弹性云服务器

故障排除

文档版本 01

发布日期 2025-09-19

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 高频故障案例

1.1 弹性云服务器访问中国大陆外网站时加载缓慢怎么办?

为什么访问中国大陆外网站卡顿?

购买的弹性云服务器可能会出现访问中国大陆外（包括中国港澳台及其他国家、地区）网站卡顿的问题。

这是由于服务器在中国大陆内，访问的网站在中国大陆外，国际带宽线路则是首选，国际带宽线路节点分布世界各地，访问过程中不可避免的出现绕节的情况，延时增加，访问卡顿，因此延迟高于国内服务器访问国内网站的情况。

视频帮助

三招帮您搞定访问中国大陆外网站加载缓慢问题

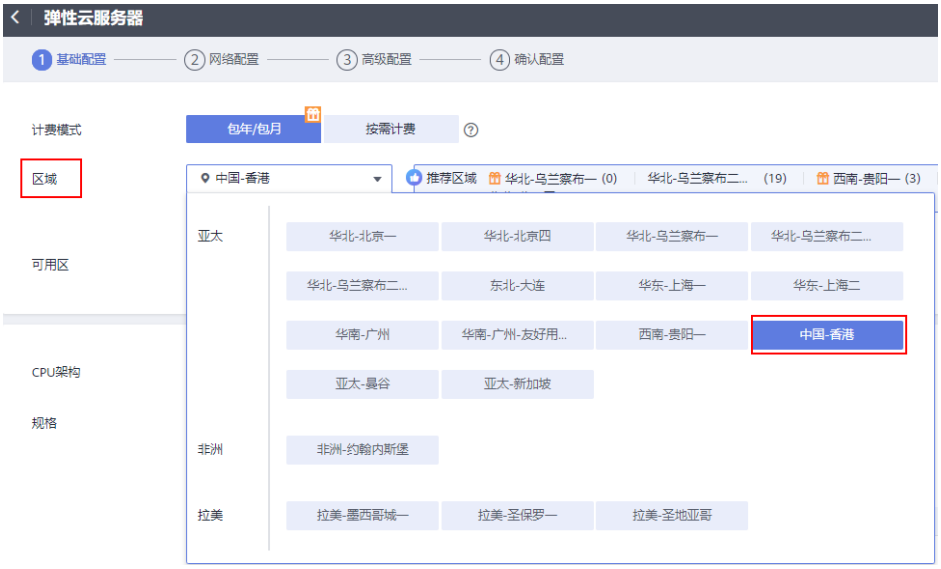
处理方法

- **重新购买中国大陆外的弹性云服务器，例如“中国-香港”区域的云服务器**

  从物理距离与网络基础设施等因素考虑方面，如果您有访问中国大陆外网站的需求，我们建议您购买中国大陆外的弹性云服务器。

  例如您可以在购买弹性云服务器时选择“中国-香港”区域的弹性云服务器。

图 1-1 选择“中国-香港”区域



- **优化访问速度**

  您还可以按照本节的操作步骤优化访问速度。

  - **修改DNS配置**
  - **修改hosts文件来优化访问速度**

  优化访问速度后，您可以进一步通过执行**ping -t 网站地址**确认丢包情况，详细操作请参考**检查访问网站的请求是否得到响应**。

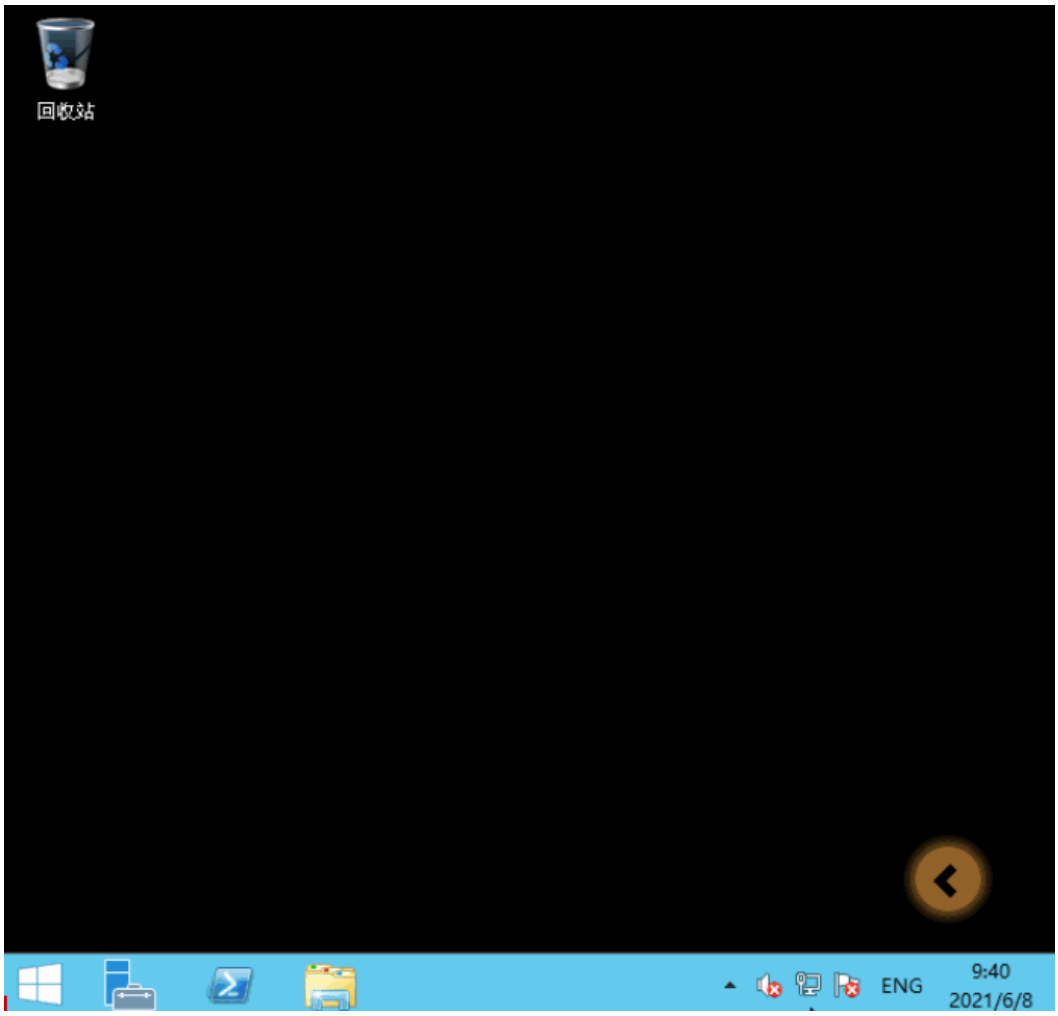
修改 DNS 配置

方法一：系统界面操作

修改DNS服务器地址为公共DNS服务器，例如：101.226.4.6 、1.1.1.1。

以下演示了Windows 2012操作系统配置DNS的操作步骤。

图 1-2 修改 DNS 配置



详细操作步骤如下：

1. 以用户名Administrator，登录Windows弹性云服务器。
2. 打开本地连接。
   a. 在任务栏的右下角，右键单击网络连接的图标。
   b. 单击“打开网络和共享中心”。

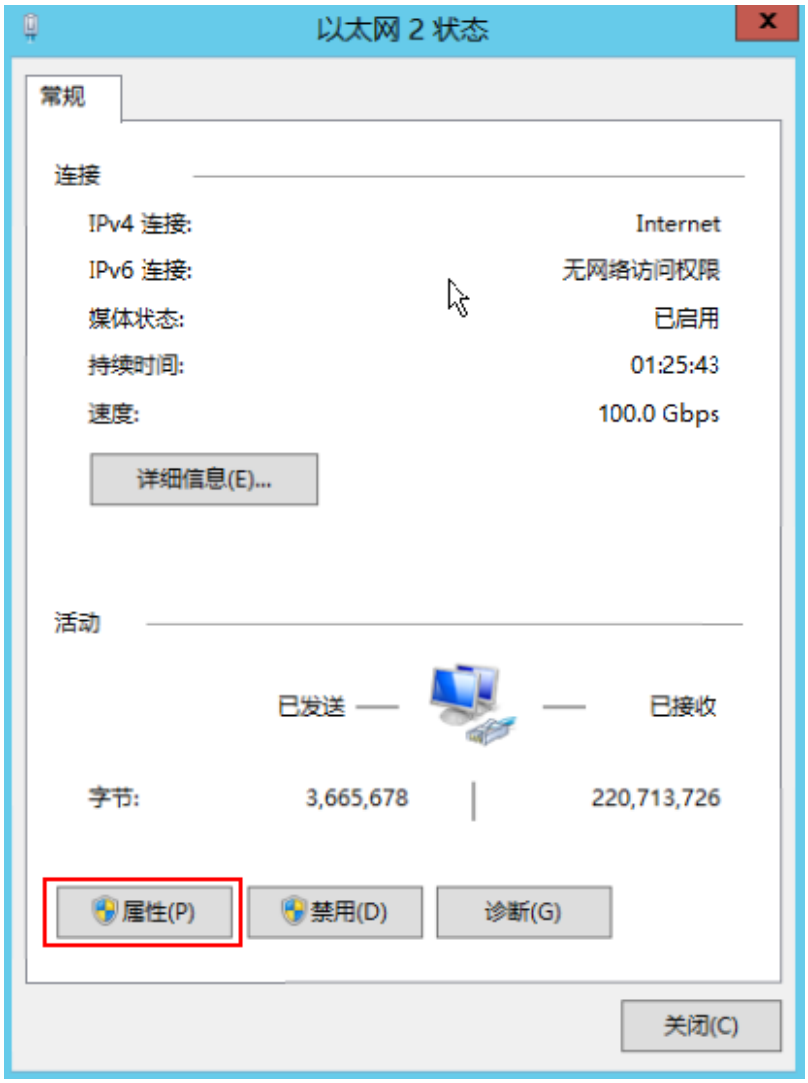
      图 1-3 打开网络和共享中心

   c. 在左侧导航栏，单击“更改适配器设置”。
3. 给弹性云服务器配置DNS服务器。
   a. 双击网络连接。

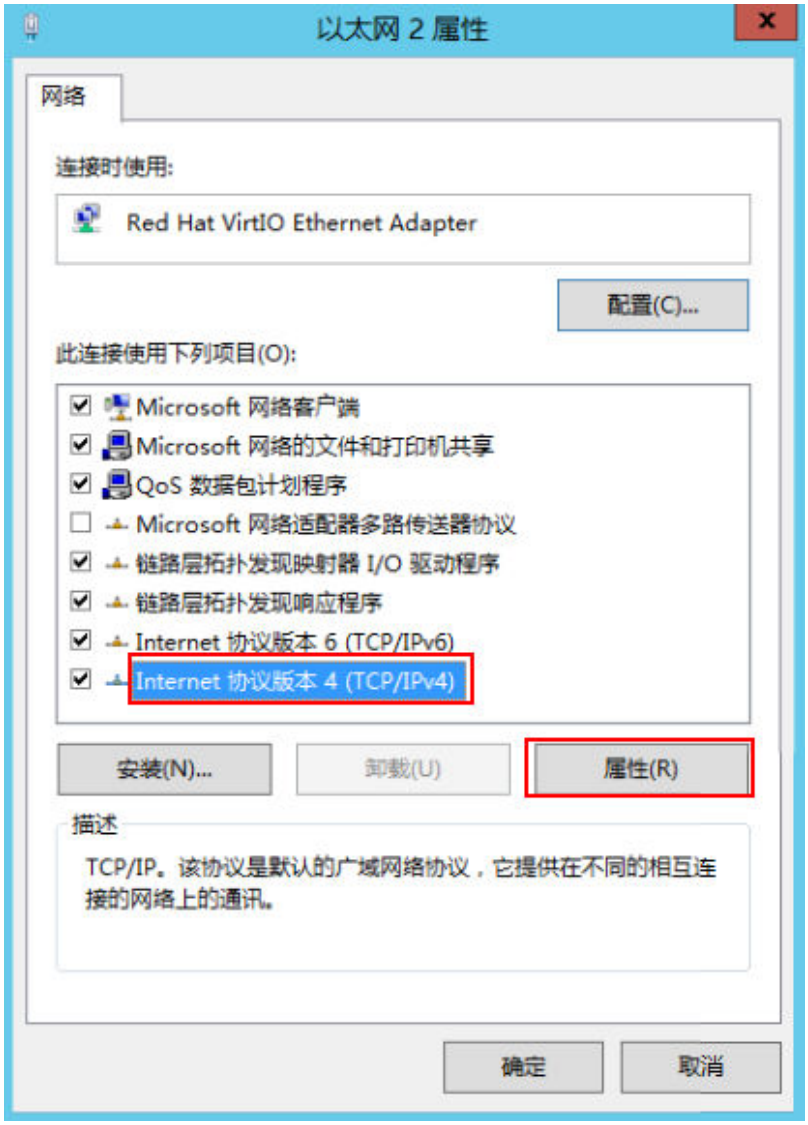
b. 单击左下角的“属性”，如图1-4所示。

图 1-4 本地连接



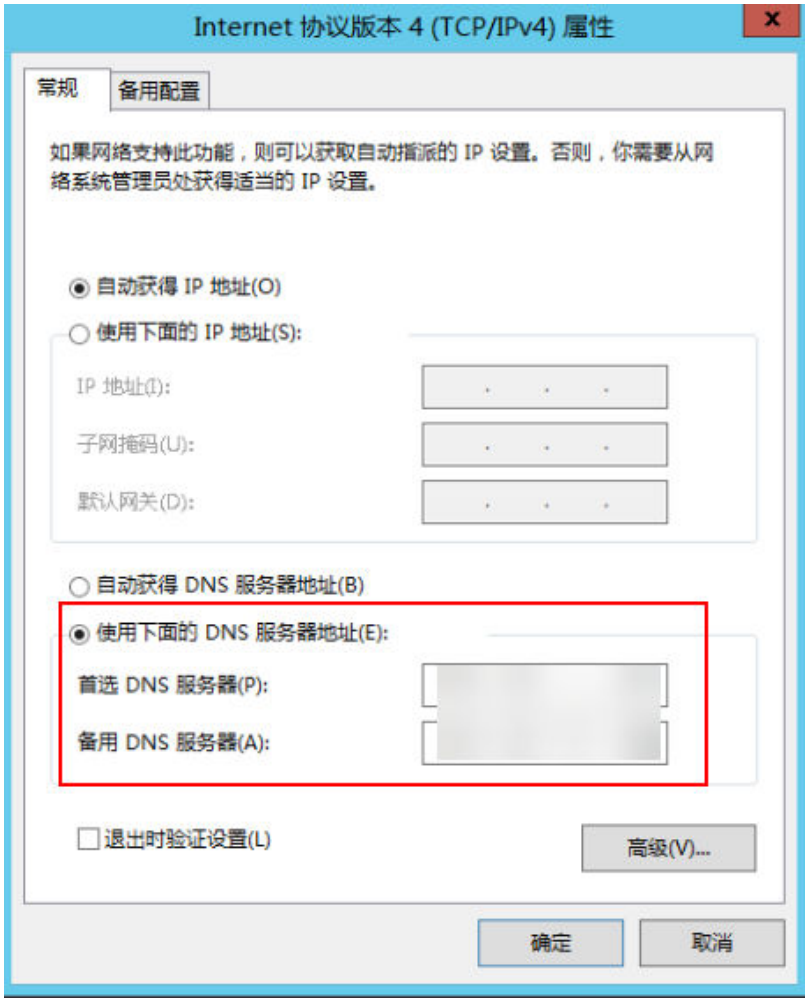
c. 选择“Internet 协议版本4（TCP/IPv4）”，并单击“属性”，如图1-5所示。

图 1-5 选择协议类型



d. 选择“使用下面的DNS服务器地址”，并根据界面提示填写DNS服务器的IP地址，如图1-6所示。

图 1-6 填写 DNS 服务器 IP 地址



方法二：命令行操作

以下演示了Windows 2012操作系统通过命令行配置DNS的操作步骤。

1. 登录Windows云服务器。
2. 单击左下角的“开始”菜单，输入“notepad”，运行记事本应用。
3. 拷贝表1-1中的脚本内容到记事本中，并另存为bat脚本文件。

表 1-1 配置 DNS 脚本内容

操作	脚本内容	云运维中心
设置静态DNS	@echo off & setlocal chcp 65001 for /F "tokens=3* delims= " %%a in ('netsh interface show interface ^|findstr "Connected"') do (netsh interface ipv4 set dns "%%b" static 首选DNS primary >nul netsh interface ipv4 add dns "%%b" 备用DNS index=2 >nul) ipconfig /flushdns >nul	1. 登录管理控制台。 2. 打开**HWC.ECS.OSOps-modify-windows-dns.bat**脚本，获取脚本内容。 **说明** 也可在云运维中心**HWC.ECS.OSOps-modify-windows-dns.bat**的执行脚本页面设置参数后，直接运行。
恢复DHCP自动配置	@echo off & setlocal chcp 65001 for /F "tokens=3* delims= " %%a in ('netsh interface show interface ^|findstr "Connected"') do (netsh interface ipv4 set dns name="%%b" dhcp >nul) ipconfig /flushdns >nul	

4. 右击bat文件，以管理员身份运行。

修改 hosts 文件来优化访问速度

选择访问速度最快的服务器，并将其IP地址和域名写入hosts文件来优化访问速度。

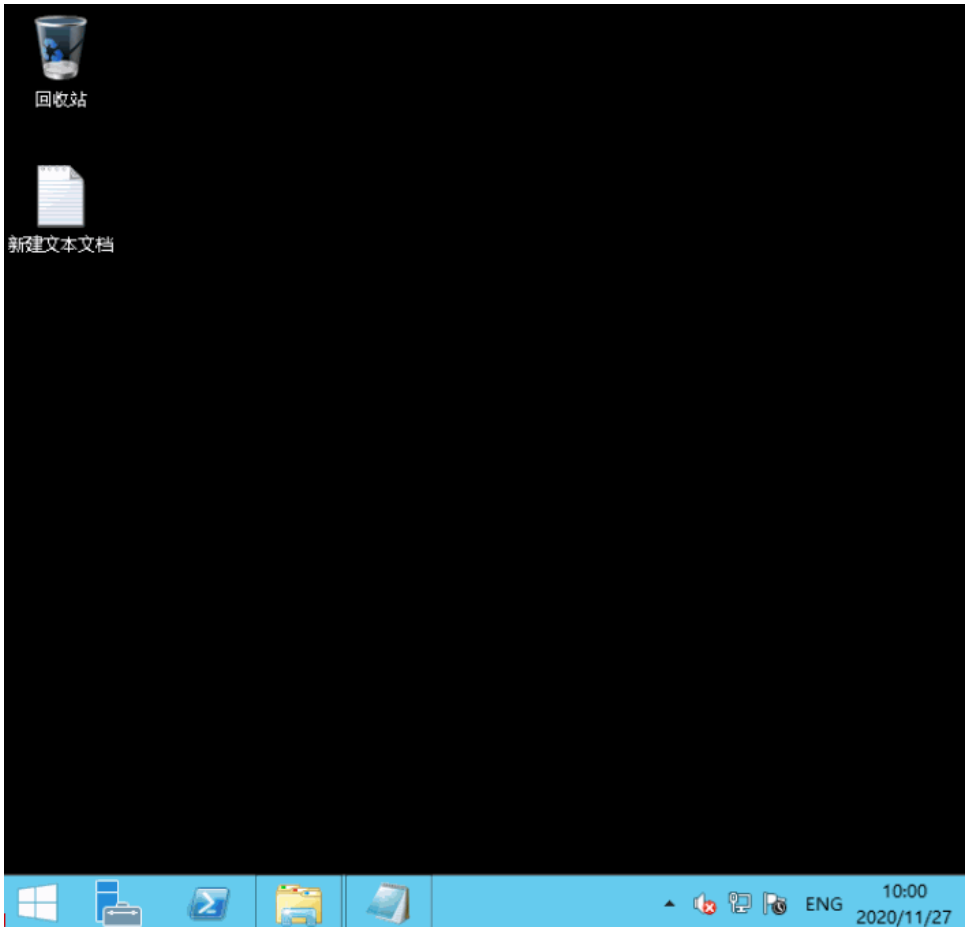
我们有以下两种方法来判断访问速度最快的服务器IP地址：

- 使用ping命令判断访问速度最快的服务器IP地址。
  具体操作请参考**方法一：使用ping命令判断访问速度最快的服务器IP地址**。
- 使用Ping检测工具和PingInfoView工具查找访问速度最快的服务器IP地址。
  具体操作请参考**方法二：使用Ping检测工具和PingInfoView工具查找访问速度最快的服务器IP地址**。

