# 云服务器

# 故障处理

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【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
实例相关故障
无法登录云服务器问题处理思路
Windows 实例登录相关问题
无法登录 Windows 实例
Windows 实例：发生身份验证错误
Windows 实例：重置密码失败或无效
Windows 实例：没有远程桌面服务登录的权限
Windows 实例：需要网络级别身份验证
Windows 实例：Mac 远程登录异常
Windows 实例：CPU 或内存占用率高导致无法登录
Windows 实例：无法连接到腾讯云服务器
Windows 实例：凭据不工作
Windows 实例：没有远程桌面授权服务器可以提供许可证
Windows 实例：端口问题导致无法远程登录
Linux 实例登录相关问题
无法登录 Linux 实例
Linux 实例：无法通过 SSH 方式登录
Linux 实例：修改密码后无法使用修改后的密码登录
Linux 实例：CPU 或内存占用率高导致登录卡顿
Linux 实例：端口问题导致无法登录
Linux 实例：VNC 登录报错 Module is unknown
Linux 实例：VNC 登录报错 Account locked due to XXX failed logins
Linux 实例：VNC 登录输入正确密码后无响应
Linux 实例：VNC 或 SSH 登录报错 Permission denied
Linux 实例：/etc/fstab 配置错误导致无法登录
Linux 实例：sshd 配置文件权限问题
Linux 实例：/etc/profile 死循环调用问题
服务器被隔离导致无法登录
带宽占用高导致无法登录
安全组设置导致无法远程连接
Linux 实例使用 VNC 及救援模式排障
关机和重启云服务器失败
内核及 IO 相关问题
系统 bin 或 lib 软链接缺失
云服务器疑似被病毒入侵问题
创建文件报错 no space left on device
系统 initramfs 或 initrd 损坏/丢失
Linux 实例内存相关故障
实例内存使用率过高
日志报错 fork：Cannot allocate memory
VNC 登录报错 Cannot allocate memory
实例内存未耗尽时触发 Out Of Memory
网络相关故障
国际链路时延
网站无法访问
网站访问卡慢
网卡多队列配置错误问题
使用 MTR 分析网络延迟及丢包
云服务器网络访问丢包
实例 IP 地址 ping 不通

域名无法解析（CentOS 6.x 系统）
Linux 上无法解析 tencentyun.com 相关域名

# 故障处理

## 实例相关故障

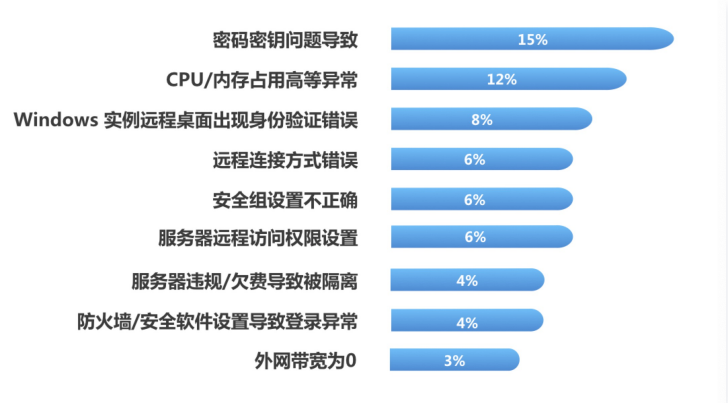
# 无法登录云服务器问题处理思路

最近更新时间：2024-12-11 11:23:42

本文主要为购买云服务器（Cloud Virtual Machine，CVM）实例后无法登录的问题提供解决思路，帮助您定位及解决无法登录云服务器问题。

## 现象描述

下图显示了无法连接 CVM 实例的主要原因分类及出现概率。若您无法连接实例，建议结合智能诊断工具，按照如下原因进行排查。




## 故障处理

### 检查确认 Windows 和 Linux 系统之间实例的不同类型

首先，您需要了解您购买的实例类型是 Windows 系统实例还是 Linux 系统实例。其次，针对不同的实例类型，可能导致无法登录云服务器的原因不同。您可以根据购买的实例类型，参考以下文档定位及解决问题：

- 无法登录 Windows 实例
- 无法登录 Linux 实例

### 通过自助诊断工具和安全组（端口）验通工具检查诊断无法登录的原因

腾讯云提供了 自助诊断工具 和 安全组（端口）验通工具 帮助您判断可能导致无法登录的原因。70%左右的登录问题可以通过工具检查并定位。

#### 自助诊断工具

诊断的问题包含带宽利用率过高、外网带宽为0、服务器高负载、安全组规则不当、DDoS 攻击封堵、安全隔离和账户欠费等。

#### 安全组（端口）验通工具

检测安全组和端口相关故障。如果存在安全组设置问题，您可以通过该工具的**一键放通**功能放通所有安全组常用接口。
如果通过工具定位到问题原因，建议您根据问题原因指引进行相应的故障处理。

### 重启实例

完成检查工具判断并处理相应故障后，或者通过检查工具仍无法定位无法登录的原因，您都可以通过重启实例，然后再次进行远程连接，查看是否连接成功。
重启实例的操作可参见 重启实例 。

## 相关参考

如果通过以上处理步骤均无法定位问题原因，或者您在登录云服务器时直接返回以下类型的错误信息，均可以参考以下解决方案。

### Windows 实例

- Windows实例：没有远程桌面服务登录的权限
- Windows 实例：Mac 远程登录异常
- Windows 实例：发生身份验证错误
- Windows 实例：需要网络级别身份验证
- Windows 实例：远程桌面无法连接到远程计算机

### Linux 实例

Linux 实例： CPU 与内存占用率高导致无法登录

如果通过以上步骤仍无法解决您无法远程登录的问题，您可以保存相关日志和自检结果，通过 在线支持 反馈和解决问题。

# Windows 实例登录相关问题

## 无法登录 Windows 实例

最近更新时间：2025-06-03 11:17:42

以下视频介绍了无法登录 Windows 实例时的排查方法：
观看视频
本文主要介绍无法连接 Windows 实例时对问题进行排查的方法，以及可能导致无法连接 Windows 实例的主要原因，指导您排查、定位并解决问题。

## 可能原因

无法登录 Windows 实例的主要原因包括：

- 密码问题导致无法登录
- 带宽利用率过高
- 服务器高负载
- 远程端口配置异常
- 安全组规则不当
- 防火墙或者安全软件导致登录异常
- 远程桌面连接出现身份验证错误

## 使用自助诊断工具

腾讯云提供自助诊断工具，可以帮助您判断是否由于带宽、防火墙以及安全组设置等常见问题导致无法连接 Windows 实例。70%的故障可以通过工具定位，您可以根据检测到的原因，定位可能引起无法登录的故障问题。

1. 单击 自助诊断，打开自助诊断工具。
2. 根据实例自助检测界面提示，选择需要诊断的云服务器，单击**开始检测**。如下图所示：

如果您的问题无法通过故障排查工具检查，建议您 通过 VNC 的方式登录 云服务器逐步排查故障。

## 故障处理

### 通过 VNC 方式登录

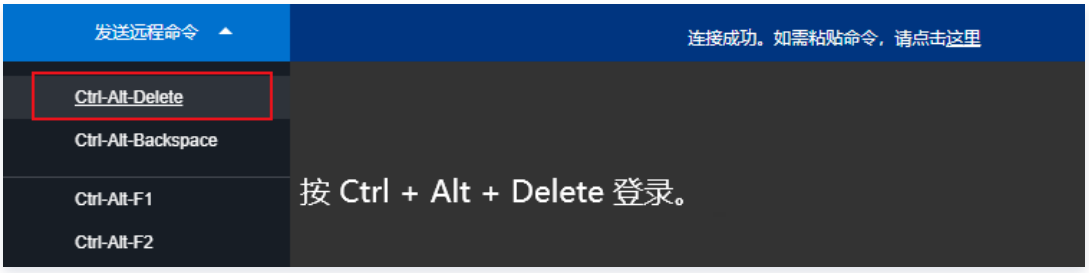
当您无法通过 RDP 或者远程登录软件登录 Windows 实例时，您可以使用腾讯云 VNC 登录的方式登录，帮助您定位故障原因。

1. 登录 腾讯云控制台 。
2. 在实例的管理页面，选择您需要登录的实例，单击**登录**。如下图所示：

3. 在弹出的**标准登录 | Windows 实例**窗口中，选择 **VNC 登录**。

> **说明：**
> 登录过程中，如果忘记密码，可以在控制台中重置该实例的密码。具体操作可参见 重置实例密码 。

4. 在弹出的登录窗口中，选择左上角的**发送远程命令**，单击 **Ctrl-Alt-Delete** 进入系统登录界面。如下图所示：




## 密码问题导致无法登录

**故障现象：**密码输入错误、忘记密码或者密码重置失败导致登录不成功。
**处理步骤：**请在 腾讯云控制台 重置该实例的密码，并重启实例。详情请参见 重置实例密码 。

## 带宽利用率过高

**故障现象：**通过自助诊断工具诊断，提示问题为带宽利用率过高。
**处理步骤：**

1. 通过 VNC 方式 登录实例。
2. 参见 带宽占用高导致无法登录，查看实例的带宽使用情况和处理故障。

## 服务器高负载

**故障现象：**通过自助检查工具或者腾讯云可观测平台，显示服务器 CPU 负载过高导致系统无法进行远程连接或者访问非常卡。
**可能原因：**病毒木马、第三方杀毒软件、应用程序异常、驱动异常或者软件后台的自动更新，会造成 CPU 占用率高，导致登录不上云服务器或者访问慢的问题。
**处理步骤：**

1. 通过 VNC 方式 登录实例。
2. 参见 Windows 实例：CPU 与内存占用率高导致无法登录，在**任务管理器**中定位高负载的进程。

## 远程端口配置异常

**故障现象：**远程无法连接，远程访问端口非默认端口、被修改或者3389端口没打开。
**定位思路：**是否能 ping 通实例的公网 IP，通过 telnet 命令检测端口是否打开。
**处理步骤：**具体操作可参见 端口问题导致无法远程登录 。

## 安全组规则不当

**故障现象：**通过自助检查工具检查，发现安全组规则设置不当导致无法登录。
**处理步骤：**通过 安全组（端口）验通工具 进行检查。

> **注意：**
> 远程登录的 Windows 实例需要放通3389端口。

如果您需要自定义设置安全组规则，请参见 添加安全组规则 重新配置安全组规则。

## 防火墙或者安全软件导致登录异常

**故障现象：**由于云服务器防火墙的配置或者安全软件导致登录异常。
**定位思路：**通过 VNC 登录的方式登录 Windows 实例，检查服务器内部是否开启防火墙，是否有安装360、安全狗等安全软件。

> **注意：**
> 此操作涉及关闭云服务器防火墙，您需要确认自己是否有权限执行此操作。

**处理步骤：**关闭防火墙或者安装的安全软件，再次尝试远程连接，确认是否能远程登录成功。以下操作以关闭 Windows Server 2016 实例的防火墙为例。

1. 通过 VNC 方式 登录实例。
2. 在操作系统界面，单击 ⊞，选择**控制面板**，打开控制面板窗口。
3. 单击**系统和安全**，再单击 **Windows 防火墙**，进入Windows 防火墙界面。
4. 单击左侧的**启用或关闭 Windows 防火墙**，进入**自定义设置**界面。
5. 将**专用网络设置**和**公用网络设置**设置为**关闭 Windows 防火墙**，单击**确定**。
6. 重启实例，再次尝试远程连接，确认是否能远程登录成功。

### 远程桌面连接出现身份验证错误

**故障现象：**通过远程桌面连接登录 Windows 实例时，出现**发生身份验证错误，给函数提供标志无效或发生身份验证错误。要求的函数不受支持**的报错。
**问题原因：**微软于2018年3月发布了一个安全更新，此更新通过更正凭据安全支持提供程序协议（CredSSP）在身份验证过程中验证请求的方式来修复 CredSSP 存在的远程执行代码漏洞。客户端和服务器都需要安装此更新，否则可能出现问题描述中的情况。
**处理步骤：**推荐通过安装安全更新的方式解决，具体可参见 Windows 实例：发生身份验证错误 。

**故障现象：**通过远程桌面连接登录 Windows 实例时，提示**安全账户管理器（SAM）或本地安全机构（LSA）服务器处于运行安全操作的错误状态**的报错。
**问题原因：**这种问题有可能是Kerberos 票证过期或不可用的原因，例如 Windows 安装了缺陷补丁或安全软件影响了 SamSs 服务的正常运行。一般是由于微软Windows 设计存在的极低概率缺陷所致。
**处理步骤：**重启机器即可恢复正常。

## 其它解决方案

通过上述排查后，仍然不能连接 Windows 实例，请您保存自助诊断结果，通过 在线支持 进行反馈。

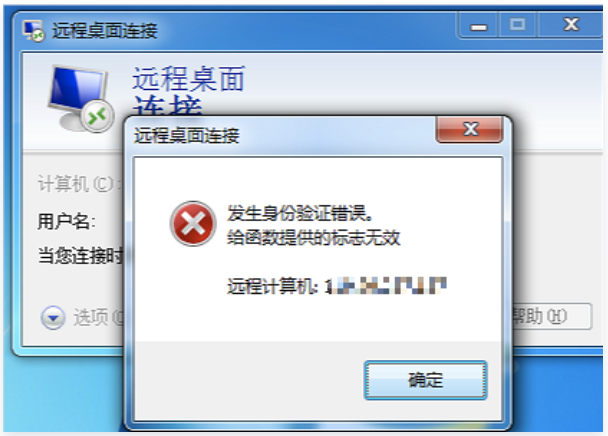
# Windows 实例：发生身份验证错误

最近更新时间：2024-09-24 10:18:41

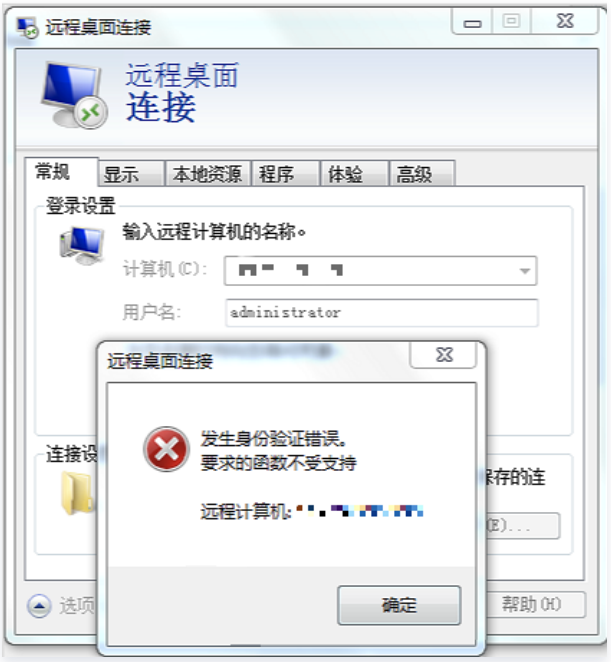
## 现象描述

通过远程桌面连接登录 Windows 实例时，出现以下报错：

- **发生身份验证错误，给函数提供的标志无效**，如下图所示：




- **发生身份验证错误。要求的函数不受支持**，如下图所示：




由于微软于2018年3月发布了一个安全更新，此更新通过更正凭据安全支持提供程序协议（CredSSP），以及在身份验证过程中验证请求的方式，修复 CredSSP 存在的远程执行代码漏洞。客户端和服务器都需要安装此更新，否则可能出现问题描述中的情况。

| | | 服务器 | | | |
|---|---|---|---|---|---|
| | | 未修补 | 强制更新的客户端 | 缓解 | 易受攻击 |
| 客户端 | 未修补 | 允许 | 阻止 | 允许 | 允许 |
| | 强制更新的客户端 | 阻止 | 允许 | 允许 | 允许 |
| | 缓解 | 阻止 | 允许 | 允许 | 允许 |
| | 易受攻击 | 允许 | 允许 | 允许 | 允许 |

如上图所示，以下三种情况均会引起远程连接失败：

- 情况一：客户端未修补，服务器安装了安全更新，并且策略配置为**强制更新的客户端**。
- 情况二：服务器未修补，客户端安装了安全更新，并且策略配置为**强制更新的客户端**。
- 情况三：服务器未修补，客户端安装了安全更新，并且策略配置为**缓解**。

## 可能原因

| 可能原因 | 处理措施 |
|---|---|
| 服务器或客户端未安装安全更新 | 检查服务端或客户端并安装安全更新（推荐） |
| 本地组策略未配置 | 检查并修改本地组策略配置 |
| 系统中的注册表未修改 | 检查并修改系统中的注册表 |

## 故障处理

### 通过 VNC 登录云服务器

VNC 登录是腾讯云为用户提供的一种通过 Web 浏览器远程连接云服务器的方式。在没有安装或者无法使用远程登录客户端，以及通过其他方式均无法登录的情况下，用户可以通过 VNC 登录连接到云服务器，观察云服务器状态，并且可通过云服务器账户进行基本的云服务器管理操作，具体操作请参见：使用 VNC 登录 Windows 实例。

### 检查服务端或客户端并安装安全更新（推荐）

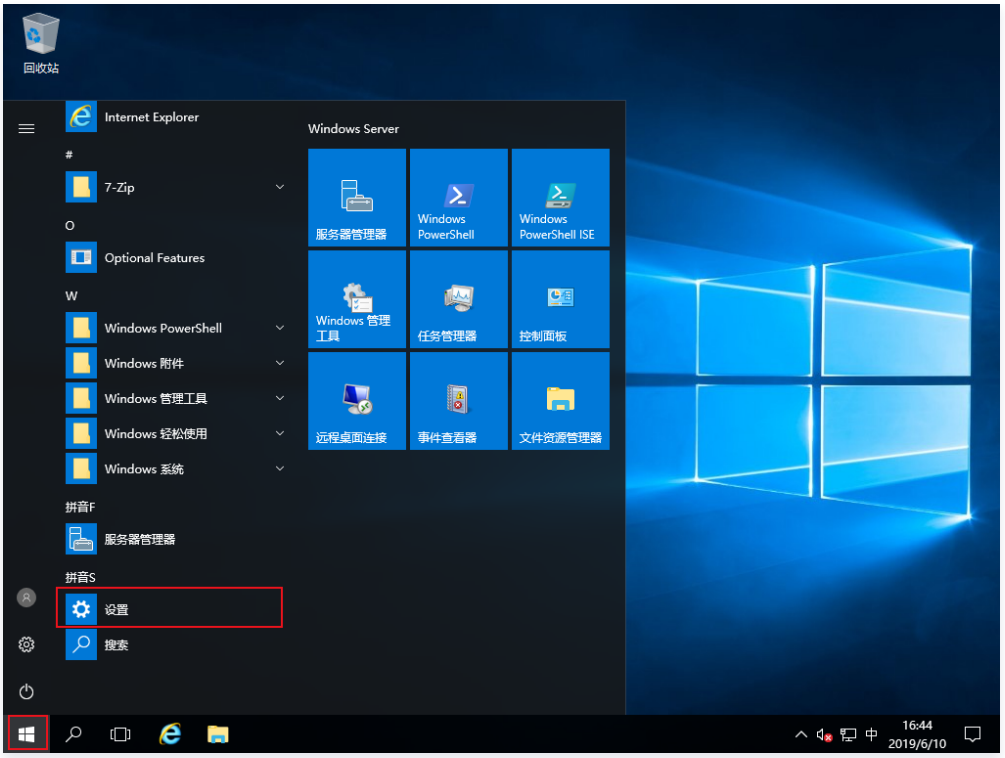
安装安全更新，可更新未修补的服务端或客户端。不同系统对应的更新情况可参见 CVE-2018-0886 | CredSSP 远程执行代码漏洞。

> **说明：**
> - 本方案以 Windows Server 2016 为例。
> - Windows Server 2016及以上版本操作方式相同。

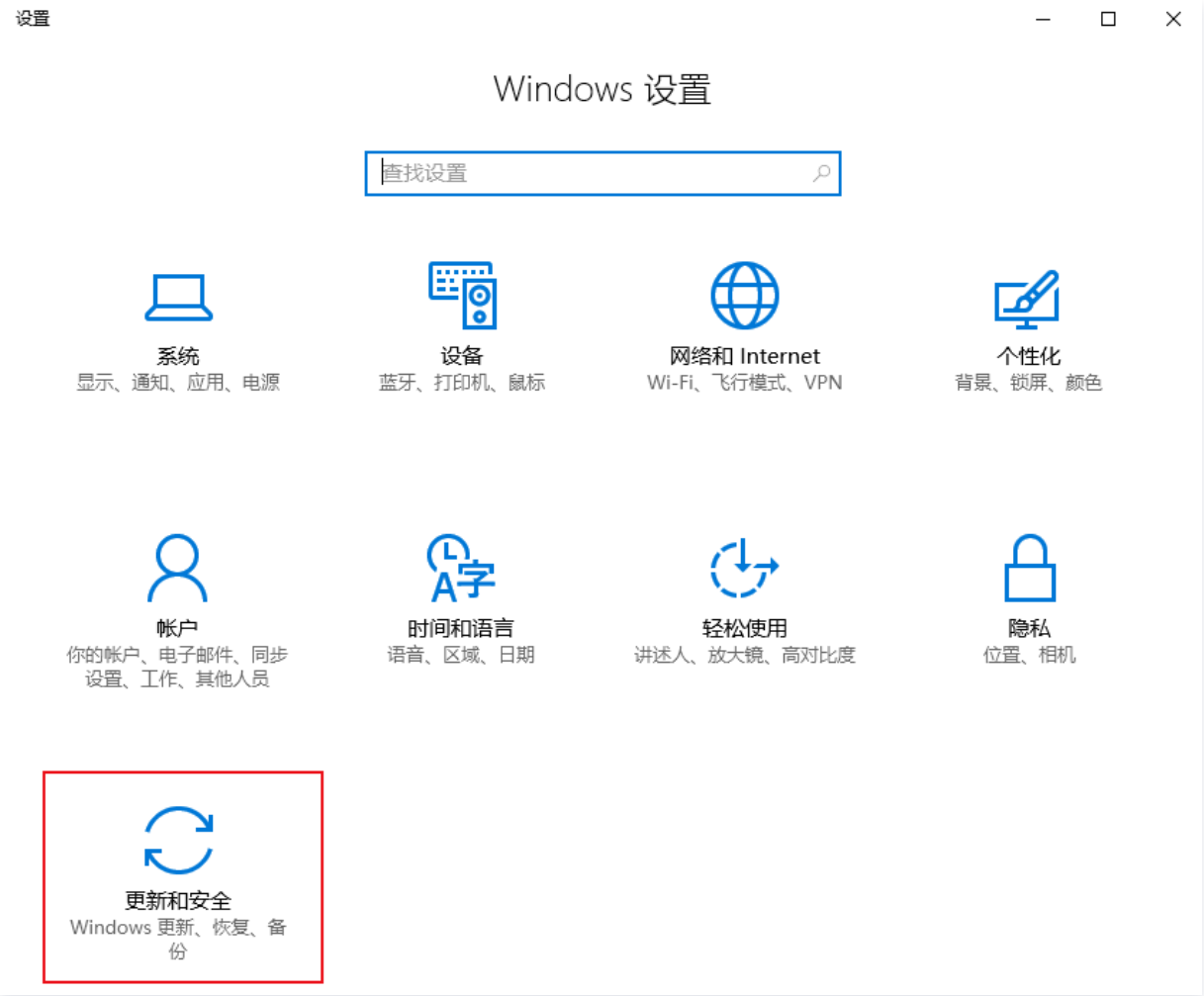
其他操作系统可参见以下操作进入 **Windows 更新**：

- Windows Server 2012：> **控制面板** > **系统和安全** > **Windows 更新**
- Windows Server 2008：**开始** > **控制面板** > **系统和安全** > **Windows Update**
- Windows10：> **设置** > **更新和安全**
- Windows 7：> **控制面板** > **系统和安全** > **Windows Update**

1. 在操作系统界面，单击 ，选择**设置**。如下图所示：




2. 在打开的**设置**窗口中，选择**更新和安全**。如下图所示：



3. 在**更新和安全**中，选择 **Windows 更新**，单击**检查更新**。如下图所示：

4. 根据界面提示，单击**开始安装**。
5. 安装完成后，重启实例，完成更新。

## 检查并修改本地组策略配置

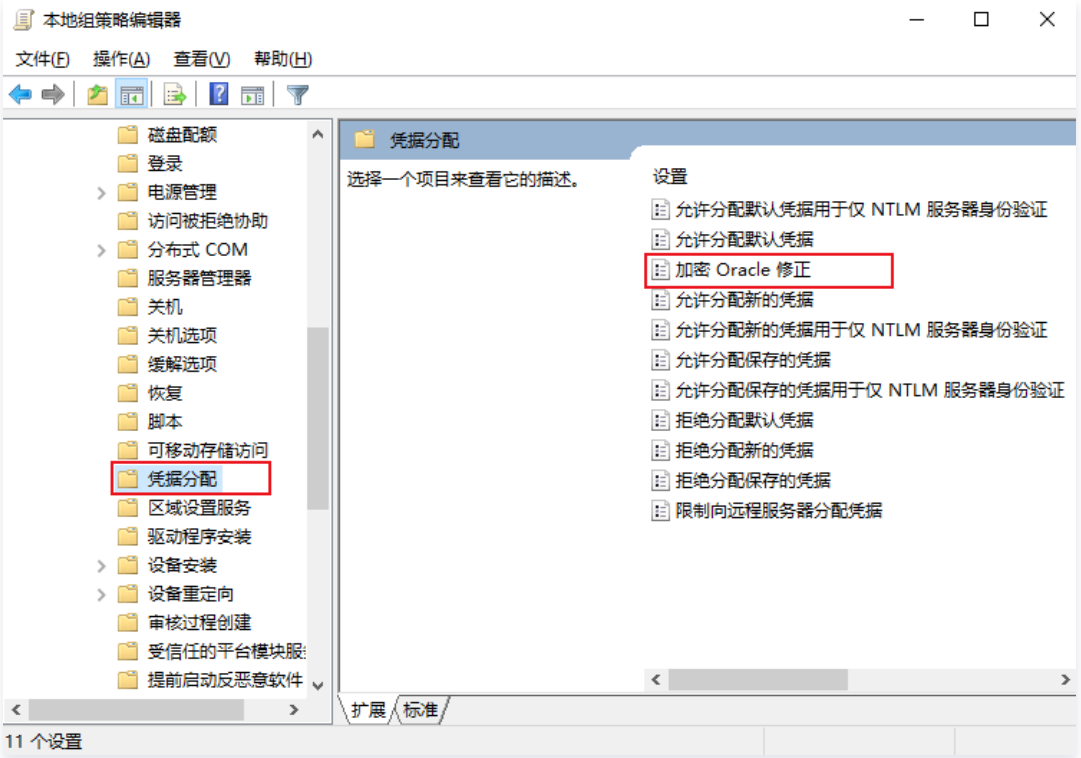
在已安装安全更新的机器中，将**加密 Oracle 数据库修正**策略设置为**易受攻击**。本方案以 Windows Server 2016 为例，其操作步骤如下：

> **注意:**
> Windows 10 家庭版操作系统中，若没有组策略编辑器，可通过修改注册表来实现。操作步骤请参见 检查并修改系统中的注册表 。

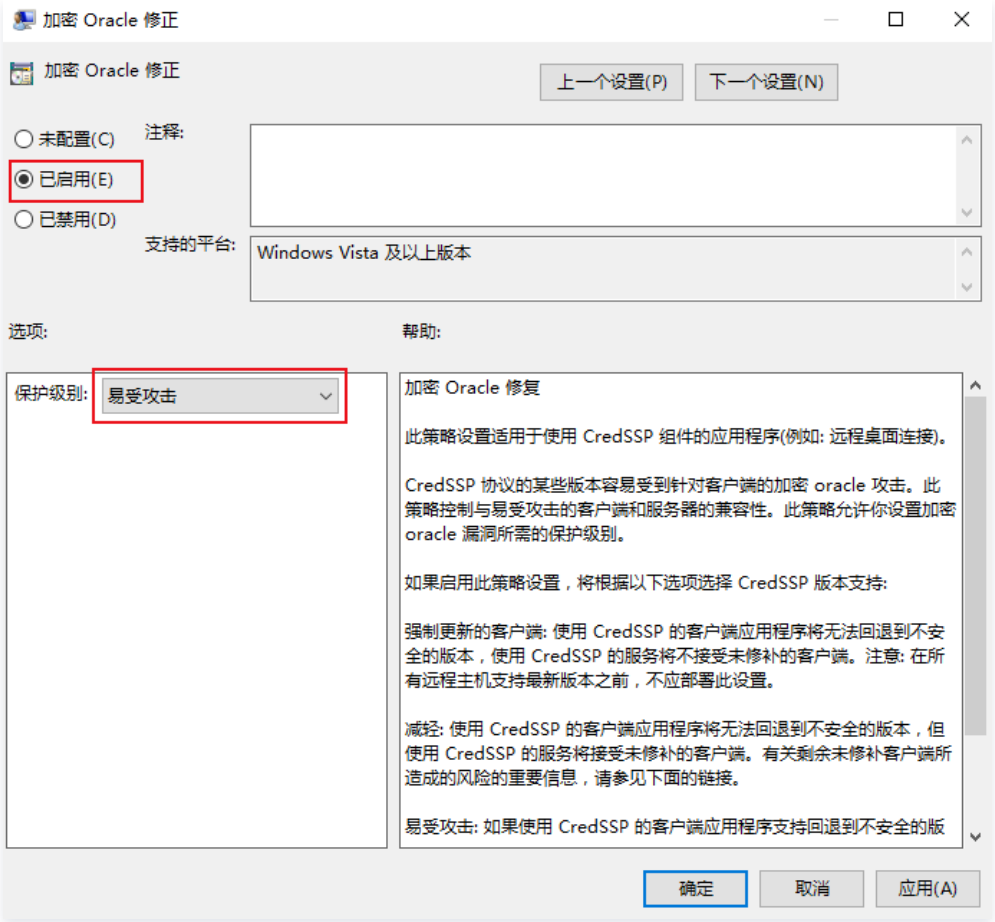
1. 在操作系统界面，单击 ，输入 **gpedit.msc**，按 **Enter**，打开**本地组策略编辑器**。

> **说明:**
> 您也可使用 **Win+R** 快捷键打开运行界面。

2. 在左侧导航栏中，选择**计算机配置 > 管理模板 > 系统 > 凭据分配**，双击**加密 Oracle 数据库修正**。如下图所示：




3. 在打开的**加密 Oracle 修正**窗口中，选择**已启用**，并将**保护级别**设置为**易受攻击**。如下图所示：




4. 单击**确定**，完成设置。

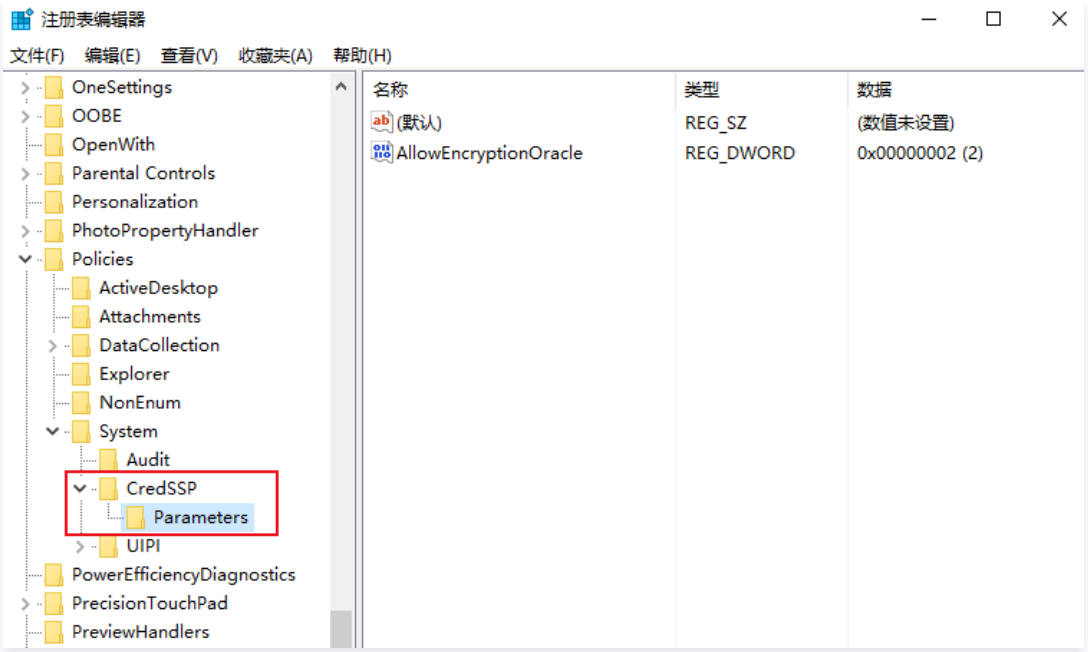
## 检查并修改系统中的注册表

1. 在操作系统界面，单击 ，输入 regedit，按 Enter，打开注册表编辑器。

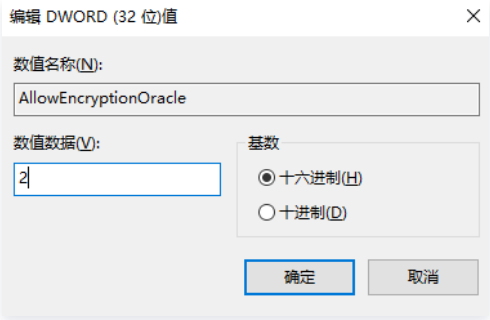
> **说明：**
> 您也可使用 Win+R 快捷键打开运行界面。

2. 在左侧导航树中，依次展开**计算机** > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Windows > CurrentVersion > Policies > System > CredSSP > Parameters 目录。如下图所示：

> **说明：**
> 若该目录路径不存在，请手动创建。




3. 右键单击 Parameters，选择**新建** > **DWORD(32位)值**，并将文件名称命名为 AllowEncryptionOracle。
4. 双击新建的 AllowEncryptionOracle 文件，将**数值数据**设置为2，单击**确定**。如下图所示：




5. 重启实例。

## 相关参考

- CVE-2018-0886 | CredSSP 远程执行代码漏洞
- CVE-2018-0886 的 CredSSP 更新

# Windows 实例：重置密码失败或无效

最近更新时间：2025-04-17 11:08:32

## 现象描述

- 重置云服务器密码后，提示“由于系统繁忙，您的实例重置实例密码失败(7617d94c)”。
- 重置云服务器密码后，新密码不生效，登录密码仍为原密码。

## 可能原因

| 可能原因 | 处理措施 |
| --- | --- |
| cloudbase-init 组件损坏、被修改、禁止或者未启动 | 检查 cloudbase-init 服务 |
| 云服务器中安装的安全软件拦截了重置密码组件 | 检查云服务器中安装的安全软件确保未拦截重置密码组件 |

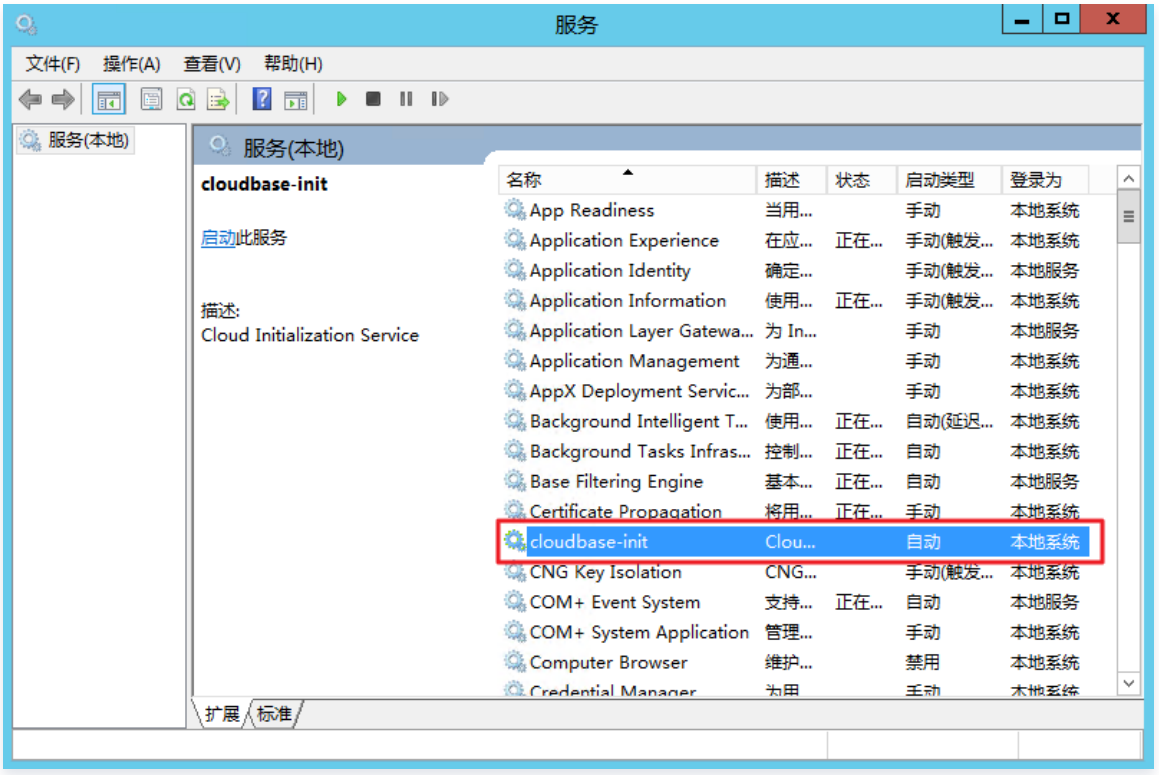
## 故障处理

> **说明：**
> 本文档以 Windows Server 2012 操作系统为例，介绍 Windows 云服务器实例因重置密码失败或者不生效的排查方法和解决方案。

根据引起密码重置不成功的可能原因，提供以下两种检查方式：

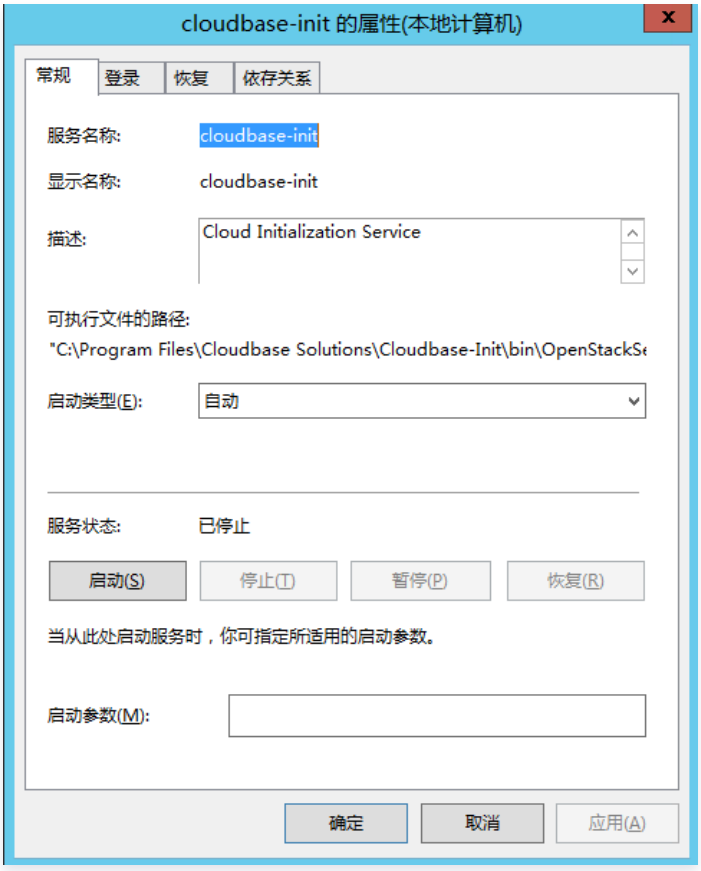
### 检查 cloudbase-init 服务

1. 参见 使用标准方式登录 Windows 实例（推荐），登录目标 Windows 实例。
2. 在操作系统界面，右键单击 ，选择**运行**，并在**运行**中输入 **services.msc**，并按 **Enter**，打开**服务**窗口。
3. 检查是否存在 `cloudbase-init` 服务。如下图所示：

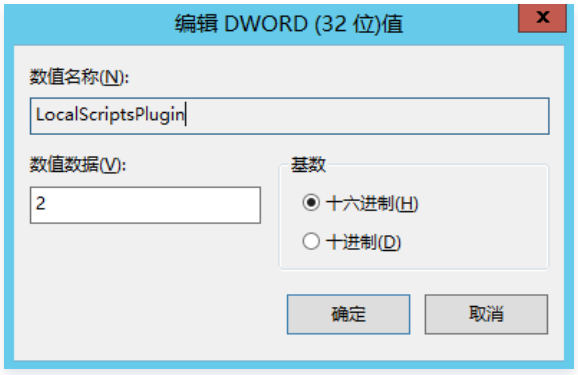



- 已存在 `cloudbase-init` 服务，执行下一步。
- 未存在 `cloudbase-init` 服务，重新安装 `cloudbase-init` 服务。具体操作请参见 Windows 操作系统安装 Cloudbase-Init。

4. 双击打开 `cloudbase-init` 的属性。如下图所示：

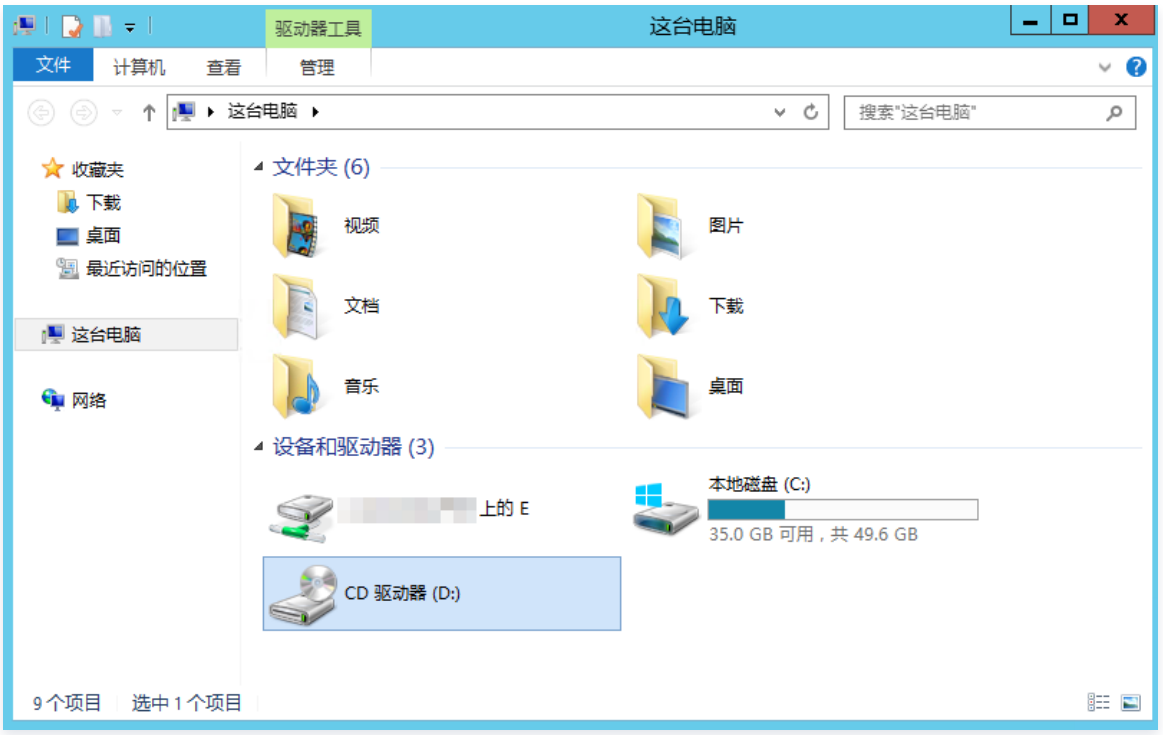



5. 在**常规**页签，检查 `cloudbase-init` 的启动类型是否设置为**自动**。
   - 已设置，执行下一步。
   - 未设置，将 `cloudbase-init` 的启动类型设置为**自动**。
6. 切换至**登录**页签，检查 `cloudbase-init` 的登录身份是否选择为**本地系统账户**。
   - 已选择为**本地系统账户**，执行下一步。
   - 未选择为**本地系统账户**，将 `cloudbase-init` 的登录身份设置为**本地系统账户**。
7. 切换至**常规**页签，单击服务状态的**启动**，手动启动 `cloudbase-init` 服务并观察是否报错。
   - 报错，检查云服务器中安装的安全软件确保未拦截重置密码组件 。
   - 未报错，执行下一步。
8. 在操作系统界面，右键单击 ，选择**运行**，并在**运行**中输入 **regedit**，并按 **Enter**，打开**注册表编辑器**窗口。
9. 在左侧的注册表导航中，依次展开 **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Cloudbase Solutions** > **Cloudbase-Init** 目录。
10. 找到 **ins-xxx** 下的全部 “LocalScriptsPlugin” 注册表，并检查 LocalScriptsPlugin 的数值数据是否为2。




   - 数值数据为2，执行下一步。
   - 数值数据不为2，将 LocalScriptsPlugin 的数值数据设置为2。

11. 在操作系统界面，单击 ，选择**这台电脑**，检查设备和驱动器中是否加载了 CD-驱动器。如下图所示：




- 已加载，检查云服务器中安装的安全软件确保未拦截重置密码组件。
- 未加载，在设备管理器中启动 CD-ROM 驱动器。

## 检查云服务器中安装的安全软件确保未拦截重置密码组件

在已安装的安全软件上，选择全盘扫描，检查云服务器是否有漏洞，以及检查 `cloudbase-init` 的核心组件是否被拦截。

- 如检查出云服务器有漏洞，请修复。
- 如检查出核心组件被拦截，请取消拦截。

`cloudbase-init` 组件检查及配置步骤如下：

1. 参见 使用标准方式登录 Windows 实例（推荐），登录目标 Windows 实例。
2. 对应实际安装的第三方安全软件，恢复并设置 `cloudbase-init` 组件。

**360安全卫士**

360安全卫士安装完成后，会定期扫描系统，如果扫描到 `cloudbase-init` 组件，则会认为其高风险，将其隔离。请参见以下步骤恢复组件，并设置为信任文件：

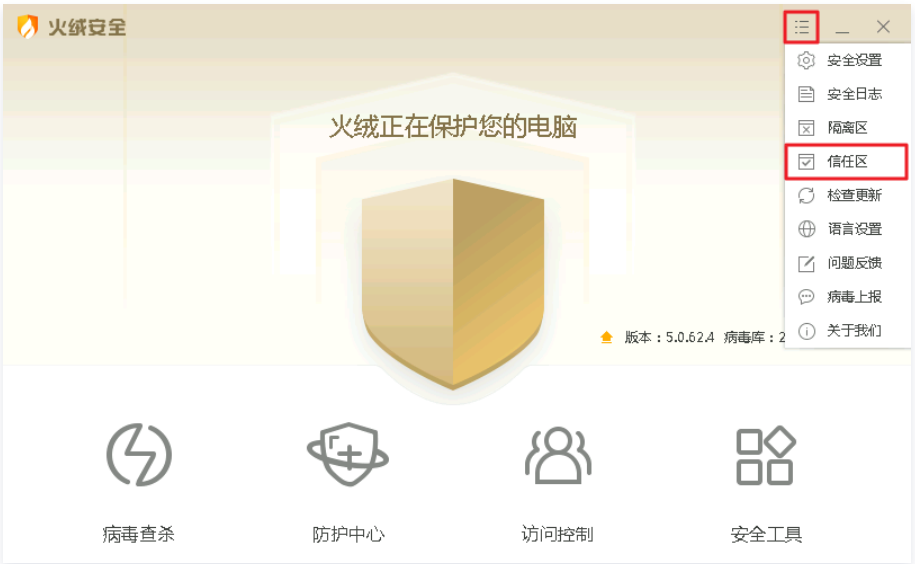
1. 打开360安全卫士，选择**木马查杀** > **恢复区**。如下图所示：

2. 在弹出的**安全操作中心**窗口中，勾选文件并单击**恢复所选**。
3. 在弹出的确定窗口中，勾选**恢复后信任此文件，不再查杀**，并单击**恢复**即可。如下图所示：

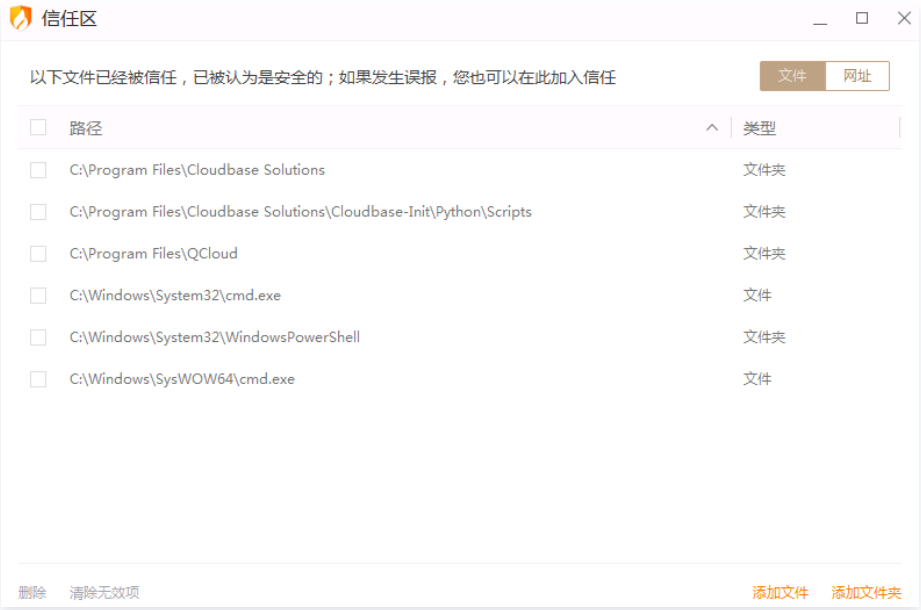
### 火绒安全软件

火绒安全软件安装完成后，不会主动将 `cloudbase-init` 组件隔离，而是会拦截 `cloudbase-init` 修改密码的行为。请参见以下步骤设置组件为信任文件：

1. 打开火绒安全软件，选择右上角的 ☰，并在弹出菜单中单击**信任区**。如下图所示：



2. 在弹出的**信任区**窗口中，依次添加下列文件及文件夹即可。如下图所示：




**文件及文件夹路径如下：**

- `C:\Program Files\Cloudbase Solutions`
- `C:\Program Files\Cloudbase Solutions\Cloudbase-Init\Python\Scripts`
- `C:\Program Files\QCloud`
- `C:\Windows\System32\cmd.exe`
- `C:\Windows\System32\WindowsPowerShell`
- `C:\Windows\SysWOW64\cmd.exe`

