgr -ato
```

4. 重命名 tokens.dat 文件后再试下：

注：以下步骤可能会对环境有影响，建议先进行**快照备份**。

对于 Windows Vista 或 Windows Server 2008。

以管理员身份运行下面 CMD 命令：

```
net stop sppsvc  
cd %windir%\serviceprofiles\networkservice\appdata\roaming\microsoft\  
softwarelicensing  
ren tokens.dat tokens.bar  
net start slsvc  
cd %windir% \System32  
slmgr.vbs -rilc
```

重启客户端两次使配置生效。

对于 Windows 7 或 Windows Server 2008 R2。

以管理员身份运行下面 CMD 命令：

```
net stop sppsvc  
cd C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Microsoft\  
SoftwareProtectionPlatform  
ren tokens.dat tokens.bar  
net start sppsvc  
cd %windir% \System32  
slmgr.vbs -rilc
```

重启客户端两次使配置生效。

对于 Windows 8, Windows Server 2012, Windows 8.1, or Windows Server 2012 R2。

以管理员身份运行下面 CMD 命令：

```
net stop sppsvc
cd %windir%\ServiceProfiles\LocalService\AppData\Local\Microsoft\WSLicense
ren tokens.dat tokens.bar
net start sppsvc
cd %windir% \System32
slmgr.vbs -rilc
```

重启客户端两次使配置生效。

! window 机器 ping 不通 KMS 服务器

简介: 分享 window 机器 ping 不通 KMS 服务器的案例。

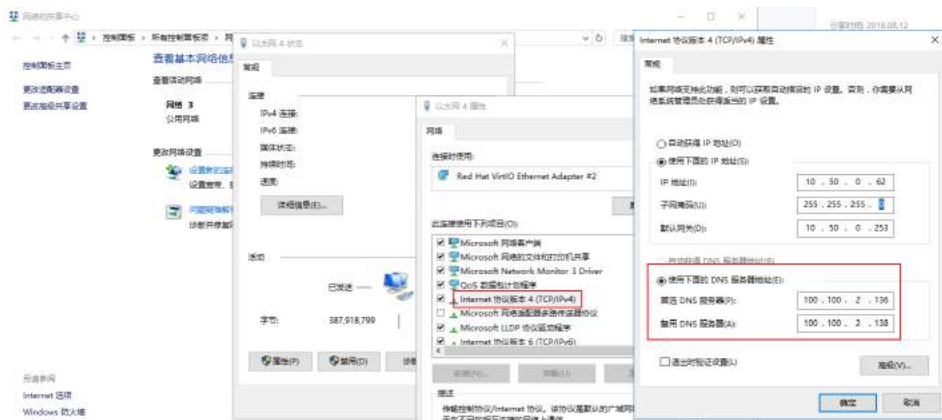
1. 检查防火墙是否开启, 临时关闭再测试一下。



2. 安全组内网出方向是否做了限制, 如果有限制, 临时放开所有地址测试一下

https://help.aliyun.com/document_detail/25471.html。

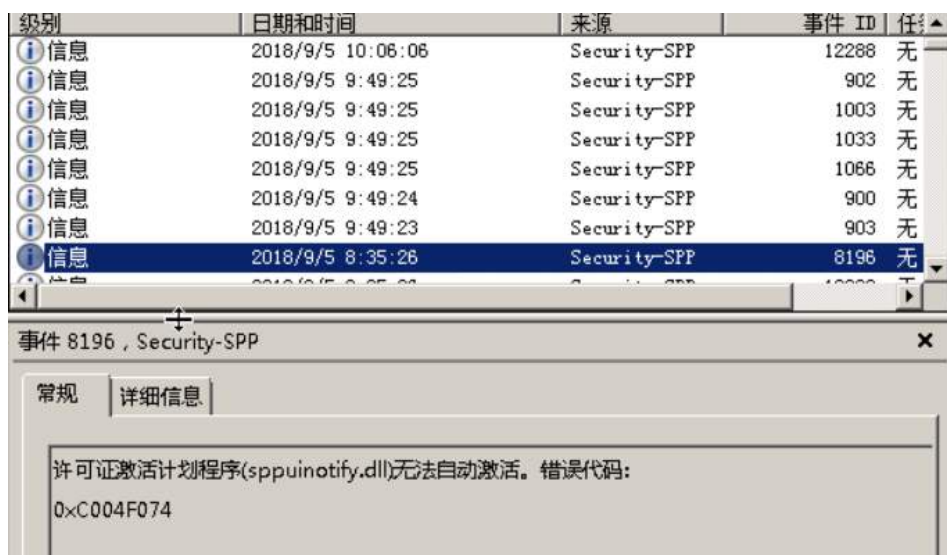
3. 在网卡属性里将 DNS 服务器设置成内网地址 (VPC 是 100.100.2.136 和 100.100.2.138, 经典网络是 10.143.22.116 和 10.143.22.118)。



windows 激活报错 0xC004F074

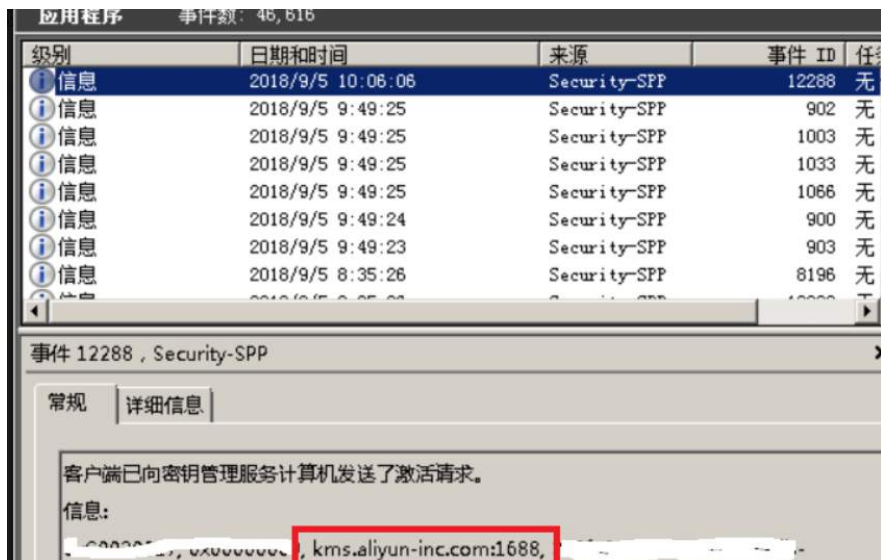
简介: windows 激活报错 0xC004F074 的案例分享。

1. 运行 `slmgr /ato` 后无任何输出。
2. 查看应用程序日志，发现报错 0xC004F074。



信息提示已经向 KMS 服务器发送了请求，所以问题就是 KMS 服务器没有响应

进一步核实发现指向了错误的 KMS 服务器，客户是 VPC 网络，截图中显示客户使用的是经典网络 KMS 服务器 (kms.aliyun-inc.com)。

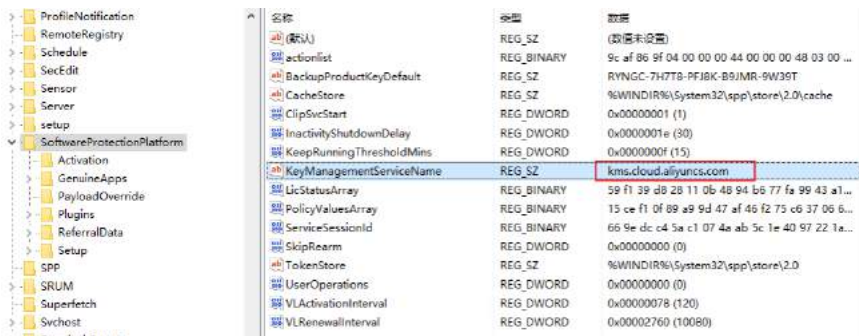


3. 运行命令更改服务器，之后重启 software protection 服务后问题依旧。

```
C:\Users\Administrator>slmgr -skms kms.cloud.aliyuncs.com
```

4. 通过注册表更改 KMS 服务器 (kms.cloud.aliyuncs.com)，之后重启 software protection 服务后激活成功。

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SoftwareProtectionPlatform\KeyManagementServiceName

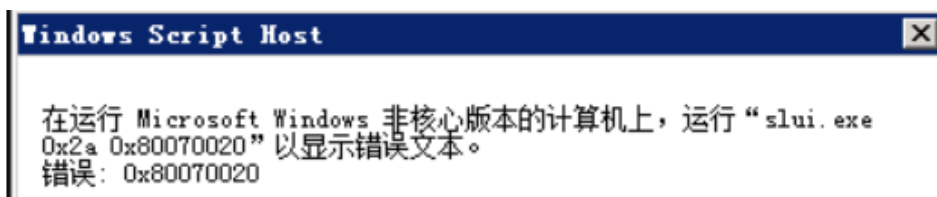


windows 激活报错 0x80070020 或 0x80041010

简介: windows 激活报错 0x80070020 或 0x80041010。

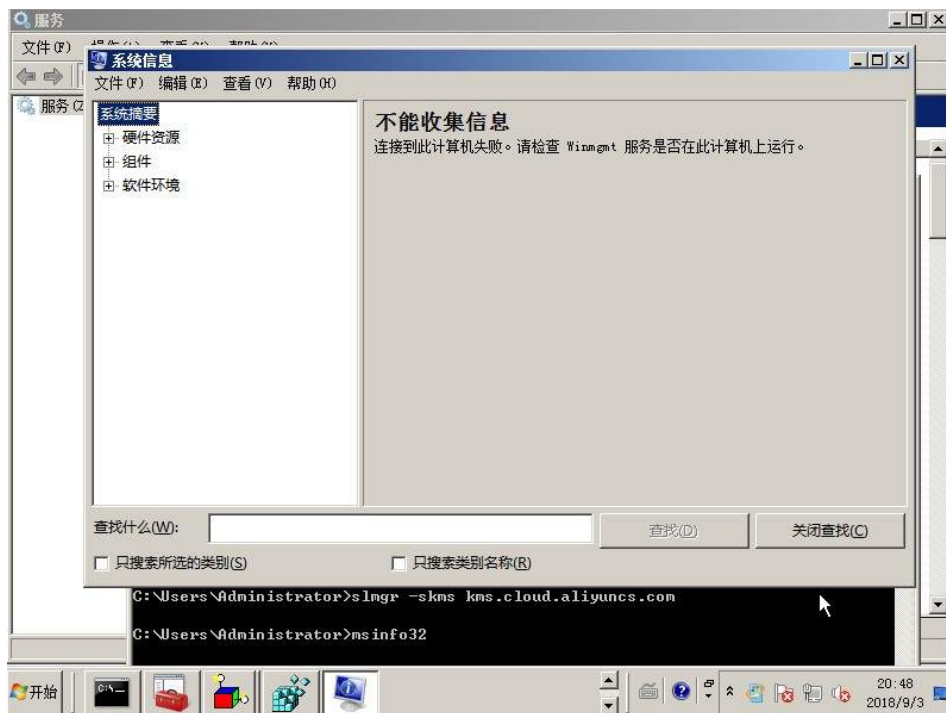
问题现象

激活报错, `slmgr /ato` 后报错代码类似如下:



排查步骤

1. 运行命令行 `slmgr /dlv` 同样报错, 说明是 `slmgr` 本身命令有问题, 不像是网络层面的问题。
2. 查看 `msinfo32`, 发现报错, 提示 `winmgmt` 服务有问题。



3. 重启 winmgmt 服务，可以正常重启，说明 winmgmt 服务本身正常，需要 rebuild wmi 数据库。

Windows Media Center Scheduler Service	仕 ...	手动	网络版...
Windows Media Center Receiver Service	电视...	手动	网络版...
Windows Management Instrumentation	提供... 已启...	自动	本地系...
Windows Installer	添加...	手动	本地系...

4. 按照以下步骤 rebuild wmi 数据库（注：此操作可能会对环境产生影响，建议先进行快照）。

windows Server 2008R2

右击 cmd，选择以管理员身份运行，运行以下命令行：

```
sc config winmgmt start= disabled
```

```
net stop winmgmt /y
cd %windir%\system32\wbem
rename repository repository.old
for /f %s in ('dir /b *.dll') do regsvr32 /s %s
wmiprvse /regserver
sc config winmgmt start= auto
net start winmgmt
for /f %s in ('dir /b *.mof *.mfl') do mofcomp %s
```

Windows Server 2012 及以后版本

右击 cmd，选择以管理员身份运行，运行以下命令行：