方法一：使用 ping 命令判断访问速度最快的服务器 IP 地址

以下演示了Windows 2012操作系统、访问www.example.com为例、使用ping命令选择IP地址的示例。

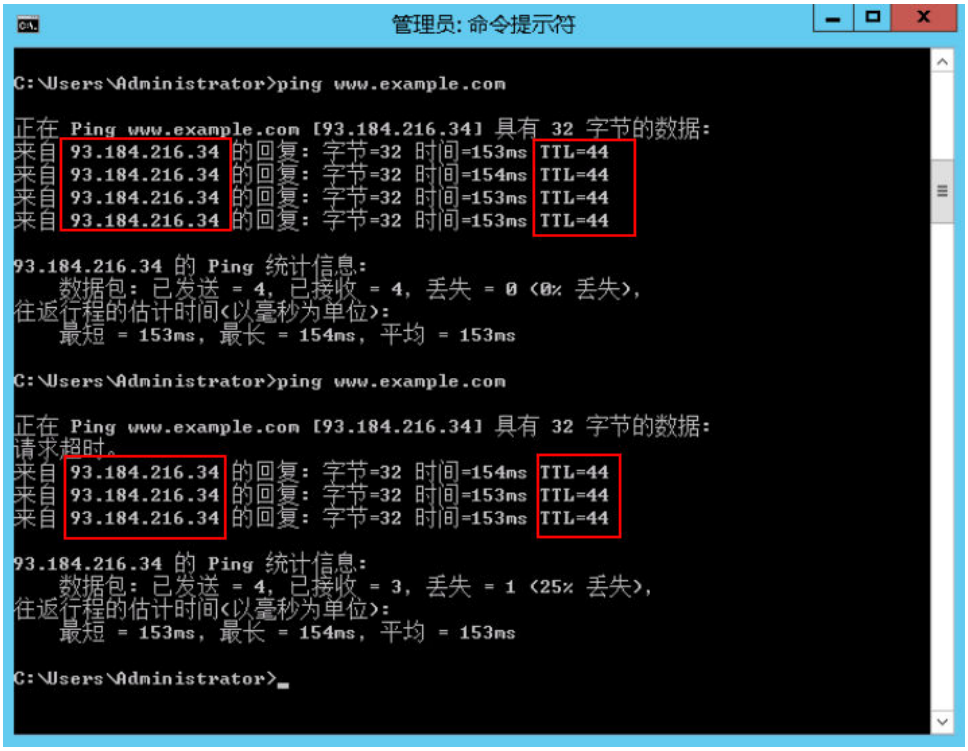
图 1-7 修改 hosts 文件来优化访问速度



详细的操作步骤如下：

1. 以访问www.example.com为例，在命令行 **ping www.example.com**，查询ping结果。

图 1-8 回显信息



2. 重复执行多次 **ping www.example.com**，记录下一条TTL值最小、且稳定的IP地址。

注意

请在ping的过程中执行**ipconfig /flushdns**刷新DNS解析缓存，否则会持续ping到同一个IP地址。

例如本例中选择的IP地址是93.184.216.34。

3. 修改hosts文件。

   打开C:\Windows\System32\drivers\etc\，将之前复制的IP地址以如下方式写入hosts文件末尾。

   例如复制的IP地址为93.184.216.34，则将93.184.216.34 www.example.com写入到hosts文件的末尾，保存后关闭。

注意

- hosts文件是操作系统的核心文件之一，请根据需要谨慎修改。

  建议您备份hosts文件，您可以直接复制粘贴hosts文件生成一个副本。也可以复制hosts文件，将内容备份。
- 如果hosts文件里写明了DNS解析IP，那么只能使用这个IP解析网站地址。
- 修改hosts文件后如果再次出现卡顿想要重新替换IP，请先去掉hosts文件里关于网站的配置，然后重复执行本节的操作选取新的IP地址。

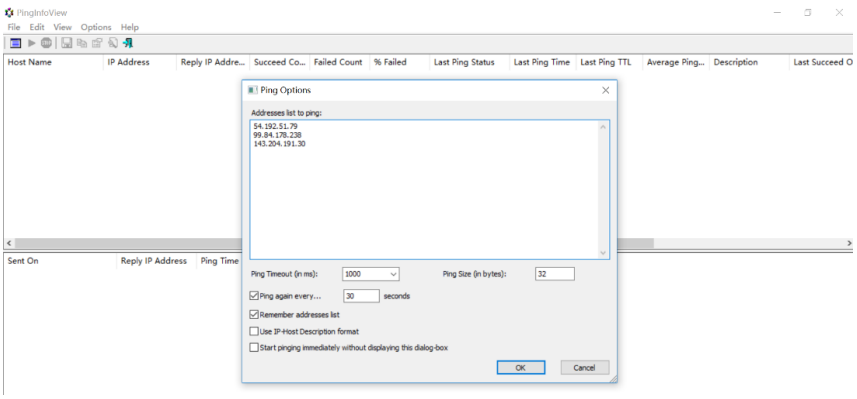
4. 重新访问中国大陆外网站，则卡顿或无法访问的问题会有所好转。

   修改hosts文件只能优化访问速度，如果重试后问题仍未解决，我们建议您购买“中国-香港”区域的服务器。

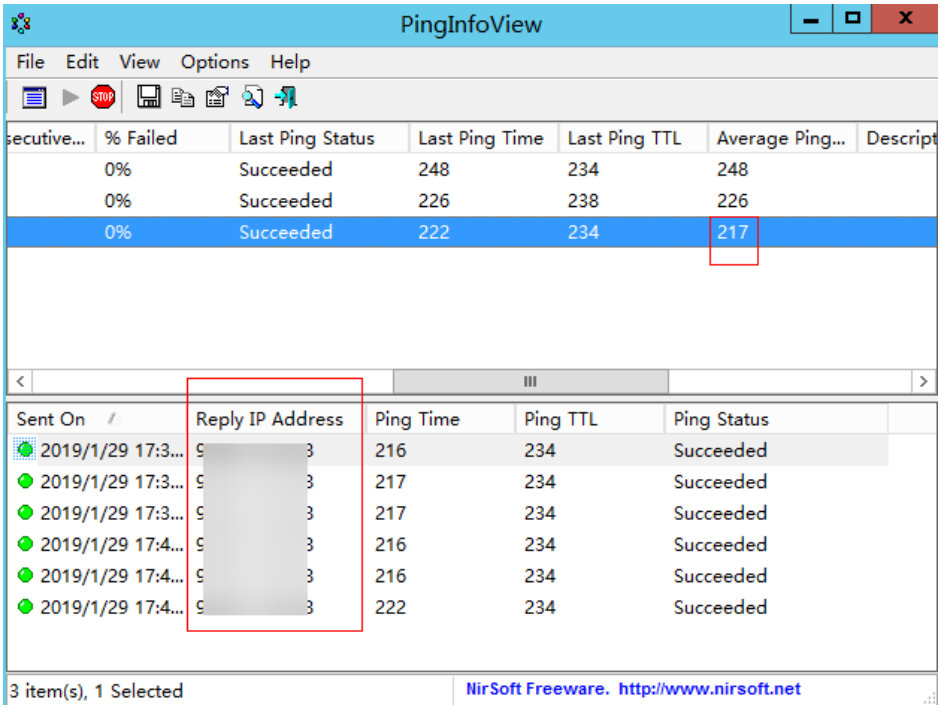
方法二：使用 Ping 检测工具和 PingInfoView 工具查找访问速度最快的服务器 IP 地址

您也可以通过修改hosts文件来优化访问速度，具体步骤如下：

1. 使用管理员角色（Administrator）登录您的弹性云服务器。
2. 通过浏览器访问Ping检测工具。我们以**http://ping.chinaz.com**为例。
3. 输入想要访问的网站，进行Ping检测。我们以访问www.example.com为例，记录检测结果列表中响应时间最低的IP 。
4. 下载**PingInfoView**，无需安装，解压后运行PingInfoView.exe即可使用。
5. 打开PingInfoView，将通过步骤**3**获取到的IP地址复制到对应的输入框中，并单击OK。



6. 复制搜索结果中延迟最低的IP地址。



7. 打开C:\Windows\System32\drivers\etc\，将之前复制的IP地址以如下方式写入hosts文件的末尾。

   ⚠ 注意

   - hosts文件是操作系统的核心文件之一，请根据需要谨慎修改。

     建议您备份hosts文件，您可以直接复制粘贴hosts文件生成一个副本。也可以复制hosts文件，将内容备份。
   - 如果hosts文件里写明了DNS解析IP，那么只能使用这个IP解析网站地址。
   - 修改hosts文件后如果再次出现卡顿想要重新替换IP，请先去掉hosts文件里关于网站的配置，然后重复执行本节的操作选取新的IP地址。

   例如复制的ip地址为99.84.178.238，则将99.84.178.238 www.example.com写入到hosts文件的末尾，保存后关闭。
8. 重新访问中国大陆外网站，则卡顿或无法访问的问题会有所好转。

   若问题仍未解决，我们建议您更换中国大陆外区域的弹性云服务器。

检查访问网站的请求是否得到响应

优化访问速度后，请在浏览器中重试打开需要访问的网站地址，如果网站可以正常打开，但仍然存在加载慢的情况，也可能是访问目标服务器存在丢包的情况，可以进一步通过执行**ping -t 网站地址**确认丢包情况。请参考**Ping不通或丢包时如何进行链路测试?**

例如：**ping -t www.example.com**

说明

Windows操作系统也可自行下载安装curl客户端，请单击**下载curl客户端**，解压后，打开bin文件夹拷贝路径，配置环境变量即可。

如果有响应状态码说明请求已经发送并得到响应，那么推断加载缓慢可能是访问目标服务器丢包等因素导致。

您可以联系客服帮助您检查丢包问题。同时推荐您使用我们**云连接服务**，访问效果可以有效的改善。详细操作请参考**基于云连接服务实现跨区域多VPC互通**。

1.2 Ping 不通或丢包时如何进行链路测试?

问题描述

在云服务器上访问其他网络资源时，出现网络卡顿。执行ping命令，存在丢包或时延过高的问题。

本节操作以Tracert和MTR工具为例，介绍如何诊断丢包或时延过高的网络问题根因。

原因分析

丢包或时延较高可能是链路拥塞、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Tracert或MTR工具进行进一步诊断。

使用网络诊断工具MTR可以帮助您确认网络问题的根因。

本节操作导航：

- Windows：
  - （推荐使用）**Windows操作系统Tracert介绍和使用**。
  - **Windows操作系统WinMTR介绍和使用**。
- Linux：
  - **Linux操作系统MTR介绍和使用**。

Windows 操作系统 Tracert 介绍和使用

Tracert是路由跟踪程序，Tracert命令用来显示数据包到达目标主机所经过的路径，并显示到达每个节点的时间。Tracert命令功能与Ping命令类似，但获得的信息要比Ping命令详细，它可以显示数据包所走的全部路径、节点的IP以及时间。

1. 登录Windows云服务器。
2. 打开cmd命令窗，执行以下命令跟踪IP地址。

   tracert IP地址/网站地址

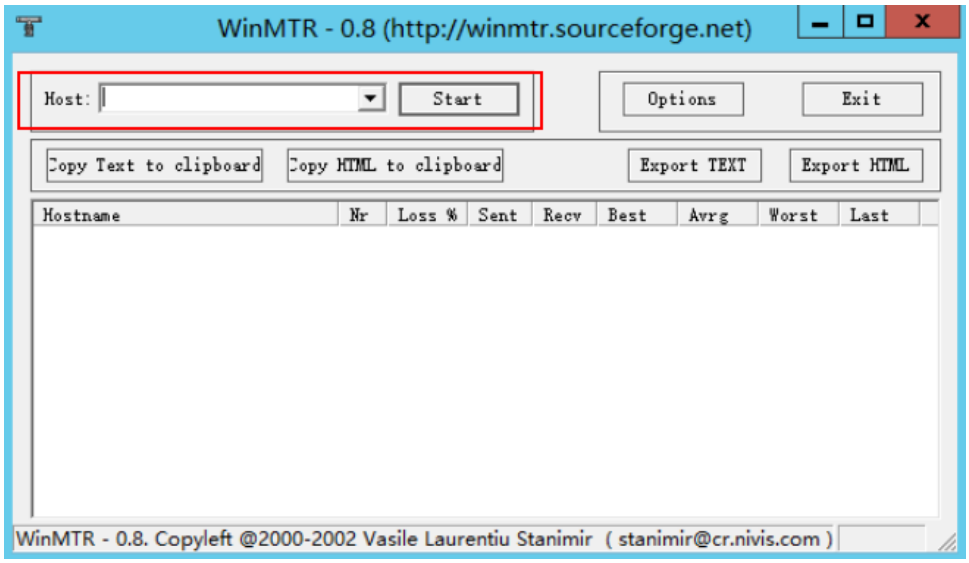
   例如：**tracert www.example.com**

   对数据节点分析如下：

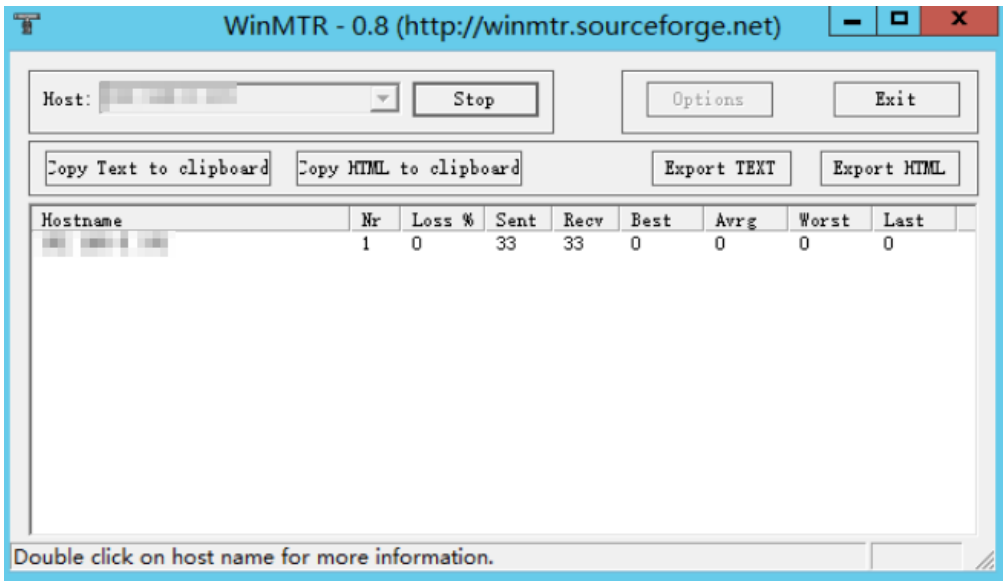
   - Tracert默认最大跳数30，第1列为起跳顺序号。
   - Tracert每次会发送三个数据包，第2、3、4列为对应三个数据包的返回时间。第5列为跳转的IP节点。
   - 假如某一层中出现了“* * * request timed out”，那么则需要定位这层的问题，可能这里导致连接不到目标节点。

Windows 操作系统 WinMTR 介绍和使用

1. 登录Windows云服务器。
2. 通过浏览器访问公网，搜索并下载WinMTR安装包。
3. 解压缩WinMTR安装包，WinMTR无需安装，可以直接解压运行。
4. 双击WinMTR.exe，打开WinMTR工具。
5. 在WinMTR窗口的Host处，输入目的服务器IP地址或者域名，单击“Start”。



6. 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或域名。
- Nr：经过节点的数量。
- Loss%：对应节点的丢包率。
- Sent：已发送的数据包数量。
- Recv：已接收到响应的数量。
- 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。

Linux 操作系统 MTR 介绍和使用

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，分别列出每次追踪的结果。
- -c/--report-cycles：指定每次探测发送的数据包数量，默认值是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。

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

回显信息如下：

```
[root@ecs-0609 ~]# mtr 119.xx.xx.xx --report
Start: Thu Aug 22 15:41:22 2019
HOST: ecs-652                    Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- 100.xx.xx.xx              0.0%    10    3.0   3.4   2.8   7.5   1.3
  2.|-- 10.xx.xx.xx               0.0%    10   52.4  51.5  34.2  58.9   6.3
  3.|-- 10.xx.xx.xx               0.0%    10    3.2   5.0   2.7  20.8   5.5
  4.|-- 10.xx.xx.xx               0.0%    10    1.0   1.0   1.0   1.1   0.0
  5.|-- 192.xx.xx.xx              0.0%    10    3.5   4.2   2.8  11.6   2.5
  6.|-- 10.xx.xx.xx               0.0%    10   35.3  34.5   6.0  56.4  22.6
  7.|-- 10.xx.xx.xx               0.0%    10    3.3   4.7   3.1  14.7   3.6
  8.|-- ???                     100.0    10    0.0   0.0   0.0   0.0   0.0
```

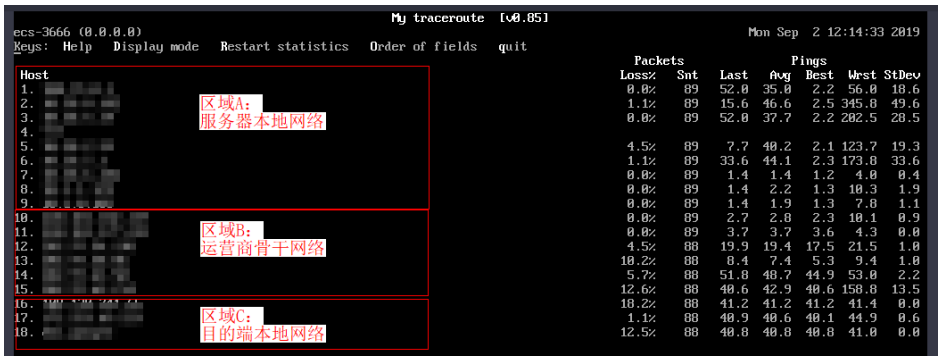
主要输出的信息如下：

- HOST：节点的IP地址或域名。
- Loss%：丢包率。
- Snt：每秒发送的数量包的数量。
- 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。