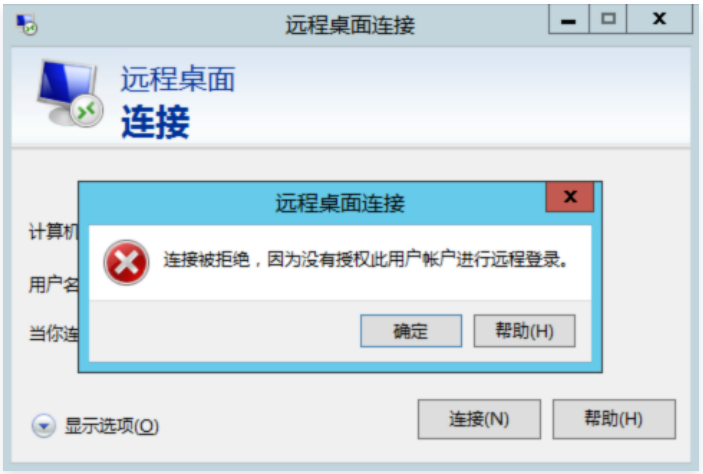
版权所有：腾讯云计算（北京）有限责任公司

# Windows 实例：没有远程桌面服务登录的权限

最近更新时间：2024-11-12 15:31:02

## 现象描述

- **现象1**：Windows 使用远程桌面连接 Windows 实例时，提示**连接被拒绝，因为没有授权此用户账户进行远程登录**。如下图所示：




- **现象2**：Windows 使用远程桌面连接 Windows 实例时，提示**要远程登录，您需要具有通过远程桌面服务进行登录的权限。默认情况下，远程桌面用户组的成员有这项权限。如果您所属的组没有这项权限，或者远程桌面用户组中已经删除了这项权限，那么需要手动为您授予这一权限**。如下图所示：

## 可能原因

| 可能原因 | 处理措施 |
| --- | --- |
| 未配置允许远程登录的权限 | 检查并配置允许远程登录的权限 |
| 未修改拒绝远程登录的权限 | 检查并修改拒绝远程登录的权限 |

## 故障处理

### 通过 VNC 方式登录云服务器

VNC 登录是腾讯云为用户提供的一种通过 Web 浏览器远程连接云服务器的方式。在没有安装或者无法使用远程登录客户端，以及通过其他方式均无法登录的情况下，用户可以通过 VNC 登录连接到云服务器，观察云服务器状态，并且可通过云服务器账户进行基本的云服务器管理操作，具体操作请参见：使用 VNC 登录 Windows 实例 。

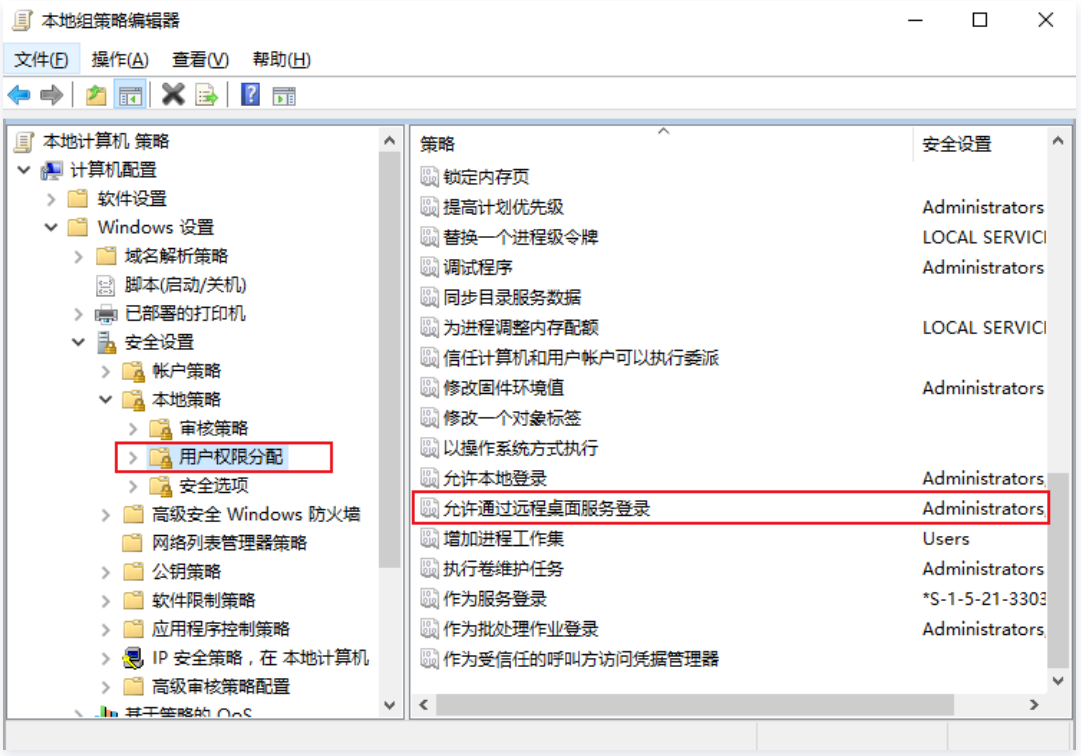
### 检查并配置允许远程登录的权限

如果您远程桌面连接 Windows 实例时，遇到 现象1 的情况，则需要将用户账号添加至 Windows 实例设置的允许通过远程桌面服务登录的列表中。具体的操作请参见 检查并配置允许远程登录的权限 。

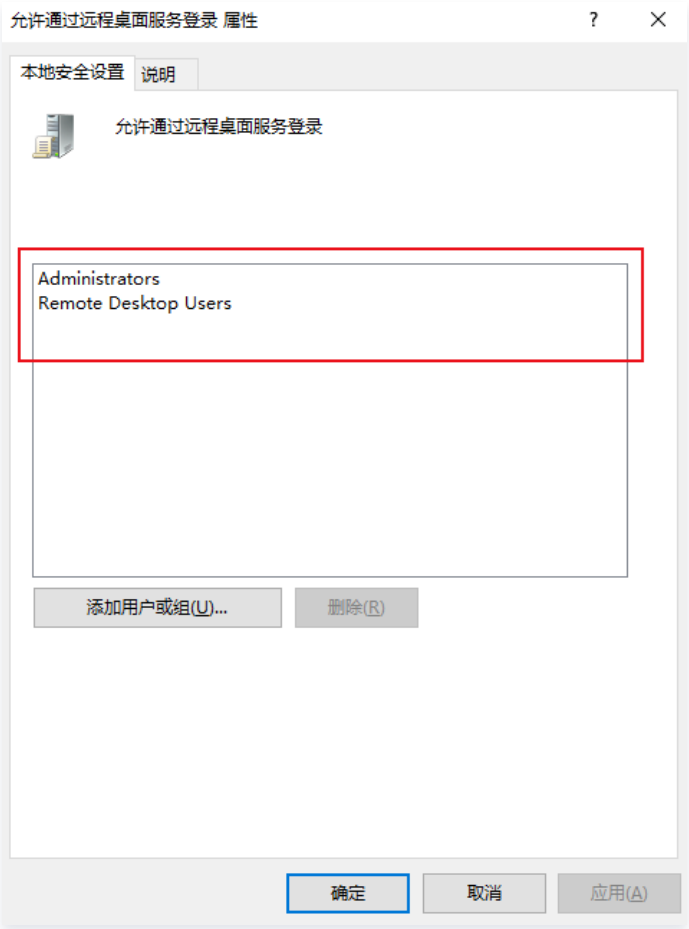
> **说明：**

> 以下操作以 Windows Server 2016 为例。

1. 在操作系统界面，单击 ，输入 **gpedit.msc**，按 **Enter**，打开**本地组策略编辑器**。
2. 在左侧导航树中，选择**计算机配置** > **Windows 设置** > **安全设置** > **本地策略** > **用户权限分配**，双击打开**允许通过远程桌面服务登录**。如下图所示：



3. 在打开的**允许通过远程桌面服务登录**属性窗口中，检查允许通过远程桌面服务登录的用户列表是否存在需要登录的账号。如下图所示：




- 如果该用户不在允许通过远程桌面服务登录的列表中，请执行 步骤4 。
- 如果该用户已经在允许通过远程桌面服务登录的列表中，请通过 在线支持 反馈。

4. 单击**添加用户或组**，打开**选择用户或组**窗口。
5. 输入需要进行远程登录的账号，单击**确定**。
6. 单击**确定**，并关闭本地组策略编辑器。
7. 重启实例，重新尝试使用该账号远程桌面连接 Windows 实例。

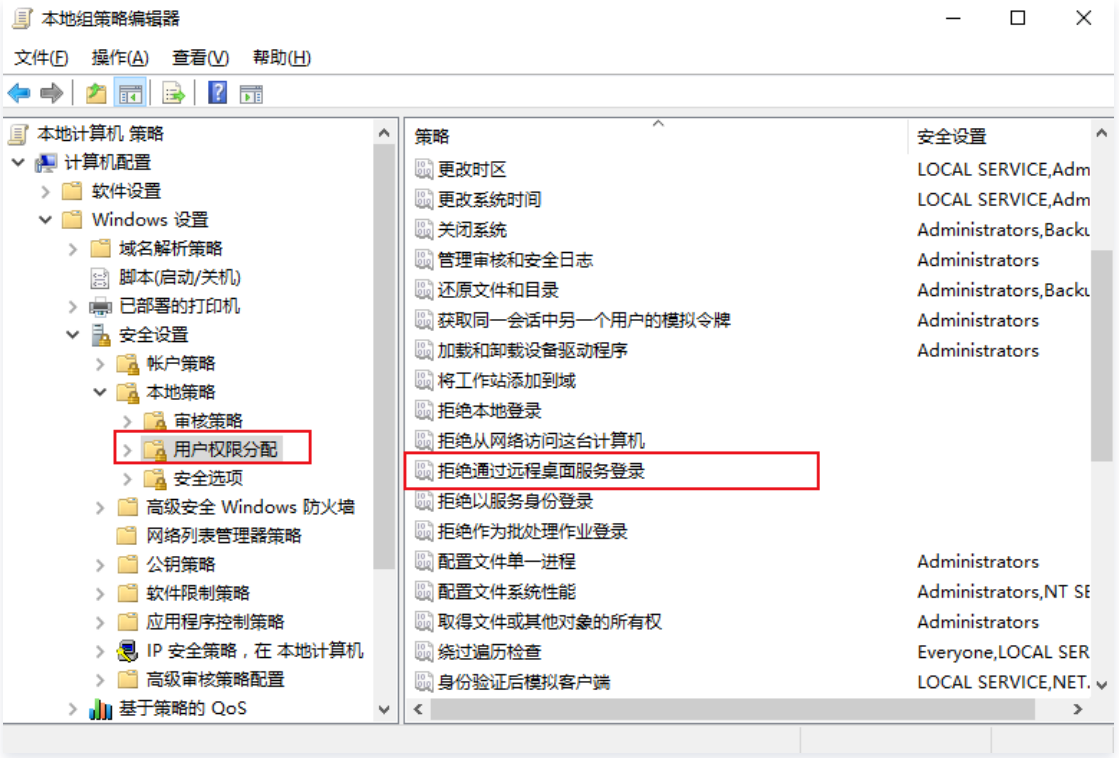
## 检查并修改拒绝远程登录的权限

如果您远程桌面连接 Windows 实例时，遇到 现象2 的情况，则需要将用户账号从 Windows 实例设置的不允许通过远程桌面服务登录的列表中删除。具体的操作请参见 检查并修改拒绝远程登录的权限 。

> **说明：**
> 以下操作以 Windows Server 2016 为例。

1. 在操作系统界面，单击 ，输入 **gpedit.msc**，按 **Enter**，打开**本地组策略编辑器**。

2. 在左侧导航树中，选择**计算机配置** > **Windows 设置** > **安全设置** > **本地策略** > **用户权限分配**，双击打开**拒绝通过远程桌面服务登录**。如下图所示：



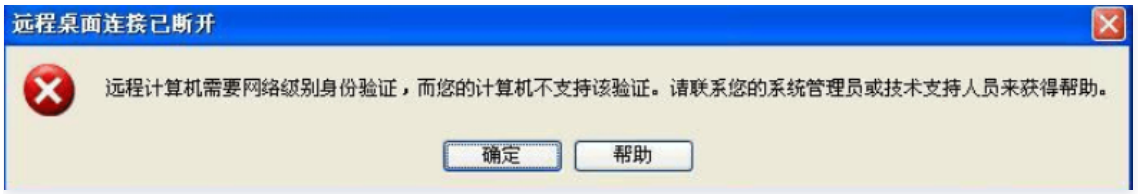

3. 在打开的**拒绝通过远程桌面服务登录**属性窗口中，检查拒绝通过远程桌面服务登录的用户列表是否存在需要登录的账号。
   - 如果该用户在拒绝通过远程桌面服务登录的列表中，请将需要登录的账号从列表中删除，并重启实例。
   - 如果该用户不在拒绝通过远程桌面服务登录的列表中，请通过 在线支持 反馈。

# Windows 实例：需要网络级别身份验证

最近更新时间：2024-09-22 14:24:12

## 现象描述

使用 Windows 系统自带远程桌面连接云服务器时，出现**需要网络级别身份验证**信息，如下图所示。




## 可能原因

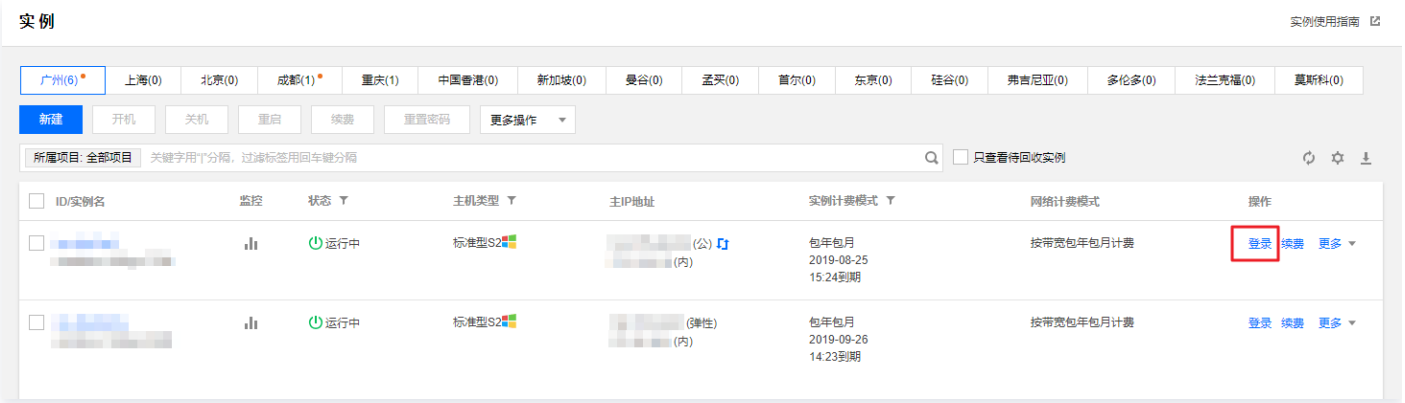
注册表设置存在问题。

## 故障处理

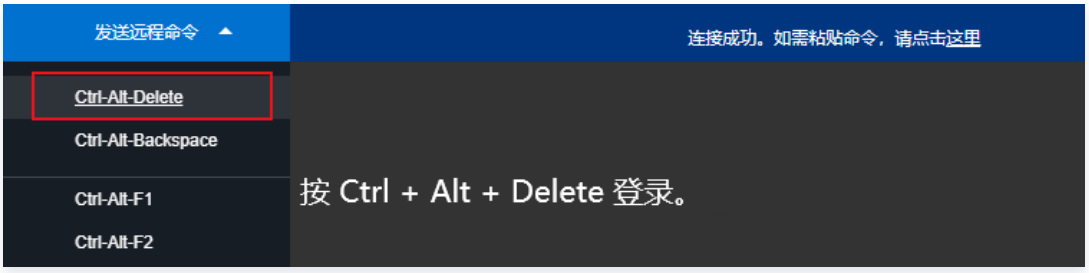
> **说明**
> 以下操作以 Windows Server 2016 为例。

### 步骤一：通过 VNC 方式登录云服务器

1. 登录 云服务器控制台 。
2. 在实例的管理页面，找到目标云服务器实例，单击**登录**。如下图所示：




3. 在弹出的**登录Windows实例**窗口中，选择 **VNC 登录**。
4. 在弹出的登录窗口中，选择左上角的**发送远程命令**，单击 **Ctrl-Alt-Delete** 进入系统登录界面。如下图所示：

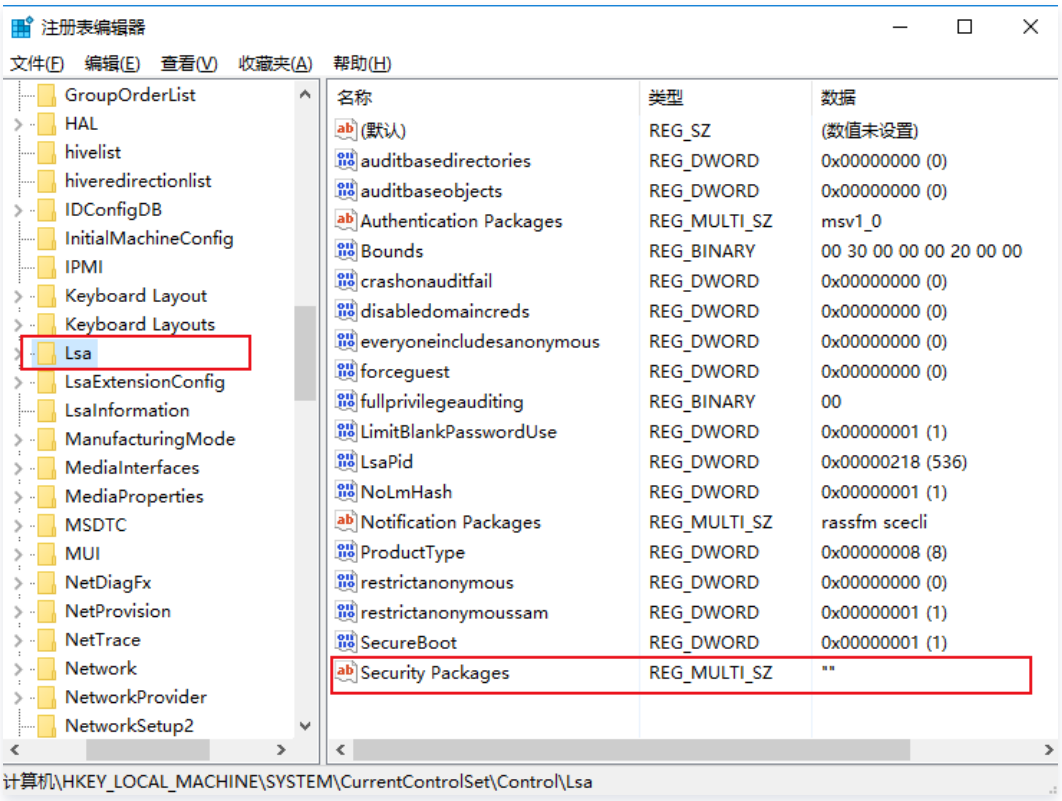



5. 输入登录密码，按 **Enter**，即可登录到 Windows 云服务器。

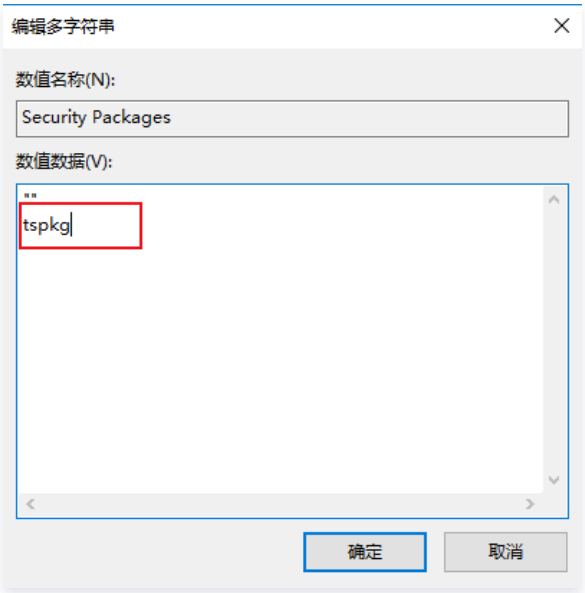
### 步骤二：修改注册表

1. 在操作系统界面，单击 ，输入 **regedit**，按 **Enter**，打开注册表编辑器。

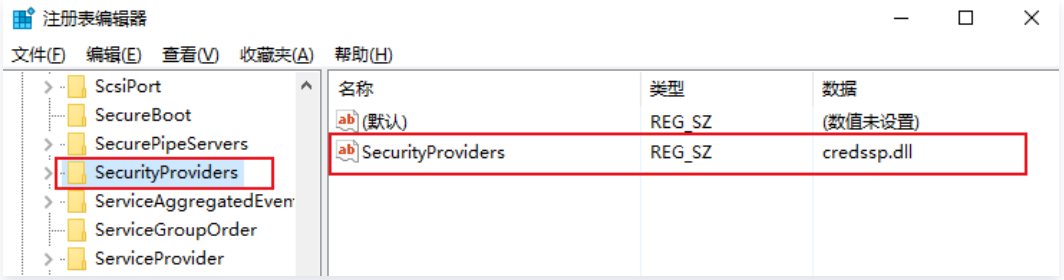
2. 在左侧导航树中，依次选择**计算机** > **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Control** > **Lsa**，并在右侧窗口中找到 **Security Packages**。如下图所示：



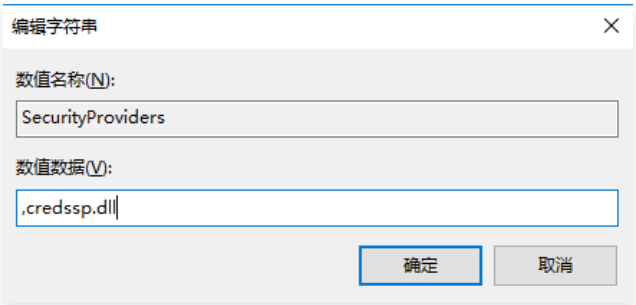

3. 双击 **Security Packages**，打开**编辑多字符串**对话框。
4. 在**编辑多字符串**对话框中，增加 **tspkg** 字符，单击**确定**。如下图所示：




5. 在左侧导航树中，依次展开**计算机** > **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Control** > **SecurityProviders** 目录，并在右侧窗口中找到 **SecurityProviders**。如下图所示：




6. 双击 **SecurityProviders**，打开**编辑多字符串**对话框。
7. 在**编辑多字符串**对话框的**数值数据**末端添加 `,credssp.dll` ，单击**确定**。如下图所示：



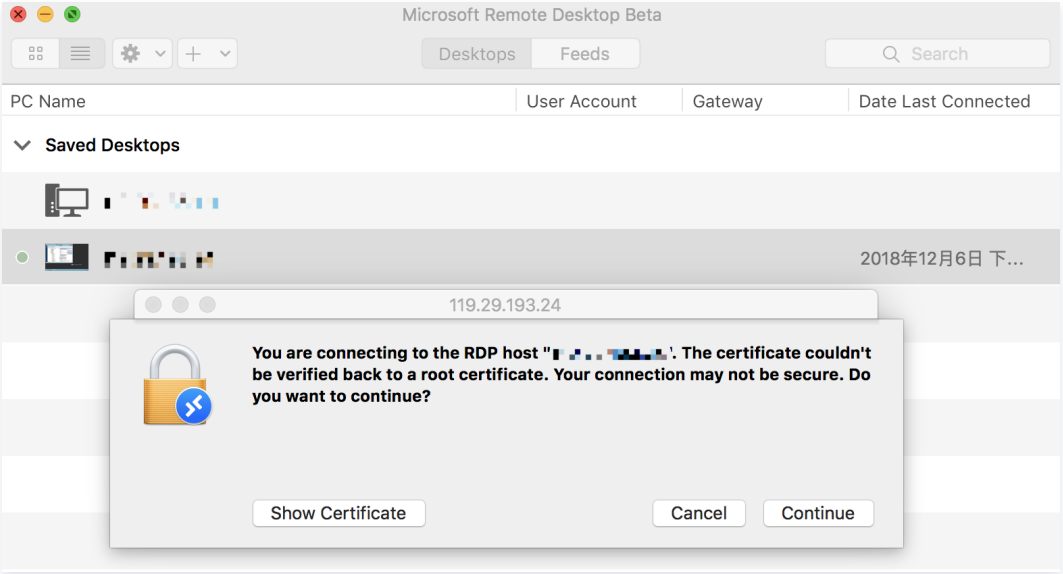

8. 关闭注册表编辑器，重启实例，即可进行远程登录。

# Windows 实例：Mac 远程登录异常

最近更新时间：2024-08-12 16:39:21

## 现象描述

- Mac 通过 Microsoft Remote Desktop 远程连接 Windows 实例时，提示 **The certificate couldn't be verified back to a root certificate**。




- Mac 通过 Microsoft Remote Desktop 远程连接 Windows 实例时，提示**远程桌面连接无法验证您希望连接的计算机的身份**。

## 可能原因

系统未修改实例本地组策略。

## 故障处理

> **说明：**
> 以下操作以 Windows Server 2016 为例。

### 步骤一：通过 VNC 方式登录云服务器

VNC 登录是腾讯云为用户提供的一种通过 Web 浏览器远程连接云服务器的方式。在没有安装或者无法使用远程登录客户端，以及通过其他方式均无法登录的情况下，用户可以通过 VNC 登录连接到云服务器，观察云服务器状态，并且可通过云服务器账户进行基本的云服务器管理操作。具体操作请参见：使用 VNC 登录 Windows 实例 。

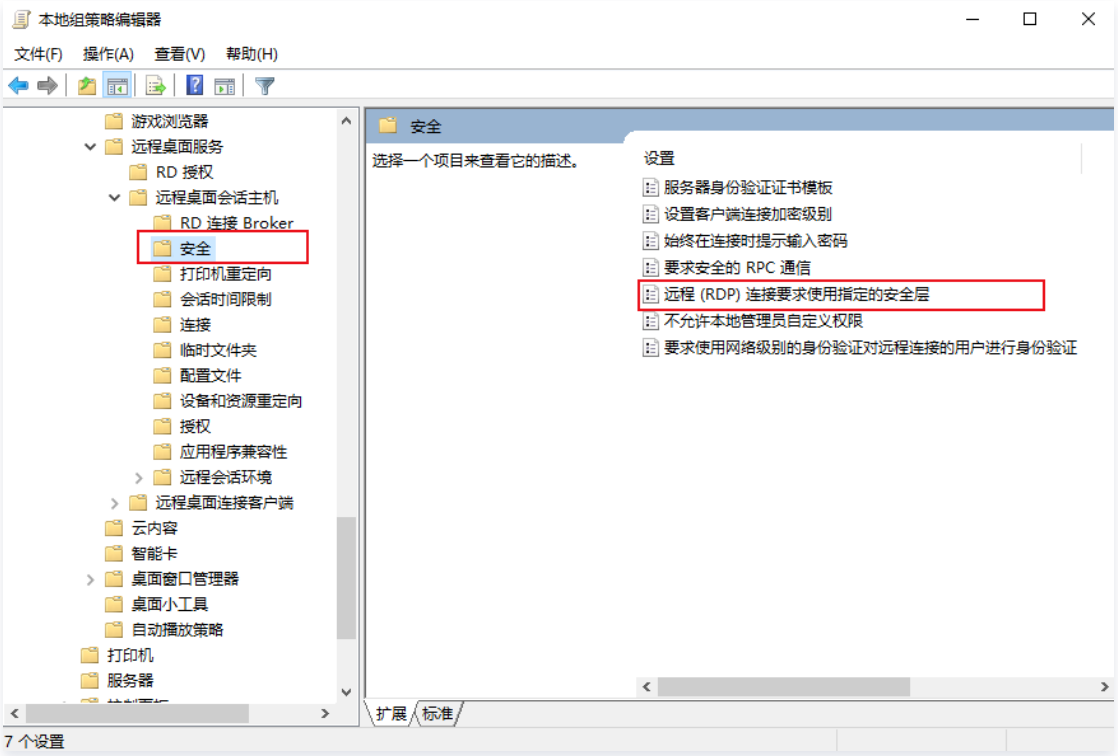
### 步骤二：检查系统是否修改实例本地组策略

1. 在操作系统界面，单击 ，输入 **gpedit.msc**，按 **Enter**，打开**本地组策略编辑器**。

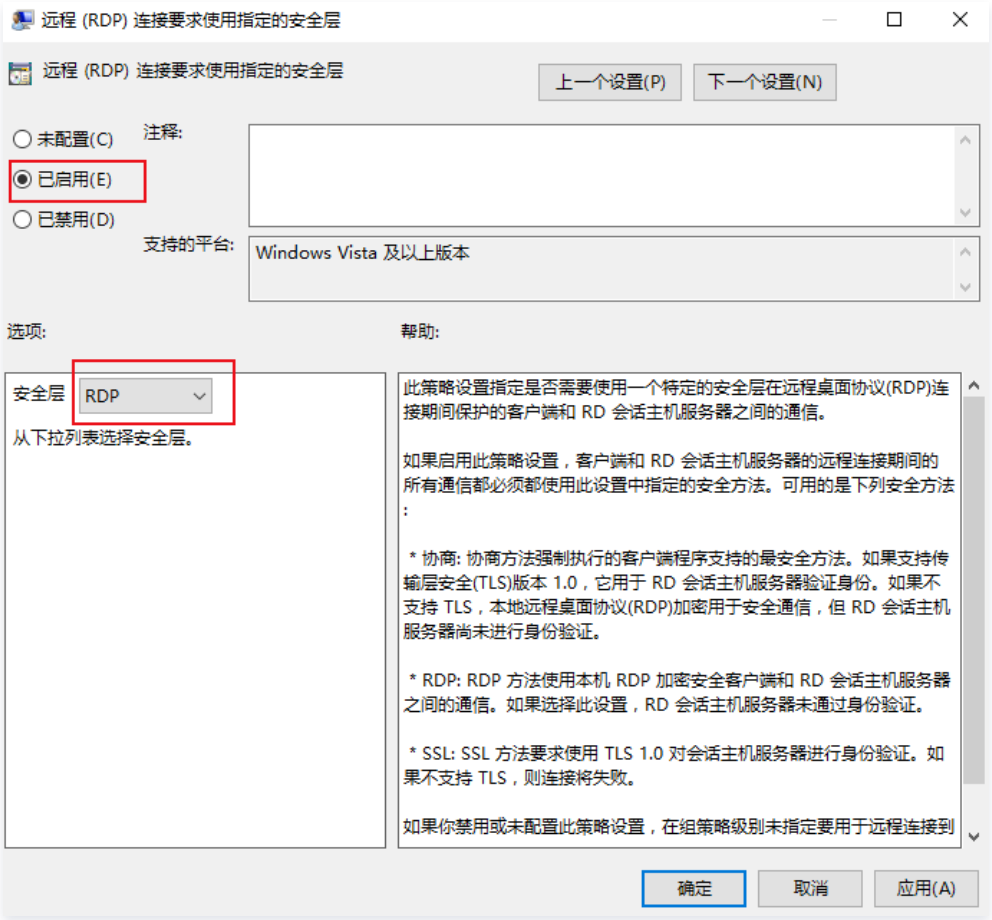
> **说明：**

> 也可使用 Win+R 快捷键打开运行界面。

2. 在左侧导航树中，选择**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**，双击**远程（RDP）连接要求使用指定的安全层**。如下图所示：




3. 在打开的**远程（RDP）连接要求使用指定的安全层**窗口中，选择**已启用**，并将**安全层**设置为 **RDP**。如下图所示：



4. 单击**确定**，完成设置。
5. 重启实例，重新尝试连接是否成功。
   如果还是无法成功，请通过 在线支持 进行反馈。

# Windows 实例：CPU 或内存占用率高导致无法登录

最近更新时间：2024-12-03 15:35:43

## 现象描述

CPU 或内存使用率过高，容易引起服务响应速度变慢、服务器登录不上等问题。

## 定位工具

**任务管理器**：Windows 自带的应用程序和进程管理工具，展示有关电脑性能和运行软件的信息，包括运行进程的名称、CPU 负载、内存使用、I/O 情况、已登录的用户和 Windows 服务的信息。

- **进程**：系统上所有正在运行的进程的列表。
- **性能**：有关系统性能的总体统计信息，例如总体 CPU 使用量和正在使用的内存量。
- **用户**：当前系统上有会话的所有用户。
- **详细信息**：进程选项卡的增强版，显示进程的 PID、状态、CPU、内存的使用情况等进程的详细信息。
- **服务**：系统中所有的服务（包括并未运行的服务）。

## 可能原因

CPU 或内存使用率过高可能由硬件、系统进程、业务进程或者木马病毒等因素所致。您可以使用 腾讯云可观测平台，创建 CPU 或内存使用率阈值告警，当 CPU 或内存使用率超过阈值时，将及时通知到您。

## 故障处理

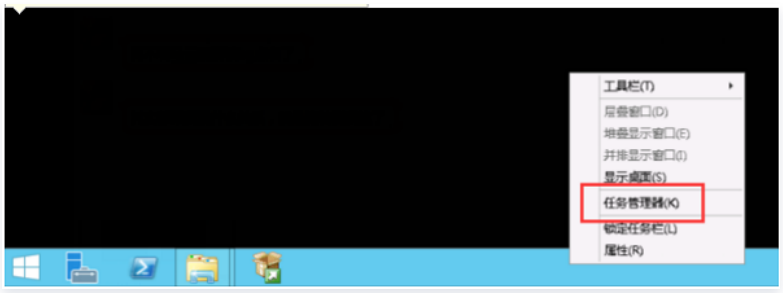
> **说明：**
> 以下操作步骤以 Windows server 2012 R2 为例，操作系统版本不同，详细操作步骤略有区别。

### 步骤一：使用 VNC 方式登录云服务器

由于云服务器负载高时会导致无法建立远程连接，推荐 使用 VNC 方式登录 Windows 实例 。

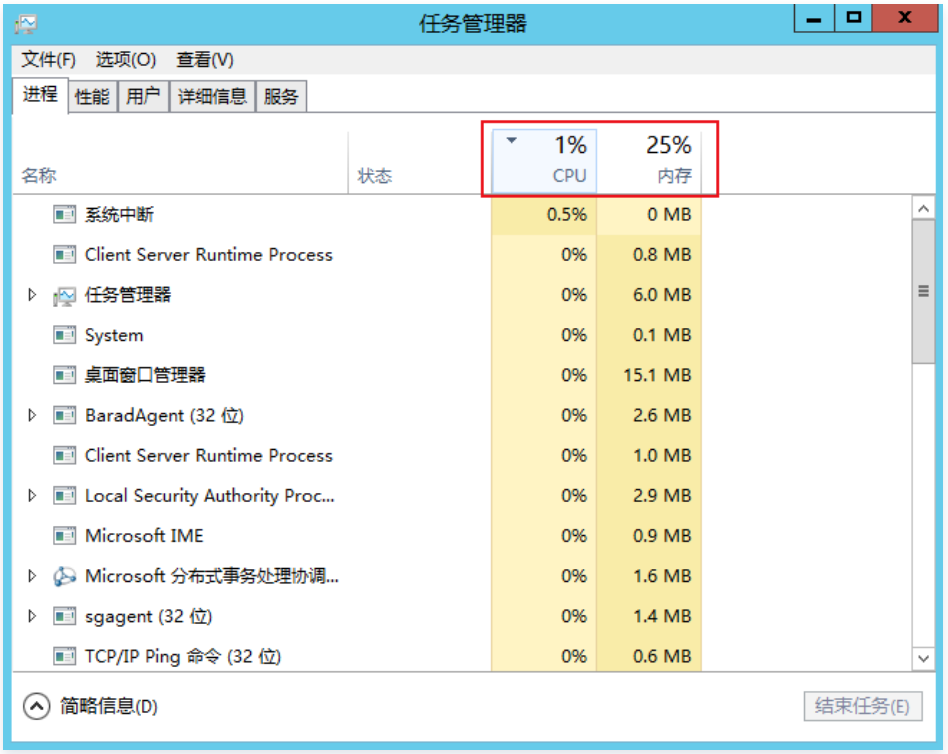
### 步骤二：检查进程占用情况

1. 在云服务器中，右键单击**任务栏**，选择**任务管理器**。如下图所示：




2. 在打开的**任务管理器**中，即可查看资源占用情况。如下图所示：

> **说明：**
> 您可单击 CPU 或内存，以升序/降序对进程进行排序。




### 步骤三：检查分析占用资源的进程情况

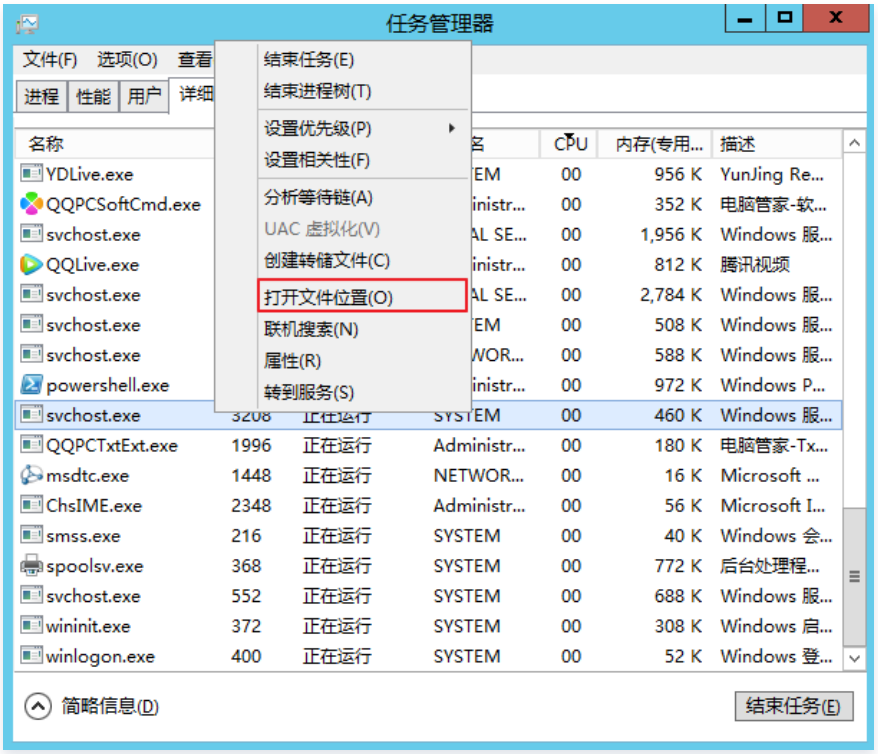
根据任务管理器中的进程，分析与排查问题，以采取对应解决方案。

#### 占用大量 CPU 或内存资源的进程为系统进程

如果您发现系统进程占用了大量 CPU 或内存资源，请排查以下内容：

1. 检查进程名称。
   部分病毒会使用与系统进程相似的名称，例如 svch0st.exe、explore.exe、iexplorer.exe 等。
2. 检查进程对应的可执行文件的所在位置。
   系统进程一般位于 `C:\Windows\System32` 目录下，并且会有完善的签名和介绍。您可以在任务管理器中，右键单击待查看的进程，选择**打开文件位置**，

即可查看具体可执行文件的位置。例如 `svchost.exe` 。如下图所示：




- 如果进程位置不在 `C:\Windows\System32` 目录下，则表示该云服务器可能中了病毒，请手动或者使用安全工具进行查杀。
- 如果进程位置在 `C:\Windows\System32` 目录下，请重启系统或关闭不需要且安全的系统进程。

常见的系统进程如下：

- System Idle Process：系统空间进程，显示 CPU 空闲时间百分比。
- system：内存管理进程。
- explorer：桌面和文件管理。
- iexplore：微软的浏览器。
- csrss：微软客户端/服务端运行时子系统。
- svchost：系统进程，用于执行 DLL。
- Taskmgr：任务管理器。
- lsass：本地安全权限服务。

### 占用大量 CPU 或内存资源的进程为异常进程

如果您发现一些命名很奇怪的进程占用了大量 CPU 或内存资源，则可能为木马病毒进程，例如 xmr64.exe（挖矿病毒）等。建议您使用搜索引擎进行搜索，确认是否为木马病毒进程。

- 如果是木马病毒进程，请使用安全工具进行查杀，必要时考虑备份数据，重装系统。
- 如果不是木马病毒进程，请重启系统或关闭不需要且安全的进程。

### 占用大量 CPU 或内存资源的进程为业务进程

如果您发现业务进程占用了大量 CPU 或内存资源，例如 IIS、HTTPD、PHP、Java 等，建议进一步分析。
例如，判断当前业务量是否较大。

- 若业务量较大，建议您 升级服务器配置；若不升级服务器配置，可以考虑业务程序是否存在优化空间，请进行优化。
- 若业务量不大，则需要进一步结合业务报错日志来分析。例如，参数配置不当导致空耗资源。

### 占用大量 CPU 或内存资源的进程为腾讯云组件进程

请通过 在线支持 联系我们进一步定位处理。

# Windows 实例：无法连接到腾讯云服务器

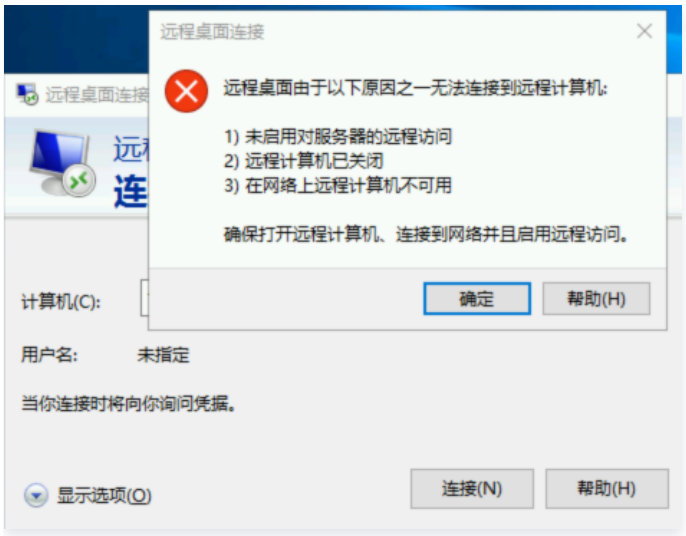
最近更新时间：2024-07-09 10:52:11

## 现象描述

使用 Windows 系统的远程连接功能连接 Windows 实例时，远程桌面由于以下原因之一无法连接到远程计算机：

- 未启用对服务器的远程访问
- 远程计算机已关闭
- 在网络上远程计算机不可用

无法连接图示如下：




您需要确保打开远程计算机、连接到网络并且启用远程访问。

## 可能原因

导致出现以上提示的具体原因包括（不限于以下情况，请根据实际情况进行分析）：

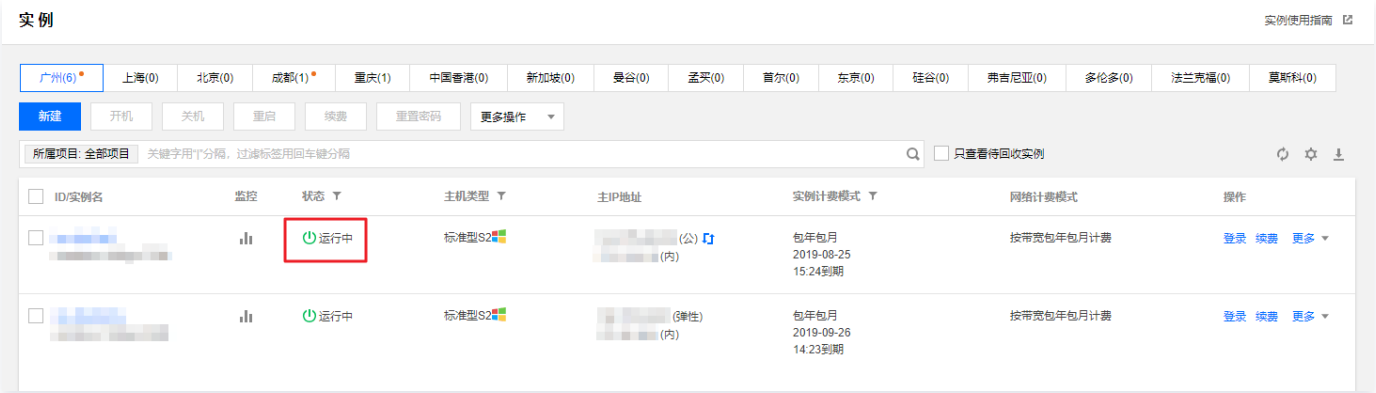
| 可能原因 | 处理措施 | 排查位置 |
| --- | --- | --- |
| 实例处于关机等非正常运行状态 | 检查实例状态并确保实例处于正常运行状态 | 控制台 |
| 服务器未设置公网 IP | 检查并确保服务器已设置公网 IP | |
| 未购买公网带宽 | 检查是否已购买公网带宽 | |
| 实例的安全组未放通远程登录端口（默认3389） | 检查实例的安全组确保已放通远程登录端口（默认3389） | |
| 服务器内远程桌面服务未启动 | 检查服务器内远程桌面服务确保已启动 | 服务器内部 |
| 服务器内 Windows 实例的防火墙设置有误 | 检查服务器内 Windows 实例的防火墙确保设置正确 | |

## 故障处理

### 检查实例状态并确保实例处于正常运行状态

1. 登录 云服务器控制台 检查实例运行状态。

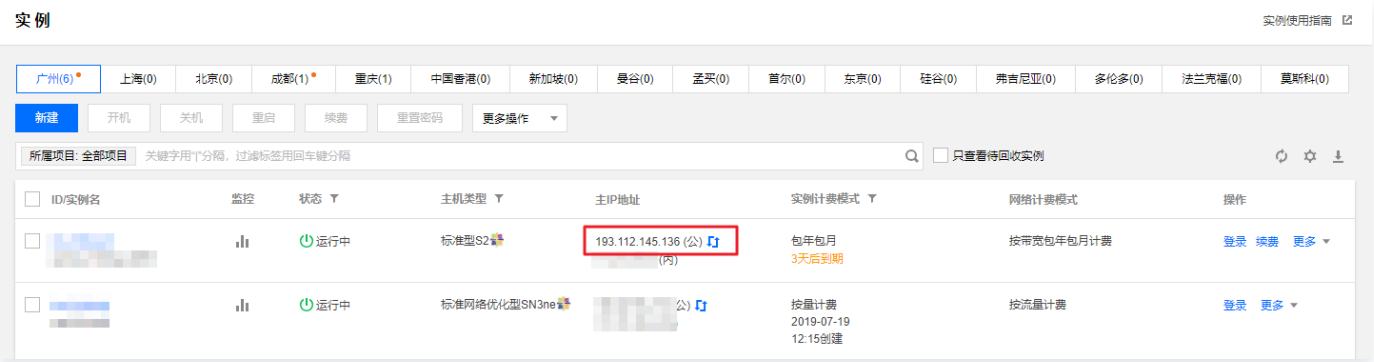
2. 在实例的管理页面，查看实例是否处于**运行中**。如下图所示：




- 实例处于正常运行状态，请 检查并确保服务器已设置公网 IP 。
- 实例处于非正常运行状态，请启动该 Windows 实例。

## 检查并确保服务器已设置公网 IP

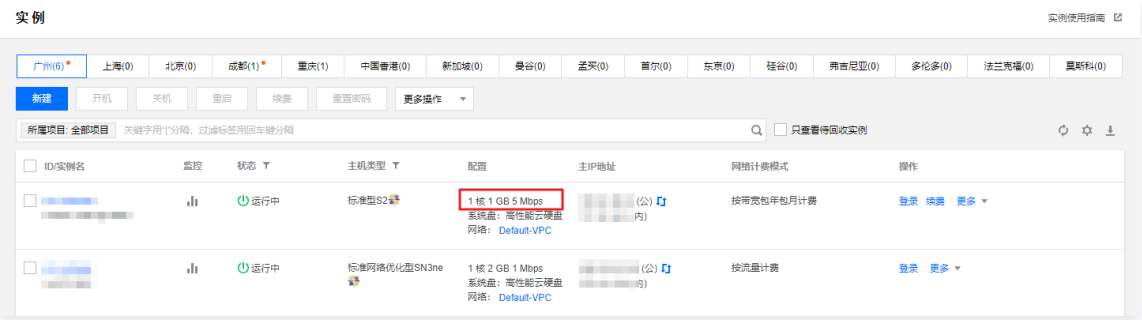
通过在 云服务器控制台 检查服务器是否设置公网 IP。如下图所示：




- 服务器已设置公网 IP，请 检查是否购买公网带宽 。
- 服务器未设置公网 IP，请 申请弹性公网 IP 并进行绑定 。

## 检查是否购买公网带宽

1. 通过登录 云服务器控制台 确认公网宽带值。
2. 检查公网带宽是否为0Mbps。
   - 已购买公网带宽，请参见 调整网络 ，建议将带宽调整到5Mbps或以上。

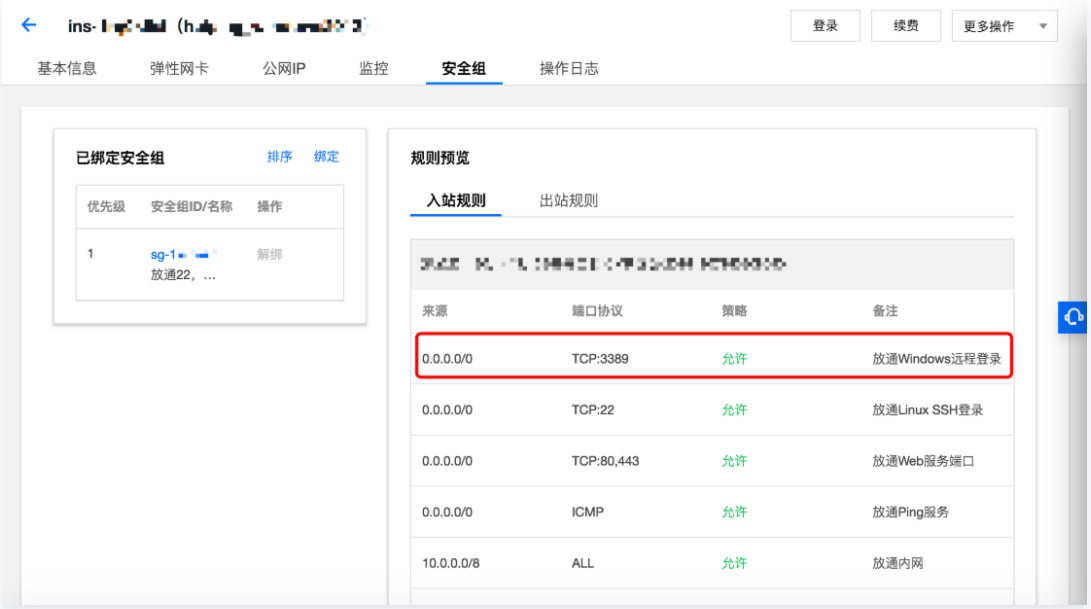



   - 未购买公网带宽，请 检查实例的安全组是否放通远程登录端口（默认3389） 。

## 检查实例的安全组确保已放通远程登录端口（默认3389）

1. 在 云服务器控制台 的实例管理页面，单击需要登录的实例 ID/实例名，进入该实例详情页面。

2. 在**安全组**页签下，检查实例的安全组是否放通远程登录接口（默认远程桌面端口：3389）。如下图所示：




- 实例的安全组已放通远程登录端口，请 检查服务器内远程桌面服务确保已启动 。
- 实例的安全组未放通远程登录端口，请编辑对应的安全组规则，进行放通。操作方法请参见 添加安全组规则 。

