Hi，王先生 & 金先生:

如刚才电话沟通，由于目前暂不方便处理此问题，经您的同意，此 case 将暂做归档处理，以下为案例总结，请您知悉

Case No: CAS-02027-G2S5S3

问题描述:
==========
用户反馈远程桌面功能无法使用

问题分析:
==========
基于 GB/T 30278-2013《信息安全技术政务计算机终端核心配置规范》的要求，使用提供的解决方案修改 CMGE 的定制内容，通过修改 CMGE 的初始配置，开启远程桌面，CMGE 在系统设置上也仅做了上述定制。针对现有的此问题，不排除安控软件的限制或网络方面的限制等因素。需要收集相关日志进行排查

问题总结:

==========

由于用户暂不方便处理此问题，经用户同意，此 case 将暂做归档处理，之后系统会发送一封满意度邮件，请您方便时进行反馈。如有其它问题，您也可以随时与我们联系，最后感谢您这段时间对我工作的大力支持。

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: Li Qi
发送时间: 2020 年 3 月 23 日 15:02
收件人: 'Chenguang CG5 Wang' <wangcg5@lenovo.com>; '911491700@qq.com' <911491700@qq.com>
抄送: CRM Case Email <casemail@cmgos.com>

主题: 回复: [External] 回复: [案例号: CAS-02027-G2S5S3] % |普通事件|联想|神州网信系统用户远程桌面功能无法使用 % 初次响应 CMIT:0001928

Hi，金先生:

由于刚才电话未联系到您。现发送第一封提醒邮件用于案例跟踪，请您知悉:

之前提供的解决方案是基于 GB/T 30278-2013《信息安全技术政务计算机终端核心配置规范》的要求，CMGE 进行的定制内容，通过上述方法可修改 CMGE 的初始配置，有关远程桌面的开启，CMGE 在系统设置上也仅做了上述定制。如现在仍有此问题，不排除安控软件的限制或网络方面的限制等因素。请方便时进行如下排查:

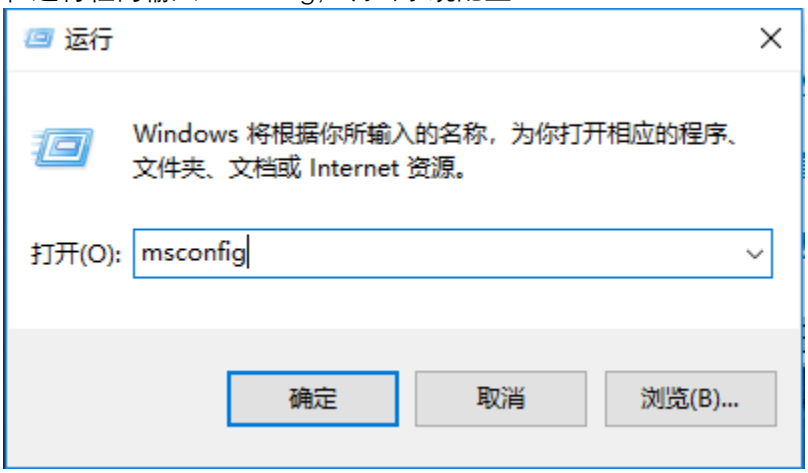
1， clean boot

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

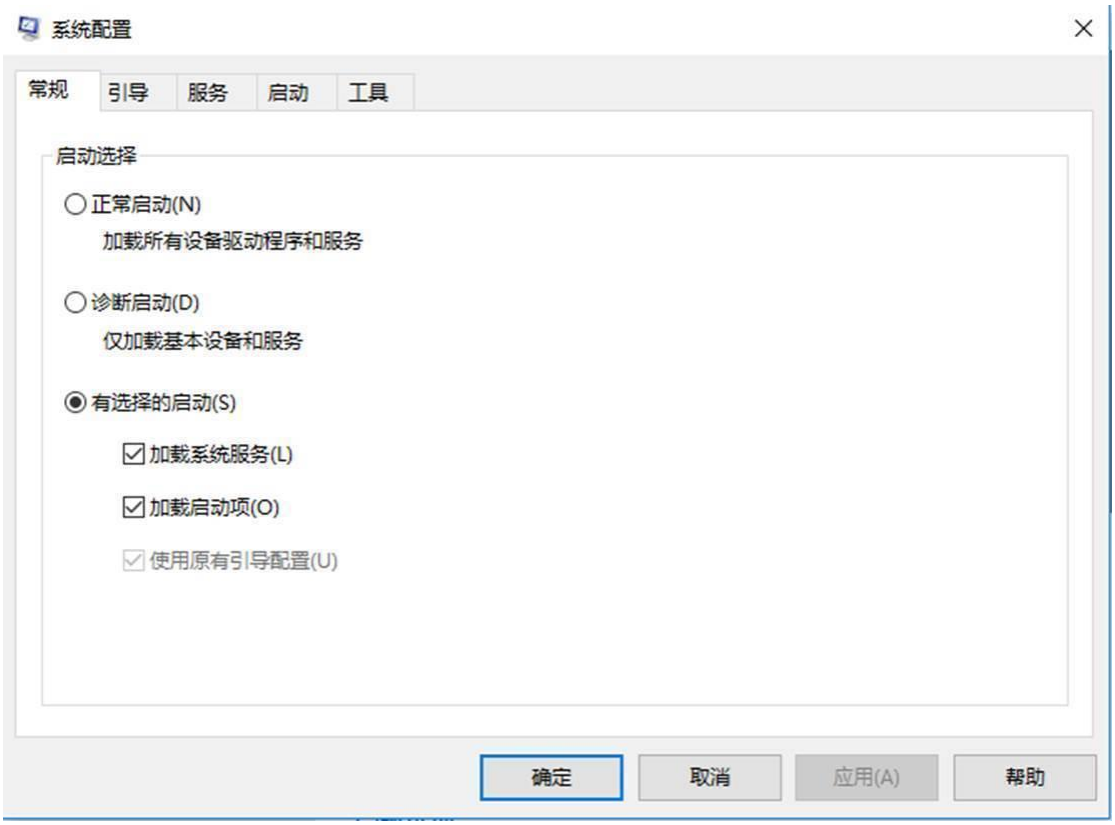
在“服务”选项下，勾选“隐藏所有 Microsoft 服务”，再点击“全部禁用”-确定，重启进入 Clean boot

步骤操作:

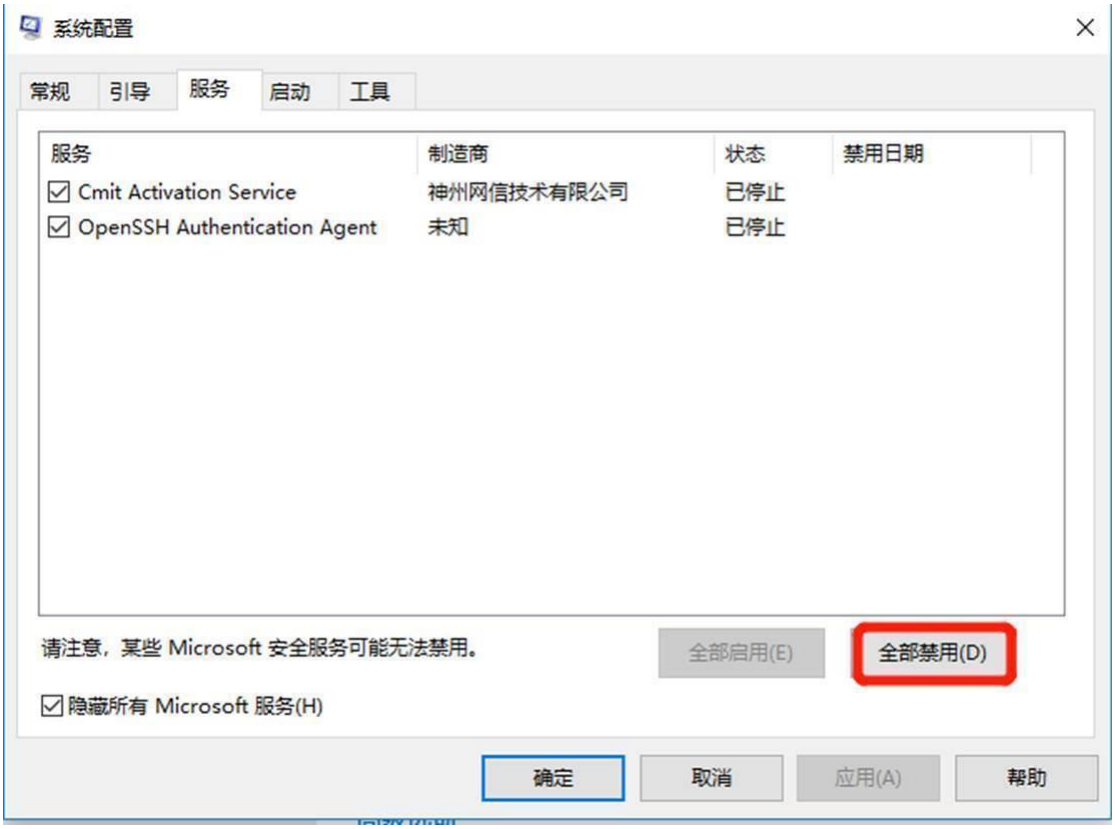
在运行栏内输入 msconfig，调出系统配置



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

2， 收集 process monitor：

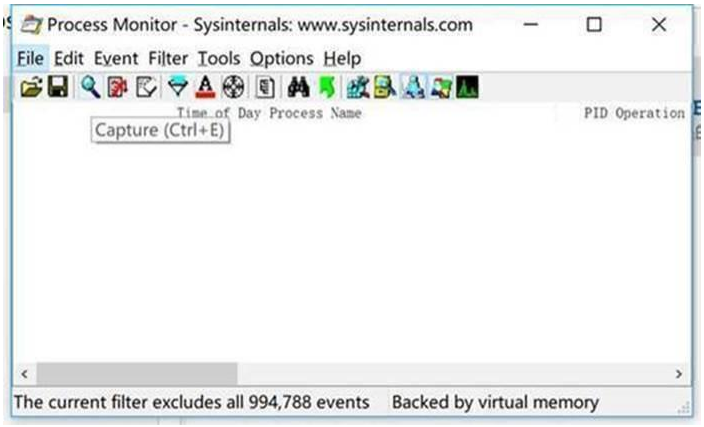
收集 procmon 日志信息：

a) 保存附件 processmonitor.zip 至本地计算机

b) 解压完成后，双击执行 procmon.exe

c) 显示如下界面，并点击 capture 按钮，先暂停收集，准备进行捕获

d) 点击 clear 按钮，清空当前窗口，然后点击 capture 按钮，开始捕获



e) 待问题复现后，再次点击 capture 按钮，停止捕获

f) 点击 File menu, 点击 Save. 选择"All events" and "Native Process Monitor Format (PML)"点击 OK，并将此文件回传给我进行分析，谢谢

PS：**请记录出现弹框错误窗口的时间戳，**方便问题定位范围

同时，收集 c:\windows\System32\Winevt\Logs\system.evtx 日志文件，一并发送给我

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: Li Qi

发送时间: 2020 年 3 月 19 日 11:17

收件人: 'Chenguang CG5 Wang' <wangcg5@lenovo.com>; '911491700@qq.com' <911491700@qq.com>

抄送: CRM Case Email <casemail@cmgos.com>

主题: 回复: [External] 回复: [案例号: CAS-02027-G2S5S3] % |普通事件|联想|神州网信系统用户远程桌面功能无法使用 % 初次响应 CMIT:0001928

Hi，金先生:

如刚才电话沟通，请您方便时按之前邮件所述进行操作，并将生成日志反馈给我用于分析，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: Li Qi
发送时间: 2020 年 3 月 17 日 10:17
收件人: 'Chenguang CG5 Wang' <wangcg5@lenovo.com>; '911491700@qq.com' <911491700@qq.com>
抄送: CRM Case Email <casemail@cmgos.com>
主题: 回复: [External] 回复: [案例号: CAS-02027-G2S5S3] % |普通事件|联想|神州网信系统用户远程桌面功能无法使用 % 初次响应 CMIT:0001928

Hi，金先生:

如刚才电话沟通，请您方便时按之前邮件所述进行操作，并将生成日志反馈给我用于分析，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: Li Qi
发送时间: 2020 年 3 月 11 日 13:28
收件人: 'Chenguang CG5 Wang' <wangcg5@lenovo.com>; 911491700@qq.com
抄送: CRM Case Email <casemail@cmgos.com>
主题: 回复: [External] 回复: [案例号: CAS-02027-G2S5S3] % |普通事件|联想|神州网信系统用户远程桌面功能无法使用 % 初次响应 CMIT:0001928