```
sc config winmgmt start= disabled
net stop winmgmt /y
%systemdrive%
cd %windir%\system32\wbem
ren repository repository-backup
for /f %s in ('dir /b *.dll') do regsvr32 /s %s
sc config winmgmt start= Auto
net start winmgmt
dir /b *.mof *.mfl | findstr /v /i uninstall > moflist.txt & for /F %s in
(moflist.txt) do mofcomp %s
```

5. 之后成功激活。

第三章 远程 / 网络相关问题排查

| windows 远程问题的 3 个排查方案

简介: 分享三个 windows 远程问题排查方案。

问题 1

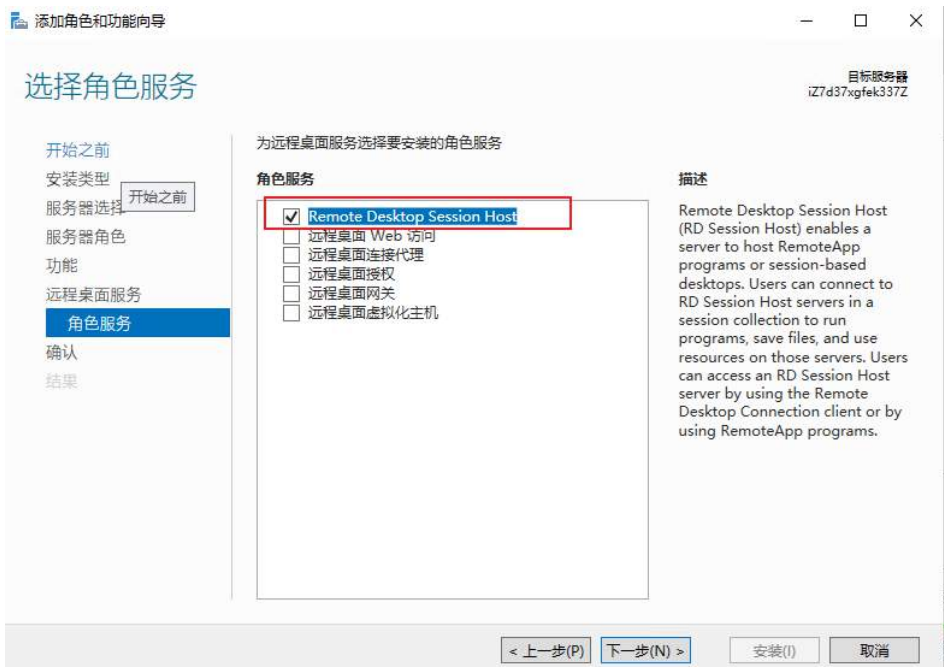
客户反馈已经安装了远程授权并且配置了证书，但是仍然无法超过 2 个用户登录。

问题原因

未安装“远程桌面会话主机”角色。

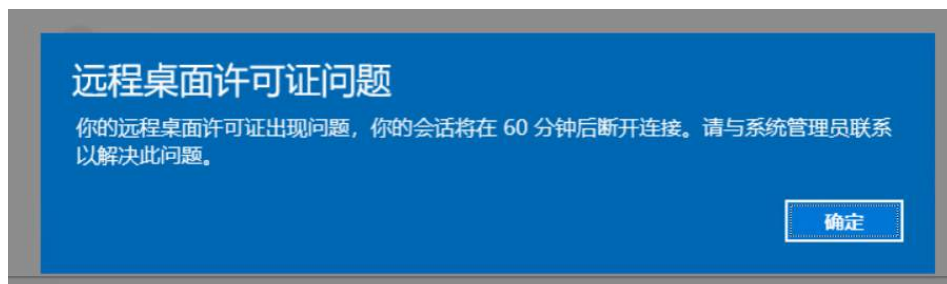
解决方案

安装“远程桌面会话主机”角色，windows 2019 是 "Remote Desktop Session Host". 安装后需要重启服务器生效。



问题 2

配置授权后，远程时报错“你的远程桌面许可证出现问题，你的会话将在 60 分钟后断开，请与系统管理员联系解决此问题。”

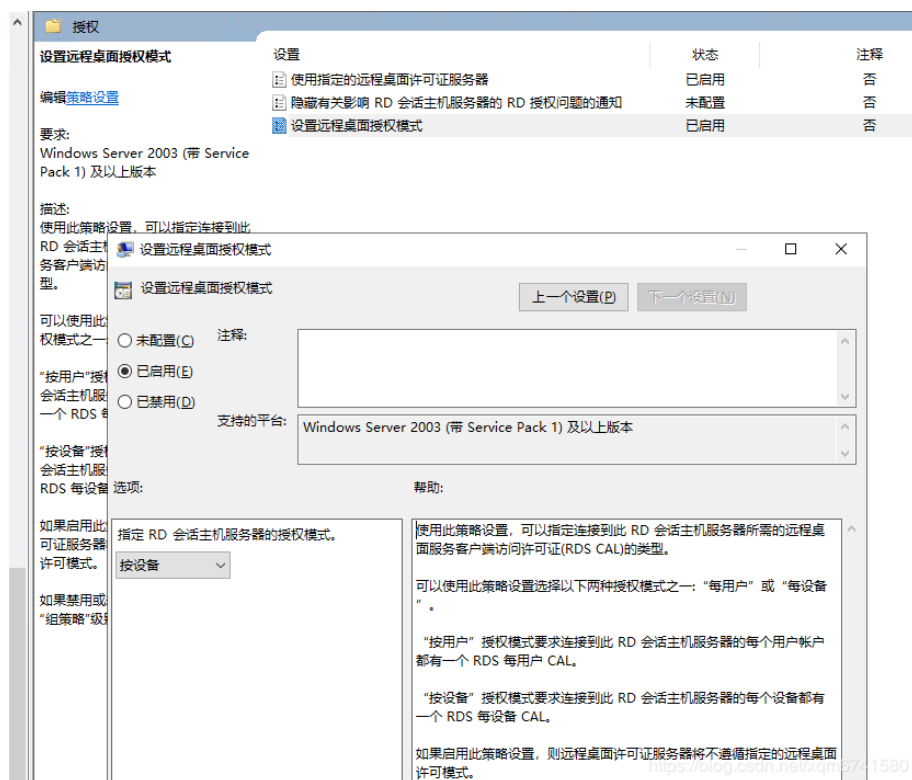


问题原因

workgroup 机器授权只能用每设备。

解决方案

组策略里授权模式改成“每设备”，RD 授权管理器里要存在每设备许可证，修改后重启服务器生效。



问题 3

远程报错“没有远程桌面授权服务器可以提供许可证”。

问题原因

未配置远程桌面许可证。

解决方案

方法一

配置远程桌面会话主机服务器后，在微软官网购买和配置相应的证书授权，相关操作方法可以[参阅微软官方文档](#)。

方法二

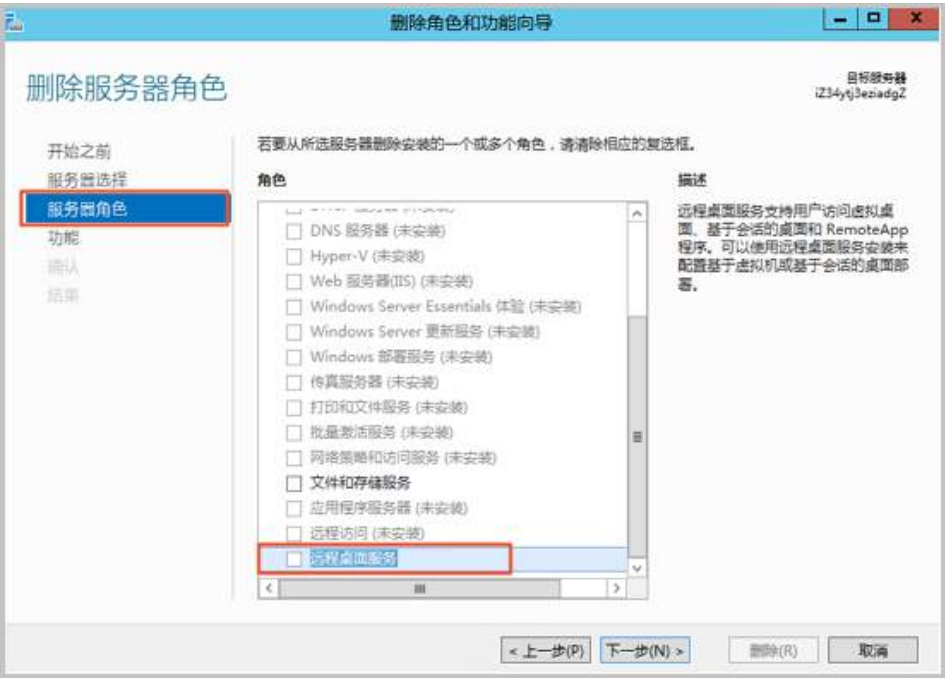
删除远程桌面会话主机角色，使用默认两个用户的免费连接授权。参考以下步骤对不同版本的 Windows 服务器进行配置。

Windows 2012 操作系统

1. 通过[管理终端连接](#) Windows 实例。
2. 选择 开始，单击 运行，在打开框中输入 servermanager.msc，单击 确定。
3. 进入服务器管理器页面，选择 管理 > 删除角色和功能。



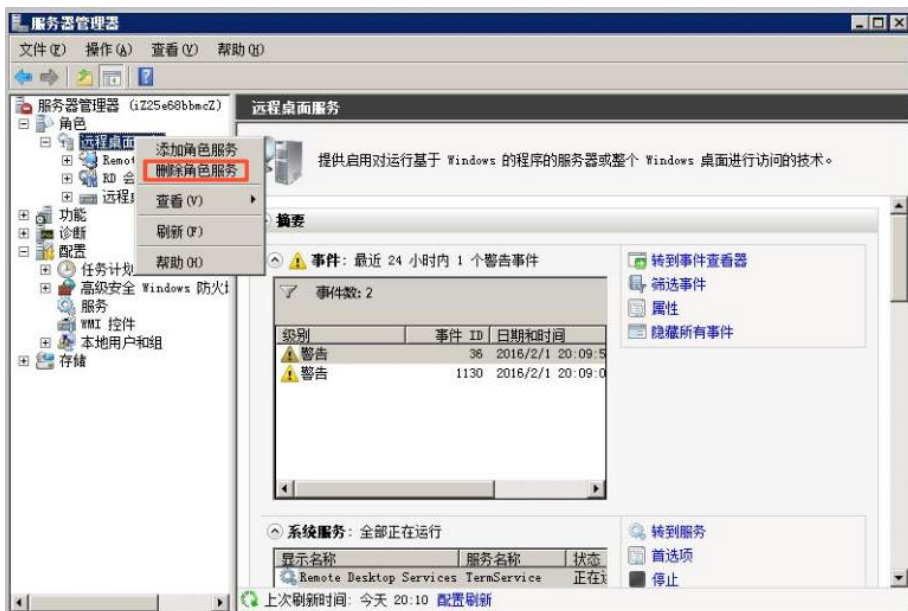
- 4. 进入删除功能和角色页面，单击下一步，单击下一步。
- 5. 在 角色 框中，取消勾选 远程桌面服务，其它配置默认，单击 下一步。



- 6. 在 Windows 实例内重启实例。

Windows 2008 操作系统

- 1. 通过[管理终端连接](#) Windows 实例。
- 2. 选择 开始，单击运行，在打开框中输入 servermanager.msc，单击确定。
- 3. 进入服务器管理页面，单击角色，右键单击远程桌面服务，选择删除角色服务。



4. 在弹出窗口中，取消勾选 远程桌面会话主机，单击 下一步，等待配置完成。



5. 在 Windows 实例内重启实例。

Windows 2003 操作系统

1. 通过[管理终端连接](#) Windows 实例。
2. 选择 开始 > 控制面板。
3. 选择 添加或者删除程序 > 添加 / 删除 Windows 组件。
4. 取消勾选 终端服务器，单击 下一步。在弹出的窗口中，单击完成。



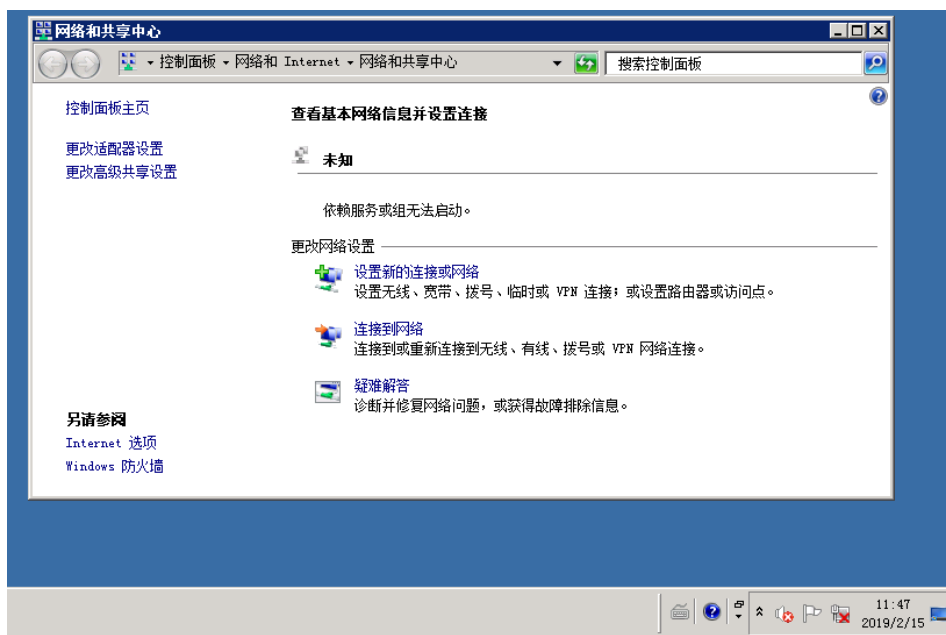
5. 在 Windows 实例内重启实例。

windows 网络状态显示 X，看不到网卡信息

简介: 分享一个 windows 网络状态显示 X，看不到网卡信息的案例。

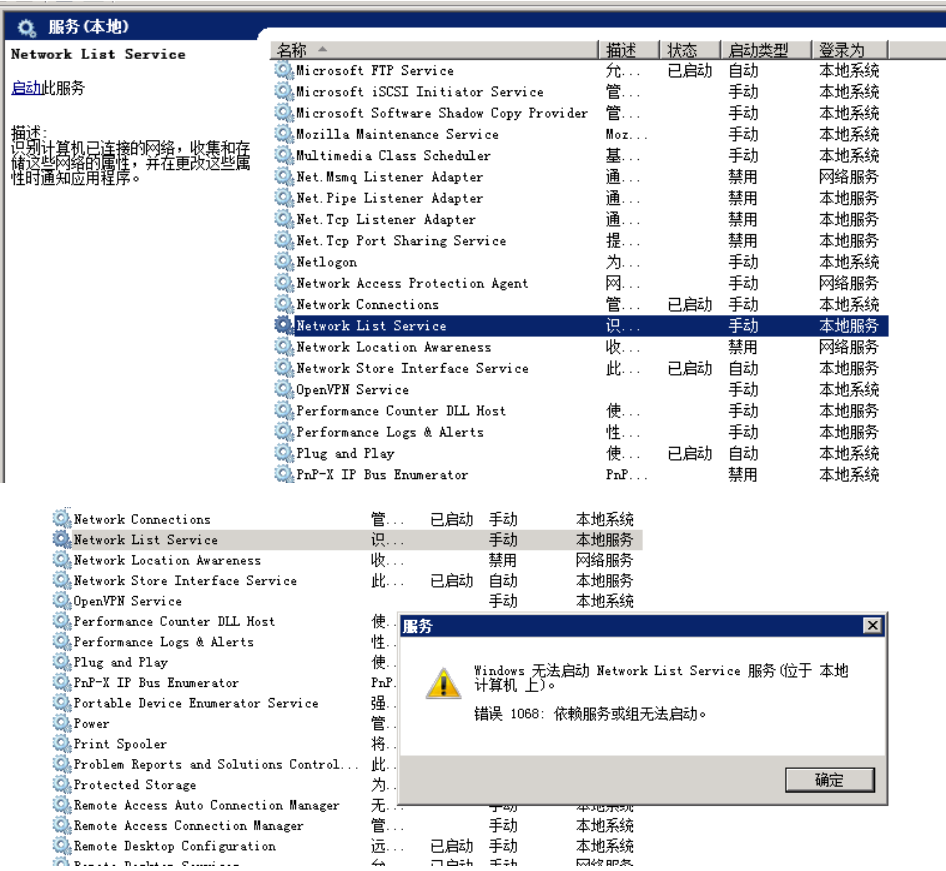
问题

windows 网络状态显示 X，看不到网卡信息。实际网络正常，可以访问。

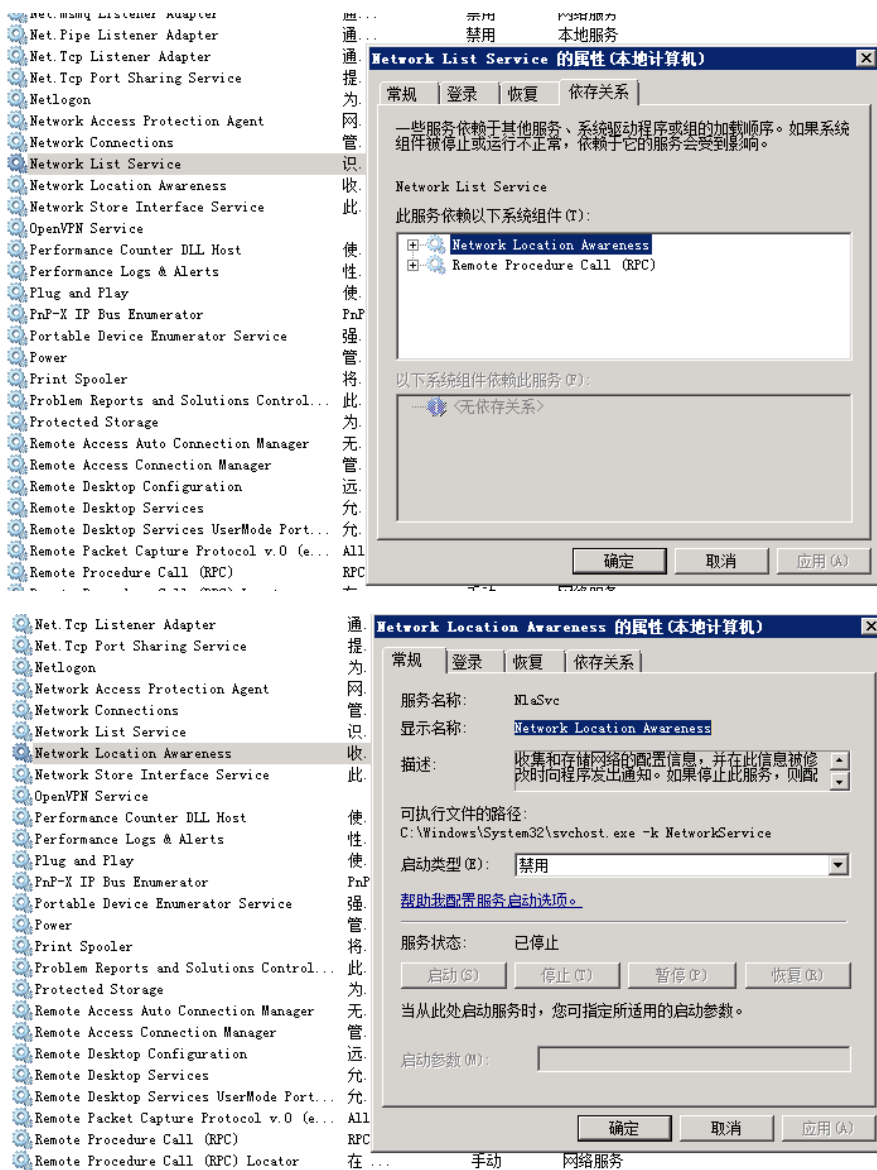


解决

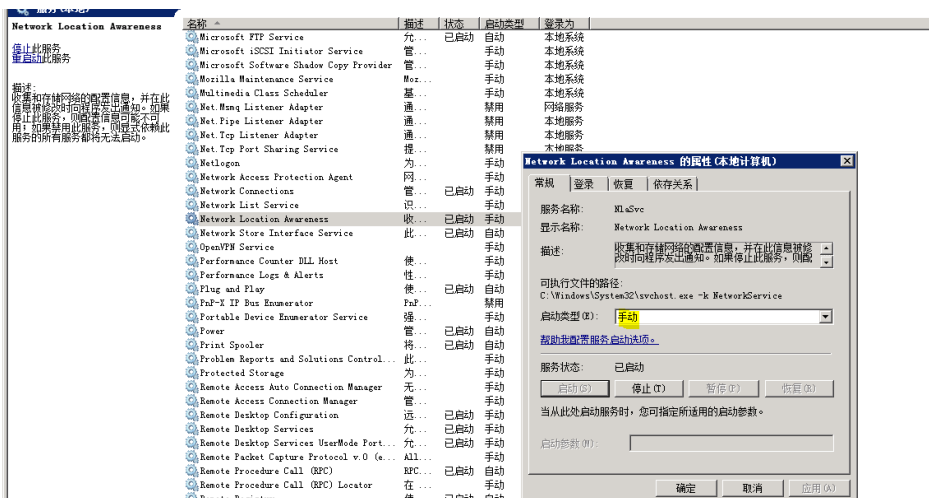
网卡等信息的显示和 Network List Service 有关，查看该服务没有启动，手动启动服务报错。



本案例是由于依存服务 Network Location Awareness 被禁用。



将 Network Location Awareness 服务启动类型改成手动, 并依次启动 Network Location Awareness, Network List Service 服务。



可以正常看到网卡信息。



Windows 网卡驱动丢失，手动安装驱动

简介：Windows 网卡驱动丢失？教你如何手动安装驱动。

windows 各系统版本网卡驱动目录(C:\ProgramData\aliyun\vmnit\kvm)如下：

Windows Server 2003 使用 wnet。

Windows Server 2008 使用 wlh。

Windows Server 2008 R2 使用 win7。

Windows Server 2012 R2 使用 win8。

Windows Server 2016 使用 win8。

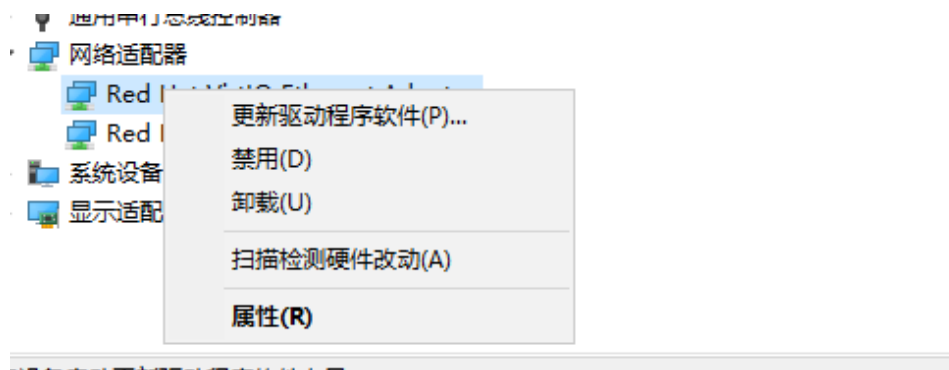
具体案例

客户自定义镜像，2012 服务器创建后网络不通，查看适配器发现为空。



打开设备管理器，手动安装驱动：

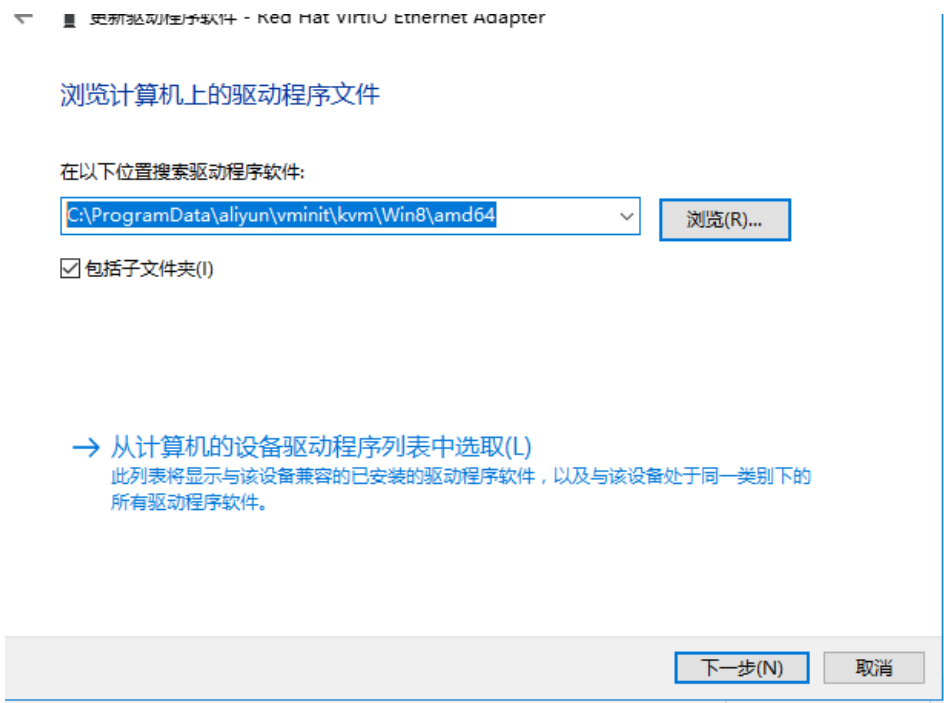
找到对应设备，选择更新驱动程序软件。



选择“浏览计算机以查找驱动程序软件”。



选到这个路径: `C:\ProgramData\aliyun\vm\init\kvm\Win8\amd64`，选择下一步，等待驱动安装完成。



驱动安装完成后，测试网络可以正常连通。

第四章 windows 更新问题排查

| windows 更新常用的 5 个排查方案

简介: windows 更新常用排查方案分享。

注: 修改操作前, 请先执行快照作为备份!!!

1. 使用自动修复工具先修复看一下:

<https://support.microsoft.com/zh-cn/help/4027322/windows-update-troubleshooter>

2. 运行如下命令行, 手动重置 windows update:

```
net stop cryptsvc
net stop BITS
net stop WUAUSERV
Ren %systemroot%\SoftwareDistribution SoftwareDistribution.bak
Ren %systemroot%\system32\catroot2 catroot2.bak
net start cryptsvc
net start BITS
net start WUAUSERV
```

3. 2008/2008R2 机器, 参考如下步骤:

(1) 运行 System File Checker utility (SFC.exe)。

右击 cmd, 选择以管理员身份运行, 运行以下命令行:

```
sfc /scannow
```

(2) 运行 checksur。

1) 点击以下链接：

<https://support.microsoft.com/zh-cn/kb/947821>

2) 根据系统版本 (是 X86 还是 X64) 选择下载对应的程序包。



3) 下载后，安装补丁 (注：这个补丁和常规意义的补丁并不一样，这个补丁是用来检测更新的库是否正常并尝试修复的一个工具)。

(3) 安装 3177467 (仅适用 2008R2 系统)。

<https://support.microsoft.com/zh-cn/help/3177467/servicing-stack-update-for-windows-7-sp1-and-windows-server-2008-r2-sp>

方法 2：Microsoft 更新目录

若要获取此更新的独立程序包，请转到 [Microsoft 更新目录](#) 网站。

2012/2016 机器，参考如下步骤：

(1) 运行 System File Checker utility (SFC.exe)。

右击 cmd，选择以管理员身份运行，运行以下命令行：

```
sfc /scannow
```

(2) 完成后在执行以下命令：

```
DISM.exe /Online /Cleanup-image /Scanhealth
DISM.exe /Online /Cleanup-image /Restorehealth
```

4. 卸载三方安全类软件比如 360，安全狗（注：将进程停止是不行的，因为驱动和组件已经加载在内核里，需要卸载并重启服务器）。

5. 还是有问题的话，需要查看日志。

```
"C:\Windows\Logs\CBS\CBS.log"
"C:\Windows\WindowsUpdate.log"
```

建议查看日志的技巧：

1. 根本 kb 号或者错误代码搜索，找到这一行（这一行就是补丁安装的结束位置）：

WER: Generating failure report for package: Package_for_KB.....



2. 查看靠近这行之前的报错（这些报错才是补丁失败的真正原因）尤其是第一个报错，以下示例，补丁安装的直接原因是 Failed call to CryptCATAdminAddCatalog. [HRESULT = 0x8000ffff - Unknown Error]。



3. 这个报错是跟 Cryptographic Services 和 catroot2 有关，查看 C:\Windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE} 缺失 catdb 文件，可以从相同版本正常机器尝试拷贝文件测试。



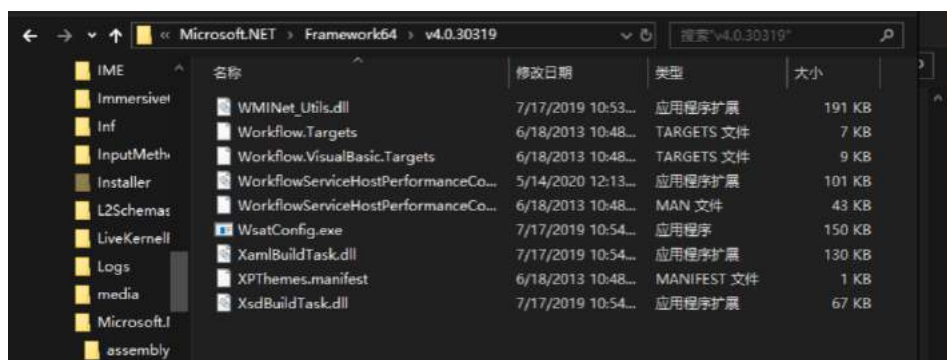
对于在重启过程发生补丁回滚的，分析日志要以 rollback 为关键字（如下示例，这行表示补丁配置失败了，开始 rollback 即回滚）。

```
1 nonSxS, PublicKeyToken = {1:8 b:31bf3856ad364e35}, Type neutral, TypeName neutral, PublicKey neutral;4568801  
N32(14109). Failure will not be ignored. A rollback will be initiated after all the operations in the installer queue are completed;
```

之后查看最靠近这行的报错，是在执行 C:\Windows\Microsoft.NET\Framework-work64\v4.0.30319\ngen.exe 的时候报错了。

```
2019-04-28 20:34:49. Info CSI 000000be Calling generic command executable (sequence 41 (0x00000029)): [66] "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe"  
2019-04-28 20:34:49. Info CSI 000000bd Failed to launch generic command [66] "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe" (createProcess) failed with error 7  
2019-04-28 20:34:49. Error CSI 000000be@2019/4/28:12:34:49.531 (F) d:\w7\ta\base\wcp\componentstore\com\generic\commands.cpp(522): Error HRESULT_FROM_WIN32 ERROR_FILE_NOT_FOUND  
[gle=0x80004005]
```

这个案例中，查看 C:\Windows\Microsoft.NET\Framework64\v4.0.30319 缺失了 ngen.exe，同时该目录下还缺失了很多其他文件，建议相同版本正常机器尝试拷贝文件测试或者重置系统。

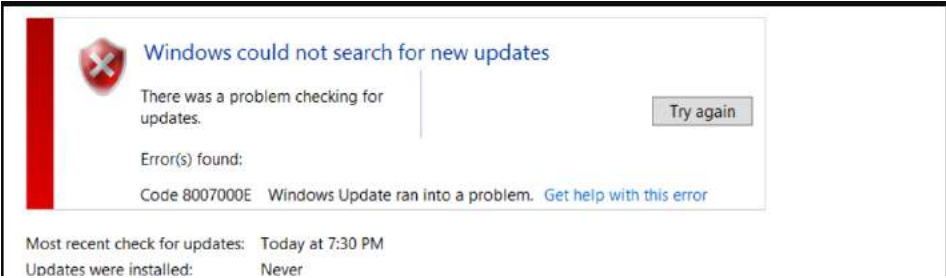


注：如果是多个补丁安装失败的情况，建议只选择一个补丁进行安装，针对这个补丁先看一下具体的报错。

查找更新时报错？2 个方案解决

简介：Windows update 查找更新时遇到报错的案例。

1. 查看具体报错，代码为 8007000e。



解析这个错误代码，表示“ran out of memory”，内存不足的意思。

关于错误代码的解析，请参考如下链接。

https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-erref/1bc92ddf-b79e-413c-bbaa-99a5281a6c90

0x8007000E E_OUTOFMEMORY	The server does not have enough memory for the new channel.
-----------------------------	---

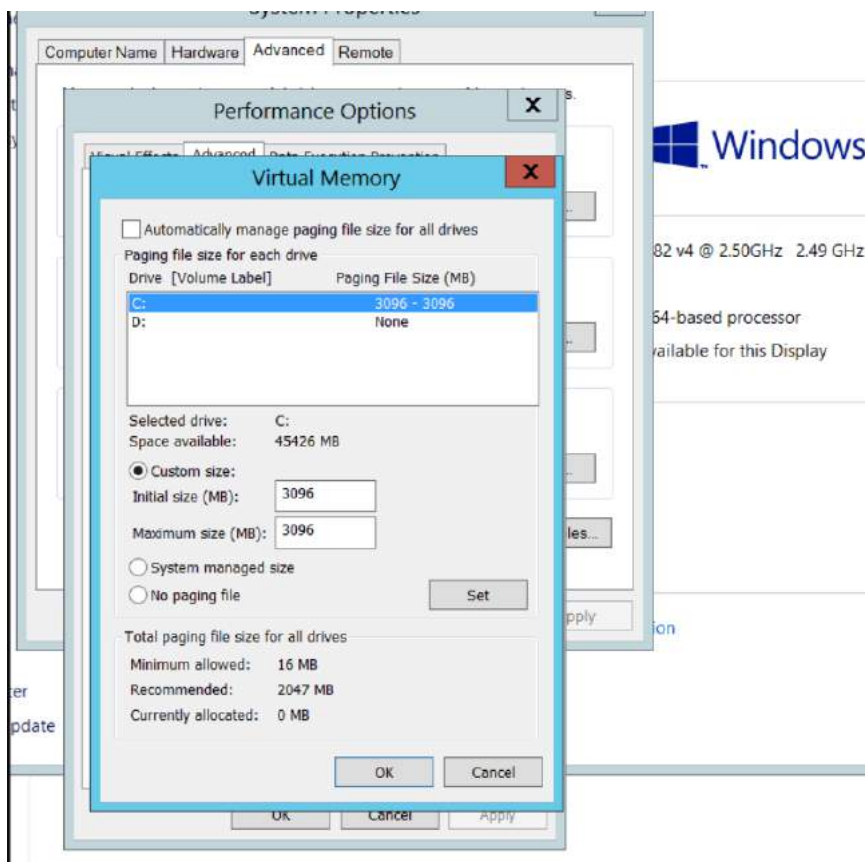
2. 查看内存占用量，确实不是很多（客户系统总共才 2G 内存），而且系统日志一直有内存资源不足的告警。

Level	Date and Time	Source	Event ID	Task Category
Warning	11/22/2018 7:39:35 PM	Resource-Exhaustion-Detector	2004	Resource Exhaustion Diagnosis Eve...
Warning	11/22/2018 7:34:47 PM	Resource-Exhaustion-Detector	2004	Resource Exhaustion Diagnosis Eve...
Warning	11/22/2018 7:31:11 PM	Resource-Exhaustion-Detector	2004	Resource Exhaustion Diagnosis Eve...
Warning	11/22/2018 7:29:56 PM	Resource-Exhaustion-Detector	2004	Resource Exhaustion Diagnosis Eve...
Warning	11/22/2018 7:29:18 PM	Resource-Exhaustion-Detector	2004	Resource Exhaustion Diagnosis Eve...
Warning	11/22/2018 4:25:23 PM	Resource-Exhaustion-Detector	2004	Resource Exhaustion Diagnosis Eve...
Warning	11/22/2018 4:20:59 PM	Resource-Exhaustion-Detector	2004	Resource Exhaustion Diagnosis Eve...

针对这种问题，建议方案如下：

1. 增加物理内存。
2. 设置虚拟内存来增加内存使用量（但是 ecs 使用须知不建议使用虚拟内存，因此最直接的方案还是方案 1 增加物理内存）。

注：设置虚拟内存后需要重启服务器生效。



“此更新不适用于你的计算机”的 3 个排查方法

简介：对于报错“此更新不适用于你的计算机”的几大原因分析。

对于报错“此更新不适用于你的计算机”，大部分都是由于补丁确实不适用于当前系统，可能原因如下：

1. 系统版本不一致，比如补丁是适用于 windows 2012 的，但是客户系统版本是 windows2012R2。
2. 系统架构不一致，比如补丁是适用于 X86 系统的，但是客户系统是 X64 的。
3. 客户已经安装了更新的补丁，如何查看：

打开补丁官方链接，找到 文件信息》对应系统版本》对应文件版本。

以下以 KB3042553 示例。

- a. 打开 <https://support.microsoft.com/zh-cn/help/3042553/ms15-034-vulnerability-in-http-sys-could-allow-remote-code-execution-a>
- b. 可以看到这个补丁是用来更新 http.sys 的，对于 windows server 2012R2 安装完这个补丁后 http.sys 将被更新到 6.3.9600.17712。

文件信息

此软件更新的英语（美国）版本安装了拥有下表所列属性的文件。这些文件的日期和时间按协调世界时 (UTC) 列出。这些文件在您本地计算机上显示的日期和时间是您的本地时间再加上当前夏令时 (DST) 偏差。此外，在您对文件执行某个操作时日期和时间也可能发生改变。

Windows 7 和 Windows Server 2008 R2 文件信息

Windows 8 和 Windows Server 2012 文件信息

Windows 8.1 和 Windows Server 2012 R2 文件信息

对于所有受支持的基于 x86 的 Windows 8.1 版本

File name	File version	File size	Date	Time	Platform
Http.sys	6.3.9600.17712	738,112	24-Feb-2015	08:20	x86

对于所有受支持的基于 x64 的 Windows 8.1 和 Windows Server 2012 R2 版本

File name	File version	File size	Date	Time	Platform
Http.sys	6.3.9600.17712	991,552	24-Feb-2015	08:32	x64

c. 对比系统当前 http.sys 版本信息为 6.3.9600.18730，高于 KB3042553 的版本，这种情况下 KB3042553 补丁安装就会提示“此更新不适用于你的计算机”。

share view

This PC > Local Disk (C:) > Windows > System32 > drivers

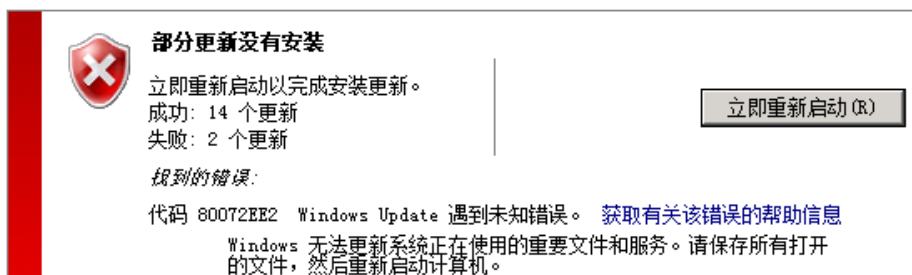
The screenshot shows a Windows File Explorer window with the address bar set to 'This PC > Local Disk (C:) > Windows > System32 > drivers'. The file list on the left includes various system files, with 'http.sys' selected. The 'http.sys Properties' dialog box is open, showing the 'General' tab. The 'File version' is highlighted in blue and reads '6.3.9600.18730'. Other details visible include 'File description: HTTP Protocol Stack', 'Type: System file', 'Product name: Microsoft® Windows® Operating System', 'Product version: 6.3.9600.18730', 'Copyright: © Microsoft Corporation. All rights reserv...', 'Size: 966 KB', 'Date modified: 9/14/2017 7:36 PM', 'Language: English (United States)', and 'Original filename: http.sys'.

更新安装报错的 3 个实战分析

简介：针对 windows 更新安装报错的实战分析。

案例 1

补丁安装失败，重启后补丁回滚并且服务器启动报错 bootmgr is missing。

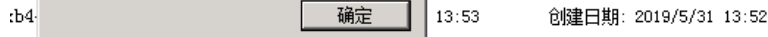


```
Booting from Hard Disk...  
  
BOOTMGR is missing  
Press Ctrl+Alt+Del to restart
```

排查

1. 查看 cbs log，回滚之前的报错是 copy bootmgr 的时候报错了，这个就解释了为什么启动会报错 bootmgr is missing。

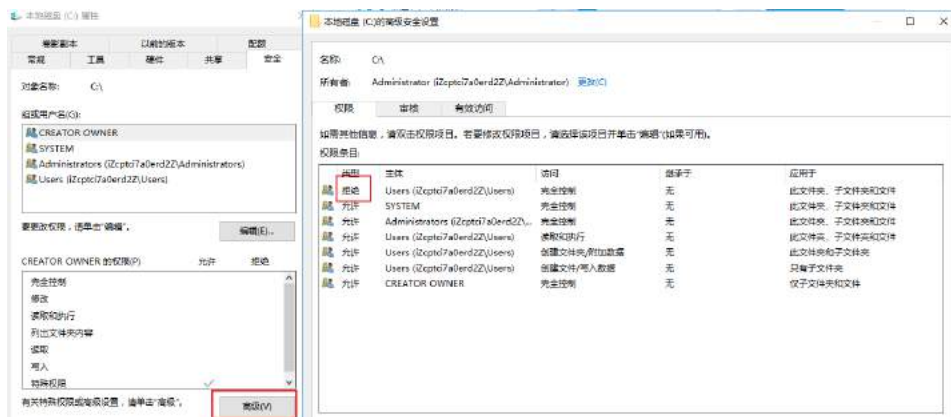
错误代码是 0x5, 这个一般表示是 accessdenied, 没有权限。



4. 收集 procmon 日志，发现在向 C 盘根目录写入文件报错了。

11:00	Explorer.exe	3744	Access Denied	Desired Access: Read Data/List Directory	Read Attributes	Synchronizing	Disposition
11:00	Explorer.exe	3744	Access Denied	Desired Access: Read Data/List Directory	Read Attributes	Synchronizing	Disposition
11:00	Explorer.exe	3744	Access Denied	Desired Access: Read Data/List Directory	Read Attributes	Synchronizing	Disposition
11:00	Explorer.exe	3744	Access Denied	Desired Access: Read Data/List Directory	Read Attributes	Synchronizing	Disposition

5. 查看 C 盘根目录的权限，发现其中有一条是拒绝用户写入的权限。



解决方案

将用户的拒绝权限删除后，补丁成功安装，服务器正常启动。

案例 2

补丁安装报错 80070005。

Windows Update



排查

1. 查看 `c:\windows\logs\cbs\cbs.log`，看到在解压补丁的时候就报错了，这种多是跟三方组件有关（客户装有 360 和安全狗），建议客户卸载，客户不同意卸载。

```

[FX] DeFacement: http://80070005_code/00017
[CS] Failed to query interface passed in handler for IID_ICbsUIHandler. [HRESULT = 0x80070005 - E_ACCESSDENIED]

```

2. 收集 procmon 日志，看到安全狗一直在对文件在进行读写请求。

```

8:3... SafeDogGuard... 1760 QueryDirectory C:\Windows\SoftwareDistribution\Download\1841993b6b4919459abeb1012a94... SUCCESS Filter:
8:3... SafeDogGuard... 1760 CloseFile C:\Windows\SoftwareDistribution\Download\1841993b6b4919459abeb1012a94... SUCCESS
8:3... SafeDogGuard... 1760 CreateFile C:\Windows\SoftwareDistribution\Download\1841993b6b4919459abeb1012a94... SUCCESS Desired
8:3... SafeDogGuard... 1760 QueryBasic C:\Windows\SoftwareDistribution\Download\1841993b6b4919459abeb1012a94... SUCCESS Creatio
8:3... SafeDogGuard... 1760 CloseFile C:\Windows\SoftwareDistribution\Download\1841993b6b4919459abeb1012a94... SUCCESS

```

解决方案

卸载安全狗后，补丁成功安装。

案例 3

安装补丁报错 80070005。



排查

需要查看 `c:\windows\windowsupdate.log` (主要是下载过程) 和 `c:\windows\logs\cs` (主要是安装过程)，看到报错 `Failed to query interface passed in handler for IID_ICbsUIHandler. [HRESULT = 0x80070005 - E_ACCESSDENIED]`。

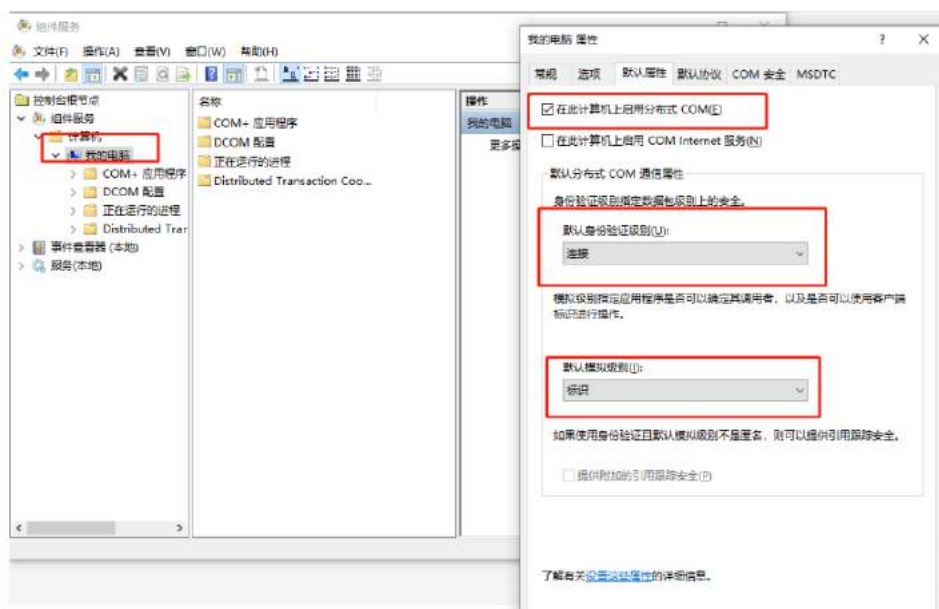
ACCESSDENIED 报错表示拒绝访问，一般怀疑是三方组件的影响，禁用三方服务

后，报错依旧。