## 检查服务器内远程桌面服务确保已启动

通过腾讯云的VNC登录进入服务器内部进行检查。

1. 使用 腾讯云 VNC 登录 检查 Windows 实例远程桌面服务是否开启。

> **说明：**
> 以下操作以 Windows Server 2016 操作系统的实例为例。

2. 右键单击 ⊞，在弹出的菜单中选择**系统**。
3. 在打开的**系统**窗口中，选择**高级系统设置**。

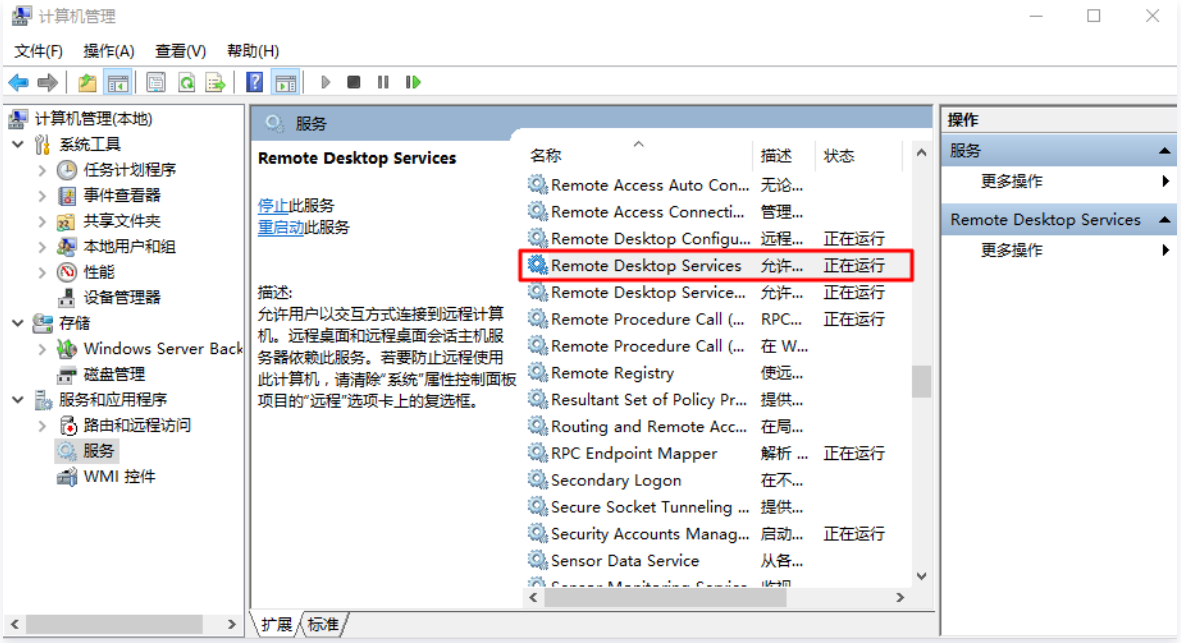
4. 在打开的**系统属性**窗口中，选择**远程**页签，检查是否勾选**允许远程连接到此计算机**。如下图所示：

- 已勾选**允许远程连接到此计算机**，请执行 步骤5 。
- 未勾选**允许远程连接到此计算机**，请勾选并单击**确定**。

5. 右键单击 ⊞，在弹出的菜单中选择**计算机管理**。

6. 在打开的**计算机管理**窗口左侧菜单栏中，选择**服务和应用程序** > **服务**。

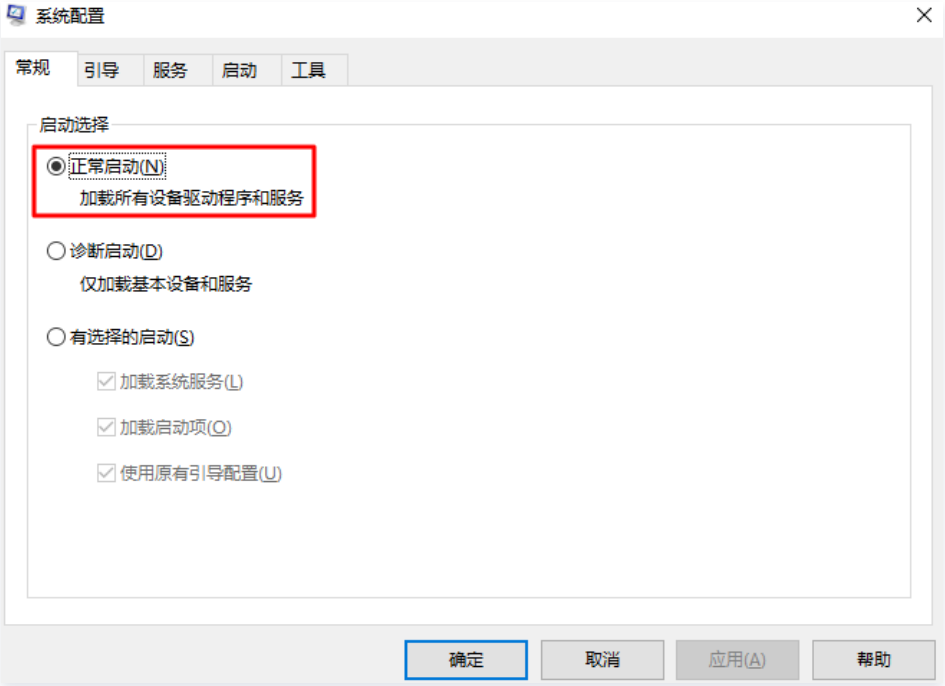
7. 在右侧的服务列表中，检查 Remote Desktop Services 是否启动。如下图所示：




- Remote Desktop Services 是已启动状态，请执行 步骤8 。

- Remote Desktop Services 是未启动状态，请启动服务。

8. 右键单击 ⊞，在弹出的菜单中选择**运行**。
9. 在弹出的**运行**窗口中，输入 **msconfig** 并单击**确定**。
10. 在打开的**系统配置**窗口中，检查是否勾选**正常启动**。如下图所示：




- 已勾选**正常启动**的状态，请 检查服务器内 Windows 实例的防火墙确保设置正确 。
- 未勾选**正常启动**的状态，请勾选并单击**确定**。

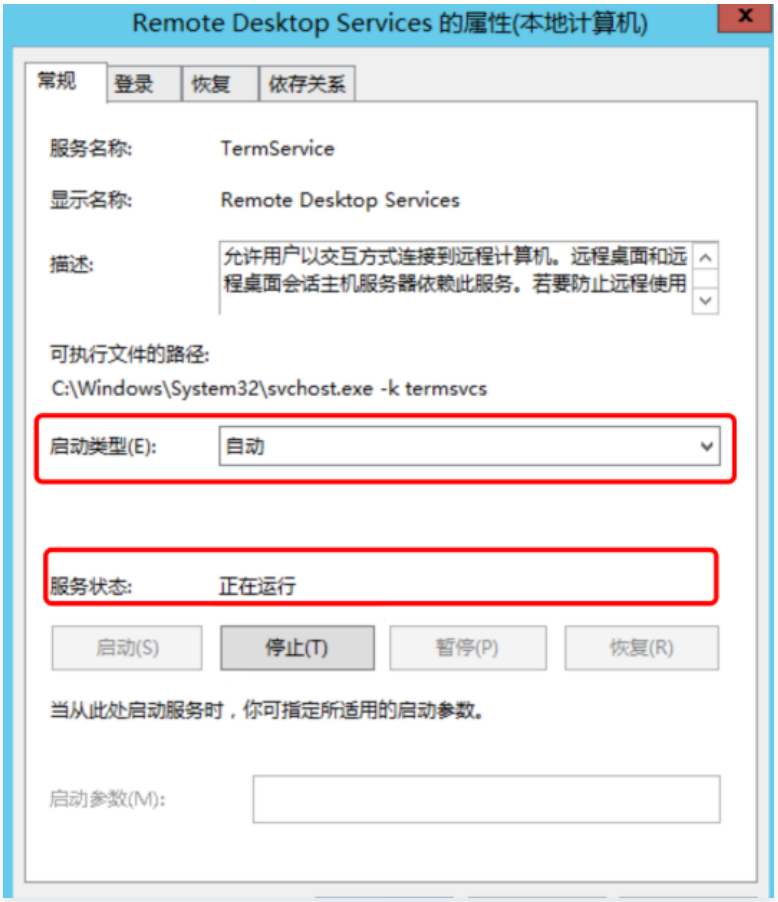
## 检查服务器内 Windows 实例的防火墙确保设置正确

1. 使用 VNC 登录实例，排查 Windows 实例的防火墙设置。

> **说明：**
> 以下操作以 Windows Server 2016 操作系统的实例为例。

2. 右键单击 ⊞，在弹出的菜单中选择**运行**。
3. 在弹出的**运行**中输入 **services.msc**，并按 **Enter**，打开 **服务** 窗口。

4. 双击打开 **Remote Desktop Services** 的属性，检查远程桌面服务是否已启动。如下图所示：

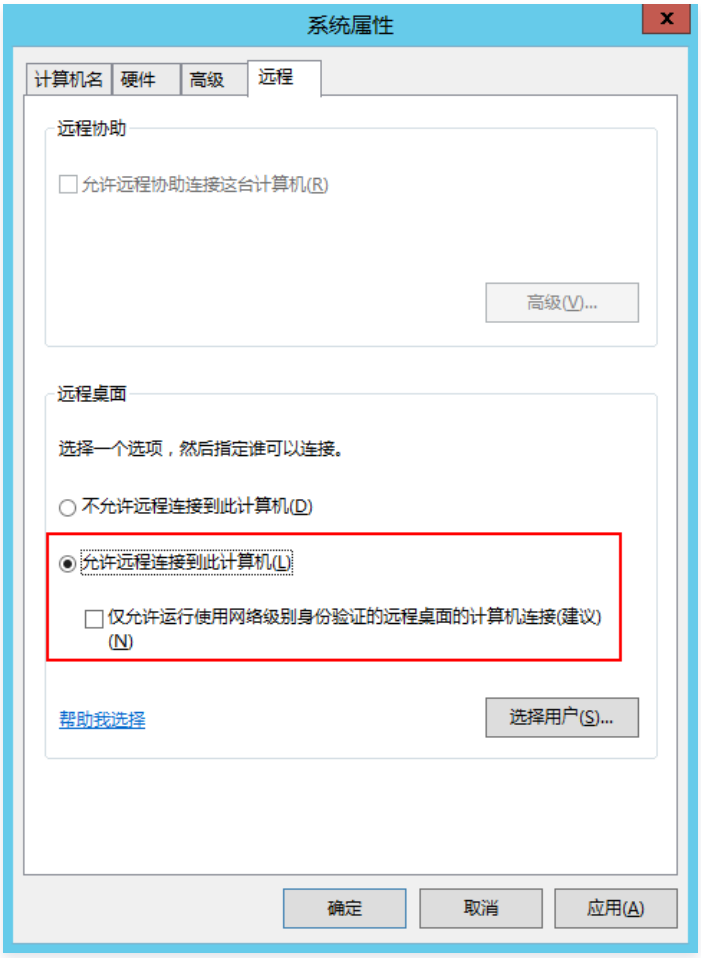



- 远程桌面服务已启动，请执行 步骤5 。
- 远程桌面服务未启动，请将**启动类型**设置为**自动**，**服务状态**设置为**正在运行**（即单击**启动**，启动服务）。

5. 右键单击 ⊞，在弹出的菜单中选择**运行**。

6. 在弹出的**运行**窗口中输入 **sysdm.cpl**，按 **Enter**，打开 **系统属性** 窗口。

7. 在**远程**页签中，检查远程桌面是否设置为**允许远程连接到此计算机(L)**。如下图所示：

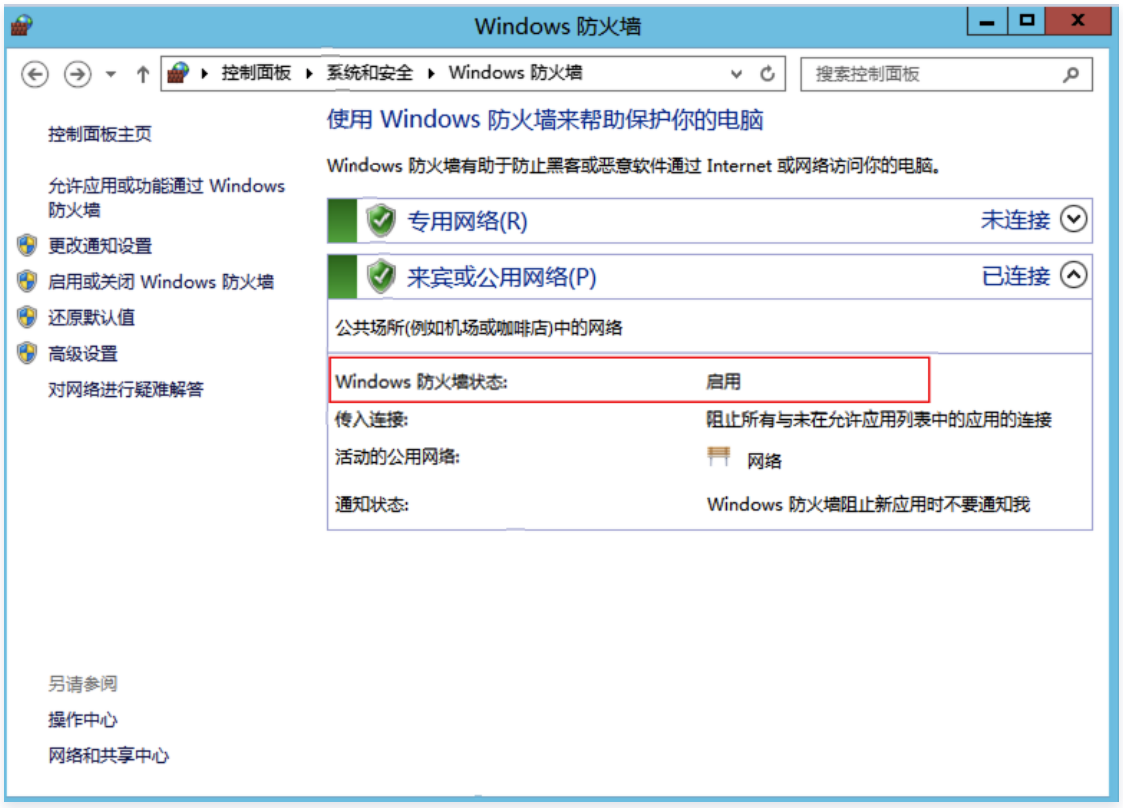



- 远程桌面已设置为**允许远程连接到此计算机(L)**，请执行 步骤8 。
- 远程桌面未设置为**允许远程连接到此计算机(L)**，请将远程桌面设置为**允许远程连接到此计算机(L)**。

8. 单击 ，选择**控制面板**，打开控制面板。

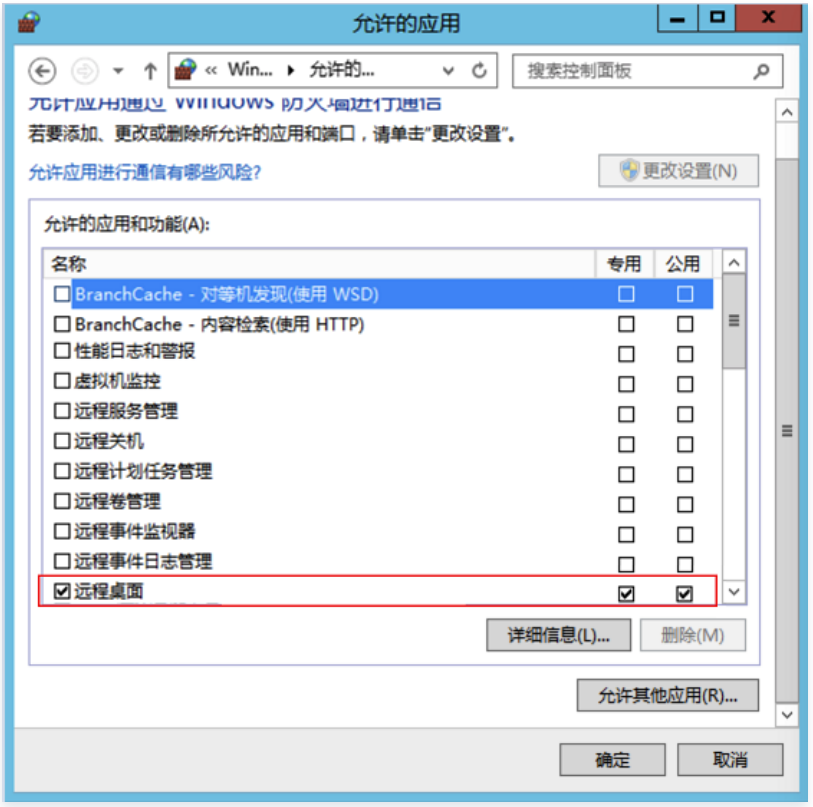
9. 在**控制面板**中，选择**系统与安全** > **Windows 防火墙**，打开**Windows 防火墙**。

10. 在 **Windows 防火墙**中，检查 Windows 防火墙状态。如下图所示：




- 为**启用**状态，请执行 步骤11 。
- 为**关闭**状态，请通过 在线支持 反馈。

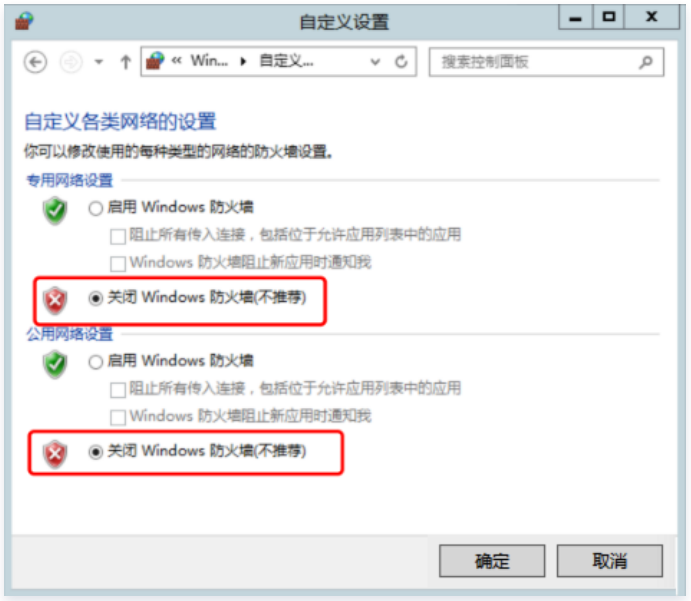
11. 在 **Windows 防火墙**中，单击**允许应用或功能通过 Windows 防火墙**，打开**允许的应用**窗口。
12. 在**允许的应用**窗口中，检查**允许的应用和功能(A)是否勾选远程桌面**。如下图所示：




- 已勾选**远程桌面**，请执行 步骤13 。

- 未勾选**远程桌面**，请勾选**远程桌面**，放通**远程桌面**。

13. 在 **Windows 防火墙**中，单击**启用或关闭 Windows 防火墙**，打开**自定义设置**窗口。
14. 在**自定义设置**窗口中，将**专用网络设置**和**公用网络设置**设置为**关闭 Windows 防火墙(不推荐)**。如下图所示：




若执行以上操作后仍无法通过远程桌面连接到 Windows 实例，请通过 在线支持 反馈。

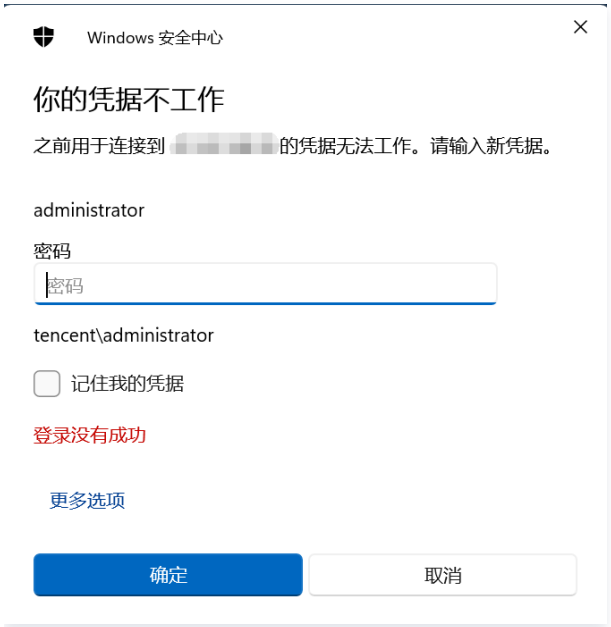
# Windows 实例：凭据不工作

最近更新时间：2025-04-17 11:08:32

## 现象描述

Windows 操作系统的本地计算机通过 RDP 协议（如 MSTSC 方式）远程桌面连接登录 Windows 云服务器时，出现如下报错：
您的凭据无法工作，之前用于连接到 `XXX.XXX.XXX.XXX` 的凭据无法工作。请输入新凭据。

> **说明**
> 如果输入新凭据，仍提示凭据不工作，请同时检查您的用户名是否拼写正确（Windows系统默认用户名为 Administrator）。




## 可能原因

| 可能原因 | 处理措施 |
| --- | --- |
| Windows 实例网络访问策略未修改 | 检查并修改 Windows 实例网络访问策略 |
| Windows 实例凭据未分配 | 检查并修改 Windows 实例凭据分配 |
| 云服务器密码保护共享未关闭 | 检查并关闭云服务器密码保护共享 |

## 故障处理

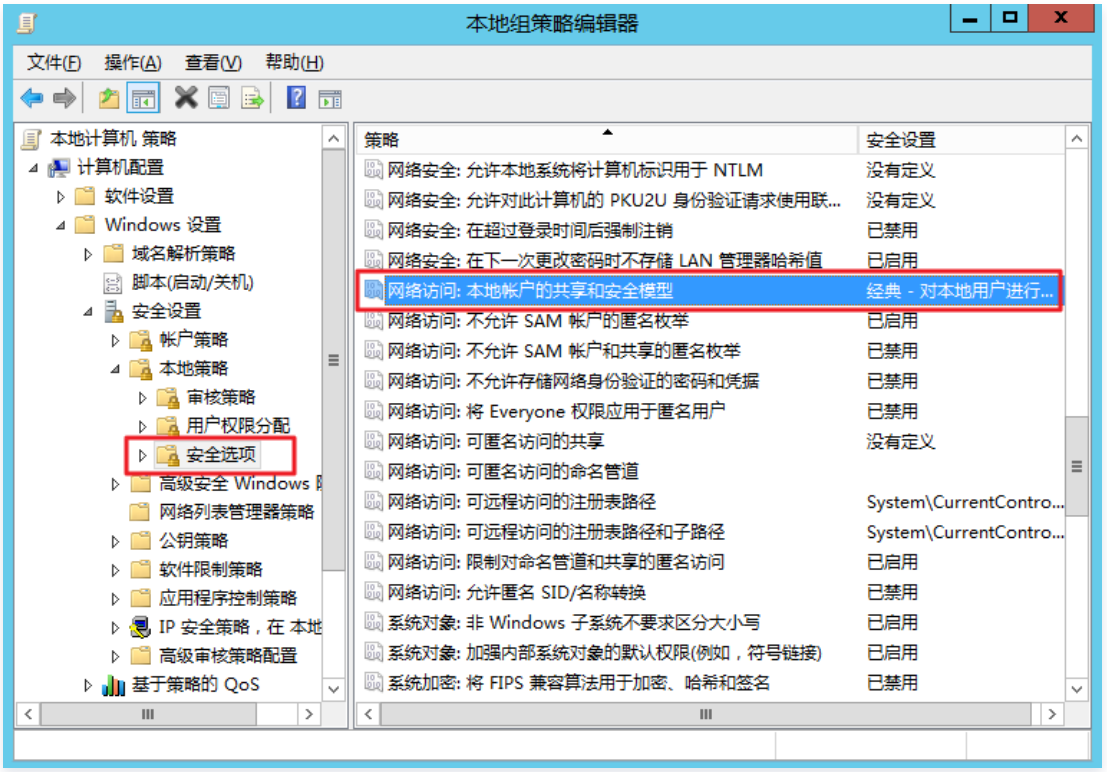
> **说明**
> - 本文以 Windows Server 2022 操作系统的腾讯云云服务器为例，根据操作系统的版本不同，详细操作步骤略有区别。
> - 请按照以下步骤依次排查，并在每一个步骤执行完后重新连接 Windows 云服务器验证问题是否解决，如未生效请继续执行下一步骤。

### 检查并修改 Windows 实例网络访问策略

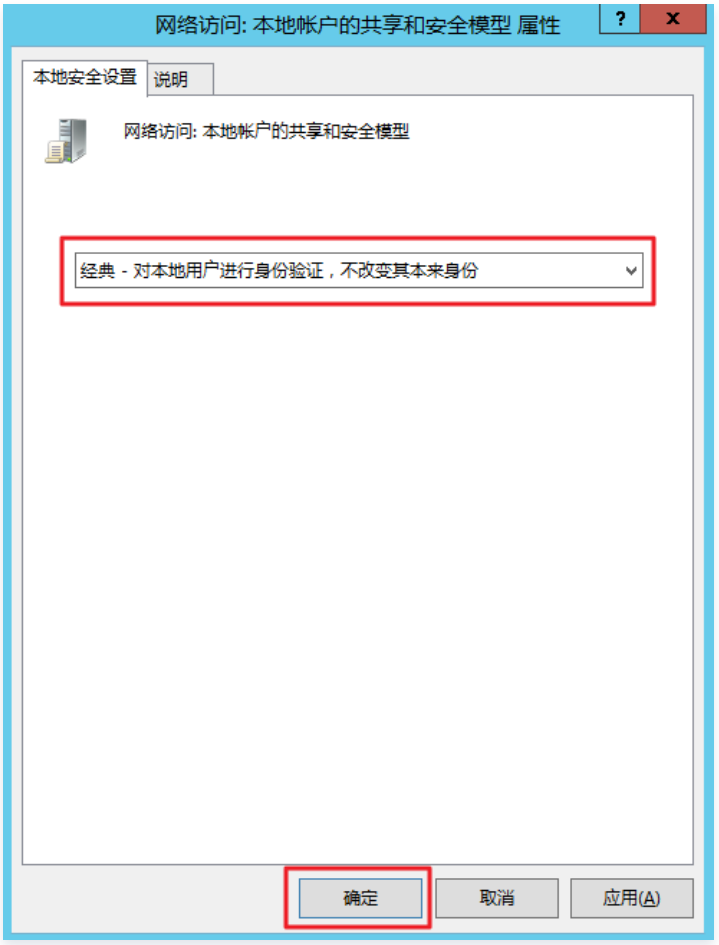
1. 使用 VNC 登录 Windows 实例。
2. 在桌面左下角，搜索框

中输入Windows PowerShell，打开 Windows PowerShell 窗口。
3. 在 Windows PowerShell 窗口中，输入 gpedit.msc，按 Enter，打开本地组策略编辑器。
4. 在左侧导航栏中，依次展开计算机配置 > Windows 设置 > 安全设置 > 本地策略 > 安全选项目录。

5. 找到并打开**安全选项**中的**网络访问：本地账户的共享和安全模型**。如下图所示：




6. 选择**经典 – 对本地用户进行身份验证，不改变其本来身份**，单击**确定**。如下图所示：

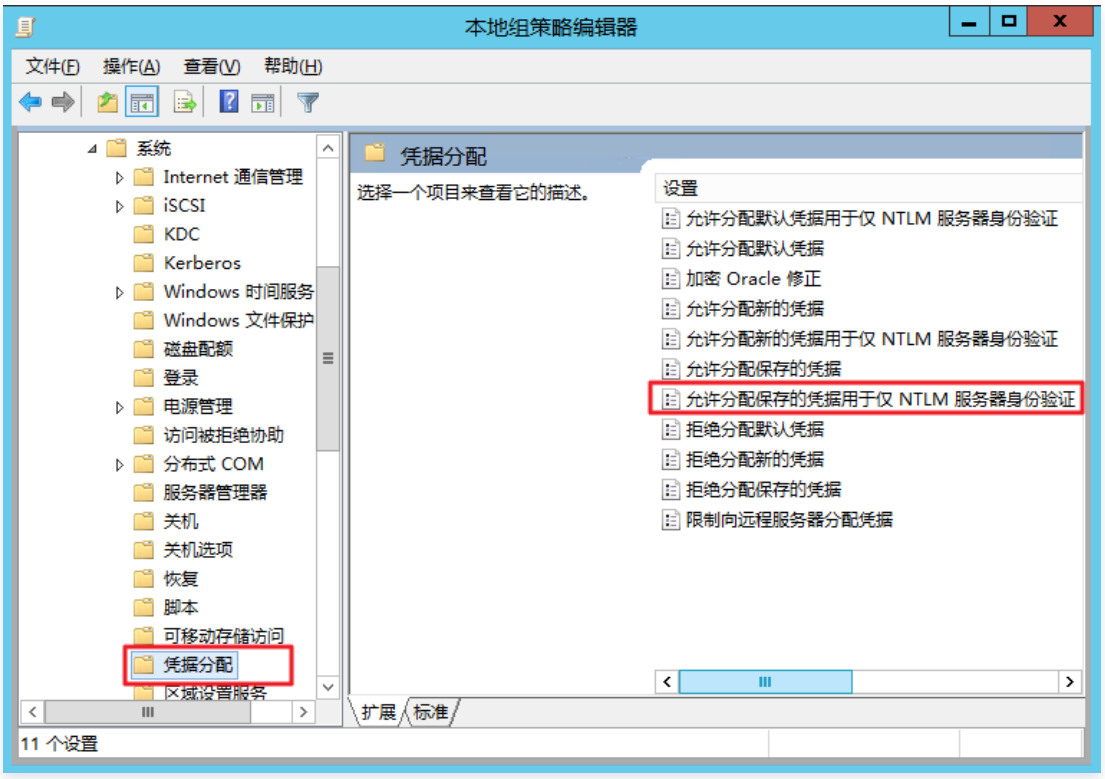



7. 重新连接 Windows 云服务器，验证连接是否成功。
   - 验证连接已成功，任务结束。

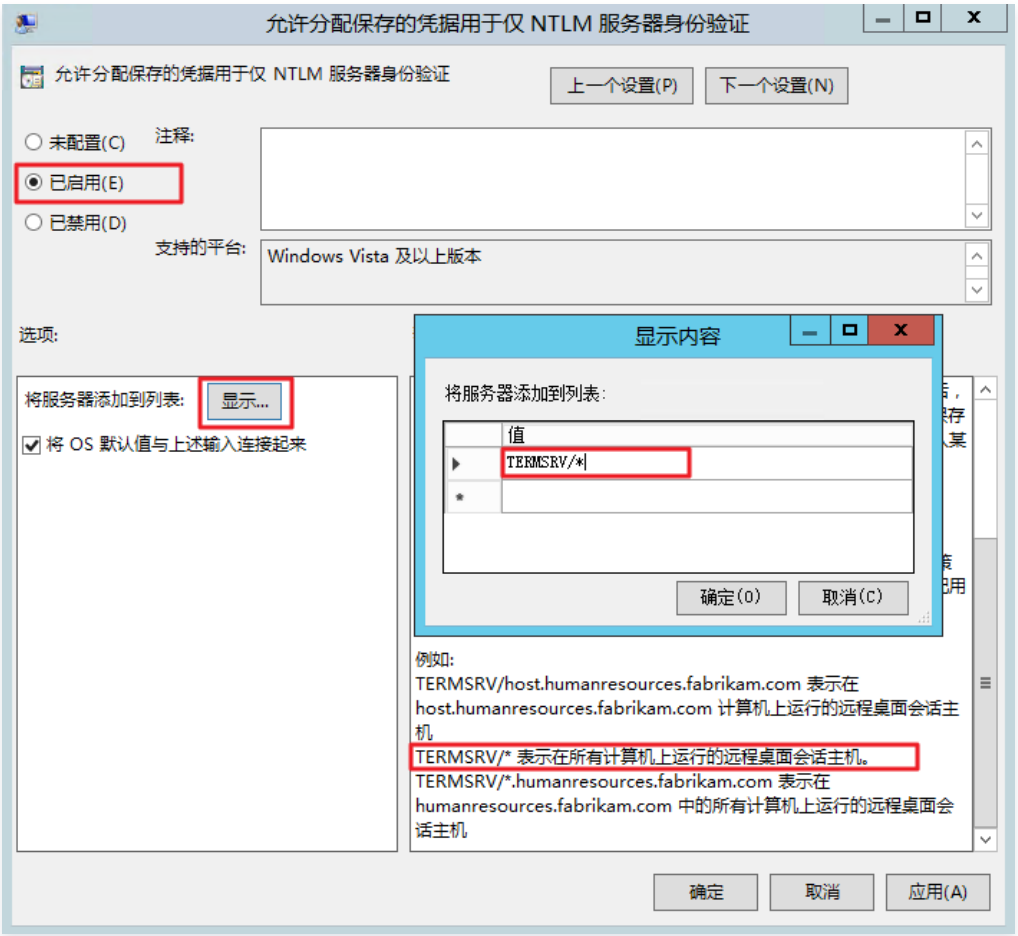
- 验证连接未成功，请 检查并修改 Windows 实例凭据分配 。

## 检查并修改 Windows 实例凭据分配

1. 在**本地组策略编辑器**的左侧导航栏中，依次展开**计算机配置** > **管理模板** > **系统** > **凭据分配**目录。
2. 找到并打开**凭据分配**中的**允许分配保存的凭据用于仅 NTLM 服务器身份验证**。如下图所示：



3. 在打开的窗口中，选择**已启用**，并在**选项**的**显示**中输入 `TERMSRV/*` ，单击**确定**。如下图所示：




4. 单击**确定**。

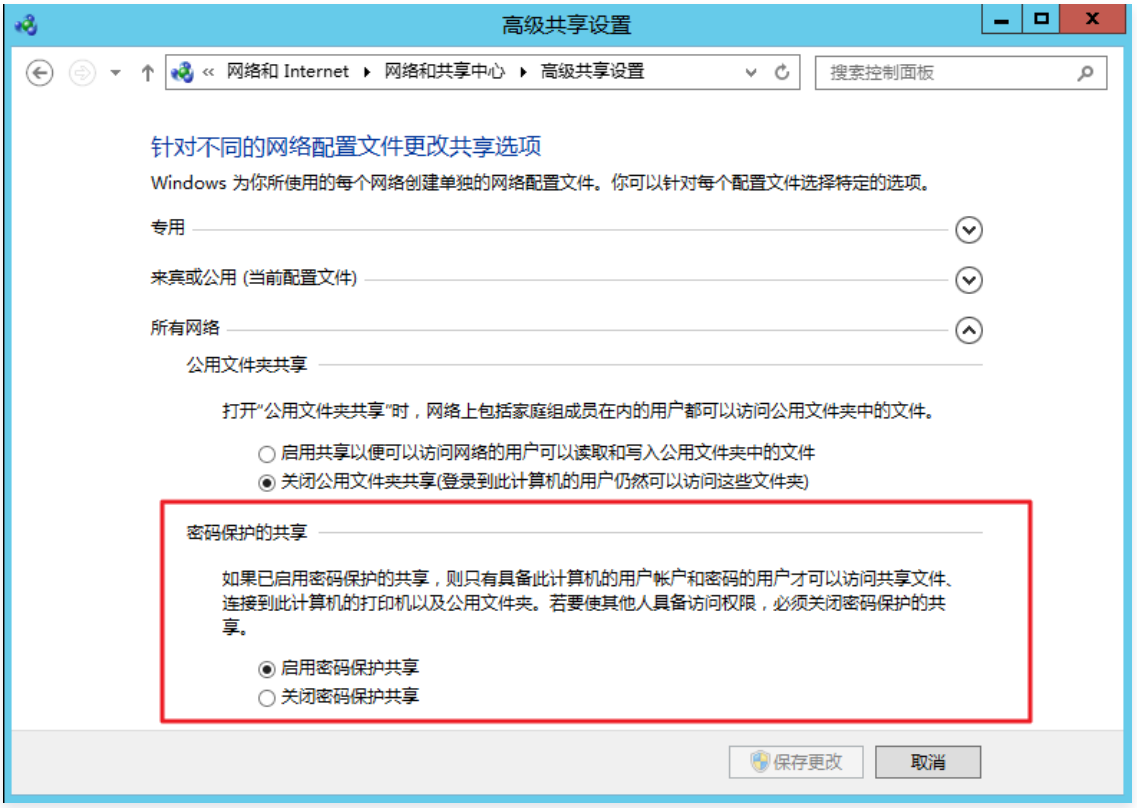
5. 在桌面左下角，搜索框 中输入**Windows PowerShell**，打开 **Windows PowerShell** 窗口。

6. 在 **Windows PowerShell** 窗口中，输入 **gpupdate /force**，按 **Enter**，更新组策略。如下图所示：

7. 重新连接 Windows 云服务器，验证连接是否成功。
   - 验证连接已成功，任务结束。
   - 验证连接未成功，请 检查并关闭云服务器密码保护共享 。

## 检查并关闭云服务器密码保护共享

1. 在操作系统界面，单击 > **控制面板** > **网络和 Internet** > **网络和共享中心** > **更改高级共享设置**，进入高级共享设置界面。如下图所示：




2. 展开**所有网络**页签，并在**密码保护的共享**下选择**关闭密码保护共享**，单击**保存更改**。
3. 重新连接 Windows 云服务器，验证连接是否成功。
   - 验证连接已成功，任务结束。
   - 验证连接未成功，请通过 在线支持 反馈。

# Windows 实例：没有远程桌面授权服务器可以提供许可证

最近更新时间：2025-06-16 17:00:21

## 现象描述

使用 Windows 远程桌面连接 Windows 实例时，提示**由于没有远程桌面授权服务器可以提供许可证，远程会话连接已断开。请跟服务器管理员联系**。如下图所示：

## 可能原因

| 可能原因 | 处理措施 |
| --- | --- |
| 远程桌面会话主机角色授权到期 | 检查并删除远程桌面会话主机角色 |
| 未在微软购买 License | 检查并确保已购买 License |

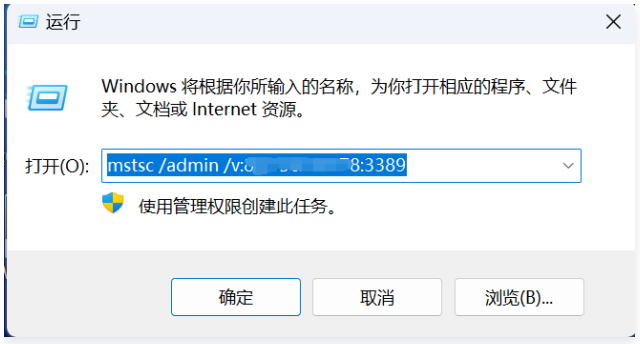
## 故障处理

### 步骤一 登录云服务器

可先通过以下两种登录方式中的任意一种登录云服务器，然后参照下方指引，执行**检查并删除远程桌面会话主机角色**。

**方法1：命令方式登录云服务器**

可在**运行**窗口或**命令提示符**窗口中输入命令：**mstsc /admin /v:云服务器IP地址:远程端口号**，登录云服务器。




**方法2：VNC 方式登录云服务器**

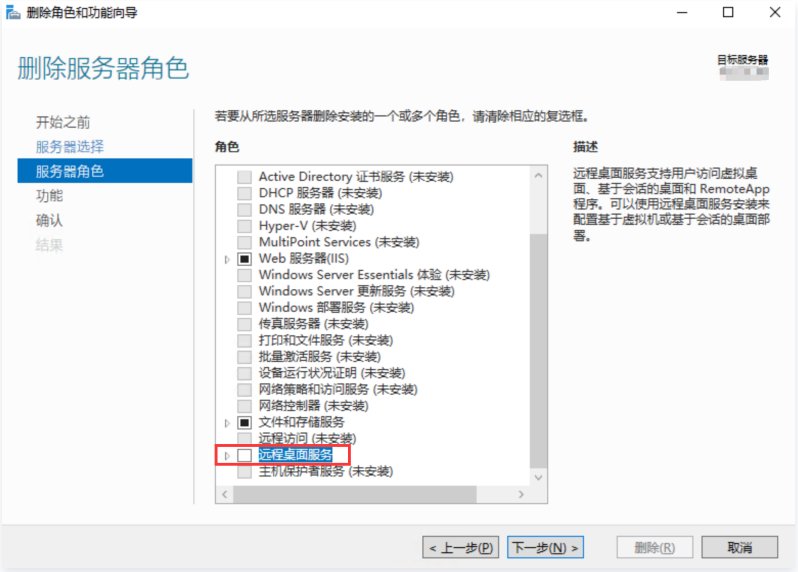
VNC 登录是腾讯云为用户提供的一种通过 Web 浏览器远程连接云服务器的方式。在没有安装或者无法使用远程登录客户端，以及通过其他方式均无法登录的情况下，用户可以通过 VNC 登录连接到云服务器，观察云服务器状态，并且可通过云服务器账户进行基本的云服务器管理操作，具体操作请参见：使用 VNC 登录 Windows 实例 。

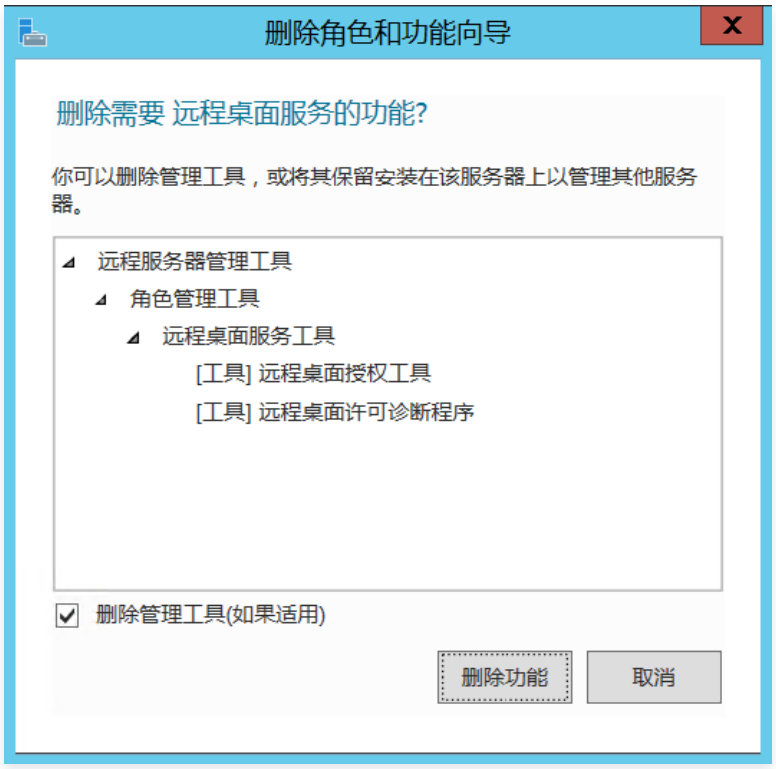
### 步骤二 检查并删除远程桌面会话主机角色

> **说明：**
> 以下操作以 Windows Server 2016操作系统的实例为例。

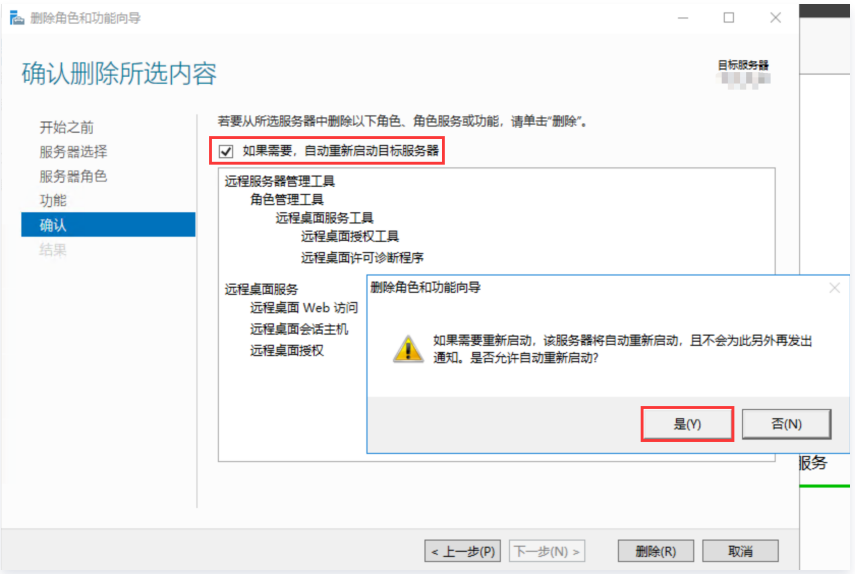
1. 在操作系统界面，单击 ，打开**服务器管理器**。
2. 单击**服务器管理器**右上方的**管理**，选择**删除角色和功能**。如下图所示：

3. 在**删除角色和功能向导**窗口中，单击**下一步**。
4. 在**删除服务器角色**界面，取消勾选**远程桌面服务**，并在弹出的提示框中，选择**删除功能**。如下图所示：






5. 单击两次**下一步**。
6. 勾选**如果需要，自动重新启动目标服务器**，并在弹出的提示框中单击**是**。如下图所示：




7. 单击**删除**，待云服务器重新启动即可恢复默认登录功能。

## 如何购买 RDS License

Windows Server 默认允许2个用户同时登录，可满足绝大多数需求。如果您有超过2个用户同时登录需求（也就是说您不能删除**远程桌面会话主机**角色），需要您联系微软或微软合作伙伴等正规渠道购买多用户登录 RDS 授权。具体您可拨打微软市场部热线：**4008203800，根据语音提示按数字选择是否录音，然后按数字2，再按数字4**，进行咨询购买，或者前往 微软官网 咨询购买与配置相应的证书授权。

> **注意：**
> 微软市场部热线电话（4008203800-x-2-4）可能会变化，也请您根据实际语音提示随机应变，这里的数字2指企事业用户/商业用户，数字4指微软采购部门，不能按错，谢谢您的理解。

# Windows 实例：端口问题导致无法远程登录

最近更新时间：2025-04-17 11:08:32

本文为您介绍云服务器因端口问题导致无法登录的排查方法，您可以通过观看如下视频或查阅本文来了解排查方案。
观看视频

> **说明：**
> 以下操作以 Windows Server 2022 系统的云服务器为例。

## 检查工具

您可以通过腾讯云提供的以下工具判断无法登录是否与端口和安全组设置相关：

- 自助诊断
- 安全组（端口）验通工具

如果检测为安全组设置的问题，您可以通过 安全组（端口）验通工具 中的**一键放通**功能放通相关端口并再次尝试登录。如果放通端口后还是登录失败，可参见以下内容逐步排查原因。

## 可能原因

| 可能原因 | 处理措施 |
| --- | --- |
| 本地和服务器间的网络未连通 | 检查本地和服务器间的网络确保连通 |
| 服务器内的远程桌面服务未配置 | 检查服务器内的远程桌面服务确保已配置 |
| 服务器内的远程访问端口未开启 | 检查服务器内的远程访问端口确保已开启 |
| 服务器内的注册表远程端口未一致 | 检查服务器内的注册表远程端口确保一致 |
| 远程登录服务异常 | 重启远程登录服务 |

## 故障处理

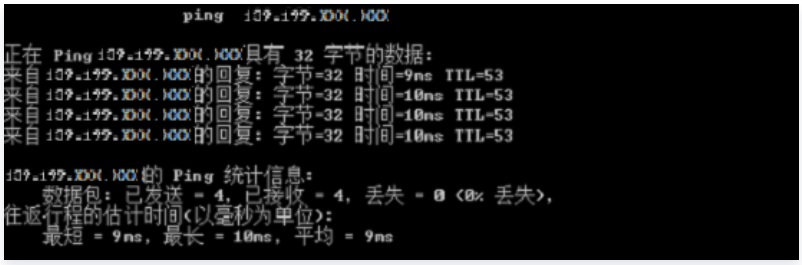
### 检查本地和服务器间的网络确保连通

您可以在本地计算机上通过本地 Ping 命令，测试网络的连通性。同时使用不同网络环境中（不同网段或不同运营商）的电脑测试，判断是本地网络问题还是服务器端问题。

1. 根据本地计算机的操作系统类型，选择命令行工具的打开方式。
   - Windows 系统：单击**开始** > **运行**，输入 **cmd**，弹出命令行对话框。
   - MacOS 系统：打开 Terminal 工具。
2. 执行以下命令，测试网络连接。

```
ping + 云服务器实例公网 IP 地址
```

   例如，执行 `ping 139.199.XXX.XXX` 命令。
   - 如果网络正常，返回类似以下结果，请 检查服务器内的远程桌面服务确保已配置 。




   - 如果网络异常，则出现**请求超时**提示，请参见 实例 IP 地址 Ping 不通 进行排查。
3. 执行以下命令，并按 **Enter**，测试远程端口开启情况，判断端口是否可以访问。

```
telnet + 云服务器实例公网 IP 地址 + 端口号
```

例如，执行 `telnet 139.199.XXX.XXX 3389` 命令。如下图所示：

```
telnet 139.199.XXX.XXX 3389_
```

- 正常情况：黑屏，仅显示光标。说明远程端口（3389）可访问，请 检查服务器内的远程桌面服务确保已配置 。
- 异常情况：连接失败，如下图所示。说明网络出现问题，请检查网络相应部分。

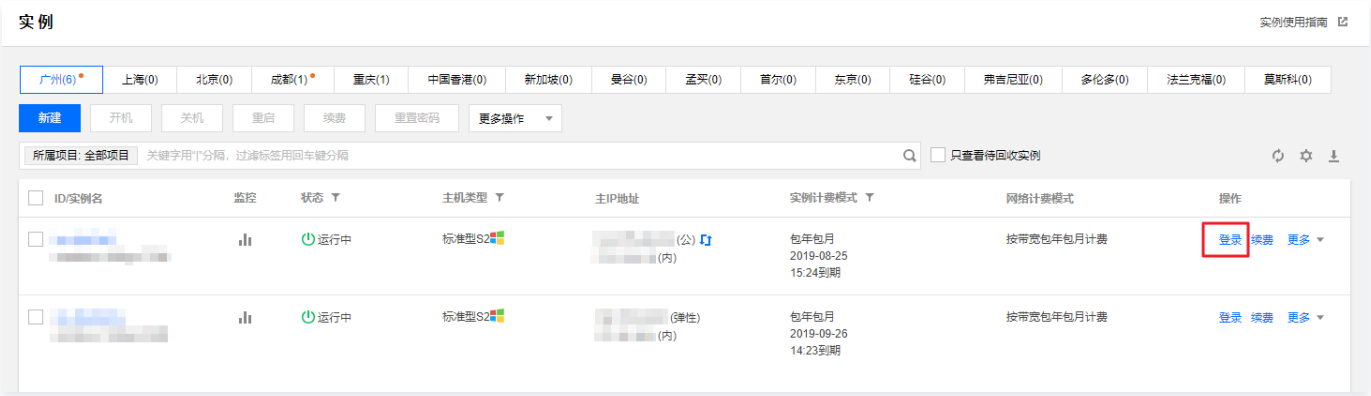
```
telnet 139.199.XXX.XXX 3389
正在连接139.199.XXX.XXX..无法打开到主机的连接。 在端口 3389: 连接失败
```

