

自动化助手 故障处理





【版权声明】

©2013-2025 腾讯云版权所有

本文档(含所有文字、数据、图片等内容)完整的著作权归腾讯云计算(北京)有限责任公司单独所有,未经腾讯云事先明确书面许可,任 何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯,腾讯云将依法采取措 施追究法律责任。

【商标声明】

🕗 腾讯云

及其它腾讯云服务相关的商标均为腾讯云计算(北京)有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标,依法由权利人所 有。未经腾讯云及有关权利人书面许可,任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为,否则将构成对腾 讯云及有关权利人商标权的侵犯,腾讯云将依法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况,部分产品、服务的内容可能不时有所调整。 您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定,除非双方另有约定,否则,腾讯云对本文档内容不 做任何明示或默示的承诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务,及相应的技术售后服务,任何问题请联系 4009100100或95716。



文档目录

故障处理

Windows 实例问题诊断及处理



故障处理 Windows 实例问题诊断及处理

最近更新时间: 2025-06-05 15:41:22

现象描述

Windows 实例通过自动化助手检查,检测结果中出现相关问题。

检测项分类

检测项	检测内容
	Windows 操作系统版本检查
	内存限制检查
	CPU 限制检查
	句柄泄露检查
	系统暴力破解和攻击检查
操作系统环境相关	系统环境变量检查
	系统激活检查
	系统时间检查
	系统路由表检查
	系统 IE 代理检查
	CD-ROM 状态检查
	内存使用率过高
	虚拟内存使用率高
亥佐次酒店田卖妇关	总 CPU 使用率过高
示机页 I 际使用平相天	单 CPU 使用率过高
	磁盘可用空间不足
	Ntfs 文件系统元文件磁盘占用高
远程连接相关	远程桌面服务状态检查
	远程桌面服务端口检查
	RDP 侦听器启用检查
	允许远程桌面连接检查
	RDP 自签证书到期时间检查

	远程桌面服务角色安装及授权检查
	网络访问账户检查
	远程桌面服务端口防火墙放通检查
	端口耗尽检查
	Timewait/Closewait 连接数检查
网络配置相关	网关状态检查
	MAC 地址检查
	内网域名解析检查

问题定位及处理

您可匹配具体检测项结果,参考以下步骤处理对应问题:

Windows 操作系统状态检查

现象描述

Windows Server 2008 R2及更早版本系统存在安全性、稳定性和兼容性方面均较差问题,且微软和腾讯云也已不再进行维护。

解决方法

- 1. 通过快照等方式进行数据备份,确保数据安全。详情请参见创建快照。
- 2. 通过控制台重装高版本系统,详情请参见 重装系统。

内存限制检查

现象描述

Windows 操作系统无法最大化使用内存,可能存在内存瓶颈导致不能充分发挥系统性能。

解决方法

- 1. 登录实例,详情请参见 登录 Windows 实例。
- 2. 在操作系统桌面左下角右键单击,在弹出菜单中选择 Windows PowerShell (管理员)。
- 3. 在 powershell 窗口中输入 resmon 并按 Enter, 打开 资源监视器 窗口。



4. 在 资源监视器 窗口中,选择内存页签,并检查"为硬件保留的内存"是否大于512MB。如下图所示:

1/1±	· 45% 已月	月物理内存					>	视图
3名称	PID	硬中断/秒	提交(KB)	工作集(KB)	可共享(KB)	专用(KB) ^	使用的物理内存	100%
svchost.exe (netsvcs)	844	0	284,236	319,344	46,240	273,104		
MsMpEng.exe	1840	2	266,220	260,316	62,952	197,364		
powershell.exe	5420	0	73,392	82,164	42,864	39,300		
ServerManager.exe	1244	0	83,388	64,416	31,968	32,448		
powershell.exe	2512	18	65,368	71,272	40,060	31,212		
svchost.exe (termsvcs)	852	0	37,368	45,516	22,236	23,280	60 秒	0%
ShellExperienceHost.exe	5076	0	22,824	60,056	41,428	18,628	内存使用	100%
svchost.exe (LocalServiceN.	992	0	17,360	26,108	11,516	14,592 🤟		
加理内存	📕 1853 MB	3 正在使用	-	📕 2173 MB म्	J用	 Image: A start of the start of		-//
为硬件保留的内存 1 MB	正在使用 1853 MB	■ 已修改 69 MB		备用 799 MB	可用 1374 MB		硬中断/秒	0%

- 大于,请参考以下步骤进行修复。
- 5. 在 powershell 窗口中输入 msconfig 并按 Enter, 打开"系统配置"窗口。
- 6. 在"系统配置"窗口中,选择**引导**页签,并单击**高级选项**。如下图所示:

见 引导 服务 启动 工具 Windows Server 2016 (C:\\Windows)	:当前 OS: 默认 OS	
windows server zoro (c.(windows)		
高级选项(/)… 设为;	默认值(S) 删除(D)	
引导选项		超时(]]:
□ 安全引导(E)	□无 GUI 引导(N)	30 秒
○ 最小(<u>M</u>)	□引导日志(B)	
○ 其他外壳(L)	□ 蓥华快观(上)	
○ 其他外壳(L) ○ Active Directory 修复(P)	□	□ 使所有引导设置成为永久设 (K)
○ 其他外壳(L) ○ Active Directory 修复(P) ○ 网络(\ <u>M</u>)	□ ☆4代UQU(E) □ OS 引导信息(<u>O</u>)	□使所有引导设置成为永久设 (L)



7. 在弹出的"引导高级选项"窗口中,取消勾选"最大内存"。如下图所示:

引导高级选项		×
□ <u>她理器个数(N)</u> 1 ~~~	□ 最大内存(<u>M</u>): 0	▲ ▼
□ PCI 锁定(P) □ 调试(D)		_
全 局调试设置 ☑ 调试端口(E): 1394 ~	波特率(<u>B</u>):	~
□通道(C): 0 ★		
056 日你杏山:	确定	取消