WinMTR 和 MTR 的报告分析处理

以下图为例分析WinMTR和MTR的报告。



- 服务器本地网络：即图中A区域，代表本地局域网和本地网络提供商网络。
  - 如果客户端本地网络中的节点出现异常，则需要对本地网络进行相应的排查分析。
  - 如果本地网络提供商网络出现异常，则需要向当地运营商反馈问题。
- 运营商骨干网络：即图中B区域，如果该区域出现异常，可以根据异常节点的IP查询其所属的运营商，向对应运营商进行反馈。
- 目标端本地网络：即图中C区域，即目标服务器所属提供商的网络。
  - 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原因，请检查目的服务器的防火墙配置。
  - 如果丢包发生在接近目的服务器的几跳，则可能是目标服务器所属提供商的网络问题。

常见的链路异常案例

- 目标主机配置不当

  如下示例所示，数据包在目标地址出现了100%的丢包。从数据上看是数据包没有到达，其实很有可能是目标服务器网络配置原因，需检查目的服务器的防火墙配置。

  ```
  Host                          Loss%   Snt   Last   Avg  Best  Wrst StDev
  1. ???
  2. ???
  3. 1XX.X.X.X                   0.0%    10  521.3  90.1   2.7 521.3 211.3
  4. 11X.X.X.X                   0.0%    10    2.9   4.7   1.6  10.6   3.9
  5. 2X.X.X.X                   80.0%    10    3.0   3.0   3.0   3.0   0.0
  6. 2X.XX.XX.XX                 0.0%    10    1.7   7.2   1.6  34.9  13.6
  7. 1XX.1XX.XX.X                0.0%    10    5.2   5.2   5.1   5.2   0.0
  8. 2XX.XX.XX.XX                0.0%    10    5.3   5.2   5.1   5.3   0.1
  9. 1XX.1XX.XX.X              100.0%    10    0.0   0.0   0.0   0.0   0.0
  ```

- ICMP限速

  如下示例所示，在第5跳出现丢包，但后续节点均未见异常。所以推断是该节点ICMP限速所致。该场景对最终客户端到目标服务器的数据传输不会有影响，分析时可以忽略此种场景。

  ```
  Host                          Loss%   Snt   Last   Avg  Best  Wrst StDev
  1. 1XX.XX.XX.XX                0.0%    10    0.3   0.6   0.3   1.2   0.3
  2. 1XX.XX.XX.XX                0.0%    10    0.4   1.0   0.4   6.1   1.8
  ```

```
3. 1XX.XX.XX.XX                0.0%    10    0.8   2.7   0.8  19.0    5.7
4. 1XX.XX.XX.XX                0.0%    10    6.7   6.8   6.7   6.9    0.1
5. 1XX.XX.XX.XX               60.0%    0    27.2  25.3  23.1  26.4   2.9
6. 1XX.XX.XX.XX                0.0%    10   39.1  39.4  39.1  39.7   0.2
7. 1XX.XX.XX.XX                0.0%    10   39.6  40.4  39.4  46.9   2.3
8. 1XX.XX.XX.XX                0.0%    10   39.6  40.5  39.5  46.7   2.2
```

- 环路

  如下示例所示，数据包在第5跳之后出现了循环跳转，导致最终无法到达目标服务器。出现此场景是由于运营商相关节点路由配置异常所致，需联系相应节点归属运营商处理。

```
Host                           Loss%   Snt   Last   Avg  Best  Wrst StDev
1. 1XX.XX.XX.XX                 0.0%    10    0.3   0.6   0.3   1.2   0.3
2. 1XX.XX.XX.XX                 0.0%    10    0.4   1.0   0.4   6.1   1.8
3. 1XX.XX.XX.XX                 0.0%    10    0.8   2.7   0.8  19.0   5.7
4. 1XX.XX.XX.XX                 0.0%    10    6.7   6.8   6.7   6.9   0.1
5. 1XX.XX.XX.65                 0.0%    10    0.0   0.0   0.0   0.0   0.0
6. 1XX.XX.XX.65                 0.0%    10    0.0   0.0   0.0   0.0   0.0
7. 1XX.XX.XX.65                 0.0%    10    0.0   0.0   0.0   0.0   0.0
8. 1XX.XX.XX.65                 0.0%    10    0.0   0.0   0.0   0.0   0.0
9. ???                         0.0%    10    0.0   0.0   0.0   0.0   0.0
```

- 链路中断

  如下示例所示，数据包在第4跳之后就无法收到任何反馈。这通常是由于相应节点中断所致。建议结合反向链路测试做进一步确认。该场景需要联系相应节点归属运营商处理。

```
Host                           Loss%   Snt   Last   Avg  Best  Wrst StDev
1. 1XX.XX.XX.XX                 0.0%    10    0.3   0.6   0.3   1.2   0.3
2. 1XX.XX.XX.XX                 0.0%    10    0.4   1.0   0.4   6.1   1.8
3. 1XX.XX.XX.XX                 0.0%    10    0.8   2.7   0.8  19.0   5.7
4. 1XX.XX.XX.XX                 0.0%    10    6.7   6.8   6.7   6.9   0.1
5. 1XX.XX.XX.XX                 0.0%    10    0.0   0.0   0.0   0.0   0.0
6. 1XX.XX.XX.XX                 0.0%    10    0.0   0.0   0.0   0.0   0.0
7. 1XX.XX.XX.XX                 0.0%    10    0.0   0.0   0.0   0.0   0.0
8. 1XX.XX.XX.XX                 0.0%    10    0.0   0.0   0.0   0.0   0.0
9 1XX.XX.XX.XX                  0.0%    10    0.0   0.0   0.0   0.0   0.0
```

1.3 访问 ECS 实例上运行的网站卡顿，如何定位问题?

问题描述

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访问ECS实例上运行的网站卡顿。

检查 DNS 是否配置正确

1. 打开cmd命令窗口，输入“**ipconfig /all**”，检查使用的DNS服务器是不是华为云默认DNS。

   推荐您使用华为云默认DNS地址。

   说明

   华为云提供的DNS地址请参考**华为云DNS地址**。

2. 如果使用的是华为云的DNS地址，请执行以下命令检查云服务器与DNS节点之间网络是否连通。

   ping *DNS IP地址*

例如：以华北-北京四为例，执行**ping 100.125.1.250**

3. 执行以下命令，查看域名解析是否正常。

   nslookup *待访问的大陆外网站地址*

   例如：**nslookup www.example.com**

   重新访问中国大陆外（包括中国港澳台及其他国家、地区）网站，查看卡顿或无法访问的问题是否有所好转。

   若问题仍未解决，请参考本节操作继续排查。

检查网络链路

1. 本地客户端ping服务器公网IP，确认是否存在丢包或延时的情况。
   - 若存在丢包或时延高的情况，请使用MTR进行诊断，具体操作可参考**Ping不通或丢包时如何进行链路测试？** 。
   - 若不存在丢包或时延高的情况，请执行**步骤2**。
2. 执行**dig/nslookup**命令，查看DNS的解析情况，排查是否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 DNS的问题导致访问慢。

   详细操作请参考：
   - **解析不生效有哪些原因？**
   - **怎样测试解析域名是否生效？**

检查云服务器

1. 登录管理控制台。
2. 单击管理控制台左上角的 ，选择区域和项目。
3. 选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表中的右上角，输入弹性云服务器名称、IP地址或ID，并进行搜索。
5. 单击弹性云服务器的名称，查看详情。
6. 在弹性云服务器详情页面，选择“监控”页签，查看监控数据。

查看弹性云服务器运行的应用程序中是否有对网络和CPU要求高的需求：

- 如果存在CPU/内存使用过高的情况，请参考**Windows云服务器卡顿怎么办？** 、**Linux云服务器卡顿怎么办？** 进行排查。
- 如果存在带宽使用过高的情况，请参考 **云服务器带宽占用高怎么办？**
  - 升级云服务器配置请参考**变更云服务器的配置**。
  - 升级带宽请参考**修改带宽**。

1.4 网站无法访问怎么办？

问题描述

网站的访问与云服务器的网络配置、端口通信、防火墙配置、安全组配置等多个环节相关联。任意一个环节出现问题，都会导致网站无法访问。本节操作介绍网站无法访问时的排查思路。

排查思路

如果打开网站有报错提示信息，首先应该根据报错提示信息，排查可能的原因。

您可以参考**通用请求返回值**中错误码说明排查可能原因。

说明

如果报错提示信息无法帮助您准确定位问题，请记录资源信息和问题时间，然后单击**提交工单**，填写工单信息，获取技术支持。

您还可以根据以下排查思路进行问题定位，排查思路根据可能原因的出现概率进行排序，建议您从高频率原因往低频率原因排查，从而帮助您快速找到问题的原因。

如果解决完某个可能原因仍未解决问题，请继续排查其他可能原因。

图 1-9 网站无法访问排查思路

表 1-2 网站无法访问排查思路

可能原因	处理措施
检查端口通信	检查Web端口是否正常监听，详细操作请参考**检查端口通信问题**。
检查安全组规则	检查安全组是否放通Web端口，详细操作请参考**检查安全组规则**。
检查防火墙配置	测试防火墙关闭后是否可以正常访问，详细操作请参考**检查防火墙配置**。
检查云服务器路由配置	查看云服务器路由表中网关信息配置是否正确，详细操作请参考**检查云服务器路由配置**。

可能原因	处理措施
检查本地网络	更换手机热点或其他网络测试是否可以正常访问，详细操作请参考**检查本地网络**。
检查云服务器CPU利用率	定位影响云服务器CPU利用率高的进程并优化进程，详细操作请参考**检查云服务器CPU利用率**。
检查域名解析（适用于域名访问的场景）	域名解析配置是否配置正确，详细操作请参考**检查备案与域名解析是否正常（使用域名无法访问时适用）**。
检查域名备案（适用于域名访问的场景）	网站的域名和服务器IP是否备案成功，详细操作请参考**检查备案与域名解析是否正常（使用域名无法访问时适用）**。

检查端口通信问题

确保服务进程和端口正常工作，处于LISTEN状态。**表1-3**为常见TCP状态。

- Linux操作系统云服务器端口通信问题排查
  使用**netstat -antpu**命令检查服务的状态，确认端口是否正常监听。
  例如：**netstat -antpu |grep sshd**

  图 1-10 查看端口监听状态_linux

  ```
  [root@elb-mq02 ~]# netstat -antpu | grep sshd
  tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      7178/sshd
  ```

  - 如果端口被正常监听，请执行**检查安全组规则**。
  - 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。
- Windows操作系统云服务器端口通信问题排查
  使用远程端口检测命令：
  a. 打开CMD命令行窗口。
  b. 执行**netstat -ano | findstr “*端口*”**命令查看进程使用的端口号。
  例如：**netstat -ano | findstr “80”**

  图 1-11 查看端口监听状态_windows

  ```
  C:\Users\Administrator>netstat -ano |findstr "80"
    TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
    TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       880
    TCP    [::]:80                [::]:0                 LISTENING       4
    TCP    [::]:49155             [::]:0                 LISTENING       880
    UDP    0.0.0.0:123            *:*                                    808
    UDP    [::]:123               *:*                                    808
  ```

  - 如果端口被正常监听，请执行**检查安全组规则**。
  - 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。

表 1-3 常见 TCP 状态

TCP状态	说明	对应场景
LISTEN	侦听来自远方的TCP端口的连接请求	正常TCP服务端
ESTABLISHED	代表一个打开的连接	正常TCP连接
TIME-WAIT	等待足够的时间以确保远程TCP接收到连接中断请求的确认	已关闭的TCP连接，一般1分钟后清除。
CLOSE-WAIT	等待从本地用户发来的连接中断请求	应用程序BUG，没有关闭socket。出现在网络中断后。一般是进程死循环或等待其他条件。可以重启对应进程。
FIN-WAIT-2	从远程TCP等待连接中断请求	网络中断过，需要12分钟左右自行恢复。
SYN-SENT	发送连接请求后等待匹配的连接请求	TCP连接请求失败。一般是服务端CPU占用率过高，处理不及时导致。DDos攻击也会出现此情况。
FIN-WAIT-1	等待远程TCP连接中断请求，或先前的连接中断请求的确认	网络中断过，此状态可能不会自行修复（等15分钟以上确认），如果长期占用端口需要重启OS恢复。

检查安全组规则

如果安全组没有网站访问使用的端口，需要在云服务器实例对应的安全组中添加放行该端口的规则。

1. 登录管理控制台。
2. 选择“计算 > 弹性云服务器”。
3. 在弹性云服务器列表，单击待变更安全组规则的弹性云服务器名称。
4. 选择“安全组”页签。
5. 在左侧的“全部安全组”区域，单击待变更的安全组右侧的“配置规则”
6. 根据网站使用的端口配置新的安全组规则，放行网站使用的端口。
   放行端口的详细操作，请参见**配置安全组规则**。

检查防火墙配置

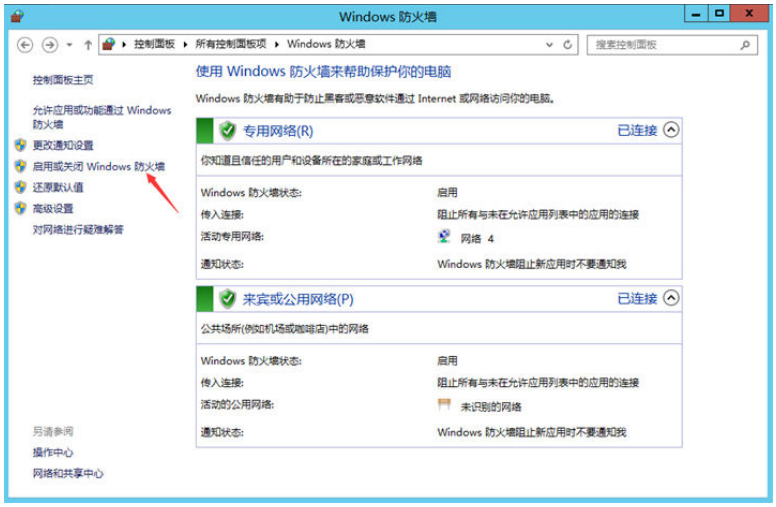
- Linux操作系统云服务器，关闭防火墙后测试是否可以正常访问。
  以CentOS 6.8操作系统80端口为例。
  a. 使用**iptables -nvL --line-number**命令查看已配置的防火墙策略。
  b. 依次执行以下命令放行80端口。
     iptables -A INPUT -p tcp --dport 80 -j ACCEPT
     iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT

c. 使用**service iptables save**命令保存添加的规则。
d. 使用**service iptables restart**命令重启iptables。
e. 使用**iptables -nvL --line-number**命令查看增加的规则是否生效。
f. 关闭防火墙后，重新测试网站访问是否正常。

- Windows操作系统云服务器，关闭防火墙后测试是否可以正常访问。

a. 登录Windows云服务器。
b. 单击桌面左下角的Windows图标，选择“控制面板 > Windows防火墙”。

c. 单击“启用或关闭Windows防火墙”。
查看并设置防火墙的具体状态：开启或关闭。



d. 关闭防火墙后，重新测试网站访问是否正常。

检查云服务器路由配置

- Linux操作系统云服务器

a. 使用**route**命令查看路由策略，确保0.0.0.0的默认路由指向网关，使用的IP和网关在相同网段，如下图第1行和第3行所示。


```
[root      ]# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         gateway         0.0.0.0         UG    100    0        0 eth0
                gateway         255.255.255.255 UGH   100    0        0 eth0
                0.0.0.0         255.255.255.0   U     100    0        0 eth0
                0.0.0.0         255.255.255.0   U     101    0        0 eth1
                0.0.0.0         255.255.255.0   U     102    0        0 eth2
[root      ]# _
```

b. 使用**ifconfig**或者**ip addr**命令查看实例的IP地址。

图 1-12 ifconfig 命令查看 IP 地址

```
[root@      ]# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet            netmask 255.255.255.0  broadcast 1
        inet6 fe80::f816:3eff:fe24:1e7f  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:24:1e:7f  txqueuelen 1000  (Ethernet)
        RX packets 227250083  bytes 21176207838 (19.7 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 149514101  bytes 276209392634 (257.2 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 14  bytes 1088 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 1088 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

图 1-13 ip addr 命令查看 IP 地址

```
[root@      ~]#  ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether fa:16:3e:24:1e:7f brd ff:ff:ff:ff:ff:ff
    inet 1          5/24 brd 1          scope global noprefixroute dynamic eth0
       valid_lft 77109sec preferred_lft 77109sec
    inet6 fe80::f816:3eff:fe24:1e7f/64 scope link
       valid_lft forever preferred_lft forever
```

c. 使用**route -n**命令通过路由表查看网关。

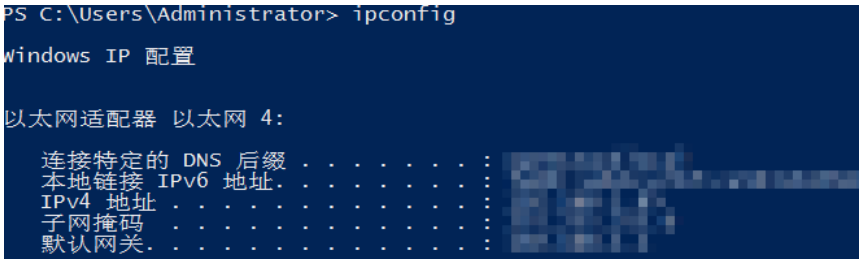
图1-14为示例，具体以云服务器网关实际地址为准。

图 1-14 route -n 命令查看网关

```
[root@      ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0                         0.0.0.0         UG    100    0        0 eth0
1                               255.255.255.255 UGH   100    0        0 eth0
1               0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

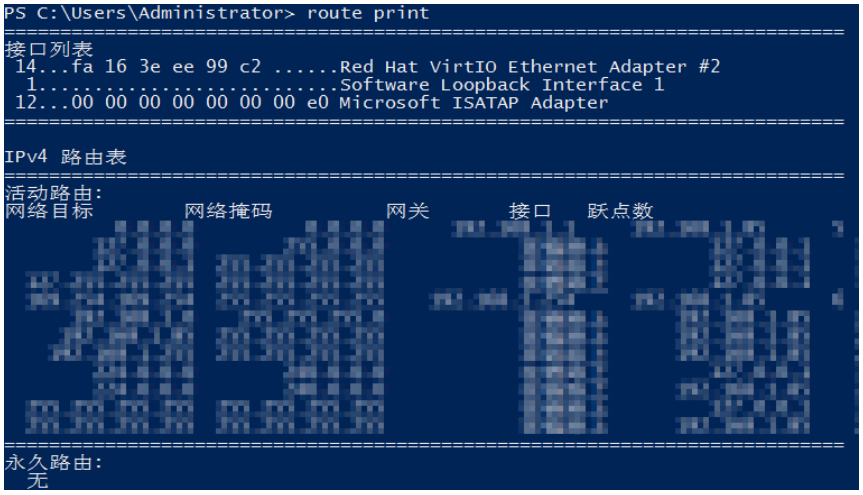
- Windows操作系统云服务器
  a. 打开CMD命令行窗口。
  b. 执行**ipconfig**命令查看实例的IP地址。