## 检查服务器内的远程桌面服务确保已配置

> **说明：**
> VNC 方式是您通过标准方式无法登录服务器时建议的登录方式。

通过腾讯云 VNC 登录进入服务器内部进行检查。

1. 登录 云服务器控制台 。
2. 选择待检查的云服务器，单击**登录**。如下图所示：

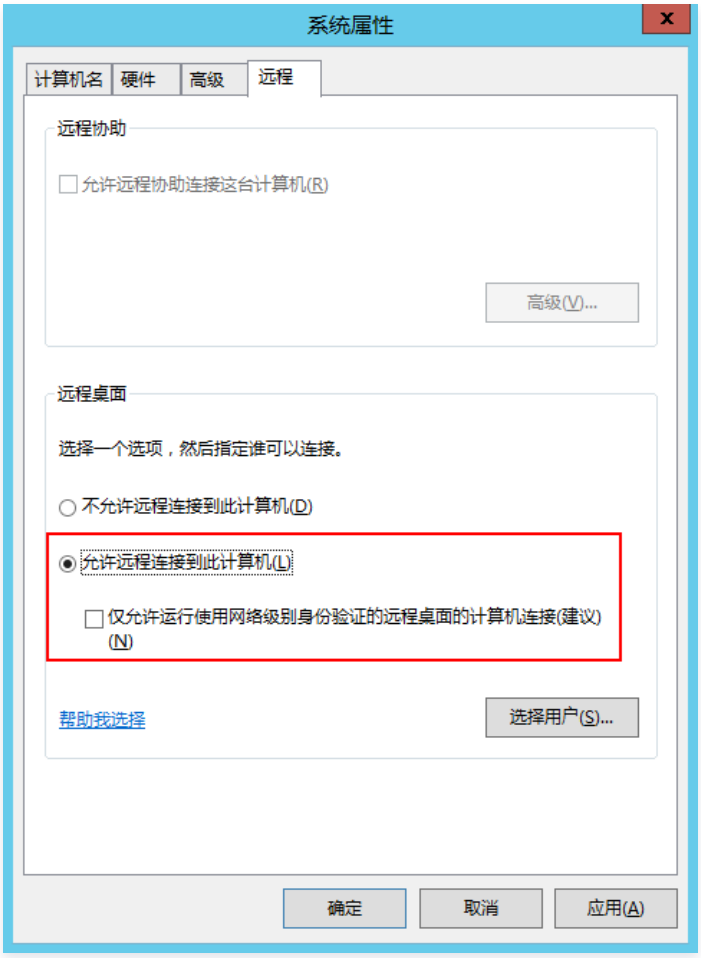



3. 在弹出的**标准登录 | Windows 实例**窗口中，选择**VNC登录**，登录云服务器。
4. 在弹出的登录窗口中，选择左上角的**发送远程命令**，单击 **Ctrl-Alt-Delete** 进入系统登录界面。如下图所示：

### 检查云服务器的远程桌面配置是否开启

1. 在云服务器中，右击 ⊞ ，单击**系统**，打开**系统**窗口。
2. 在**系统**窗口中，选择**高级系统设置**，打开**系统属性**窗口。

3. 在**系统属性**窗口中，选择**远程**页签，检查**远程桌面**功能栏中是否勾选**允许远程连接到此计算机**。如下图所示：



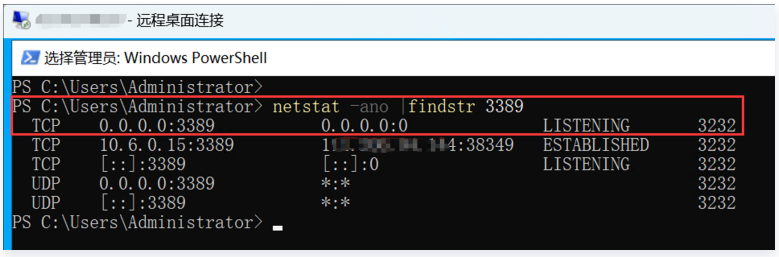

- 已勾选**允许远程连接到此计算机**，表示已开启远程连接配置，请 检查服务器内的远程访问端口确保已开启 。
- 未勾选**允许远程连接到此计算机**，请勾选并重新进行远程连接实例，查看是否连接成功。

## 检查服务器内的远程访问端口确保已开启

1. 在云服务器中，单击 ，打开 Windows PowerShell 窗口。
2. 在 Windows PowerShell 窗口中，执行以下命令，检查远程桌面运行情况（默认情况下，远程桌面服务端口号为3389）。

```
netstat -ano | findstr 3389
```

- 若返回类似以下结果，表示正常情况，请 重启远程登录服务 ，并重新进行远程连接实例，查看是否连接成功。

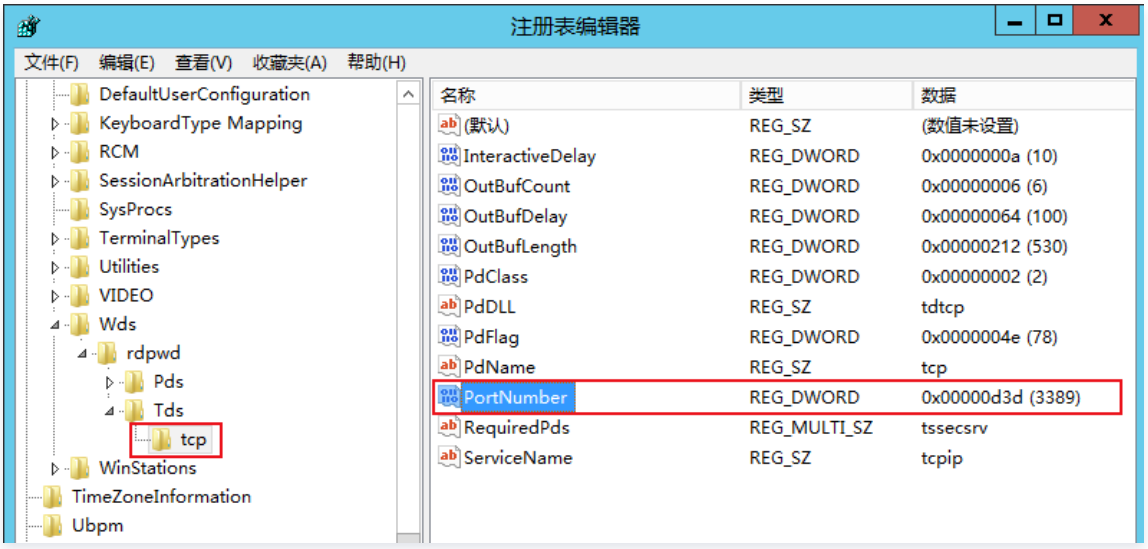



- 若不显示任何连接，表示异常情况，请 检查服务器内的注册表远程端口确保一致 。

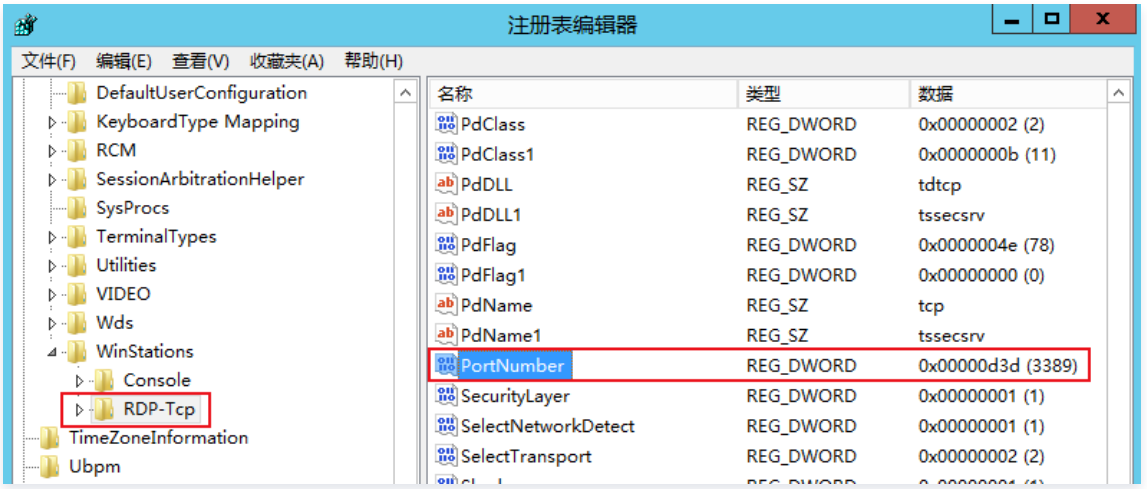
## 检查服务器内的注册表远程端口确保一致

> **注意：**
> 该步骤指导您检查 TCP PortNumber 和 RDP Tcp PortNumber 两处端口号，两处端口号必须一致。

1. 在云服务器中，单击 ⊞，选择 🔍，输入 **regedit**，按 **Enter**，打开**注册表编辑器**窗口。
2. 在左侧的注册表导航中，依次展开 **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Control** > **Terminal Server** > **Wds** > **rdpwd** > **Tds** > **tcp** 目录。
3. 找到 **tcp** 中的 PortNumber，并记录 PortNumber 的数据（即端口号，默认为3389）。如下图所示：




4. 在左侧的注册表导航中，依次展开 **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Control** > **Terminal Server** > **WinStations** > **RDP-Tcp** 目录。
5. 找到 **RDP-Tcp** 中的 PortNumber，并确认 **RDP-Tcp** 中的 PortNumber 数据（端口号）是否与 **tcp** 中的 PortNumber 数据（端口号）一致。如下图所示：

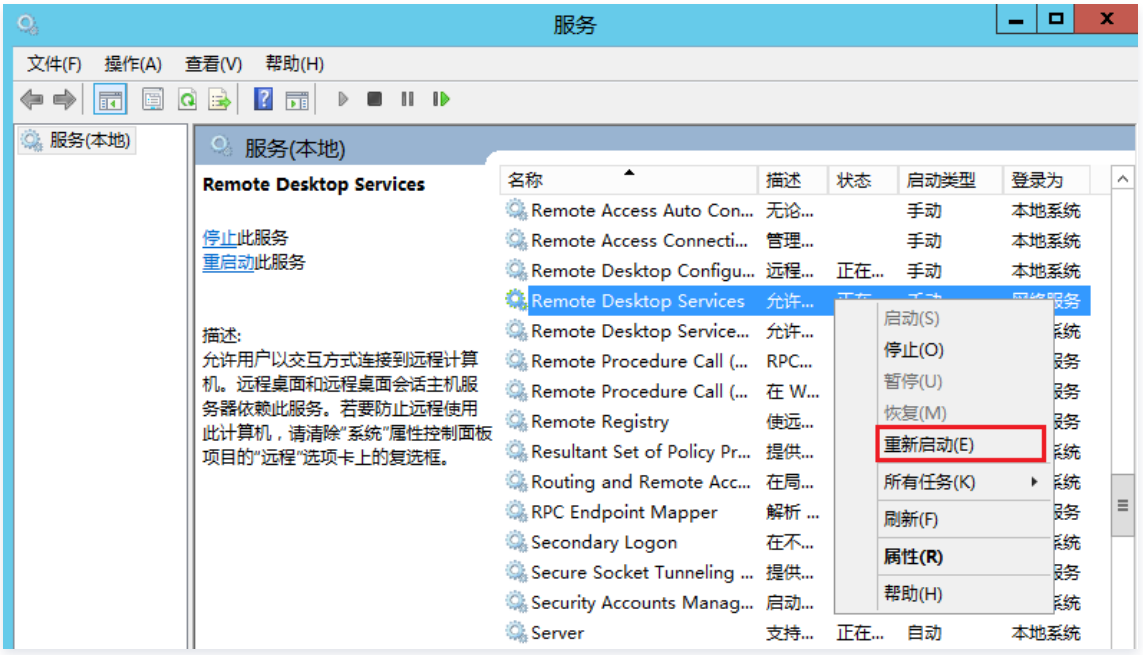



   - 若访问端口号不一致，请执行 步骤 6 。
   - 若访问端口号一致，请 重启远程登录服务 。
6. 双击 **RDP-Tcp** 中的 PortNumber。
7. 在弹出的对话框中，将**数值数据**修改为0 – 65535之间未被占用端口，使 **TCP PortNumber** 和 **RDP Tcp PortNumber** 端口号保持一致，单击**确定**。
8. 修改完成后，在 云服务器控制台 重启该实例，并重新进行远程连接实例，查看是否连接成功。

## 重启远程登录服务

1. 在云服务器中，单击 ⊞，选择 🔍，输入 **services.msc**，按 **Enter**，打开**服务**窗口。

2. 在**服务**窗口中，找到 **Remote Desktop Services**，并右键单击 **Remote Desktop Services**，选择**重新启动**，重启远程登录服务。如下图所示：




如若执行以上操作仍未解决无法远程登录问题，请通过 在线支持 进行反馈。

# Linux 实例登录相关问题
# 无法登录 Linux 实例

最近更新时间：2025-06-16 17:00:21

以下视频介绍了无法登录 Linux 实例时的排查方法：
观看视频
本文主要介绍无法连接 Linux 实例时对问题进行排查的方法，以及可能导致无法连接 Linux 实例的主要原因，指导您排查、定位并解决问题。

## 问题定位

### 使用实例自助检测工具

腾讯云提供实例自助检测工具，可以帮助您判断是否由于带宽、防火墙以及安全组设置等常见问题引起。70%的故障可以通过工具定位，您可以根据检测到的原因，定位可能引起无法登录的故障问题。

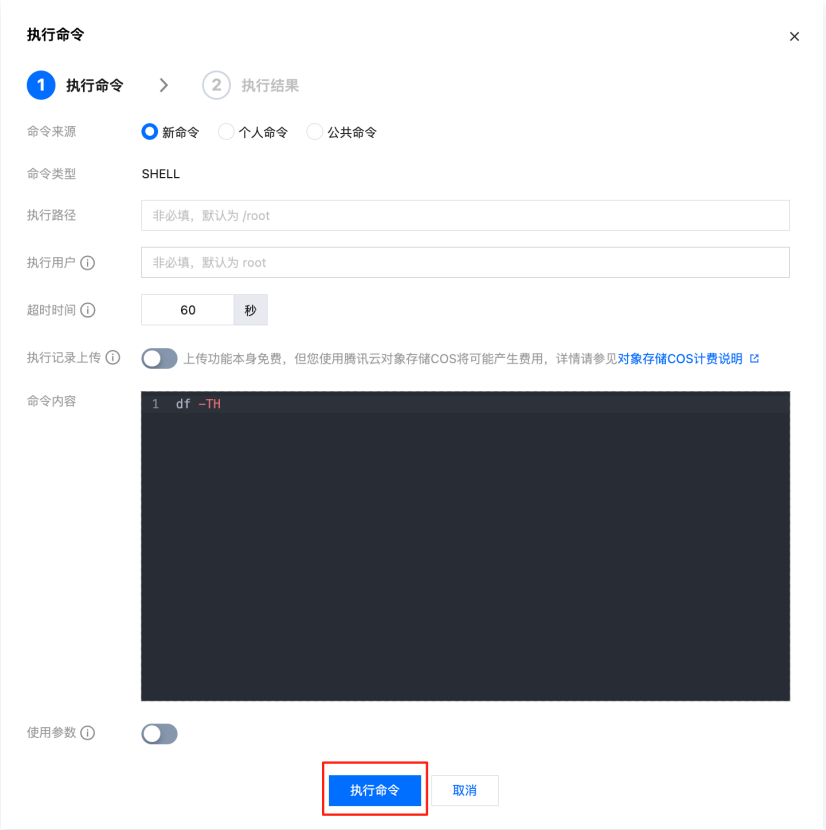
1. 单击 实例自助检测 ，打开自助检测工具。
2. 根据实例自助检测界面提示，选择需要检测的云服务器，单击**开始检测**。如下图所示：

### 使用自动化助手发送命令

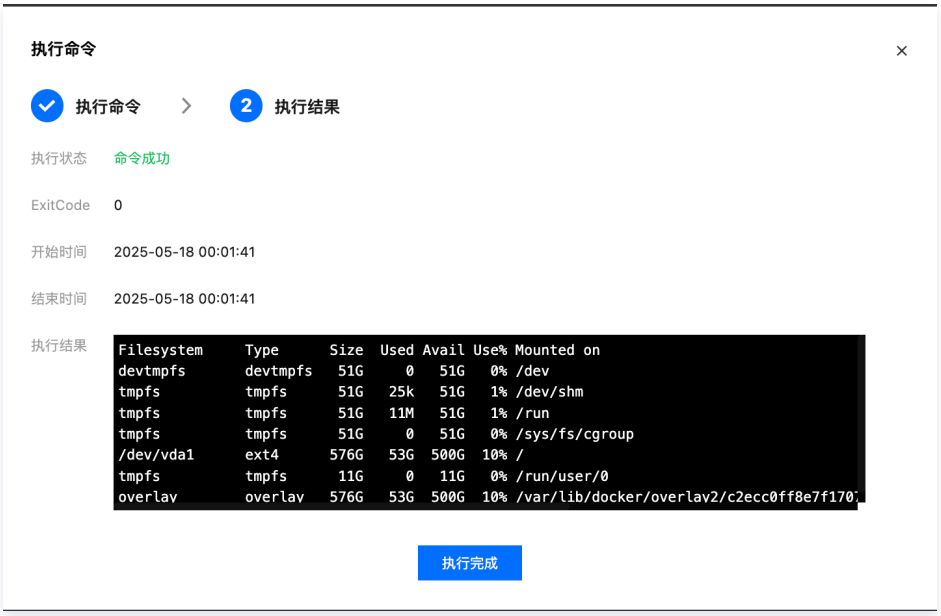
您可使用自动化助手向实例发送命令，进行问题排查及定位。使用步骤如下：

1. 登录 云服务器控制台 ，在实例列表中单击实例 ID。
2. 在实例详情页中，选择**执行命令**页签，并单击**执行命令**。如下图所示：

3. 在弹出的**执行命令**窗口中，您可按需选择命令，单击**执行命令**即可执行命令并查看命令结果。
   例如，输入新命令 `df -TH` 并单击**执行命令**，即可在不登录实例的情况下查看其结果。如下图所示：




执行完成后可查看执行结果，如下图所示。




如需了解自动化助手的更多信息，请参见 自动化助手 。

> **说明**
> 如果您的问题无法通过故障排查工具检查，建议您 通过 VNC 的方式登录 云服务器逐步排查故障。

## 可能原因

无法登录 Linux 实例的主要原因包括：

- SSH 问题导致无法登录
- 密码问题导致无法登录
- 带宽利用率过高

- 服务器高负载
- 安全组规则不当

## 故障处理

### 通过 VNC 方式登录

当您无法通过标准方式（orcaterm）或者远程登录软件登录 Linux 实例时，您可以使用腾讯云 VNC 登录的方式登录，帮助您定位故障原因。

1. 登录 云服务器控制台 。
2. 在实例的管理页面，选择您需要登录的实例，单击**登录**。如下图所示：

3. 在弹出的**登录**窗口中，选择 **VNC登录**。如下图所示：

> **说明**
> 登录过程中，如果忘记密码，可以在控制台中重置该实例的密码。具体操作可参见 重置实例密码 。

4. 输入用户名和密码登录，完成登录。

### SSH 问题导致无法登录

**故障现象：** 使用 SSH 登录 Linux 实例 时，提示无法连接或者连接失败。
**处理步骤：** 参见 无法通过 SSH 方式登录 Linux 实例 进行排查。

### 密码问题导致无法登录

**故障现象：** 密码输入错误、忘记密码或者密码重置失败导致登录不成功。
**解决方法：** 请在 腾讯云控制台 重置该实例的密码，并重启实例。

**处理步骤：**重置实例密码的方法请参见 重置实例密码 。

### 带宽利用率过高

**故障现象：**通过实例自助检测工具诊断，提示问题为带宽利用率过高。
**处理步骤：**
1. 通过 VNC 登录 实例。
2. 参见 带宽占用高导致无法登录 ，查看实例的带宽使用情况和处理故障。

### 服务器高负载

**故障现象：**通过自助检查工具或者腾讯云可观测平台，显示服务器 CPU 负载过高导致系统无法进行远程连接或者访问非常卡。
**可能原因：**病毒木马、第三方杀毒软件、应用程序异常、驱动异常或者软件后台的自动更新，会造成 CPU 占用率高，导致登录不上云服务器或者访问慢的问题。
**处理步骤：**
1. 通过 VNC 登录 实例。
2. 参见 Linux 实例：CPU 与内存占用率高导致无法登录 ，在 “任务管理器” 中定位高负载的进程。

### 安全组规则不当

**故障现象：**通过自助检查工具检查，发现安全组规则设置不当导致无法登录。
**处理步骤：**通过 安全组（端口）验通工具 进行检查。

如果确定为安全组端口设置问题，可以参见 安全组设置 添加放通对应的端口规则即可。
如果您需要自定义设置安全组规则，请参见 添加安全组规则 重新配置安全组规则。

## 其他解决方案

通过上述排查后，仍然不能连接 Linux 实例，请您保存自助检测结果，通过 在线支持 进行反馈。

# Linux 实例：无法通过 SSH 方式登录

最近更新时间：2025-06-03 11:17:42

**说明：**
- 本文来源于社区贡献，仅供参考，与腾讯云相关产品无关。您可前往 社区 获取更多帮助和支持。
- 文中涉及的相关文件操作，请务必谨慎执行。如有必要，可通过创建快照等方式进行数据备份。

## 现象描述

使用 SSH 登录 Linux 实例 时，提示无法连接或者连接失败，导致无法正常登录 Linux 实例。

| 现象描述 | 处理措施 |
| --- | --- |
| SSH 登录报错 User root not allowed because not listed in AllowUsers | 排查 SSH 登录报错 User root not allowed because not listed in AllowUsers |
| SSH 登录报错 Disconnected:No supported authentication methods available | 排查 SSH 登录报错 Disconnected:No supported authentication methods available |
| SSH 登录报错 ssh_exchange_identification: read: Connection reset by peer | 排查 SSH 登录报错 ssh_exchange_identification: read: Connection reset by peer |
| SSH 登录报错 Permission denied, please try again | 排查 SSH 登录报错 Permission denied, please try again |
| SSH 登录时报错 Too many authentication failures for root | 排查 SSH 登录时报错 Too many authentication failures for root |
| SSH 启动时报错 error while loading shared libraries | 排查 SSH 启动时报错 error while loading shared libraries |
| SSH 服务启动时报错 fatal: Cannot bind any address | 排查 SSH 服务启动时报错 fatal: Cannot bind any address |
| SSH 服务启动时报错 Bad configuration options | 排查 SSH 服务启动时报错 Bad configuration options |
| SSH 启用 UseDNS 导致 SSH 登录或数据传输速度变慢 | 排查 SSH 启用 UseDNS 导致 SSH 登录或数据传输速度变慢 |
| SSH 登录报错 No supported key exchange algorithms | 排查 SSH 登录报错 No supported key exchange algorithms |
| SSH 服务启动时报错 must be owned by root and not group or word-writable | 排查 SSH 服务启动时报错 must be owned by root and not group or word-writable |
| SSH 登录时报错 Host key verification failed | 排查 SSH 登录时报错 Host key verification failed |
| SSH 登录报错 pam_listfile(sshd:auth): Refused user root for service sshd | 排查 SSH 登录报错 pam_listfile(sshd:auth): Refused user root for service sshd |
| SSH 登录时报错 requirement "uid >= 1000" not met by user "root" | 排查 SSH 登录时报错 requirement "uid >= 1000" not met by user "root" |
| SSH 登录时报错 Maximum amount of failed attempts was reached | 排查 SSH 登录时报错 Maximum amount of failed attempts was reached |
| SSH 登录时报错 login: Module is unknown | 排查 SSH 登录时报错 login: Module is unknown |
| 病毒引起 SSH 服务运行异常报错 fatal: mm_request_send: write: Broken pipe | 排查 病毒引起 SSH 服务运行异常报错 fatal: mm_request_send: write: Broken pipe |
| SSH 服务启动时报错 main process exited, code=exited | 排查 SSH 服务启动时报错 main process exited, code=exited |
| SSH 登录时报错 pam_limits(sshd:session)：could not sent limit for ‘nofile’ | 排查 SSH 登录时报错 pam_limits(sshd:session)：could not sent limit for ‘nofile’ |
| SSH 登录报错 pam_unix(sshdsession) session closed for user | 排查 SSH 登录报错 pam_unix(sshdsession) session closed for user |

## 故障处理

当使用 SSH 登录 Linux 实例失败，并返回报错信息时，您可记录报错信息，并匹配以下常见的报错信息，快速定位问题并参考步骤进行解决。

## 排查 SSH 登录报错 User root not allowed because not listed in AllowUsers

### 现象描述

使用 SSH 登录 Linux 实例时，无法正常登录。客户端或服务端的 secure 日志中出现类似如下信息：

- Permission denied, please try again.
- User test from 192.X.X.1 not allowed because not listed in AllowUsers.
- User test from 192.X.X.1 not allowed because listed in DenyUsers.
- User root from 192.X.X.1 not allowed because a group is listed in DenyGroups.
- User test from 192.X.X.1 not allowed because none of user's groups are listed in AllowGroups.

### 可能原因

该问题通常是由于 SSH 服务启用了用户登录控制参数，对登录用户进行了限制。参数说明如下：

- **AllowUsers**：允许登录的用户白名单，只有该参数标注的用户可以登录。
- **DenyUsers**：拒绝登录的用户黑名单，该参数标注的用户都被拒绝登录。
- **AllowGroups**：允许登录的用户组白名单，只有该参数标注的用户组可以登录。
- **DenyGroups**：拒绝登录的用户组黑名单，该参数标注的用户组都被拒绝登录。

> **说明：**
> 拒绝策略优先级高于允许策略。

### 解决思路

1. 参见 处理步骤，进入 SSH 配置文件 `sshd_config` 检查配置。
2. 删除用户登录控制参数，并重启 SSH 服务即可。

### 处理步骤

1. 使用 VNC 登录 Linux 实例。
2. 执行以下命令，使用 VIM 编辑器进入 `sshd_config` 配置文件。

```
vim /etc/ssh/sshd_config
```

3. 按 **i** 进入编辑模式，找到并删除以下配置，或在每行行首增加 `#` 进行注释。

```
AllowUsers root test
DenyUsers test
DenyGroups test
AllowGroups root
```

4. 按 **Esc** 退出编辑模式，输入 **:wq** 保存修改。
5. 对应实际使用的操作系统，执行以下命令，重启 SSH 服务。
   - CentOS

     ```
     systemctl restart sshd.service
     ```

   - Ubuntu

     ```
     service sshd restart
     ```

   重启 SSH 服务后，即可使用 SSH 登录。详情请参见 使用 SSH 登录 Linux 实例。

## 排查 SSH 登录报错 Disconnected:No supported authentication methods available

### 现象描述

使用 SSH 登录时，出现如下报错信息：

```
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
sshd[10826]: Connection closed by xxx.xxx.xxx.xxx.
Disconnected:No supported authentication methods available.
```

### 可能原因

SSH 服务修改了 `PasswordAuthentication` 参数，禁用了密码验证登录。

### 解决思路

1. 参见 处理步骤，进入 SSH 配置文件 `sshd_config` 。
2. 修改 `PasswordAuthentication` 参数，并重启 SSH 服务即可。
3. 部分系统相关配置在 `/etc/ssh/sshd_config.d/50-cloud-init.conf` 文件，如果存在对应文件，建议同时检查该文件是否存在 `PasswordAuthentication` 配置项。

### 处理步骤

1. 使用 VNC 登录 Linux 实例 。
2. 执行以下命令，使用 VIM 编辑器进入 `sshd_config` 配置文件。

   ```
   vim /etc/ssh/sshd_config
   ```

3. 按 **i** 进入编辑模式，将 `PasswordAuthentication no` 修改为 `PasswordAuthentication yes` 。
4. 按 **Esc** 退出编辑模式，并输入 **:wq** 保存修改。
5. 对应实际使用的操作系统，执行以下命令，重启 SSH 服务。
   - CentOS

     ```
     systemctl restart sshd.service
     ```

   - Ubuntu

     ```
     service sshd restart
     ```

   重启 SSH 服务后，即可使用 SSH 登录。详情请参见 使用 SSH 登录 Linux 实例 。

## 排查 SSH 登录报错 ssh_exchange_identification: read: Connection reset by peer

### 现象描述

使用 SSH 登录时，出现如下报错信息：

- “ssh_exchange_identification: read: Connection reset by peer”
- “ssh_exchange_identification: Connection closed by remote host”
- “kex_exchange_identification: read: Connection reset by peer”
- “kex_exchange_identification: Connection closed by remote host”

### 可能原因

导致出现该类问题的原因较多，常见原因有以下几种：

- 本地访问控制限制了连接。
- 某些入侵防御软件更改了防火墙规则，例如 Fail2ban 及 denyhost 等。
- sshd 配置的最大连接数限制。
- 本地网络存在问题。

### 解决思路

参见 处理步骤，从访问策略、防火墙规则、sshd 配置及网络环境几方面定位及解决问题。

### 处理步骤

#### 检查及调整访问策略设置

Linux 中可以通过 `/etc/hosts.allow` 和 `/etc/hosts.deny` 文件设置访问策略，两个文件分别对应允许和阻止的策略。例如，可以在 `hosts.allow` 文件中设置信任主机规则，在 `hosts.deny` 文件中拒绝所有其他主机。以 `hosts.deny` 为例，阻止策略配置如下：

```
in.sshd:ALL          # 阻止全部ssh连接
in.sshd:218.64.87.0/255.255.255.128 # 阻止218.64.87.0--127的ssh
ALL:ALL              # 阻止所有TCP连接
```

使用 VNC 登录 Linux 实例 后，请检查 `/etc/hosts.deny` 文件及 `/etc/hosts.allow` 文件。并根据检查结果选择以下处理方式：

- 配置有误，请按需修改，更改即时生效。
- 未配置或配置无误，请进行下一步。

> **说明**
> 若您未配置访问策略，则默认文件均为空，且允许所有连接。

#### 检查 iptables 防火墙规则

检查 iptables 防火墙规则是否被修改，包括使用某些入侵防御软件，例如 Fail2ban 及 denyhost 等。执行以下命令，查看防火墙是否阻止过 SSH 连接。

```
sudo iptables -L --line-number
```

根据上面命令输出结果，如果有对应 ssh 连接 ip 或者端口的 DROP 或者 REJECT 规则，则是连接被阻止；如果没有，则是未被阻止。

- 若 SSH 连接被阻止，请通过对应软件白名单等相关策略自行设置。
- 若 SSH 连接未被阻止，请进行下一步。

#### 检查及调整 sshd 配置

1. 执行以下命令，使用 VIM 编辑器进入 `sshd_config` 配置文件。

   ```
   vim /etc/ssh/sshd_config
   ```

2. 检查 `MaxStartups` 值是否需调整。`sshd_config` 配置文件中通过 `MaxStartups` 设置允许的最大连接数，如果短时间需建立较多连接，则需适当调整该值。
3. 若需调整，则请参考以下步骤修改：

   3.1 按 **i** 进入编辑模式，修改完成后按 **Esc** 退出编辑模式，并输入 **:wq** 保存修改。

   > **说明：**
   > MaxStartups 10:30:100为默认配置，指定 SSH 守护进程未经身份验证的并发连接的最大数量。10:30:100表示从第10个连接开始，以30%的概率拒绝新的连接，直到连接数达到100。

   3.2 执行以下命令，重启 sshd 服务。

   ```
   service sshd restart
   ```

4. 若无需调整，请进行下一步。

#### 测试网络环境

1. 检查是否使用了 内网 IP 进行登录。
   - 是，请切换为 公网 IP 后再次进行尝试。
   - 否，请进行下一步。
2. 使用其他网络环境测试是否连接正常。

- 是，请重启实例后使用 VNC 登录实例。
- 否，请根据测试结果解决网络环境问题。

若至此您仍未解决 SSH 登录问题，则可能是由于系统内核出现异常或其他潜在原因导致，请通过 在线支持 联系我们进一步处理问题。

## 排查 SSH 登录报错 Permission denied, please try again

### 现象描述

root 用户使用 SSH 登录 Linux 实例时，出现报错信息 “Permission denied, please try again”。

### 可能原因

系统启用了 SELinux 服务，或是 SSH 服务修改了 `PermitRootLogin` 配置。

### 解决思路

参见 处理步骤，检查 SELinux 服务及 SSH 配置文件 `sshd_config` 中的 `PermitRootLogin` 参数，核实问题原因并解决问题。

### 处理步骤

#### 检查及关闭 SELinux 服务

1. 使用 VNC 登录 Linux 实例。
2. 执行以下命令，查看当前 SELinux 服务状态。

```
/usr/sbin/sestatus -v
```

若返回参数为 `enabled` 即处于开启状态， `disabled` 即处于关闭状态。如下所示，则为开启状态：

```
SELinux status:       enabled
```

3. 您可结合实际情况，临时或永久关闭 SELinux 服务。
   - 临时关闭 SELinux 服务
     执行以下命令，临时关闭 SELinux。修改实时生效，无需重启系统或实例。

     ```
     setenforce 0
     ```

   - 永久关闭 SELinux 服务
     执行以下命令，关闭 SELinux 服务。

     ```
     sed -i 's/SELINUX=enforcing/SELINUX=disabled/' /etc/selinux/config
     ```

     **注意：**
     - 该命令仅适用于 SELinux 服务为 enforcing 状态时。
     - 执行命令后需重启系统或实例，使修改生效。

#### 检查及调整 sshd 配置

1. 使用 VNC 登录 Linux 实例。
2. 执行以下命令，使用 VIM 编辑器进入 `sshd_config` 配置文件。

```
vim /etc/ssh/sshd_config
```

3. 按 i 进入编辑模式，将 `PermitRootLogin no` 修改为 `PermitRootLogin yes` 。

**说明：**
- 若 `sshd_config` 中未配置该参数，则默认允许 root 用户登录。

> - 该参数仅影响 root 用户使用 SSH 登录，不影响 root 用户通过其他方式登录实例。

4. 按 **Esc** 退出编辑模式，并输入 **:wq** 保存修改。
5. 执行以下命令，重启 SSH 服务。

```
service sshd restart
```

重启 SSH 服务后，即可使用 SSH 登录。详情请参见 使用 SSH 登录 Linux 实例 。

## 排查 SSH 登录时报错 Too many authentication failures for root

### 现象描述

使用 SSH 登录时，登录时多次输入密码后返回报错信息 “Too many authentication failures for root”，并且连接中断。

### 可能原因

在多次连续输入错误密码后，触发了 SSH 服务密码重置策略。

### 解决思路

1. 参见 处理步骤，进入 SSH 配置文件 `sshd_config` 。
2. 检查并修改 SSH 服务密码重置策略的 `MaxAuthTries` 参数配置，并重启 SSH 服务即可。

### 处理步骤

1. 使用 VNC 登录 Linux 实例 。
2. 执行以下命令，使用 VIM 编辑器进入 `sshd_config` 配置文件。

```
vim /etc/ssh/sshd_config
```

3. 查看是否包含类似如下配置。

```
MaxAuthTries 5
```

> **说明：**
> - 该参数默认未启用，用于限制用户每次使用 SSH 登录时，能够连续输入错误密码的次数。超过设定的次数则会断开 SSH 连接，并显示相关错误信息。但相关账号不会被锁定，仍可重新使用 SSH 登录。
> - 请您结合实际情况确定是否需修改配置，如需修改，建议您备份 `sshd_config` 配置文件。

4. 按 **i** 进入编辑模式，修改以下配置，或在行首增加 `#` 进行注释。

```
MaxAuthTries <允许输入错误密码的次数>
```

5. 按 **Esc** 退出编辑模式，输入 **:wq** 保存修改。
6. 执行以下命令，重启 SSH 服务。

```
service sshd restart
```

重启 SSH 服务后，即可使用 SSH 登录。详情请参见 使用 SSH 登录 Linux 实例 。

## 排查 SSH 启动时报错 error while loading shared libraries

### 现象描述

Linux 实例启动 SSH 服务，在 secure 日志文件中，或直接返回类似如下错误信息：

- “error while loading shared libraries： libcrypto.so.10: cannot open shared object file: No such file or directory”

- “PAM unable to dlopen(/usr/lib64/security/pam_tally.so): /usr/lib64/security/pam_tally.so: cannot open shared object file: No such file or directory”

**可能原因**

SSH 服务运行依赖的相关系统库文件丢失或权限配置等异常。

**解决思路**

参见 处理步骤 检查系统库文件并进行修复。

**处理步骤**

> **说明：**
> 本文以处理 libcrypto.so.10 库文件异常为例，其他库文件异常的处理方法类似，请结合实际情况进行操作。

**获取库文件信息**

1. 使用 VNC 登录 Linux 实例。
2. 执行以下命令，查看 libcrypto.so.10 库文件信息。

```
ll /usr/lib64/libcrypto.so.10
```

返回类似如下信息，表示 `/usr/lib64/libcrypto.so.10` 是 `libcrypto.so.1.0.2k` 库文件的软链接。

```
lrwxrwxrwx 1 root root 19 Jan 19  2021 /usr/lib64/libcrypto.so.10 -> libcrypto.so.1.0.2k
```

3. 执行以下命令，查看 `libcrypto.so.1.0.2k` 库文件信息。

```
ll /usr/lib64/libcrypto.so.1.0.2k
```

返回类似如下信息：

```
-rwxr-xr-x 1 root root 2520768 Dec 17  2020 /usr/lib64/libcrypto.so.1.0.2k
```

4. 记录正常库文件的路径、权限、属组等信息，并通过以下方式进行处理：
   - 查找及替换库文件
   - 外部文件上传
   - 通过快照回滚恢复

**查找及替换库文件**

1. 执行以下命令，查找 `libcrypto.so.1.0.2k` 文件。

```
find / -name libcrypto.so.1.0.2k
```

2. 根据返回结果，执行以下命令，将库文件拷贝至正常目录。

```
cp <步骤1获取的库文件绝对路径> /usr/lib64/libcrypto.so.1.0.2k
```

3. 依次执行以下命令，修改文件权限、所有者及属组。

```
chmod 755 /usr/lib64/libcrypto.so.1.0.2k
```

```
chown root:root /usr/lib64/libcrypto.so.1.0.2k
```

4. 执行以下命令，创建软链接。

```
ln -s /usr/lib64/libcrypto.so.1.0.2k /usr/lib64/libcrypto.so.10
```

5. 执行以下命令，启动 SSH 服务。

```
service sshd start
```

#### 外部文件上传

1. 通过 FTP 软件将其他正常服务器上的 `libcrypto.so.1.0.2k` 的库文件上传至目标服务器的 `\tmp` 目录。

> **说明：**
> 本文以上传至目标服务器的 `\tmp` 目录为例，您可结合实际情况进行修改。

2. 执行以下命令，将库文件拷贝至正常目录。

```
cp /tmp/libcrypto.so.1.0.2k /usr/lib64/libcrypto.so.1.0.2k
```

3. 依次执行以下命令，修改文件权限、所有者及属组。

```
chmod 755 /usr/lib64/libcrypto.so.1.0.2k
```

```
chown root:root /usr/lib64/libcrypto.so.1.0.2k
```

4. 执行以下命令，创建软链接。

```
ln -s /usr/lib64/libcrypto.so.1.0.2k /usr/lib64/libcrypto.so.10
```

5. 执行以下命令，启动 SSH 服务。

```
service sshd start
```

#### 通过快照回滚恢复

可通过回滚实例系统盘的历史快照进行库文件恢复，详情请参见 从快照回滚数据 。

> **注意：**
> - 快照回滚会导致快照创建后的数据丢失，请谨慎操作。
> - 建议按快照创建时间从近到远的顺序逐一尝试回滚，直至 SSH 服务正常运行。若回滚后仍无法正常运行 SSH 服务，则说明该时间点的系统已经出现异常。

## 排查 SSH 服务启动时报错 fatal: Cannot bind any address

#### 现象描述

Linux 实例启动 SSH 服务时，直接返回或在 secure 日志文件中出现类似如下错误信息：

```
FAILED.
fatal: Cannot bind any address.
address family must be specified before ListenAddress.
```

#### 可能原因

SSH 服务的 `AddressFamily` 参数配置不当。`AddressFamily` 参数用于指定运行时使用的协议簇，若参数仅配置了 IPv6，而系统内未启用 IPv6 或 IPv6 配置无效，则可能出现该问题。

#### 解决思路

1. 参见 处理步骤，进入 SSH 配置文件 `sshd_config` 检查配置。
2. 修改 `AddressFamily` 参数，并重启 SSH 服务即可。

#### 处理步骤

1. 使用 VNC 登录 Linux 实例。
2. 执行以下命令，使用 VIM 编辑器进入 `sshd_config` 配置文件。

```
vim /etc/ssh/sshd_config
```

3. 查看是否包含类似如下配置。

```
AddressFamily inet6
```

常用参数说明如下：
- **inet**：使用 IPv4 协议簇，为默认值。
- **inet6**：使用 IPv6 协议簇。
- **any**：同时启用 IPv4 和 IPv6 协议簇。

4. 按 i 进入编辑模式，修改为以下配置，或在行首增加 `#` 进行注释。

```
AddressFamily inet
```

> **注意：**
> `AddressFamily` 参数需在 `ListenAddress` 前配置才可生效。

5. 按 Esc 退出编辑模式，并输入 :wq 保存修改。
6. 执行以下命令，重启 SSH 服务。

```
service sshd restart
```

重启 SSH 服务后，即可使用 SSH 登录。详情请参见 使用 SSH 登录 Linux 实例。

### 排查 SSH 服务启动时报错 Bad configuration options

#### 现象描述

Linux 实例启动 SSH 服务时，直接返回或在 secure 日志文件中出现类似如下错误信息：

```
/etc/ssh/sshd_config: line 2: Bad configuration options:\\
/etc/ssh/sshd_config: terminating, 1 bad configuration options
```

#### 可能原因

配置文件存在文件编码或配置错误等异常问题。

#### 解决思路

参考处理步骤提供的以下处理项，修复 `sshd_config` 配置文件。
- 对应错误信息修改配置文件
- 外部文件上传
- 重新安装 SSH 服务
- 通过快照回滚恢复

#### 处理步骤

#### 对应错误信息修改配置文件

若错误信息中明确指出了错误配置，则可通过 VIM 编辑器直接修改 `/etc/ssh/sshd_config` 配置文件。您可参考其他实例的正确配置文件进行修改。

#### 外部文件上传

1. 通过 FTP 软件将其他正常服务器上的 `/etc/ssh/sshd_config` 的库文件上传至目标服务器的 `\tmp` 目录。

> **说明：**
> 本文以上传至目标服务器的 `\tmp` 目录为例，您可结合实际情况进行修改。

2. 执行以下命令，将库文件拷贝至正常目录。

```
cp /tmp/sshd_config /etc/ssh/sshd_config
```

3. 依次执行以下命令，修改文件权限、所有者及属组。

```
chmod 600 /etc/ssh/sshd_config
``` ```
chown root:root /etc/ssh/sshd_config
```

4. 执行以下命令，启动 SSH 服务。

```
service sshd start
```

#### 重新安装 SSH 服务

1. 使用 VNC 登录 Linux 实例。
2. 执行以下命令，卸载 SSH 服务。

```
rpm -e openssh-server
```

3. 执行以下命令，安装 SSH 服务。

```
yum install openssh-server
```

4. 执行以下命令，启动 SSH 服务。

```
service sshd start
```

#### 通过快照回滚恢复

可通过回滚实例系统盘的历史快照进行库文件恢复，详情请参见 从快照回滚数据 。

> **注意：**
> - 快照回滚会导致快照创建后的数据丢失，请谨慎操作。
> - 建议按快照创建时间从近到远的顺序逐一尝试回滚，直至 SSH 服务正常运行。若回滚后仍无法正常运行 SSH 服务，则说明该时间点的系统已经出现异常。

### 排查 SSH 启用 UseDNS 导致 SSH 登录或数据传输速度变慢

#### 现象描述

Linux 实例通过外网使用 SSH 登录或进行数据传输时，速度很慢。在切换为内网后，登录及数据传输速度仍然很慢。
```

### 可能原因

可能是由于 SSH 服务启用了 UseDNS 特性。UseDNS 特性是 SSH 服务的安全增强特性，默认未开启。开启后，服务端会先根据客户端 IP 进行 DNS PTR 反向查询，得到客户端主机名。再根据得到的客户端主机名进行 DNS 正向 A 记录查询，最后比对得到的 IP 与原始 IP 是否一致，用以防止客户端欺骗。
通常情况下，客户端使用的都是动态 IP，没有相应的 PTR 记录。该特性开启后，不仅无法用于信息比对，反而由于相关查询操作增加了操作延迟，最终导致客户端连接速度变慢。

### 解决思路

1. 参见 处理步骤，进入 SSH 配置文件 `sshd_config` 。
2. 检查并修改 SSH 服务的 UseDNS 配置，并重启 SSH 服务即可。

### 处理步骤

1. 使用 VNC 登录 Linux 实例 。
2. 执行以下命令，使用 VIM 编辑器进入 `sshd_config` 配置文件。

```
vim /etc/ssh/sshd_config
```

3. 查看是否包含如下配置：

```
UseDNS yes
```

4. 按 i 进入编辑模式，删除配置或在行首增加 `#` 进行注释。
5. 执行以下命令，重启 SSH 服务。

```
service sshd restart
```

重启 SSH 服务后，即可使用 SSH 登录。详情请参见 使用 SSH 登录 Linux 实例 。

## 排查 SSH 登录报错 No supported key exchange algorithms

### 现象描述

使用 SSH 登录 Linux 实例时，无法正常登录。客户端或服务端的 secure 日志中可能出现类似如下错误信息：

- Read from socket failed: Connection reset by peer.
- Connection closed by 192.X.X.1.
- sshd error: could not load host key.
- fatal: No supported key exchange algorithms [preauth].
- DSA host key for 192.X.X.1 has changed and you have requested strict checking.
- Host key verification failed.
- ssh_exchange_identification: read: Connection reset by peer.