- 8. 单击确定。
- 9. 在操作系统桌面左下角右键单击 🛨 ,选择**设置**。
- 10. 在"设置"窗口中选择更新与安全,并在左侧单击激活。
- 11. 检查系统是否已激活。
 - 是,则进行下一步。
 - 否,则请参考 系统激活 进行激活。
- 12. 通过控制台重启实例,使配置生效。

CPU 限制检查

现象描述

Windows 操作系统无法最大化使用 CPU,可能存在 CPU 瓶颈导致不能充分发挥系统性能。

解决方法

1. 登录实例,详情请参见 使用标准方式登录 Windows 实例。

- 2. 在操作系统桌面左下角右键单击 🕀 , 在弹出菜单中选择 Windows PowerShell (管理员)。
- 3. 在 powershell 窗口中输入 msconfig 并按 Enter, 打开"系统配置"窗口。



4. 在"系统配置"窗口中,选择**引导**页签,并单击**高级选项**。如下图所示:

高级选项(/)	设为默认值(<u>S</u>) 删除(<u>D</u>)	
引导选项		超时(]]:
□ 安全引导(E)	□无 GUI 引导(N)	30 秒
○ 最小(<u>M</u>)	□引导日志(B)	
○ 其他外売(L) ○ Active Directory 修复(<u>F</u> ○ 网络(<u>W</u>)	□ 基本视频(E) 2) □ OS 引导信息(O)	□使所有引导设置成为永久设置 (K)
	确定取消	应用(4) 帮助
· 弹出的"引导高级选项"中, ¹	取消勾选"处理器个数"。如下图所示	
导高级选项	×	
」处理器个数(N):	□ 最大内存(<u>M</u>):	
1 ~	0	
_ PCI 锁定(P)		
] 调试(D)		
人已润净况率		
→ 通過満日(E):	波特率(B):	
1394 ~		
□ 通道(∩)•		
通道(C):		
〕通道(C): 0 ▲		
〕 通道(C): 0 ◆ USB 目标名①:		
〕 通道(C): 0 ▲ USB 目标名①:		



6. 在弹出的"选择列"窗口中,勾选"句柄"并单击确定。

腾讯云



7. 单击行首的**句柄**,进行降序排列。如下图所示:

№ 任务管理器							—	\times
文件(F) 选项(O) 查	看(V)							
进程 性能 用户 详	细信息	服务						
名称	PID	状态	用户名	CPU	内存(专用	句柄	描述	^
svchost.exe	844	正在	SYSTEM	00	24,872 K	1,738	Windows 服务主进	
axplorer.exe	3980	正在	Administr	00	13,100 K	1,373	Windows 资源管理	
sass.exe	564	正在	SYSTEM	00	5,184 K	995	Local Security Aut	
📧 System	4	正在	SYSTEM	00	28 K	925	NT Kernel & Syste	
svchost.exe	852	正在	NETWOR	00	23,508 K	747	Windows 服务主进	
ShellExperience	5076	正在	Administr	00	18,516 K	688	Windows Shell Ex	
svchost.exe	640	正在	SYSTEM	00	5,072 K	678	Windows 服务主进	
SearchUI.exe	4164	已暫停	Administr	00	12,200 K	670	Search and Corta	
svchost.exe	352	正在	LOCAL SE	00	7,236 K	644	Windows 服务主进	
svchost.exe	1088	正在	NETWOR	00	7,484 K	628	Windows 服务主进	
svchost.exe	700	正在	NETWOR	00	4,136 K	578	Windows 服务主进	
svchost.exe	948	正在	SYSTEM	00	6,712 K	561	Windows 服务主进	
📥 ServerManager	1244	正在	Administr	00	41,428 K	504	Server Manager	
svchost.exe	992	正在	LOCAL SE	00	9,928 K	502	Windows 服务主进	
svchost.exe	412	正在	LOCAL SE	00	9,244 K	476	Windows 服务主进	
MsMpEng.exe	1840	正在	SYSTEM	00	196,840 K	472	Antimalware Servi	
🔀 powershell.exe	5420	正在	Administr	00	39,820 K	466	Windows PowerS	
👰 Taskmgr.exe	3964	正在	Administr	00	7,792 K	425	Task Manager	
svchost.exe	1752	正在	SYSTEM	00	4,800 K	410	Windows 服务主进	
LogonUI.exe	800	正在	SYSTEM	00	7,236 K	408	Windows Logon	
Teril attack and	2225	π π	Administration	00	2 1 2 4 12		Chall Information	¥

○ 简略信息(D)

8. 右键单击占用句柄最多的进程,在弹出菜单中选择创建转储文件。

9. 在弹出的"转储进程"窗口中单击确定。

10. 按需更新系统补丁、安装杀毒软件,进行全盘病毒扫描。

系统暴力破解和攻击检查

现象描述

可能导致系统卡顿,严重时系统会被打挂,影响正常业务,甚至有丢数据风险。

解决方法

通过控制台合理设置安全组策略,仅放通必要的 IP 及端口号,其他默认拒绝。详情请参见 安全组概述 。

系统环境变量检查

现象描述

可能导致系统部分命令无法正常运行,提示命令不存在或运行后出现异常,例如不断弹窗等。

解决方法

1. 登录实例,详情请参见 使用标准方式登录 Windows 实例(推荐)。

- 2. 在操作系统桌面左下角右键单击 日, 在弹出菜单中选择 Windows PowerShell (管理员)。
- 3. 在 powershell 窗口中输入 sysdm.cpl 并按 Enter, 打开"系统属性"窗口。

结束任务(E)



4. 在"系统属性"窗口中,选择**高级**页签,并单击环境变量。如下图所示:

系统属性	×
计算机名 硬件 高级 远程	
要进行大多数更改,你必须作为管理员登录。	
性能	
视觉效果,处理器计划,内存使用,以及虚拟内存	
	设置(S)
用户配置文件	
与登录帐户相关的桌面设置	
	设置(E)
启动和故障恢复	
系统启动、系统故障和调试信息	
	设置①
I	不境变量(N)
确定取消	应用(A)

5. 双击"系统变量"中的 Path ,检查环境变量。 请确保以下4个环境变量存在、顺序无误且位置处在最顶端。若您还有其他自定义环境变量,请尽量放在最底端。如下图所示:



编辑环境变量	×	
%SystemRoot%\system32	辛戌事(N)	
%SystemRoot%		
%SystemRoot%\System32\Wbem	编辑(E)	
%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\		
C:\Program Files\QCloud\Monitor\Barad	浏览(<u>B</u>)	
	删除(D)	
	上移山	
	下移(0)	
	编辑文本①	
御気		
若您的环境变量出现问题,请进行修复:		
O %SystemRoot%\system32		
O %SystemRoot%		
O %SystemRoot%\System32\Wbem		
O %SYSTEMROOT%\System32\WindowsPowerShell\v	1.0\	
充激活检查		
象描述		
充未激活会很小概率会引发 Windows 实例出现一些未知异常 系统限制为微软设计的默认值2GB等。	。例如,系统激活注册表可能被损	坏,当机器在重启后出现内存
夬方法		
参考 Windows Server 系统激活 及 使用 slmgr 命令激活 '	Windows 系统 进行系统激活。	
时间检查		

现象描述

Windows 实例系统时间异常会导致依赖时间的业务出现异常,例如系统无法激活。

解决方法

请参考 Windows 实例: 配置 NTP 服务 配置系统时间同步。

系统路由表检查



现象描述

Windows 实例缺少系统默认路由会导致对应 IP 段路由不通,影响正常通信。

解决方法

Windows 实例初始化会执行以下7条命令来调整路由,您可通过以下命令进行修复。其中 \$Gateway 需替换为实例中实际的网 卡网关地址。

```
route delete 0.0.0.0 -p
route delete 169.254.0.0 -p
route add 0.0.0.0 mask 0.0.0.0 $Gateway -p
route add 169.254.0.0 mask 255.255.128.0 $Gateway -p
route change 10.0.0.0 mask 255.0.0.0 $Gateway -p
route change 172.16.0.0 mask 255.240.0.0 $Gateway -p
route change 192.168.0.0 mask 255.255.0.0 $Gateway -p
```

▲ 注意

若 route change xxx 相关命令执行失败,请替换为 route add xxx。

系统 IE 代理检查

现象描述

Window 实例内部若配置了 IE 代理,则可能影响网络访问和域名解析。

解决方法

1. 登录实例,详情请参见 使用标准方式登录 Windows 实例(推荐)。

2. 在操作系统中打开 IE 浏览器,选择浏览器右上方的 🐵,单击弹出菜单中的 Internet 选项。



3. 在弹出的 "Internet 选项"窗口中,选择连接页签,并单击局域网设置。如下图所示:

Internet	t 选项							?	×
常规	安全	隐私	内容	连接	程序	高级			
ĸ	要没	置 Intern	et 连接,	, 单击"设置	₽".		设置	<u>{(U)</u>	
拨号	和虚拟专员	用网络设置	Ē						-
							添加	(D)	
							添加 VI	PN(<u>P</u>)	
							删除	(R)	
如界	腰为连接	酒置代理	服务器,	请选择"资	置".		设置	Ê(<u>S</u>)	
局域 LA 上ī	涵(LAN) N 设置不J 面的"设置	2 置 立用到拨 ⁴ "按钮。	寻连接。	对于拨号	受置 , 単き	⊧ [局域网	役置心]
				确定		取消	≝	应用促	Ŋ

- 🔗 腾讯云
 - 4. 在弹出的"局域网(LAN)窗口中",取消勾选"使用自动配置脚本"及"为 LAN 使用代理服务器"。如下图所示:

局域网(LAN)设置	>
自动配置	
自动酒置会覆盖手动设置。要确保使用手动设置,请禁用自动酒置。	
□自动检测设置(A)	
□使用自动配置脚本(S)	
地址(R)	
代理服务器	
□为 LAN 使用代理服务器(这些设置不用于拨号或 VPN 连接)区	
地址(上):	
· 确定 取消	

5. 单击确定。

CD-ROM 状态检查

现象描述

开源组件 Cloudbase-init 需要借助 CD-ROM 来完成一些基本功能配置,若 CD-ROM 不可用,则会影响控制台密码重置等功能。

解决方法

- 1. 登录实例,详情请参见 使用标准方式登录 Windows 实例(推荐)。
- 2. 在操作系统桌面左下角右键单击日,在弹出菜单中选择 设备管理器。
- 3. 在弹出的"设备管理器"窗口中,展开"DVD/CD-ROM驱动器",并检查"QEMU QEMU DVD-ROM ATA Device"。



若 "QEMU QEMU DVD-ROM ATA Device"设备如下图所示,则请右键单击设备,并在弹出菜单中选择启用设备。



- 4. 在操作系统桌面左下角右键单击于,在弹出菜单中选择磁盘管理。
- 5. 在弹出的"磁盘管理器"中,查看 CD-ROM 是否具备驱动器号。



5.1 若 CD-ROM 如下图所示无驱动器号,则请右键单击 CD-ROM,选择更改驱动器号和路径。

🗃 磁盘管理						_		×
文件(F) 操作(A) 3	查看(V) 帮助(H)						
	1 🔎 🖅							
卷	布局	类型	文件系统	状态	容量	可用空间	% 可用	
🕳 (C:)	简单	基本	NTFS	状态良好 (49.46 GB	33.96 GB	69 %	
- System Reserved	简单	基本	NTFS	状态良好 (549 MB	514 MB	94 %	
- 磁盘 0								^
基本	System Rese	rved		(C:)				_
50.00 GB	549 MB NTFS		4	49.46 GB NTFS				
時利	状态良好 (系统	,活动,主分图	≍) ≯	伏态良好 (启动, 页)	面文件,故障转储,	主分区)		
CD-ROM 0								
CD-ROM								
无媒体								~
■ 未分配 ■ 主分区								