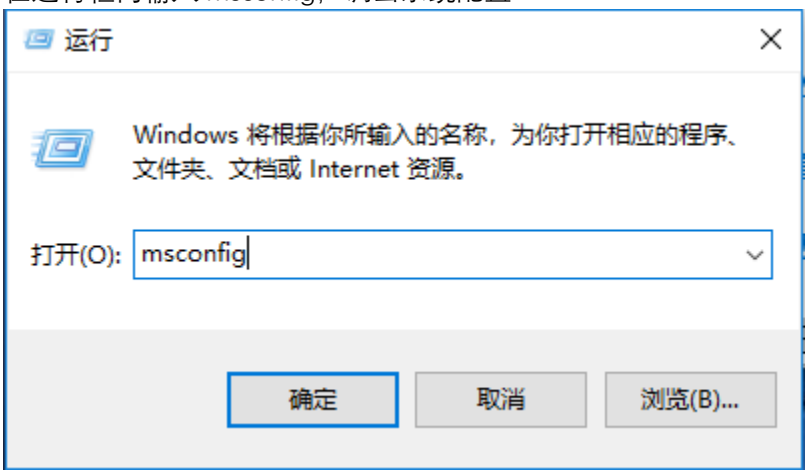
金先生 & 王先生，您们好:

如刚才电话沟通，之前提供的解决方案是基于 GB/T 30278-2013《信息安全技术政务计算机终端核心配置规范》的要求，CMGE 进行的定制内容，通过上述方法可修改 CMGE 的初始配置，有关远程桌面的开启，CMGE 在系统设置上也仅做了上述定制。如现在仍有此问题，不排除安控软件的限制或网络方面的限制等因素。请方便时进行如下排查:
1， clean boot

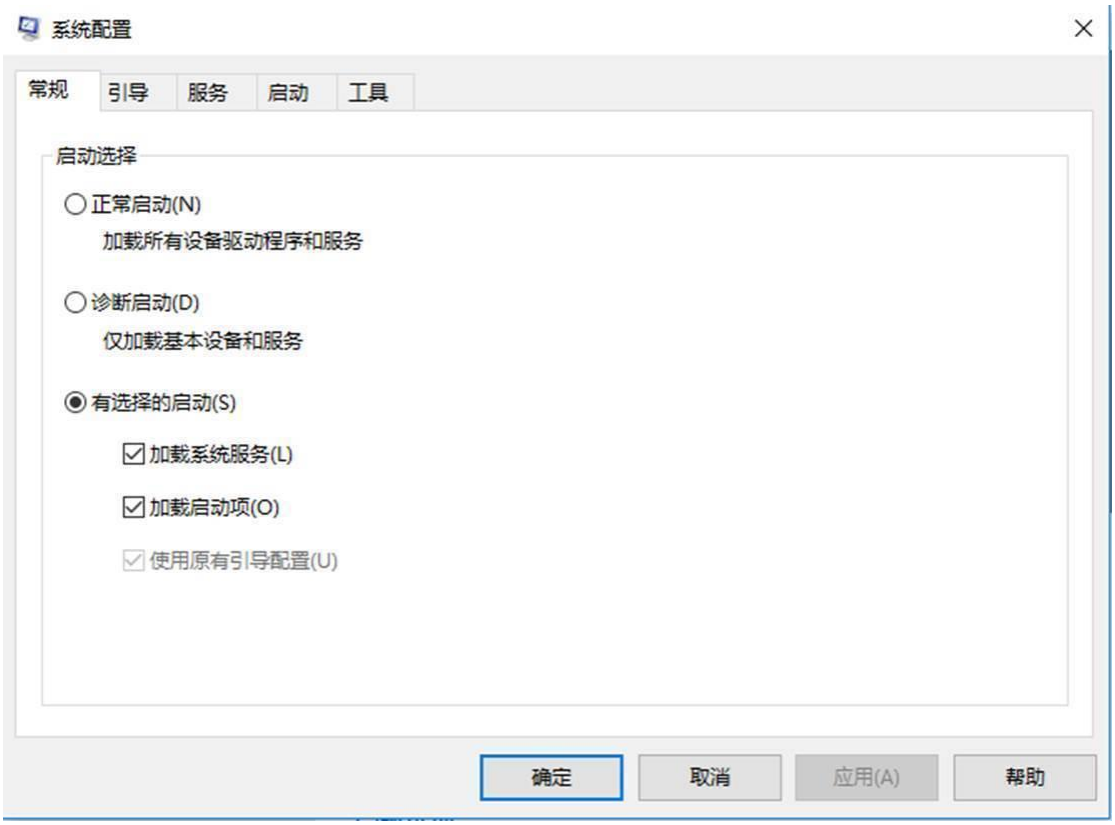
在运行栏内输入 msconfig，调出系统配置，在“常规”下选择“有选择的启动”，勾选加载系统服务和加载启动项