### 可能原因

通常是由于 SSH 服务相关的密钥文件出现异常，导致 sshd 守护进程无法加载到正确的 SSH 主机密钥。常见异常原因如下：

- 相关密钥文件异常。例如，文件损坏、被删除或篡改等。
- 相关密钥文件权限配置异常，无法正确读取。

### 解决思路

参考处理步骤提供的以下处理项，进行配置检查及修改。

- 检查及修改文件权限
- 检查及修改文件有效性

### 处理步骤

#### 检查及修改文件权限

SSH 服务会对相关密钥文件的权限进行检查。例如，私钥文件默认权限为600，如果配置为777等其他权限，导致其他用户也具备读取或修改权限。则 SSH 服务会认为该配置存在安全风险，导致客户端连接失败。检查及修复步骤如下：

1. 使用 VNC 登录 Linux 实例。
2. 依次执行以下命令，恢复相关文件的默认权限。

```
cd /etc/ssh/
``` ```
chmod 600 ssh_host_*
``` ```
chmod 644 *.pub
```

3. 执行 `ll` 命令，查看文件权限。返回如下结果，表明文件权限正常。

```
total 156
-rw-------. 1 root root 125811 Nov 23 2013 moduli
-rw-r--r--. 1 root root 2047 Nov 23 2013 ssh_config
-rw------- 1 root root 3639 May 16 11:43 sshd_config
-rw------- 1 root root 668 May 20 23:31 ssh_host_dsa_key
-rw-r--r-- 1 root root 590 May 20 23:31 ssh_host_dsa_key.pub
-rw------- 1 root root 963 May 20 23:31 ssh_host_key
-rw-r--r-- 1 root root 627 May 20 23:31 ssh_host_key.pub
-rw------- 1 root root 1675 May 20 23:31 ssh_host_rsa_key
-rw-r--r-- 1 root root 382 May 20 23:31 ssh_host_rsa_key.pub
```

### 检查及修改文件有效性

1. SSH 服务在启动时会自动重建丢失的密钥文件。依次执行以下命令，确认存在 `ssh_host_*` 文件。

```
cd /etc/ssh/
```

```
ll
```

返回如下结果，表明存在 `ssh_host_*` 文件。

```
total 156
-rw-------. 1 root root 125811 Nov 23  2013 moduli
-rw-r--r--. 1 root root   2047 Nov 23  2013 ssh_config
-rw-------  1 root root   3639 May 16 11:43 sshd_config
-rw-------  1 root root    672 May 20 23:08 ssh_host_dsa_key
-rw-r--r--  1 root root    590 May 20 23:08 ssh_host_dsa_key.pub
-rw-------  1 root root    963 May 20 23:08 ssh_host_key
-rw-r--r--  1 root root    627 May 20 23:08 ssh_host_key.pub
-rw-------  1 root root   1675 May 20 23:08 ssh_host_rsa_key
-rw-r--r--  1 root root    382 May 20 23:08 ssh_host_rsa_key.pub
```

2. 执行以下命令，删除相关文件。

```
rm -rf ssh_host_*
```

Ubuntu 及 Debain 类操作系统，请执行以下命令，删除相关文件。

```
sudo rm -r /etc/ssh/ssh*key
```

3. 执行 `ll` 命令，确认文件是否成功删除。返回结果如下所示，则说明已成功删除。

```
total 132
-rw-------. 1 root root 125811 Nov 23  2013 moduli
-rw-r--r--. 1 root root   2047 Nov 23  2013 ssh_config
-rw-------  1 root root   3639 May 16 11:43 sshd_config
```

4. 执行以下命令，重启 SSH 服务，自动生成相关文件。

```
service sshd restart
```

Ubuntu 及 Debain 类操作系统，请执行以下命令，重启 SSH 服务。

```
sudo dpkg-reconfigure openssh-server
```

5. 执行 `ll` 命令，确认是否成功生成 `ssh_host_*` 文件。返回结果如下，则说明已成功生成。

```
total 156
-rw-------. 1 root root 125811 Nov 23  2013 moduli
-rw-r--r--. 1 root root   2047 Nov 23  2013 ssh_config
-rw-------  1 root root   3639 May 16 11:43 sshd_config
-rw-------  1 root root    668 May 20 23:16 ssh_host_dsa_key
-rw-r--r--  1 root root    590 May 20 23:16 ssh_host_dsa_key.pub
-rw-------  1 root root    963 May 20 23:16 ssh_host_key
-rw-r--r--  1 root root    627 May 20 23:16 ssh_host_key.pub
-rw-------  1 root root   1671 May 20 23:16 ssh_host_rsa_key
-rw-r--r--  1 root root    382 May 20 23:16 ssh_host_rsa_key.pub
```

使用 SSH 登录实例，详情请参见 使用 SSH 登录 Linux 实例 。

## 排查 SSH 服务启动时报错 must be owned by root and not group or word-writable

### 现象描述

Linux 实例启动 SSH 服务时，返回 **must be owned by root and not group or word-writable** 错误信息。

### 可能原因

通常是由于 SSH 服务相关权限，或属组异常。基于安全性考虑，SSH 服务对相关目录或文件的权限配置及属组等均有一定要求。

### 解决思路

参考处理步骤中提供的处理项，检查并修改错误配置。

- 检查及修复 /var/empty/sshd 目录配置
- 检查及修复 /etc/securetty 文件配置

### 处理步骤

> **说明：**
> 本步骤以 CentOS 7.6 操作系统环境为例，请您结合实际业务情况进行操作。

#### 检查及修复 /var/empty/sshd 目录配置

1. 使用 VNC 登录 Linux 实例 。
2. 执行以下命令，查看 `/var/empty/sshd` 目录权限配置。

```
ll -d /var/empty/sshd/
```

以下内容为默认权限配置。

```
drwx--x--x. 2 root root 4096 Aug  9  2019 /var/empty/sshd/
```

3. 对比实际返回结果与默认权限配置，若不相同，则请依次执行以下命令，恢复默认配置。

> **说明：**
> `/var/empty/sshd` 目录权限默认为711，默认为 root 属组的 root 用户。

```
chown -R root:root /var/empty/sshd
```

```
chmod -R 711 /var/empty/sshd
```

4. 执行以下命令，重启 SSH 服务。

```
systemctl restart sshd.service
```

### 检查及修复 /etc/securetty 文件配置

1. 执行如下命令，查看 `/etc/securetty` 文件权限配置。

```
ll /etc/securetty
```

以下内容为默认权限配置。

```
-rw-------. 1 root root 255 Aug  5  2020 /etc/securetty
```

2. 对比实际返回结果与默认权限配置，若不相同，则请依次执行以下命令，恢复默认配置。

> **说明：**
> `/etc/securetty` 文件权限默认为600，默认为 root 属组的 root 用户。

```
chown root:root /etc/securetty
```

```
chmod 600 /etc/securetty
```

3. 执行以下命令，重启 SSH 服务。

```
systemctl restart sshd.service
```

使用 SSH 登录实例，详情请参见 使用 SSH 登录 Linux 实例 。

## 排查 SSH 登录时报错 Host key verification failed

### 现象描述

使用 SSH 登录 Linux 实例时，无法正常登录，且出现以下报错信息：

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
```

```
ae:6e:68:4c:97:a6:91:81:11:38:8d:64:ff:92:13:50.
Please contact your system administrator.
Add correct host key in /root/.ssh/known_hosts to get rid of this message.
Offending key in /root/.ssh/known_hosts:70
RSA host key for x.x.x.x has changed and you have requested strict checking.
Host key verification failed.
```

若客户端为 Windows 操作系统，则通常 SSH 客户端在连接时出现以下报错信息：

```
x.x.x.x （端口：xx）的主机密钥与本地主机密钥数据库中保存的不一致。主机密钥已更改或有人试图监听此连接。若无法确定，建议取消此连接。
```

### 可能原因

Linux 实例重装系统操作后，账户信息等变更使 SSH 公钥变更，造成客户端保存的公钥指纹与服务器端不一致，导致 SSH 认证失败拒绝登录。

### 解决思路

对应客户端实际使用操作系统，参考处理步骤中提供的步骤进行操作。

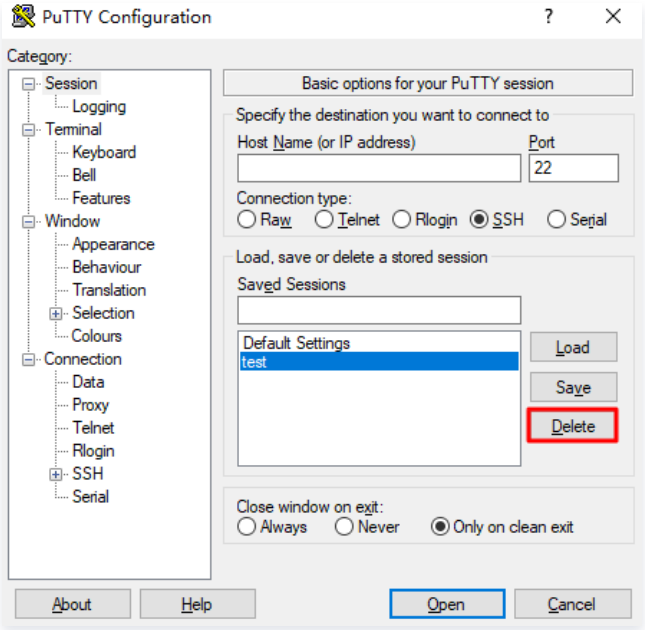
- Windows 客户端
- Linux 客户端

### 处理步骤

## Windows 客户端

> **说明：**
> 本文 SSH 客户端以 PuTTY 为例，请您结合实际情况进行操作。

1. 启动 PuTTY。
2. 在登录页面，选择会话后单击 **Delete** 进行删除。如下图所示：




3. 参见 使用远程登录软件登录 Linux 实例，重新使用用户名及密码登录实例，确认保存新的公钥指纹后，即可成功登录。

## Linux 客户端

> **说明：**
> 本文 Linux 实例操作系统以 CentOS 6.5 为例，不同版本操作系统可能存在区别，请您结合实际情况操作。

1. 使用 VNC 登录 Linux 实例。

2. 执行如下命令，进入对应账号的 `known_hosts` 文件。

```
vi ~/.ssh/known_hosts
```

3. 按 i 进入编辑模式，删除 Linux 实例 IP 对应的条目。类似如下信息：

```
1.14.xxx.xx
skowcenw96a/pxka32sa....
dsaprgpck2wa22mvi332ueddw...
```

4. 按 Esc 输入 :wq 保存修改并退出。
5. 参见 使用 SSH 登录 Linux 实例，重新连接 Linux 实例，确认保存新的公钥指纹后，即可成功登录。

## 排查 SSH 登录报错 pam_listfile(sshd:auth): Refused user root for service sshd

### 现象描述

使用 SSH 登录 Linux 实例时，即使输入正确密码，仍无法登录实例。该问题出现时，通过控制台或 SSH 两种登录方式可能均登录失败，或仅其中一种可登录成功。secure 日志出现类似如下错误信息：

- sshd[1199]: pam_listfile(sshd:auth): Refused user root for service sshd
- sshd[1199]: Failed password for root from 192.X.X.1 port 22 ssh2
- sshd[1204]: Connection closed by 192.X.X.2

### 可能原因

pam 模块（pam_listfile.so）相关访问控制策略导致用户登录失败。

### pam 模块介绍

pam（Pluggable Authentication Modules）是由 Sun 提出的一种认证机制。通过提供一些动态链接库和一套统一的 API，将系统提供的服务和该服务的认证方式分开。使系统管理员可以灵活地根据需求给不同的服务配置不同的认证方式，而无需更改服务程序，同时也便于向系统中添加新的认证手段。
每个启用了 pam 模块的应用程序，在 `/etc/pam.d` 目录中都有对应的同名配置文件。例如，login 命令的配置文件是 `/etc/pam.d/login`，可以在相应配置文件中配置具体的策略。关于更多 pam_listfile 信息，请查阅 linux-pam.org 官方文档。

### 解决思路

参见 处理步骤 检查并修复 pam 模块。

### 处理步骤

> **说明：**
> 本文处理步骤以 CentOS 6.5 操作系统为例，不同操作系统版本有一定区别，请结合实际情况进行操作。

1. 使用 VNC 登录 Linux 实例。
2. 使用 `cat` 命令，查看对应 pam 配置文件。说明如下：

| 文件 | 功能说明 |
| --- | --- |
| /etc/pam.d/login | 控制台（管理终端）对应配置文件 |
| /etc/pam.d/sshd | SSH 登录对应配置文件 |
| /etc/pam.d/system-auth | 系统全局配置文件 |

3. 查看是否存在类似如下配置。

```
auth required pam_listfile.so item=user sense=allow file=/etc/ssh/whitelist onerr=fail
```

说明如下：
- **item**：设置访问控制的对象类型。可选值为 tty、user、rhost、ruser、group 和 shell。

- sense：在配置文件中找到符合条件项目的控制方式。可选值为 allow 和 deny。allow 代表白名单方式，deny 代表黑名单方式。
- file：用于指定配置文件的全路径名称。
- onerr：定义出现错误时的缺省返回值。例如，无法打开配置文件的错误。

4. 使用 VIM 编辑器，删除策略配置，或在行首增加 `#` 进行注释。

> **说明：**
> 相关策略配置可一定程度提高服务器的安全性，请您结合实际情况进行修改，建议修改前进行备份。

```
# auth required pam_listfile.so item=user sense=allow file=/etc/ssh/whitelist onerr=fail
```

5. 使用 SSH 登录实例，详情请参见 使用 SSH 登录 Linux 实例 。

## 排查 SSH 登录时报错 requirement "uid >= 1000" not met by user "root"

### 现象描述

使用 SSH 登录 Linux 实例时，输入正确的用户名及密码也无法登录成功。该问题出现时，通过控制台或 SSH 两种登录方式可能均登录失败，或仅其中一种可登录成功。secure 日志出现类似如下错误信息：

```
pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root".
```

### 可能原因

pam 模块的策略配置禁止了 UID 小于1000的用户进行登录。

### 解决方案

参见 处理步骤 检查并修复 pam 模块。

### 处理步骤

> **说明：**
> 本文处理步骤以 CentOS 6.5 操作系统为例，不同操作系统版本有一定区别，请结合实际情况进行操作。

1. 使用 VNC 登录 Linux 实例 。
2. 使用 `cat` 命令，查看对应 pam 配置文件。说明如下：

| 文件 | 功能说明 |
| --- | --- |
| /etc/pam.d/login | 控制台（管理终端）对应配置文件 |
| /etc/pam.d/sshd | SSH 登录对应配置文件 |
| /etc/pam.d/system-auth | 系统全局配置文件 |

3. 查看是否存在类似如下配置。

```
auth required pam_succeed_if.so uid >= 1000
```

4. 使用 VIM 编辑器，修改、删除策略配置或在行首增加 `#` 进行注释。请结合实际情况进行修改，建议修改前进行备份。

```
auth        required      pam_succeed_if.so uid <= 1000    # 修改策略
# auth        required      pam_succeed_if.so uid >= 1000  # 注释相关配置
```

5. 使用 SSH 登录实例，详情请参见 使用 SSH 登录 Linux 实例 。

## 排查 SSH 登录时报错 Maximum amount of failed attempts was reached

### 现象描述

使用 SSH 登录 Linux 实例时，出现 “Maximum amount of failed attempts was reached” 报错信息。

### 可能原因

连续多次输入错误密码，触发系统 pam 认证模块策略限制，导致用户被锁定。

> **说明：**
> 更多 pam 安全认证相关信息，请参考官网文档 pam_tally2 – login counter (tallying) module 。

### 解决方案

参考处理步骤提供的处理项，结合实际情况进行操作：

- root 用户未被锁定
- root 用户被锁定

### 处理步骤

> **说明：**
> 本文处理步骤以 CentOS 7.6 及 CentOS 6.5 操作系统为例，不同操作系统版本有一定区别，请结合实际情况进行操作。

#### root 用户未被锁定

1. 使用 root 用户登录实例，详情请参见 使用 VNC 登录 Linux 实例 。
2. 执行以下命令，查看系统全局 pam 配置文件。

```
cat /etc/pam.d/system-auth
```

3. 执行以下命令，查看本地终端对应的 pam 配置文件。

```
cat /etc/pam.d/login
```

4. 执行以下命令，查看 SSH 服务对应的 pam 配置文件。

```
cat /etc/pam.d/sshd
```

5. 使用 VIM 编辑器编辑以上文件相关内容，修改、删除对应配置或在行首增加 `#` 注释配置。本文以注释配置为例，修改完成后，相关配置如下所示：

```
#auth required pam_tally2.so deny=3 unlock_time=5
#auth required pam_tally.so onerr=fail no_magic_root
#auth requeired pam_tally2.so deny=5 lock_time=30 unlock_time=10 even_deny_root root_unlock_time=10
```

说明如下：

- 此处使用 `pam_tally2` 模块，如果不支持则可以使用 `pam_tally` 模块。不同的 pam 版本，设置可能有所不同，具体使用方法请参照相关模块的使用规则。
- `pam_tally2` 与 `pam_tally` 模块都可以用于账户锁定策略控制。两者的区别是前者增加了自动解锁时间的功能。
- `even_deny_root` 指限制 root 用户。
- `deny` 指设置普通用户和 root 用户连续错误登录的最大次数。超过最大次数，则锁定该用户。
- `unlock_time` 指设定普通用户锁定后，指定时间后解锁，单位为秒。
- `root_unlock_time` 指设定 root 用户锁定后，指定时间后解锁，单位为秒。

6. 使用 SSH 登录实例，详情请参见 使用 SSH 登录 Linux 实例 。

#### root 用户被锁定

1. 使用单用户模式登录实例，详情请参见 设置 Linux 云服务器进入单用户模式 。
2. 在单用户模式下，依次执行以下命令，手动解锁 root 用户。

```
pam_tally2 -u root #查看root用户登录密码连续输入错误次数
```
```
pam_tally2 -u root -r #清除root用户密码连续输入错误次数
```
```
authconfig --disableldap --update #更新PAM安全认证记录
```

3. 重启实例。
4. 参见 root 用户未被锁定 步骤，在对应的 pam 配置文件进行注释、修改或更新即可。
5. 使用 SSH 登录实例，详情请参见 使用 SSH 登录 Linux 实例 。

## 排查 SSH 登录时报错 login: Module is unknown

### 现象描述

使用 SSH 登录 Linux 实例时，无法登录成功，且 secure 日志中出现类似如下报错信息：

```
login: Module is unknown.
login: PAM unable to dlopen(/lib/security/pam_limits.so): /lib/security/pam_limits.so: cannot open shared
object file: No such file or directory.
```

### 可能原因

每个启用了 pam 模块的应用程序，在 `/etc/pam.d` 目录中都有对应的同名配置文件。例如，login 命令的配置文件是 `/etc/pam.d/login` ，可以在相应配置文件中配置具体的策略。如下表所示：

| 文件 | 功能说明 |
| --- | --- |
| /etc/pam.d/login | 控制台（管理终端）对应配置文件 |
| /etc/pam.d/sshd | SSH 登录对应配置文件 |
| /etc/pam.d/system-auth | 系统全局配置文件 |

远程连接登录时，某些启用了 pam 的应用程序加载模块失败，导致配置了相应策略的登录方式交互失败。

### 解决思路

参见 处理步骤 ，检查并修复配置文件。

### 处理步骤

> **说明：**
> 本文主要查看 `/etc/pam.d/sshd` 和 `/etc/pam.d/system-auth` 文件，若 `/etc/pam.d/login` 出现问题，请通过 在线支持 联系我们寻求帮助。

1. 使用 VNC 登录 Linux 实例 。
2. 执行以下命令，查看 pam 配置文件。

```
cat [对应 pam 配置文件的绝对路径]
```

查看配置文件是否包含类似如下配置信息，该配置信息模块文件路径为 `/lib/security/pam_limits.so` 。

```
session    required     pam_limits.so
```

3. 执行以下命令，确认 `/lib/security/pam_limits.so` 路径是否错误。

```
ll /lib/security/pam_limits.so
```

- 是，则使用 VIM 编辑器编辑 pam 配置文件，修复 `pam_limits.so` 模块路径。64位系统的 Linux 实例中，正确路径应该为 `/lib64/security` 。修改后配置信息应如下所示：

```
session     required     /lib64/security/pam_limits.so
```

- 否，则请通过 在线支持 寻求帮助。

4. 使用 SSH 登录实例，详情请参见 使用 SSH 登录 Linux 实例 。

## 排查病毒引起 SSH 服务运行异常报错 fatal: mm_request_send: write: Broken pipe

### 现象描述

病毒引发 SSH 服务运行异常，系统提示 “fatal: mm_request_send: write: Broken pipe” 报错信息。

### 可能原因

可能是由于 udev-fall 等病毒影响了 SSH 服务的正常运行。

### 解决思路

参考处理步骤中提供的处理项，结合实际情况处理病毒问题。

- 临时处理方法
- 可靠处理方法

### 处理步骤

### 临时处理方法

本文以 udev-fall 病毒为例，您可通过以下步骤，临时恢复 SSH 服务的正常运行。

1. 使用 VNC 登录 Linux 实例 。
2. 执行以下命令，查看 udev-fall 病毒进程信息，并记录该进程 ID。

```
ps aux | grep udev-fall
```

3. 执行以下命令，根据获取的 udev-fall 病毒进程 ID，结束 udev-fall 病毒进程。

```
kill -9 [病毒进程 ID]
```

4. 执行以下命令，取消 udev-fall 病毒程序的自动运行设置。

```
chkconfig udev-fall off
```

5. 执行以下命令，删除所有 udev-fall 病毒程序相关指令和启动配置。

```
for i in ` find / -name "udev-fall"`;
do echo '' > $i && rm -rf $i;
done
```

6. 执行以下命令，重启 SSH 服务。

```
systemctl restart sshd.service
```

### 可靠处理方法

由于无法明确病毒或者恶意入侵者是否对系统做过其他篡改，或隐藏了其他病毒文件。为了服务器的长期稳定运行，建议通过回滚实例系统盘历史快照的方式，来将服务器恢复到正常状态。详情请参见 从快照回滚数据 。

> **注意：**
> - 快照回滚会导致快照创建后的数据丢失，请谨慎操作。

- 建议按快照创建时间从近到远的顺序逐一尝试回滚，直至 SSH 服务正常运行。若回滚后仍无法正常运行 SSH 服务，则说明该时间点的系统已经出现异常。

## 排查 SSH 服务启动时报错 main process exited, code=exited

### 现象描述

在 Linux 实例中，使用 service 或 systemctl 命令启动 SSH 服务时，命令行没有返回报错信息，但服务没有正常运行。secure 日志中发现类似如下错误信息：

```
sshd.service: main process exited, code=exited, status=203/EXEC.
init: ssh main process (1843) terminated with status 255.
```

### 可能原因

通常是 PATH 环境变量配置异常，或 SSH 软件包相关文件被移除导致。

### 解决方案

参见 处理步骤，检查并修复 PATH 环境变量，或重新安装 SSH 软件包。

### 处理步骤

> **说明：**
> 本文处理步骤以 CentOS 6.5 操作系统为例，不同操作系统版本有一定区别，请结合实际情况进行操作。

1. 使用 VNC 登录 Linux 实例。
2. 执行以下命令，检查环境变量配置。

   ```
   echo $PATH
   ```

3. 对比实际返回 PATH 环境变量与默认值。PATH 环境变量默认值：

   ```
   /usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin
   ```

   若实际返回 PATH 环境变量若与默认值不相同，则需执行以下命令，重置 PATH 环境变量。

   ```
   export PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin
   ```

4. 执行如下命令，查找并确认 sshd 程序路径。

   ```
   find / -name sshd
   ```

   - 返回结果如下，则说明 sshd 程序文件已存在。

     ```
     /usr/sbin/sshd
     ```

   - 若对应文件不存在，则请重新安装 SSH 软件包。
5. 执行以下命令，重启 SSH 服务。

   ```
   service sshd restart
   ```

   使用 SSH 登录实例，详情请参见 使用 SSH 登录 Linux 实例。

## 排查 SSH 登录时报错 pam_limits(sshd:session)：could not sent limit for ‘nofile’

### 现象描述

使用 SSH 登录 Linux 实例后，返回如下错误信息：

```
-bash: fork: retry: Resource temporarily unavailable.
pam_limits(sshd:session): could not sent limit for 'nofile':operaton not permitted.
Permission denied.
```

### 可能原因

通常是由于当前 Shell 进程或文件开启的数量，超出服务器 Ulimit 系统环境限制导致。

### 解决思路

参见 处理步骤，结合实际使用的操作系统版本，修改 limits.conf 文件永久变更 Ulimit 系统环境限制。

### 处理步骤

> **说明：**
> - CentOS 6系统版本及之后发行版本中，增加了 `X-nproc.conf` 文件管理 Ulimit 系统环境限制，操作步骤以 CentOS 6进行区分。`X-nproc.conf` 文件在不同系统版本中前缀数字不同，在 CentOS 6中为 `90-nproc.conf`，在 CentOS 7中为 `20-nproc.conf`，请以实际情况环境为准。
> - 本文以 CentOS 7.6 及 CentOS 5 操作系统环境为例，请您结合实际业务情况进行操作。

#### CentOS 6之前版本

1. 使用 VNC 登录 Linux 实例。
2. 执行以下命令，查看系统当前 Ulimit 系统资源限制信息。

   ```
   cat /etc/security/limits.conf
   ```

   说明如下：
   - **<domain>**：需要限制的系统用户，可以用 * 代替所有用户。
   - **<type>**：soft、hard 和 – 三种参数。
     - soft 指当前系统已经生效的 <value> 值。
     - hard 指系统中设定的最大 <value> 值。
     - soft 的限制不能比 hard 限制高，– 表示同时设置 soft 和 hard 的值。
   - **<item>**：需要限制的使用资源类型。
     - core 指限制内核文件的大小。
     - rss 指最大持久设置大小。
     - nofile 指打开文件的最大数目。
     - noproc 指进程的最大数目。
3. 默认未设置系统资源限制，请根据实际情况进行判断，如果系统开启并配置系统资源限制，则需通过编辑 `limits.conf` 文件，选择注释、修改或删除 `noproc` 或 `nofile` 参数限制的资源类型代码操作。
   修改前建议执行以下命令，备份 `limits.conf` 文件。

   ```
   cp -af /etc/security/limits.conf /root/limits.conf_bak
   ```

4. 修改完成后，重启实例即可。

#### CentOS 6之后版本

1. 使用 VNC 登录 Linux 实例。
2. 执行以下命令，查看系统当前 Ulimit 系统资源限制信息。

```
cat /etc/security/limits.d/20-nproc.conf
```

返回结果如下图所示，表示已开启系统资源限制，并允许 root 用户以外的所有用户最大连接进程数为4096。

```
[root@VM-5-21-centos ~]# cat /etc/security/limits.d/20-nproc.conf
# Default limit for number of user's processes to prevent
# accidental fork bombs.
# See rhbz #432903 for reasoning.

*          soft    nproc     4096
root       soft    nproc     unlimited
```

3. 参见 CentOS 6之前版本 步骤，修改 `/etc/security/limits.d/20-nproc.conf` 文件，建议修改前进行文件备份。
4. 修改完成后，重启实例即可。

## 排查 SSH 登录报错 pam_unix(sshdsession) session closed for user

### 现象描述

使用 SSH 登录 Linux 实例时，输入正确的用户名及密码无法登录成功。直接返回或在 secure 日志出现类似如下错误信息：

- This account is currently not available.
- Connection to 127.0.0.1 closed.
- Received disconnect from 127.0.0.1: 11: disconnected by user.
- pam_unix(sshd:session): session closed for user test.

### 可能原因

通常由于对应用户的默认 Shell 被修改导致。

### 解决思路

参见 处理步骤，检查并修复对应用户的默认 Shell 配置。

### 处理步骤

1. 使用 VNC 登录 Linux 实例。
2. 执行以下命令，查看 test 用户的默认 Shell。

```
cat /etc/passwd | grep test
```

系统返回类似如下信息，表示 test 用户的 Shell 被修改成 nologin。

```
test:x:1000:1000::/home/test:/sbin/nologin
```

3. 执行以下命令，使用 VIM 编辑器编辑 `/etc/passwd` 文件。建议在修改前进行文件备份。

```
vim /etc/passwd
```

4. 按 **i** 进入编辑模式，将 `/sbin/nologin` 修改为 `/bin/bash` 。
5. 按 **Esc** 输入 **:wq**，保存编辑并退出。
6. 使用 SSH 登录实例，详情请参见 使用 SSH 登录 Linux 实例 。

若您的问题仍未解决，请通过 在线支持 联系我们寻求帮助。

# Linux 实例：修改密码后无法使用修改后的密码登录

最近更新时间：2024-12-11 16:28:02

## 现象描述

在腾讯云的 云服务器控制台 修改 root 密码后，无法使用新密码登录 CVM 服务器。

## 可能原因

可能是该 CVM 实例账号对应的 `/etc/shadow` 或 `/etc/passwd` 文件属性配置错误。例如：配置了 `i` 、 `a` 属性（表示不能删除、修改数据），导致修改账号密码不生效。此时，只能使用修改前的密码登录。

> **说明：**
> Linux 系统中的 `/etc/passwd` 文件用于存放账号信息， `/etc/shadow` 文件用于存放密码信息。当 `/etc/shadow` 或 `/etc/passwd` 文件属性配置错误，可能导致实例的部分功能无法正常工作。例如：修改 root 账号的密码不生效。

`/etc/shadow` 或 `/etc/passwd` 文件常见属性说明如下：

| 属性 | 说明 |
| --- | --- |
| i | • 对文件设置 `i` 属性，不允许对文件进行删除、重命名，也不能添加和修改数据。<br>• 对目录设置 `i` 属性，只能修改目录下文件中的数据，但不允许新建和删除文件。 |
| a | • 对文件设置 `a` 属性，只能在文件中新增数据，但是不能删除和修改数据。<br>• 对目录设置 `a` 属性，只能在目录中新增和修改文件，但是不允许删除文件。 |
| u | • 对文件或目录设置 `u` 属性，在删除时，其内容会被保存，以保证后期能够恢复，<br>• 一般用来防止意外删除文件或目录。 |
| s | 对文件或目录设置 `s` 属性，在删除文件或目录时，会被彻底删除，不可恢复。 |
| e | Linux 中绝大多数的文件都默认拥有 `e` 属性，表示该文件是使用 `ext` 文件系统进行存储的。 |

## 解决方案

您可以参考以下步骤，根据实际需要修改 `/etc/shadow` 或 `/etc/passwd` 文件属性，来解决修改 root 账号的密码不生效的问题。

> **说明：**
> 只有 root 用户才可以修改 `/etc/passwd` 文件和 `/etc/shadow` 文件。

1. 使用 root 用户修改前的密码通过终端连接（SSH）或免密连接（TAT）方式登录云服务器。

   > **注意：**
   > `/etc/shadow` 或 `/etc/passwd` 文件属性错误导致修改密码不生效，但使用修改前的密码仍然可以正常登录。

   如果忘记密码，可以通过免密连接（TAT）方式登录服务器，详细操作请参见 使用标准登录方式登录 Linux 实例（推荐）。
2. 执行 `lsattr [文件类型]` 命令，查看并确认 `/etc/shadow` 或 `/etc/passwd` 文件属性是否有误。

   以本文描述的故障为例，若文件存在 `i` 或 `a` 属性（禁止修改数据），则有误。例如：

   2.1 执行如下命令查看 `/etc/passwd` 文件属性。

   ```
   lsattr /etc/passwd
   ```

   2.2 发现 `/etc/passwd` 文件具有 `i` 属性（禁止修改数据），导致修改密码不生效，需要移除文件 `i` 属性。

   ```
   [root@[redacted]~]$lsattr /etc/passwd
   ----i--------e-- /etc/passwd
   ```

3. 执行 `chattr` 命令修改 `/etc/shadow` 或 `/etc/passwd` 文件属性。

```
chattr [+-=] [属性] 文件或目录名
```

> **说明：**
> - +：为文件或目录添加属性。
> - -：移除文件或目录已有的某些属性。
> - =：为文件或目录设定一些属性。

针对上述修改密码不生效无法登录实例问题，可选择移除 `/etc/passwd` 的 `i` 属性来解决，命令示例如下：

```
chattr -i /etc/passwd
```

```
[root@[illegible]]$chattr -i /etc/passwd
[root@[illegible]]$lsattr /etc/passwd
----------e-- /etc/passwd
[root@[illegible]]$
```

4. 重新为云服务器 重置密码 。
5. 使用重置后的密码登录实例，如果可以正常登录，说明问题已解决。

# Linux 实例：CPU 或内存占用率高导致登录卡顿

最近更新时间：2024-07-30 11:17:21

## 现象描述

CPU 或内存使用率过高，引起服务响应速度变慢、服务器登录卡顿等问题。

## 定位工具

**Top**：Linux 系统下常用的监控工具，用于实时获取进程级别的 CPU 或内存使用情况。以下图 top 命令的输出信息为例。

```
top - 22:16:25 up  6:18,  1 user,  load average: 0.00, 0.01, 0.05
Tasks:  68 total,   1 running,  67 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.3 sy,  0.0 ni, 99.7 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  1016516 total,   605016 free,    77224 used,   334276 buff/cache
KiB Swap:        0 total,        0 free,        0 used.   778708 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
  257 root      20   0       0      0      0 S  0.3  0.0   0:00.73 jbd2/vda1-8
  984 root      20   0  569592   5068   2568 S  0.3  0.5   0:16.51 YDService
 1253 root      20   0  534620  12288   2104 S  0.3  1.2   0:34.21 barad_agent
    1 root      20   0   43104   3512   2404 S  0.0  0.3   0:01.87 systemd
    2 root      20   0       0      0      0 S  0.0  0.0   0:00.00 kthreadd
    3 root      20   0       0      0      0 S  0.0  0.0   0:00.33 ksoftirqd/0
    4 root      20   0       0      0      0 S  0.0  0.0   0:00.00 kworker/0:0
    5 root       0 -20       0      0      0 S  0.0  0.0   0:00.00 kworker/0:0H
    7 root      rt   0       0      0      0 S  0.0  0.0   0:00.00 migration/0
    8 root      20   0       0      0      0 S  0.0  0.0   0:00.00 rcu_bh
    9 root      20   0       0      0      0 S  0.0  0.0   0:01.20 rcu_sched
   10 root      rt   0       0      0      0 S  0.0  0.0   0:00.05 watchdog/0
```

Top 命令的输出信息主要分为两部分，上半部分显示 CPU 和内存资源的总体使用情况：

- 第一行：系统当前时间，当前登录用户个数以及系统负载。
- 第二行：系统总进程数、运行中进程数、睡眠、暂停和僵尸进程数量。
- 第三行：CPU 当前使用情况。
- 第四行：内存当前使用情况。
- 第五行：Swap 空间当前使用情况。

下半部分以进程为维度显示资源的占用情况：

- PID：进程 ID。
- USER：进程所有者。
- PR：进程优先级 。
- NI：NICE 值，NICE 值越小，优先级越高。
- VIRT：使用的虚拟内存大小，单位 KB。
- RES：使用的内存大小，单位 KB。
- SHR：使用的共享内存的大小，单位 KB。
- S：进程状态。
- %CPU：更新时间间隔内进程所使用的 CPU 的百分比。
- %MEM：更新时间间隔内进程所使用的内存的百分比。
- TIME+：进程使用的 CPU 时间，精确到 0.01s。
- COMMAND：进程名称。

## 可能原因

引起 CPU 或内存使用率过高的原因可能由硬件因素、系统进程、业务进程或者木马病毒等因素导致。您可以使用 腾讯云可观测平台，创建 CPU 或内存使用率阈值告警，当 CPU 或内存使用率超过阈值时，将及时通知到您。

## 故障处理

### 步骤一：登录云服务器

根据实际需求，选择不同的登录方式登录云服务器：

- 通过第三方软件远程登录 Linux 云服务器。

> **注意：**
> Linux 云服务器处于 CPU 高负荷状态时，可能出现无法登录状态。

- 使用 VNC 登录 Linux 实例。

> **注意：**
> Linux 云服务器处于 CPU 高负荷状态时，控制台可以正常登录。

### 步骤二：检查进程的占用情况

执行以下命令，查看系统负载，并根据 `%CPU` 列与 `%MEM` 列，确定占用较多资源的进程。

```
top
```

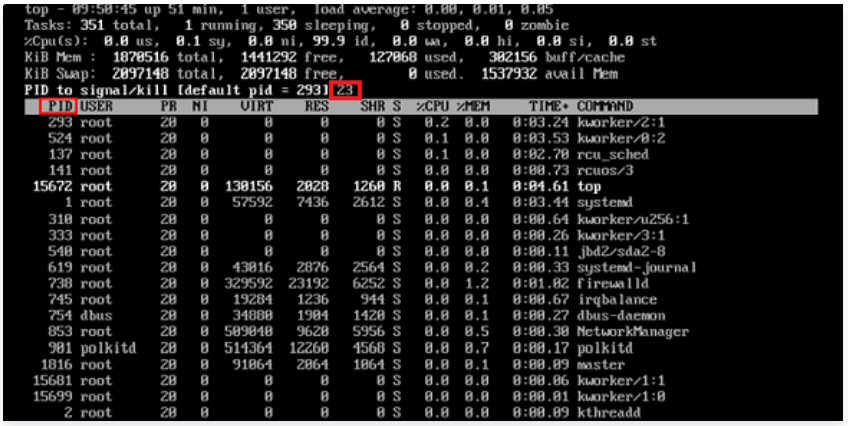
### 步骤三：检查并分析占用资源的进程

根据任务管理器中的进程，分析与排查问题，以采取对应解决方案。

- 如果是业务进程占用了大量 CPU 或内存资源，建议分析业务程序是否有优化空间，进行优化或者 升级服务器配置 。
- 如果是异常进程占用了大量 CPU 或内存资源，则实例可能中毒，您可以自行终止进程或者使用安全软件进行查杀，必要时考虑备份数据，重装系统。
- 如果是腾讯云组件进程占用了大量 CPU 或内存资源，请通过 在线支持 联系我们进行进一步定位处理。
  常见的腾讯云组件有：
  - sap00x：安全组件进程
  - Barad_agent：监控组件进程
  - secu-tcs-agent：安全组件进程

### 步骤四：终止占用资源的进程

1. 根据分析的占用资源的进程情况，记录需要终止的进程 PID。
2. 输入 `k` 。
3. 输入需要终止进程的 PID ，按 **Enter**。如下图所示：
   此处以终止 PID 为23的进程为例。




> **注意：**
> 若按 **Enter** 后出现 `kill PID 23 with signal [15]:` ，则继续按 **Enter** 保持默认设定即可。

4. 操作成功后，界面会出现 `Send pid 23 signal [15/sigterm]` 的提示信息，按 **Enter** 确认即可。

## 相关参考

## CPU 空闲但高负载情况处理

### 问题描述

Load average 是 CPU 负载的评估，其值越高，说明其任务队列越长，处于等待执行的任务越多。
通过 top 观察，类似如下图所示，CPU 很空闲，但是 load average 却非常高。

```
top - 19:46:57 up 27 days,  5:33,  1 user,  load average: 23, 22, 23
Tasks:  94 total,   1 running,  93 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.3 us,  0.0 sy,  0.0 ni, 99.7 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem:   1016656 total,   950428 used,    66228 free,   170148 buffers
KiB Swap:        0 total,        0 used,        0 free.   452740 cached Mem
```

### 解决措施

执行以下命令，查看进程状态，并检查是否存在 D 状态进程。如下图所示：

```
ps -axjf
```

```
    1   516   516   516 ?           -1 Ss       0   0:00 /sbin/iprinit --daemon
    1   569   569   569 ?           -1 Ss       0   0:00 /sbin/iprdump --daemon
    1   863   863   863 ?           -1 D+      38   0:16 /usr/sbin/ntpd -u ntp:ntp -g
    1   874   874   874 ?           -1 Ss       0   0:01 /usr/sbin/sshd -D
  874  8823  8823  8823 ?           -1 Ss       0   0:03  \_ sshd: root@pts/0
 8823  8825  8825  8825 pts/0     9006 Ss       0   0:00      \_ -bash
 8825  9006  9006  8825 pts/0     9006 D+       0   0:00          \_ ps -axjf
```

> **说明：**
> D 状态指不可中断的睡眠状态。该状态进程无法被关闭，也无法自行退出。

若出现较多 D 状态进程，可通过恢复该进程依赖资源或重启系统进行解决。

## Kswapd0 进程占用 CPU 较高情况处理

### 问题描述

Linux 系统通过分页机制管理内存的同时，将磁盘的一部分划出来作为虚拟内存。而 kswapd0 是 Linux 系统虚拟内存管理中负责换页的进程。当系统内存不足时，kswapd0 会频繁的进行换页操作。换页操作非常消耗 CPU 资源，导致该进程持续占用高 CPU 资源。

### 解决措施

1. 执行以下命令，找到 kswapd0 进程。

   ```
   top
   ```

2. 观察 kswapd0 进程状态。
   若持续处于非睡眠状态，且运行时间较长并持续占用较高 CPU 资源，请执行 步骤3，查看内存的占用情况。
3. 执行 `vmstat` 、 `free` 、 `ps` 等指令，查询系统内进程的内存占用情况。
   根据内存占用情况，重启系统或终止不需要且安全的进程。如果 si，so 的值也比较高，则表示系统存在频繁的换页操作，当前系统的物理内存已经不能满足您的需要，请考虑升级系统内存。

# Linux 实例：端口问题导致无法登录

最近更新时间：2025-06-03 11:17:42

本文档为您介绍云服务器因端口问题导致无法远程登录的排查方法和解决方案。

> **说明**
> 以下操作以 CentOS 7.8 系统的云服务器为例。

## 检查工具

您可以通过腾讯云提供的以下工具判断无法登录是否与端口和安全组设置相关：

- 自助诊断
- 实例端口验通工具

如果检测为安全组设置的问题，您可以通过 实例端口验通工具 中的**一键放通**功能放通相关端口并再次尝试登录。如果放通端口后还是登录失败，可参考以下内容逐步排查原因。

## 可能原因

| 可能原因 | 处理措施 |
| --- | --- |
| 本地和服务器间的网络未连通 | 检查本地和服务器间的网络确保连通 |
| 实例远程端口未处于连通状态 | 检查实例远程端口确保已连通 |
| sshd 端口未被监听或服务未启动 | 检查 sshd 端口是否被监听或服务是否启动 |

## 故障处理

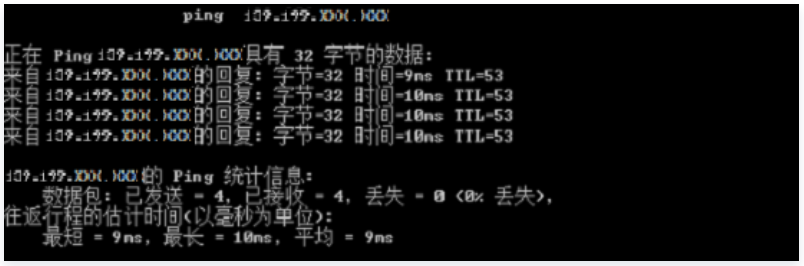
### 检查本地和服务器间的网络确保连通

您可以通过本地 Ping 命令，测试网络的连通性。同时使用不同网络环境中（不同网段或不同运营商）的电脑测试，判断是本地网络问题还是服务器端问题。

1. 根据本地计算机的操作系统不同，选择命令行工具的打开方式。
   - **Windows 系统**：单击**开始** > **运行**，输入 cmd，弹出命令行对话框。
   - **MacOS 系统**：打开 Terminal 工具。
2. 执行以下命令，测试网络连接。

```
ping + 云服务器实例公网 IP 地址
```

   可参见 获取公网 IP 地址 获取云服务器实例公网 IP。例如，执行 `ping 139.199.XXX.XXX` 。
   - 如果网络正常，则返回类似以下结果。




   - 如果网络异常，则出现**请求超时**提示，请参见 实例 IP 地址 Ping 不通 进行排查。

### 检查实例远程端口确保已连通

通过腾讯云 VNC 登录进入服务器内部进行检查。

1. 使用 VNC 方式登录云服务器，详情请参见 使用 VNC 登录 Linux 实例 。
2. 执行以下命令，并按 **Enter**。测试远程端口开启情况，判断端口是否可以访问。

```
telnet + 云服务器实例公网 IP 地址 + 端口号
```

> **注意：** 若是服务器没有 telnet 命令，可以执行 `sudo yum install -y telnet` 命令安装。

例如，执行 `telnet 119.XX.XXX.67 22` 命令，测试22端口的连通性。

- 正常情况：返回如下图所示信息，22端口可访问。

```
[root@VM-8-25-centos ~]# telnet 119.[illegible].67 22
Trying 119.[illegible].67...
Connected to 119.[illegible].67.
Escape character is '^]'.
SSH-2.0-OpenSSH_7.4
```

- 异常情况：返回类似如下图所示信息，说明22端口不可访问。请检查问题网络相关部分，例如实例的防火墙或安全组是否放通22端口。

```
[root@VM-8-25-centos ~]# telnet 119.[illegible].67 22
Trying 119.[illegible].67...
telnet: connect to address 119.[illegible].67: Connection timed out
```

## 检查 sshd 端口是否被监听或服务是否启动

当 使用 SSH 登录 Linux 实例 时，提示无法连接或者连接失败。可能是由于 sshd 端口未被监听或 sshd 服务未启动引起。请参见 无法通过 SSH 方式登录 Linux 实例 进行排查。

# Linux 实例：VNC 登录报错 Module is unknown

最近更新时间：2024-08-22 10:41:51

## 现象描述

使用 VNC 登录云服务器时，即使输入正确密码也无法成功登录，并提示 “Module is unknown” 错误。如下图所示：

```
[redacted] login: root
Password:
Last failed login: Mon Oct 26 10:24:25 CST 2020 from [redacted] on ssh:notty
There were 46 failed login attempts since the last successful login.

Module is unknown
```

## 可能原因

使用 VNC 登录会调用 `/etc/pam.d/login` pam 模块进行校验，而该模块会将 `/etc/pam.d/system-auth` 模块引入进行校验。`/etc/pam.d/login` 配置文件的内容，如下图所示：

```
#%PAM-1.0
auth [user_unknown=ignore success=ok ignore=ignore default=bad] pam_securetty.so
auth       substack     system-auth
auth       include      postlogin
account    required     pam_nologin.so
account    include      system-auth
password   include      system-auth
# pam_selinux.so close should be the first session rule
session    required     pam_selinux.so close
session    required     pam_loginuid.so
session    optional     pam_console.so
# pam_selinux.so open should only be followed by sessions to be executed in the user context
session    required     pam_selinux.so open
session    required     pam_namespace.so
session    optional     pam_keyinit.so force revoke
session    include      system-auth
session    include      postlogin
-session   optional     pam_ck_connector.so
~
```

可能导致登录失败的原因是 `system-auth` 配置文件中的 `pam_limits.so` 模块路径配置错误。如下图所示：

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        required      pam_faildelay.so delay=2000000
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     required      pam_permit.so

password    requisite     pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
password    sufficient    pam_unix.so md5 shadow nullok try_first_pass use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      /lib/security/pam_limits.so
-session     optional      pam_systemd.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
```

> **说明：**

> `pam_limits.so` 模块的主要功能是限制用户会话过程中对各种系统资源的使用情况。模块路径需根据操作系统实际情况进行填写，若写错路径会导致无法找到对应的认证模块，导致登录认证报错。

您可以参见 故障处理，进入 `system-auth` 文件，并找到 `pam_limits.so` 模块路径配置，修改为正确配置。

## 故障处理

1. 尝试使用 SSH 登录云服务器，详情请参见 使用 SSH 登录 Linux 实例 。
   - 登录成功，则执行下一步。
   - 登录失败，则需使用单用户模式，详情请参见 通过控制台进入 Linux 实例单用户模式 。
2. 登录成功后，执行以下命令查看日志信息。

```
vim /var/log/secure
```

此文件一般用来记录安全相关的信息，其中大部分记录为用户登录云服务器的相关日志。如下图所示，可从信息中获取有 `/lib/security/pam_limits.so` 的报错信息。

```
Oct 28 15:51:01 VM-96-4-centos crond[3803]: PAM unable to dlopen(/lib/security/pam_limits.so): /lib/security/pam_limits.so: cannot open shared object f
ile: No such file or directory
Oct 28 15:51:01 VM-96-4-centos crond[3803]: PAM adding faulty module: /lib/security/pam_limits.so
Oct 28 15:51:06 VM-96-4-centos login: PAM unable to dlopen(/lib/security/pam_limits.so): /lib/security/pam_limits.so: cannot open shared object file: N
o such file or directory
```

3. 依次执行以下命令，进入 `/etc/pam.d` 目录后，搜索日志中报错 pam 模块的关键字 `/lib/security/pam_limits.so` 。

```
cd /etc/pam.d
```

```
find . | xargs grep -ri "/lib/security/pam_limits.so" -l
```

返回类似如下图所示信息，则表示 `system-auth` 文件中配置了该参数。

```
bash-4.2# find .| xargs grep -ri "/lib/security/pam_limits.so" -l
./system-auth-ac
./system-auth
./system-auth-ac
```

4. 进入 `system-auth` 文件，修复 `pam_limits.so` 模块路径配置。
   例如，在64位的操作系统中，该模块路径可配置为绝对路径 `/lib64/security/pam_limits.so` ，也可配置为相对路径 `pam_limits.so` 。

# Linux 实例：VNC 登录报错 Account locked due to XXX failed logins

最近更新时间：2025-06-03 11:17:42

## 现象描述

使用 VNC 无法正常登录云服务器，在输入登录密码前就出现报错信息 “Account locked due to XXX failed logins” 。如下图所示：

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1062.18.1.el7.x86_64 on an x86_64

[redacted] login: root
Account locked due to 10 failed logins
Password:
```

## 可能原因

使用 VNC 登录会调用 `/etc/pam.d/login` pam 模块进行校验，而在 login 配置文件中具备 `pam_tally2.so` 模块的认证。 `pam_tally2.so` 模块的功能是设置 Linux 用户连续 N 次输入错误密码进行登录时，自动锁定 X 分钟或永久锁定。其中，永久锁定需进行手工解锁，否则将一直锁定。
如果登录失败超过配置的尝试次数，登录账户就会被锁定一段时间，且暴力破解也有可能导致账户被锁定从而无法登录。下图为已配置的登录可尝试次数：

```
#%PAM-1.0
auth required pam_tally2.so deny=3 lock_time=10 unlock_time=300 even_deny_root root_unlock_time=600
auth [user_unknown=ignore success=ok ignore=ignore default=bad] pam_securetty.so
auth       substack     system-auth
auth       include      postlogin
account    required     pam_nologin.so
account    include      system-auth
password   include      system-auth
# pam_selinux.so close should be the first session rule
session    required     pam_selinux.so close
session    required     pam_loginuid.so
session    optional     pam_console.so
# pam_selinux.so open should only be followed by sessions to be executed in the user context
session    required     pam_selinux.so open
session    required     pam_namespace.so
session    optional     pam_keyinit.so force revoke
session    include      system-auth
session    include      postlogin
-session   optional     pam_ck_connector.so
~
```

`pam_tally2` 模块参数说明见下表：

| 参数 | 说明 |
| --- | --- |
| deny=n | 登录失败次数超过 n 次后拒绝访问。 |
| lock_time=n | 登录失败后锁定的时间（秒）。 |
| unlock_time=n | 超出登录失败次数限制后，解锁所需的时间。 |
| no_lock_time | 不在日志文件 /var/log/faillog 中记录 .fail_locktime 字段。 |
| magic_root | root 用户（uid=0）调用该模块时，计数器不会递增。 |
| even_deny_root | root 用户登录失败次数超过 deny=n 次后拒绝访问。 |
| root_unlock_time=n | 与 even_deny_root 相对应的选项。如果配置该选项，root 用户在登录失败次数超出限制后被锁定的时间。 |

您可以参考 故障处理，修改服务器的 `/etc/pam.d/login` 配置文件，临时注释 `pam_tally2.so` 模块配置，核实账户锁定的原因，并加固安全策略。

## 故障处理

1. 尝试使用 SSH 登录云服务器，详情请参见 使用 SSH 登录 Linux 实例 。
   - 登录成功，则执行下一步。
   - 登录失败，则需使用单用户模式，详情请参见 通过控制台进入 Linux 实例单用户模式 。
2. 登录成功后，执行以下命令查看日志信息。

```
vim /var/log/secure
```

此文件一般用来记录安全相关的信息，其中大部分记录为用户登录云服务器的相关日志。如下图所示，可从信息中获取有 `pam_tally2` 的报错信息。

```
Oct 28 17:14:45 VM-96-4-centos sshd[16704]: Failed password for invalid user dell from 202.153.37.205 port 13069 ssh2
Oct 28 17:14:45 VM-96-4-centos sshd[16704]: Received disconnect from 202.153.37.205 port 13069:11: Bye Bye [preauth]
Oct 28 17:14:45 VM-96-4-centos sshd[16704]: Disconnected from 202.153.37.205 port 13069 [preauth]
Oct 28 17:14:59 VM-96-4-centos login: pam_tally2(login:auth): user root (0) tally 12, deny 2
Oct 28 17:14:59 VM-96-4-centos login: pam_succeed_if(login:auth): requirement "uid >= 1000" not met by user "root"
Oct 28 17:15:01 VM-96-4-centos login: FAILED LOGIN 2 FROM tty1 FOR root, Authentication failure
Oct 28 17:15:01 VM-96-4-centos login: pam_tally2(login:auth): unknown option: un_lock_time=300
Oct 28 17:15:03 VM-96-4-centos login: pam_tally2(login:auth): user root (0) tally 13, deny 2
Oct 28 17:15:04 VM-96-4-centos sshd[16738]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rh
ost=203.213.66.170  user=root
```

3. 依次执行以下命令，进入 `/etc/pam.d` 目录后，搜索日志中报错 pam 模块的关键字 `pam_tally2` 。

```
cd /etc/pam.d
```

```
find . | xargs grep -ri "pam_tally2" -l
```

返回类似如下图所示信息，则表示 `login` 文件中配置了该参数。

```
bash-4.2# find . |  xargs grep -ri "pam_tally2" -l
./login
./login
bash-4.2# _
```

4. 执行以下命令，临时注释 `pam_tally2.so` 模块配置。配置完成后，即可恢复登录。

```
sed -i "s/.*pam_tally.*/#&/" /etc/pam.d/login
```

5. 核实账户锁定是由人为误操作还是暴力破解引起。若是由暴力破解引起，建议选择以下方案加固安全策略：
   - 修改云服务器密码，推荐密码设置为由大写字母、小写字母、特殊字符、数字组成的12位以上的复杂随机密码。详情请参见 重置实例密码 。
   - 删除云服务器中已不再使用的用户。
   - 将 sshd 的默认22端口改为1024 – 65525间的其他非常用端口。详情请参见 修改云服务器远程默认端口 。
   - 管理云服务器已关联安全组中的规则，只需放通业务和协议所需端口，不建议放通所有协议及端口。详情请参见 添加安全组规则 。
   - 不建议向公网开放核心应用服务端口访问。例如，mysql 及 redis 等。您可将相关端口修改为本地访问或禁止外网访问。
   - 安装云镜等防护软件，并添加实时告警，以便及时获取异常登录信息。

# Linux 实例：VNC 登录输入正确密码后无响应

最近更新时间：2025-05-26 19:42:53

## 现象描述

使用 VNC 登录云服务器时，输入正确的密码无法登录，会卡在如下图所示界面，稍后会再次提示需要输入账号。

```
VM-55-10-centos login: root
Password:
-
```

且使用 SSH 远程登录时，会出现报错信息 “Permission denied,please try again.”。如下图所示：

```
[root@VM-96-14-centos ~]# ssh root@[redacted]
root@4[redacted]'s password:
Permission denied, please try again.
```

## 可能原因

可能是由于频繁暴力破解导致 `/var/log/btmp` 日志容量过大。该文件用于记录错误登录的日志，容量过大会导致登录时写入日志异常，造成无法正常登录。如下图所示：

```
bash-4.2# ll -h
bash: ll: command not found
bash-4.2# ls -alh
total 9.8G
drwxr-xr-x  10 root   root           4.0K Oct 28 17:53 .
drwxr-xr-x  19 root   root           4.0K Apr 22  2020 ..
drwxr-xr-x   2 root   root           4.0K Mar  7  2019 anaconda
drwx------   2 root   root           4.0K Aug  8  2019 audit
-rw-------   1 root   root            24K Oct 28 17:30 boot.log
-rw-------   1 root   root              1 Oct 28 15:43 boot.log-20191106
-rw-------   1 root   root              1 Oct 28 15:43 boot.log-20200807
-rw-------   1 root   utmp           9.8G Oct 28 17:41 btmp
-rw-------   1 root   utmp              1 Oct 28 15:43 btmp-20200807
drwxr-xr-x   2 chrony chrony         4.0K Aug  8  2019 chrony
-rw-r--r--   1 syslog adm            181K Oct 28 17:30 cloud-init.log
-rw-r--r--   1 root   root           7.8K Oct 28 17:30 cloud-init-output.log
-rw-------   1 root   root            14K Oct 28 17:42 cron
-rw-r--r--   1 root   root            36K Oct 28 17:30 dmesg
-rw-r--r--   1 root   root            36K Oct 28 16:26 dmesg.old
```

您可以参考 故障处理 查看日志文件 `/var/log/btmp` 容量是否过大，核实是否为暴力破解导致，并加固安全策略。

## 故障处理

1. 尝试使用 SSH 登录云服务器，详情请参见 使用 SSH 登录 Linux 实例 。
   - 登录成功，则执行下一步。
   - 登录失败，则需使用单用户模式，详情请参见 通过控制台进入 Linux 实例单用户模式 。
2. 进入 `/var/log` 查看日志文件 `/var/log/btmp` 容量。
3. 若日志文件 `/var/log/btmp` 容量过大，则执行以下命令，对 btmp 日志内容进行清空。清空日志文件后，即可恢复登录。