5.2 在弹出的"更改 0 MB CDFS CD-ROM 0 的驱动器号和路径"窗口中,单击添加。

5.3 在"添加驱动器号或路径"窗口中选择"分配以下驱动器号",按需选择驱动器号后,单击确定。

内存使用率过高

现象描述

内存使用率过高,系统性能会降低,可用内存资源不足可能会导致系统变得卡顿。

解决方法

1. 登录实例,详情请参见 使用标准方式登录 Windows 实例(推荐)。 若因内存过高无法登录,请参考 Windows 实例:CPU 或内存占用率高导致无法登录 进行排查。

2. 通过检查结果,或任务管理器查看占用内存最高的进程。本文以使用任务管理器查看,步骤如下:

2.1 在操作系统桌面左下角右键单击 , 在弹出菜单中选择 Windows PowerShell (管理员)。

2.2 在 powershell 窗口中输入 resmon 并按 Enter, 打开"资源监视器"。

2.3 在"资源监视器"窗口中,确认占用内存最高的进程运行是否正常。如下图所示:

1641A CPU P315 182								
进程	🧮 35% 已月	物理内存				۲		视图
	PID	硬中断/秒	提交(KB)	工作集(KB)	可共享(KB)	专用(KB) /	使用的物:	
MsMpEng.exe	1840	0	279,444	250,920	66,196	184,724		
ServerManager.exe	1244	0	89,308	73,864	27,544	46,320		
powershell.exe	5420	0	73,920	83,368	43,492	39,876		
svchost.exe (netsvcs)	844	0	37,616	159,808	127,372	32,436		
svchost.exe (termsvcs)	852	0	38,340	45,460	21,600	23,860		
dwm.exe	1916	0	28,316	60,472	41,492	18,980	60 秒	0
ShellExperienceHost.exe	5076	0	21,592	60,460	41,908	18,552	内存使用	100
explorer.exe	3980	0	21,200	77,940	64,084	13,856	-	
物理内存	📕 1461 ME	正在使用		2610 MB 🖪	J用			
为硬件保留的内存	正在使用	已修改		备用				0
1 MB	1461 MB	24 MB	_	1804 MB	806 MB		硬中断/利	۵ ا
		可用 2	610 MB					
		缓存 1	828 MB					
		总数 4	095 MB					
		D.S.衣 4	090 1010					

- 为业务目身需要,则请参考 调整实例配置 进行配置升级。
- 非业务自身进程,可优先通过更新系统补丁、安装杀毒软件进行全盘病毒扫描。

虚拟内存使用率高

腾讯云

现象描述

长期虚拟内存不足可能会导致 Windows 激活注册表损坏,出现内存被限制或登录受限制等问题。

解决方法

- 1. 登录实例,详情请参见 使用标准方式登录 Windows 实例(推荐)。
- 2. 在操作系统桌面左下角右键单击 田,在弹出菜单中选择 Windows PowerShell (管理员)。

3. 在 powershell 窗口中输入 sysdm.cpl 并按 Enter, 打开"系统属性"窗口。

- 🔗 腾讯云
 - 4. 在弹出的"系统属性"窗口中,选择**高级**页签,并单击"性能"下的设置。如下图所示:

系统属性	×
计算机名 硬件 高级 远程	
要进行大多数更改,你必须作为管理员登录。	
性能	
视觉效果,处理器计划,内存使用,以及虚拟内存	
设置(5)	•
用户配置文件	
与登录帐户相关的桌面设置	
设置(E)	
启动和故障恢复	
系统启动、系统故障和调试信息	
设置①	
环境变量(N)	
确定 取消 应	Ħ(A)



5. 在弹出的"性能选项"窗口中,选择**高级**页签,并单击**更改**。如下图所示:

性能选项	×
视觉效果 高级 数据执行保护	
处理器计划 选择如何分酉处理器资源。	
调整以优化性能:	
虚拟内存 分页文件是硬盘上的一块区域,Windows 当作 RAM 使用。	
所有驱动器总分页文件大小: 704 MB	,
	-
确定 取消 应用	(<u>A</u>)

6. 在弹出的"虚拟内存"窗口中,勾选"自动管理所有驱动器的分页文件大小",系统会自动选择磁盘空间充足的盘符进行虚拟 页面文件存放。如下图所示:



导个驱动器的分页文例	大小	
驱动器 [卷标](D)	分页文件	大小(MB)
C:	托	曾的系统
沂选驱动器:	C:	
可用空间:	35445 MB	
○ 自定义大小(C):		
初始大小(MB)():		
最大值(MB)(凶:		
◎ 系统管理的大小(Y)	
○无分页文件(№)		设置(S)
所有驱动器分页文件力	大小的总数	
允许的最小值:	16 MB	
推荐:	1407 MB	
当前已分配:	704 MB	

7. 单击确定。

() 说明

- 若您需自定义分页文件大小,则最大值务必不小于页面下方的"推荐值"。
- 因虚拟内存受物理内存和磁盘可用空间的影响,同时建议您调整实例资源配置,增加物理内存。详情请参见 调整实例配置。

总 CPU 使用率过高

现象描述

CPU 使用率过高,系统性能会降低,可用 CPU 资源不足系统可能导致实例变得卡顿,甚至无法登录。

解决方法

- 1. 登录实例,详情请参见 使用标准方式登录 Windows 实例(推荐)。 若因内存过高无法登录,请参考 Windows 实例:CPU 或内存占用率高导致无法登录 进行排查。
- 2. 通过检查结果、任务管理器或资源监视器查看占用 CPU 最高的进程。本文以使用资源监视器查看,步骤如下:

2.1 在操作系统桌面左下角右键单击 🕂, 在弹出菜单中选择 Windows PowerShell (管理员)。

2.2 在 powershell 窗口中输入 resmon 并按 Enter, 打开"资源监视器"。

2.3 在"资源监视器"窗口中,选择 CPU 页签,确认占用 CPU 最高的进程运行是否正常。如下图所示:

							-	- 🗆 X
文件(F) 监视器(M) 帮助(H)	100							
NGAL CFO MIF NGG	网络						1	
进程	10% CP	U 使用率		📃 100% 最大频率	ž		$\mathbf{\mathfrak{S}}$	视图 🚽
□ 名称	PID	描述	状态	线程数	СРО	平均 CPU 🔨	CPU - 总计	ך 100%
perfmon.exe	4512	资源和性…	正在运行	19	2	1.89		
svchost.exe (NetworkService)	1088	Windows	正在运行	22	2	0.11		
svchost.exe (termsvcs)	852	Windows	正在运行	30	1	0.45		
svchost.exe (netsvcs)	844	Windows	正在运行	47	1	0.06		
powershell.exe	5420	Windows	正在运行	13	1	0.06		
MsMpEng.exe	1840		正在运行	23	0	0.22	60 秒	0%
□ 系统中断	-	延迟过程…	正在运行	-	0	0.11	服务 CPU 使用率	ך 100% ד
rdpclip.exe	2680	RDP 剪贴	正在运行	10	0	0.11		
svchost.exe (LocalServiceN	412	Windows	正在运行	21	0	0.11		
NisSrv.exe	2820	Microsoft	正在运行	11	0	0.06		
svchost.exe (LocalServiceN	992	Windows	正在运行	15	0	0.06		
dwm.exe	1916	桌面窗口	正在运行	13	0	0.06		
csrss.exe	348		正在运行	10	0	0.05		0%
services.exe	548		正在运行	5	0	0.05	CPU 0	100% д
csrss.exe	2440		正在运行	10	0	0.05		
ntpdate.exe	2732	ntpdate	正在运行	4	0	0.00		
conhost.exe	4984	Console	正在运行	5	0	0.00 🗸		
服务	2% CPU	使用率				\odot		
关联的句柄				搜索句柄		₽ 4 📎		0%
关联的模块	_				_	\odot		100%

若排查出的业务:

- 为业务自身需要,则请参考 调整实例配置 进行配置升级。
- 非业务自身进程,可优先通过更新系统补丁、安装杀毒软件进行全盘病毒扫描。

单 CPU 使用率过高

腾讯云

现象描述

单个逻辑 CPU 使用率过高,而其他逻辑 CPU 使用率较低,导致 CPU 资源分配不均,无法充分发挥系统性能。

解决方法

- 1. 请通过检查结果定位占用单 CPU 最高的进程名。
- 2. 确认该进程运行是否正常。
 - 正常,则请忽略。
 - 异常,若非特定设置则建议优化异常进程 CPU 使用,或请联系程序设计厂商进行优化适配。

磁盘可用空间不足

现象描述

磁盘可用空间不足,会导致系统性能降低,磁盘写满可能会导致业务异常。

解决方法

确认磁盘中哪些文件占用空间最多:

- 是否为日志文件,或可清理文件。
- 若为业务正常需求文件,则建议尽快扩容磁盘,详情请参见 扩容场景介绍。



Ntfs 文件系统元文件磁盘占用高

现象描述

Ntfs 文件系统隐藏的元文件总大小占用过高,导致系统可用空间不足。

解决方法

可确定是有超大量文件生成导致该问题。若偶然出现该问题,则建议备份数据后,使用格式化磁盘的方式进行恢复。若经常出现该 问题,则建议检查业务程序是否有超大量文件生成,并优化业务程序。

远程桌面服务状态检查

现象描述

远程桌面服务状态异常,无法远程登录,只能通过 VNC 登录。

解决方法

- 1. 使用 VNC 登录 Windows 实例。
- 2. 在操作系统桌面左下角右键单击 —, 在弹出菜单中选择 Windows PowerShell (管理员)。
- 3. 在 powershell 窗口中执行以下命令,启动服务。

Get-Service termservice |Start-Service -Verbose

○ 正确返回结果如下图所示:



- 若在服务重启过程中卡住,则参考以下步骤处理。
- 3.1 执行以下命令,获取 PID。

sc.exe queryex termservice

如下图所示,PID 值为800。

 VICL_NUMPL
 : 20
 THE2_SMARK_PROCESS

 STAT
 : 4
 DERING

 STAT
 : 4
 DERING

 STAT
 : 0
 GANAR

 STAT
 CONTRACTOR

 STAT</td

3.2 使用已获取 PID,执行以下命令强制结束进程。

taskkill.exe /f /pid "PID**数字**"

PID 值为800,则执行以下命令。

taskkill.exe /f /pid 800

^{3.3} 执行以下命令,启动远程桌面服务。



Start-Service TermService

远程桌面服务端口检查

现象描述

远程桌面服务端口未监听,无法远程登录,只能通过 VNC 登录。

解决方法

🕛 说明

执行以下步骤时,请在每执行完一步后检查一次问题是否修复,若未修复则继续执行步骤。

1. 执行命令恢复

- 1.1 使用 VNC 登录 Windows 实例。
- 1.2 在操作系统桌面左下角右键单击 🛨,在弹出菜单中选择 Windows PowerShell (管理员)。
- 1.3 在 powershell 窗口中,执行以下命令进行恢复。

Set-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\' -Name fEnableWinStation -Value "1" -Force