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

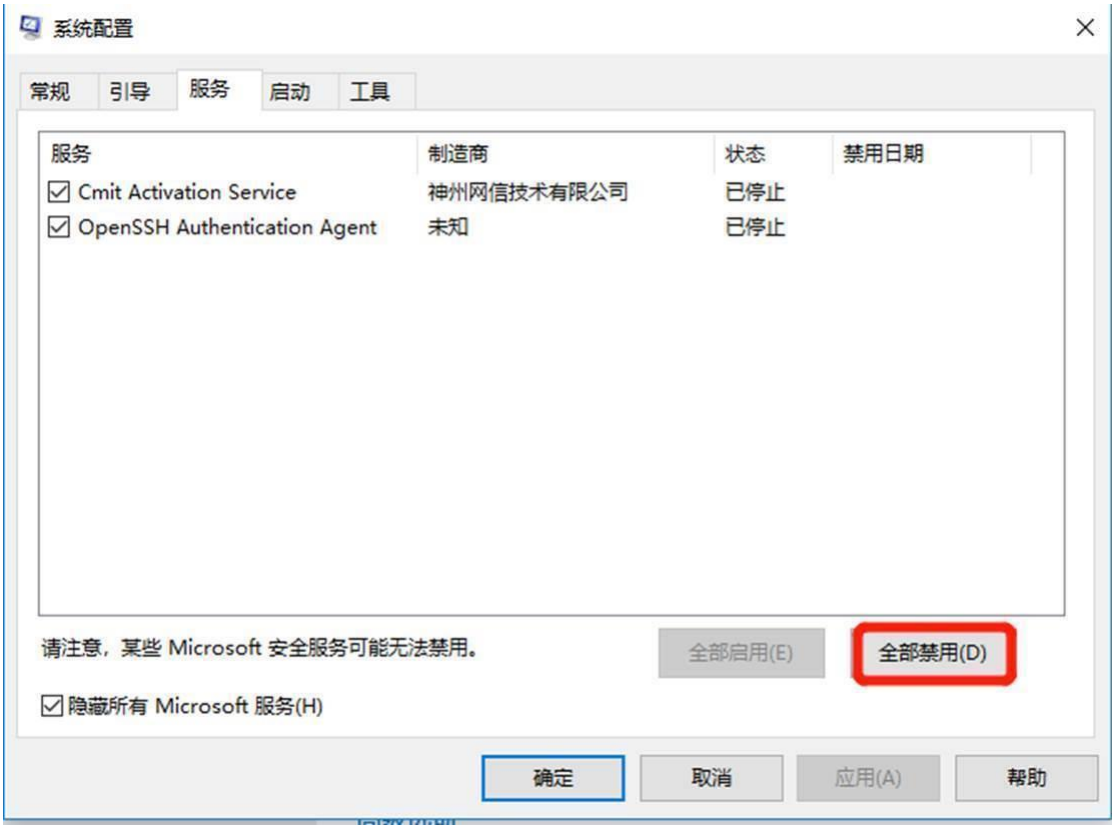
步骤操作:
在运行栏内输入 msconfig，调出系统配置



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

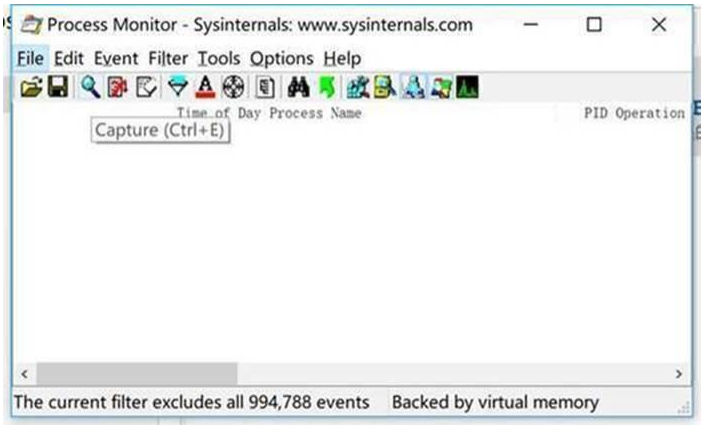


在“服务”选项下，勾选“隐藏所有 Microsoft 服务”，再点击“全部禁用”-确定



重启进入 Clean boot

2， 收集 process monitor：
收集 procmon 日志信息：
a) 保存附件 processmonitor.zip 至本地计算机
b) 解压完成后，双击执行 procmon.exe
c) 显示如下界面，并点击 capture 按钮，先暂停收集，准备进行捕获
d) 点击 clear 按钮，清空当前窗口，然后点击 capture 按钮，开始捕获



e) 待问题复现后，再次点击 capture 按钮，停止捕获
有关问题复现，分两部分内容：
- 双击 IE 浏览器：等待至 IE 浏览器窗口弹出，且无响应报错之后停止捕获
- 连接 VPN：等待至连接 VPN 失败，且无响应报错之后停止捕获

f) 点击 File menu, 点击 Save. 选择"All events" and "Native Process Monitor Format (PML)"点击 OK，并将此文件回传给我进行分析，谢谢

PS：**请记录出现弹框错误窗口的时间戳，**方便问题定位范围
同时，收集 c:\windows\System32\Winevt\Logs\system.evtx 日志文件，一并发送给我