```
echo >/var/log/btmp
```

4. 核实账户锁定是由人为误操作还是暴力破解引起。若是由暴力破解引起，建议选择以下方案加固安全策略：
   - 修改云服务器密码，推荐密码设置为由大写字母、小写字母、特殊字符、数字组成的12位以上的复杂随机密码。详情请参见 重置实例密码 。
   - 删除云服务器中已不再使用的用户。
   - 将 sshd 的默认22端口改为1024 – 65525间的其他非常用端口。详情请参见 修改云服务器远程默认端口 。
   - 管理云服务器已关联安全组中的规则，只需放通业务和协议所需端口，不建议放通所有协议及端口。详情请参见 添加安全组规则 。
   - 不建议向公网开放核心应用服务端口访问。例如，mysql 及 redis 等。您可将相关端口修改为本地访问或禁止外网访问。
   - 安装云镜、云锁等防护软件，并添加实时告警，以便及时获取异常登录信息。

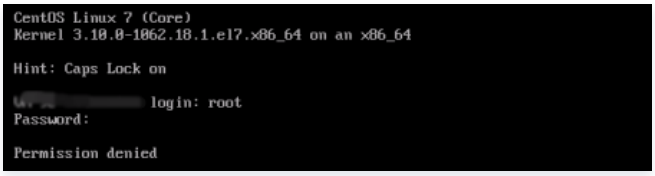
# Linux 实例：VNC 或 SSH 登录报错 Permission denied

最近更新时间：2025-06-03 11:17:42

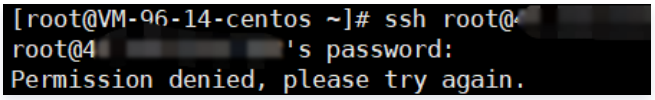
## 现象描述

使用 VNC 或 SSH 登录时，提示报错信息 “Permission denied”。

- VNC 登录报错如下图所示：




- SSH 登录报错如下图所示：




## 可能原因

使用 VNC 或 SSH 登录会调用 `/etc/pam.d/login` pam 模块进行校验，在 `/etc/pam.d/login` 配置中默认会引入 `system-auth` 模块进行认证，`system-auth` 模块默认会引入 `pam_limits.so` 模块进行认证。`system-auth` 的默认配置如下图所示：

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     required      pam_permit.so

password    requisite     pam_cracklib.so try_first_pass retry=3 type=
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
```

`pam_limits.so` 模块的主要功能是限制用户会话过程中对各种系统资源的使用情况。默认情况下该模块的配置文件是 `/etc/security/limits.conf`，该配置文件规定了用户可使用的最大文件数、最大线程数、最大内存等资源使用量。参数说明如下表：

| 参数 | 说明 |
| --- | --- |
| soft nofile | 可打开的文件描述符的最大数（软限制）。 |
| hard nofile | 可打开的文件描述符的最大数（硬限制），不能超过该设定值。 |
| fs.file-max | 系统级别的能够打开的文件句柄（内核中 struct file）的数量。针对整个系统的限制，并不针对用户。 |
| fs.nr_open | 单个进程可分配的最大文件描述符数目（fd 个数）。 |

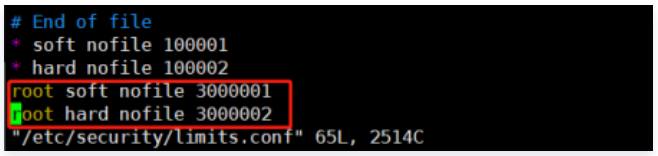
可能导致无法正常登录的原因是配置文件 `/etc/security/limits.conf` 中关于 root 用户最大能打开的文件描述符个数配置错误，正确的配置应满足 `soft nofile ≤ hard nofile ≤ fs.nr_open` 关系。
您可以参考 故障处理 将 `soft nofile`、`hard nofile` 及 `fs.nr_open` 修改为正确配置。

## 故障处理

1. 尝试使用 SSH 登录云服务器，详情请参见 使用 SSH 登录 Linux 实例 。
   - 登录成功，则执行下一步。
   - 登录失败，则需使用单用户模式，详情请参见 通过控制台进入 Linux 实例单用户模式 。
2. 查看参数 `soft nofile` 、 `hard nofile` 及 `fs.nr_open` 值是否满足 `soft nofile ≤ hard nofile ≤ fs.nr_open` 关系：
   - 执行以下命令，查看 `soft nofile` 及 `hard nofile` 值。

     ```
     cat /etc/security/limits.conf
     ```

     本文获取结果为3000001及3000002。如下图所示：

   - 执行以下命令，查看 `fs.nr_open` 值。

     ```
     sysctl -a 2>/dev/null | grep -Ei "file-max|nr_open"
     ```

     本文获取结果为1048576。如下图所示：

3. 修改 `/etc/security/limits.conf` 文件，在文件末尾添加或修改如下配置：
   - `root soft nofile` ：100001
   - `root hard nofile` ：100002
4. 修改 `/etc/sysctl.conf` 文件，在文件末尾添加或修改如下配置：

   > **说明**
   > 在满足 `soft nofile ≤ hard nofile ≤ fs.nr_open` 关系时，此步骤非必选，可在系统最大限制不足时再进行调整。

   - `fs.file-max` = 2000000
   - `fs.nr_open` = 2000000
5. 执行以下命令，使配置立即生效。配置完成后，即可恢复登录。

   ```
   sysctl -p
   ```

# Linux 实例：/etc/fstab 配置错误导致无法登录

最近更新时间：2025-05-26 19:42:53

## 现象描述

无法正常使用 SSH 远程登录 Linux 云服务器，但使用 VNC 方式登录后，查看系统启动失败且提示信息 **Welcome to emergency mode**。如下图所示：

```
[  OK  ] Reached target Remote File Systems (Pre).
[  OK  ] Reached target Remote File Systems.
         Starting Crash recovery kernel arming...
[  OK  ] Started Security Auditing Service.
         Starting Update UTMP about System Boot/Shutdown...
[  OK  ] Started Update UTMP about System Boot/Shutdown.
         Starting Update UTMP about System Runlevel Changes...
[  OK  ] Started Update UTMP about System Runlevel Changes.                    t
Welcome to emergency mode! After logging in, type "journalctl -xb" to view  c   i
system logs, "systemctl reboot" to reboot, "systemctl default" or ^D to
try again to boot into default mode.
Give root password for maintenance
(or press Control-D to continue):
```

## 可能原因

可能由于 `/etc/fstab` 配置不当导致。
例如，已在 `/etc/fstab` 中配置使用设备名称自动挂载磁盘，但云服务器重启时设备名称发生改变，导致系统无法正常启动。
您可以参见 故障处理 修复 `/etc/fstab` 配置文件，重启服务器后再进行核验。

## 故障处理

您可通过以下2种方式进入实例并处理该问题：

**方式1：使用 VNC 登录（推荐）**

1. 使用 VNC 登录 Linux 实例 。
2. 进入 VNC 界面后，查看到如 现象描述 中所示界面，请输入 root 账户密码并按 **Enter** 登录服务器。
   - 输入的密码默认不显示。
   - 若您不具备或忘记 root 账户密码，则请参考方式2进行处理。
3. 执行以下命令，备份 `/etc/fstab` 文件。本文以备份到 `/home` 目录下为例：

```
cp /etc/fstab /home
```

4. 执行以下命令，使用 VI 编辑器打开 `/etc/fstab` 文件。

```
vi /etc/fstab
```

5. 按 **i** 进入编辑模式，将光标移动至错误配置行首，并输入 `#` 注释该行配置。如下图所示：

> **说明：**
> 若您无法确定错误配置，则建议先注释除系统盘外的所有挂载盘配置，待服务器恢复正常后再参见 步骤8 进行配置。

```
# /etc/fstab
# Created by anaconda on Tue Nov 26 02:11:36 2019
#
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#
UUID=659e6f89-71fa-463d-842e-ccdf2c06e0fe /                       ext4    defaults        1 1
#/dev/vdc1_/data auto rw,relatime,data=ordered 0 2
```

6. 按 **Esc** 输入 **:wq** 后，按 **Enter** 保存设置并退出编辑器。
7. 通过控制台重启实例，并验证是否能正常启动及登录。

> **说明:**
> 通过控制台重启实例具体步骤请参见 重启实例 。

8. 登录成功后，若您需设置磁盘自动挂载，请参见 配置 /etc/fstab 文件 进行对应配置。

**方式2：使用救援模式**

1. 参见 使用救援模式 ，进入实例救援模式。

> **注意:**
> 需执行 使用救援模式进行系统修复 步骤中的 `mount` 及 `chroot` 相关命令，且确保已进入业务本身的系统。

2. 按照 方式1 中的 步骤3 – 步骤6，修复 `/etc/fstab` 文件。
3. 参见 退出救援模式 ，退出实例救援模式。
4. 实例退出救援模式后，会保持为进入救援模式之前的状态。若是进入救援模式之前做了关机操作，实例退出救援模式后将处于关机状态，请参见 开机实例 开机，并在启动后验证系统是否可正常启动及登录。
5. 登录成功后，若您需设置磁盘自动挂载，请参见 配置 /etc/fstab 文件 进行配置。

# Linux 实例：sshd 配置文件权限问题

最近更新时间：2024-09-24 16:49:27

## 现象描述

使用 SSH 登录 Linux 实例时，报错 ssh_exchange_identification: Connection closed by remote host 或 no hostkey alg。

## 可能原因

| 可能原因 | 处理措施 |
| --- | --- |
| /var/empty/sshd 文件权限未修改 | 检查 /var/empty/sshd 文件权限是否已修改 |
| /etc/ssh/ssh_host_rsa_key 文件权限未修改 | 检查 /etc/ssh/ssh_host_rsa_key 文件权限是否已修改 |

## 故障处理

### 检查 /var/empty/sshd 文件权限是否已修改

1. 使用 VNC 登录 Linux 实例。
2. 执行以下命令，查看报错原因。

```
sshd -t
```

返回类似如下信息：

```
"/var/empty/sshd must be owned by root and not group or world-writable."
```

3. 执行以下命令，修改 `/var/empty/sshd/` 文件权限。

```
chmod 711 /var/empty/sshd/
```

### 检查 /etc/ssh/ssh_host_rsa_key 文件权限是否已修改

1. 使用 VNC 登录 Linux 实例。
2. 执行以下命令，查看报错原因。

```
sshd -t
```

返回信息中包含如下字段：

```
"/etc/ssh/ssh_host_rsa_key are too open"
```

3. 执行以下命令，修改 `/etc/ssh/ssh_host_rsa_key` 文件权限。

```
chmod 600 /etc/ssh/ssh_host_rsa_key
```

# Linux 实例：/etc/profile 死循环调用问题

最近更新时间：2024-09-24 16:49:27

## 现象描述

使用 SSH 登录 Linux 实例时，SSH 命令在输出 “Last login: ” 相关信息后卡住。

## 可能原因

可能由于 `/etc/profile` 文件被修改过，出现在 `/etc/profile` 中调用 `/etc/profile` 的现象，导致陷入死循环调用，无法成功登录。您可以参见 处理步骤，检查并修复 `/etc/profile` 文件。

## 故障处理

1. 使用 VNC 登录 Linux 实例。
2. 执行以下命令，查看 `/etc/profile` 文件。

```
vim /etc/profile
```

3. 检查 `/etc/profile` 文件中是否包含 `/etc/profile` 相关命令。
   - 是，执行下一步。
   - 否，请通过 在线支持 联系我们寻求帮助。
4. 按 **i** 进入编辑模式，在 `/etc/profile` 相关命令前增加 `#` 以注释该命令。
5. 按 **Esc** 退出编辑模式，并输入 **:wq** 保存修改。
6. 参见 使用 SSH 登录 Linux 实例 进行登录。

版权所有：腾讯云计算（北京）有限责任公司

# 服务器被隔离导致无法登录

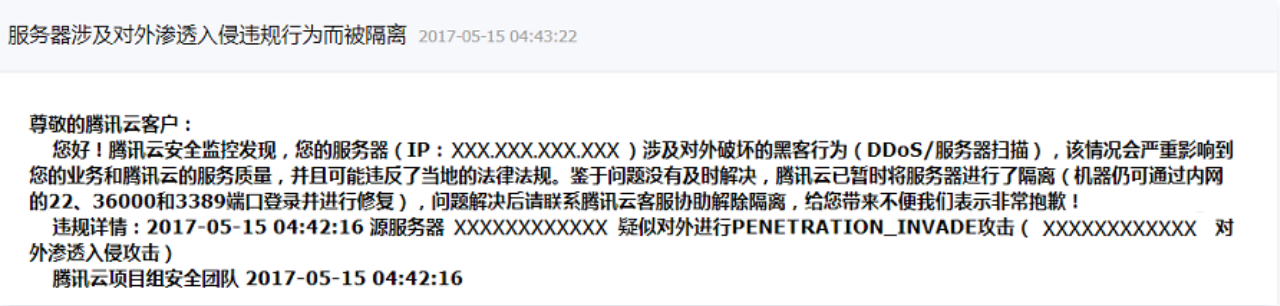
最近更新时间：2025-06-16 17:00:22

## 现象描述

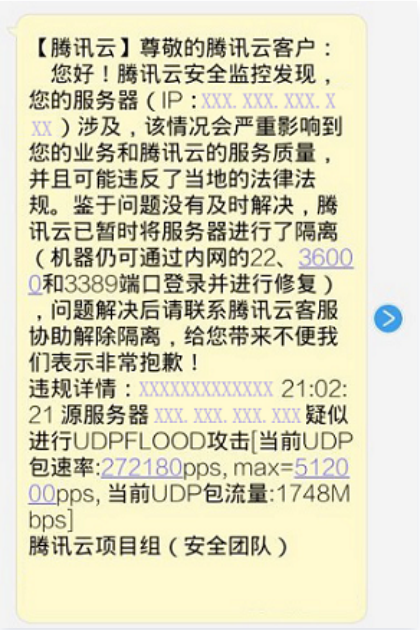
云服务器可能会因安全违规（内容或行为违规）或因 DDoS 攻击被封堵隔离，被隔离的云服务器在控制台显示为 “BANNING” 状态。
云服务器被隔离可能由于该台服务器违反了当前法律法规的要求。您可以通过以下方式查看该台服务器是否处于被隔离的状态。

- 云服务器外网被隔离时，将会通过 站内信 或发送短信的方式将违规隔离通知到您。
  - 站内信图片：

或者




  - 短信图片：




- 云服务器控制台 中的"状态"栏 显示该云服务器状态为：隔离中。

## 可能原因

云服务器出现违规事件或风险事件时，会对违规机器进行部分隔离操作（除内网的22、36000、3389登录接口，其余网络访问全部隔离，开发者可以通过跳板机的方式登录服务器）。
详情请参见 云安全违规事件的等级划分及处罚说明 。

## 故障处理

1. 按照站内信或者短信提示处理违规内容。处理好安全隐患，必要时重装系统。
2. 如果不是您个人行为导致的违规，那么您的服务器有可能已被恶意入侵。解决方案请参见：主机安全 。
3. 排除安全隐患或停止违规后，请通过 在线支持 联系客服解除隔离。

版权所有：腾讯云计算（北京）有限责任公司

# 带宽占用高导致无法登录

最近更新时间：2025-06-16 17:00:22

本文档介绍 Linux 和 Windows 云服务器因带宽占用高导致无法远程连接的排查方法和解决方案。

## 故障现象

- 通过登录 腾讯云云服务器控制台，查看到云服务器的带宽监控数据提示带宽占用过高，无法连接腾讯云服务器。
- 通过 自助诊断 工具诊断出带宽占用过高。

## 故障定位及处理

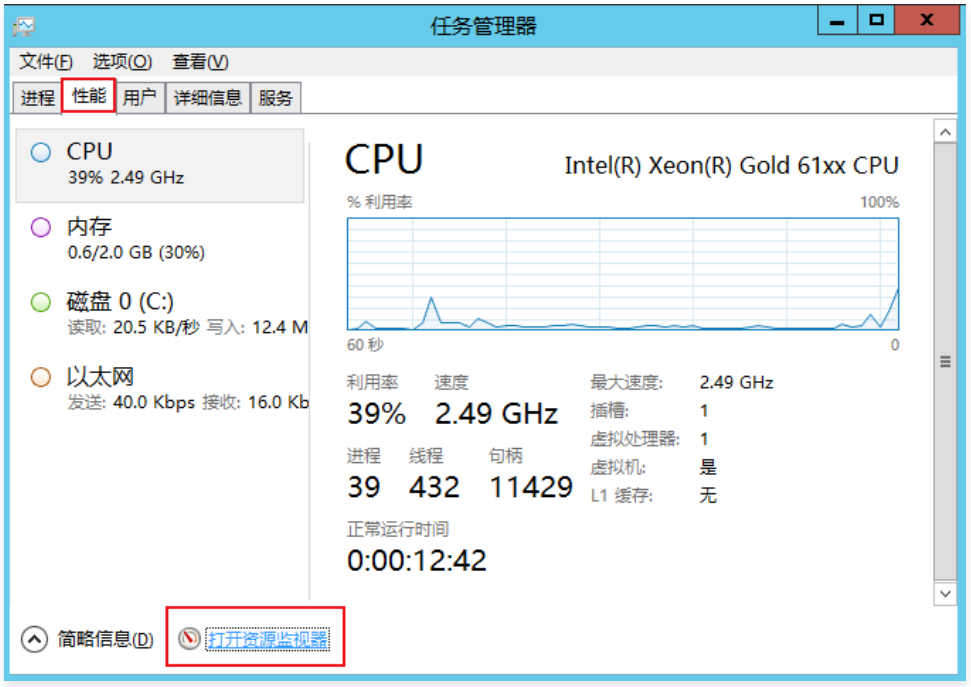
1. 对应实际使用的云服务器实例，使用 VNC 方式登录：
   - Windows 实例：使用 VNC 登录 Windows 实例
   - Linux 实例：使用 VNC 登录 Linux 实例
2. 针对云服务器进行排障及问题处理：

针对 Windows 服务器

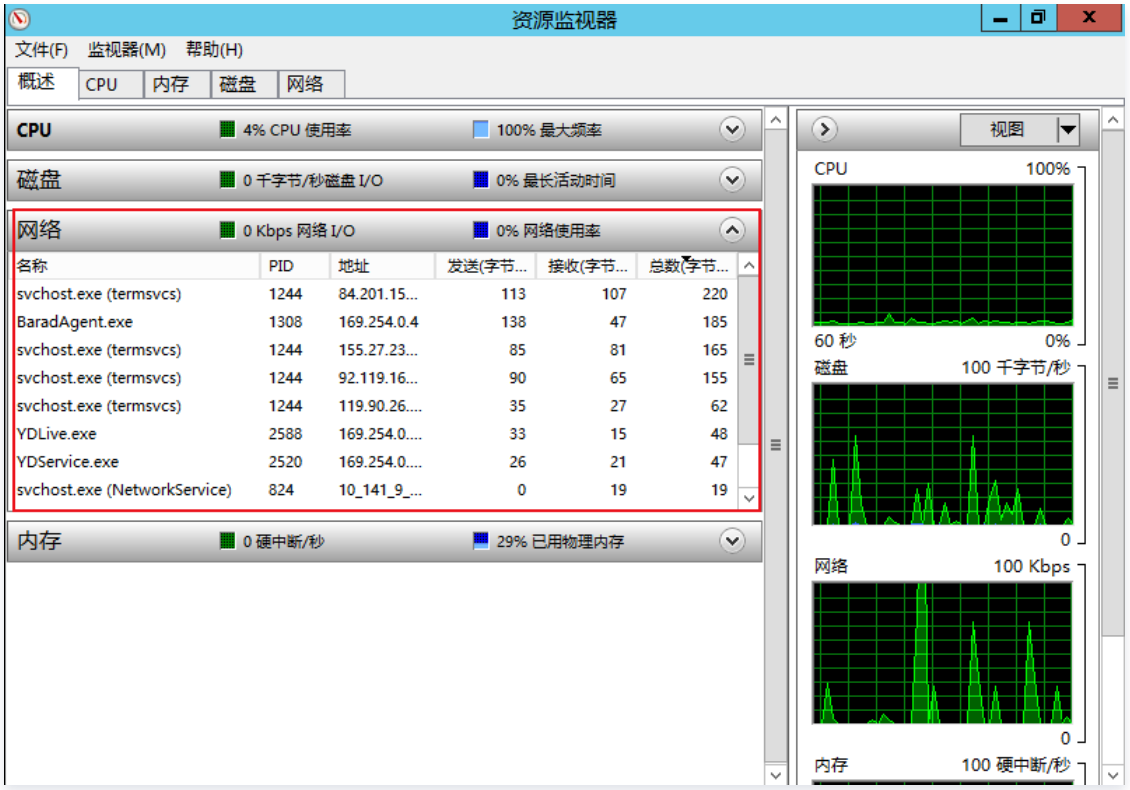
通过 VNC 方式登录 Windows 云服务器之后，您需要执行以下操作：

> **说明：**
> 以下操作以 Windows Server 2012 系统的云服务器为例。

1. 在云服务器中，单击 ，选择**任务管理器**，打开“任务管理器”窗口。
2. 选择**性能**页签，单击**打开资源监视器**。如下图所示：



3. 在打开的**资源监视器**中，查看消耗带宽较多的进程，并根据您的实际业务，判断此进程是否正常。如下图所示：




- 如果消耗带宽较多的进程为业务进程，则需要分析是否由于访问量变化引起，是否需要优化空间或者 升级服务器配置 。
- 如果消耗带宽较多的进程为异常进程，可能是病毒或木马导致，您可以自行终止进程或者使用安全软件进行查杀，也可以对数据备份后，重装系统。

> **注意：**
> Windows 系统下很多病毒程序会伪装成系统进程，您可以通过**任务管理器** > **进程**中的进程信息来进行初步鉴别：
> 正常的系统进程都会有完整的签名以及介绍，并且多数位于 C:\Windows\System32 目录下。病毒程序名字可能同系统进程一样，但缺少签名及描述，位置也会比较不寻常。

- 如果消耗带宽较多的进程为腾讯云组件进程，请通过 在线支持 联系我们进行进一步定位处理。

### 针对 Linux 服务器

通过 VNC 方式登录 Linux 云服务器之后，您需要执行以下操作：

> **说明：**
> 以下操作以 CentOS 7.6 系统的云服务器为例。

1. 执行以下命令，安装 iftop 工具（iftop 工具为 Linux 服务器下的流量监控小工具）。

```
yum install iftop -y
```

> **说明：**
> 如果是 Ubuntu 系统，请执行 `apt-get install iftop -y` 命令。

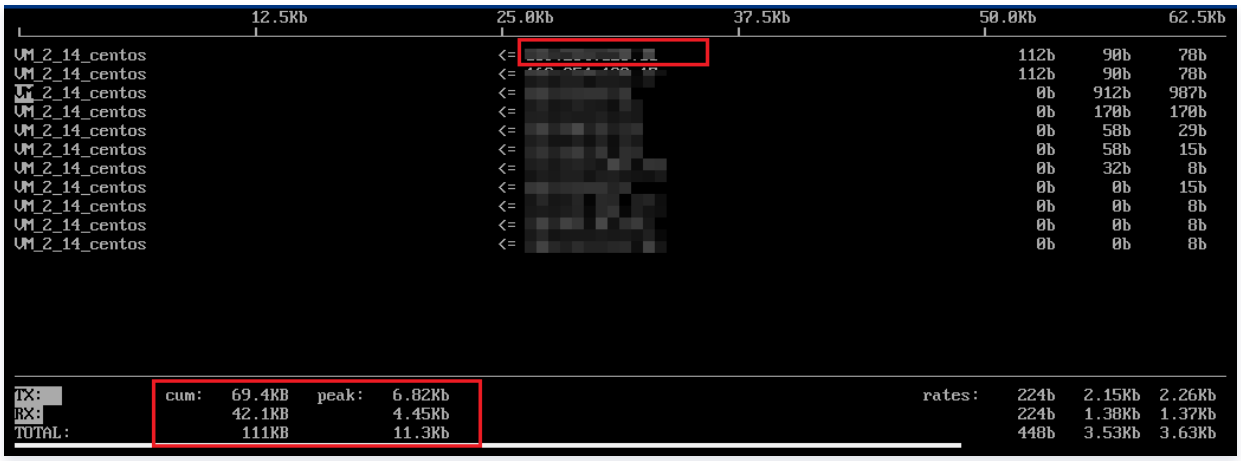
2. 执行以下命令，安装 lsof。

```
yum install lsof -y
```

> **说明：**
> 如果是 Ubuntu 系统，请执行 `apt-get install lsof -y` 命令。

3. 执行以下命令，运行 iftop。如下图所示：

```
iftop
```




- `<=` 、 `=>` 表示流量的方向。
- TX 表示发送流量。
- RX 表示接收流量。
- TOTAL 表示总流量。
- cum 表示运行 iftop 到目前时间的总流量。
- peak 表示流量峰值。
- rates 分别表示过去2s、10s和40s的平均流量。

4. 根据 iftop 中消耗流量的 IP，执行以下命令，查看连接该 IP 的进程。

```
lsof -i | grep IP
```

例如，消耗流量的 IP 为201.205.141.123，则执行以下命令：

```
lsof -i | grep 201.205.141.123
```

根据返回的如下结果，得知此服务器带宽主要由 SSH 进程消耗。

```
sshd       12145    root    3u  IPV4  3294018       0t0   TCP 10.144.90.86:ssh-
>203.205.141.123:58614(ESTABLISHED)
sshd       12179  ubuntu    3u  IPV4  3294018       0t0   TCP 10.144.90.86:ssh-
>203.205.141.123:58614(ESTABLISHED)
```

5. 查看消耗带宽的进程，判断此进程是否正常。
   - 如果消耗带宽较多的进程为业务进程，则需要分析是否由于访问量变化引起，是否需要优化空间或者 升级服务器配置 。
   - 如果消耗带宽较多的进程为异常进程，可能是病毒或木马导致，您可以自行终止进程或者使用安全软件进行查杀，也可以先对数据进行备份，可以使用 创建快照 的方式进行备份，然后 重装系统 。
   - 如果消耗带宽较多的进程为腾讯云组件进程，请通过 在线支持 联系我们进行进一步定位处理。

建议您重点核查目的端 IP 归属地，可以通过 IP138查询网站 进行 IP 归属地查询。如果发现目的端 IP 归属地为国外，安全隐患更大，请务必重点关注！

# 安全组设置导致无法远程连接

最近更新时间：2025-06-16 17:00:22

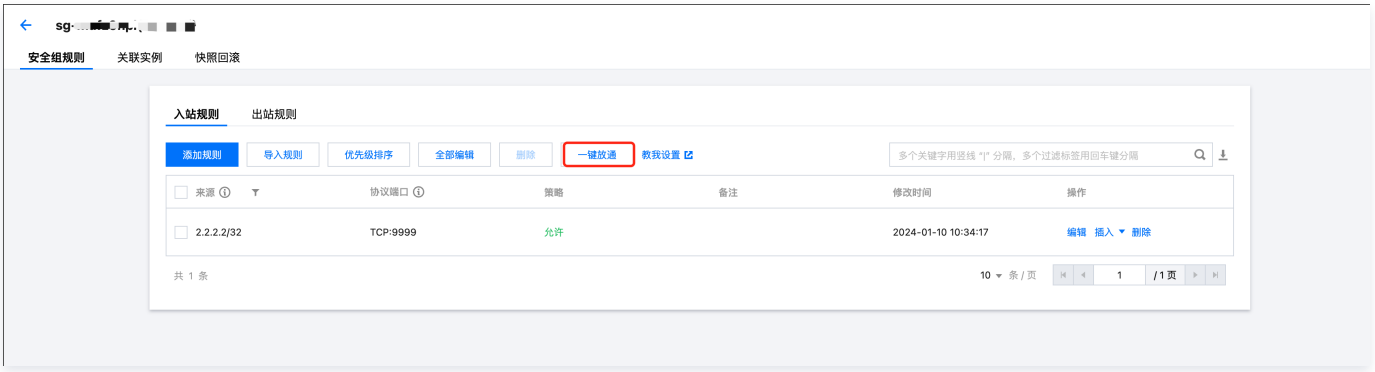
本文档介绍云服务器因安全组设置问题导致无法远程连接的排查方法和解决方案。

## 检查工具

您可以通过腾讯云提供的 实例端口验通 判断无法远程连接是否与安全组设置相关。

1. 登录 实例端口验通 。
2. 在**实例端口验通**页面，选择您需要检测的实例，单击**一键检测**。如下图所示：

3. 如果该实例检测出有未放通的端口，可以登录 安全组控制台 ，进入安全组管理页面。单击进入对应安全组详情页后，通过**一键放通**功能放通服务器常用端口，并再次尝试远程登录。




## 修改安全组设置

如果通过工具检查，确认为安全组端口设置问题，但您不想通过**一键放通**功能放通所有云服务器的常用端口，或者您需要自定义远程登录端口，您还可以通过自定义配置安全组的入站和出站规则，解决无法远程连接的问题。具体操作请参见 修改安全组规则 。

# Linux 实例使用 VNC 及救援模式排障

最近更新时间：2025-03-07 09:07:32

在通常情况下，多数 Linux 系统类问题可通过 VNC 方式及救援模式进行排查及修复。本文介绍如何使用这两种方式排查 Linux 实例无法 SSH 登录、系统失败问题。您可通过本文了解并在遇到实例问题时，进行排查及修复。

## 排查工具

- VNC 登录是通过 Web 浏览器远程连接云服务器的方式，一般在无法正常 SSH 远程登录实例时使用。使用 VNC 登录方式可直接观察云服务器状态，或进行修改系统内配置文件等操作。
- 救援模式一般在 Linux 系统无法正常启动，或无法通过 VNC 登录时使用。常见使用场景例如 fstab 配置异常、系统关键文件缺失、lib 动态库文件损坏/缺失等。

## 问题定位及处理

### VNC 方式排查 SSH 无法登录问题

#### 现象描述

使用 SSH 登录 Linux 实例时，出现报错信息 “ssh_exchange_identification: Connection closed by remote host” 。如下图所示：

```
[root@[redacted] ~]# ssh root[redacted]
kex_exchange_identification: read: Connection reset by peer
```

#### 可能原因

kex_exchange_identification 阶段的 connection reset 报错，一般代表 ssh 相关进程已启动，但是配置可能存在异常，例如 sshd 配置文件权限被修改。

#### 解决思路

参见 处理步骤 ，检查 sshd 进程，定位并解决问题。

#### 处理步骤

1. 参考以下步骤，使用 VNC 登录 Linux 实例：
   1.1 登录 云服务器控制台 ，找到需要登录的 Linux 云服务器，单击右侧的**登录**。如下图所示：

   1.2 在打开的**登录**窗口，单击 **VNC 登录**。如下图所示：

1.3 在 **login** 后输入用户名，按 **Enter**，在 **Password** 后输入密码，按 **Enter**。如下图所示即为登录成功：

2. 执行以下命令，查看 sshd 进程是否正常运行。

```
ps -ef | grep sshd
```

返回结果如下图所示，sshd 进程正常。

```
[root@VM-0-11-centos ~]# ps -ef | grep sshd
root        1173       1  0 22:08 ?        00:00:00 /usr/sbin/sshd -D -oCiphers=aes256-gcm@openssh.com,chacha20-poly1305@openssh
.com,aes256-ctr,aes256-cbc,aes128-gcm@openssh.com,aes128-ctr,aes128-cbc -oMACs=hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@opens
sh.com,umac-128-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha1,umac-128@openssh.com,hmac-sha2-512 -oGSSAP
IKexAlgorithms=gss-curve25519-sha256-,gss-nistp256-sha256-,gss-group14-sha256-,gss-group16-sha512-,gss-gex-sha1-,gss-group14-sha
1- -oKexAlgorithms=curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffi
e-hellman-group-exchange-sha256,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie
-hellman-group-exchange-sha1,diffie-hellman-group14-sha1 -oHostKeyAlgorithms=ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@op
enssh.com,ecdsa-sha2-nistp384,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521,ecdsa-sha2-nistp521-cert-v01@openssh.
com,ssh-ed25519,ssh-ed25519-cert-v01@openssh.com,rsa-sha2-256,rsa-sha2-256-cert-v01@openssh.com,rsa-sha2-512,rsa-sha2-512-cert-v
01@openssh.com,ssh-rsa,ssh-rsa-cert-v01@openssh.com -oPubkeyAcceptedKeyTypes=ecdsa-sha2-nistp256,ecdsa-sha2-nistp256-cert-v01@op
enssh.com,ecdsa-sha2-nistp384,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521,ecdsa-sha2-nistp521-cert-v01@openssh.
com,ssh-ed25519,ssh-ed25519-cert-v01@openssh.com,rsa-sha2-256,rsa-sha2-256-cert-v01@openssh.com,rsa-sha2-512,rsa-sha2-512-cert-v
01@openssh.com,ssh-rsa,ssh-rsa-cert-v01@openssh.com -oCASignatureAlgorithms=ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-n
istp521,ssh-ed25519,rsa-sha2-256,rsa-sha2-512,ssh-rsa
root        2473    1722  0 22:13 tty1     00:00:00 grep --color=auto sshd
```

3. 执行以下命令，查看报错原因。

```
sshd -t
```

返回类似如下图所示信息 “/var/empty/sshd must be owned by root and not group or world-writable.”，可定位错误原因为 `/var/empty/sshd/` 权限问题导致。

```
[root@[redacted] ~]# sshd -t
/var/empty/sshd must be owned by root and not group or world-writable.
[root@[redacted] ~]#
```

您还可通过查看 `/var/log/secure` 日志中的报错信息来辅助排查。如下图所示：

```
systemd[1]: Started Session 174 of user root.
systemd[1]: session-174.scope: Succeeded.
systemd[1]: Started Session 175 of user root.
systemd[1]: session-175.scope: Succeeded.
systemd[1]: Started Session 176 of user root.
systemd[1]: session-176.scope: Succeeded.
sshd[123651]: fatal: /var/empty/sshd must be owned by root and not group or world-writable.
```

4. 执行以下命令，查看 `/var/empty/sshd` 目录权限。

```
ll -d /var/empty/sshd/
```

返回结果如下图所示，可知权限被修改为777。

```
[root@[illegible] ~]# ll -d /var/empty/sshd/
drwxrwxrwx. 2 root root 4096 Jul 13  2021 /var/empty/sshd/
```

5. 执行以下命令，修改 `/var/empty/sshd/` 文件权限。

```
chmod 711 /var/empty/sshd/
```

参见 使用 SSH 登录 Linux 实例 测试后，可正常远程登录实例。

## VNC 方式排查 Linux 系统启动失败问题

### 现象描述

无法正常 SSH 远程登录 Linux 云服务器，但使用 VNC 方式登录后，查看系统启动失败且提示信息 “Welcome to emergency mode”。如下图所示：

```
[  OK  ] Reached target Remote File Systems (Pre).
[  OK  ] Reached target Remote File Systems.
         Starting Crash recovery kernel arming...
[  OK  ] Started Security Auditing Service.
         Starting Update UTMP about System Boot/Shutdown...
[  OK  ] Started Update UTMP about System Boot/Shutdown.
         Starting Update UTMP about System Runlevel Changes...
[  OK  ] Started Update UTMP about System Runlevel Changes.
Welcome to emergency mode! After logging in, type "journalctl -xb" to view
system logs, "systemctl reboot" to reboot, "systemctl default" or ^D to
try again to boot into default mode.
Give root password for maintenance
(or press Control-D to continue):
```

### 可能原因

可能由于 `/etc/fstab` 配置不当导致。
例如，已在 `/etc/fstab` 中配置使用设备名称自动挂载磁盘，但云服务器重启时设备名称发生改变，导致系统无法正常启动。

### 解决思路

参见 处理步骤 修复 `/etc/fstab` 配置文件，重启服务器后再进行核验。

### 处理步骤

1. 参见 处理步骤1，使用 VNC 登录 Linux 实例。
2. 进入 VNC 界面后，查看到如 现象描述 中所示界面，请输入 root 账户密码并按 **Enter** 登录服务器。输入的密码默认不显示，如下图所示：

```
Give root password for maintenance
(or press Control-D to continue):
[root@[illegible] ~]#
```

3. 进入系统后，执行以下命令，查看 fstab 文件中盘符信息是否正确。

```
lsblk
```

返回结果如下图所示，文件中盘符信息有误：

```
[root@[illegible] ~]# lsblk
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sr0     11:0    1 184.1M  0 rom
vda    253:0    0    50G  0 disk
└vda1 253:1    0    50G  0 part /
[root@[illegible] ~]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Tue Nov 26 02:11:36 2019
#
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#
UUID=659e6f89-71fa-463d-842e-ccdf2c06e0fe /                       ext4    defaults        1 1
/dev/vdb1       /data   ext3    defaults        0       0
[root@[illegible] ~]#
```

4. 执行以下命令，备份 fstab 文件。

```
cp /etc/fstab /home
```

5. 执行以下命令，使用 VI 编辑器打开 `/etc/fstab` 文件。

```
vi /etc/fstab
```

6. 按 i 进入编辑模式，将光标移动至错误配置行首，并输入 `#` 注释该行配置。如下图所示：

```
#
# /etc/fstab
# Created by anaconda on Tue Nov 26 02:11:36 2019
#
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#
UUID=659e6f89-71fa-463d-842e-ccdf2c06e0fe /                       ext4    defaults        1 1
#/dev/vdb1       /data   ext3    defaults        0       0
~
~
```

7. 按 Esc 输入 :wq 后，按 Enter 保存设置并退出编辑器。
8. 通过控制台重启实例，详情请参见 重启实例 。
9. 验证是否能正常启动及登录。

## 救援模式排查 Linux 系统启动失败问题

### 现象描述

Linux 系统重启之后无法正常启动，提示信息有诸多 FAILED 启动失败项。如下图所示：

```
[  OK  ] Reached target Local File Systems (Pre).
[  OK  ] Reached target Local File Systems.
         Starting Restore /run/initramfs on shutdown...
         Starting Tell Plymouth To Write Out Runtime Data...
         Starting Create Volatile Files and Directories...
[FAILED] Failed to start Restore /run/initramfs on shutdown.
See 'systemctl status dracut-shutdown.service' for details.
[  OK  ] Started Tell Plymouth To Write Out Runtime Data.
[FAILED] Failed to start Create Volatile Files and Directories.
See 'systemctl status systemd-tmpfiles-setup.service' for details.
         Starting Security Auditing Service...
[FAILED] Failed to start Security Auditing Service.
See 'systemctl status auditd.service' for details.
         Starting Update UTMP about System Boot/Shutdown...
[FAILED] Failed to start Update UTMP about System Boot/Shutdown.
See 'systemctl status systemd-update-utmp.service' for details.
[DEPEND] Dependency failed for Update UTMP about System Runlevel Changes.
[  OK  ] Reached target System Initialization.
[  OK  ] Listening on D-Bus System Message Bus Socket.
[  OK  ] Listening on Open-iSCSI iscsid Socket.
[  OK  ] Started daily update of the root trust anchor for DNSSEC.
[  OK  ] Started Daily Cleanup of Temporary Directories.
[  OK  ] Started dnf makecache --timer.
[  OK  ] Reached target Timers.
[  OK  ] Listening on ACPID Listen Socket.
[  OK  ] Listening on SSSD Kerberos Cache Manager responder socket.
[  OK  ] Listening on Open-iSCSI iscsiuio Socket.
[  OK  ] Reached target Sockets.
[  OK  ] Reached target Basic System.
         Starting Authorization Manager...
[  OK  ] Started libstoragemgmt plug-in server daemon.
[  OK  ] Started Machine Check Exception Logging Daemon.
         Starting System Security Services Daemon...
[  OK  ] Started ACPI Event Daemon.
         Starting Hardware RNG Entropy Gatherer Wake threshold service...
[FAILED] Failed to start NTP client/server.
See 'systemctl status chronyd.service' for details.
         Starting VDO volume services...
[  OK  ] Started D-Bus System Message Bus.
         Starting Network Manager...
[  OK  ] Reached target sshd-keygen.target.
[FAILED] Failed to start Hardware RNG Entropy Gatherer Wake threshold service.
See 'systemctl status rngd-wake-threshold.service' for details.
[DEPEND] Dependency failed for Hardware RNG Entropy Gatherer Daemon.
[FAILED] Failed to start VDO volume services.
See 'systemctl status vdo.service' for details.
[  OK  ] Started D-Bus System Message Bus.
-
```

### 可能原因

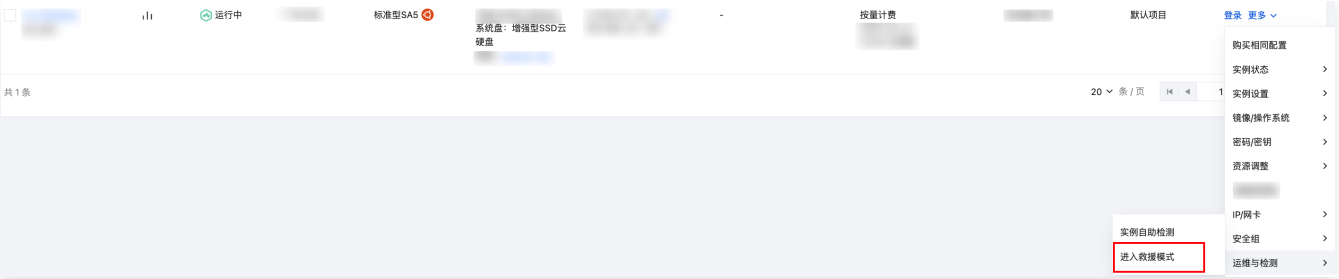
可能由于关键系统文件缺失导致启动失败，例如 bin 或 lib 文件缺失。

### 解决思路

参见 处理步骤，通过控制台进入实例救援模式，进行问题排查及修复。

### 处理步骤

1. 进入救援模式前，强烈建议您对实例进行备份，以防止由于出现误操作等造成的影响。云硬盘可通过 创建快照 备份，本地系统盘可通过 创建自定义镜像 镜像备份。
2. 登录 云服务器控制台，在“实例”页面中，选择实例所在行右侧的**更多** > **运维与检测** > **进入救援模式**。如下图所示：




3. 在弹出的**进入救援模式**窗口中，设置救援模式期间登录实例的密码，勾选**同意强制关机**。如下图所示：

4. 单击**进入救援模式**，此时实例状态会变为**进入救援模式中**。如下图所示，该过程一般会在几分钟内完成：

5. 正常进入救援模式后实例的状态会变为红色叹号的**救援模式**。如下图所示：

6. 使用 `root` 账户及 步骤3 中设置的密码，通过以下方式登录实例。
   - 若实例有公网 IP，则请参见 使用 SSH 登录 Linux 实例 。
   - 若实例无公网 IP，则请参见 使用 VNC 登录 Linux 实例 。
7. 本文以 VNC 方式登录为例，登录成功后，依次执行以下命令挂载系统盘根分区。

> **说明**
> 救援模式下实例系统盘设备名为 vda，根分区为 vda1，默认未挂载。

```
mkdir -p /mnt/vm1
```

```
mount /dev/vda1 /mnt/vm1
```

执行完成后，返回结果如下图所示：

```
[root@[redacted] ~]# mkdir -p /mnt/vm1
[root@[redacted] ~]# mount /dev/vda1 /mnt/vm1
[root@[redacted] ~]# _
```

8. 挂载成功后，即可操作原系统根分区中的数据。
   您也可使用 mount -o bind 命令，挂载原文件系统的一部分子目录，并通过 chroot 命令用来在指定的根目录下运行指令，具体操作命令如下：

```
mount -o bind /dev /mnt/vm1/dev
mount -o bind /dev/pts /mnt/vm1/dev/pts
mount -o bind /proc /mnt/vm1/proc
mount -o bind /run /mnt/vm1/run
mount -o bind /sys /mnt/vm1/sys
chroot /mnt/vm1 /bin/bash
```

执行 `chroot` 命令时：

- 若无报错信息，可继续执行 `cd /` 命令。
- 若出现如下图所示报错信息，说明无法正常切换根目录，此时可执行 `cd /mnt/vm1` 查看根分区数据。

```
[root@VM-0-11-centos ~]# mkdir -p /mnt/vm1
[root@VM-0-11-centos ~]# mount /dev/vda1 /mnt/vm1
[root@VM-0-11-centos ~]# mount -o bind /dev /mnt/vm1/dev
[root@VM-0-11-centos ~]# mount -o bind /dev/pts /mnt/vm1/dev/pts
[root@VM-0-11-centos ~]# mount -o bind /proc /mnt/vm1/proc
[root@VM-0-11-centos ~]# mount -o bind /run /mnt/vm1/run
[root@VM-0-11-centos ~]# mount -o bind /sys /mnt/vm1/sys
[root@VM-0-11-centos ~]# chroot /mnt/vm1 /bin/bash
chroot: failed to run command '/bin/bash': No such file or directory
[root@VM-0-11-centos ~]#
```

9. 通过命令，可查看原系统根分区中 `/usr/bin` 目录下的所有文件被删除。如下图所示：

```
bin  boot  data  dev  etc  home  lib  lib64  lost+found  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
[root@VM-0-11-centos vm1]# ll
total 72
lrwxrwxrwx    1 root root     7 Nov  3  2020 bin -> usr/bin
dr-xr-xr-x.   5 root root  4096 Apr 14 17:53 boot
drwxr-xr-x    2 root root  4096 Dec 10  2019 data
drwxr-xr-x   19 root root  3260 Apr 14 18:09 dev
drwxr-xr-x. 100 root root 12288 Apr 14 17:53 etc
drwxr-xr-x.   2 root root  4096 Jun 28  2021 home
lrwxrwxrwx    1 root root     7 Nov  3  2020 lib -> usr/lib
lrwxrwxrwx    1 root root     9 Nov  3  2020 lib64 -> usr/lib64
drwx------.   2 root root 16384 Nov 26  2019 lost+found
drwxr-xr-x.   2 root root  4096 Nov  3  2020 media
drwxr-xr-x.   2 root root  4096 Nov  3  2020 mnt
drwxr-xr-x.   2 root root  4096 Nov  3  2020 opt
dr-xr-xr-x  125 root root     0 Apr 14 18:08 proc
dr-xr-x---.   5 root root  4096 Mar 10 19:24 root
drwxr-xr-x   37 root root  1140 Apr 14 18:10 run
lrwxrwxrwx    1 root root     8 Nov  3  2020 sbin -> usr/sbin
drwxr-xr-x.   2 root root  4096 Nov  3  2020 srv
dr-xr-xr-x   13 root root     0 Apr 14 18:12 sys
drwxrwxrwt.   8 root root  4096 Apr 14 17:56 tmp
drwxr-xr-x.  12 root root  4096 Jun 10  2021 usr
drwxr-xr-x.  20 root root  4096 Jun 10  2021 var
[root@VM-0-11-centos vm1]# cd ./usr/bin/
[root@VM-0-11-centos bin]# pwd
/mnt/vm1/usr/bin
[root@VM-0-11-centos bin]# ls
[root@VM-0-11-centos bin]#
```

10. 此时，可创建一台同操作系统的正常机器，并执行以下命令将正常系统 `/usr/bin` 目录下的文件压缩后远程拷贝至异常机器上。
    - 正常机器：依次执行以下命令

```
cd /usr/bin/ && tar -zcvf bin.tar.gz *
```

```
scp bin.tar.gz root@异常实例ip: /mnt/vm1/usr/bin/
```

> **说明**
> 有公网 IP 可通过公网拷贝，无公网 IP 需通过内网拷贝。

执行结果如下图所示：

```
[root@VM-10-12-centos bin]# scp bin.tar.gz root@81.70.163.225:/mnt/vm1/usr/bin/
The authenticity of host '81.70.163.225 (81.70.163.225)' can't be established.
ECDSA key fingerprint is SHA256:e+y4JYiXm44,[illegible]GLmHaVo8ihDvNtbeA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '81.70.163.225' (ECDSA) to the list of known hosts.
root@81.70.163.225's password:
bin.tar.gz                                                    100%   33MB 121.9KB/s   04:33
[root@VM-10-12-centos bin]#
```

- 异常机器：在救援模式下依次执行以下命令

```
cd /mnt/vm1/usr/bin/
```

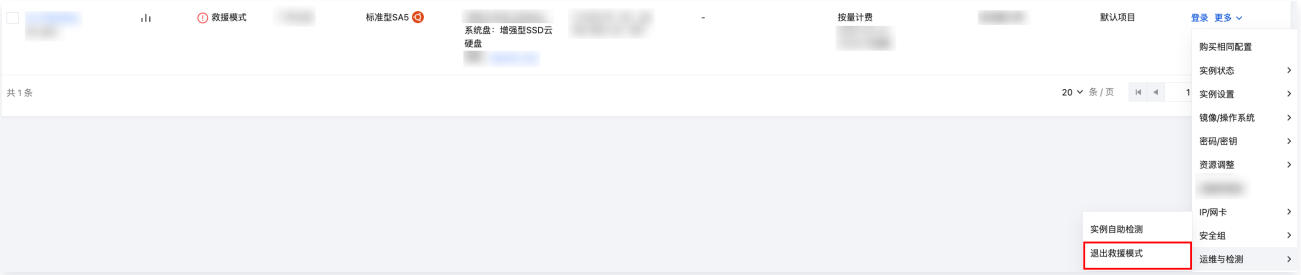
```
tar -zxvf bin.tar.gz
```

```
chroot /mnt/vm1 /bin/bash
```

执行结果如下图所示：

```
[root@VM-0-11-centos /]# chroot /mnt/vm1 /bin/ba
baobab      base64      basename    bash        bashbug     bashbug-64  batch
[root@VM-0-11-centos /]# chroot /mnt/vm1 /bin/bash
[root@VM-0-11-centos /]#
```

11. 实例修复完成后，选择实例所在行右侧的**更多** > **运维与检测** > **退出救援模式**。如下图所示：




12. 退出救援模式后实例处于关机状态，开机后进行系统验证。如下图所示，系统已恢复。

```
CentOS Linux 8 (Core)
Kernel 4.18.0-348.7.1.el8_5.x86_64 on an x86_64

Activate the web console with: systemctl enable --now cockpit.socket

VM-0-11-centos login:
```

# 关机和重启云服务器失败

最近更新时间：2025-06-16 17:00:22

## 现象描述

对云服务器执行关机、重启操作时，有较低的概率会出现关机失败或者重启失败的情况。如果您遇到此类情况，可以对云服务器进行如下排查和处理。

## 可能原因

| 可能原因 | 处理措施 |
| --- | --- |
| CPU 或内存的使用率过高 | 检查 CPU 或内存的使用率是否处于过高情况 |
| Linux 操作系统的云服务器未安装 ACPI 管理程序 | 检查 Linux 操作系统的云服务器是否安装 ACPI 管理程序 |
| Windows 系统的云服务器进行更新的时间过长 | 检查 Windows 系统的云服务器进行更新的时间是否过长 |
| 初次购买 Windows 云服务器时未完成初始化 | 检查初次购买 Windows 云服务器时是否完成初始化 |
| 系统安装的软件处于非正常状态 | 检查系统已安装的软件是否正常 |

## 故障处理

登录到云服务器，详情请参见 使用标准登录方式登录 Linux 实例 。

### 检查 CPU 或内存的使用率是否处于过高情况

1. 根据云服务器操作系统的类型，检查 CPU/内存的使用情况。
   - Windows 云服务器：在云服务器中，右键单击**任务栏**，选择**任务管理器**。
   - Linux 云服务器：执行 `top` 命令，如下图所示查看 `%CPU` 列与 `%MEM` 列的信息。

```
top - 22:36:07 up 1 day, 12:03,  2 users,  load average: 1.08, 1.18, 1.16
Tasks:  96 total,   4 running,  91 sleeping,   0 stopped,   1 zombie
%Cpu(s): 50.5 us,  1.6 sy,  0.0 ni, 47.9 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  3717152 total,   132420 free,   246912 used,  3337820 buff/cache
KiB Swap:        0 total,        0 free,        0 used.  3175320 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
 5803 root      20   0    4624    616    388 R 100.0  0.0   0:59.80 gzip
 5802 root      20   0  126252   1948   1268 R   3.2  0.1   0:01.27 tar
 8916 root      20   0  889060  19208   3348 S   1.1  0.5  10:54.92 barad_agent
    1 root      20   0  191064   4116   2640 S   0.0  0.1   0:17.81 systemd
    2 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kthreadd
```