```
2019-05-23 16:00:20, info: SFX Ended SFX phase: Remove and Uninstall Job
2019-05-23 16:00:20, error: CBS Failed to query interface passed in handler for IID_ICMSTHandler. [HRESULT = 0x80070005 - E_ACCESSDENIED]
```

解决方案

运行 dcomcnfg 打开组件服务，在组件服务——计算机——我的电脑上点击右键——属性，按如下截图所示设置。



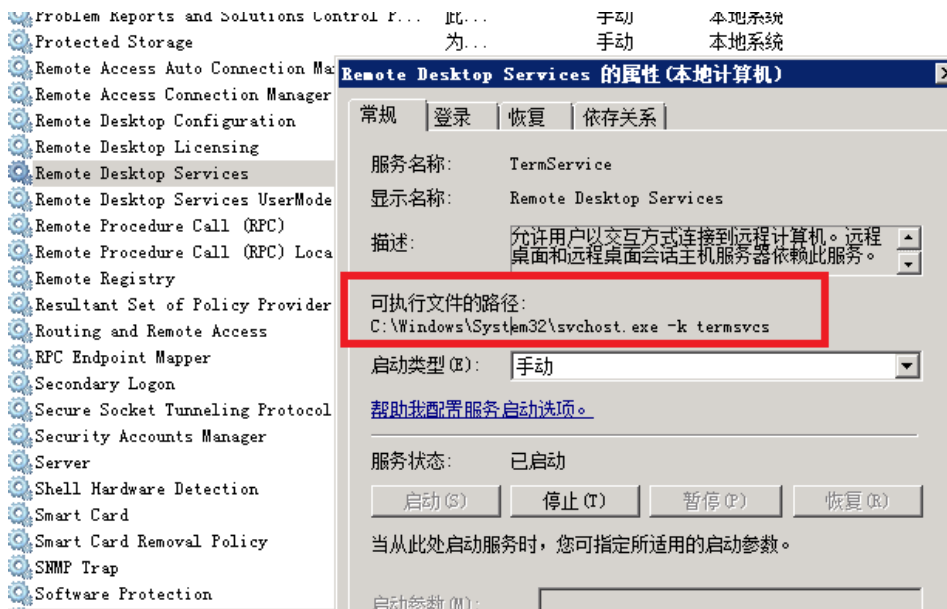
第五章 windows 服务问题排查

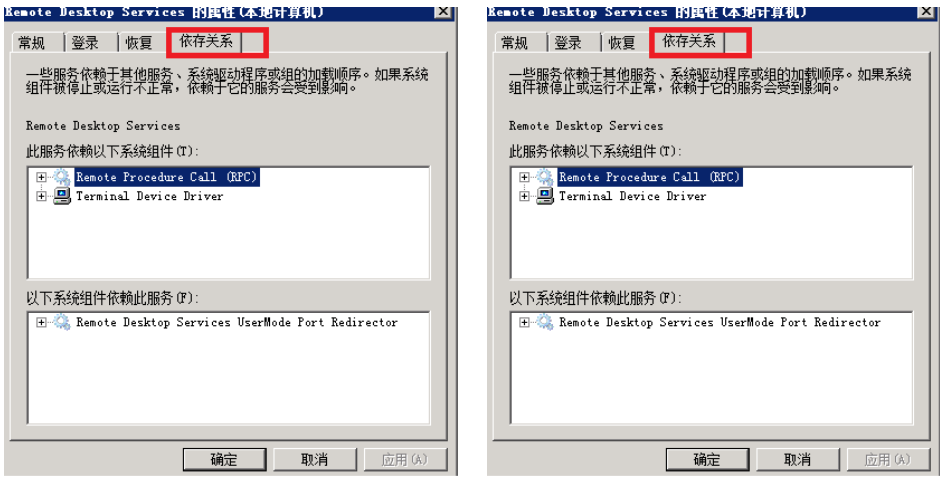
服务启动失败？2 步轻松搞定

简介：本篇文章带你从几大方面排查服务启动失败的问题。

服务启动失败的问题，从以下几个方面进行排查：

1. 服务的属性信息是否正确，包括可执行文件的路径，登录身份，依存关系。





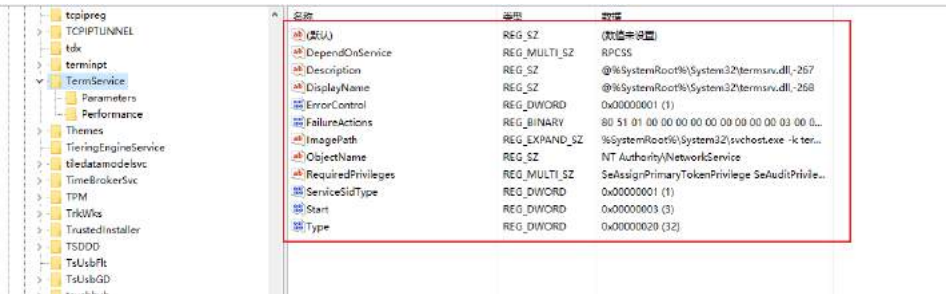
2. 服务对应的注册表各键值是否正确，注册表权限是否正常。

注册表路径: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\<服务名称>`

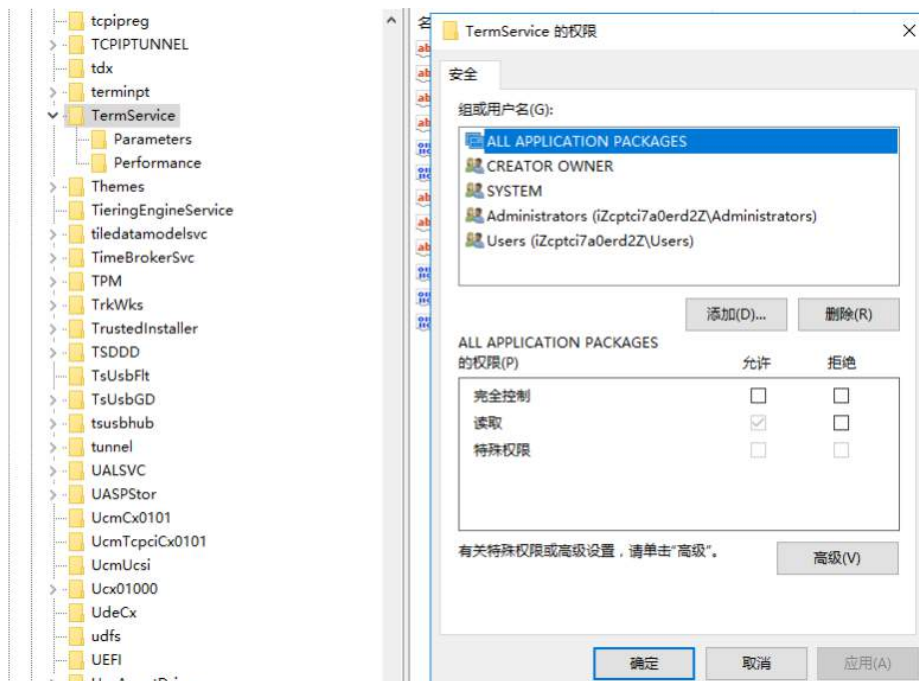
比如 Remote DesktopServices 服务名称是 TermService，对应路径就是

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\TermService`

a. 各项键值是否正确。



b. 权限是否正确。

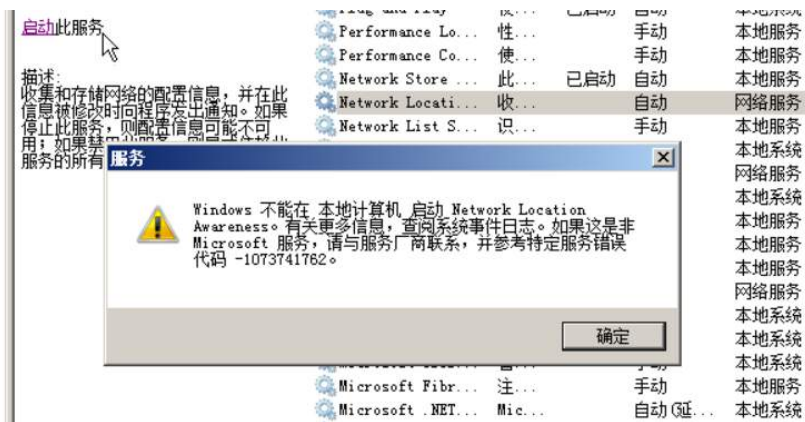


服务启动报错“不能在本地计算机启动”

简介：本文分享服务启动报错“不能在本地计算机启动”的案例。

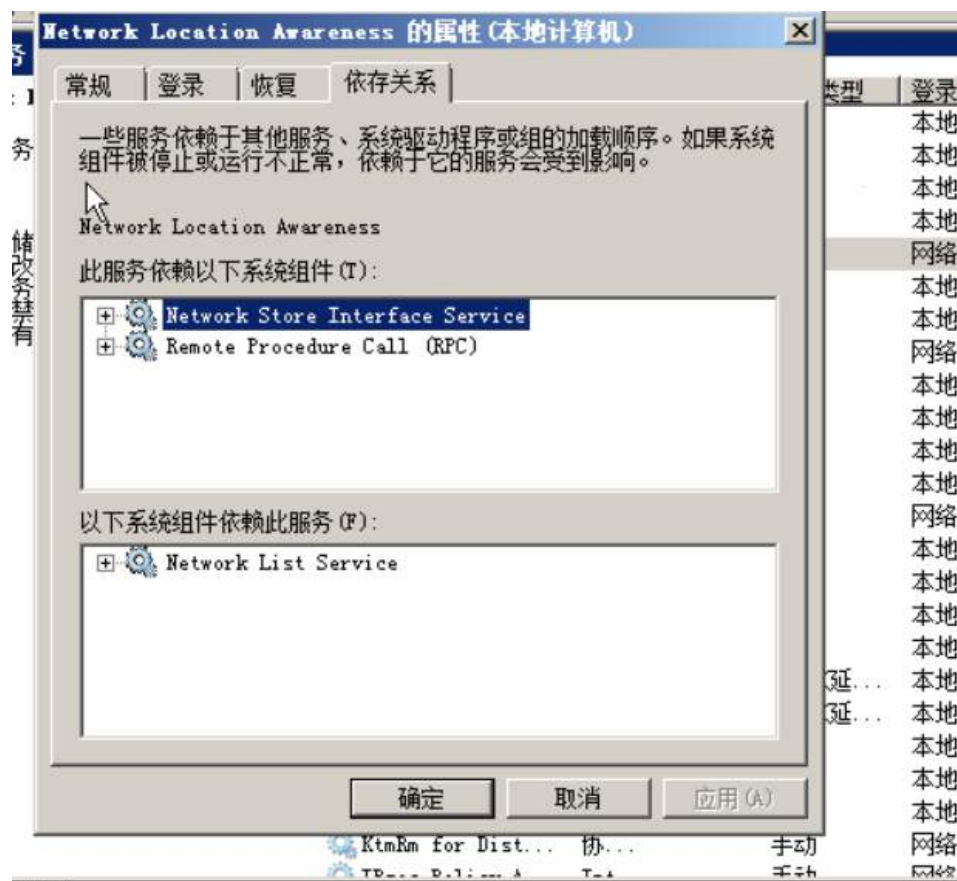
问题现象

NetworkLocation Awareness 服务无法启动，报错如下。



排查

1. 此类报错代码并不常见，从错误代码没有更多线索。查看服务属性，依存关系缺少了 tcpip 协议驱动程序。



2. 此类问题的话，需要找到一台相同系统版本的正常机器，手动替换该服务的注册表。有如下方案：

- (1) 找一台正常机器的注册表文件导出后复制到当前实例，进行导入。

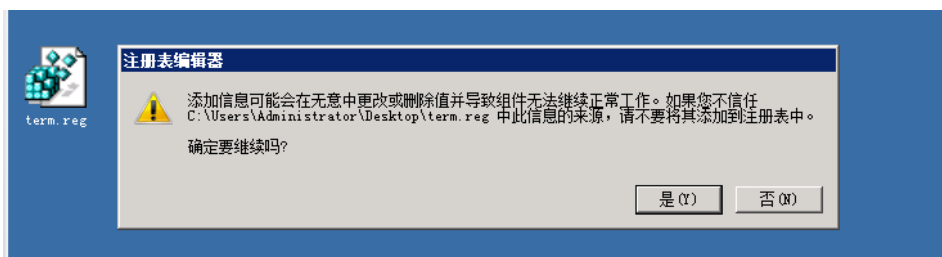
注册表导出：

右键注册表，选择导出即可。



注册表导入：

双击 .reg 文件，选择是即可。



- (2) 替换系统当前的 system 注册表 (此操作可能会引起某些配置和应用的丢失，谨慎使用)。

把系统盘挂载到其他实例，挂载步骤请参考 https://help.aliyun.com/document_detail/146752.html。

2008 之后系统

服务器备份注册表路径为: `Windows\System32\config\RegBack`

名称	修改日期	类型	大小
DEFAULT	2018/9/8 14:55	文件	252 KB
DEFAULT.LOG1	2018/5/25 14:53	LOG1 文件	0 KB
DEFAULT.LOG2	2018/5/25 14:53	LOG2 文件	0 KB
SAM	2018/9/8 14:55	文件	24 KB
SAM.LOG1	2018/5/25 14:53	LOG1 文件	0 KB
SAM.LOG2	2018/5/25 14:53	LOG2 文件	0 KB
SECURITY	2018/9/8 14:55	文件	32 KB
SECURITY.LOG1	2018/5/25 14:53	LOG1 文件	0 KB
SECURITY.LOG2	2018/5/25 14:53	LOG2 文件	0 KB
SOFTWARE	2018/8/28 18:29	文件	80,876 KB
SOFTWARE.LOG1	2018/5/25 14:53	LOG1 文件	0 KB
SOFTWARE.LOG2	2018/5/25 14:53	LOG2 文件	0 KB
SYSTEM	2018/9/8 14:55	文件	16,720 KB
SYSTEM.LOG1	2018/5/25 14:53	LOG1 文件	0 KB
SYSTEM.LOG2	2018/5/25 14:53	LOG2 文件	0 KB

替换步骤

1. 把系统盘挂载到其他实例，找到源实例的系统盘，假设为 D 盘，将 `D:\windows\system32\config\system` 重命名为 `system.old` (万一重启仍然有问题，我们可以将该文件重命名成 `system` 进行恢复)。
2. `D:\Windows\System32\config\RegBack\system` 拷贝至 `D:\windows\system32\config`。

注：备份注册表可能比较旧，让客户确认一下应用和数据情况。

2003 系统

服务器备份注册表路径在 `WINDOWS\repair`。

名称	大小	类型	修改日期	属性
default	228 KB	文件	2018-5-29 22:39	A
ntuser.dat	228 KB	DAT 文件	2018-5-29 22:32	A
sam	24 KB	文件	2018-5-29 22:39	A
secsetup.inf	790 KB	安装信息	2018-5-29 22:32	A
security	36 KB	文件	2018-5-29 22:39	A
setup.log	267 KB	文本文档	2018-5-29 22:32	A
software	15,220 KB	文件	2018-5-29 22:39	A
system	1,240 KB	文件	2018-5-29 22:39	A

替换步骤

1. 把系统盘挂载到其他实例，找到源实例的系统盘，假设为 D 盘，将 `D:\windows\system32\config\system` 重命名为 `system.old`(万一重启仍然有问题，我们可以将该文件重命名成 `system` 进行恢复)
2. `D:\WINDOWS\repair\system` 拷贝至 `D:\windows\system32\config`。

注：备份注册表可能比较旧，替换后需要确认一下应用和数据情况。

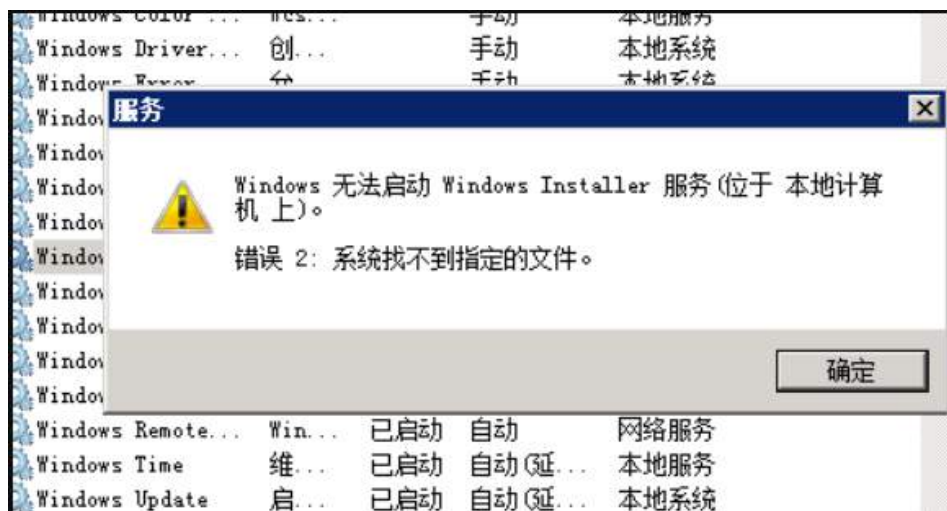
卸载系统盘，挂回源实例 (https://help.aliyun.com/document_detail/146752.html)，启动机器。

服务启动失败“系统找不到指定文件”

简介：服务启动失败“系统找不到指定文件”的案例分享。

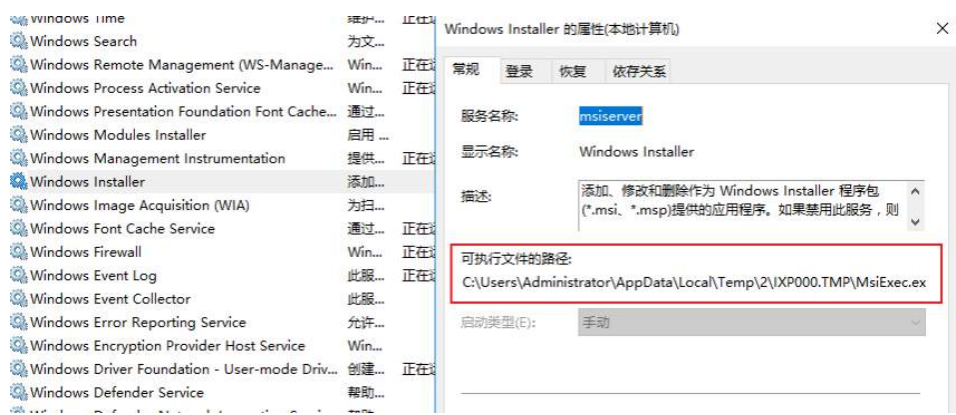
问题现象

Windows installer 服务启动失败。



排查

1. 首先从报错来看，提示就是找不到对应文件，查看服务属性，可执行文件的路径被篡改改成 `C:\Users\Administrator\AppData\Local\Temp\2\IXP000.TMP\MsiExec.exe`。



2. 找到对应注册表 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\msiserver`

将 ImagePath 改为默认 `%systemroot%\system32\msiexec.exe /v` 即可。

	名称	类型	数据
> MSDTC Bridge 4.0.0.0	(默认)	REG_SZ	(数值未设置)
> Msfs	DependOnService	REG_MULTI_SZ	rpcss
> msgpiwin32	Description	REG_SZ	@%SystemRoot%\system32\msimg.dll,-32
> mshidkmdf	DisplayName	REG_SZ	@%SystemRoot%\system32\msimg.dll,-27
> mshidmndf	ErrorControl	REG_DWORD	0x00000001 (1)
> msisadrv	FailureActions	REG_BINARY	84 03 00 00 00 00 00 00 00 00 03 00 00
> MSISCSI	ImagePath	REG_EXPAND_SZ	%systemroot%\system32\msiexec.exe /v
> msiserver	ObjectName	REG_SZ	LocalSystem
> MsLbfProvider	RequiredPrivileges	REG_MULTI_SZ	SeTcbPrivilege SeCreatePagefilePrivilege SeL...
> MsLdp	ServiceSidType	REG_DWORD	0x00000001 (1)
> MsRPC	Start	REG_DWORD	0x00000003 (3)
> MSSCNTRS	Type	REG_DWORD	0x00000010 (16)
> mssmbios			
> MSSQL\$MICROSOFT#WID			
> MTConfig			
> Mup			

如何手动恢复服务

简介：本文教你如何手动恢复服务。

问题背景：

如果替换过 system 注册表或者意外删除了服务，可尝试通过注册表恢复服务。

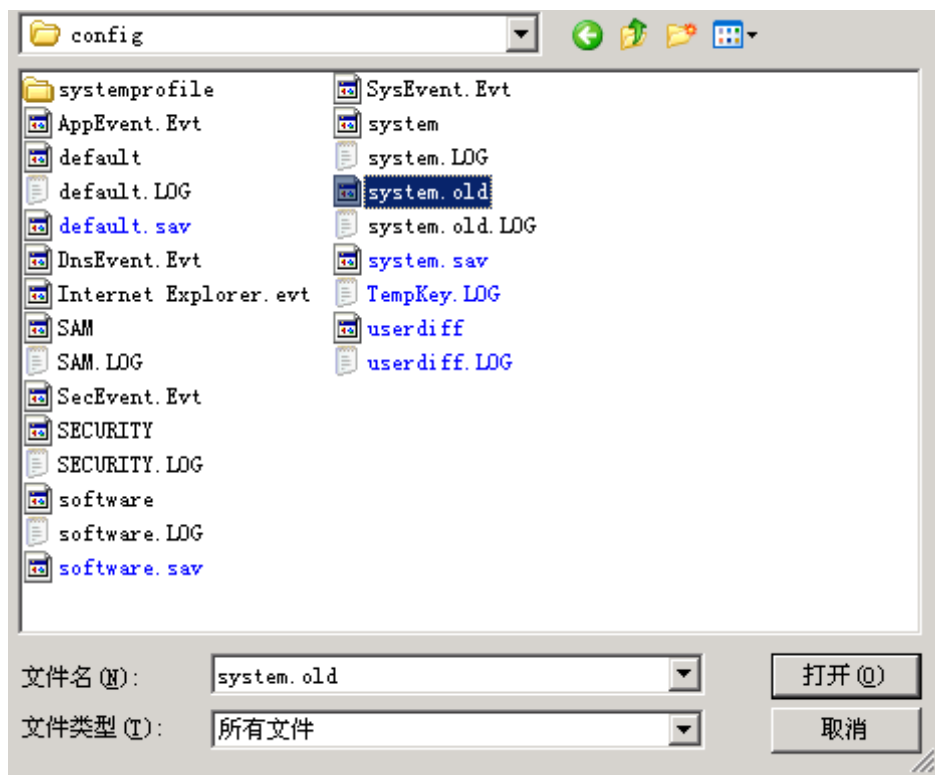
具体步骤：

服务对应的注册表路径是 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services< 服务名称 >`，可尝试以下步骤恢复服务：

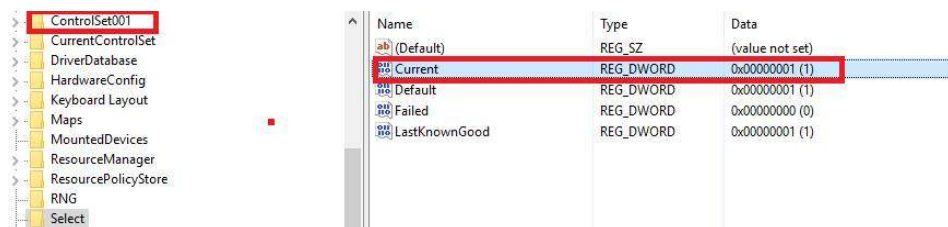
1. 将替换的原始注册表 load 起来，查看服务的配置信息。
 - a. cmd 命令行输入 regedit。
 - b. 找到 HKEY_LOCAL_MACHINE, 然后点击文件，选择加载配置单元。



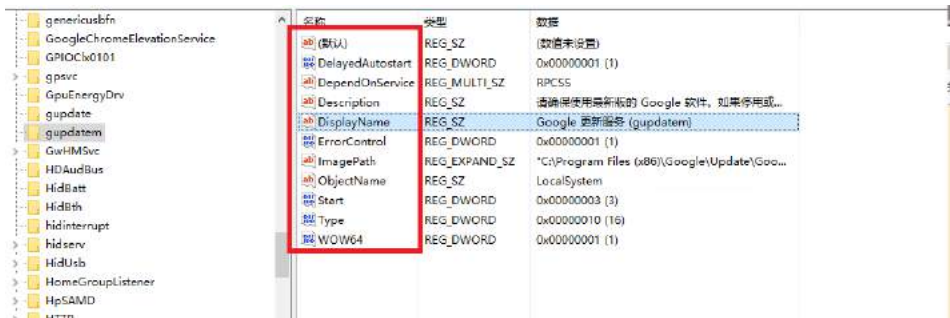
c. 找到之前替换的原始注册表，比如 system.old，任意命名（例如 test）。



d. 展开 test，查看 select 项，current 值为 1，则我们应该去找 ControlSet001。



展开 ControlSet001，展开 services，找到对应服务，以 Google 更新服务 (gupdatem) 为例，先确认下各项属性信息。



2. 运行以下命令行创建服务。

注意: binpath 对应 ImagePath。

type 对应类型和注册表键值:

注册表键值 (Type)	服务类型
0x00000002	filesystem
0x00000001	kernel
0x00000008	rec
0x00000010	own
0x00000020	share
0x00000100	interact

start 对应类型和注册表键值:

注册表键值 (start)	启动类型
0x00000000	Boot
0x00000001	system
0x00000002	auto
0x00000003	manual
0x00000004	disabled

error 对应 ErrorControl，注册表键值对应如下：

注册表键值 (ErrorControl)	error 类型
0x00000000	ignore
0x00000001	normal
0x00000002	severe
0x00000003	critical

depend 对应 DependOnService，多个服务的话以 / 分隔。

有些注册表项不在创建服务参数中，之后再手动添加即可。

sc create 的各项参数可以在命令行直接查询：