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

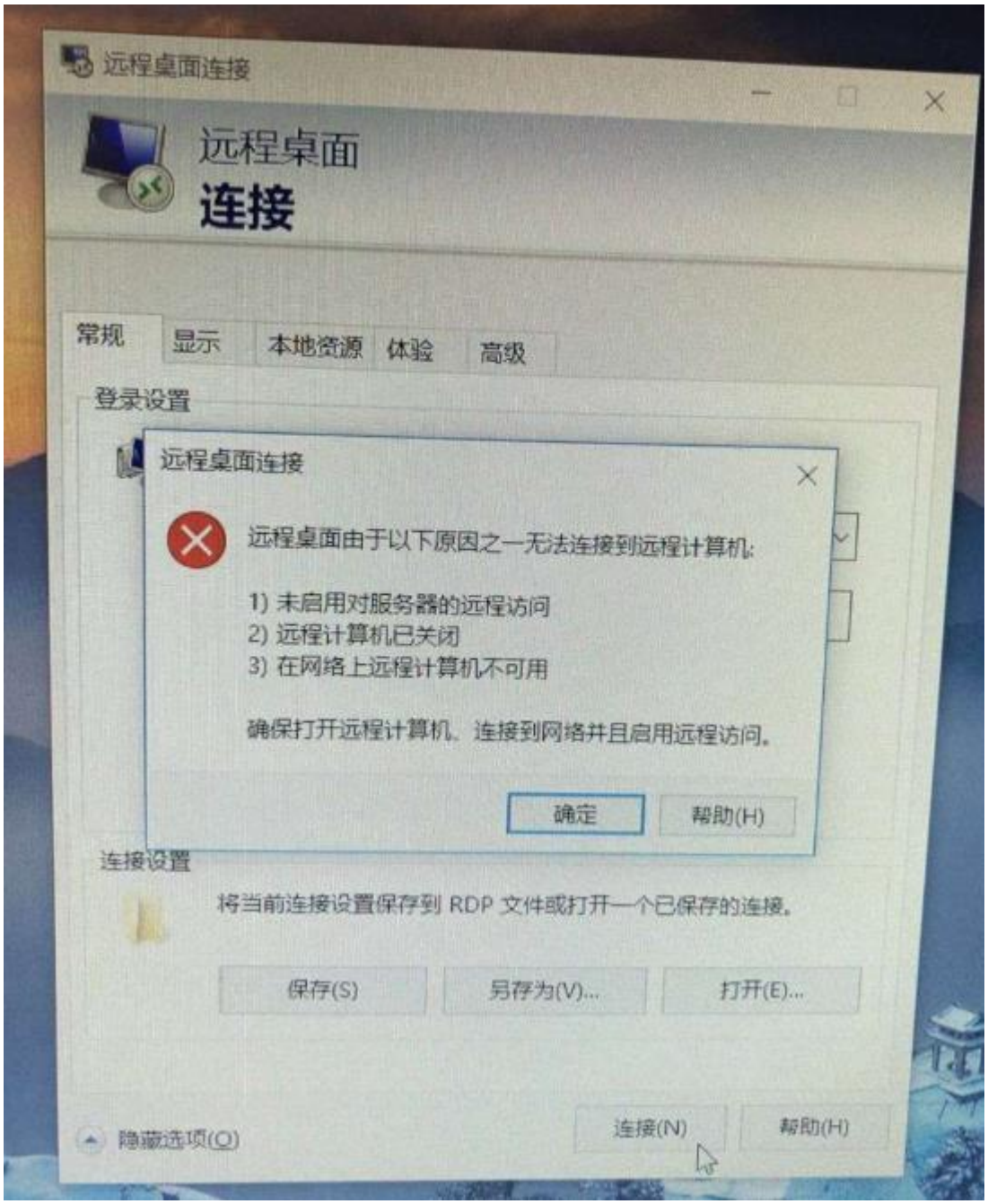
神州网信
CMIT

发件人: Chenguang CG5 Wang <wangcg5@lenovo.com>
发送时间: 2020 年 3 月 11 日 10:44
收件人: Li Qi <liqi@cmgos.com>; 911491700@qq.com
抄送: CRM Case Email <casemail@cmgos.com>

主题: 回复: [External] 回复: [案例号: CAS-02027-G2S5S3] % |普通事件|联想|神州网信系统用户远程桌面功能无法使用 % 初次响应 CMIT:0001928

您好

这个操作用户已经做过，我们这边有你们提供的文档已经发给用户测试，如附件文档，更改之后并重启还是不能解决问题，依旧有如下的报错，还麻烦协助处理



CPSD CC 王晨光 400-810-6666

Commerical Product Services Delivery
Lenovo Wuxi
www.lenovo.com.cn

010-58859506
lenovoka@lenovo.com

Plan | Perfor | Prioritize | Practice | Pioneer

发件人: Li Qi <liqi@cmgos.com>
发送时间: 2020 年 3 月 11 日 10:23
收件人: 911491700@qq.com
抄送: CRM Case Email <casemail@cmgos.com>; Chenguang CG5 Wang <wangcg5@lenovo.com>
主题: [External] 回复: [案例号: CAS-02027-G2S5S3] % |普通事件|联想|神州网信系统用户远程桌面功能无法使用 % 初次响应 CMIT:0001928

金先生，您好:

如刚才电话沟通，我谨在此阐述问题涉及的范围定义:
问题范围：用户反馈远程桌面功能无法使用
问题定义：协助用户分析并处理此问题。
如您对以上问题范围定义有任何疑问请直接与我联系。

请您检查如下步骤，是否在之前已成功开启:

1.以管理员身份进入 CMD. 运行 gpedit.msc 命令进行组策略编辑，分别设置以下几项:

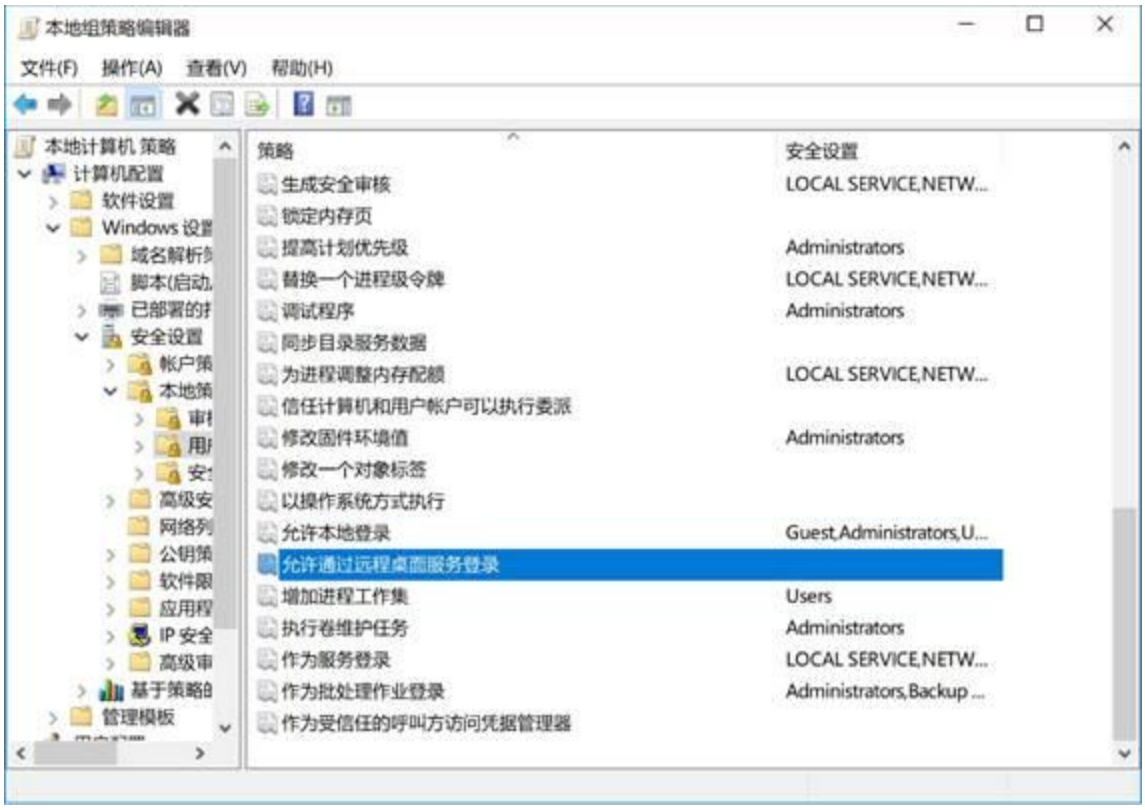
计算机配置-管理模板-Windows 组件-远程桌面服务-远程桌面会话主机-连接，将“允许用户通过使用桌面服务进行远程连接”设置为“未配置”。

计算机配置-管理模板-Windows 组件-远程桌面服务-远程桌面会话主机-安全，将“远程（RDP）连接要求使用指定的安全层”设置为“已启用”，安全层为“RDP”。