图 1-15 ipconfig 命令查看 IP 地址



c. 执行**route print**命令通过路由表查看网关。

图 1-16 route print 命令查看网关



检查本地网络

更换手机热点或其他网络测试是否可以访问网站。

如果可以正常访问说明云服务器的网络配置正常，请排除本地网络故障后重新测试访问网站。

检查云服务器 CPU 利用率

云服务器的带宽和CPU利用率过高可能导致网站无法访问。如果您已经通过云监控服务**创建过告警任务**，当CPU或带宽利用率高时，系统会自动发送告警给您。

1. 定位影响云服务器带宽和CPU利用率高的进程。
   - Windows操作系统本身提供了较多工具可以定位问题，包括任务管理器、性能监视器(Performance Monitor)、资源监视器(Resource Monitor)、Process Explorer、Xperf (Windows server 2008 以后)和抓取系统Full Memory Dump检查。
   - Linux操作系统执行**top**命令查看当前系统的运行状态。
2. 问题处理：排查进程是否正常，并分类进行处理。
   - 正常进程：优化程序，或参考**变更规格通用操作**变更云服务器配置。
   - 异常进程：建议您手动关闭进程，您也可以借助第三方工具关闭进程。

检查备案与域名解析是否正常（使用域名无法访问时适用）

完成上述的排查后，请使用弹性公网IP进行访问。如果使用IP地址可以访问，但是域名访问失败，则可能是域名备案或者解析相关问题造成网站无法访问。

网站的访问与域名的状态、域名实名认证状态、网站备案状态、解析是否生效、网站网络环境等多个环节有关系。在这些环节中，任意一个环节出现问题，都会导致网站无法访问。

关于域名与备案解析的排查思路请参考**网站无法访问排查思路（排查域名与备案解析）**。

1. 检查域名备案。

   备案是中国大陆的一项法规，网站的域名和服务器IP需要进行备案，备案成功后您的域名才可以指向服务器开通访问。

   - 如果您使用中国大陆节点服务器提供互联网信息服务，需要先在服务器提供商处提交备案申请，备案成功后域名才可以指向服务器开通访问。**如何备案?**
   - 如果您使用的是中国大陆地区以外的服务器（包括中国港澳台及其他国家、地区）提供互联网信息服务，无需备案。
   - 如果您的域名已在其他接入商办理过备案并取得备案号，现在更换到华为云服务器进行域名解析（或者二级域名指向华为云），因接入商有变更，需要您在华为云做**接入备案**。

     说明

     - 请确保网站内容与备案信息一致，且备案信息真实有效。
     - 如果您的网站已备案成功仍无法访问，请等待一个工作日。由于信息同步延迟，备案通过一个工作日后网页会自动开放。
2. 检查域名解析。

   如果域名已备案，但未正确配置域名解析也可能会导致域名无法Ping通。

   您可以DNS服务控制台查看域名解析详情。
3. 检查DNS服务器配置。

   如果ping *域名*显示找不到主机可能是DNS服务器速度慢，导致的访问卡顿，建议您参考案例：**弹性云服务器访问中国大陆外网站时加载缓慢怎么办?** 进行优化。

1.5 云服务器端口不通怎样排查?

操作场景

如果网站直接无法访问，可能是由于安全组没有放行网站或者远程连接工具使用的端口。

本节操作以80端口为例介绍排查云服务器端口不通问题的操作步骤。

问题定位步骤

如果实例无法对外提供HTTP服务，可以按以下思路检查Web服务相关的接口（默认为TCP 80）是否正常工作。

1. 在ECS管理控制台，确认安全组已经放行该端口。
2. 远程连接ECS实例，确认服务已经开启。
3. 确认端口正常被监听。如没有，请修改监听地址。
4. 确认实例防火墙已经放行服务。

Windows 操作系统

以下操作以Windows 2012操作系统云服务器，安装了IIS服务为例。

步骤1 确认安全组已经放行80端口。

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表，单击待变更安全组规则的弹性云服务器名称。
   系统跳转至该弹性云服务器详情页面。
5. 选择“安全组”页签，查看安全组规则。
6. 确保云服务器所在的安全组已添加如下安全组规则。

图 1-17 安全组规则

步骤2 远程登录云服务器，确认服务已经开启。

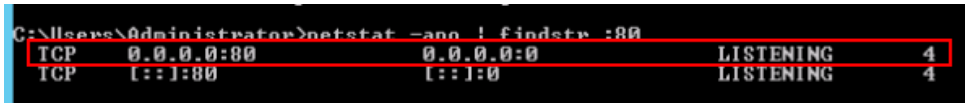
1. 在“服务器管理器”窗口，单击“工具 > Internet Information Services (IIS) 管理器”。
   如果找不到这个选项，则说明没有成功安装IIS服务，需要重新安装IIS服务。
2. 在Internet Information Services (IIS) 管理器窗口中确认以下信息。
   - 在“连接”导航栏里，右键单击实例ID，如果“启动”处于灰色状态，表示IIS服务已经开启。
   - 单击“网站”，在右边列表页查看您安装的网站的状态。如果网站状态为“已停止”，则单击网站，在右侧操作栏的“管理站点”，单击“启动”，启动网站。

步骤3 查看端口在实例中是否正常被监听的操作步骤。

打开cmd窗口，执行如下命令。

netstat -ano | findstr :80

如果回显信息如下则说明80端口正常全网监听。否则，请修改监听地址。



步骤4 确认实例防火墙已经放行服务。

1. 单击“控制面板 > Windows防火墙”。
2. 根据防火墙状态，执行不同操作。
   - 如果防火墙处于关闭状态，不需要再做其他处理。
   - 如果防火墙处于开启状态，则执行以下操作。
     i. 单击“高级设置”。
     ii. 在弹出窗口的左侧导航栏中，单击“入站规则”。
     iii. 选择“万维网服务 (HTTP 流入量)”，如果处于禁用状态，请重新启用规则。

----结束

Linux 操作系统

以下操作以CentOS 7操作系统云服务器安装Nginx服务为例。

步骤1 确认安全组已经放行80端口。

1. 登录管理控制台。
2. 单击管理控制台左上角的，选择区域和项目。
3. 选择“计算 > 弹性云服务器”。
4. 在弹性云服务器列表，单击待变更安全组规则的弹性云服务器名称。
   系统跳转至该弹性云服务器详情页面。
5. 选择“安全组”页签，查看安全组规则。
6. 确保云服务器所在的安全组已添加如下安全组规则。

图 1-18 安全组规则

步骤2 远程连接ECS实例，确认服务已经开启。

执行如下命令，检查nginx服务是否已经开启。

systemctl status nginx

回显信息如下所示，则说明Nginx已经启动。


```
[root@iZ7jvkxk5ylphzZ ~]# systemctl status nginx
● nginx.service - The nginx HTTP and reverse proxy server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; disabled; vendor prese
t: disabled)
   Active: active (running) since Tue 2017-09-12 21:14:08 CST; 44s ago
  Process: 9624 ExecStart=/usr/sbin/nginx (code=exited, status=0/SUCCESS)
  Process: 9622 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=0/SUCCESS)
  Process: 9620 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=
0/SUCCESS)
 Main PID: 9627 (nginx)
   CGroup: /system.slice/nginx.service
           ├─9627 nginx: master process /usr/sbin/nginx
           └─9628 nginx: worker process

Sep 12 21:14:08 iZ7jvkxk5ylphzZ systemd[1]: Starting The nginx HTTP and reve....
Sep 12 21:14:08 iZ7jvkxk5ylphzZ nginx[9622]: nginx: the configuration file /...k
Sep 12 21:14:08 iZ7jvkxk5ylphzZ nginx[9622]: nginx: configuration file /etc/...l
Sep 12 21:14:08 iZ7jvkxk5ylphzZ systemd[1]: Failed to read PID from file /ru...t
Sep 12 21:14:08 iZ7jvkxk5ylphzZ systemd[1]: Started The nginx HTTP and rever....
Hint: Some lines were ellipsized, use -l to show in full.
```

如果未开启，则执行以下命令启动Nginx。

systemctl start nginx

步骤3 执行如下命令，查看端口在实例中是否正常被监听。

netstat -an | grep 80

回显信息则说明80端口正常全网监听。如果返回的不是上述结果，请修改监听地址。

```
tcp    0 0 0.0.0.0:80     0.0.0.0:*      LISTEN
```

步骤4 查看云服务器防火墙iptables规则列表。

- 执行以下命令，查看防火墙状态。

  systemctl status firewalld

  或

  firewall-cmd --state

- 如果防火墙关闭可以执行以下命令开启。

  systemctl start firewalld

  如果开启命令执行后提示“Failed to start firewalld.service: Unit is masked.”请执行以下命令后再重新执行开启防火墙的命令。

  systemctl unmask firewalld

- 查看打开的端口

  firewall-cmd --zone=public --list-ports

- 放行TCP 80端口

  firewall-cmd --zone=public --add-port=80/tcp --permanent

- 更新防火墙规则

  firewall-cmd --reload

----结束

1.6 云服务器带宽占用高怎么办?

操作场景

如果云服务器操作卡顿或无法连接，可能是由于云服务器带宽占用过高导致的，本节操作介绍排查云服务器带宽占用高的方法及相应的解决方案。

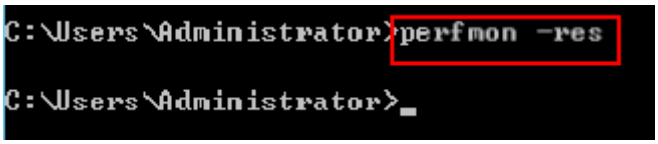
Windows 操作系统云服务器

1. 在管理控制台远程登录云服务器。

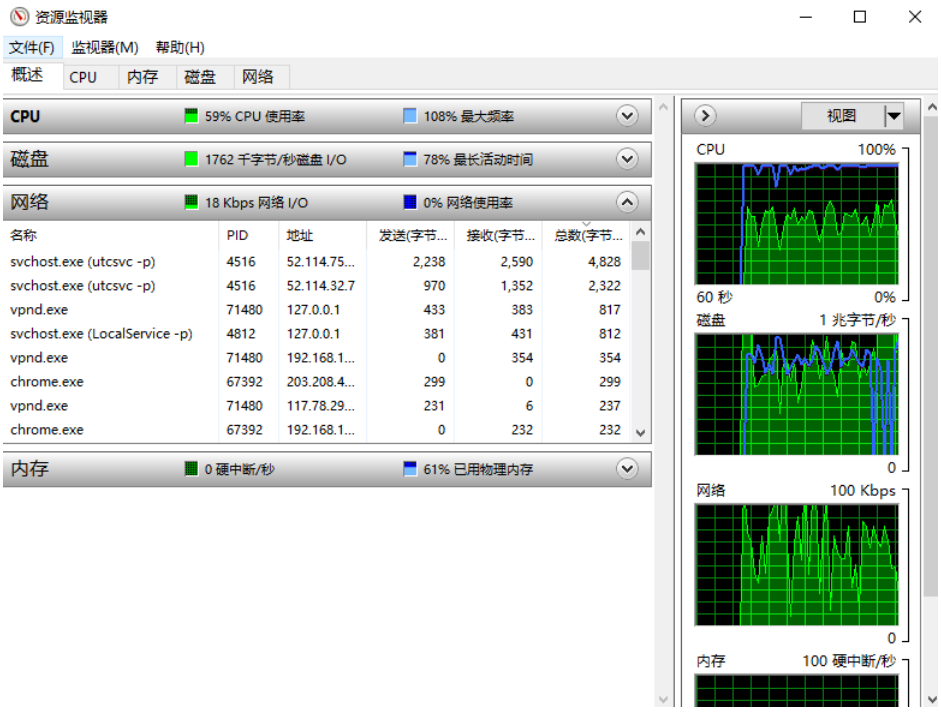
   以Windows2012操作系统云服务器为例。

2. 打开“运行”窗口，输入“perfmon -res”。

   图 1-19 打开资源监视器

3. 在“资源监视器”中，单击“CPU”或“网络”，查看CPU占用率或带宽使用情况。

4. 查看带宽占用率较高的进程名。
   - 如果消耗带宽较多的进程为业务进程，建议您**变更云服务器的配置**。
   - 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，建议您可以自行终止进程或者使用安全软件进行查杀。

Linux 操作系统云服务器

1. 通过管理控制台登录云服务器。

   以下操作以CentOS 6.8 64bit操作系统云服务器为例。

2. 执行以下命令安装Linux流量监控工具iftop。

   yum install iftop -y

   ```
   [root@ecs-fccf ~]# yum install iftop -y
   Loaded plugins: fastestmirror, security
   Setting up Install Process
   Determining fastest mirrors
   epel/metalink
    * base: mirrors.163.com
    * epel: mirrors.njupt.edu.cn
    * extras: ftp.sjtu.edu.cn
    * updates: ftp.sjtu.edu.cn
   base
   base/primary_db                                          69%
   ```

3. 执行如下命令，查看导致流量较高的端口与消耗流量的IP，以eth0端口为例。

   iftop -i *eth0* -P

4. 执行如下命令查看端口对应的进程，以38366端口为例。

   netstat -tunlp |grep *38366*

   - =>代表发送数据，<=代表接收数据。
   - TX表示发送流量，RX表示接收流量，TOTAL表示总流量。
   - cum：表示第一列各种情况的总流量。
   - peak：表示第一列各种情况的流量峰值。
   - rates：表示第一列各种情况2秒、10秒、40秒内的平均流量。

5. 查看带宽占用率较高的进程名。
   - 如果消耗带宽较多的进程为业务进程，建议您**变更云服务器的配置**。
   - 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，建议您可以自行终止进程或者使用安全软件进行查杀。

1.7 Windows 云服务器卡顿怎么办?

当您发现云服务器的运行速度变慢或云服务器突然出现网络断开现象，则可能是由以下原因导致的：

- 云服务器使用共享资源型实例。

  由于共享型资源实例是多实例共享CPU，当资源不足时，实例间可能出现CPU资源争抢，导致云服务器卡顿。

- 云服务器的带宽和CPU使用率过高。

  如果您已经通过云监控服务**创建过告警任务**，当CPU或带宽利用率高时，系统会自动发送告警给您。

当云服务器使用共享资源型实例时，您可以按如下步骤进行排查：

1. 问题定位：检查当前云服务器的规格类型，共享型和独享型实例的说明请参考**实例类型**。
2. 问题处理：如果对业务稳定性有较高要求，建议您通过**变更规格**操作将共享型实例变更为独享型实例。

当Windows云服务器带宽流量过高或CPU利用率高，您可以按如下步骤进行排查：

1. 问题定位：定位影响云服务器带宽和CPU利用率高的进程和不明来源驱动。

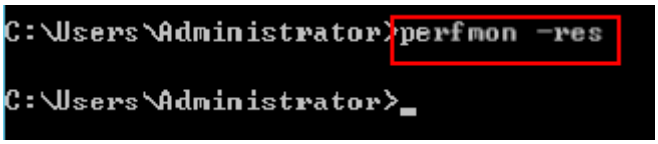
   Windows操作系统本身提供了较多工具可以定位问题，包括任务管理器、性能监视器(Performance Monitor)、资源监视器(Resource Monitor)、Process Explorer、Xperf (Windows server 2008 以后)和抓取系统Full Memory Dump检查。在流量大的情况下，您还可以使用Wireshark抓取一段时间的网络包，分析流量使用情况。

2. 问题处理：排查进程和驱动是否正常，并分类进行处理。
   - 正常进程：优化程序，或**变更云服务器的配置**。
   - 异常进程：建议您手动关闭进程，您也可以借助第三方工具关闭进程。
   - 正规来源驱动：系统自带驱动不进行处理，第三方软件驱动根据您的需求决定是否卸载对应软件。
   - 不明来源驱动：建议您卸载不明驱动，您也可以使用正规商业杀毒软件或第三方安全管理工具进行删除。

问题定位步骤

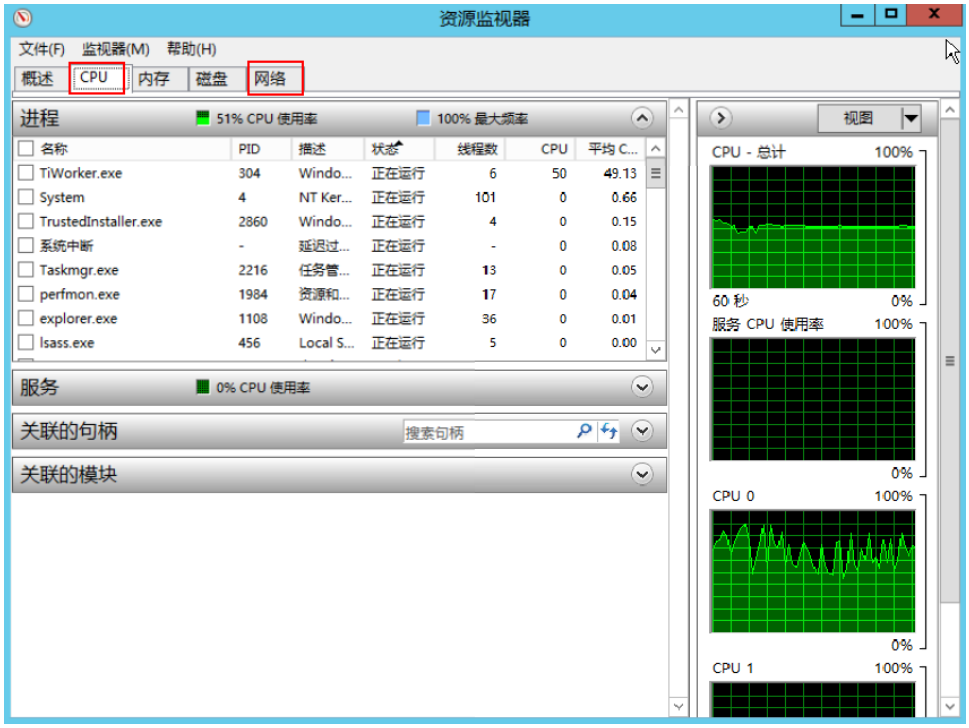
1. 在管理控制台使用VNC方式登录云服务器。
2. 打开“运行”窗口，输入“perfmon -res”。