2. 根据实际 CPU/内存的使用情况，终止 CPU 或者内存使用率过高的进程。
   若仍无法关机/重启，请 强制关机或重启云服务器 。

### 检查 Linux 操作系统的云服务器是否安装 ACPI 管理程序

> **说明**
> 此操作针对 Linux 操作系统的云服务器。

执行以下命令，查看是否存在 ACPI 进程。

```
ps -ef | grep -w "acpid" | grep -v "grep"
```

- 如果存在 ACPI 进程，请 强制关机或重启云服务器 。
- 如果不存在 ACPI 进程，请安装 ACPI 管理程序。具体操作可参见 Linux 电源管理配置 。

### 检查 Windows 系统的云服务器进行更新的时间是否过长

> **说明**
> 此操作针对 Windows 操作系统的云服务器。

在 Windows 云服务器操作系统界面，单击**开始** > **控制面板** > **Windows 更新**，查看是否存在正在更新的补丁或程序。

- Windows 在做某些补丁操作时，会在关闭系统时做一些处理，此时可能存在更新时间过长导致关机/重启失败。建议您等待 Windows 更新完成后，再尝试关机/重启云服务器的操作。
- 如果没有正在更新的补丁或程序，请 强制关机或重启云服务器 。

## 检查初次购买 Windows 云服务器时是否完成初始化

> **说明**
> 此操作针对 Windows 操作系统的云服务器。

初次购买 Windows 云服务器时，系统通过 Sysprep 方式进行分发镜像，初始化过程稍长。在初始化完成之前，Windows 会忽略关机/重启的操作，导致关机/重启失败。

- 如果您购买的 Windows 云服务器正在初始化，建议您等待 Windows 云服务器初始化完成后，再尝试关机/重启云服务器的操作。
- 如果 Windows 云服务器已完成初始化，请 强制关机或重启云服务器 。

## 检查系统已安装的软件是否正常

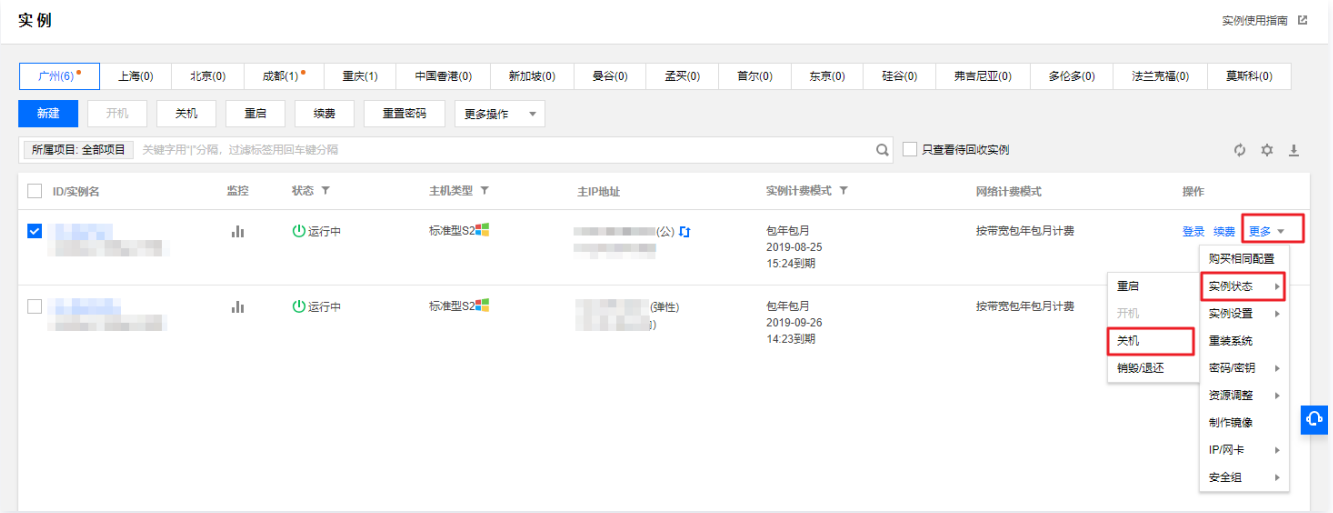
通过检查工具或者杀毒软件检查云服务器中安装的软件是否正常或者中了木马，病毒等。

- 如果发现异常，表示可能是系统本身遭破坏，导致关机/重启失败。建议您卸载该软件，使用安全软件进行查杀或者进行数据备份后，重装系统。
- 如果未发现异常，请 强制关机或重启云服务器 。

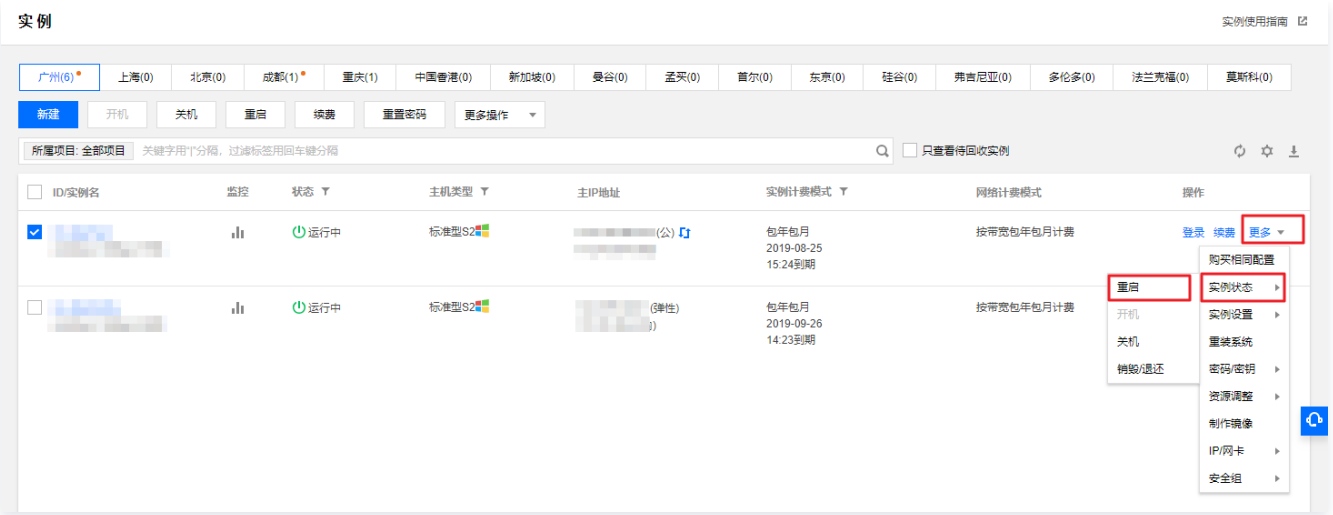
## 强制关机或重启云服务器

> **注意**
> 腾讯云提供强制关机/重启的功能，在多次尝试对云服务器进行关机/重启失败的情况下可以使用该功能。该操作会强制对云服务器进行**关机/重启**操作，可能会导致云服务器数据丢失或者文件系统损坏。

1. 登录 云服务器控制台 。
2. 在实例的管理页面，选择待关机或重启的云服务器，并根据实际需求进行不同的操作。
   - 关闭云服务器：单击**更多** > **实例状态** > **关机**。如下图所示：




   - 重启云服务器：单击**更多** > **实例状态** > **重启**。如下图所示：




3. 在弹出的**关机**或者**重启实例**窗口中，勾选**强制关机**或者**强制重启**，单击**确定**。
   - 勾选**强制关机**，如下图所示：

   - 勾选**强制重启**，如下图所示：

重启实例
您已选 1台 实例， 查看详情
No.
实例名
实例ID
当前带宽上限
1
1 Mbps
确定对选中的实例进行重启?
重启期间，实例将无法正常提供服务，请您做好准备，以免造成影响
强制重启
强制重启的效果等同于关闭计算机的电源后再接入电源启动。强制重启可能会导致实例数据丢失或者文件系统损坏，请仅在实例无法正常重启的情况下使用。
确定
取消

# 内核及 IO 相关问题

最近更新时间：2025-06-16 17:00:22

使用实例自助检测，可从检测报告中获取实例的异常情况。本文主要介绍实例自助检测报告中，内核及 IO 相关问题现象、引发原因及处理步骤。

## 内核问题定位及处理

### 故障现象

内核相关故障，可能导致机器无法登录或异常重启。

### 可能原因

#### 内核 hung_task

hung task 机制通过内核线程 khungtaskd 实现，khungtaskd 监控 TASK_UNINTERRUPTIBLE 状态的进程。如果在 `kernel.hung_task_timeout_secs` （默认120秒）周期内一直处于 D 状态，则会打印 hung task 进程的堆栈信息。
如果配置 `kernel.hung_task_panic=1` ，则会触发内核 panic 重启机器。

#### 内核软死锁 soft lockup

soft lockup 指 CPU 被内核代码占据以至于无法执行其他进程。检测 soft lockup 的原理是给每个 CPU 分配一个定时执行的内核线程 [watchdog/x]，如果该线程在一定周期内（默认为 `2*kernel.watchdog_thresh` ，3.10内核 `kernel.watchdog_thresh` 默认为10秒）没有得到执行，则表明发生了 soft lockup。
如果配置了 `kernel.softlockup_panic=1` ，则会触发内核 panic 重启机器。

#### 内核 panic

内核异常 crash 导致机器异常重启，常见的内核 panic 场景如下：

- 内核出现了 hung_task 且配置了 `kernel.hung_task_panic=1` 。
- 内核出现了软死锁 soft lockup 且配置了 `kernel.softlockup_panic=1` 。
- 触发了内核 bug。

### 处理步骤

内核相关问题排查及处理步骤较复杂，建议通过 在线支持 进一步定位及处理。

## 硬盘问题定位及处理

### 硬盘 inode 满

**故障现象：** 创建新文件时提示 No space left on device 错误信息，且使用 `df -i` 命令查看 inode 空间使用率100%。
**可能原因：** 文件系统 inode 耗尽。
**处理步骤：** 可参考文档 创建文件报错 no space left on device 。

### 硬盘空间使用率满

**故障现象：** 创建新文件时提示 No space left on device 错误信息，且使用 `df -h` 命令查看到硬盘空间使用率100%。
**可能原因：** 硬盘空间耗尽。
**处理步骤：** 可参考文档 创建文件报错 no space left on device 。

### 硬盘只读

**故障现象：** 文件系统只能读文件，不能创建新文件。
**可能原因：** 文件系统有损坏。
**处理步骤：**

1. 创建快照以备份硬盘数据，详情请参见 创建快照 。
2. 根据硬盘类型，执行对应处理步骤：

| 系统盘 |
| --- |
| |

建议直接重启实例，详情请参见 重启实例 。

数据盘

1. 执行以下命令，查看只读盘对应的文件系统类型。

```
lsblk -f
```

输出信息如下图所示。其中第1列为磁盘名；第2列为文件系统类型；第5列为磁盘挂载路径。

```
NAME   FSTYPE  LABEL    UUID                                   MOUNTPOINT
sr0    iso9660 config-2 [redacted]
vda
└vda1 ext4             4b499d76-769a-40a0-93dc-4a31a59add28 /
```

2. 执行以下命令，卸载数据盘。

```
umount <对应盘挂载路径>
```

3. 对应文件系统类型，执行以下命令进行修复：

- **ext3/ext4** 文件系统，执行以下命令：

```
fsck -y /dev/对应盘
```

- **xfs** 文件系统，执行以下命令：

```
xfs_repair /dev/对应盘
```

## 硬盘 %util 高

**故障现象：**实例卡顿，使用 SSH 或 VNC 登录慢或无响应。
**可能原因：**IO 高导致硬盘 %util 达到100%。
**处理步骤：**可参考 Linux 实例使用 atop 监控工具 文档，使用 atop 查看 IO 高是否合理，且需评估是否减少 IO 读写或者置换更高性能的硬盘。

# 系统 bin 或 lib 软链接缺失

最近更新时间：2025-05-26 19:42:53

## 现象描述

执行命令或系统启动的过程中，出现命令找不到或 lib 库找不到等报错信息。

## 可能原因

CentOS 7、CentOS 8、Ubuntu 20 等系统的 bin、sbin、lib 及 lib64 是软链接。如下所示：

```
lrwxrwxrwx   1 root root     7 Jun 19  2018 bin -> usr/bin
lrwxrwxrwx   1 root root     7 Jun 19  2018 lib -> usr/lib
lrwxrwxrwx   1 root root     9 Jun 19  2018 lib64 -> usr/lib64
lrwxrwxrwx   1 root root     8 Jun 19  2018 sbin -> usr/sbin
```

若软链接被删除，则会导致在执行命令或系统启动的过程中出现报错。您可以参见 故障处理 ，检查并新建所需软链接。

## 故障处理

1. 参见 使用救援模式 文档进入救援模式，并执行到文档中的 使用救援模式进行系统修复 步骤。
2. 执行其中的 `chroot` 命令时：
   - 有报错，执行 `cd /mnt/vm1` 。
   - 无报错，执行 `cd /` 。
3. 执行以下命令， 查看对应的软链接是否存在。

   ```
   ls -al ./ | grep -E "lib|bin"
   ```

   - 是，请通过 在线支持 联系我们寻求帮助。
   - 否，请按需执行以下命令，新建对应软链接并执行下一步。

   ```
   ln -s usr/lib64 lib64
   ln -s usr/sbin sbin
   ln -s usr/bin bin
   ln -s usr/lib lib
   ```

4. 执行以下命令，检查软链接。

   ```
   chroot /mnt/vm1 /bin/bash
   ```

   无报错信息，则说明软链接已成功修复。
5. 参见 使用救援模式 ，退出救援模式，启动系统。

版权所有：腾讯云计算（北京）有限责任公司

# 云服务器疑似被病毒入侵问题

最近更新时间：2024-03-26 16:55:43

云服务器可能由于弱密码、开源组件漏洞的问题被黑客入侵，本文介绍如何判断云服务器是否被病毒入侵，及其解决方法。

## 问题定位

使用 SSH 方式 或 使用 VNC 方式 登录实例后，通过以下方式进行判断云服务器是否被病毒入侵：

### rc.local 被增加恶意命令

执行以下命令，查看 `rc.local` 文件。

```
cat /etc/rc.local
```

若输出信息为非业务或公告镜像添加的命令，例如 `wget xx` 及 `/tmp/xx` 等，则云服务器已大概率被病毒入侵。

### crontab 被增加恶意任务

执行以下命令，列出目前的时程表。

```
crontab -l
```

若输出信息为非业务或公告镜像添加的命令，例如 `wget xx` 及 `/tmp/xx` 等，则云服务器已大概率被病毒入侵。

### ld.so.preload 增加动态库劫持

执行以下命令，查看 `/etc/ld.so.preload` 文件。

```
cat /etc/ld.so.preload
```

若输出信息为非业务增加的动态库，则云服务器已大概率被病毒入侵。

### sysctl.conf 配置大页内存

执行以下命令，查看大页内存使用情况。

```
sysctl -a | grep "nr_hugepages "
```

若输出非0，且业务自身程序并未使用大页内存，则云服务器已大概率被病毒入侵。

## 处理步骤

1. 参见 创建快照，完成系统数据备份。
2. 参见 重装系统，重装实例系统，并参考如下措施加固安全策略：
   - 修改云服务器密码，密码设置为由大写、小写、特殊字符、数字组成的12 – 16位的复杂随机密码。详情请参见 重置实例密码 。
   - 删除云服务器中已不再使用的用户。
   - 将 sshd 的默认22端口改为1024 – 65525间的其他非常用端口。详情请参见 修改云服务器远程默认端口 。
   - 管理云服务器已关联安全组中的规则，只需放通业务和协议所需端口，不建议放通所有协议及端口。详情请参见 添加安全组规则 。
   - 不建议向公网开放核心应用服务端口访问。例如，mysql 及 redis 等。您可将相关端口修改为本地访问或禁止外网访问。
   - 安装云镜、云锁等防护软件，并添加实时告警，以便及时获取异常登录信息。

版权所有：腾讯云计算（北京）有限责任公司

# 创建文件报错 no space left on device

最近更新时间：2025-06-16 17:00:22

## 现象描述

在 Linux 云服务器中创建新文件时，出现 **no space left on device** 报错。

## 可能原因

| 可能原因 | 处理措施 |
| --- | --- |
| 硬盘空间处于已满状态 | 检查硬盘空间是否已满 |
| 文件系统 inode 满 | 检查文件系统是否 inode 满 |
| df du 处于不一致状态 | 检查 df du 是否不一致 |

## 故障处理

### 检查硬盘空间是否已满

1. 登录云服务器，详情请参见 使用标准登录方式登录 Linux 实例 。
2. 执行以下命令，查看硬盘使用率。

```
df -h
```

3. 定位硬盘使用率较高的挂载点，并执行以下命令进入该挂载点。

```
cd 对应挂载点
```

例如，如需 cd 系统盘挂载点，则执行 `cd /` 。

4. 执行以下命令，查找占用空间较大的目录。

```
du -x --max-depth=1 | sort -n
```

根据定位到占用空间最大的目录容量情况，执行以下步骤：

- 如果目录容量远低于硬盘总空间，请 检查 df du 是否不一致 步骤继续排查问题。
- 如果目录容量较大，请再次从 步骤3 开始执行，注意此时是执行 cd 进入到占用空间较大的文件夹。最后可定位到占用空间较大的文件，综合业务情况评估是否可删除。若无法删除，请通过 扩容云硬盘 扩大硬盘存储空间。

### 检查文件系统是否 inode 满

1. 登录云服务器，详情请参见 使用标准登录方式登录 Linux 实例 。
2. 执行以下命令，查看硬盘使用率。

```
df -i
```

3. 定位硬盘使用率较高的挂载点，并执行以下命令进入该挂载点。

```
cd 对应挂载点
```

例如，如需 cd 系统盘挂载点，则执行 `cd /` 。

4. 执行以下命令，查找文件个数最多的目录，解决该问题。该命令较耗时，请耐心等待。

```
find / -type f | awk -F / -v OFS=/ '{$NF="";dir[$0]++}END{for(i in dir)print dir[i]" "i}' | sort -k1 -
nr | head
```

## 检查 df du 是否不一致

### 解决进程占用文件句柄问题

1. 登录云服务器，详情请参见 使用标准登录方式登录 Linux 实例 。
2. 执行以下命令，查看占用文件的进程。

```
lsof | grep delete
```

3. 若返回结果有输出，则应如下图所示：

```
[root@[redacted] ~]# lsof |grep delete
gzip      15725                root    1w      REG              253,1  352878592     394572 /root/lssls.tar.gz (deleted)
```

上图输出中第二列为进程对应的 pid，请使用此列 pid 执行如下命令。

```
systemctl status 由上图所示的进程pid
```

4. 请根据上述命令的输出情况执行相应的步骤。

- 若输出如下图所示，说明此进程不是 systemd 服务管理的进程。

```
[root@[redacted] ~]# systemctl status 15725
Failed to get unit for PID 15725: PID 15725 does not belong to any loaded unit.
```

请执行如下步骤 kill 对应进程。请使用此进程 pid 执行如下命令。

```
kill -9 进程pid
```

- 若输出如下图所示，说明此进程是 systemd 服务管理的进程。

```
[root@[redacted] ~]# systemctl status 4395
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since [redacted] ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 4395 (sshd)
   CGroup: /system.slice/sshd.service
           └─4395 /usr/sbin/sshd -D
```

请执行如下命令重启服务。

```
systemctl restart 服务名
```

- 若较多进程占用文件句柄，可重启服务器。

### 解决 mount 挂载嵌套问题

1. 执行 mount 命令，mount 占用空间大的磁盘到 `/mnt` 。例如：

```
mount /dev/vda1 /mnt
```

2. 执行以下命令，进入 `/mnt` 。

```
cd /mnt
```

3. 执行以下命令，查找占用空间较大的目录。

```
du -x --max-depth=1 | sort -n
```

根据返回结果，综合业务情况评估是否可删除目录或文件。

4. 执行 umount 命令，umount 磁盘。例如：

```
umount /mnt
```

# 系统 initramfs 或 initrd 损坏/丢失

最近更新时间：2025-04-17 11:08:32

## 现象描述

执行命令或系统启动的过程中，出现 VFS： Unable to mount root fs on unknow-block 或者 error：file '/boot/initramfs-`uname -r`.img' not found 等报错信息。

## 可能原因

1. 系统启动失败，输出 VFS： Unable to mount root fs on unknow-block 可能是 initramfs 或 initrd 有问题，需要重新生成 initramfs 或 initrd:。如下图所示：

```
[    1.543687] Kernel panic - not syncing: VFS: Unable to mount root fs on unkno
wn-block(0,0)
[    1.546440] CPU: 1 PID: 1 Comm: swapper/0 Not tainted 3.10.0-1160.119.1.el7.x
86_64 #1
[    1.549125] Hardware name: Tencent Cloud CVM, BIOS seabios-1.9.1-qemu-project
.org 04/01/2014
[    1.551938] Call Trace:
[    1.553065]  [<ffffffffa2fb1bec>] dump_stack+0x19/0x1f
[    1.555622]  [<ffffffffa2fab708>] panic+0xe8/0x21f
[    1.557707]  [<ffffffffa358c81c>] mount_block_root+0x291/0x2a4
[    1.559992]  [<ffffffffa358c882>] mount_root+0x53/0x5a
[    1.562101]  [<ffffffffa358c9c5>] prepare_namespace+0x13c/0x178
[    1.564119]  [<ffffffffa358c472>] kernel_init_freeable+0x222/0x24d
[    1.565851]  [<ffffffffa358bb64>] ? initcall_blacklist+0xb4/0xb4
[    1.567541]  [<ffffffffa2fa0400>] ? rest_init+0x80/0x80
[    1.569113]  [<ffffffffa2fa040e>] kernel_init+0xe/0x100
[    1.570675]  [<ffffffffa2fc51f7>] ret_from_fork_nospec_begin+0x21/0x21
[    1.572461]  [<ffffffffa2fa0400>] ? rest_init+0x80/0x80
[    1.574059] Kernel Offset: 0x21800000 from 0xffffffff81000000 (relocation ran
ge: 0xffffffff80000000-0xffffffffbfffffff)
[    1.577086] Rebooting in 5 seconds..
```

2. 系统启动失败，输出 error：file '/boot/initramfs-`uname -r`.img' not found 可能是 /boot 目录下缺少 initramfs/initrd 文件。如下图所示：

```
error: file `/boot/initramfs-3.10.0-1160.119.1.el7.x86_64.img' not found.

Press any key to continue...
```

上面两种情况，都会导致系统无法正常启动。您可以参见 故障处理 ，检查并重新生成 initramfs/initrd。

## 故障处理

1. 参见 使用救援模式 ，进入救援模式。
2. 执行其中的 `mount` 及 `chroot` 等命令。

```
mkdir -p /mnt/vm1
mount /dev/vda1 /mnt/vm1
mount -o bind /dev /mnt/vm1/dev
mount -o bind /dev/pts /mnt/vm1/dev/pts
mount -o bind /proc /mnt/vm1/proc
mount -o bind /run /mnt/vm1/run
mount -o bind /sys /mnt/vm1/sys
chroot /mnt/vm1 /bin/bash
```

3. 执行以下命令，重新生成 initramfs/initrd。

```
wget http://mirrors.tencentyun.com/install/cts/linux/cvmrescue_main.sh && chmod +x cvmrescue_main.sh &&
./cvmrescue_main.sh -m rebuild_initramfs
```

如果您遇到域名解析失败的问题，可以在 /etc/hosts 中配置 169.254.0.3 mirrors.tencentyun.com 用于解析软件源，添加后的内容如下图所示。

```
[root@ [redacted] ~]# cat /etc/hosts
127.0.0.1 [redacted] ;
127.0.0.1 localhost.localdomain localhost
127.0.0.1 localhost4.localdomain4 localhost4

::1 [redacted]
::1 localhost.localdomain localhost
::1 localhost6.localdomain6 localhost6
169.254.0.3 mirrors.tencentyun.com
```

输出如下，表示 initramfs 或 initrd 新建成功。

```
making 3.10.0-1160.119.1.el7.x86_64 initramfs or initrd...
success: successfully make 3.10.0-1160.119.1.el7.x86_64 initramfs or initrd
[4]Clearing Env...
[5]done
```

4. 参见 使用救援模式，退出救援模式，启动系统。

# Linux 实例内存相关故障
# 实例内存使用率过高

最近更新时间：2025-06-16 17:00:22

## 现象描述

Linux 云服务器实例出现由内存问题引发的故障。例如，系统内部服务响应速度变慢、服务器登录不上、系统触发 OOM（Out Of Memory）等。

## 可能原因

可能是实例内存使用率过高等问题引起。通常情况下当实例内存使用率持续高于90%时，可判断为实例内存使用率过高。
您可以参见 故障处理，判断问题是否由内存使用率过高引起。参见 其他内存问题典型案例分析，定位问题原因。

## 故障处理

1. 参见 相关操作，查看内存使用率是否过高。
   - 内存使用率过高，执行下一步。
   - 内存使用率正常，请参见 其他内存问题典型案例分析，进一步定位问题原因。
2. 在系统内部执行以下命令进入 `top` 界面。

```
top
```

进入 `top` 界面后按 M，此时查看 RES 及 SHR 列是否有进程占用内存过高，如下图所示。

```
top - 21:06:44 up 37 days,  9:23,  3 users,  load average: 0.01, 0.04, 0.03
Tasks: 207 total,   2 running, 205 sleeping,   0 stopped,   0 zombie
%Cpu(s):   0.7/0.8     1[||
MiB Mem :  15742.0 total,   3175.3 free,   1010.8 used,  11917.6 buff/cache
MiB Swap:      0.0 total,      0.0 free,      0.0 used.  14731.2 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
   1620 root      20   0   82924   7528   4224 R   2.0   0.0     11,42 sap1001
   2259 root      20   0  500548  50052   8320 S   1.3   0.3     12,56 sap1008
   1628 root      20   0   40116  39772   1536 S   1.0   0.2      9,41 sap1002
   1994 root      20   0   95304  10692   2688 S   0.7   0.1  95:04.50 sap1004
   3557 root      20   0  762180  22628   5632 S   0.7   0.1      8,40 barad_agent
     17 root      20   0       0      0      0 I   0.3   0.0  48:39.04 rcu_preempt
     27 root      20   0       0      0      0 S   0.3   0.0   1:26.32 ksoftirqd/2
```

   - 否，执行下一步。
   - 是，对进程进行操作，详情请参见 分析进程。
3. 执行以下命令，查看共享内存占用是否过高。

```
cat /proc/meminfo | grep -i shmem
```

返回结果如下图所示：

```
[root@[illegible] ~]# cat /proc/meminfo | grep -i shmem
Shmem:           556 kB
```

4. 执行以下命令，查看不可回收的 slab 内存占用是否过高。

```
cat /proc/meminfo | grep -i SUnreclaim
```

返回结果如下图所示：

```
[root@[illegible] ~]# cat /proc/meminfo | grep -i SUnreclaim
SUnreclaim:        13780 kB
```

5. 执行以下命令，查看是否存在内存大页。

```
cat /proc/meminfo | grep -iE "HugePages_Total|Hugepagesize"
```

返回结果如下图所示：

```
[root@V[redacted] ~]# cat /proc/meminfo | grep -iE "HugePages_Total|Hugepagesize"
HugePages_Total:       0
Hugepagesize:       2048 kB
```

- `HugePages_Total` 输出为0，请参见 其他内存问题典型案例分析，进一步定位问题原因。
- `HugePages_Total` 输出非0，表示配置了内存大页。内存大页的大小为 `HugePages_Total*Hugepagesize`， 您需确认 hugepage 是否为其他恶意程序配置。若确认已不需要内存大页，可通过执行以下命令注释 `/etc/sysctl.conf` 文件中的 `vm.nr_hugepage` 配置项。

  ```
  sed -i '/^[[:space:]]*vm\.nr_hugepage/s/^/#/' /etc/sysctl.conf
  ```

  再执行以下命令取消内存大页。

  ```
  sysctl -p
  ```

## 相关操作

### 查看内存使用率

由于不同 Linux 发行版的 `free` 命令输出的含义可能有区别，内存使用率不能通过简单的 `free` 命令输出信息进行计算得出。请按照以下步骤，通过腾讯云内存监控得到内存使用率：

1. 登录 云服务器控制台，进入实例管理页面。
2. 选择实例 ID，进入实例详情页面，并选择**监控**页签。
3. 在**内存监控**中可查看该实例的内存利用率。如下图所示：

### 计算内存使用率

内存监控中内存使用率计算方法为：用户使用的内存量与总内存量之比，不包括缓冲区与系统缓存占用的内容。计算过程如下：

= `(` MemTotal `-` MemAvailable `)100% /` MemTotal

计算过程中使用的 MemTotal MemAvailable 参数可从 `/proc/meminfo` 中获取。`/proc/meminfo` 示例如下：

```
1. [root@VM_0_113_centos test]# cat /proc/meminfo
2. MemTotal: 16265592 kB
3. MemAvailable:    3005888 kB
3. MemFree: 1880084 kB
4. ......
5. Buffers: 194384 kB
6. Cached: 13647556 kB
7. ......
8. Shmem: 7727752 kB
9. Slab: 328864 kB
10. SReclaimable: 306500 kB
11. SUnreclaim: 22364 kB
12. ......
13. HugePages_Total: 0
```

```
14. Hugepagesize: 2048 kB
```

参数说明如下：

| 参数 | 说明 |
| --- | --- |
| MemTotal | 系统总内存。 |
| MemAvailable | 可用内存 |
| MemFree | 系统剩余内存。 |
| Buffers | 表示块设备（block device）所占用的缓存页，包括直接读写块设备，以及文件系统元数据（metadata），例如 SuperBlock 所使用的缓存页。 |
| Cached | page cache，包含 tmpfs 中的文件 POSIX/SysV shared memory 及 shared anonymous mmap。 |
| Shmem | 包括共享内存，tmpfs 等。 |
| Slab | 内核 slab 分配器分配的内存，可以用 slabtop 查看。 |
| SReclaimable | 可回收的 slab。 |
| SUnreclaim | 不可回收的 slab。 |
| HugePages_Total | 内存大页总共的页数。 |
| Hugepagesize | 内存大页的大小。 |

如果不存在 MemAvailable， 则内存使用率 = （ MemTotal `-` MemFree `- Buffers - Cached - SReclaimable + Shmem`）`100%/` MemTotal

## 其他内存问题典型案例分析

如通过以上步骤均无法处理问题，或您使用云服务器时出现以下类型的错误信息，则可以参考以下解决方案：

- 日志报错 fork：Cannot allocate memory
- VNC 登录报错 Cannot allocate memory
- 实例内存未耗尽时触发 Out Of Memory

# 日志报错 fork：Cannot allocate memory

最近更新时间：2025-06-16 17:00:22

## 现象描述

日志中出现报错信息 “fork：Cannot allocate memory”。如下图所示：

```
Jan 30 18:26:45 VM_130_173_centos sshd[2110]: error: fork: Cannot allocate memory
Jan 30 18:26:48 VM_130_173_centos sshd[2110]: error: fork: Cannot allocate memory
Jan 30 18:27:03 VM_130_173_centos sshd[2110]: error: fork: Cannot allocate memory
Jan 30 18:27:11 VM_130_173_centos sshd[2110]: error: fork: Cannot allocate memory
Jan 30 18:27:15 VM_130_173_centos sshd[2110]: error: fork: Cannot allocate memory
Jan 30 18:33:24 VM_130_173_centos sshd[2110]: error: fork: Cannot allocate memory
Jan 30 18:35:24 VM_130_173_centos sshd[2110]: error: fork: Cannot allocate memory
Jan 30 18:41:14 VM_130_173_centos sshd[2110]: error: fork: Cannot allocate memory
Jan 30 18:41:15 VM_130_173_centos sshd[2110]: error: fork: Cannot allocate memory
Jan 30 18:41:16 VM_130_173_centos sshd[2110]: error: fork: Cannot allocate memory
Jan 30 18:41:17 VM_130_173_centos sshd[2110]: error: fork: Cannot allocate memory
Jan 30 18:41:20 VM_130_173_centos sshd[2110]: error: fork: Cannot allocate memory
Jan 30 18:41:21 VM_130_173_centos sshd[2110]: error: fork: Cannot allocate memory
Jan 30 18:42:18 VM_130_173_centos sshd[2110]: error: fork: Cannot allocate memory
Jan 30 18:42:22 VM_130_173_centos sshd[2110]: error: fork: Cannot allocate memory
```

## 可能原因

可能是进程数超限导致。系统内部的总进程数达到了 `pid_max` 时，再创建新进程时会报 “fork：Cannot allocate memory” 错。

## 解决思路

1. 参见 处理步骤，查看实例内存使用率是否过高。
2. 核实总进程数是否超限，并修改总进程数 `pid_max` 配置。

## 处理步骤

1. 参见 内存使用率过高问题处理 ，查看实例是否内存使用率过高。若实例内存使用率正常，则执行下一步。
2. 执行以下命令，查看系统 `pid_max` 值。

```
sysctl  -a | grep pid_max
```

根据返回结果，进行对应操作：

- 返回结果如下图所示， `pid_max` 默认值为32768，请执行下一步。

```
[root@VM-55-2-centos ~]# sysctl -a | grep pid_max
kernel.pid_max = 32768
```

- 返回报错信息 “fork：Cannot allocate memory”，则需执行以下命令，临时调大 `pid_max` 。

```
echo 42768 > /proc/sys/kernel/pid_max
```

您可再次执行命令，查看系统 `pid_max` 值。

3. 执行以下命令，查看系统内部总进程数。

```
pstree -p | wc -l
```

若总进程数达到了 `pid_max` ，则系统在创建新进程时会报 “fork Cannot allocate memory” 错误。

> **说明**
> 您可执行以下命令，定位启动进程较多的程序。

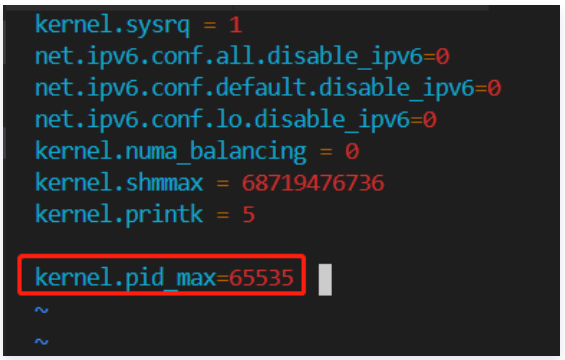
```
ps -efL
```

4. 将 `/etc/sysctl.conf` 配置文件中的 `kernel.pid_max` 值修改为65535，以增加进程数。

   执行以下命令，设置系统 pid_max 值。

```
echo "kernel.pid_max=65535" >> /etc/sysctl.conf
```

   修改完成后如下图所示：




5. 执行以下命令，使配置立即生效。

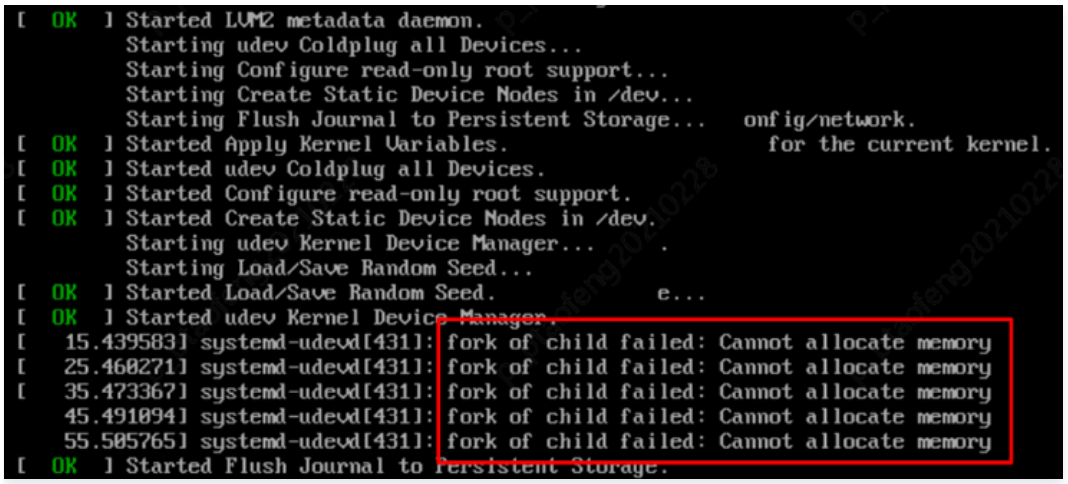
```
sysctl -p
```

# VNC 登录报错 Cannot allocate memory

最近更新时间：2024-08-22 10:41:51

## 现象描述

使用 VNC 登录云服务器时，无法正常进入系统，且出现 **Cannot allocate memory** 报错信息。如下图所示：




## 可能原因

可能是系统中存在多个大页内存导致。一个大页内存默认占用2048KB，根据 `/etc/sysctl.conf` 里的大页内存个数计算，以下图为例，1280个大页内存等于2.5GB。如果实例的配置较低，但仍将2.5GB分配给大页内存池（Huge Pages pool），则将导致系统没有可用内存，重启后无法进入系统。

您可以参考参见 故障处理，查看总进程数是否超限，核实大页内存配置，并修改为合适的配置。

## 故障处理

1. 参见 日志报错 fork：Cannot allocate memory，核实进程数是否超限。若进程数未超限，则执行下一步。
2. 使用单用户模式登录云服务器，详情请参见 设置 Linux 云服务器进入单用户模式 。
3. 执行以下命令，参见 可能原因 核实大页内存配置。

   ```
   cat /etc/sysctl.conf | grep hugepages
   ```

   若存在多个大页内存，则请按照以下步骤修改配置。
4. 执行以下命令，使用 VIM 编辑器打开 `/etc/sysctl.conf` 配置文件。

   ```
   vim /etc/sysctl.conf
   ```

5. 按 **i** 进入编辑模式，结合实例实际配置将 `vm.nr_hugepages` 配置项调低至合理数值。
6. 按 **Esc** 并输入 **:wq** 后，按 **Enter** 保存并退出 VIM 编辑器。
7. 执行以下命令，使配置立即生效。

```
sysctl -p
```

8. 配置完成后，重启云服务器即可恢复登录。

## 实例内存未耗尽时触发 Out Of Memory

最近更新时间：2024-09-24 15:05:29

## 现象描述

Linux 云服务器在内存使用率未占满的情况下触发了 OOM（Out Of Memory）。如下图所示：

```
kernel: Out of memory: Kill process 802931 (java) score 620 or sacrifice chilo
kernel: Killed process 802931 (java) total-vm:9125940kB, anon-rss:5114236kB, f
```

## 可能原因

| 可能原因 | 处理措施 |
| --- | --- |
| 内存使用率过高 | 检查内存使用率是否过高 |
| 进程数超限 | 检查进程数是否超限 |
| 系统可用内存低于 min_free_kbytes 值 | 检查系统可用内存是否低于 min_free_kbytes 值 |

## 故障处理

### 检查内存使用率是否过高

参见 内存使用率过高问题处理 ，查看实例是否内存使用率过高。若实例内存使用率正常，请 检查进程数是否超限 。

### 检查进程数是否超限

1. 参见 日志报错 fork：Cannot allocate memory，核实进程数是否超限。若总进程数未超限，则执行下一步。
2. 登录云服务器，执行以下命令查看 `min_free_kbytes` 值。

```
sysctl -a | grep min_free
```

`min_free_kbytes` 值单位为 kbytes，下图所示 `min_free_kbytes = 1024000` 即为1GB。

```
[root@[redacted]]# sysctl -a | grep min_free
vm.min_free_kbytes = 1024000
```

3. 执行以下命令，使用 VIM 编辑器打开 `/etc/sysctl.conf` 配置文件。

```
vim /etc/sysctl.conf
```

4. 按 i 进入编辑模式，修改 `vm.min_free_kbytes` 配置项。若该配置项不存在，则直接在配置文件中增加即可。

> **说明**
> 建议修改 `vm.min_free_kbytes` 值为不超过总内存的1%即可。

5. 按 Esc 并输入 :wq 后，按 Enter 保存并退出 VIM 编辑器。
6. 执行以下命令，使配置生效即可。

```
sysctl -p
```

### 检查系统可用内存是否低于 min_free_kbytes 值

可能是由系统可用内存低于 `min_free_kbytes` 值导致。`min_free_kbytes` 值表示强制 Linux 系统最低保留的空闲内存（Kbytes），如果系统可用内存低于设定的 `min_free_kbytes` 值，则默认系统启动 oom-killer 或强制重启。具体行为由内核参数 `vm.panic_on_oom` 值决定：

- 若 `vm.panic_on_oom=0` ，则系统会提示 OOM，并启动 oom-killer 杀掉占用最高内存的进程。
- 若 `vm.panic_on_oom =1` ，则系统会自动重启。

# 网络相关故障
# 国际链路时延

最近更新时间：2024-11-06 20:44:52

## 现象描述

北美地域云服务器登录时延太长。

## 可能原因

因全国国际路由出口较少及其他原因，当并发数大时，国际链路会非常拥塞并导致访问不稳定。腾讯云已经将此情况反馈至运营商。
目前，如果您购买了北美地域云服务器，需要在国内进行管理运维，可通过使用在中国香港地域购买的云服务器中转登录您购买的北美地域云服务器解决该问题。

## 故障处理

1. 购买中国香港地域的 Windows 云服务器，用作 “跳板机” 。

> **注意：**
> - 在**自定义配置**页的**1.选择地域与机型**中，选择**中国香港**地域。
> 点此进行选购 >>
> - Windows 云服务器支持登录北美地域的 Windows 和 Linux 云服务器，推荐选购。
> - **购买中国香港地域的 Windows 云服务器时，需要购买至少1Mbps的带宽，否则跳板机无法登录。**

2. 购买成功后，根据实际需求，选择登录中国香港地域 Windows 云服务器的方式：
   - 使用 RDP 文件登录 Windows 云服务器
   - 使用远程桌面连接登录 Windows 云服务器
   - 使用 VNC 登录 Windows 云服务器
3. 在中国香港地域的 Windows 云服务器内，根据实际需求，选择登录您位于北美地域云服务器的方式：
   - 登录北美地域的 Linux 云服务器
     - 使用标准登录方式登录 Linux 云服务器
     - 使用远程登录软件登录 Linux 云服务器
     - 使用 VNC 登录 Linux 云服务器
   - 登录北美地域的 Windows 云服务器
     - 使用 RDP 文件登录 Windows 云服务器
     - 使用远程桌面连接登录 Windows 云服务器
     - 使用 VNC 登录 Windows 云服务器

版权所有：腾讯云计算（北京）有限责任公司

# 网站无法访问

最近更新时间：2025-06-16 17:00:22

本文档为您介绍如何排查及定位网络无法访问的问题。

## 可能原因

| 可能原因 | 处理措施 |
| --- | --- |
| 服务器关机、硬件故障、CPU、内存和带宽使用率过高造成网站无法访问 | 检查并排查服务器相关问题 |
| 因丢包或延时高造成网站无法访问 | 检查并排查网络相关问题 |
| 安全组端口未放通造成网络无法访问 | 检查并排查安全组设置相关问题 |
| 防火墙端口限制导致网站无法访问 | 检查并排查防火墙设置相关问题 |
| 域名未备案和解析造成网络无法访问 | 检查并排查域名备案和解析相关问题 |

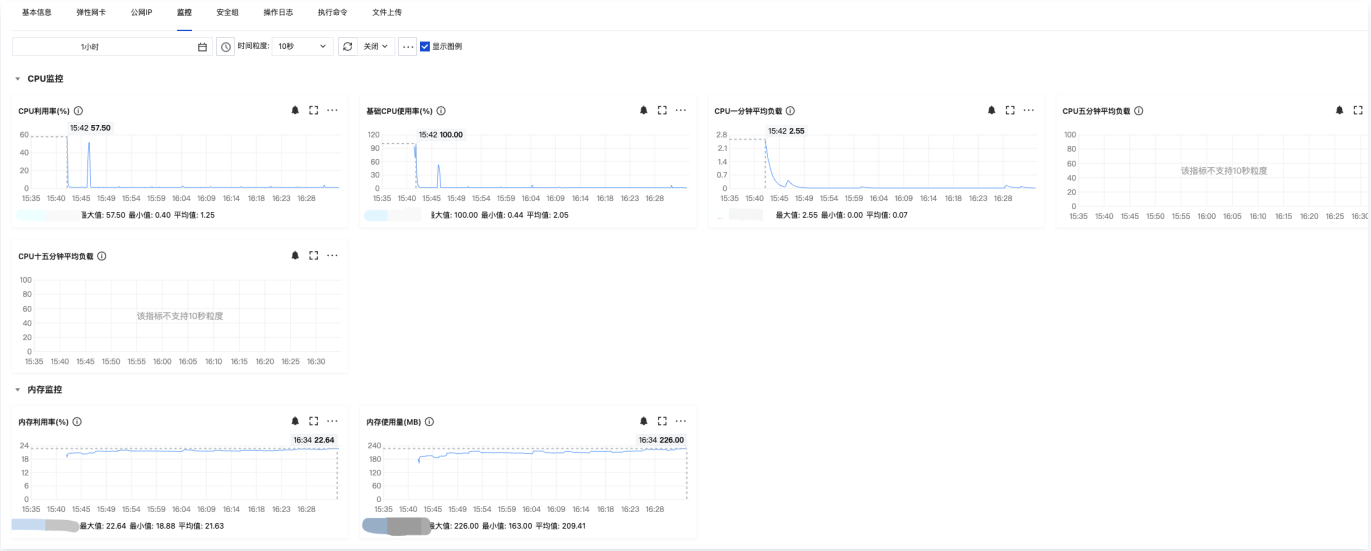
## 故障处理

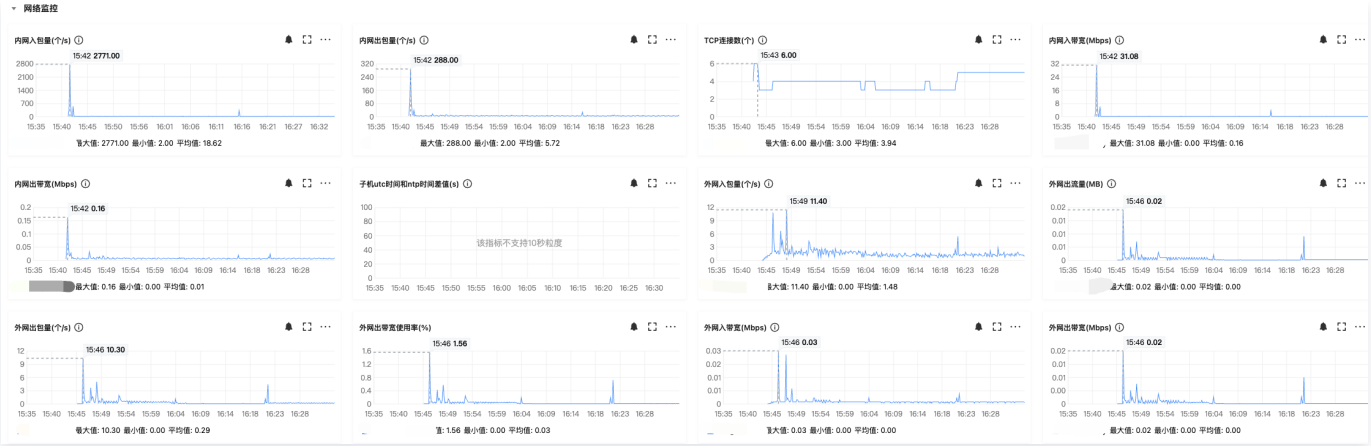
### 检查并排查服务器相关问题

服务器关机、硬件故障、CPU、内存和带宽使用率过高都可能造成网站无法访问，因此建议您依次排查服务器的运行状态、CPU、内存和带宽的使用情况。

1. 登录 云服务器控制台 ，并在实例的管理页面查看实例的运行情况是否正常。如下图所示：

   - 实例的运行情况正常，请执行 步骤2 。
   - 实例的运行情况异常，请重启云服务器实例。
2. 单击实例的 ID/实例名，进入该实例的详情页面。
3. 选择**监控**页签，查看 CPU、内存和带宽的使用情况。如下图所示：






- 如果存在 CPU/内存使用过高的情况，请参见 Windows 实例：CPU 与内存占用率高导致无法登录 和 Linux 实例：CPU 与内存占用率高导致无法登录 进行排查。
- 如果存在带宽使用过高的情况，请参见 带宽占用高导致无法登录 进行排查。
- 如果 CPU/内存/带宽的使用情况正常，请执行 步骤4 。

4. 执行以下命令，检查 Web 服务相应的端口是否被正常监听。

> **说明：**
> 以下操作以 HTTP 服务常用的80端口为例。

- Linux 实例：执行 `netstat -ntulp |grep 80` 命令。如下图所示：

```
[root@VM_2_184_centos ~]# netstat -ntulp |grep 80
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      1309/httpd
```

- Windows 实例：打开 CMD 命令行工具，执行 `netstat -ano|findstr :80` 命令。如下图所示：

```
C:\Users\Administrator>netstat -ano|findstr :80
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    10.135.182.70:53406    10.225.30.181:80       TIME_WAIT       0
  TCP    10.135.182.70:53419    10.225.30.181:80       TIME_WAIT       0
  TCP    10.135.182.70:53423    10.225.30.181:80       TIME_WAIT       0
  TCP    [::]:80                [::]:0                 LISTENING       4
```

  - 如果端口被正常监听，请执行 步骤5 。
  - 如果端口没有被正常监听，请检查 Web 服务进程是否启动或者正常配置。

5. 检查防火墙设置，是否放行 Web 服务进程对应的端口。
   - Linux 实例：执行 `iptables -vnL` 命令，查看 iptables 是否放通80端口。
     - 若已放通80端口，请 检查并排查网络相关问题 。
     - 若未放通80端口，请执行 `iptables -I INPUT 5 -p tcp  --dport 80 -j ACCEPT` 命令，放通80端口。
   - Windows 实例：在操作系统界面，单击**开始** > **控制面板** > **防火墙设置**，查看 Windows 防火墙是否关闭。
     - Windows 防火墙已关闭，请 检查并排查网络相关问题 。
     - Windows 防火墙未关闭，请关闭防火墙设置。

## 检查并排查网络相关问题

网络相关问题也有可能引起网站无法访问，您可以执行以下命令，检查网络是否有丢包或延时高的情况。

```
ping 目的服务器的公网 IP
```

- 如果返回类似如下结果，则表示存在丢包或延时高的情况，请使用 MTR 进一步进行排查。具体操作请参见 云服务器网络延迟和丢包 。

```
MB0:~ chenhuiping$ ping 193.112.12.138
.12.138 (193.112.12.138): 56 data bytes
64 bytes from 193.112.12.138: icmp_seq=0 ttl=43 time=161.240 ms
64 bytes from 193.112.12.138: icmp_seq=1 ttl=43 time=161.996 ms
64 bytes from 193.112.12.138: icmp_seq=2 ttl=43 time=164.837 ms
64 bytes from 193.112.12.138: icmp_seq=3 ttl=43 time=215.650 ms
64 bytes from 193.112.12.138: icmp_seq=4 ttl=43 time=166.375 ms
64 bytes from 193.112.12.138: icmp_seq=5 ttl=43 time=160.576 ms
64 bytes from 193.112.12.138: icmp_seq=6 ttl=43 time=161.016 ms
64 bytes from 193.112.12.138: icmp_seq=7 ttl=43 time=164.129 ms
64 bytes from 193.112.12.138: icmp_seq=8 ttl=43 time=192.682 ms
64 bytes from 193.112.12.138: icmp_seq=9 ttl=43 time=163.376 ms
64 bytes from 193.112.12.138: icmp_seq=10 ttl=43 time=161.859 ms
^C
--- 193.112.12.138 ping statistics ---
11 packets transmitted, 11 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 160.576/170.340/215.650/16.765 ms
```