计算机配置-管理模板-系统-远程协助，将“配置请求的远程协助”设置为“未配置”。

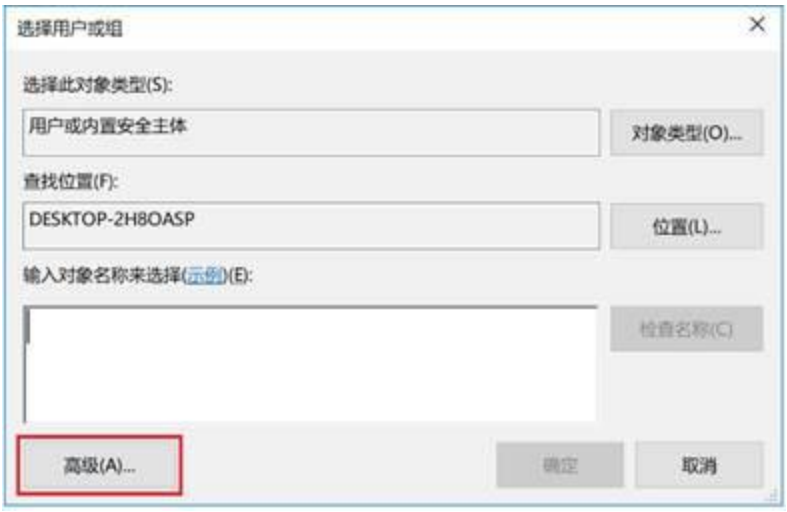
计算机配置-Windows 设置-安全设置-本地策略-用户权限分配-允许通过远程桌面服务登录，将用户添加到列表中。

1.


本地组策略编辑器
文件(F) 操作(A) 查看(V) 帮助(H)
本地计算机 策略
计算机配置
软件设置
Windows 设置
域名解析
脚本(启动
已部署的
安全设置
帐户策
本地策
审
用
安
高级安
网络列
公钥策
软件限
应用程
IP 安全
高级审
基于策略的
管理模板
策略
安全设置
生成安全审核
LOCAL SERVICE,NETW...
锁定内存页
提高计划优先级
Administrators
替换一个进程级令牌
LOCAL SERVICE,NETW...
调试程序
Administrators
同步目录服务数据
为进程调整内存配额
LOCAL SERVICE,NETW...
信任计算机和用户帐户可以执行委派
修改固件环境值
Administrators
修改一个对象标签
以操作系统方式执行
允许本地登录
Guest,Administrators,U...
允许通过远程桌面服务登录
增加进程工作集
Users
执行卷维护任务
Administrators
作为服务登录
LOCAL SERVICE,NETW...
作为批处理作业登录
Administrators,Backup ...
作为受信任的呼叫方访问凭据管理器

2.

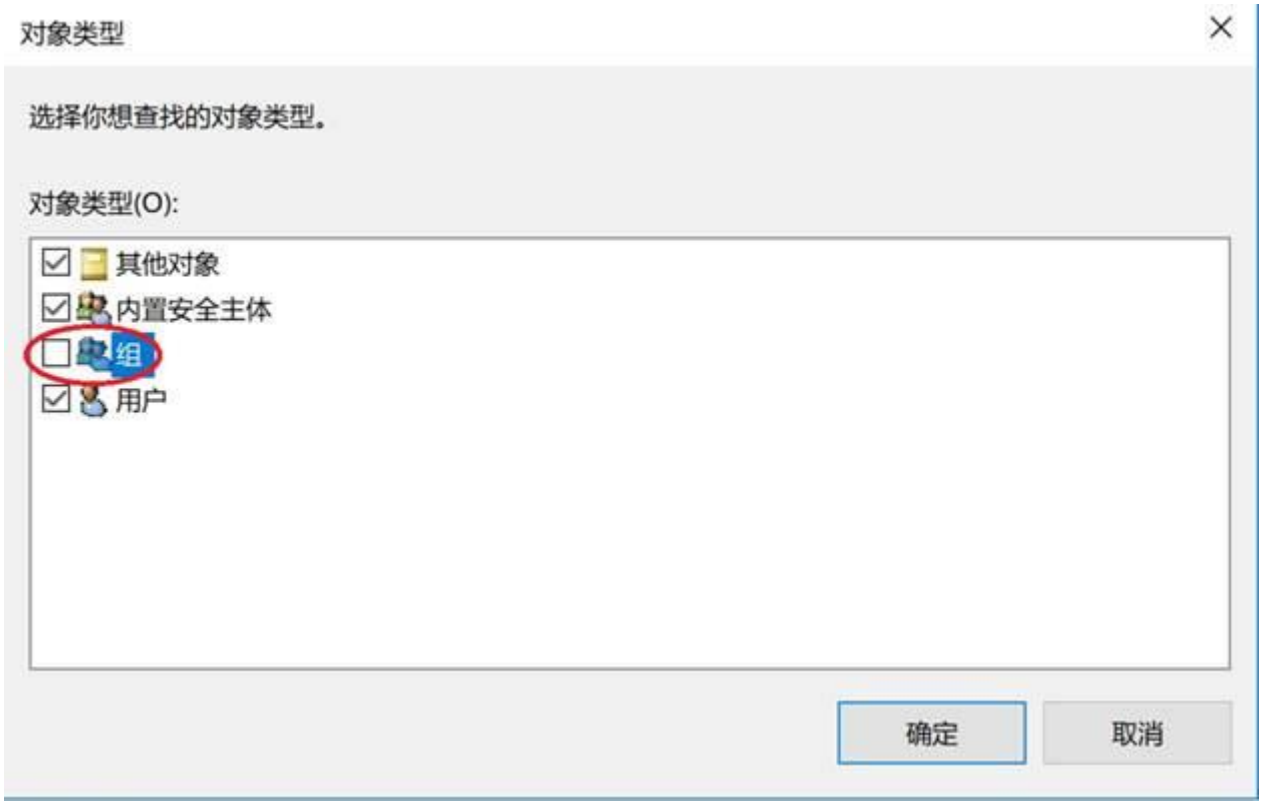
3.


选择用户或组
选择此对象类型(S):
用户或内置安全主体
对象类型(O)...
查找位置(F):
DESKTOP-2H8OASP
位置(L)...
输入对象名称来选择(示例)(E):
检查名称(C)
高级(A)...
确定
取消