2. 检查系统是否激活

- 2.1 在操作系统桌面左下角右键单击 🖽,选择设置。
- 2.2 在"设置"窗口中选择更新与安全,并在左侧单击激活。

2.3 检查系统是否已激活。若未激活,则请参考系统激活进行激活。

- 3. 重置 WinSock
 - 3.1 执行以下命令,重置 WinSock。

netsh.exe winsock reset

3.2 执行该命令后需重启实例,使配置生效。详情请参见 重启实例。

4. 修复多用户登录远程

若您已安装多用户登录的远程桌面功能,建议先卸载,待排查后再安装。 请参考以下步骤,导出及备份问题实例的注册表文件,并将正常实例的注册表文件导入至问题实例。

4.1 在操作系统桌面左下角右键单击 🕂 , 在弹出菜单中选择 Windows PowerShell (管理员)。

4.2 在 powershell 窗口中, 输入 regedit 并按 Enter, 打开"注册表编辑器"。

- 4.3 在"注册表编辑器"左侧文件树中,根据
 - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations 路径找 到 WinStations 文件。



4.4 右键单击 WinStations 文件,在弹出菜单中选择导出。如下图所示:

				-	×
文件(F) 编辑(E) 查看(V) 收藏夹(A) 帮助(H)	各称 eb (默认) 它 ConsoleSecurity 它 DefaultSecurity 同 Flags 题 SelfSignedCert eb SelfSignedCert	类型 REG_SZ REG_BINARY REG_BINARY REG_DWORD REG_BINARY REG_SZ	数据 (数值未设置) 01 00 14 80 9c 00 00 00 a8 00 00 00 00 00 00 00 01 00 14 80 b8 00 00 00 c4 00 00 00 14 00 0 0x0000001 (1) 8c 74 dd aa bb 1d c9 1f 47 b8 d7 c4 d3 c5 e Remote Desktop		
Video WalletServ WalletServ Wdf					

才算机\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations

4.5 在弹出窗口中设置导出文件名,本文以 WinStations.reg 为例。

4.6 单击确定,即可在已指定位置查看导出文件 WinStations.reg 。

- **4.7 备份完成后,请参考以上步骤导出正常实例的注册表** WinStations 文件,并将导出的 WinStations 文件导入异常 实例。请双击需导入的 WinStations.reg 文件,并在弹出窗口中单击是即可完成导入。
- 5. 检查 UMBus Root Bus Enumerator 设备状态
 - 5.1 右击桌面左下角 🕂 图标,选择设备管理器。如下图所示:



	应用和功能(F)			
	电源选项(O)			
	事件查看器(V)			
	系统(Y)			
	设备管理器(M)			
	网络连接(W)			
	磁盘管理(K)			
	计算机管理(G)			
	Windows PowerShell(I)			
	Windows PowerShell (管理员)(A)			
	任务管理器(T)			
	设置(N)			
	文件资源管理器(E)			
	搜索(S)			
	运行(R)			
	关机或注销(U) >			
	桌面(D)			
-	▶ 在此键入进行搜索	∐i	0	

5.2 在打开的设备管理器中,展开**系统设备**,检查 UMBus Root Bus Enumerator 设备状态,确保如下图所示,没有被禁用。



書 设备管理器	– 🗆 X
文件(F) 操作(A) 查看(V) 帮助(H)	
🗢 🔿 📰 📴 🗾 💷 🖳 🗶 🏵	
✓ 븝 10_7_0_8	
> 🔐 DVD/CD-ROM 驱动器	
> 📲 IDE ATA/ATAPI 控制器	
> 🔲 处理器	
> 🔜 磁盘驱动器	
> 🚂 存储控制器	
> 🏺 端囗 (COM 和 LPT)	
> 🛄 计算机	
> 🛄 监视器	
> 🔤 键盘	
> 🙀 人体学输入设备	
> 📓 软件设备	
> 📲 软盘驱动器控制器	
> 🕕 鼠标和其他指针设备	
> 🏺 通用串行总线控制器	
> 🚽 网络适配器	
> 1 系统设备	
🏣 ACPI 处理器容器设备	
🏣 ACPI 固定功能按钮	
🏣 CPU 到 PCI 桥	
🏣 Microsoft ACPI-Compliant System	
🏣 Microsoft System Management BIOS Driver	
🏣 Microsoft 虚拟驱动器枚举器	
🏣 NDIS 虚拟网络适配器枚举器	
🏣 PCI 到 ISA 桥	
The PCI 总线	
The UMBus Enumerator	
UMBus Root Bus Enumerator	
VirtIO Balloon Driver	
■ 即插即用软件设备枚举器	
■ 系统 CMOS/定时时轴	

RDP 侦听器启用检查

现象描述

RDP 侦听器未启用,无法远程登录,建议使用 VNC 登录进行恢复。

解决方法

- 1. 使用 VNC 登录 Windows 实例。
- 2. 在操作系统桌面左下角右键单击 🖽, 在弹出菜单中选择 Windows PowerShell (管理员)。
- 3. 在 powershell 窗口中,执行以下命令进行恢复。

Set-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp\' -Name fEnableWinStation -Value "1" -Force



:::

允许远程桌面连接检查

现象描述

RDP 被禁用,无法远程登录,建议使用 VNC 登录进行恢复。

解决方法

- 1. 使用 VNC 登录 Windows 实例。
- 2. 在操作系统桌面左下角右键单击 —, 在弹出菜单中选择 Windows PowerShell (管理员)。
- 3. 在 powershell 窗口中,执行以下命令进行恢复。

Set-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\' -Name
"fDenyTSConnections" -Value 0 -Force

RDP 自签证书到期时间检查

现象描述

RDP 自签证书过期,可能无法远程登录,建议使用 VNC 登录进行恢复。

解决方法

- 1. 使用 VNC 登录 Windows 实例。
- 2. 在操作系统桌面左下角右键单击 日, 在弹出菜单中选择 Windows PowerShell (管理员)。
- 3. 在 powershell 窗口中,依次执行以下命令进行恢复。

Remove-Item -Path 'Cert:\LocalMachine\Remote Desktop*' -Force -ErrorAction SilentlvContinue