```
C:\Program Files\PuTTY>sc create
描述：      在注册表和服务数据库中创建服务项。
用法：      sc <server> create [service name] [binPath= ] <option1> <option2>...
选项：
注意：      选项名称包括等号。
            等号和值之间需要一个空格。
type= <own|share|interact|kernel|filesys|rec>
            (默认 = own)
start= <boot|system|auto|demand|disabled|delayed-auto>
            (默认 = demand)
error= <normal|severe|critical|ignore>
            (默认 = normal)
binPath= <BinaryPathName>
group= <LoadOrderGroup>
tag= <yes|no>
depend= <依存关系(以 / (斜杠) 分隔)>
obj= <AccountName|ObjectName>
            (默认 = LocalSystem)
DisplayName= <显示名称>
password= <密码>
```

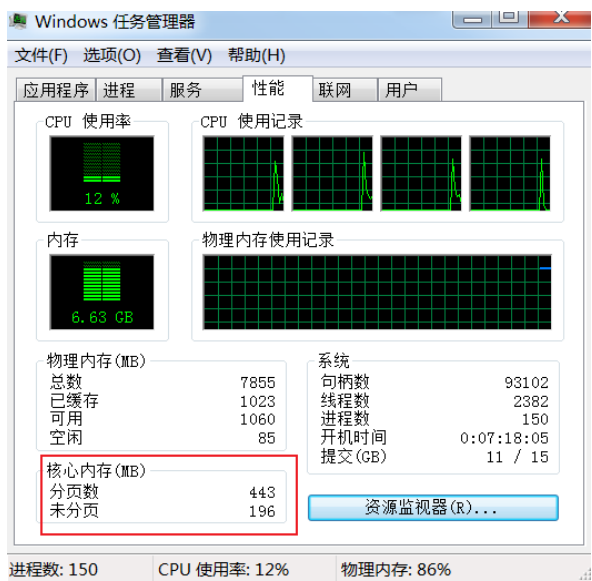
第六章 windows 性能问题排查

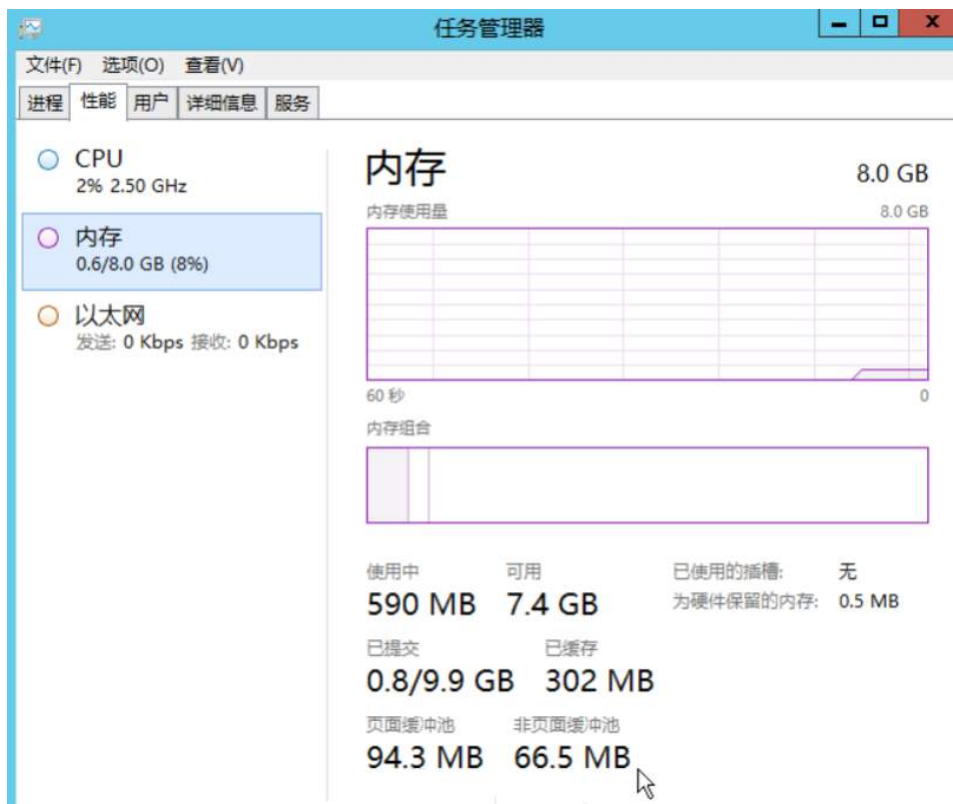
占用内存高 – 分页数 / 未分页

简介：任务管理器看到内存占用高，内存占用主要是分页或未分页 (windows 2012 之后显示是页面 / 非页面缓冲池)。

问题现象

任务管理器看到内存占用高，内存占用主要是分页或未分页 (windows 2012 之后显示是页面 / 非页面缓冲池)。





排查步骤

1. 下载 windows driver kit 并安装。

<https://docs.microsoft.com/zh-cn/windows-hardware/drivers/download-the-wdk>



步骤 2：安装 WDK 适用于 Windows 10 版本 1803

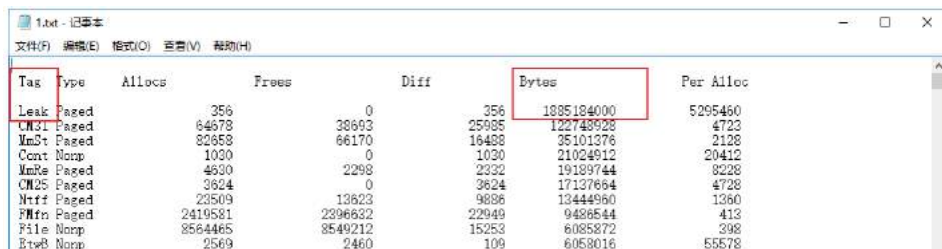
- 下载 WDK 适用于 Windows 10 版本 1803

2. 默认 poolmon 的路径是 C:\Program Files(x86)\Windows Kits\10\Tools\x64 或 C:\ProgramFiles (x86)\Windows Kits\10\Tools\x86

3. 运行如下命令:

```
cd <poolmon.exe 的路径>
poolmon -u -n c:\1.txt
```

4. 查看 1.txt, 在 Bytes 这列找到占用 pool 最高的 tag。

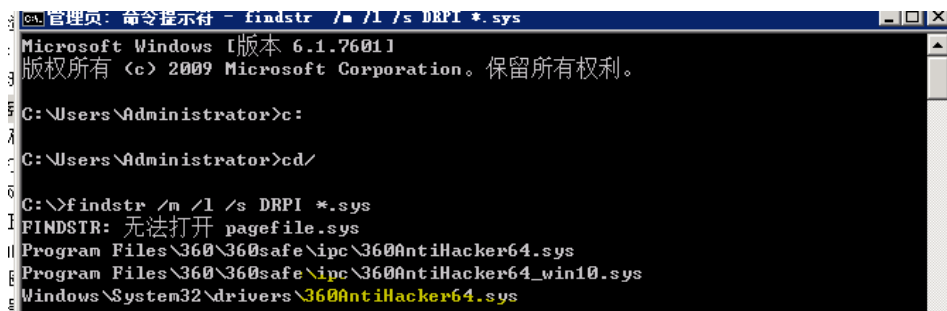


Tag	Type	Allocs	Frees	Diff	Bytes	Per Alloc
Leak	Paged	356	0	356	1885184000	5295460
CM31	Paged	64978	38693	25985	122748928	4723
VMSt	Paged	82859	66170	16488	35101376	2128
Cont	Nonp	1030	0	1030	21024612	20412
VMRe	Paged	4630	2298	2332	19189744	8228
CM25	Paged	3624	0	3624	17137664	4728
MMf	Paged	23509	13623	9886	13444960	1360
PMfn	Paged	2419581	2296632	22949	9486544	413
File	Nonp	8564465	8549212	15253	6085872	398
EtwB	Nonp	2569	2460	109	6058016	55578

5. 之后查找 tag 对应的组件。

右击 cmd, 选择以管理员身份运行以下命令:

```
c:
cd\
findstr /m /l /s Leak*.sys (标黄部分换成具体 tag)
```



6. 根据查到的组件找到对应的应用, 建议升级或临时卸载。

内存占用高 -AWE

简介: 分享一个 AWE 占用内存高的案例。

问题现象

内存占用高，任务管理器看不到问题，使用 RAMMAP，看到 AWE 占用了大部分内存

<https://docs.microsoft.com/en-us/sysinternals/downloads/rammap>



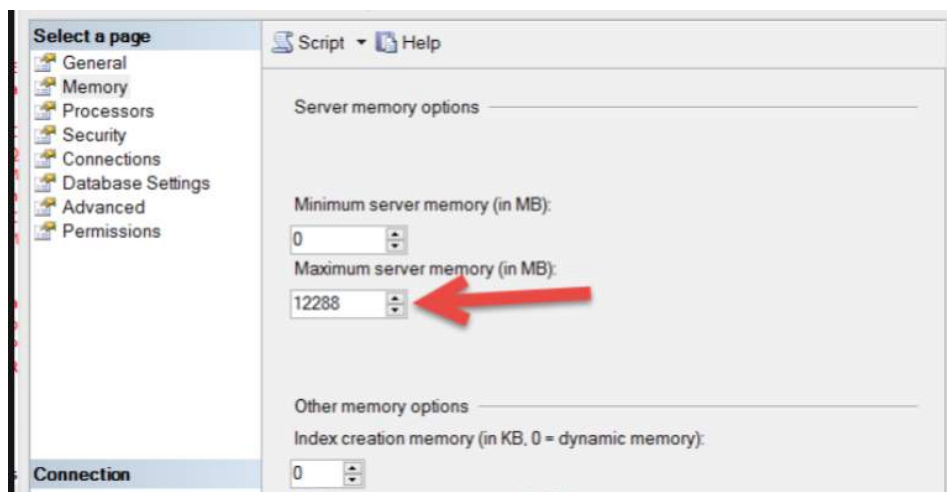
Usage	Total	Active	Standby	Modified	Modified
Total	8,388,088 K	7,282,532 K	212,012 K	15,672 K	
AWE	5,718,016 K	5,718,016 K			

解决方案:

AWE 占用内存高的问题一般发生在 SQL 服务器上，一般建议客户调整 “maximum server memory”。

<https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/server-memory-server-configuration-options?view=sql-server-ver15>

如果服务器上只安装了 SQL 应用，建议给系统留 2-4G 内存，其他内存留给 SQL。



可以参考如下指标：

物理内存

MaxServerMem Setting

2GB	1500
4GB	3200
6GB	4800
8GB	6400
12GB	10000
16GB	13500
24GB	21500
32GB	29000
48GB	44000
64GB	60000
72GB	68000
96GB	92000
128GB	124000

explorer.exe 占用 cpu 或者内存高

简介: 本文分享一个 explorer.exe 占用 cpu 或者内存高的案例。

问题现象

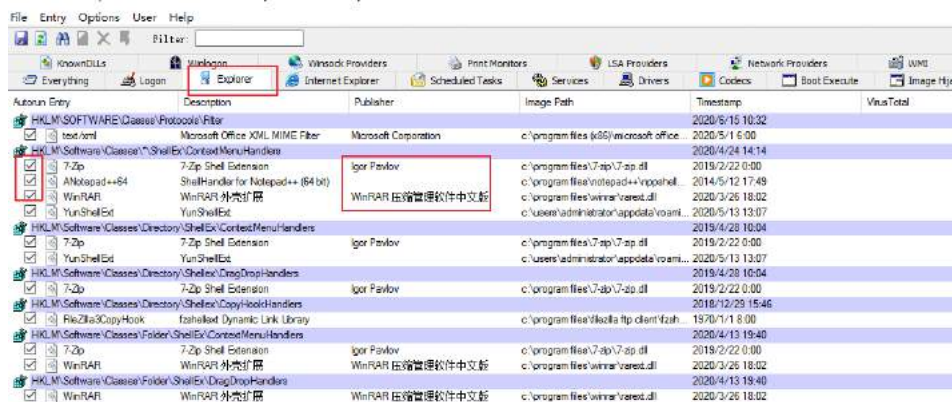
explorer.exe 占用 cpu 或者内存高, 或者无响应情况。

处理方案

1. 下载 autoruns 工具。

<https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns>

2. 运行 autoruns 工具 (右击选择以管理员身份运行, 64 位系统选择 Autoruns64), 找到 explorer, 把所有非 Microsoft 的勾都去掉 (注: 这个步骤不会影响已安装应用, 只是把 explorer 下的 hook 取消掉)。



3. 重启 explorer.exe 观察。

C 盘空间占满? 主要是这 2 个原因

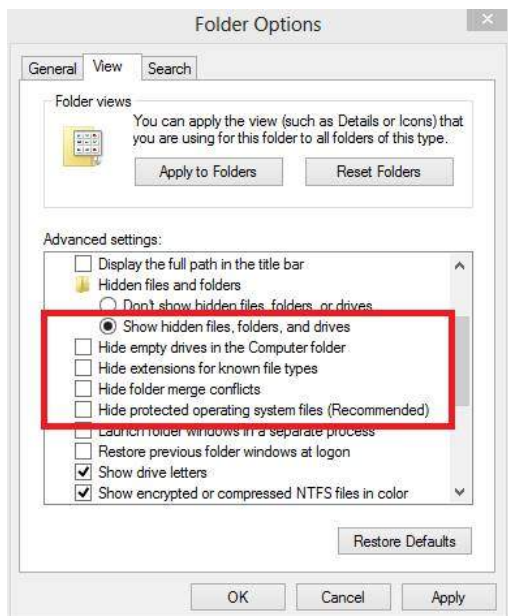
C 盘空间占满的问题，首先要明确一下，空间被占满就是说明有文件把空间给占用了，右键所有文件属性看到差距很大的原因，总结有如下两个：

1. 隐藏文件（包括 pagefile.sys）。
2. 系统管理员没有权限访问的文件比如 System volume information 这个文件夹。

排查方案如下：

1. 将隐藏文件设为可见。

Computer>Local Disk (C)>View>Options>Change folder and search options, 显示隐藏文件。



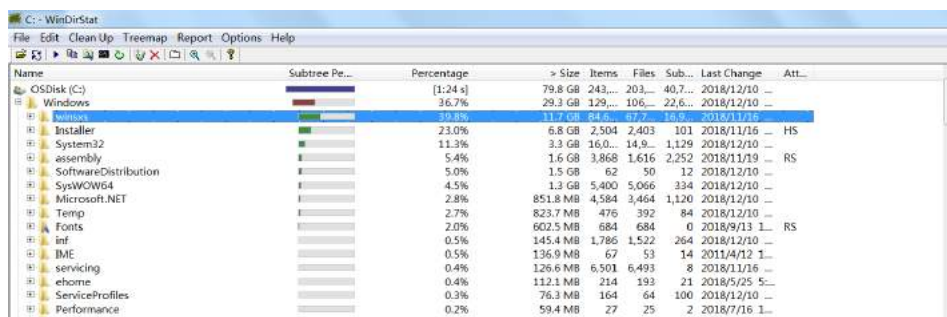
2. 默认情况下, System volumeinformation 这个文件夹系统管理员没有权限访问, 所以大小为 0。

运行以下命令行赋予管理员完全控制权限这样才知道这个文件夹的实际大小。用管理员权限运行以下命令行:

```
takeown /f "C:\system volumeinformation" /r /a
icacls "c:\system volumeinformation" /grant builtin\administrators:F
```

3. 使用工具 windirstat 或者 treesize 工具, 这两个工具都可以非常直观的显示每个目录及文件夹占用大小。

<https://windirstat.net/>



4. 如果以上两个工具也未能定位到问题, 说明还是存在管理员没有权限查看的文件, 比如:

IIS 服务器: 主要是 log 文件, 默认是如下路径: C:\inetpub\logs\LogFiles。

SQL server: 查看如下路径 C:\Program Files\Microsoft SQLServer\MS-SQL10_50.MSSQLSERVER\MSSQL。

PS: 第三步中使用工具如果看到占用最多的是 winsxs 或者任何系统目录的话, 不要轻易去清除这个文件夹, 而是应该查看除了这个文件夹以外哪些文件占用了磁盘空间。

Winsxs 相当于系统的备份数据库, 不可以完全删除或者移除, 一般来讲清理的空间非常有限, 如果坚持要清理, 请参考如下链接:

2008R2:

<https://support.microsoft.com/zh-cn/help/2852386/disk-cleanup-wizard-addon-lets-users-delete-outdated-windows-updates-o>

2012&2012R2:

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-8.1-and-8/dn251565\(v=win.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-8.1-and-8/dn251565(v=win.10)?redirectedfrom=MSDN)

第七章 windows 系统相关问题排查

如何追踪 Windows 进程自动异常退出

简介: 教你如何追踪 Windows 进程自动异常退出。

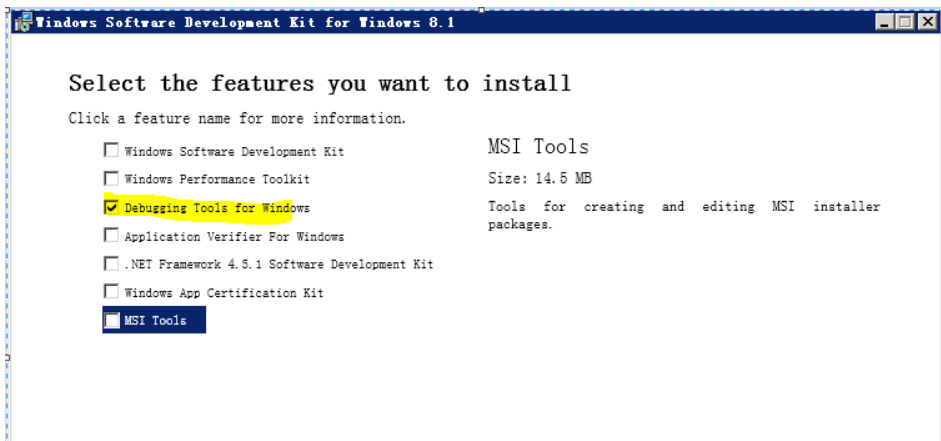
对于进程突然退出的问题，我们可以使用 gflags 进行监控：

1. 点击链接，进行安装。

<https://developer.microsoft.com/zh-cn/windows/downloads/sdk-archive>

Windows 8 此 SDK 发布于 2012 年 11 月，可用于创建使用 Web 技术、本机和托管代码的 Microsoft Store 应用（适用于 Windows 8 或更早版本）或者使用本机或托管编程模型的桌面应用。 [安装 >](#)

2. 安装的时候只选择 debugging tools。

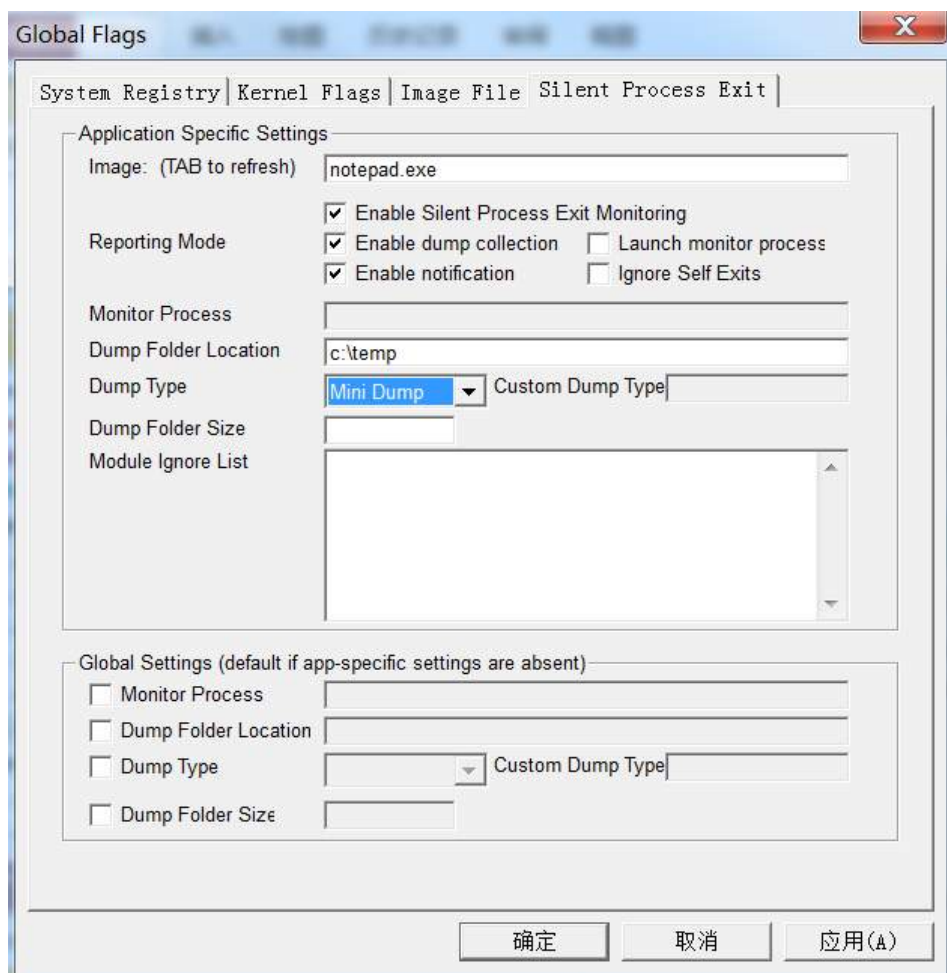


3. 安装完成后，找到 `C:\ProgramFiles (x86)\Windows Kits\8.0\Debuggers\x64`，右击 `gflags.exe` 选择“以管理员身份运行”，选择“SilentProcess Exit”。

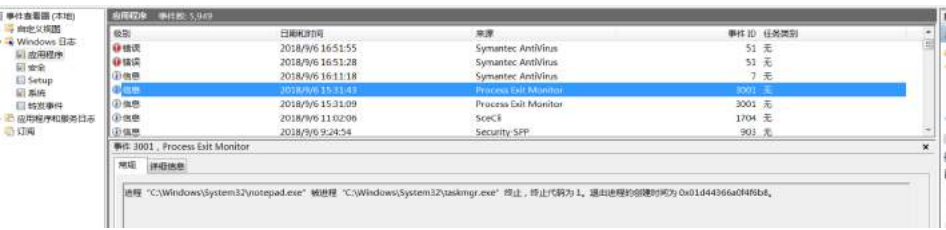
在 image 填写想要监控的进程，之后勾选如下。

在 dump folder location 填写存放 dump 的路径。

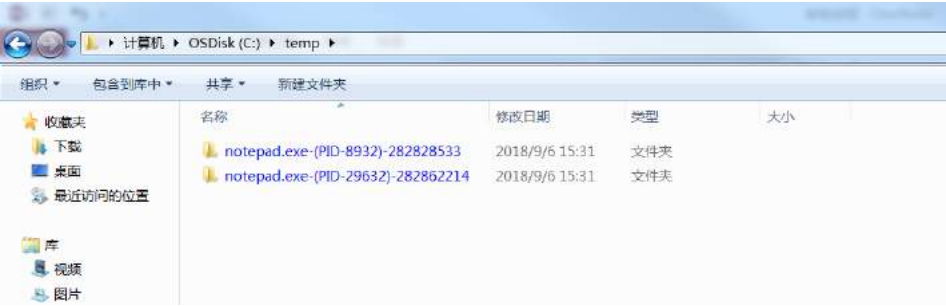
点击确定后重启机器生效。



4. 之后如果进程被终止，会在应用程序日志中有如下记录：



刚才设置的 dump 路径也会生成以进程命名的 dump 文件：



进程 crash 报错 1000

简介: 进程 crash, 在应用程序日志里看到有 1000 的报错。

问题现象

进程 crash, 在应用程序日志里看到有 1000 的报错。

2008R2 之后的系统可以配置 WER, 收集进程 dump 进一步分析, 配置步骤:

1. 运行 regedit.exe 去创建 LocalDumps key:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting
```

2. 在新建的 LocalDumps key, 创建一下键值:

```
Value name: DumpFolder  
Type: REG_EXPAND_SZ
```

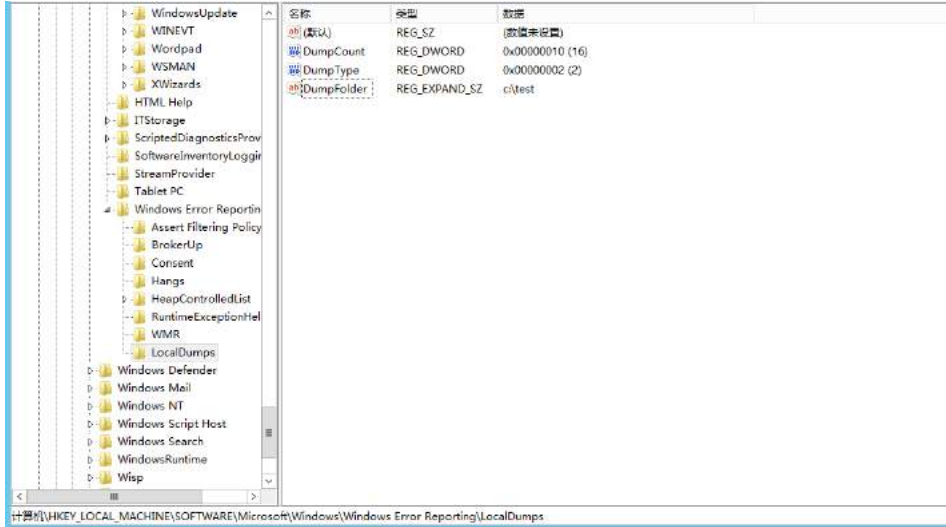
Value: 希望创建 Dump 的路径 . 默认路径是:

```
%LOCALAPPDATA%\CrashDumps
```

```
Value name: DumpCount  
Type: REG_DWORD  
Value: 10  
Note: 设置最大 Dump 数量 .
```

```
Value name: DumpType  
Type: REG_DWORD  
Value: 2  
Note: 0 = custom, 1= mini dump (default), 2 = full dump
```

排查阶段我们需要设置 full dump 以获取足够信息。



| windows 桌面显示黑屏或者蓝屏

简介: windows 机器登录后桌面显示蓝屏。

问题现象

windows 机器登录后桌面显示蓝屏。

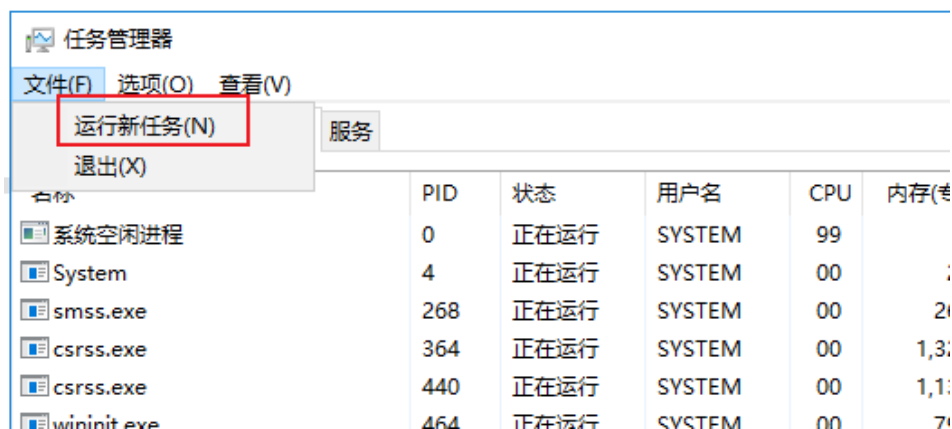


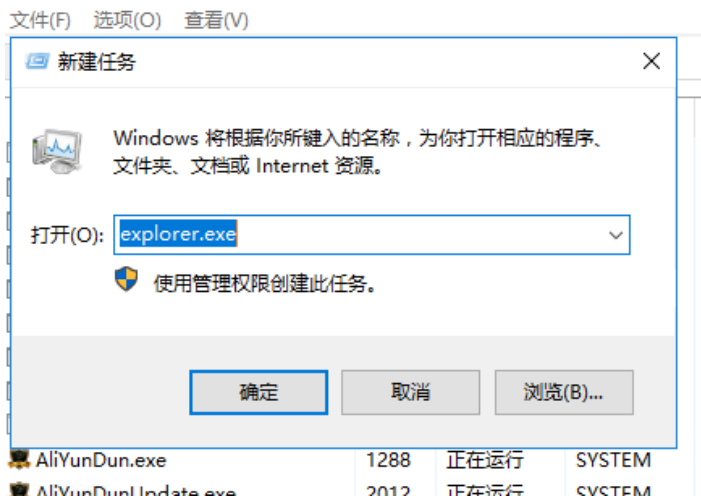
处理方案

1. ctrl+alt+delete 调出任务管理器，之后查看是否存在 explorer.exe。

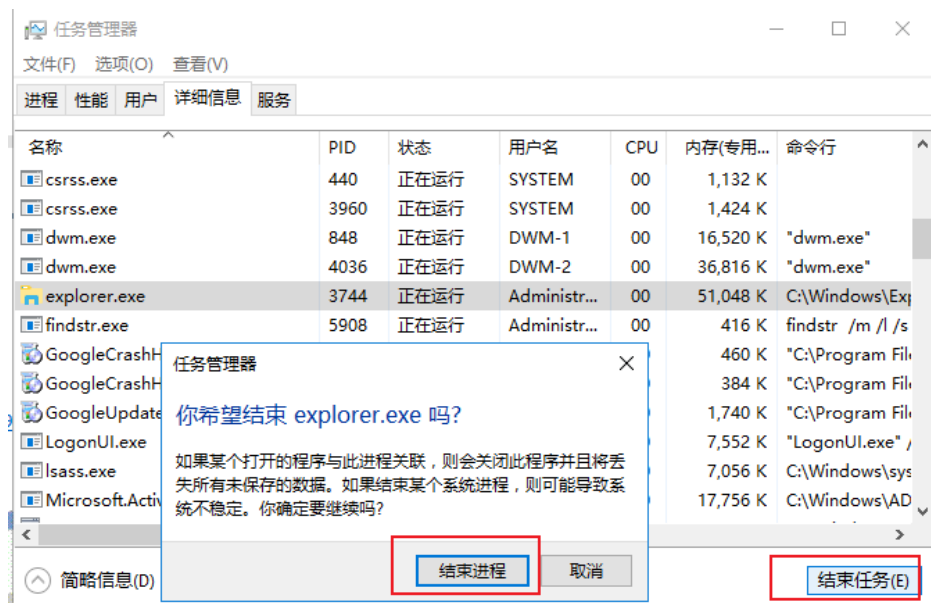


2. explorer.exe 不存在的情况下，文件》新建任务，输入 explorer.exe 后可以正常看到桌面。






3. explorer.exe 存在的情况下，先将 explorer.exe 全都结束，再新建 explorer.exe。



4. 以上操作无效的话，启动 cmd 运行以下命令行（这个命令行的作用是检查系统是否存在系统文件损坏，若有会尝试修复）：

sfc /scannow



```
管理员: 命令提示符 - sfc /scannow
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>sfc /scannow

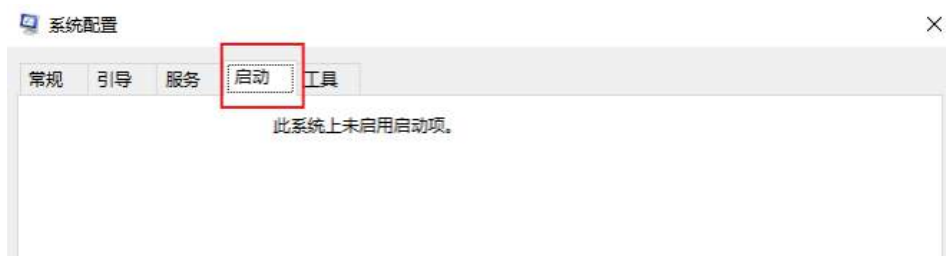
开始系统扫描。此过程将需要一些时间。
开始系统扫描的验证阶段。
验证 0% 已完成。
```