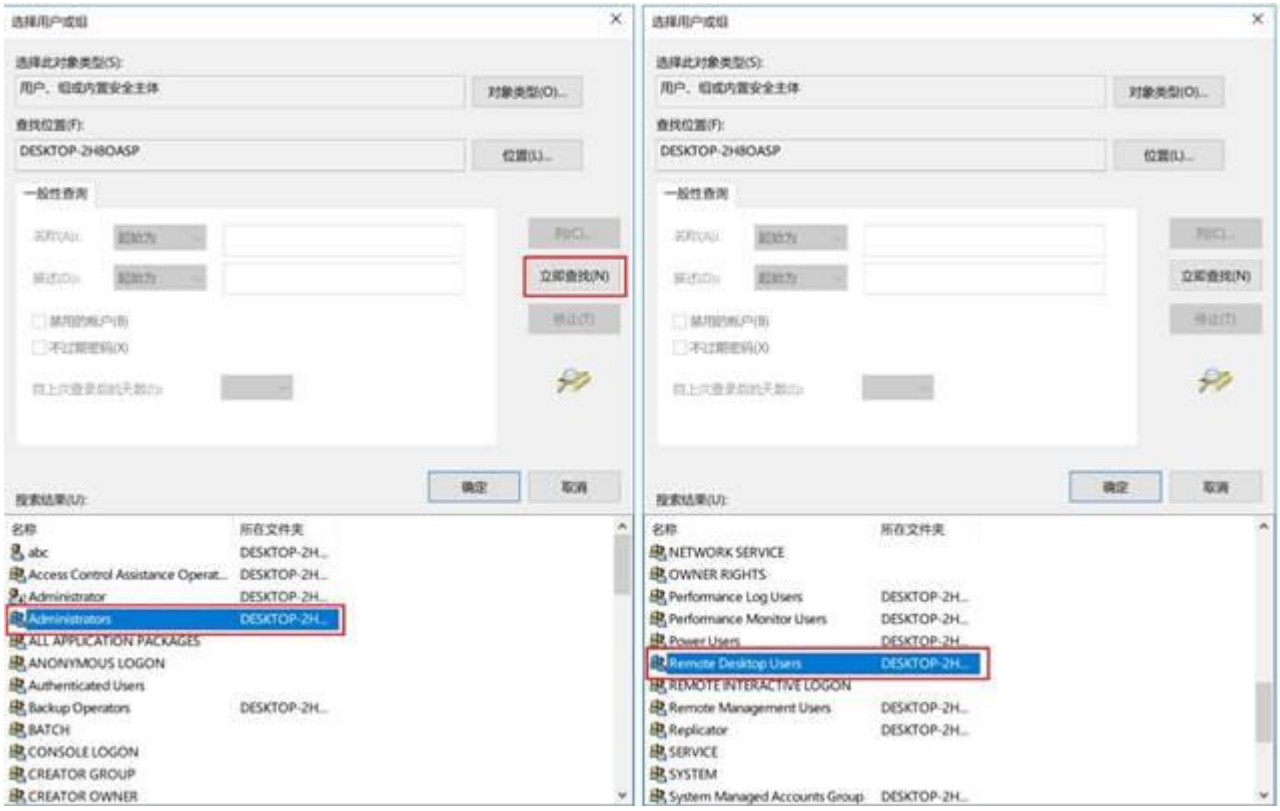
4.


选择用户或组
选择此对象类型(S):
用户或内置安全主体
对象类型(O)...
查找位置(F):
DESKTOP-2H8OASP
位置(L)...
一般性查询
立即查找(N)
停止(T)
确定
取消
搜索结果(U):
名称
所在文件夹

5.勾选“组”