   图 1-20 打开资源监视器

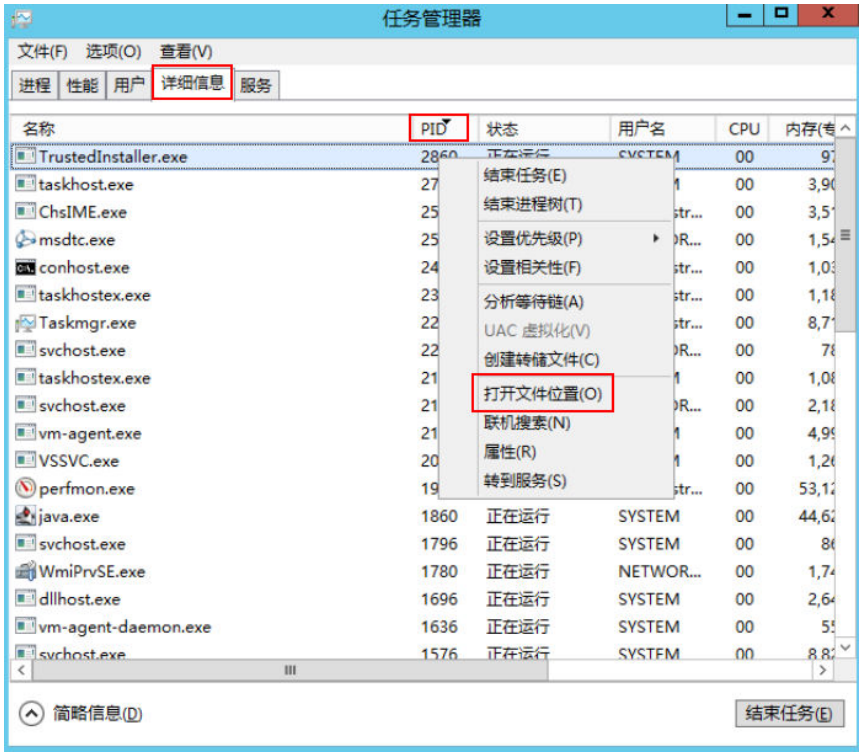
3. 在“资源监视器”中，单击“CPU”或“网络”，查看CPU占用率或带宽使用情况。

图 1-21 资源监视器



4. 查看CPU和带宽占用率较高的进程ID和进程名。
5. 在控制台VNC登录页面单击“Ctrl+Alt+Del”，打开“Windows任务管理器”。
   或打开“运行”窗口，输入“taskmgr”，打开“Windows任务管理器”。
   以下步骤为您介绍在任务管理器中打开PID，找到进程的具体位置，核对是否异常进程。
   a. 选择“详细信息”选项卡。
   b. 单击PID进行排序。
   c. 在查找到的CPU或带宽占用率高的进程上右键单击“打开文件位置”。
   d. 定位进程是否是正常或是否为恶意程序。

图 1-22 检查进程



6. 打开“运行”窗口，输入“**fltmc**”，查看系统的文件系统过滤驱动。

   下图以windows10操作系统为例，不同操作系统内置驱动不同，请以官网网站说明为准。如果安装了第三方的驱动，也会在这个列表中显示。

图 1-23 查看系统驱动

```
C:\WINDOWS\system32>fltmc
筛选器名称                     数字实例    高度          框架
WdFilter                       5           328010        1
storqosflt                     0           244000        1
wcifs                          1           189900        1
MWSecWal                                   149998.99     <过时>
FileCrypt                      0           141100        0
luafv                          1           135000        0
npsvctrig                      1           46000         0
Wof                            4           40700         0
FileInfo                       5           40500         0
```

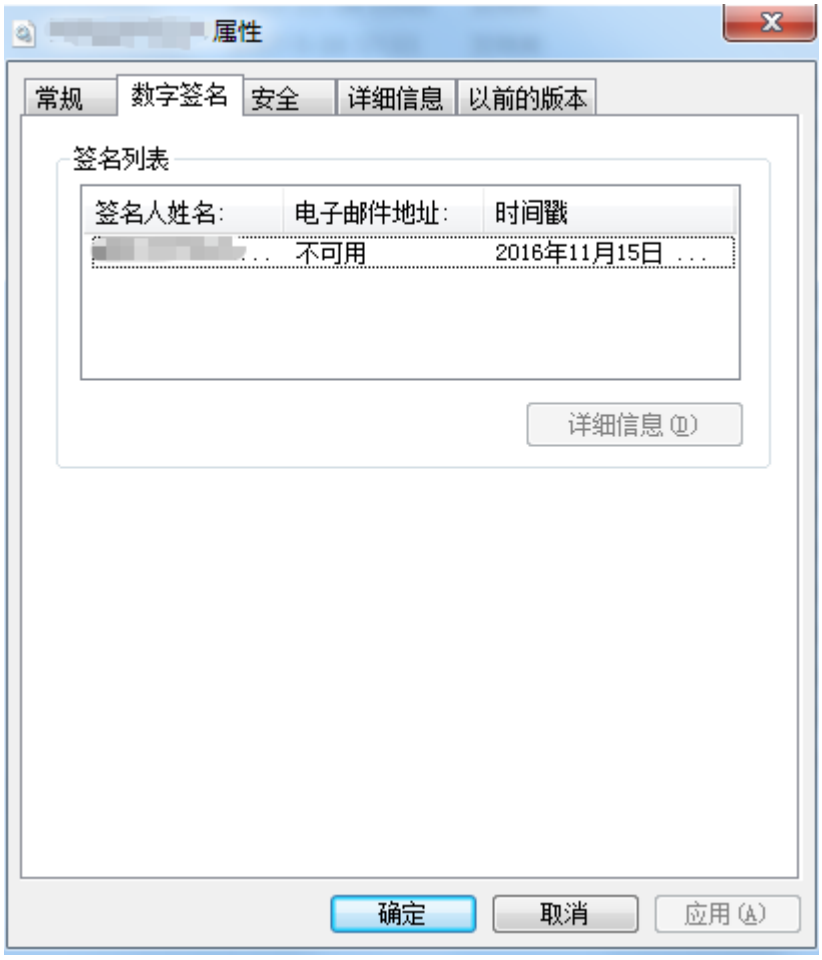
以下步骤为您介绍如何查看驱动的来源，核对是否为不明来源驱动。

a. 打开系统路径“C:\Windows\System32\drivers”。

b. 在不明驱动名称上单击，选择“属性”，查看详细信息。

c. 选择“数字签名”，查看驱动的来源。

图 1-24 查看驱动来源



分析处理

在您采取措施处理问题前，首先需要判断影响CPU或带宽占用率高的进程和驱动是否正常，并分类进行处理。

正常进程分析处理建议

1. 如果您的操作系统是Windows 2008/Windows 2012，请检查内存大小，建议内存配置在2GB或以上。
2. 检查后台是否有执行Windows Update的行为。
3. 检查杀毒软件是否正在后台执行扫描操作。
4. 核对云服务器运行的应用程序中是否有对网络和CPU要求高的需求，如果是，建议您**变更云服务器的配置**或**修改带宽**。
5. 如果云服务器配置已经比较高，建议考虑云服务器上应用场景的分离部署，例如将数据库和应用分开部署。

异常进程分析处理建议

如果CPU或带宽利用率高是由于病毒、木马入侵导致的，那么需要手动结束进程。建议的处理顺序如下：

1. 使用商业版杀毒软件或安装微软安全工具**Microsoft Safety Scanner**，在安全模式下扫描病毒。

2. 安装Windows最新补丁。
3. 使用MSconfig禁用所有非微软自带服务驱动，检查问题是否再次发生，具体请参考微软官方文档《如何在Windows中执行干净启动》。
4. 若服务器或站点遭受DDOS攻击或CC攻击等，短期内产生大量的访问需求。

   您可以登录管理控制台执行以下操作：

   - 查看Anti-DDOS攻击是否开启，并检查防护策略是否配置合适；如未配置，请参考：**配置开启Anti-DDoS防护**。
   - 查看CC防护策略是否开启，并检查防护策略是否配置合适；如未配置，请参考：**配置CC防护策略**。

不明来源驱动分析处理建议

有些病毒和木马会通过文件系统过滤驱动加载。如果您发现不明来源的驱动，建议您卸载该驱动，也可以使用正规商业杀毒软件或第三方安全管理工具进行删除。

如果发现有无法删除的不明驱动，或者删除后还会再次出现的不明驱动，一般都是病毒或木马的驱动。如果使用正规商业杀毒软件或第三方安全管理工具也不能彻底删除，建议您重装操作系统，在这之前请做好数据备份避免造成损失。

1.8 Linux 云服务器卡顿怎么办?

当您发现云服务器的运行速度变慢或云服务器突然出现网络断开现象，则可能是由以下原因导致的：

- 云服务器使用共享资源型实例。

  由于共享型资源实例是多实例共享CPU，当资源不足时，实例间可能出现CPU资源争抢，导致云服务器卡顿。
- 云服务器的带宽和CPU使用率过高。

  如果您已经通过云监控服务**创建过告警任务**，当CPU或带宽利用率高时，系统会自动发送告警给您。

当云服务器使用共享资源型实例时，您可以按如下步骤进行排查：

1. 问题定位：检查当前云服务器的规格类型，共享型和独享型实例的说明请参考**实例类型**。
2. 问题处理：如果对业务稳定性有较高要求，建议您通过**变更规格**操作将共享型实例变更为独享型实例。

当Linux实例带宽流量过高或CPU使用率高时，您可以按如下步骤进行排查：

1. 问题定位：定位影响云服务器带宽和CPU使用率高的进程。
2. 问题处理：排查进程是否正常，并分类进行处理。
   - 正常进程：优化程序，或**变更云服务器的配置**。
   - 异常进程：建议您手动关闭进程，或者借助第三方工具关闭进程。

常用命令

本文相关操作命令以CentOS 7.2 64位操作系统为例。其它版本的Linux操作系统命令可能有所差异，具体情况请参阅相应操作系统的官方文档。

Linux云服务器查看CPU使用率等性能相关问题时的常用命令如下：

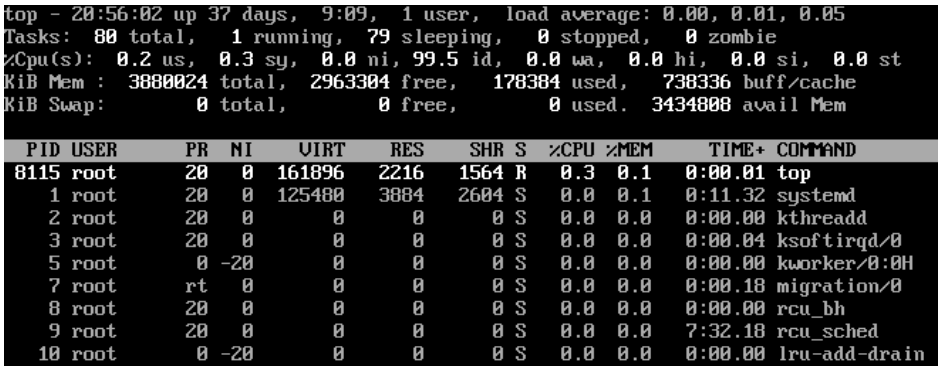
- **ps -aux**
- **ps -ef**
- **top**

CPU 占用率高问题定位

1. 使用VNC功能登录云服务器。
2. 执行如下命令查看当前系统的运行状态。

   top

   系统回显样例如下：



3. 查看显示结果。
   - 命令回显第一行：20:56:02 up 37 days，1 user, load average: 0.00, 0.01, 0.05的每个字段含义如下：

     系统当前时间为20:56:02，该云服务器已运行37天，当前共有1个用户登录，最近1分钟、最近5分钟和最近15分钟的CPU平均负载。
   - 命令回显第三行：CPU资源总体使用情况。
   - 命令回显第四行：内存资源总体使用情况。
   - 回显最下方显示各进程的资源占用情况。

     说明

     1. 在top页面，可以直接输入小写“q”或者在键盘上按“Ctrl+C”退出。
     2. 除了直接输入命令，您还可以单击VNC登录页面屏幕右上角的“Input Command”，在弹出的对话框中粘贴或者输入相应命令，单击“Send”。
     3. 在top运行中常用的内容命令如下：

        s：改变画面更新频率。

        l：关闭或开启第一部分第一行top信息的表示。

        t：关闭或开启第一部分第二行Tasks和第三行Cpus信息的表示。

        m：关闭或开启第一部分第四行Mem和 第五行Swap信息的表示。

        N：以PID的大小的顺序排列进程列表。

        P：以CPU占用率大小的顺序排列进程列表。

        M：以内存占用率大小的顺序排列进程列表。

        h：显示命令帮助。

        n：设置在进程列表所显示进程的数量。
4. 通过**ll /proc/***PID*/**exe**命令可以查看每个进程ID对应的程序文件。

CPU 使用率高问题处理

对于导致CPU使用率高的具体进程，如果确认是异常进程，可以直接通过top命令终止进程。对于kswapd0进程导致的CPU使用率高的问题，则需要对应用程序进行优化，或者通过增加内存进行系统规格的升级。

kswapd0是系统的虚拟内存管理程序，如果物理内存不够用，系统就会唤醒kswapd0进程，由kswapd0分配磁盘交换空间用作缓存，因而占用大量的CPU资源。

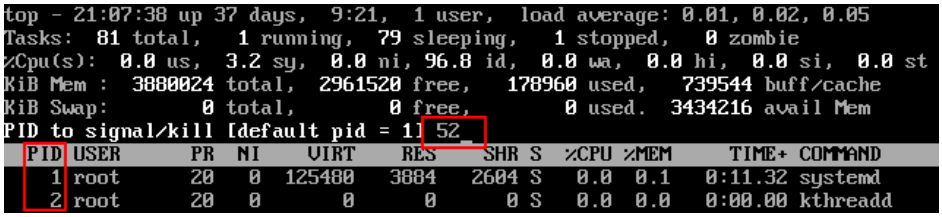
- 使用top命令终止CPU占用率高的进程

  您可以直接在top运行界面快速终止相应的异常进程。操作步骤如下：

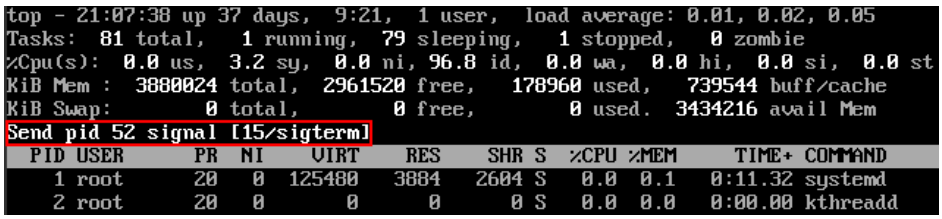
  a. 在top命令运行的同时，按下小写的“k”键。

  b. 输入要终止进程的PID。

  进程的PID为top命令回显的第一列数值。例如，要终止PID为52的进程，直接输入“52”后回车。



  c. 操作成功后，会出现如下图所示类似信息，按回车确认。

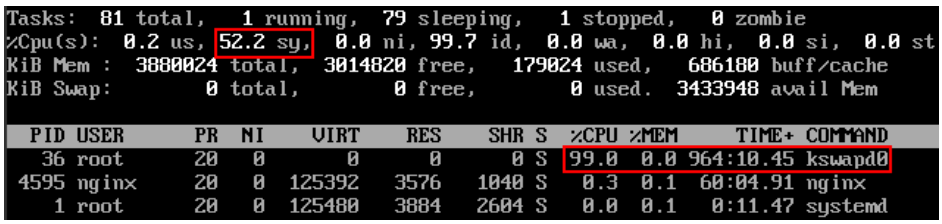


- kswapd0进程占用导致CPU使用率高

  可通过以下步骤排查进程的内存占用情况。

  a. 通过top命令查看kswapd0进程的资源使用。

  b. 如果kswapd0进程持续处于非睡眠状态，且运行时间较长，可以初步判定系统在持续的进行换页操作，可以将问题转向内存不足的原因来排查。



  c. 通过vmstat命令进一步查看系统虚拟内存的使用情况。

  如果si和so的值也比较高，说明系统存在频繁的换页操作，系统物理内存不足。

  - si：每秒从交换区写到内存的大小，由磁盘调入内存。
  - so：每秒写入交换区的内存大小，由内存调入磁盘。

  d. 对于内存不足问题，可以通过free、ps等命令进一步查询系统及系统内进程的内存占用情况，做进一步排查分析。

e. 临时可通过在业务空闲期重启应用或者系统释放内存。

如果要从根本上解决内存不足的问题，需要对服务器内存进行扩容，扩大内存空间。如果不具备扩容的条件，可通过优化应用程序，以及配置使用大页内存来进行缓解。

带宽使用率高问题分析

如果是正常业务访问以及正常应用进程导致的带宽使用率高，需要升级服务器的带宽进行解决。如果是非正常访问，如某些特定IP的恶意访问，或者服务器遭受到了CC攻击。或者异常进程导致的带宽使用率高。可以通过流量监控工具nethogs来实时监测统计各进程的带宽使用情况，并进行问题进程的定位。

- 使用nethogs工具进行排查

a. 执行以下命令，安装nethogs工具。

yum install nethogs -y

安装成功后可以通过nethogs命令查看网络带宽的使用情况。

nethogs命令常用参数说明如下：

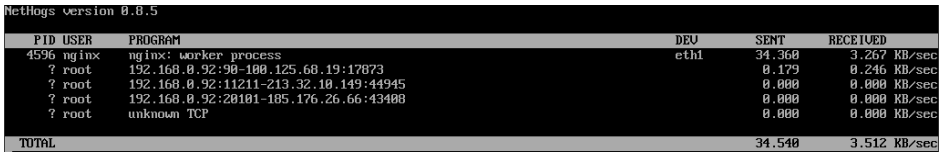
- -d：设置刷新的时间间隔，默认为 1s。
- -t：开启跟踪模式。
- -c：设置更新次数。
- device：设置要监测的网卡，默认是eth0。

运行时可以输入以下参数完成相应的操作：

- q：退出nethogs工具。
- s：按发送流量大小的顺序排列进程列表。
- r：按接收流量大小的顺序排列进程列表。
- m：切换显示计量单位，切换顺序依次为KB/s、KB、B、MB。

b. 执行以下命令，查看指定的网络端口每个进程的网络带宽使用情况。

nethogs *eth1*



回显参数说明如下：

- PID：进程 ID。
- USER：运行该进程的用户。
- PROGRAM：进程或连接双方的IP地址和端口，前面是服务器的IP和端口，后面是客户端的IP和端口。
- DEV：流量要去往的网络端口。

- SENT：进程每秒发送的数据量。
- RECEIVED：进程每秒接收的数据量。

c. 终止恶意程序或者屏蔽恶意访问IP。

如果确认大量占用网络带宽的进程是恶意进程，可以使用**kill *PID***命令终止恶意进程。

如果是某个IP恶意访问，可以使用iptables服务来对指定IP地址进行处理，如屏蔽IP地址或限速。

- 使用Web应用防火墙防御CC攻击

若服务遭受了CC攻击，请在Web应用防火墙控制台开启CC安全防护。Web应用防火墙的使用指导请参见**配置CC防护策略**。

1.9 弹性云服务器启动缓慢

如果弹性云服务器启动时间较长，可以通过修改默认等待时间，提高启动速度。

1. 登录弹性云服务器。
2. 执行以下命令，切换至root用户。

   sudo su
3. 执行以下命令，查询grub文件的版本。

   rpm -qa | grep grub

图 1-25 查询 grub 版本

```
[root@ ]# rpm -qa | grep grub
grub2-2.02-0.44.el7.centos.x86_64
```