Restart-Service TermService -Force

远程桌面服务角色安装及授权检查

现象描述

120天宽限期过后,还未导入 License 会导致无法远程登录,只能使用 VNC 登录。

解决方法

通常情况下,微软系统默认允许最多2个账号同时登录。若非必须,则建议您卸载远程桌面服务角色以快速修复问题。若需使用多 用户同时登录,则请拨打微软市场部热线(拨通 400-820-3800 后转2再转4)进行咨询购买 RDS CALs,详情请参见 设置允 许多用户远程登录 Windows 云服务器。

卸载及修复步骤步骤如下:

- 1. 使用 VNC 登录 Windows 实例。
- 2. 在操作系统桌面左下角右键单击 🖽,在弹出菜单中选择 Windows PowerShell (管理员)。
- 3. 在 powershell 窗口中,执行以下命令进行卸载。



Remove-WindowsFeature Remote-Desktop-Services

4. 重启实例,使配置生效。详情请参见 重启实例。

网络访问账户检查

现象描述

网络访问账户为仅来宾,无法远程登录,建议使用 VNC 登录进行恢复。

解决方法

- 1. 使用 VNC 登录 Windows 实例。
- 2. 在操作系统桌面左下角右键单击 🕂 , 在弹出菜单中选择 Windows PowerShell (管理员)。
- 3. 在 powershell 窗口中,依次执行以下命令进行恢复。

Set-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Control\Lsa -Name forceguest -Value 0 -Force

远程桌面服务端口防火墙放通检查

现象描述

Windows 实例内部防火墙未放通远程桌面服务端口,无法远程登录,只能使用 VNC 登录。

解决方法

- 1. 使用 VNC 登录 Windows 实例。
- 2. 在操作系统桌面左下角右键单击 🕂 , 在弹出菜单中选择 Windows PowerShell (管理员)。
- 3. 在 powershell 窗口中,输入 wf 并按 Enter, 打开 "高级安全 Windows 防火墙" 窗口。
- 4. 在"高级安全 Windows 防火墙"中,单击"概述"中的 Windows 防火墙属性。如下图所示:

```
💣 高级安全 Windows 防火墙
文件(F) 操作(A) 查看(V) 帮助(H)
🗢 🔿 🗖 🔂 👘
🔐 本地计算机 上的高级安全 Wind 本地计算机 上的高级安全 Windows 防火墙
 🌄 入站规则
 🌇 出站规则
                      高级安全 Windows 防火墙为 Windows 计算机提供网络安全。
 🍡 连接安全规则
> 🔜 监视
                   概述
                    域配置文件
                    😵 Windows 防火墙已关闭。
                    专用配置文件
                    🔯 Windows 防火墙已关闭。
                    公用配置文件是活动的
                    🔯 Windows 防火墙已关闭。
                    📑 Windows 防火墙属性
```

5. 在弹出的"本地计算机-属性"窗口中,分别切换至**域配置文件/专用配置文件/公用配置文件**页签,并将"防火墙状态"设置 为"关闭"。



```
        6. 单击确定保存设置。
        关闭实例本身防火墙后,请通过控制台中的安全组放通实例远程桌面端口,详情请参见 添加安全组规则。
```

端口耗尽检查

现象描述

由于高位可用 TCP 或 UDP 端口耗尽,可能导致网络不通。

解决方法

- 1. 使用 VNC 登录 Windows 实例。
- 2. 在操作系统桌面左下角右键单击 🕂 , 在弹出菜单中选择 Windows PowerShell (管理员)。
- 3. 在 powershell 窗口中,您可根据实际情况,选择以下方式:
 - 扩容端口。优先快速恢复业务,无需重启实例。

netsh int ipv4 set dynamicport tcp start=10000 num=55536

netsh int ipv4 set dynamicport udp start=10000 num=55536

```
○ 加快端口释放,同时扩容端口。推荐使用该方式,但需重启实例。
```

Set-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ -Name TcpTimedWaitDelay -Value 30 -Force

Timewait/Closewait 连接数检查

现象描述

可能会导致无法远程登录,甚至出现端口耗尽网络不通现象。

解决方法

- 1. 使用 VNC 登录 Windows 实例。
- 2. 在操作系统桌面左下角右键单击 任,在弹出菜单中选择 Windows PowerShell (管理员)。
- 3. 在 powershell 窗口中,执行以下命令,加快端口释放。

Set-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\ -Name TcpTimedWaitDelay -Value 30 -Force

建议优先使用安全组,仅放通必要的 IP 及端口号,以过滤部分恶意请求。同时按需更换 wait 连接数过多的默认业务端口号, 例如远程桌面服务默认端口号3389。

网关状态检查

现象描述

网关异常可能会导致机器网络不通。

解决方法

- 1. 使用 VNC 登录 Windows 实例。
- 2. 在操作系统桌面左下角右键单击 🕂 , 在弹出菜单中选择 Windows PowerShell (管理员)。
- 3. 在 powershell 窗口中,执行以下命令,对现有 IP 信息进行备份输出。

ipconfig /all >>C:\ip.txt

- 4. 在 powershell 窗口中,输入 ncpa.cpl 并按 Enter, 打开 "网络连接" 窗口。
- 5. 在"网络连接"窗口中,重启网卡:
 - 右键单击网卡,在弹出的菜单中选择禁用。
 - 再次右键单击后,再选择**启用**,以尝试快速修复。
- 6. 若仍未修复,请确认网卡是否为自动获取 IP 地址。若非此设置,建议调整为自动获取 IP 地址。步骤如下:
 - 6.1 在 "网络连接" 窗口中,右键单击网卡,在弹出的菜单中选择属性。

6.2 在弹出的"以太网 属性"窗口中,选择"Internet 协议版本 4(TCP/IPv4)",并单击属性。如下图所示:

网络	
连接时使用:	
Tencent VirtIO Ethernet Adapter	
酉晋(C)	
此连接使用下列项目():	
 ✓ 望QoS 数据包计划程序 ✓ Internet 协议版本 4 (TCP/IPv4) □ Microsoft 网络适酉器多路传送器协议 	
☑ _ Microsoft LLDP 协议驱动程序	
☑ _ Internet 协议版本 6 (TCP/IPv6)	
☑ _ 链路层拓扑发现响应程序	
安装(N) 卸载(U) 属性(R)	
描述	
传输控制协议/Internet 协议。该协议是默认的广域网络协议,用于在不同的相互连接的网络上通信。	
确定取消	
在弹出的 "Internet 协议版本 4(TCP/IPv4)"窗口中,选择"自动获得 IP 地址"。	
单击 确定 ,设置完成后再次检查网关状态。 若您无法通过此步骤修复,则可使用 <mark>步骤3</mark> 中备份的 IP 信息进行还原。	

MAC 地址检查

现象描述

MAC 地址异常可能会导致机器网络不通。

分 腾讯云

解决方法

- 1. 使用 VNC 登录 Windows 实例。
- 2. 在操作系统桌面左下角右键单击 🕂 , 在弹出菜单中选择 Windows PowerShell (管理员)。
- 3. 在 powershell 窗口中, 输入 ncpa.cpl 并按 Enter, 打开 "网络连接" 窗口。
- 4. 在"网络连接"窗口中,右键单击网卡,在弹出的菜单中选择属性。
- 5. 在弹出的"以太网 属性"窗口中,单击配置。如下图所示:

💚 以太网 属性	\times
网络	
连接时使用:	
🚽 Tencent VirtIO Ethernet Adapter	
配置(C)	٦
此连接使用下列项目():	-
✓ In Microsoft 网络客户端	•
☑ 🥊 Microsoft 网络的文件和打印机共享	
☑ 🦞 QoS 数据包计划程序	
☑ _ Internet 协议版本 4 (TCP/IPv4)	
🗌 🔔 Microsoft 网络适雪器多路传送器协议	
☑ _ Microsoft LLDP 协议驱动程序	
☑ _ Internet 协议版本 6 (TCP/IPv6)	
☑ _ 難路层拓扑发现响应程序	1
< >	
安装(N) 卸载(U) 属性(R)	
描述	
允许你的计算机访问 Microsoft 网络上的资源。	
确定取消	

6. 在弹出的 "Tencent VirtIO Ethernet Adapter 属性"窗口中,选择**高级**页签,并选择属性中的 Assign MAC,设置其为"不存在"。如下图所示:



带刀化	高级	驱动程序	详细信息	事	件			
此网络 边选 属性 Init. Init. Init. Init.	客适面器可 译它的值。 (P): Do802.1P ⁱ MaxRxBuf MaxTxBuf MTUSize Checksui	使用下列原 Q fers fers m Offload	摇性。 在左ù			更改的属 值(V):	3性 <i>, 然</i> D	ī
Larg Larg Log Max Offi Offi	ge Send C ge Send C ging.Enab ging.Leve kimum Nu oad.Rx.Ch oad.Tx.Ch	m Onibad iffload V2 iffload V2 ile mber of R ecksum ecksum O	(IPv4) (IPv6) RSS Queue					
Prio	rity and V	'LAN tagg	ing	*				

7. 甲击确定,保存设置。

8. 在"网络连接"窗口中,重启网卡:

○ 右键单击网卡,在弹出的菜单中选择禁用。

○ 再次右键单击后,再选择**启用**。

内网域名解析检查

现象描述

无法 nslookup 和 ping 通内网,导致系统无法激活、无法进行时间同步等。

解决方法

- 1. 使用 VNC 登录 Windows 实例。
- 2. 在操作系统桌面左下角右键单击 🕂 ,在弹出菜单中选择 Windows PowerShell (管理员)。
- 3. 在 powershell 窗口中,输入 ncpa.cpl 并按 Enter, 打开 "网络连接" 窗口。
- 4. 在"网络连接"窗口中,右键单击网卡,在弹出的菜单中选择属性。

5. 在弹出的"以太网 属性"窗口中,选择 "Internet 协议版本 4(TCP/IPv4)",并单击属性。如下图所示:

🚽 Te	en cent VirtlO	Ethernet Adapt	er		
				配置(C)	
比连接使	用下列项目(0):			
🗹 🖳 (QoS 数据包计:	划程序			^
⊻ _[nternet 协议提	反本 4 (TCP/IPv4			
🗆 💶 T	Microsoft 网络	話酒器多路传送	器协议		
🗹 🔔 ľ	Microsoft LLD	P 协议驱动程序			
ا 💶 🗹	nternet 协议提	反本 6 (TCP/IP∨6)		
🗹 🔔 🕯	莲路层拓扑发 现	则应程序			
🗹 🔔 🕯	莲路层拓扑发 现	₩映射器 /0 驱泳	腥序		
					. ×
`			_	,	
安	装(<u>N</u>)	卸载(U)		属性(R)	
描述					
14100	atilitativi /lintore		7日明治しめたね	ት አማቂ ቋቂ ተሰራ የፖ	m l
154803	Tell&rX/Inrei	uer Wirter Balarie	CE#AMAD/ 8	CMARHINLIX /	лэ

腾讯云

- 6. 在弹出的 "Internet 协议版本 4 (TCP/IPv4)" 窗口中:
 - 建议使用"自动获得 DNS 服务器地址"设置,或者添加 CVM 默认 DNS 地址(私有网络通常是 183.60.83.19 和 183.60.82.98)。
 - 若实例为域环境,则请单击高级,在"高级 TCP/IP 设置"窗口中,建议将 CVM 默认 DNS 地址放置在域 DNS 后。
- 7. 在 powershell 窗口中,执行以下命令,检查永久路由。

route print	
若返回结果中未包含 169.254.0.0 开头的路由信息,则建议执行以下命令进行添加。	
route add	169.254.0.0 mask 255.255.128.0 \$Gateway -p
▲ 注意 \$Gateway	需替换为您实际的网关地址。