- 如果没有丢包或延时高的情况，请 检查并排查安全组设置相关问题 。

## 检查并排查安全组设置相关问题

安全组是一个虚拟防火墙，可以控制关联实例的入站流量和出站流量。安全组的规则可以指定协议、端口、策略等。如果您没有放通 Web 进程相关的端口也会造成网站无法访问。

1. 登录 云服务器控制台 ，并在**实例列表**页面单击实例的 ID/实例名，进入该实例的详情页面。
2. 选择**安全组**页签，查看绑定的安全组以及对应安全组的出站和入站规则，确认是否放通 Web 进程相关的端口。如下图所示：

- 已放通 Web 进程相关的端口，请 检查并排查防火墙设置相关问题 。
- 未放通 Web 进程相关的端口，请修改安全组设置，放通 Web 进程相关的端口。

## 检查并排查防火墙设置相关问题

`iptables` 是 Linux 中常用的防火墙软件，可通过直接配置的方式进行设置。

1. 执行以下命令以查看 `iptables` 的四张表，如下图所示：

```
iptables -t filter -nvL
iptables -t nat -nvL
iptables -t mangle -nvL
iptables -t raw -nvL
```

```
[root@VM-0-15-tencentos ~]# iptables -t filter -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  *      *       0.0.0.0/0            8.8.8.8

Chain YJ-FIREWALL-INPUT (0 references)
 pkts bytes target     prot opt in     out     source               destination
[root@VM-0-15-tencentos ~]# iptables -t nat -nvL
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
[root@VM-0-15-tencentos ~]# iptables -t mangle -nvL
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
[root@VM-0-15-tencentos ~]# iptables -t raw -nvL
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

2. 请在表中检查是否有 drop 记录以及具体的 drop 规则。例如，以下案例记录了 IP 地址 8.8.8.8 被 iptables 拦截的情况，如下图所示：

```
[root@VM-0-15-tencentos ~]# iptables -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x17/0x02 match-set YJ-FIREWALL-BLOCK src,dst
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x17/0x02 match-set YJ-GLOBAL-INBLOCK src

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x17/0x02 match-set YJ-GLOBAL-OUTBLOCK dst
    2   168 DROP       all  --  *      *       0.0.0.0/0            8.8.8.8
```

3. 如果发现非预期的拦截，可以手动执行以下类似命令清除掉 iptables 规则，如下图所示：

```
iptables -D OUTPUT -d 8.8.8.8 -j DROP
```

```
[root@VM-0-15-tencentos ~]# iptables -D OUTPUT -d 8.8.8.8 -j DROP
[root@VM-0-15-tencentos ~]# iptables -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x17/0x02 match-set YJ-FIREWALL-BLOCK src,dst
    1    40 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x17/0x02 match-set YJ-GLOBAL-INBLOCK src

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       tcp  --  *      *       0.0.0.0/0            0.0.0.0/0            tcp flags:0x17/0x02 match-set YJ-GLOBAL-OUTBLOCK dst

Chain YJ-FIREWALL-INPUT (0 references)
 pkts bytes target     prot opt in     out     source               destination
```

4. 除非有特殊需求，建议仅通过安全组对公有云进行访问控制，并关闭内部防火墙。在完全关闭之前，请记得手动以下命令进行临时备份，以防意外删除部分规则。

```
//内部关闭防火墙命令
iptables -t filter -F
iptables -t nat -F
iptables -t raw -F
iptables -t mangle -F

//备份防火墙命令
iptables-save > iptables-save.bak
```

## 检查并排查域名备案和解析相关问题

排查了 服务器相关问题 、网络相关问题 和 安全组设置相关问题 后，您可以尝试使用云服务器的公网 IP 进行访问。如果使用 IP 地址可以访问，而使用域名访问失败，则可能是域名备案或者解析相关问题造成网站无法访问。

1. 国家工信部规定，对未取得许可或者未履行备案手续的网站不得从事互联网信息服务，否则就属于违法行为。为不影响网站长久正常运行，如需开办网站，建议您先办理网站备案，待备案成功取得通信管理局下发的 ICP 备案号后，才开通访问。
   - 如果您的域名没有备案，请先进行 域名备案 。
   - 如果您使用的是腾讯云的域名服务，您可以登录 域名管理控制台 查看相应的域名情况。
   - 如果您的域名已备案，请执行 步骤2 。
2. 参见 解析生效相关 ，排查解析相关问题。

- 如果已解决网站无法访问的问题，则任务完成。
- 如果仍无法解决网站无法访问的问题，请通过 在线支持 反馈。

# 网站访问卡慢

最近更新时间：2025-06-03 11:17:42

## 现象描述

网站访问卡慢。

## 可能原因

一次完整的 HTTP 请求包括域名解析、建立 TCP 连接、发起请求、服务器接收到请求进行处理并返回处理结果、浏览器对 HTML 代码进行解析并请求其他资源，以及对页面进行渲染呈现。其中，HTTP 的请求过程经历了用户本地客户端、客户端到接入服务器之间的网络节点以及服务器。在这三个环节中，任意一个环节出现问题都有可能导致网站访问卡慢。

| 可能原因 | 处理措施 |
| --- | --- |
| 本地网络异常 | 检查并测试本地客户端访问域名的速度 |
| 网络链路存在丢包或延时高的情况 | 检查是否因为网络链路存在丢包或延时高的情况 |
| 实例 CPU、内存、宽带使用过高 | 检查并登录服务器查看实例资源的使用情况 |
| 服务器负载引起资源消耗增大 | 检查并判断是否因为服务器负载引起资源消耗增大 |

## 故障处理

### 检查并测试本地客户端访问域名的速度

1. 通过本地客户端访问 华佗诊断分析系统，测试本地访问各域名的速度。
2. 根据测试结果，确认本地网络是否存在问题。
   测试结果示意图如下：

以下是腾讯域名测试结果

| | |
|---|---|
| i.gtimg.cn: | 网络正常，延时46毫秒 |
| cloud.tencent.com: | 网络正常，延时222毫秒 |
| imgcache.qq.com: | 网络正常，延时230毫秒 |
| buluo.qq.com: | 网络正常，延时253毫秒 |
| qzone.qq.com: | 网络正常，延时186毫秒 |
| now.qq.com: | 网络正常，延时140毫秒 |
| www.qq.com: | 网络正常，延时62毫秒 |
| qianbao.qq.com: | 网络正常，延时47毫秒 |
| v.qq.com: | 网络正常，延时200毫秒 |
| mail.qq.com: | 网络正常，延时102毫秒 |
| qpay.qq.com: | 网络正常，延时17毫秒 |
| qun.qq.com: | 网络正常，延时44毫秒 |
| mmbiz.qpic.cn: | 网络正常，延时67毫秒 |
| puui.qpic.cn: | 网络正常，延时105毫秒 |
| inews.gtimg.com: | 网络正常，延时145毫秒 |
| emoji.qpic.cn: | 网络正常，延时173毫秒 |
| captcha.gtimg.com: | 网络正常，延时206毫秒 |

以下是其他域名测试结果

| | |
|---|---|
| www.baidu.com: | 网络正常，延时59毫秒 |
| www.youku.com: | 网络正常，延时247毫秒 |
| www.zhihu.com: | 网络正常，延时86毫秒 |
| www.163.com: | 网络正常，延时442毫秒 |

我们可从结果中获知访问各个域名的延时情况，以及网络是否正常。

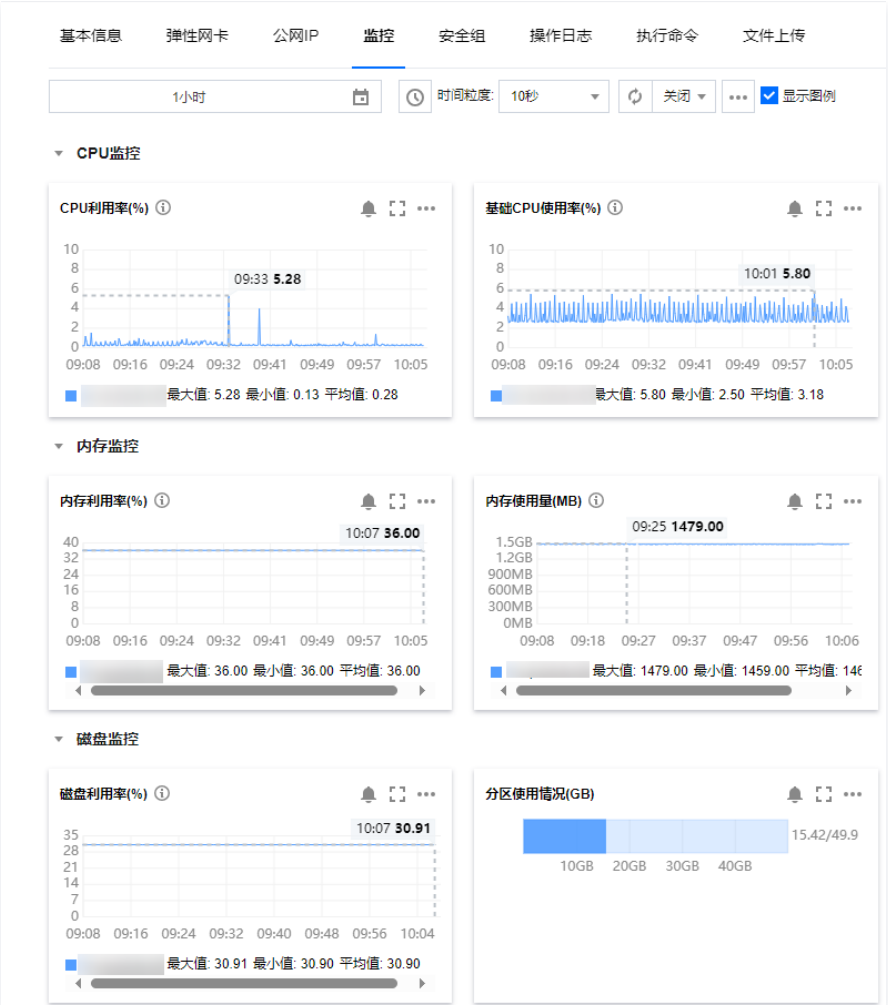
- 如果网络异常，请联系您的网络服务提供商协助定位解决。
- 如果出现丢包或网络延时高，请 检查是否因为网络链路存在丢包或延时高的情况 。

## 检查是否因为网络链路存在丢包或延时高的情况

1. 通过本地客户端 ping 服务器公网 IP，确认是否存在丢包或延时高的情况。
   - 若存在丢包或延时高的情况，请使用 MTR 进行诊断，具体操作可参见 服务器网络延迟和丢包处理 。
   - 若不存在丢包或延时高的情况，请执行 步骤2 。
2. 使用 `dig/nslookup` 命令，查看 DNS 的解析情况，排查是否是 DNS 解析引起的问题。
   您也可以直接使用公网 IP 访问对应页面，排查是否为 DNS 的问题导致网站访问卡慢。
   - 若是 DNS 的问题导致网站访问卡慢，请检查 DNS 解析，具体操作可参见 解析生效相关 。
   - 若不是 DNS 的问题导致网站访问卡慢，请 检查并登录服务器查看实例资源的使用情况 。

## 检查并登录服务器查看实例资源的使用情况

1. 登录 云服务器控制台 。
2. 选择待检查实例的 ID/实例名，进入该实例详情页面。
3. 在实例的详情页面，选择**监控**页签，查看实例资源的使用情况。如下图所示：




- 如果存在 CPU/内存使用过高的情况，请参见 Windows 实例：CPU 与内存占用率高导致无法登录 或 Linux 实例：CPU 与内存占用率高导致无法登录 进行排查。
- 如果存在带宽使用过高的情况，请参见 带宽占用高导致无法登录 进行排查。
- 如果实例资源消耗增大，请 检查并判断是否因为服务器负载引起资源消耗增大 。

## 检查并判断是否因为服务器负载引起资源消耗增大

根据实例资源使用情况，判断是否为服务器负载引起资源消耗增大。

- 若是服务器负载引起资源消耗增大，建议优化业务程序或 升级服务器配置 。您也可以通过购买新的服务器，分担现有服务器的压力。
- 若不是服务器负载引起资源消耗增大，建议查看日志文件，定位问题并进行针对性的优化。

# 网卡多队列配置错误问题

最近更新时间：2024-03-26 16:49:28

## 现象描述

云服务器网卡多队列配置错误。

## 可能原因

云服务器默认配置网卡多队列，该方式把网卡中断分布至不同的 CPU，可提升网络处理性能。可能存在人为修改的情况，导致网卡多队列配置错误。您可以参见 故障处理，修正网卡队列个数。

## 故障处理

以下步骤云服务器默认主网卡为 `eth0`，网卡队列个数为2。

1. 执行以下命令，查看当前网卡队列个数。

```
ethtool -l eth0
```

返回如下结果，表示当前队列个数设置小于最大网卡队列个数，设置不合理，需进行修复。

```
Channel parameters for eth0:
Pre-set maximums:
RX:             0
TX:             0
Other:          0
Combined:       2          ### 服务器支持的最大网卡队列个数
Current hardware settings:
RX:             0
TX:             0
Other:          0
Combined:       1         ###当前设置的网卡队列个数
```

2. 执行以下命令，设置当前网卡队列个数。

```
ethtool -L eth0  combined 2
```

命令中队列数设置为2，可根据实际情况调整，设置值为服务器支持的最大网卡队列个数。

3. 执行以下命令，检查当前网卡队列个数配置。

```
ethtool -l eth0
```

服务器支持的最大网卡队列个数与当前设置的网卡队列个数相等，即为配置成功。

# 使用 MTR 分析网络延迟及丢包

最近更新时间：2025-06-03 11:17:42

## 问题描述

本地访问云服务器，或者在云服务器上访问其他网络资源时，发现网络卡顿。使用 `ping` 命令，发现网络存在丢包或时延较高的情况。

## 问题分析

丢包或时延较高可能是骨干链路拥塞、链路节点故障、服务器负载高、系统设置问题等原因引起。在排除云服务器自身原因后，您可以使用 MTR 进行进一步诊断。
MTR 是一款网络诊断工具，其工具诊断出的报告可以帮助您确认网络问题的症结所在。

## 解决方案

本文档以 Linux 和 Windows 云服务器为例，介绍如何使用 MTR 以及如何对 MTR 的报告结果进行分析。

> **说明**
> 如果本地或云服务器禁用 Ping，则 MTR 将无结果。

请根据运行 MTR 的主机操作系统的不同，查看 MTR 的介绍和使用方法。

WinMTR 的介绍和使用（Windows 操作系统）

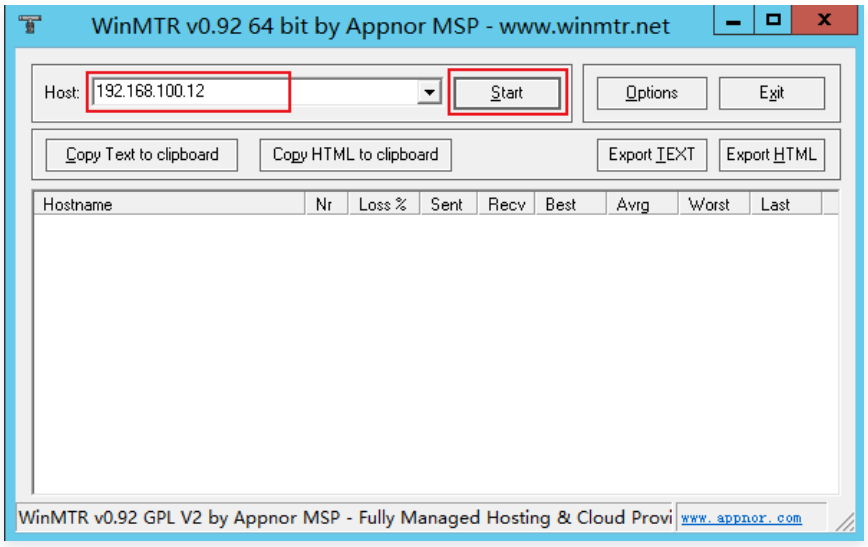
**WinMTR**：适用于 Windows 系统的免费网络诊断工具，集成了 Ping 和 tracert 的功能，具有图形界面，可以直观地看到各个节点的响应时间和丢包情况。

### 安装 WinMTR

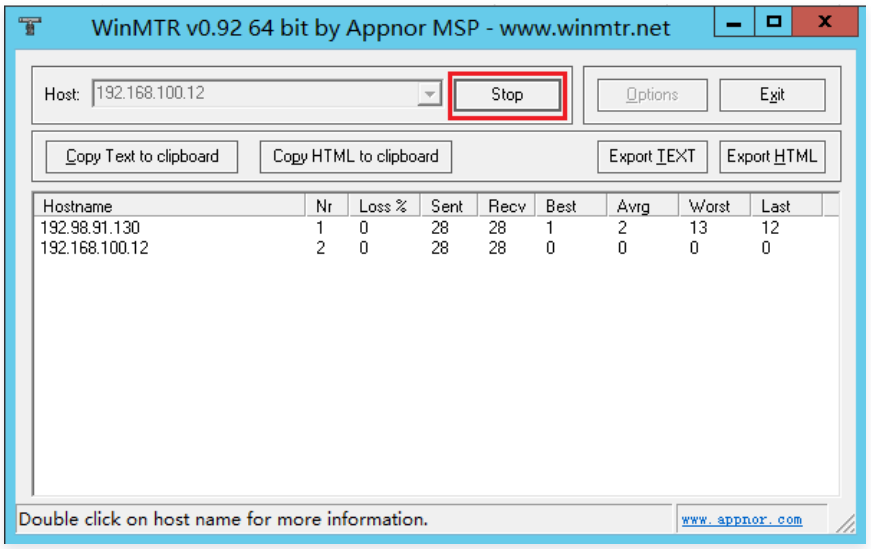
1. 登录 Windows 云服务器 。
2. 在操作系统界面，通过浏览器访问官方网站（或合法渠道）下载对应操作系统类型的 WinMTR 安装包。
3. 解压缩 WinMTR 安装包。

### 使用 WinMTR

1. 双击 WinMTR.exe，打开 WinMTR 工具。
2. 在 WinMTR 窗口的 Host 处，输入目的服务器 IP 或者域名，单击 **Start**。如下图所示：



3. 根据实际情况，等待 WinMTR 运行一段时间，单击 **Stop**，结束测试。如下图所示：




测试结果的主要信息如下：

- **Hostname**：到目的服务器要经过的每个主机 IP 或名称。
- **Nr**：经过节点的数量。
- **Loss%**：对应节点的丢包率。
- **Sent**：发送的数据包数量。
- **Recv**：接收到响应的数量。
- **Best**：最短的响应时间。
- **Avrg**：平均响应时间。
- **Worst**：最长的响应时间。
- **Last**：最近一次的响应时间。

MTR 的介绍和使用（Linux 操作系统）

**MTR**：Linux 平台上诊断网络状态的工具，继承了 Ping、traceroute、nslookup 的功能，默认使用 ICMP 包测试两个节点之间的网络连接情况。

### 安装 MTR

目前现有的 Linux 发行版本都预装了 MTR，如果您的 Linux 云服务器没有安装 MTR，则可以执行以下命令进行安装：

- CentOS 操作系统：

```
yum install mtr
```

- Ubuntu 操作系统：

```
sudo apt-get install mtr
```

### MTR 相关参数说明

- **-h/--help**：显示帮助菜单。
- **-v/--version**：显示 MTR 版本信息。
- **-r/--report**：结果以报告形式输出。
- **-p/--split**：与 **--report** 相对，分别列出每次跟踪的结果。
- **-c/--report-cycles**：设置每秒发送的数据包数量，默认是10。
- **-s/--psize**：设置数据包的大小。
- **-n/--no-dns**：不对 IP 地址做域名解析。

- **-a/--address**：用户设置发送数据包的 IP 地址，主要用户单一主机多个 IP 地址的场景。
- **-4**：IPv4
- **-6**：IPv6

**使用示例**

以本机到 IP 为119.xx.xx.xx的服务器为例。
执行以下命令，以报告形式输出 MTR 的诊断报告。

```
mtr 119.xx.xx.xx --report
```

返回类似如下信息：

```
[root@VM_103_80_centos ~]# mtr 119.xx.xx.xx --report
Start: Mon Feb  5 11:33:34 2019
HOST:VM_103_80_centos            Loss%   Snt   Last   Avg  Best  Wrst StDev
1.|-- 100.xx.xx.xx                0.0%    10    6.5   8.4   4.6  13.7   2.9
2.|-- 100.xx.xx.xx                0.0%    10    0.8   8.4   0.6   1.1   0.0
3.|-- 10.xx.xx.xx                 0.0%    10    0.4   8.4   0.4   2.5   0.6
4.|-- 10.xx.xx.xx                 0.0%    10    1.6   8.4   1.4   1.6   0.0
5.|-- 14.xx.xx.xx                 0.0%    10    1.0   8.4   1.0   4.1   0.9
6.|-- 14.xx.xx.xx                 0.0%    10    4.1   8.4   3.3  10.2   1.9
7.|-- 113.xx.xx.xx                0.0%    10    5.8   8.4   3.1  10.1   2.1
8.|-- 113.xx.xx.xx                0.0%    10    3.9   8.4   3.9  11.0   2.5
9.|-- 202.xx.xx.xx               30.0%    10    2.4   8.4   2.4   2.5   0.0
10.|-- 202.xx.xx.xx               0.0%    10    3.5   4.6   3.5   7.0   1.2
11.|-- 202.xx.xx.xx               0.0%    10  164.7   8.4 161.3 165.3   1.2
12.|-- 202.xx.xx.xx               0.0%    10  162.3   8.4 161.7 167.8   2.0
13.|-- ix-xe-10-2-6-0.tcore2.LVW 10.0%    10  168.4   8.4 161.5 168.9   2.3
14.|-- 180.xx.xx.xx              10.0%    10  348.1   8.4 347.7 350.2   0.7
15.|-- 180.xx.xx.xx               0.0%    10  345.0   8.4 343.4 345.0   0.3
16.|-- 180.xx.xx.xx               0.0%    10  187.4   8.4 187.3 187.6   0.0
17.|-- ???                     100.0%    10    0.0   8.4   0.0   0.0   0.0
18.|-- 100.xx.xx.xx               0.0%    10  187.7   8.4 187.3 194.0   2.5
19.|-- 119.xx.xx.xx               0.0%    10  186.5   8.4 186.4 186.5   0.0
```

主要输出的信息如下：

- **HOST**：节点的 IP 地址或域名。
- **Loss%**：丢包率。
- **Snt**：每秒发送的数据包的数量。
- **Last**：最近一次的响应时间。
- **Avg**：平均响应时间。
- **Best**：最短的响应时间。
- **Wrst**：最长的响应时间。
- **StDev**：标准偏差，偏差值越高，说明各个数据包在该节点的响应时间相差越大。

## 报告结果分析及处理

> **说明**
> 由于网络状况的非对称性，遇到本地到服务器的网络问题时，建议您收集双向的 MTR 数据（从本地到云服务器以及云服务器到本地）。

1. 根据报告结果，查看目的服务器 IP 是否丢包。
   - 如果目的地没有丢包，则表示网络正常。
   - 如果目的地发生丢包，则执行 步骤2 。
2. 往上查看报告结果，定位第一次丢包的节点。

- 如果丢包发生在目的服务器，则可能是目的服务器的网络配置不当引起，请检查目的服务器的防火墙配置。
- 如果丢包开始于前三跳，一般为本地运营商网络问题，建议检查访问其他网址是否存在相同情况。如果存在相同情况，请反馈给您的运营商进行处理。
- 如果有频繁丢包的情况，确实为网络不稳定的场景，则请 提交工单 进行咨询，并附上测试截图，以便工程师进行定位。

# 云服务器网络访问丢包

最近更新时间：2025-05-26 19:42:53

本文主要介绍可能引起云服务器网络访问丢包问题的可能原因及对应解决方法。

## 可能原因

引起云服务器网络访问丢包问题的可能原因如下：

| 可能原因 | 处理措施 |
| --- | --- |
| 触发限速导致 TCP 丢包 | 检查是否触发限速导致 TCP 丢包 |
| 触发限速导致 UDP 丢包 | 检查是否触发限速导致 UDP 丢包 |
| 触发软中断丢包 | 检查是否触发软中断丢包 |
| UDP 发送缓冲区满导致丢包 | 检查是否 UDP 发送缓冲区满导致丢包 |
| UDP 接收缓冲区满 | 检查是否 UDP 接收缓冲区满导致丢包 |
| TCP 全连接队列满导致丢包 | 检查是否 TCP 全连接队列满导致丢包 |
| TCP 请求溢出导致丢包 | 检查是否 TCP 请求溢出导致丢包 |
| 连接数达到上限导致丢包 | 检查是否连接数达到上限导致丢包 |
| iptables policy 设置的规则导致丢包 | 检查 iptables policy 设置的规则 |
| firewalld 是否开启 | 检查 firewalld 是否开启 |

## 故障处理

在进行问题定位及处理前需登录实例，详情请参见 登录 Linux 实例 及 登录 Windows 实例 。

### 检查是否触发限速导致 TCP 丢包

云服务器实例具备多种规格，且不同规格有不同的网络性能。当实例的带宽或流量超过实例规格对应的标准时，会触发平台侧的限速，导致丢包。排查及处理步骤如下：

1. 查看实例的带宽及包量。
   Linux 实例可执行 `sar -n DEV 2` 命令查看带宽及包量。其中，`rxpck/s` 和 `txpck/s` 指标是收发包量，`rxkB/s` 和 `txkB/s` 指标是收发带宽。
2. 使用获取的带宽及包量数据对比 实例规格，查看是否达到实例规格性能瓶颈。
   - 若已达到实例规格性能瓶颈，则需升级实例规格或调整业务量。
   - 若未达到实例规格性能瓶颈，则可通过 在线支持 进一步定位处理。

### 检查是否触发限速导致 UDP 丢包

参见 检查是否触发限速导致 TCP 丢包 步骤，判断是否由实例规格性能瓶颈引起丢包。

- 是否由实例规格性能瓶颈引起丢包，则需升级实例规格或调整业务量。
- 若未达到实例规格性能瓶颈，则可能是由平台对 DNS 请求额外的频率限制引起。在实例整体带宽或包量达到实例规格的性能瓶颈时，可能会触发 DNS 请求限速而出现 UDP 丢包。可通过 在线支持 进一步定位处理。

### 检查是否触发软中断丢包

当操作系统检测到 `/proc/net/softnet_stat` 的第二列计数值在增长时，则会判断为“软中断丢包”。当您的实例触发了软中断丢包时，可通过以下步骤进行排查及处理：

查看是否开启 RPS：

- 开启，则内核参数 `net.core.netdev_max_backlog` 偏小时会引发丢包，需调大。内核参数详细信息请参见 Linux 实例常用内核参数介绍 。
- 未开启，则查看是否为 CPU 单核软中断高，导致未能及时收发数据。若是，您可以：
  - 选择开启 RPS，使软中断分配更为均衡。
  - 检查业务程序是否会引发软中断分配不均匀。

### 检查是否 UDP 发送缓冲区满导致丢包

若您的实例因 UDP 发送缓冲区不足而导致丢包时，可通过以下步骤进行排查处理：

1. 使用 `nstat` 命令来查看 UDP 相关的统计信息。您可以通过 `nstat | grep Udp` 来查看与 UDP 有关的统计。
   以下是其中一些有关的参数及含义：
   - UdpInDatagrams：已接收的 UDP 数据包数量
   - UdpNoPorts：没有任何端口接收的 UDP 数据包数量
   - UdpInErrors：因数据包错误（如数据包长度错误，IP 校验和错误等）而不能交付的 UDP 数据包数量。
   - UdpOutDatagrams：已发送的 UDP 数据包数量
   - UdpRcvbufErrors：由于接收缓冲区满而不能接收的 UDP 数据包数量
   - UdpSndbufErrors：由于发送缓冲区满而不能发送的 UDP 数据包数量
2. 重点关注 `UdpSndbufErrors` 字段，该字段表示由于发送缓冲区满而不能发送的 UDP 数据包数量。如果该值较高或者持续增加，可能就是因为 UDP 发送缓冲区满而导致的丢包。
3. 如果 `UdpSndbufErrors` 字段较高或者持续增加，您可以尝试通过调大内核参数 `net.core.wmem_max` 和 `net.core.wmem_default` 来增加发送缓冲区的大小，并重启 UDP 程序以生效。具体如何调整内核参数可以参见 Linux 实例常用内核参数介绍 。
4. 验证发送缓冲区大小是否调整成功，执行 `ss -nump` 命令查看 UDP 的状态信息，该命令会显示出各个 UDP socket 的详细信息。
   输出中的部分信息如 `skmem:(r0 ,rb62914560,t0,tb62914560,f0,w0,o0,bl0)` 表明 socket 的内存使用情况，部分字段具体含义如下：
   - r: 已接收但还未读取的字节数（receive queue）
   - rb: 接收缓冲区大小 (receive buffer size)
   - t: 发送队列中等待发送的数据的字节数（send queue）
   - tb: 发送缓冲区大小 (send buffer size)

   确认发送缓冲区是否符合预期。
5. 若调整后仍存在丢包问题，再次使用 `nstat | grep UdpSndbufErrors` 命令查看 `UdpSndbufErrors` 字段，看其是否仍持续增加。若是，您需要检查业务代码是否通过 `setsockopt` 设置了 `SO_SNDBUF` 。如果已设置，您可能需要修改代码来增大 SO_SNDBUF 值。虽然您可以通过修改 `net.core.wmem_max` 和 `net.core.wmem_default` 参数来尝试增大发送缓冲区的大小，但是如果程序中 SO_SNDBUF 设置得过小，无论系统级别的缓冲区大小如何，都可能会因为此限制导致发送缓冲区满。

## 检查是否 UDP 接收缓冲区满导致丢包

若您的实例因 UDP 接收缓冲区不足而导致丢包时，可通过以下步骤进行排查处理：

1. 参见 检查是否 UDP 发送缓冲区满导致丢包 步骤，用 `nstat` 命令检查 `UdpRcvbufErrors` 字段。该字段表示由于接收缓冲区满而不能接收的 UDP 数据包数量。如果该值较高或者持续增加，可能是因为 UDP 接收缓冲区满而导致的丢包。
2. 如果 `UdpRcvbufErrors` 字段较高或者持续增加，您可以尝试通过调大内核参数 `net.core.rmem_max` 和 `net.core.rmem_default` 来增加接收缓冲区的大小，并重启 UDP 程序以生效。具体如何调整内核参数可以参见 Linux 实例常用内核参数介绍 。
3. 验证接收缓冲区大小是否调整成功，执行 `ss -nump` 命令查看 rb: 接收缓冲区大小 (receive buffer size)，确认接收缓冲区是否符合预期。
4. 若调整后仍存在丢包问题，再次使用 `nstat | grep UdpRcvbufErrors` 命令查看 `UdpRcvbufErrors` 字段，看其是否仍持续增加。若是，您需要检查业务代码是否通过 `setsockopt` 设置了 SO_RCVBUF。如果设置了，您可能需要修改代码来增大 SO_RCVBUF 值。这是因为虽然我们可以通过修改 `net.core.rmem_max` 和 `net.core.rmem_default` 参数来尝试增大接收缓冲区的大小，但是如果程序中 SO_RCVBUF设置得过小，那么无论系统级别的缓冲区大小如何，都可能会因为这个限制导致接收缓冲区满。

## 检查是否 TCP 全连接队列满导致丢包

当您的实例发生 TCP 全连接队列满导致丢包时，**优先检查业务应用是否处理延迟过大，业务进程 CPU 使用率是否过高**，造成无法及时接收新连接。
若已确认业务进程 CPU 使用率及处理延迟都较低，可以检查是否属于以下常见 Case：

1. 打开文件数目达到限制，可能会造成业务进程 Accept 失败，从而无法正常处理新增连接。这种情况，一般来说，系统日志里会有 **Too many open files** 的报错。注意，调整 open file 相关限制的时候，需要检查 `/etc/security/limits.conf` 中针对用户级别的限制和内核参数 fs.file-nr 针对系统级别的限制两个方面。
2. 业务层面负责处理新增连接的线程数有限制。常见于 Java 类业务。需要从业务层面调整线程数。

若不属于以上常见 Case，可尝试按以下步骤调整参数，以应对可能的请求突发造成的全连队列满丢包：

1. 调大内核参数 `net.core.somaxconn` 。内核参数详细信息请参见 Linux 实例常用内核参数介绍 。
2. 检查业务进程是否传入了 backlog 参数。若是，则相应调大。

## 检查是否 TCP 请求溢出导致丢包

在 TCP 接收数据时，若 socket 被 user 锁住，则会将数据送到 backlog 队列。若此过程失败，则会引起 TCP 请求溢出导致丢包。通常情况下，假设业务程序性能正常，则可参见以下方式从系统层面排查及处理问题：
检查业务程序是否通过 setsockopt 自行设置了 buffer 大小：

- 若已设置，且该值不够大，可以修改业务程序指定一个更大的值，或不再通过 setsockopt 指定大小。

> **说明**
> setsockopt 的取值受内核参数 `net.core.rmem_max` 和 `net.core.wmem_max` 限制。调整业务程序的同时，可以同步调整 `net.core.rmem_max` 和 `net.core.wmem_max` 。调整后请重启业务程序使配置生效。

- 若未设置，则可以调大 `net.ipv4.tcp_mem` 、 `net.ipv4.tcp_rmem` 和 `net.ipv4.tcp_wmem` 内核参数来调整 TCP socket 的水位。内核参数修改请参见 Linux 实例常用内核参数介绍 。

## 检查是否连接数达到上限导致丢包

云服务器实例具备多种规格，且不同规格有不同的连接数性能指标。当实例的连接数超过实例规格对应的标准时，会触发平台的限速，导致丢包。处理步骤如下：

> **说明**
> 连接数指宿主机上保存的云服务器实例的会话数，包含 TCP、UDP 和 ICMP。该数值大于在云服务器实例上通过 `ss` 或 `netstat` 命令获取的网络连接数。

查看您实例的连接数，并对比 实例规格 ，查看是否达到实例规格性能瓶颈。

- 若已达到实例规格性能瓶颈，则需升级实例规格或调整业务量。
- 若未达到实例规格性能瓶颈，则可通过 在线支持 进一步定位处理。

## 检查 iptables policy 设置的规则

在云服务器 iptables 未设置相关规则的情况下，可能是 iptables policy 相关规则设置导致到达云服务器的包都被丢弃。处理步骤如下：

1. 执行以下命令，查看 iptables policy 规则。

```
iptables -L | grep policy
```

iptables policy 规则默认为 ACCEPT。若 INPUT 链 policy 非 ACCEPT，则会导致所有到服务器的包都被丢弃。例如，若返回如下结果，表示进入云服务器的包都会被 drop。

```
Chain INPUT (policy DROP)
Chain FORWARD (policy ACCEPT)
Chain OUTPUT (policy ACCEPT)
```

2. 执行如下命令，按需调整 `-P` 后的值。

```
iptables -P INPUT ACCEPT
```

调整后，可再次执行 步骤1 命令查看，应返回如下结果：

```
Chain INPUT (policy ACCEPT)
Chain FORWARD (policy ACCEPT)
Chain OUTPUT (policy ACCEPT)
```

## 检查 firewalld 是否开启

在使用云服务器时，可能会遇到网络连接问题，这可能是由于防火墙（firewalld）设置不当导致的。在进行故障排查时，首先需要检查 firewalld 是否启动，然后确认规则是否是自己添加的还是误操作增加的，最后可以考虑关闭 firewalld。以下是详细的检查和处理步骤：

1. 确认 firewalld 是否启动， 执行以下命令，查看 firewalld 状态，如果 firewalld 已启动，输出结果会显示 **active (running)**，则继续检查。如果 firewalld 未启动，说明不是 firewalld 导致的问题，则不需要继续流程。

```
systemctl status firewalld
```

2. 使用 `iptables -nvL` 命令检查防火墙规则，通过查看输出结果，可以确认是否有自己添加的规则或误操作添加的规则。

```
iptables -nvL
```

3. 关闭 firewalld。

   如果确认规则是误操作添加的，可以先关闭 firewalld 后观察是否正常。执行以下命令关闭 firewalld。

```
systemctl stop firewalld
```

通过以上步骤，可以排查并解决由于 firewalld 设置不当导致的网络连接问题。在进行配置调整时，请务必谨慎操作，以免影响服务器的正常运行。

版权所有：腾讯云计算（北京）有限责任公司

# 实例 IP 地址 ping 不通

最近更新时间：2025-05-26 19:42:53

## 现象描述

无法 ping 通云服务器实例。

## 可能原因

在确保本地网络正常的情况下（即您可以正常 ping 通其他网站），出现上述现象的可能原因如下：

| 可能原因 | 处理措施 |
| --- | --- |
| 服务器内实例未配置公网 IP | 检查服务器内实例确保已配置公网 IP |
| 实例的安全组未设置 | 检查实例安全组确保已设置 |
| 系统内实例处于未设置状态 | 检查系统内实例确保处于设置状态 |
| 域名未备案 | 检查域名确保已备案 |
| 服务器内 Windows 实例网络未设置 | 检查服务器内 Windows 实例网络确保已设置 |
| 服务器内域名解析未正确配置 | 检查服务器内域名解析确保配置正确 |

## 故障处理

### 检查服务器内实例确保已配置公网 IP

> **说明：**
> 实例必须具备公网 IP 才能与 Internet 上的其他计算机相互访问。若实例没有公网 IP，外部则无法直接 ping 通实例。

1. 通过登录 云服务器控制台 检查服务器是否设置公网 IP。
2. 在**实例列表**页面中，选择需要 ping 通的实例 ID/实例名，进入该实例的详情页面。如下图所示：

3. 在**网络信息**栏，查看实例是否配置了公网 IP。
   - 实例已配置公网 IP，请 检查实例安全组确保已设置 。
   - 实例未配置公网 IP，请 EIP 绑定云资源 。

### 检查实例安全组确保已设置

安全组是一个虚拟防火墙，可以控制关联实例的入站流量和出站流量。而安全组的规则可以指定协议、端口、策略等。由于 ping 使用的是 ICMP 协议，请确认实例关联的安全组是否允许 ICMP。执行以下操作，查看实例使用的安全组以及详细的入站和出站规则：

1. 通过登录 云服务器控制台，检查实例安全组设置。
2. 在**实例列表**页面中，选择需要设置安全组的实例 ID/实例名，进入该实例的详情页面。
3. 选择**安全组**页签，进入该实例的安全组管理页面。如下图所示：

4. 根据实例所使用的安全组以及详细的入站和出站规则，判断实例关联的安全组是否允许 ICMP。
   - 实例关联的安全组已允许 ICMP，请 检查系统内实例确保处于设置状态 。
   - 实例关联的安全组未允许 ICMP，请将 ICMP 协议策略设置为允许。

## 检查系统内实例确保处于设置状态

判断实例的操作系统类型，选择不同的检查方式。

- Linux 操作系统，请 检查 Linux 内核参数和防火墙设置 。
- Windows 操作系统，请 检查 Windows 防火墙设置 ，若非防火墙问题，可尝试 检查服务器内 Windows 实例网络确保已设置 。

### 检查 Linux 内核参数和防火墙设置

> **说明：**
> Linux 系统是否允许 ping 由内核和防火墙设置两个共同决定，任何一个禁止，都会造成 ping 包 **Request timeout**。

通过腾讯云 VNC 登录进入服务器内部进行检查。

#### 检查内核参数 icmp_echo_ignore_all

1. 通过 VNC 登录实例，详见：
   - 使用 VNC 登录 Linux 实例
   - 使用 VNC 登录 Windows 实例
2. 执行以下命令，查看系统 icmp_echo_ignore_all 设置。

```
cat /proc/sys/net/ipv4/icmp_echo_ignore_all
```

   - 若返回结果为0，表示系统允许所有的 ICMP Echo 请求，请 检查防火墙设置 。
   - 若返回结果为1，表示系统禁止所有的 ICMP Echo 请求，请执行 步骤3 。
3. 执行以下命令，修改内核参数 icmp_echo_ignore_all 的设置。

```
echo "0" >/proc/sys/net/ipv4/icmp_echo_ignore_all
```

#### 检查防火墙设置

执行以下命令，查看当前服务器的防火墙规则以及 ICMP 对应规则是否被禁止。

```
iptables -L
```

- 若返回如下结果，表示 ICMP 对应规则未被禁止，请 检查域名确保已备案 。

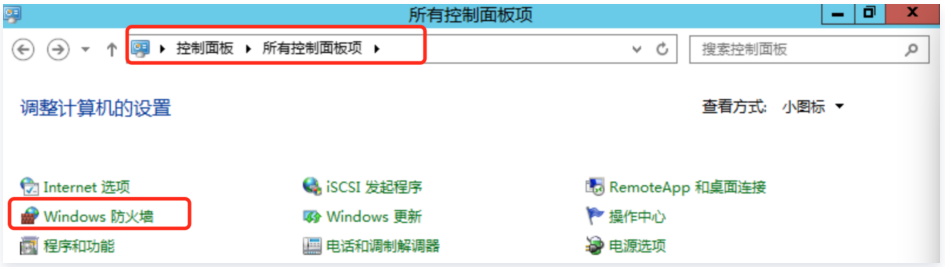
```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
```

- 若返回结果 ICMP 对应规则被禁止，请执行以下命令，启用对应规则。

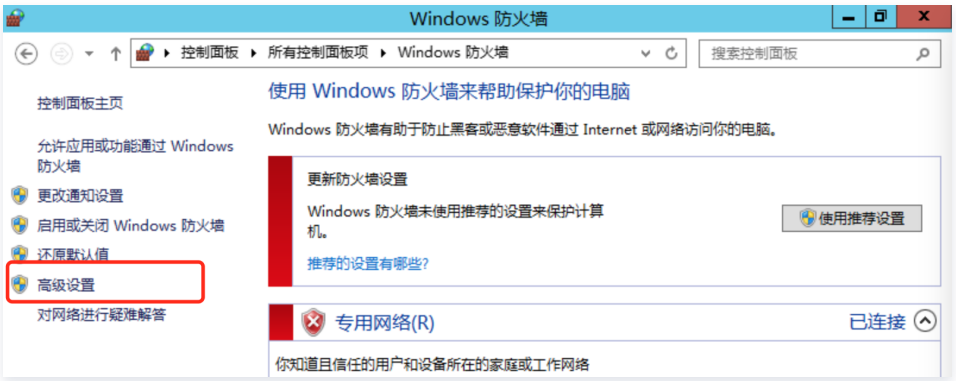
```
#Chain INPUT
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
#Chain OUTPUT
iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
```

### 检查 Windows 防火墙设置

1. 登录实例。
2. 打开**控制面板**，选择 **Windows 防火墙设置**。如下图所示：

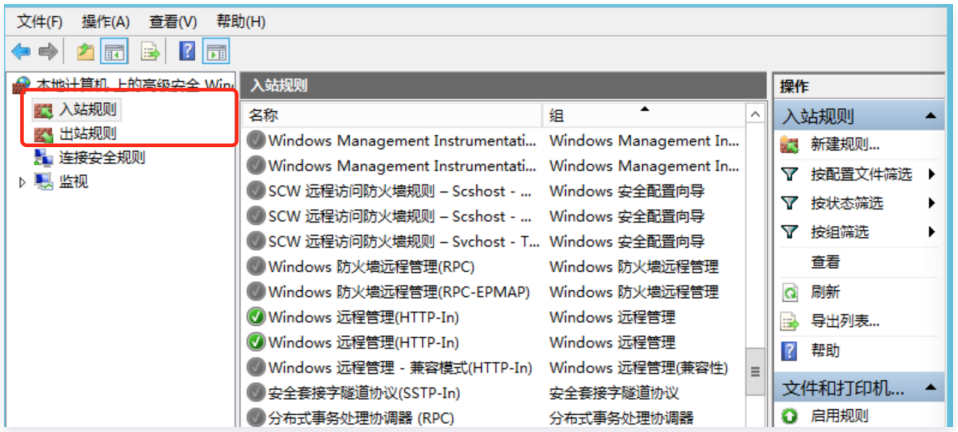



3. 在**Windows 防火墙**界面，选择**高级设置**。如下图所示：




4. 在弹出的**高级安全 Windows 防火墙**窗口中，查看 ICMP 有关的出入站规则是否被禁止。

- 若如下图所示，ICMP 有关的出入站规则被禁用，请启用该规则。




- 若 ICMP 有关的出入站规则已启用，请 检查域名确保已备案 。

## 检查域名确保已备案

> **说明：**
> 如果您可以 ping 通公网 IP，而 ping 不通域名，可能是域名没有备案或者域名解析的问题导致。

国家工信部规定，对未取得许可或者未履行备案手续的网站不得从事互联网信息服务，否则就属于违法行为。为不影响网站长久正常运行，如需开办网站，建议您先办理网站备案，待备案成功取得通信管理局下发的 ICP 备案号后，才开通访问。

- 如果您的域名没有备案，请先进行 域名备案 。
- 如果您使用的是腾讯云的域名服务，您可以登录 域名服务控制台 查看相应的域名情况。
- 如果您的域名已备案，请 检查服务器内域名解析确保配置正确 。

## 检查服务器内 Windows 实例网络确保已设置

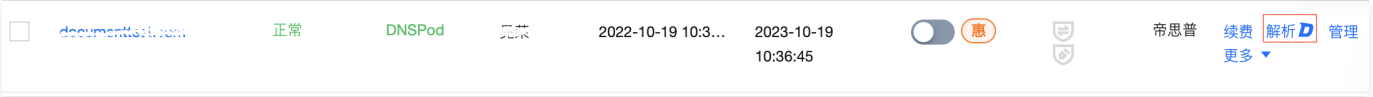
1. 请确认您的 VPC 网络是否支持 DHCP（如为2018年6月后创建的 VPC 网络，均支持 DHCP），若不支持，请确认网络设置中的静态 IP 是否正确。
2. 如果支持 DHCP，查看 DHCP 分配到的内网 IP 是否正确，若不正确，您可通过官网的登录功能（VNC 登录），以管理员身份运行 PowerShell，在其中执行 `ipconfig /release` 以及 `ipconfig /renew` （无需重启机器）尝试令 DHCP 组件重新获取 IP。
3. 若 DHCP 分配到的IP正确，但网络仍旧不通，可使用开始菜单中的**运行**功能，输入 `ncpa.cpl` 并单击确定。打开本地连接，尝试禁用、启用网卡。
4. 若以上方式仍不能解决问题，可以管理员身份执行在 CMD 中执行以下命令并重启机器。

```
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles"  /f
```

## 检查服务器内域名解析确保配置正确

ping 不通域名的另外一个原因是由于域名解析没有正确配置。如果您使用的是腾讯云的域名服务，您可以执行以下操作，检查域名解析。

1. 登录 域名服务控制台，检查域名解析。
2. 在**我的域名**管理页面，选择需检查域名解析的域名行，单击**解析**，查看域名解析详情。如下图所示：




## 相关参考

若上述步骤无法解决问题：

- 域名 ping 不通，请检查您的网站配置。
- 公网 IP ping 不通，请附上实例的相关信息和双向 MTR 数据（从本地到云服务器以及云服务器到本地），通过 在线支持 联系工程师协助定位。MTR 的使用方法请参见 服务器网络延迟和丢包处理 。

# 域名无法解析（CentOS 6.x 系统）

最近更新时间：2024-12-02 16:30:04

## 现象描述

操作系统为 CentOS 6.x 的云服务器进行重启或者执行命令 `service network restart` 后，云服务器出现无法解析域名的情况。同时，查看 `/etc/resolv.conf` 配置文件时，发现 DNS 信息被清空。

## 可能原因

在 CentOS 6.x 操作系统中，因为 grep 版本的不同，initscripts 的版本低于 9.03.49-1 存在缺陷。此时，需要升级 initscripts 到最新的版本，并重新生成 DNS 信息。

## 故障处理

1. 登录云服务器。
2. 执行以下命令，查看 initscripts 的版本，确认 initscripts 是否存在因版本低于 9.03.49-1 而存在缺陷的问题。

   ```
   rpm -q initscripts
   ```

   返回类似如下信息：

   ```
   initscripts-9.03.40-2.el6.centos.x86_64
   ```

   可得知，initscripts-9.03.40-2 低于问题版本 initscripts-9.03.49-1，存在 DNS 被清空的风险。
3. 依次执行以下命令，将 initscripts 升级到最新的版本，并重新生成 DNS 信息。

   ```
   yum makecache
   yum -y update initscripts
   service network restart
   ```

4. 完成升级后，执行以下命令，检查 initscripts 的版本信息，确认升级是否成功。

   ```
   rpm -q initscripts
   ```

   返回类似如下信息：

   ```
   initscripts-9.03.58-1.el6.centos.2.x86_64
   ```

   可得知，显示的版本不同于之前版本，且高于 initscripts-9.03.49-1，操作升级成功。

版权所有：腾讯云计算（北京）有限责任公司

# Linux 上无法解析 tencentyun.com 相关域名

最近更新时间：2024-12-31 16:28:02

## 现象描述

Linux 实例无法解析 mirrors.tencentyun.com 和 mirror.ccs.tencentyun.com 等域名。

## 可能原因

- 未配置 DNS 地址或者 DNS 地址错误。
- 防火墙设置了 53 端口的相关规则。
- 开启了 DNS 的 NSCD 缓存服务。
- /lib64/libnss_dns.so.2 库文件丢失导致无法解析域名。

## 解决方案

请按照以下方法进行排查并定位问题，然后根据现场实际情况，选择对应的处理方式：

1. 执行以下命令，查看是否正确配置 DNS 服务器。

```
cat /etc/resolv.conf #(tlinux/redhat/centos/rockylinux)
cat /run/systemd/resolve/resolv.conf #(ubuntu)
```

若 DNS 服务器配置不正确，则需修改 DNS 服务器地址。建议您参见 如何在 Linux 实例中自定义 DNS 配置 文档进行 DNS 配置。
腾讯云的 DNS 服务器：

```
nameserver 183.60.82.98
nameserver 183.60.83.19
```

2. 执行以下命令，查看防火墙是否添加了53端口的相关规则。

```
iptables -L
```

如果防火墙设置中包含针对53端口的规则，请关闭防火墙或删除该规则。有关防火墙的使用，请参见 防火墙问题 。

3. 执行以下命令，查看是否启动了 DNS 的 NSCD 缓存服务。

```
systemctl status nscd
```

若启动了 NSCD 缓存服务，请执行 `systemctl stop nscd` 命令，关闭 NSCD 缓存服务。

4. 查看 /lib64/libnss_dns.so.2 等关键 lib 库文件是否丢失或被修改。

```
ls -l /lib64/libnss_dns.so.2
#/lib64/libnss_dns.so.2库文件由glibc包产生，可以通过校验glibc查看包是否被修改。
rpm -V glibc
```

进一步判断是否存在软链接对应源文件，如 CentOS 7的是 /usr/lib64/libnss_dns-2.17.so，如果不存在则可在同 OS 版本的正常服务器上下载替换。
如果还存在 /usr/lib64/libnss_dns-2.17.so，可以通过软链接修复。

```
ln -s /usr/lib64/libnss_dns-2.17.so /usr/lib64/libnss_dns.so.2
```

版权所有：腾讯云计算（北京）有限责任公司