4. 将grub文件中timeout时间修改为0s。

注意

本操作涉及修改grub配置文件，误操作可能会导致系统无法启动。操作前，请务必对grub配置文件进行备份，以便在发生误操作时能够进行恢复。

- grub版本小于2的：

  打开文件“/boot/grub/grub.cfg”或“/boot/grub/menu.lst”，并修改等待时间“timeout=0”。
- grub版本为2的：

  打开文件/boot/grub2/grub.cfg，并修改等待时间“timeout=0”。

图 1-26 修改 timeout

```
#boot=/dev/sda
default=0
timeout=0
splashimage=(hd0,1)/boot/grub/splash.xpm.gz
hiddenmenu
title CentOS (2.6.32-696.16.1.el6.x86_64)
        root (hd0,1)
        kernel /boot/vmlinuz-2.6.32-696.16.1.el6.x86_64 ro root=UUID=2bc0f5fd-e0
19-4ba5-8ce0-0fe12b6efc24 rd_NO_LUKS rd_NO_LVM LANG=en_US.UTF-8 rd_NO_MD SYSFONT
=latarcyrheb-sun16 crashkernel=auto  KEYBOARDTYPE=pc KEYTABLE=us rd_NO_DM rhgb q
```

1.10 配置云服务器实现多网卡多 IP 访问

问题描述

当云服务器配置了多张网卡时，需要在云服务器内部配置策略路由来实现非主网卡的通信，具体操作步骤如下。

可能原因

未设置路由规则，导致扩展网卡的IP无法访问。

操作指引

本文提供Linux和Windows云服务器的操作指导，具体请参见**表1-4**。

表 1-4 操作指引说明

操作系统类型	IP类型	操作步骤
Linux	IPv4	本文以CentOS 8.0 64bit操作系统为例： **为多网卡Linux云服务器配置策略路由（IPv4/IPv6）**
	IPv6	
Windows	IPv4	本文以Windows 2012 64bit操作系统为例： **为多网卡Windows云服务器配置策略路由（IPv4/IPv6）**
	IPv6	

2 操作系统类（Windows）

2.1 Windows 云服务器如何保持会话连接长时间不断开?

操作场景

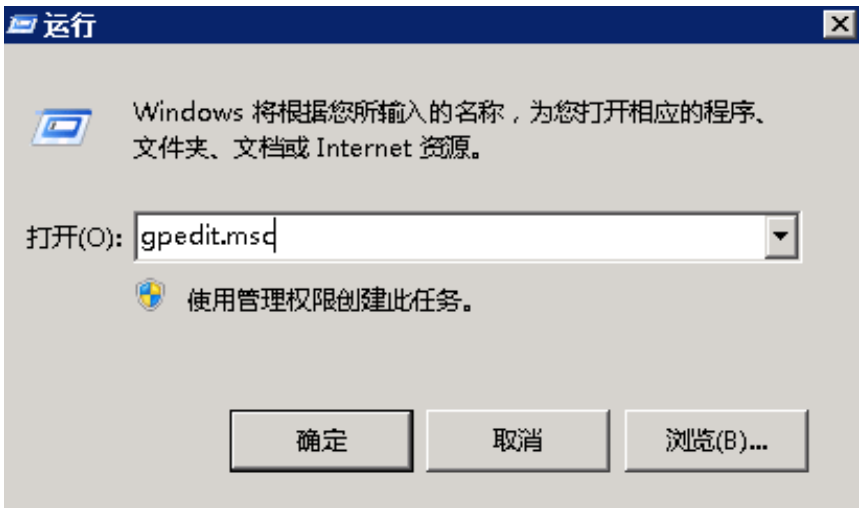
本节操作介绍如何设置Windows服务器长时间保持远程桌面不被自动断开。

操作步骤

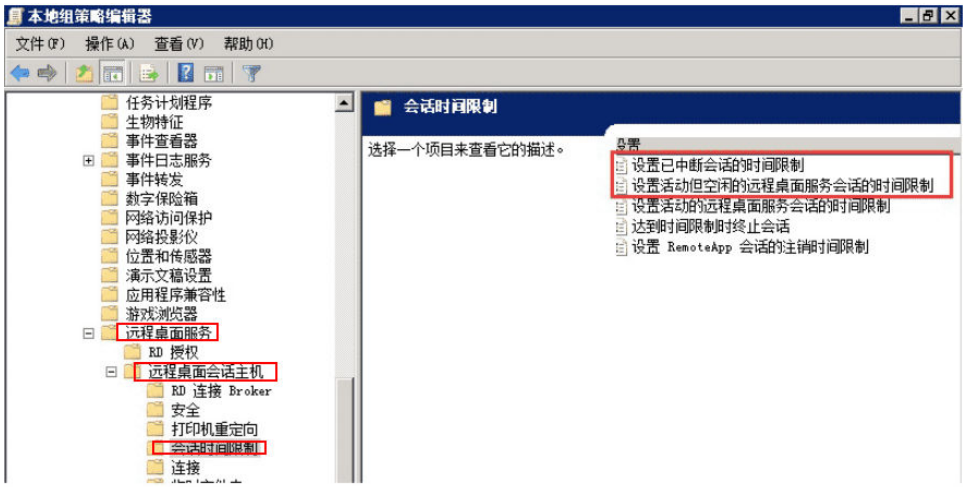
以下操作以Windows 2008操作系统为例。

1. 打开“开始 > 运行”，输入“gpedit.msc”，打开“本地组策略编辑器”。

图 2-1 gpedit.msc

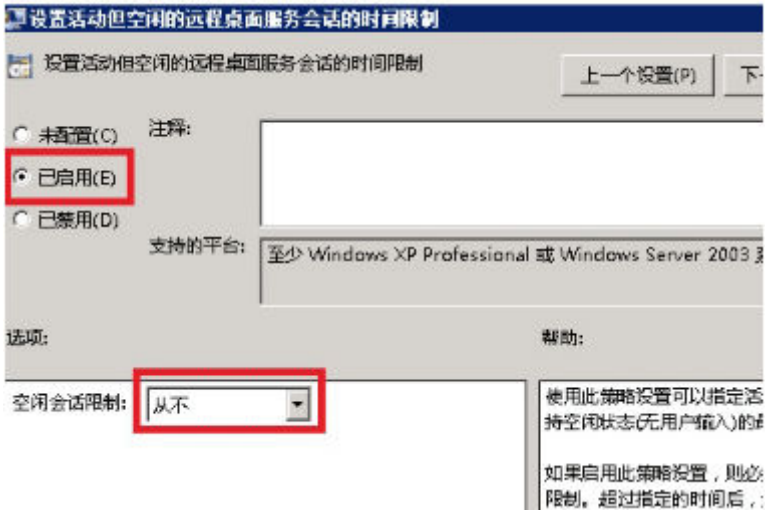


2. 选择“计算机配置 < 管理模板 < Windows组件 < 远程桌面服务 < 远程桌面会话主机 < 会话时间限制”。



3. 设置已中断会话的时间限制。
   - 选择“已启用”。
   - 结束已断开连接的会话：从不。

4. 设置活动但空闲的远程桌面服务会话的时间限制。
   - 选择“已启用”。
   - 空闲会话限制：从不。

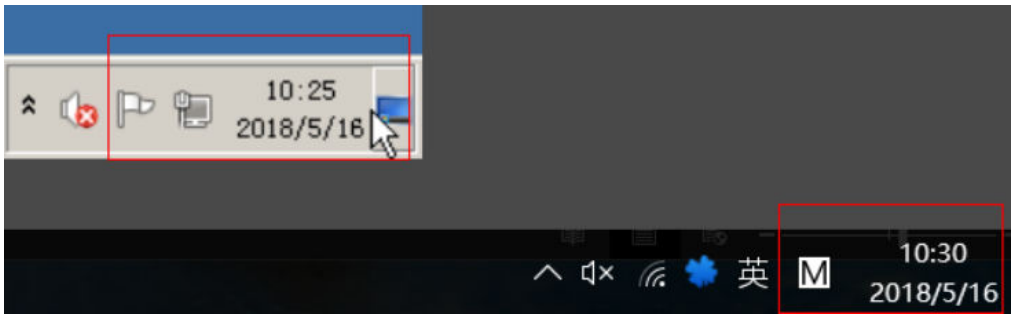


2.2 云服务器时间与标准时间不一致

问题描述

云服务器显示的Windows操作系统时间与本地标准时间不一致。

图 2-2 操作系统时间与本地标准时间不一致



可能原因

系统时间由于受到网络或一些进程驱动的影响可能会出现和标准时间不一致的情况。

处理方法 1

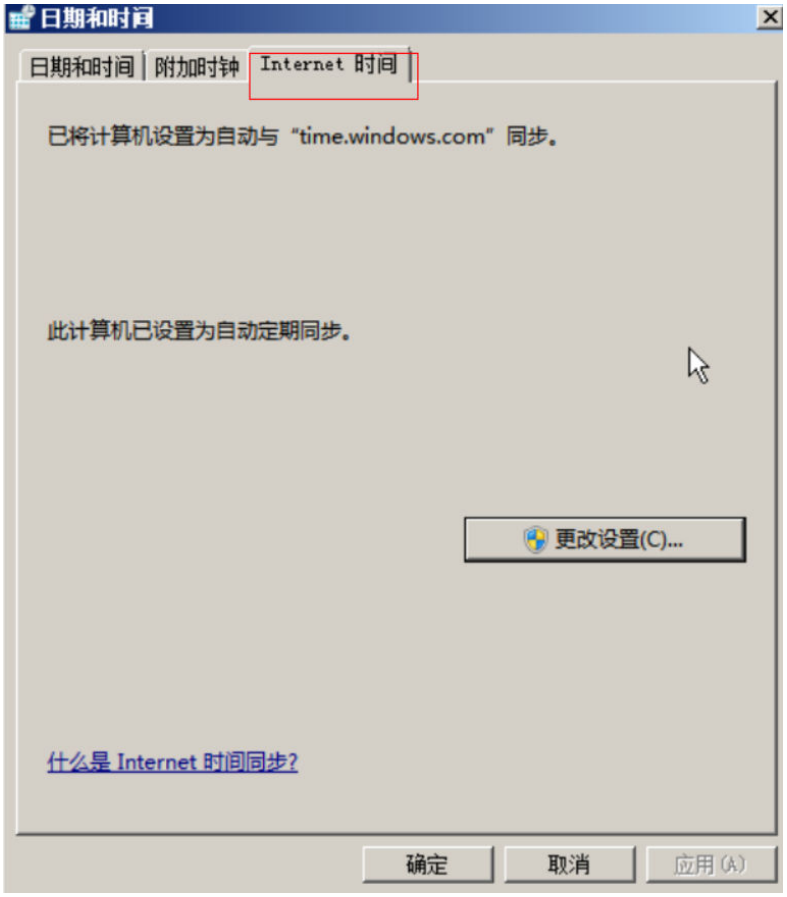
手动同步系统时间。

1. 单击桌面右下角的“更改日期和时间设置”，打开“日期和时间”窗口。

图 2-3 日期和时间

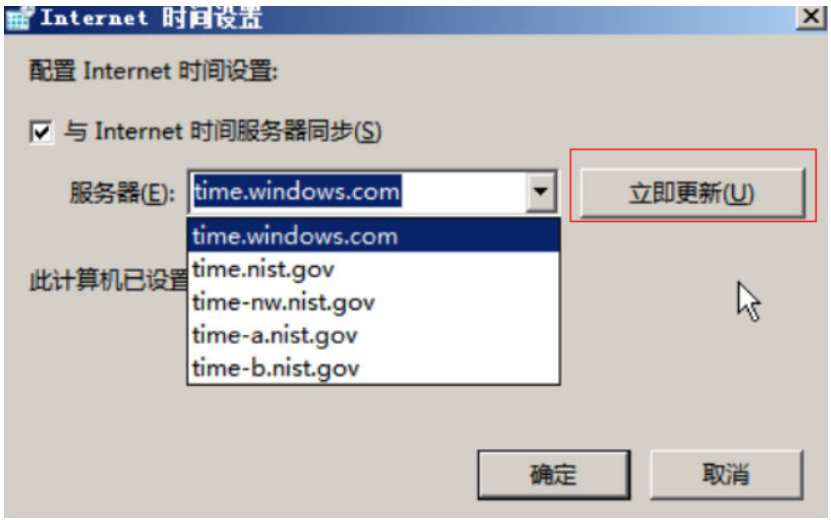
2. 选择“Internet时间”页签。

图 2-4 Internet 时间



3. 单击“更改设置”，并选择时间源。
   默认时间源为“time.windows.com”。
4. 依次单击“立即更新 > 确定”。

图 2-5 更改时间源



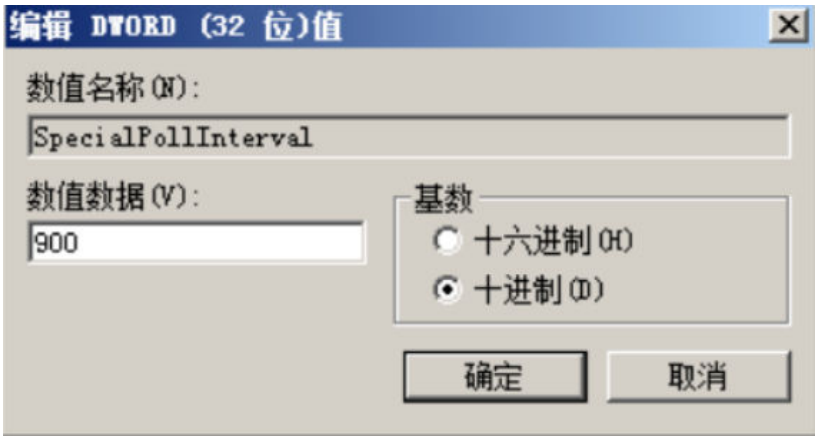
5. 检查Windows系统时间与本地标准时间是否一致。

处理方法 2

通过注册表，修改Windows时间的更新频率。

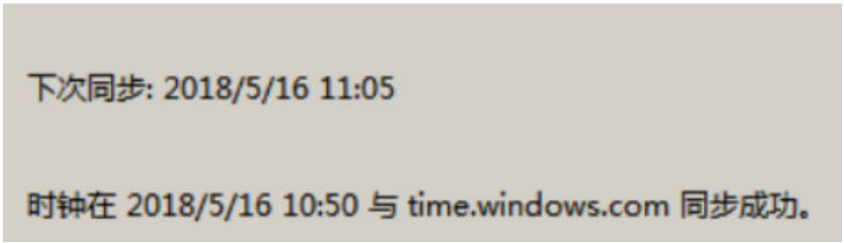
1. 打开“运行”对话框，输入“regedit”进入注册表编辑器。
2. 依次选择HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > W32Time > TimeProviders > NtpClient ，并双击SpecialPollInterval键值。
3. 将对话框中的“基数”栏选择为“十进制”。
4. 设定时间同步周期。
   “数值数据”中显示的数字正是自动对时的间隔（以秒为单位），请根据具体情况设置。

   图 2-6 设定时间同步周期



5. 单击“确定”保存关闭对话框。
6. 配置完成后，打开“cmd”命令窗，执行以下命令，刷新组策略。
   gpupdate
7. 在Internet时间里查看，如图2-7所示，可见时间同步频率已经每变成15分钟一次。

   图 2-7 查看时间同步频次



处理方法 3

安装NTP服务器，具体操作请参见“**华为云有没有提供NTP服务器，怎样安装？**”。

2.3 Windows 云服务器配置双网卡公网访问

操作场景

Windows云服务器共计1块主网卡、1块扩展网卡，且两块网卡均绑定弹性公网IP，实现公网访问。

约束限制

操作过程中，请保持主网卡的配置，不要修改。

操作步骤

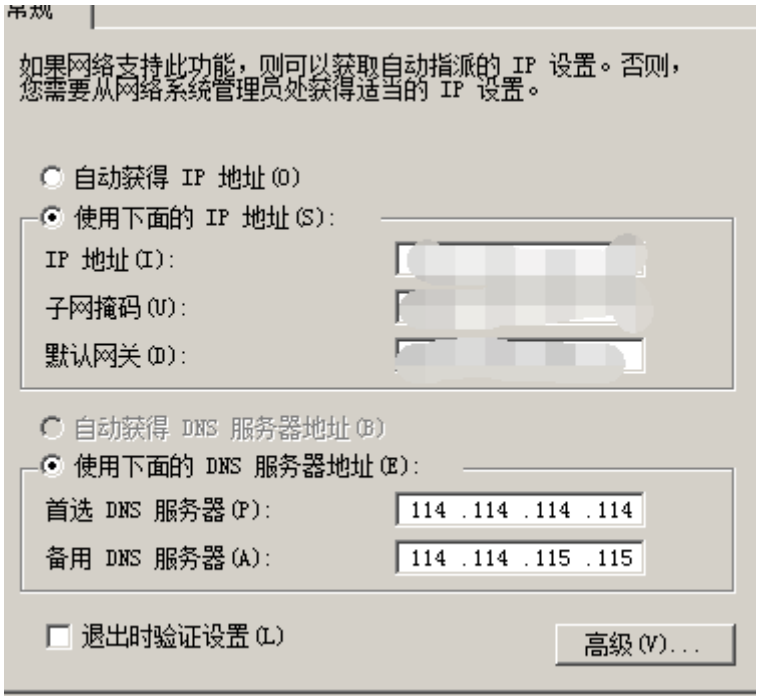
1. 登录控制台，并选择“计算 > 弹性云服务器”。
2. 在云服务器列表页，选中待添加网卡的云服务器。
3. 单击云服务器名称，进入详情页。
4. 选择“弹性网卡”页签。
5. 单击“绑定弹性网卡”，根据界面提示添加扩展网卡。

   扩展网卡的安全组、子网需和主网卡保持一致。

   扩展网卡添加成功后，系统会自动获取私有IP地址。
6. 远程登录云服务器。
7. 单击右下角“打开网络和共享中心”，打开左上角“更改适配器设置”，找到新添加的网卡。

8. 选择您要设置网络连接，然后右击图标，选择“属性”。
9. 在网络连接属性面板中“网络”选项下，选中“Internet 协议版本 4(TCP/IPv4)”，然后单击下面的“属性”。
10. 在属性面板中，切换到常规选项下，将5中自动获取的私有IP地址，使用静态地址配置给新添加的网卡。



示例：

- 私有IP地址：192.168.1.11
- IP地址：192.168.1.11
- 子网掩码：255.255.255.0
- 默认网关：192.168.1.1
- 首选DNS服务器：114.114.114.114
- 备用DNS服务器：114.114.115.115