windows 异常问题 – 怀疑中毒

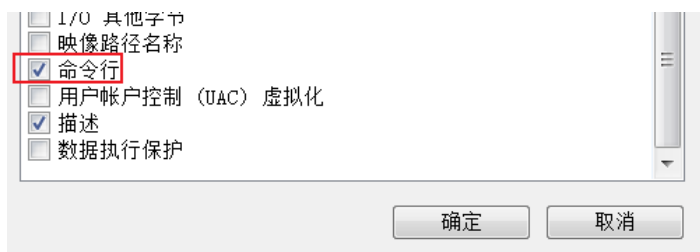
简介: windows 中毒迹象一般都表现在服务，进程和启动项里，分享该异常的排查步骤。

windows 中毒迹象一般都表现在服务，进程和启动项里，参考如下步骤排查：

1. 运行 msconfig，查看启动项。



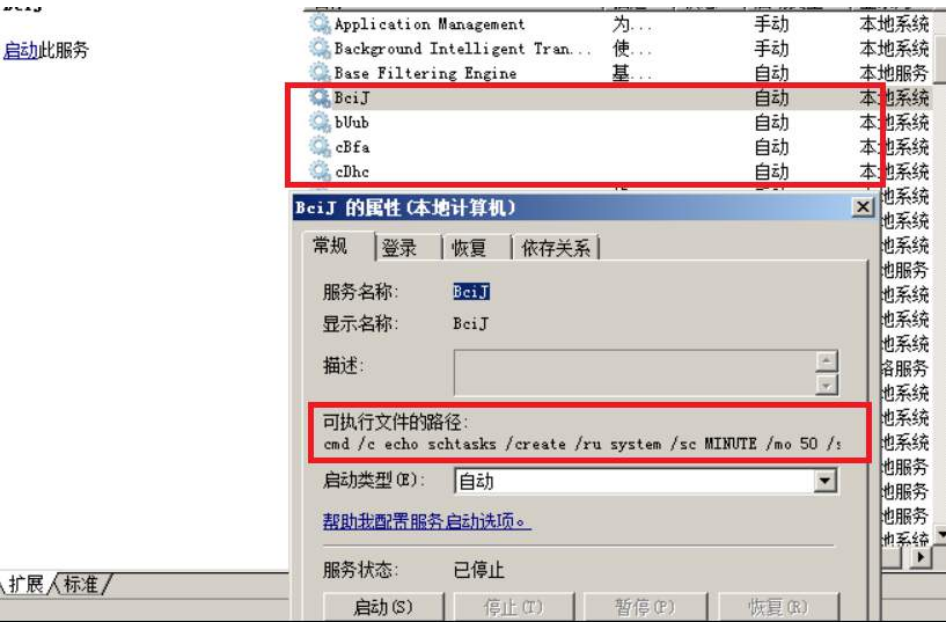
2. 任务管理器查看进程，查看《选择列》，勾选命令行。



以命令行排序，查看是否有异常路径和进程。

名称	PID	状态	用户名称	CPU	内存/专用	命令行	描述
chrome.exe	1320	正在运行	Administr...	00	15,924 K	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=gpu-process --field-trial-handle=1380,5557...	Google Chrome
chrome.exe	7748	正在运行	Administr...	00	21,960 K	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1380,5557337...	Google Chrome
chrome.exe	7852	正在运行	Administr...	00	31,972 K	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1380,5557337...	Google Chrome
chrome.exe	6320	正在运行	Administr...	00	38,888 K	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1380,5557337...	Google Chrome
chrome.exe	300	正在运行	Administr...	00	28,204 K	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1380,5557337...	Google Chrome
chrome.exe	5956	正在运行	Administr...	00	8,744 K	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1380,5557337...	Google Chrome
chrome.exe	6456	正在运行	Administr...	00	5,560 K	"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --type=renderer --field-trial-handle=1380,5557337...	Google Chrome

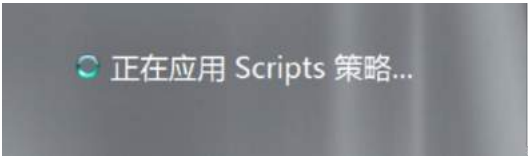
3. 查看是否有异常服务（主要从服务名称和可执行文件的路径来判断）。



以下是具体案例分析

案例 1

重启后卡在“正在应用 scripts 策略”。



排查

1. 开机按 F8 进入安全模式，可以正常启动，查看是否配置了开机或者登陆脚本，本案例并没有配置脚本。

(gpedit.msc> 计算机配置》windows 设置> 脚本 和 用户配置 >windows 设置 > 脚本)

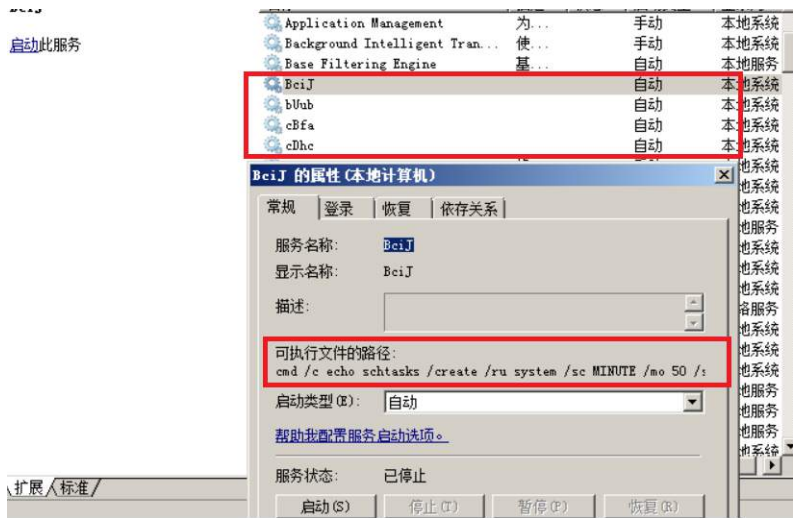


2. 尝试禁用三方服务和启动项，重启仍然卡住。

<https://support.microsoft.com/zh-cn/help/929135/how-to-perform-a-clean-boot-in-windows>

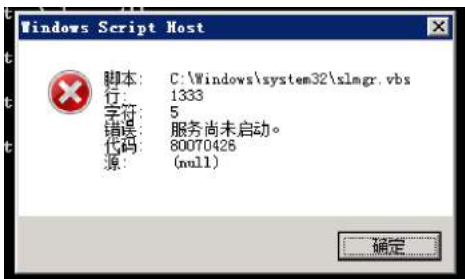
3. 安全模式没问题 说明肯定是三方问题，把三方服务和启动项禁用没有用，就说明大概率不是正常三方应用的问题。查看服务，发现有很多命名异常的服务，查看服务属性 > 可执行文件的路径，可以看到是创建了计划任务。

这些异常服务信息基本可以确认服务器已经中毒。



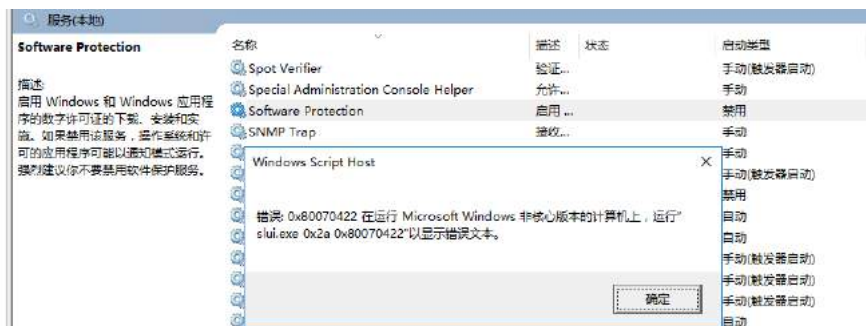
案例 2

windows 激活失败，报错如下



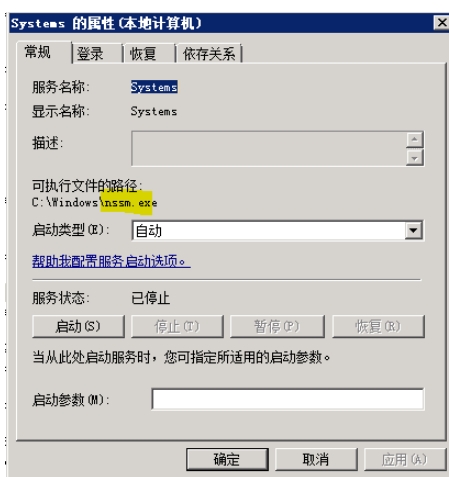
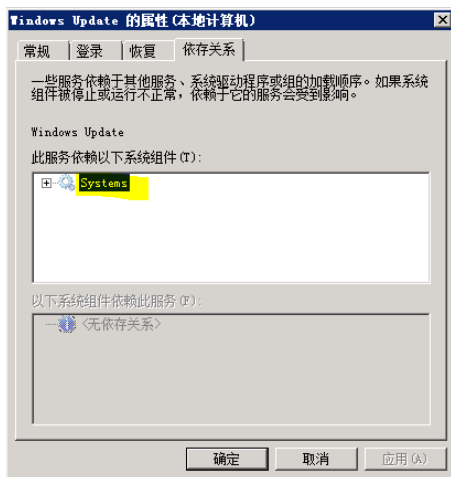
排查

1. 查看 software protection 是运行中状态 (其实这个报错并不是指 software protection 服务没启动，如果是 software protection 未启动，报错码应该是 0x80070422)



2. google 查看 80070426 多是跟补丁安装有关, 查看 windows update 服务未启动, 尝试启动失败。

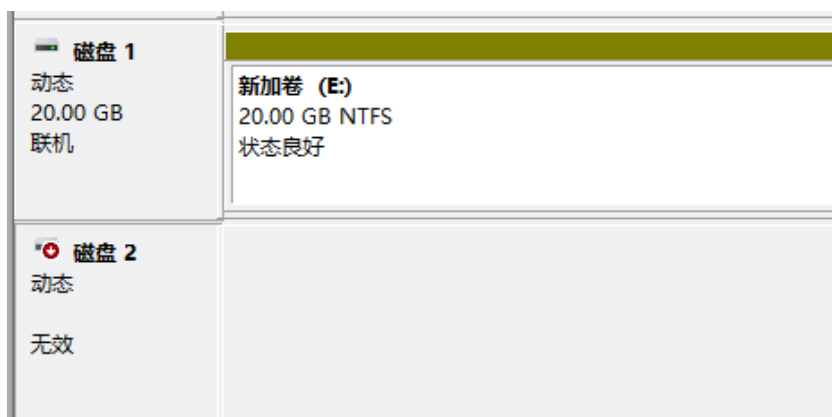
查看 windows update 属性, 依存关系不对, 而且 systems 服务对应一个异常进程。



Windows 数据恢复 – 动态盘显示无效

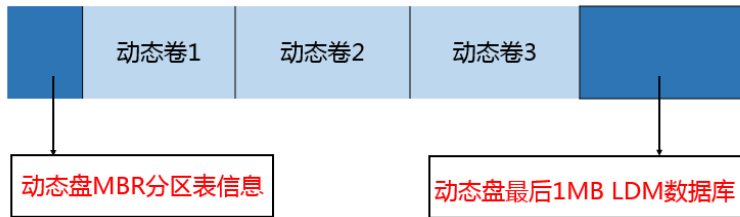
背景

很多客户在使用磁盘时选择了动态盘，又对这块动态盘创建了快照，之后在数据恢复或其他场景下用快照创建了新的磁盘，将新磁盘挂载到相同实例时，发现新磁盘显示无效。



问题原因

动态盘通过 LDM 进行管理，对于 mbr 分区，LDM 保存在磁盘的最后 1MB(如下图所示)，这 1MB 空间保存了磁盘信息，分区信息以及磁盘 id, group id 等，由于源磁盘和新磁盘最后 1MB 空间是一样的，两块盘的 ldm 数据库完全相同，对应的磁盘 id, group id 也是完全相同，导致系统只能识别一块磁盘。



可以通过微软的 LDMDump 工具查看 LDM database 的具体信息:

<https://docs.microsoft.com/en-us/sysinternals/downloads/ldmdump>

```
E:\BaiduNetdiskDownload\LdmDump>ldmdump.exe /dl

Logical Disk Manager Configuration Dump v1.03
Copyright (C) 2000-2002 Mark Russinovich

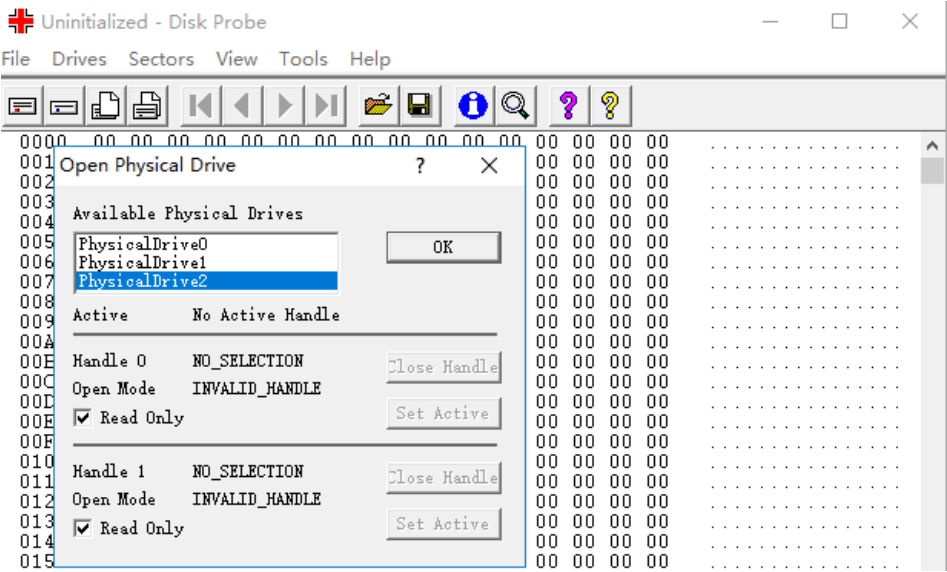
PRIVATE HEAD:
Signature           : PRIVHEAD
Version            : 2.12
Disk Id             : 984ce974-a4ee-11ea-b0f9-8d4e7aaa8b4f
Host Id             : 1b77da20-c717-11d0-a5be-00a0c91db73c
Disk Group Id       : 984ce973-a4ee-11ea-b0f9-8d4e7aaa8b4f
Disk Group Name     : iZcptci7a0erd2Z-Dg0
Logical disk start  : 3F
Logical disk size   : 27FF7C1 (20478 MB)
Configuration start : 27FF800
Configuration size  : 800 (1 MB)
Number of TOCs      : 2
TOC size            : 7FD (1022 KB)
Number of Configs   : 1
Config size         : 5C9 (740 KB)
Number of Logs      : 1
Log size            : E0 (112 KB)

TOC 0:
Signature           :
Sequence            : 0x0
Config bitmap start : 0x0
Config bitmap size  : 0x0
Log bitmap start    : 0x0
Log bitmap size     : 0x0
TOC 1:
Signature           : TOCBLOCK
Sequence            : 0x1
Config bitmap start : 0x11
Config bitmap size  : 0x5C9
Log bitmap start    : 0x5DA
Log bitmap size     : 0xE0
```

解决方案

将新磁盘在无损数据的前提下从动态盘转换到基本盘：重新配置分区表并将 system id 从 dynamic 改为 ntfs。需要借助 diskprobe 工具（包含在 Windows XP Service Pack 2 Support Tools）<https://www.microsoft.com/en-us/download/details.aspx?id=18546>

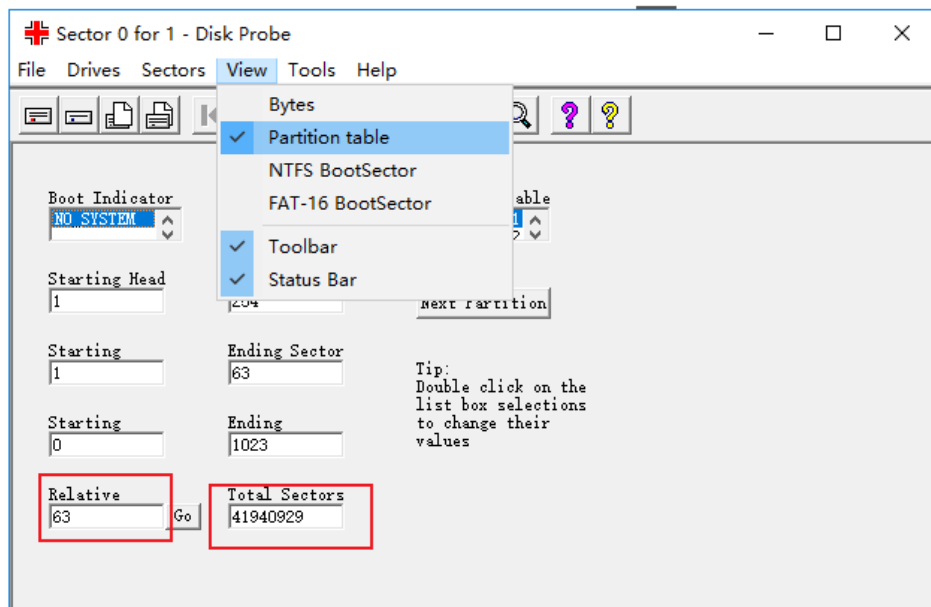
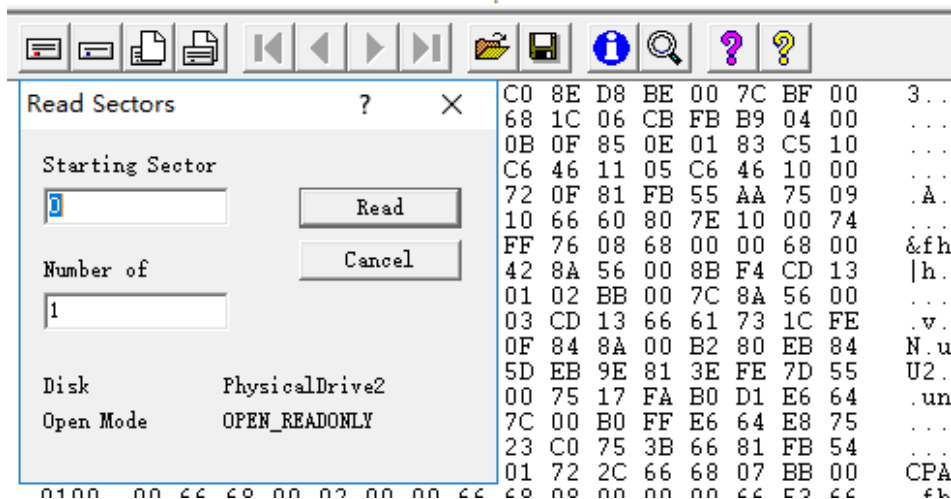
Drives 找到对应的磁盘，选择 Set Active（以 drive2 为例）