对象类型
选择你想查找的对象类型。
对象类型(O):
其他对象
内置安全主体
组
用户
确定
取消

6.点击立即查找后，搜索结果会显示出多个选项，请选择 Administrators 与 Remote Desktop Users



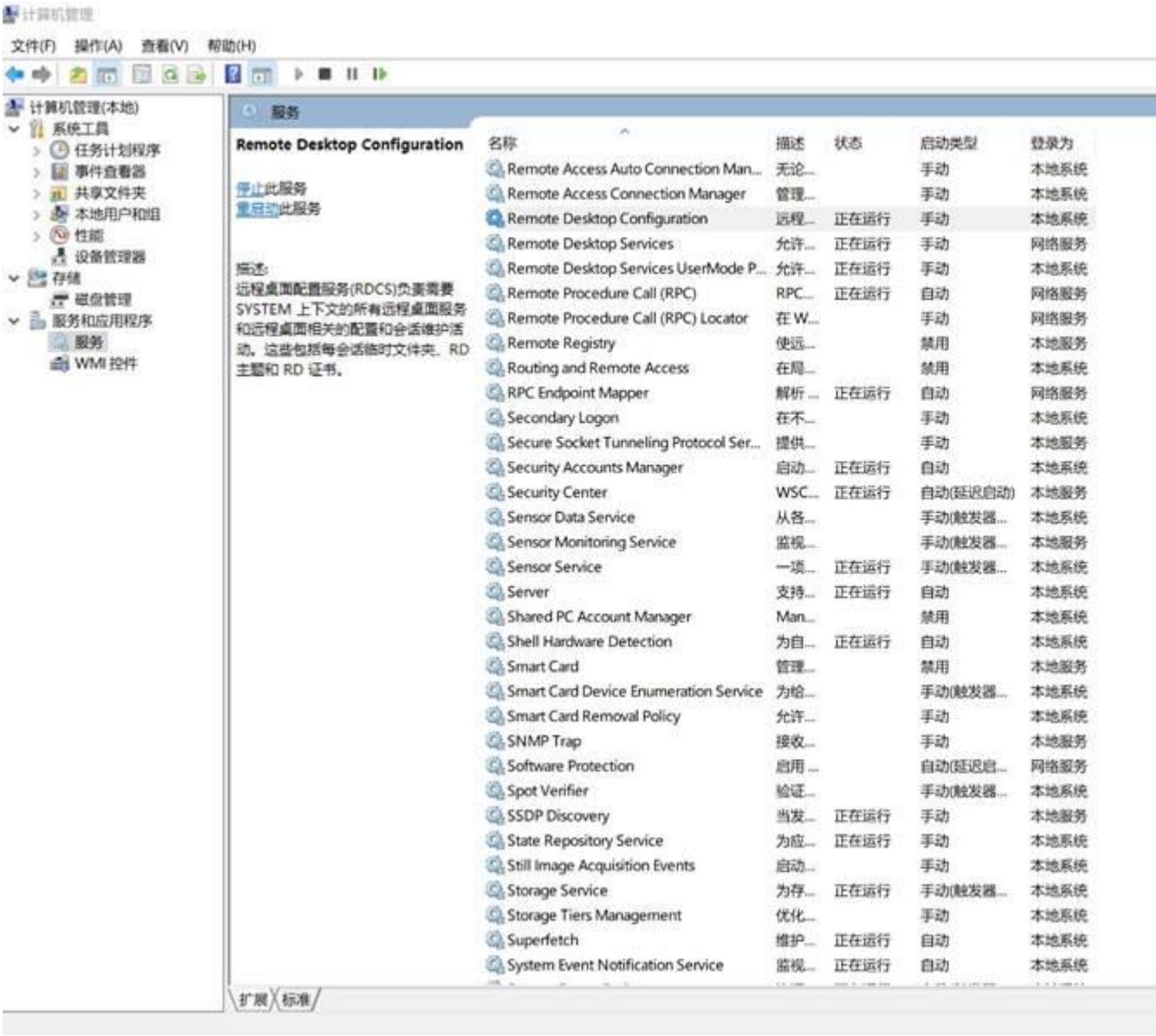
2.在 CMD 中运行 gpupdate /force

3.检查下列服务是否开启

Remote Desktop Configuration

Remote Desktop Services

Remote Desktop Services UserMode Port Redirector

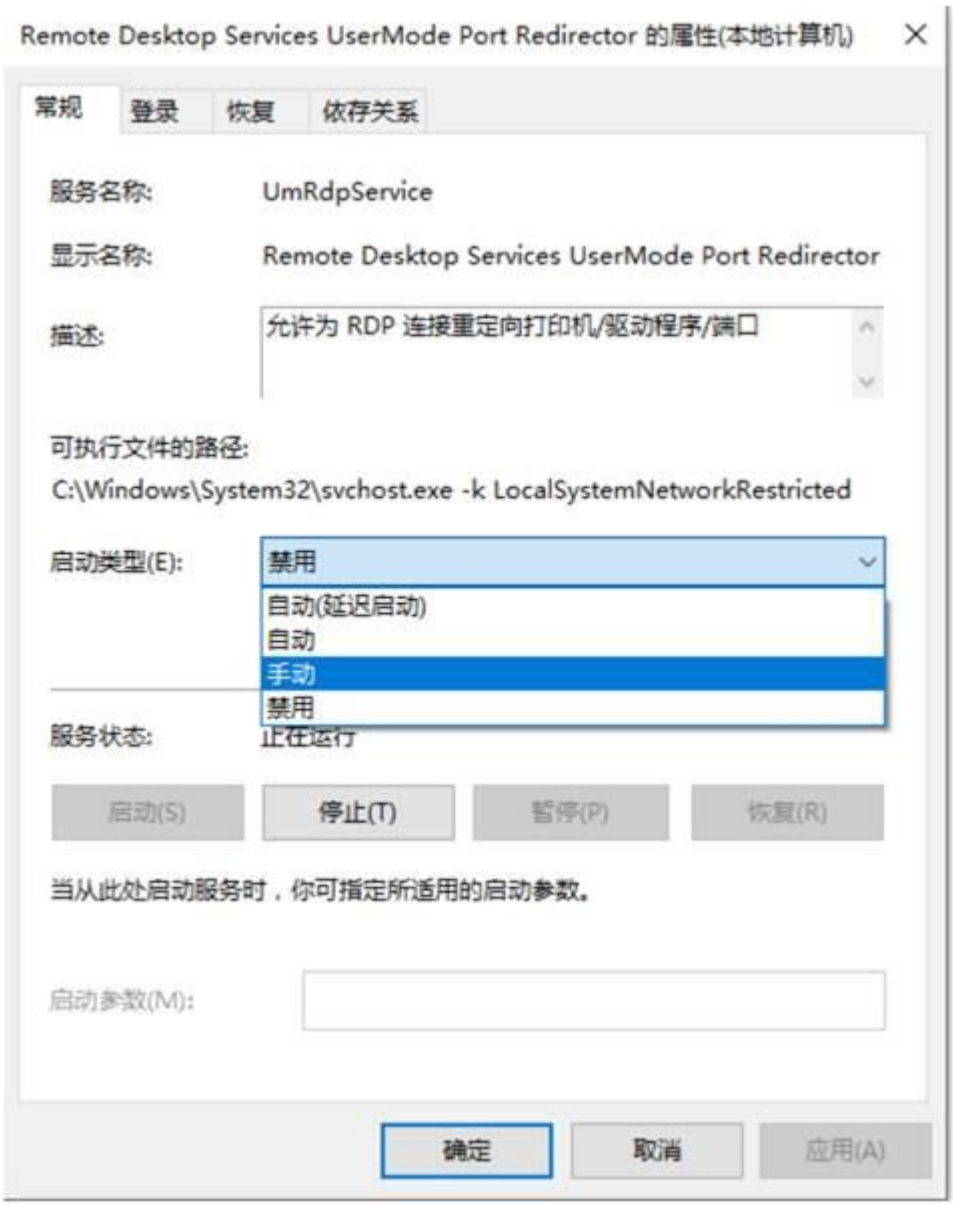


如果服务启动类型为禁用，请调整为手动:

1.


名称
描述
状态
启动类型
登录为
Remote Access Auto Connection Man...
无论什么时候...
手动
本地系统
Remote Access Connection Manager
管理从这台计...
正在...
手动
本地系统
Remote Desktop Configuration
远程桌面配置...
正在...
手动
本地系统
Remote Desktop Services
允许用户以交...
正在...
手动
网络服务
Remote Desktop Services UserMode ...
允许为 RDP ...
正在...
禁用
本地系统
Remote Procedure Call (RP
正在...
自动
网络服务
Remote Procedure Call (RP
手动
网络服务
Remote Registry
禁用
本地服务
Routing and Remote Acce
禁用
本地系统
RPC Endpoint Mapper
正在...
自动
网络服务
Secondary Logon
手动
本地系统
Secure Socket Tunneling P
正在...
手动
本地服务
Security Accounts Manage
正在...
自动
本地系统
Security Center
正在...
自动(延迟启动)
本地服务
Sensor Data Service
手动(触发器启动)
本地系统
Sensor Monitoring Service
手动(触发器启动)
本地服务
Sensor Service
一项用于管理...
手动(触发器启动)
本地系统
Server
支持此计算机...
正在...
自动
本地系统
启动(S)
停止(O)
暂停(U)
恢复(M)
重新启动(E)
所有任务(K)
刷新(F)
属性(R)
帮助(H)

2.



（使用 CMD 命令 netstat -ano |findstr 3389，查看下 3389 端口是否已监听，如果没有需要重启计算机）

4.右键点击“计算机”->属性→远程设置，启用远程协助和远程桌面功能，参考如下图:

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: Li Qi <liqi@cmgos.com>
发送时间: 2020 年 3 月 11 日 9:36
收件人: 王晨光 <wangcg5@lenovo.com>
抄送: Li Qi <liqi@cmgos.com>

主题: [案例号: CAS-02027-G2S5S3] % |普通事件|联想|神州网信系统用户远程桌面功能无法使用 % 初次响应 CMIT:0001928

王晨光 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 CAS-02027-G2S5S3 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