11. 配置完成后，勾选“退出时验证设置”。
12. 重启网卡，然后绑定弹性公网IP即可。

2.4 Windows 云服务器不能复制粘贴内容?

问题描述

远程连接Windows云服务器后，不能复制、粘贴内容，右键单击菜单栏，“粘贴”选项置灰。

可能原因

- 未进行本地驱动器映射。
- 服务器rdpclip.exe进程异常。
- 系统禁止云服务器和本地主机之间进行文件的复制粘贴功能。

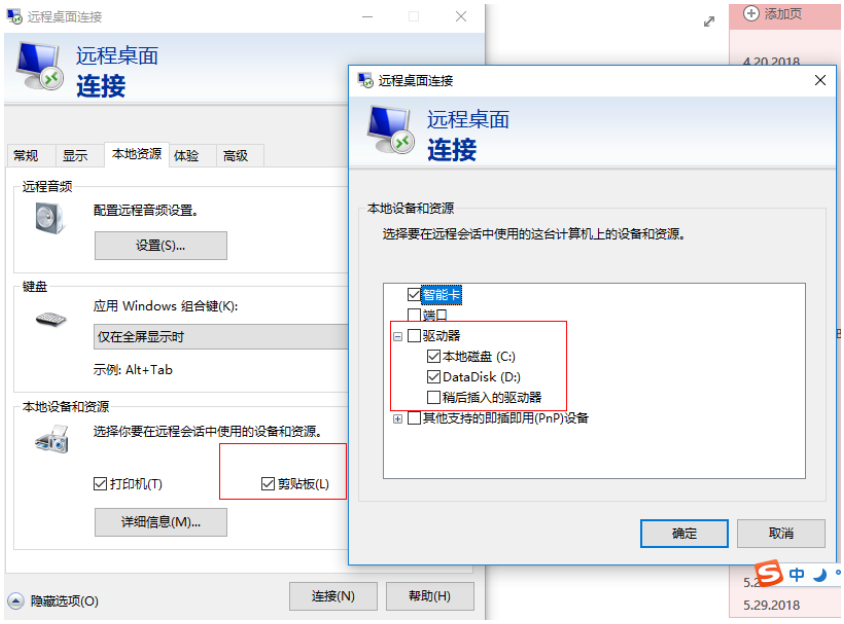
处理方法

- 未进行本地驱动器映射，图2-8以使用本地的C盘、D盘映射为例。
  a. 在运行窗口输入“mstsc”回车打开“远程桌面连接”。

b. 选择“本地资源”页签，并勾选“本地设备和资源”栏的“剪切板”、“驱动器”。

c. 单击“确定”，检查复制、粘贴功能是否恢复正常。

图 2-8 本地资源



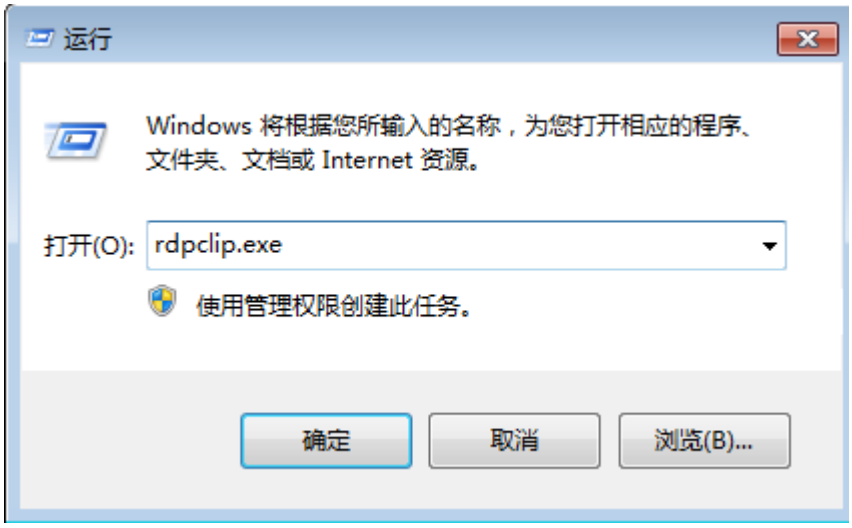
- 服务器rdpclip.exe进程异常，需要重启rdpclip.exe进程。

  a. 远程桌面连接服务器，启动Windows任务管理器，在进程页签下结束rdpclip.exe进程。

  图 2-9 结束 rdpclip.exe 进程

  b. 打开“开始”菜单中的“运行”窗口，输入“rdpclip.exe”，重新启动rdpclip.exe。

图 2-10 启动 rdpclip.exe 进程



c. 检查复制、粘贴功能是否恢复正常。

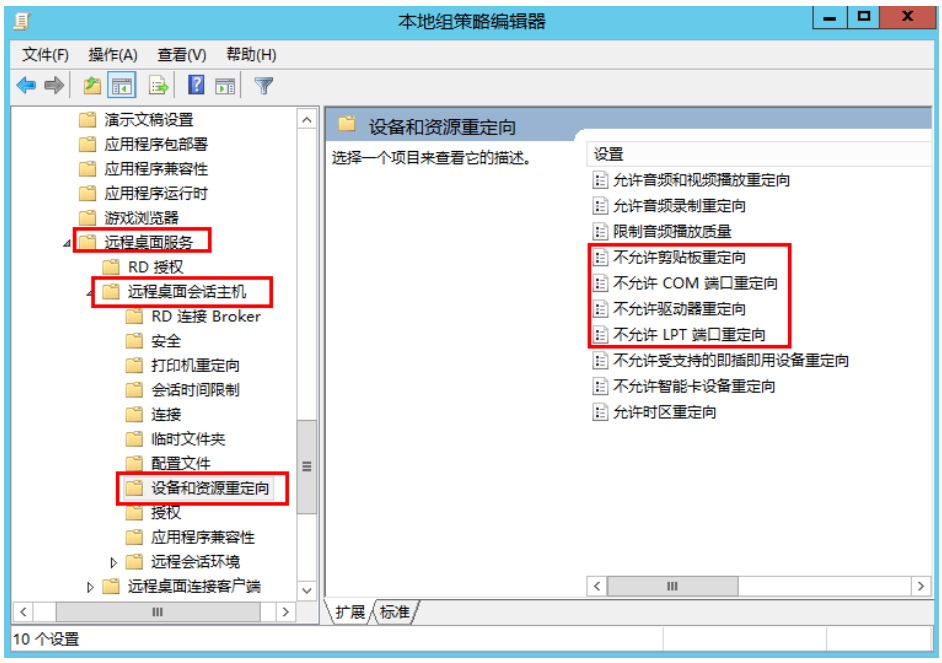
- 系统禁止云服务器和本地主机之间进行文件的复制粘贴功能，需重新配置云服务器的本地组策略编辑器，开启复制粘贴功能。

  a. 打开“开始 > 运行”，输入“gpedit.msc”，打开“本地组策略编辑器”。

  b. 依次找到：“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 > 设备和资源重定向”。

  c. 将“不允许剪切板重定向”、“不允许COM端口重定向”、“不允许驱动器重定向”、“不允许LPT端口重定向”都设置为“已禁用”。

图 2-11 设备和资源重定向



d. 设置完成之后重启云服务器使配置生效，检查复制、粘贴功能是否恢复正常。

2.5 Windows 云服务器配置文件共享和网络磁盘映射方法

操作场景

本节操作介绍在内网环境下，Windows云服务器之间怎样实现文件夹共享。

约束限制

部分运营商可能会屏蔽139、445端口，导致广域网无法访问共享。因此，Windows云服务器文件共享方案建议仅在内网环境下使用。

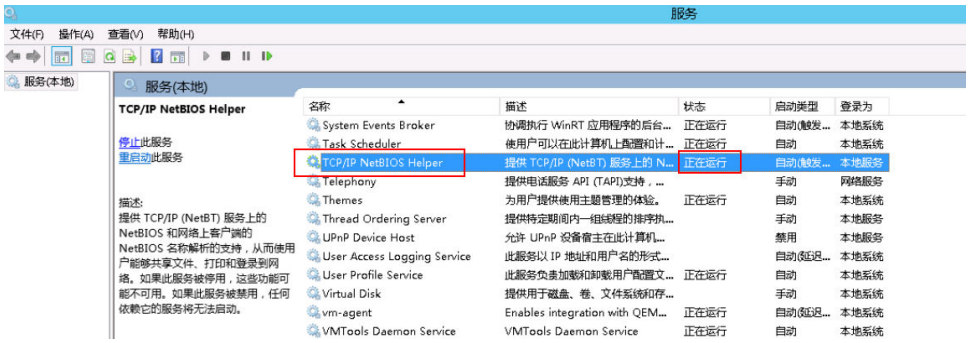
操作步骤

步骤1 确认共享的两台Windows云服务器配置正确，具体包括如下几个方面：

- 确保“Tcp/IP NetBIOS Helper”服务状态为“已启动”。

  打开cmd窗口执行命令**services.msc**，找到TCP/IP NetBIOS Helper服务，查看TCP/IP NetBIOS Helper服务的状态。

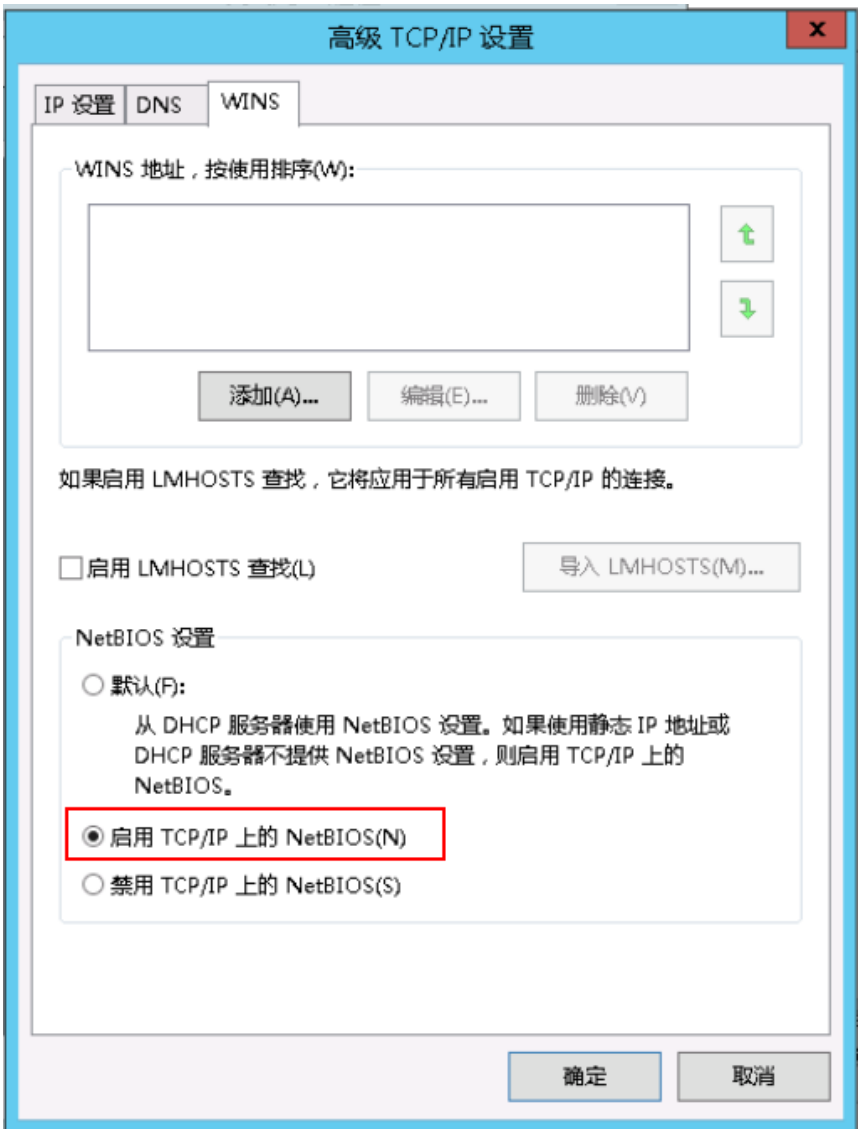
  图 2-12 Tcp/IP NetBIOS Helper

- 网卡中启用TCP/IP上的NetBIOS服务。

  右键单击“打开网络和共享中心”，单击“更改适配器设置”，选择以太网，右键单击“属性”，双击“internet协议版本4（TCP/IPv4）”，单击“高级 > WINS”页签，选择“启用TCP/IP上的NetBIOS（N）”。

图 2-13 启用 TCP/IP 上的 NetBIOS 服务



- Windows云服务器防火墙开放了139、445端口的入站访问策略。

步骤2 修改网络和共享中心。

1. 打开“网络和共享中心”。
2. 单击“更改高级共享设置”。

图 2-14 更改高级共享设置

3. 两台Windows云服务器所属的网络应一致，如均为“公用”或均为“专用”，并勾选“启用网络发现”、“启用共享以便可以访问网络的用户可以读取和写入公用文件夹中的文件”。

图 2-15 启用网络发现

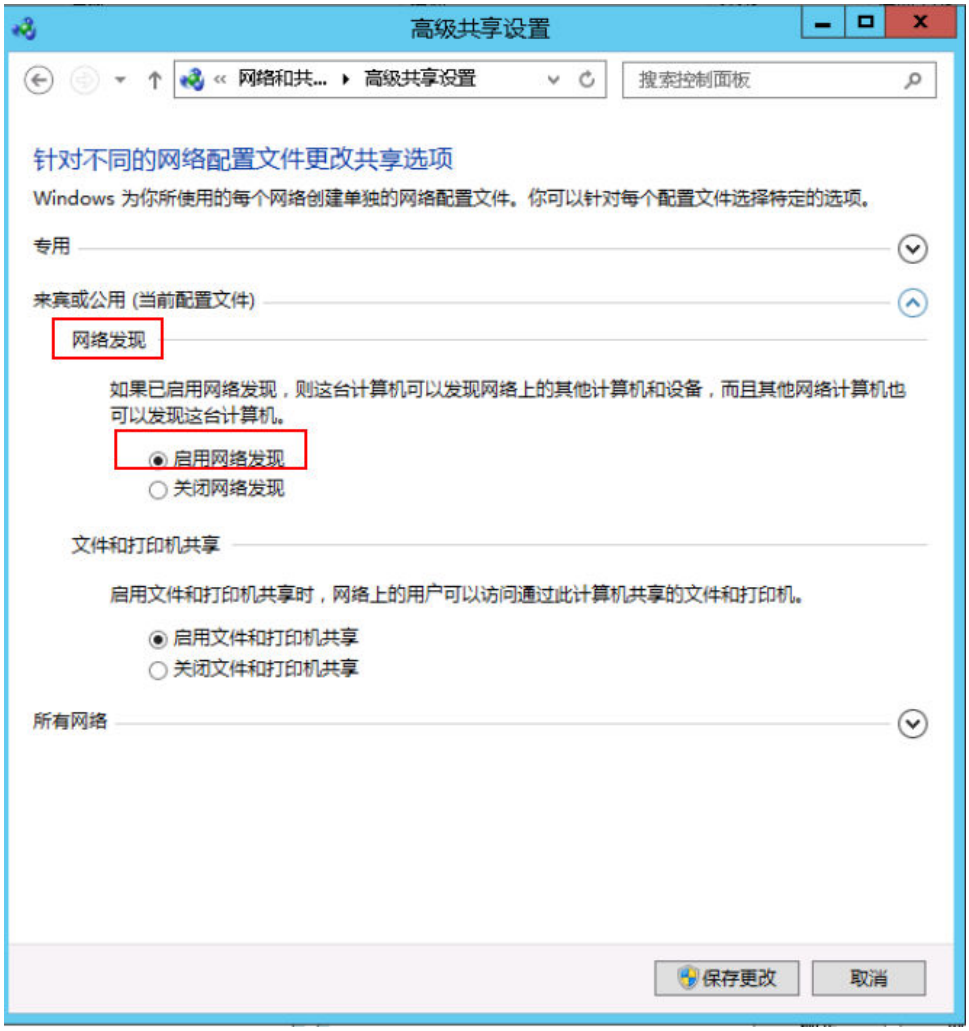
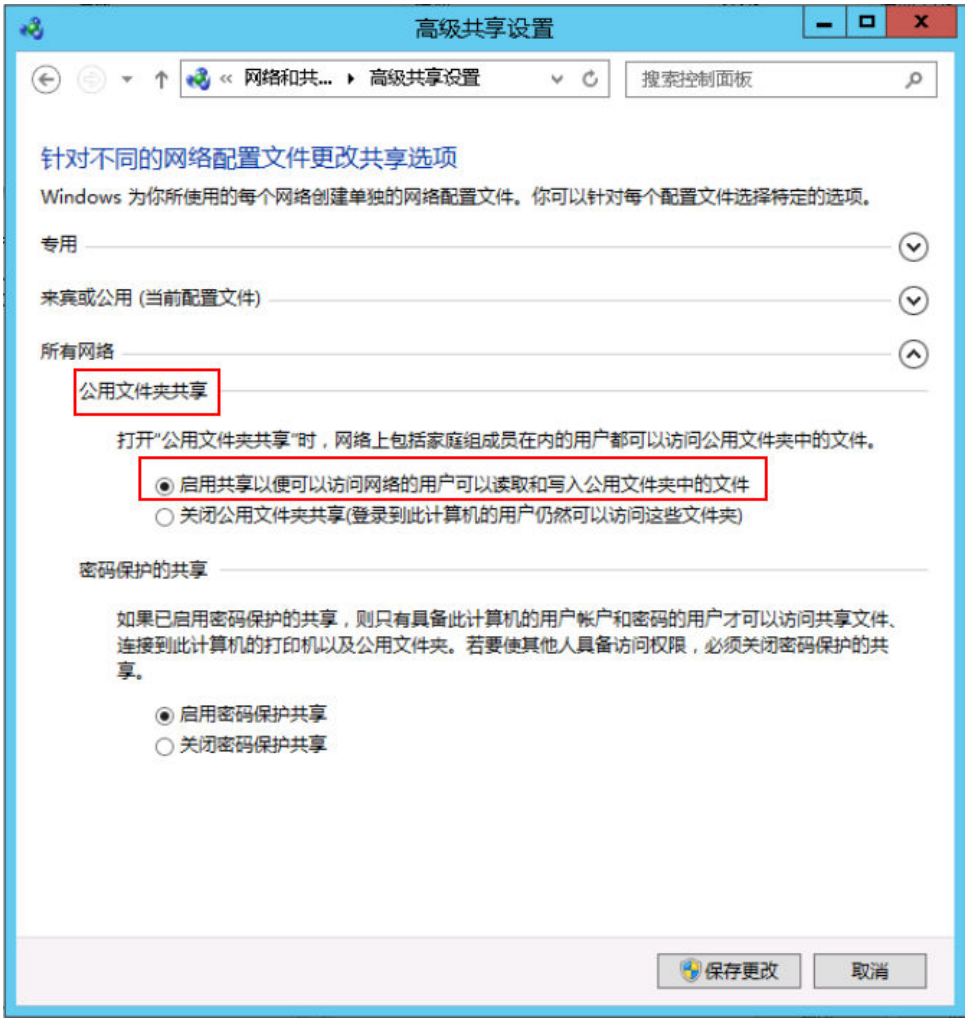