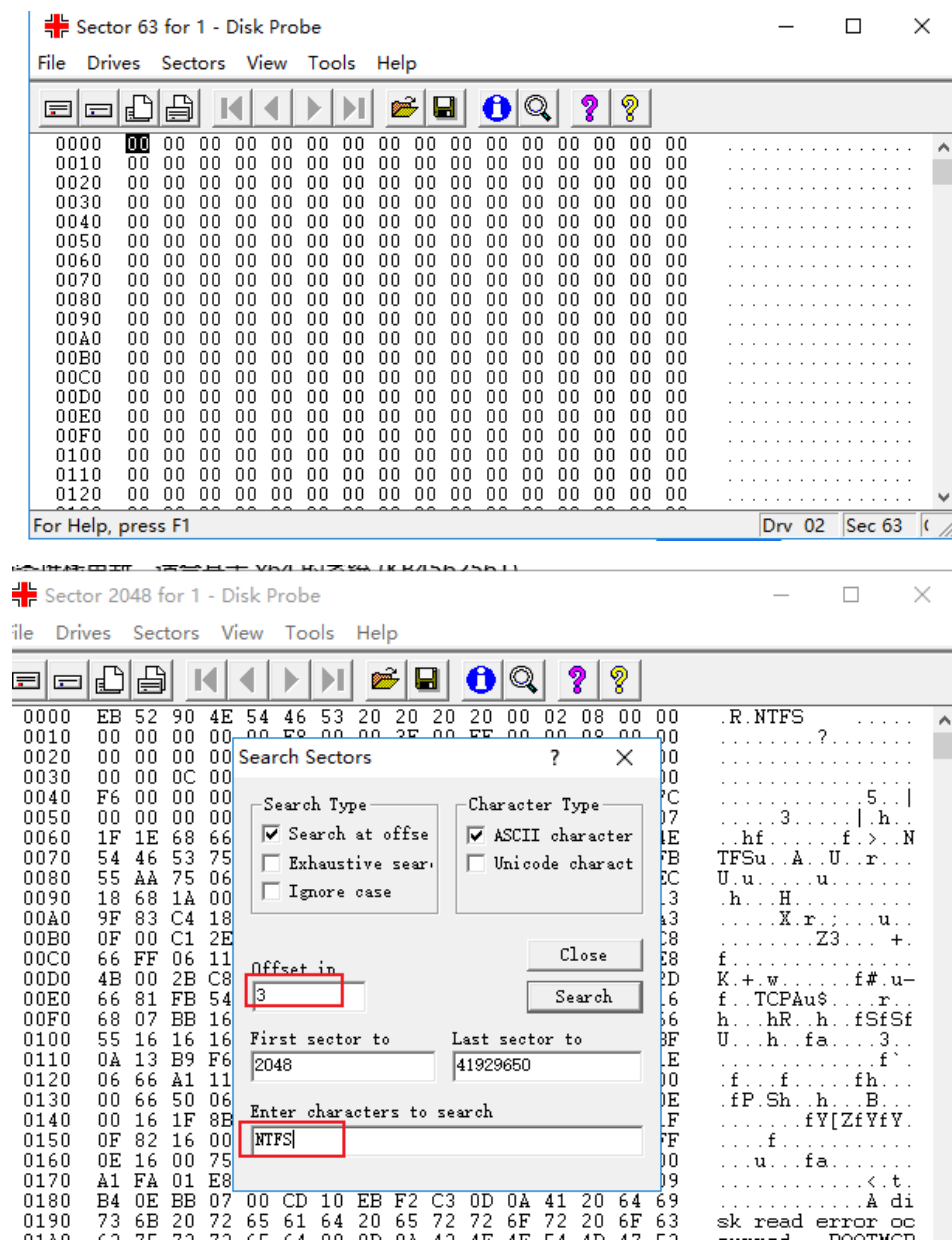
首先读取 sector0 的信息，view 以 partition table 展示，其中 relative 表示起始扇区，total sectors 表示总扇区数。从截图看到起始扇区是 63，总扇区数是 41940929，总扇区数 = 结束扇区 - 开始扇区 + 1，因此结束扇区是 41940991。

✚ Sector 0 for 1 - Disk Probe

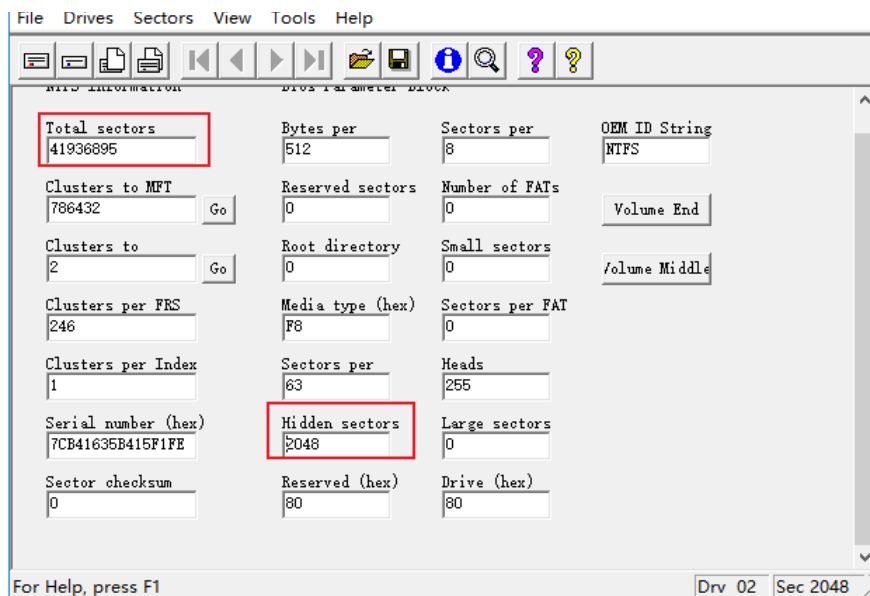
File Drives Sectors View Tools Help



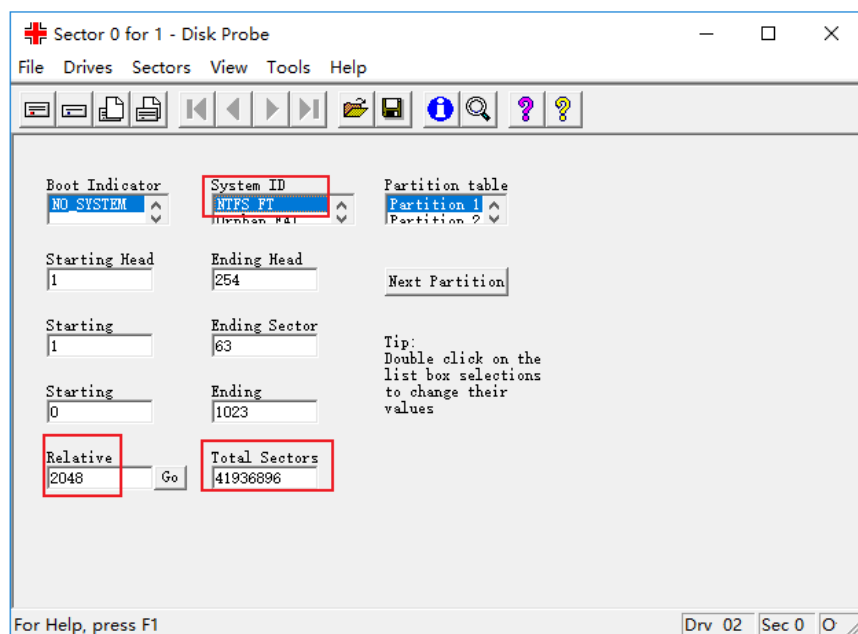
之后判断起始扇区和结束扇区是否正确，查看 sector 63 和 sector 41940991 都是空，说明起始和结束扇区不正确，需要在偏移位 3 的位置用 ntfs 标志查找起始和结束扇区，分别是 2048 和 41938943。



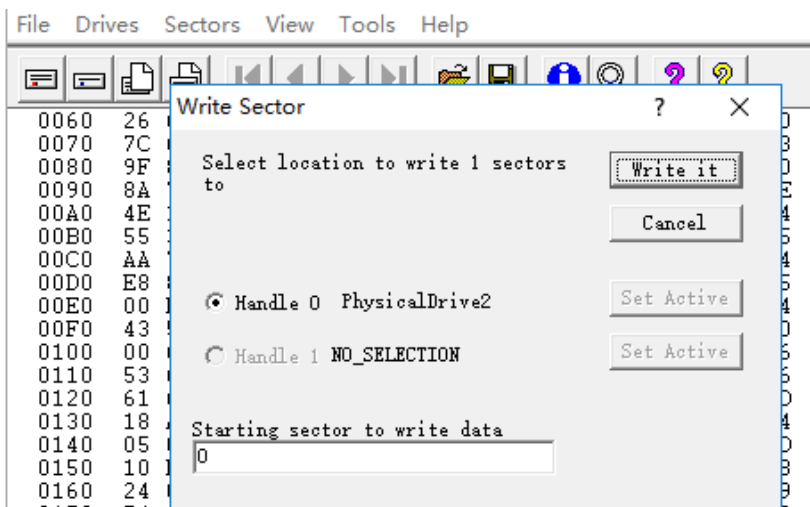
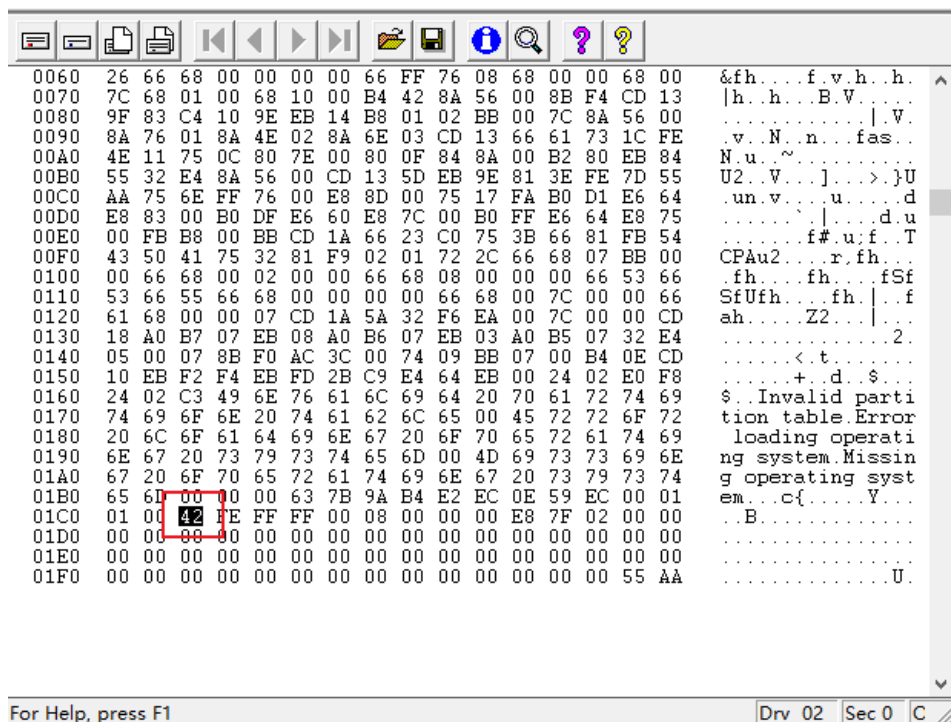
转到 sector 2048, View 以 NTFS BootSector 展示, Hidden sector 设置为起始扇区 2048, Total sectors 设置为结束扇区 - 起始扇区 = 41936895。



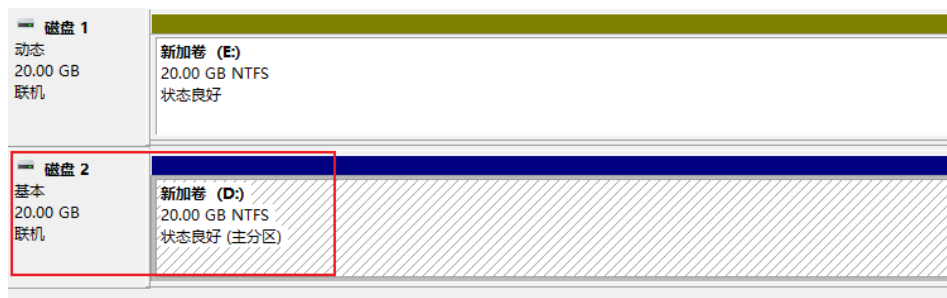
最后查看 sector0, View 以 Partition table 展示, relative 设置为起始扇区 2048, Total Sectors 为结束扇区 - 起始扇区 + 1 = 41936896。



sector 0 以 Bytes 显示, 将 42 改为 07 (42 表示的是动态分区, 07 表示是 NTFS 分区), write sector 进行保存。



重新扫描磁盘后，可以看到磁盘显示为一个基本盘，可以进行数据读取写入操作。



WMI 异常问题要如何重置？

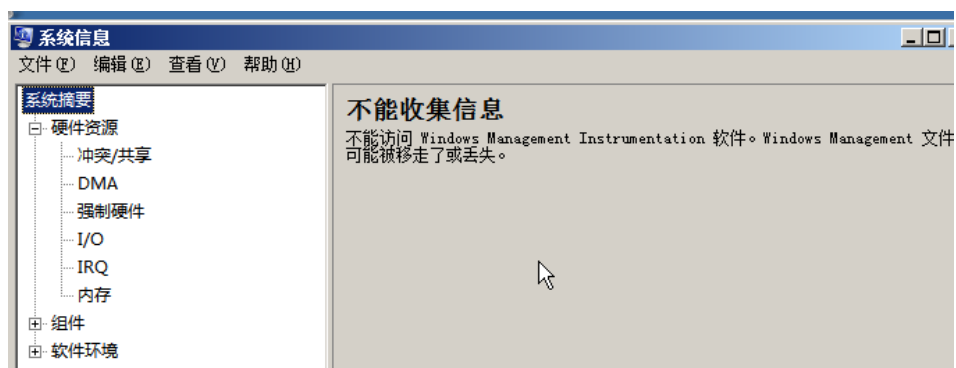
简介: 分享一个 WMI 异常问题，重置 WMI 的案例。

问题现象

1. 系统属性显示不可用。



2. msinfo32 提示不能访问 WMI。



修复方案

注：以下操作可能会对客户环境产生影响，建议客户先进行快照。

windows Server 2008R2

右击 cmd，选择以管理员身份运行，运行以下命令行：

```
sc config winmgmt start= disabled
net stop winmgmt /y
cd %windir%\system32\wbem
rename repository repository.old
for /f %s in ('dir /b *.dll') do regsvr32 /s %s
wmiprvse /regserver
sc config winmgmt start= auto
net start winmgmt
for /f %s in ('dir /b *.mof *.mfl') do mofcomp %s
```

Windows Server 2012 及以后版本

右击 cmd，选择以管理员身份运行，运行以下命令行：

```
sc config winmgmt start= disabled
net stop winmgmt /y
%systemdrive%
cd %windir%\system32\wbem
ren repository repository-backup
for /f %s in ('dir /b *.dll') do regsvr32 /s %s
sc config winmgmt start= Auto
net start winmgmt
dir /b *.mof *.mfl | findstr /v /i uninstall > moflist.txt & for /F %s in
(moflist.txt) do mofcomp %s
```

提示权限有问题？3步修改注册表搞定

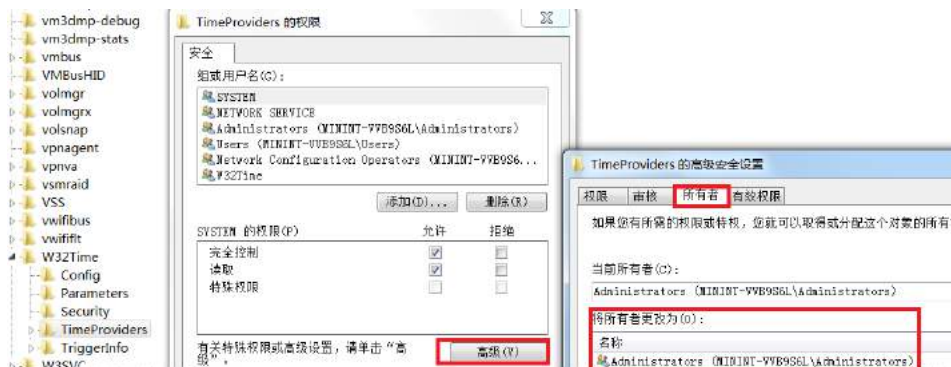
一般这种报错都是提示权限有问题，我们可以手动修改注册表权限。



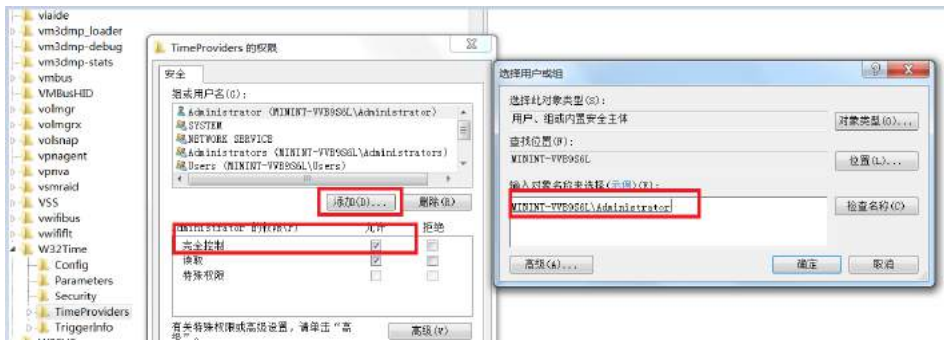
注：此方案同样适用于新建 / 修改文件时报错无权限情况（可参考如下步骤修改对应的文件权限），具体步骤如下：

首先比对这个注册表和正常服务器的权限，如果不一致，按如下步骤进行修改（以下示例以 TimeProviders 为例）：

1. 右击相应注册表，选择权限，点击高级，将所有者改为当前登录的用户（示例以管理员为例），之后点击 OK，关闭所有窗口。



2. 再次右击注册表，选择权限，赋予刚才更改的用户完全控制。若没有此用户，先点击添加。之后点击 OK，关闭所有窗口。



3. 重复第 2 步，参考正常机器，添加剩余用户的权限。



云服务技术大学
云产品干货高频分享



云服务技术课堂
和大牛零距离沟通



阿里云开发者“藏经阁”
海量免费电子书下载