图 2-16 启用共享以便可以访问网络的用户可以读取和写入公用文件夹中的文件



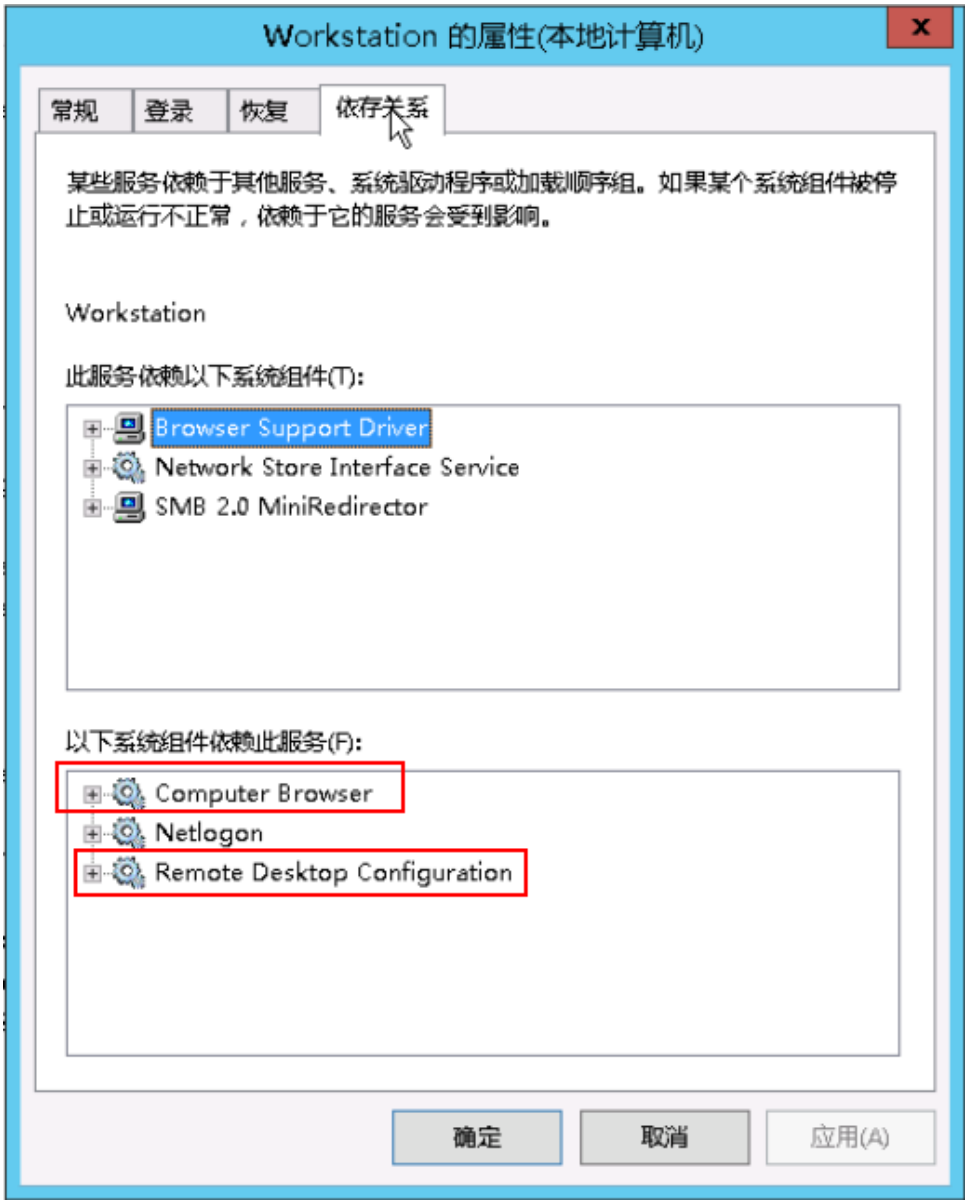
如果无法启用网络发现功能，您可以通过运行services.msc，启动“服务”管理器。请检查网络发现功能依赖的服务是否均已启用。网络发现功能依赖的服务包括：

- Function Discovery Resource Publication
- SSDP Discovery
- UPnP Device Host

4. 在“服务”管理器中，开启Workstation服务。

   该服务有依赖组件，开启workstation服务时，必须启动依赖组件Computer Browser和Remote Desktop Configuration。

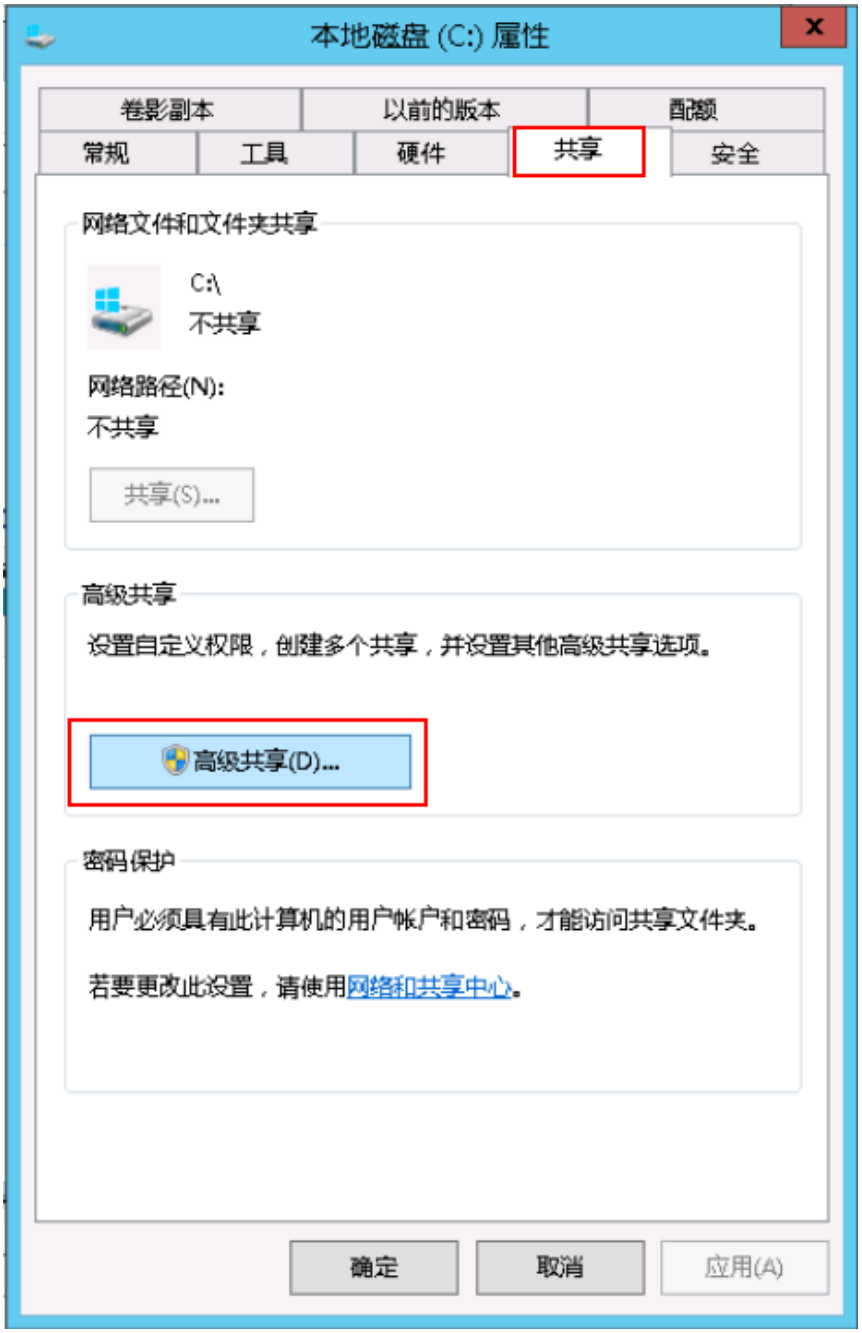
图 2-17 开启 Workstation 服务



步骤3 在需要提供磁盘共享访问的云服务器上，设置磁盘共享。

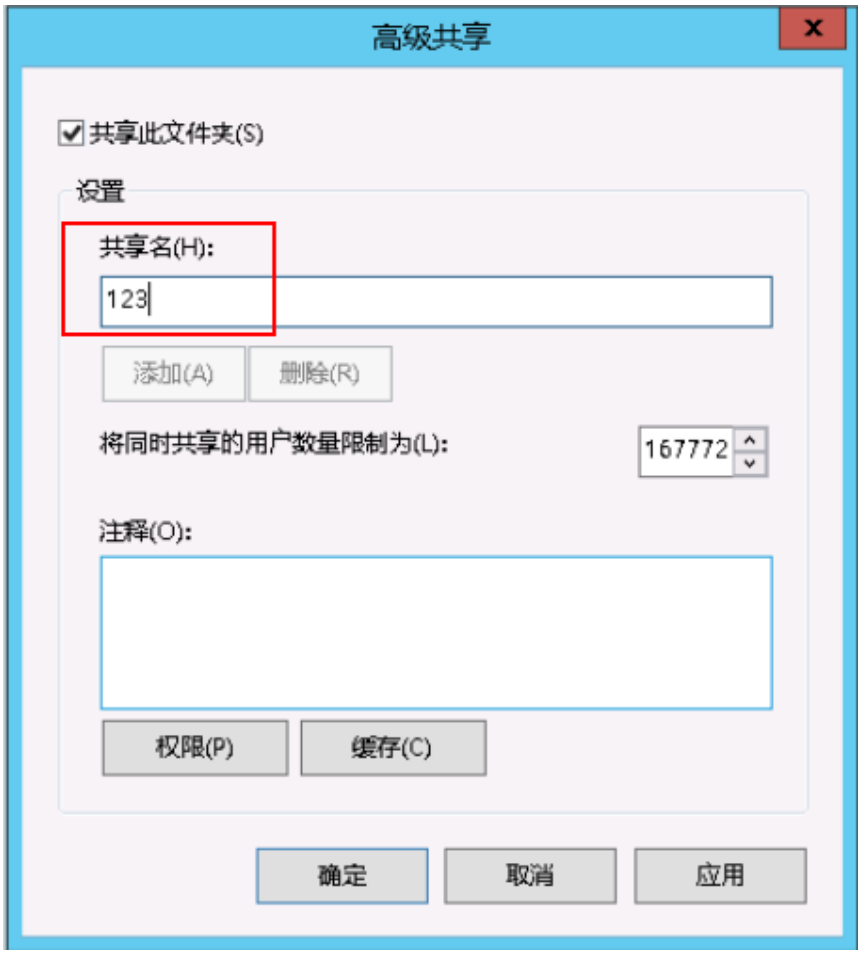
1. 右键单击磁盘，选择“属性”。
2. 选择“共享”页签，并单击“高级共享”。

图 2-18 设置磁盘共享



3. 设置“共享名”，并单击“确定”。
   给共享文件夹自定义一个名称。

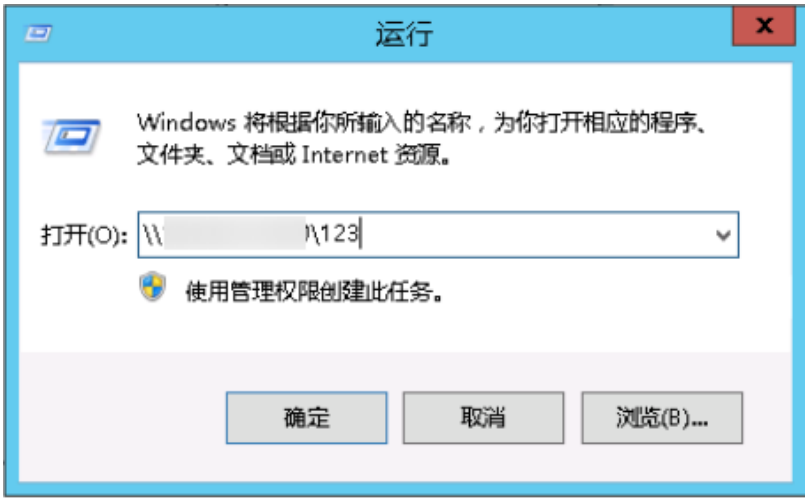
图 2-19 设置共享文件夹名称



步骤4 打开同一地域下的另一台云服务器，通过内网访问共享文件夹。

1. 打开“运行”窗口。
2. 输入“\\内网IP地址\123”，并单击“确定”，即可打开共享文件夹。

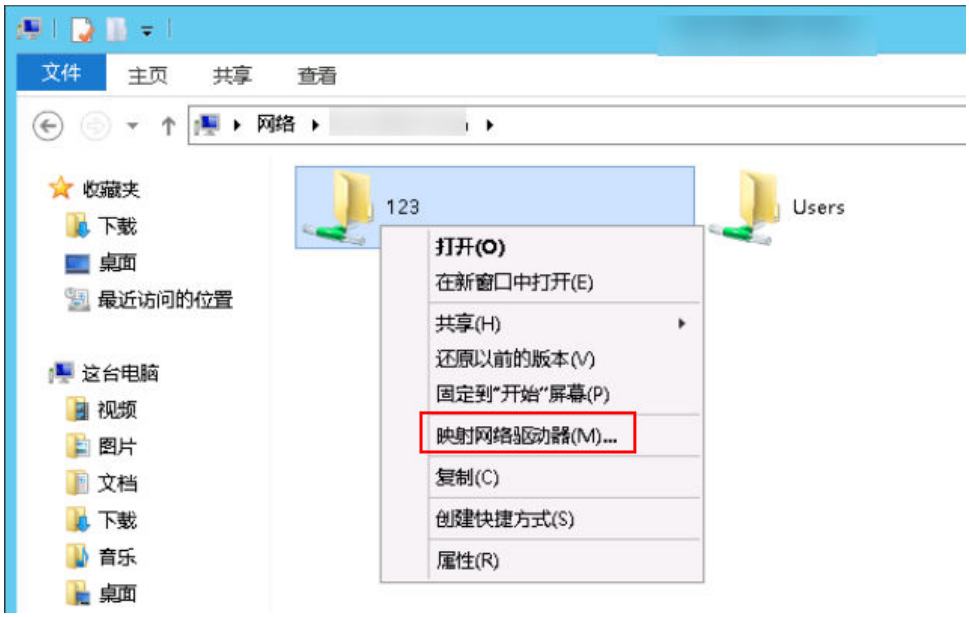
图 2-20 访问共享文件夹



步骤5 （可选）为了更加方便的访问共享文件夹，您可以将共享路径文件，创建一个网络驱动器映射。

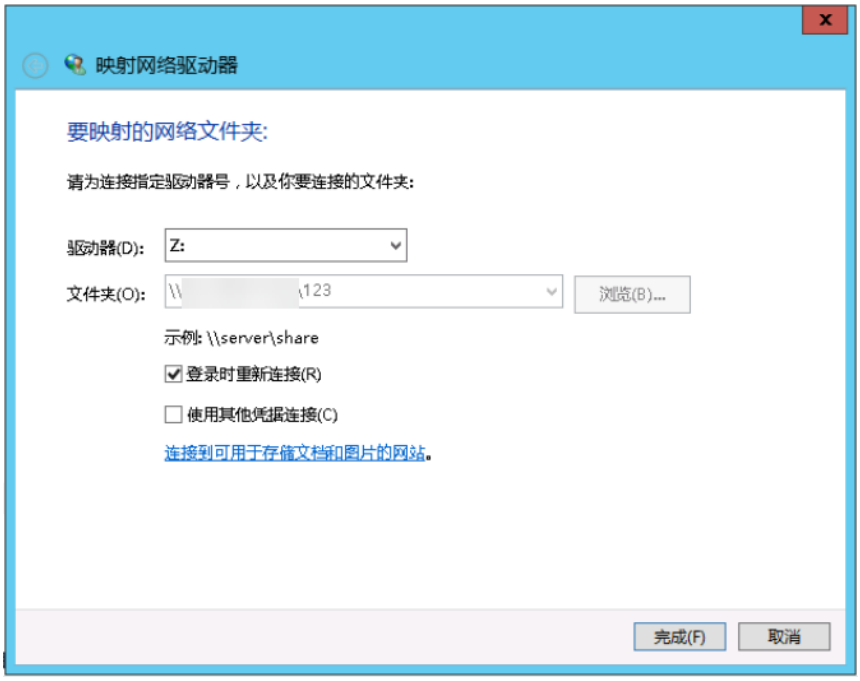
1. 选择共享的文件夹，右键单击“映射网络驱动器”。

图 2-21 创建映射



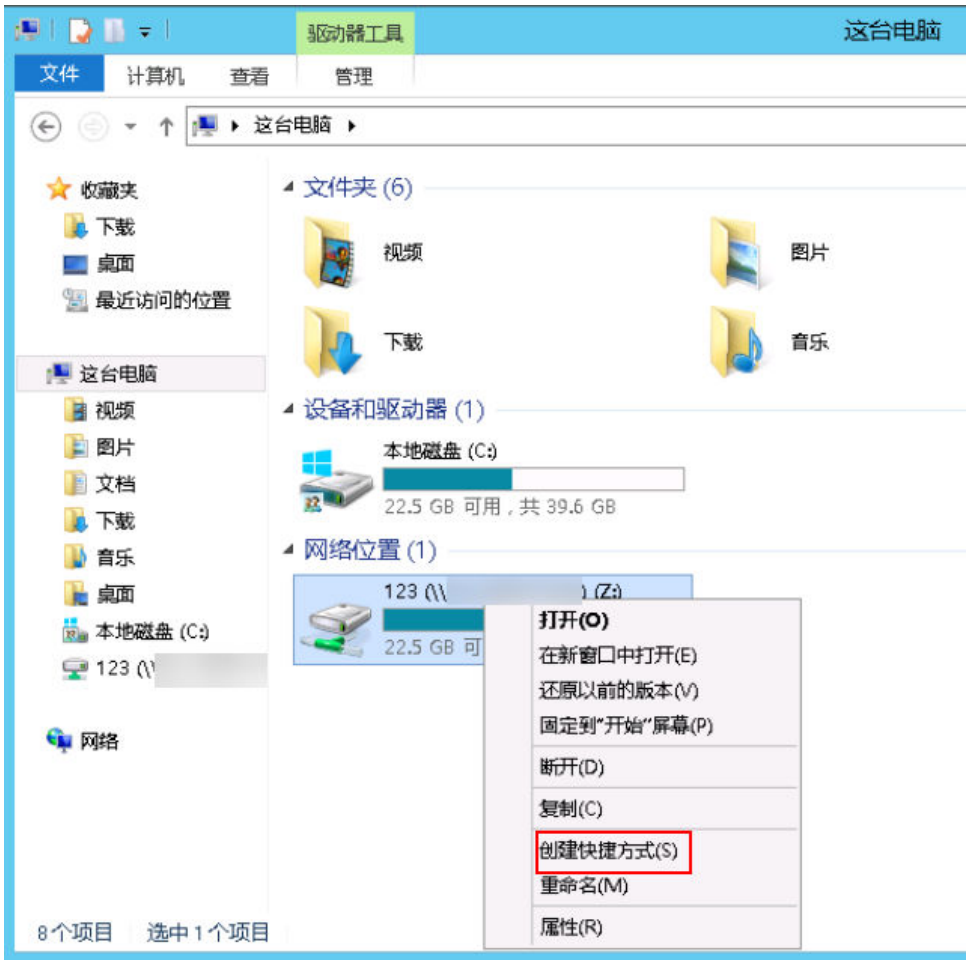
2. 创建映射网络驱动器。

图 2-22 映射网络驱动器



3. 单击映射网络驱动器名称，单击“创建快捷方式”并发送到桌面。
   您就可以通过双击创建的快捷方式，快速访问共享文件夹了。

图 2-23 创建快捷方式



----结束

2.6 启动 Tomcat 时报错，提示 80 端口被占用怎么办?

问题描述

当Windows系统云服务器启动Tomcat时报错，提示80端口被占用。

本节操作以Windows Server 2008 R2操作系统为例介绍排查80端口占用的操作步骤。

可能原因

此应用使用的端口被其他程序或者病毒木马占用。

1. 使用**netstat -ano | find "80"** 看到占用端口的进程ID是4。

   说明

   请根据实际情况修改端口。

图 2-24 查看占用端口的进程 ID

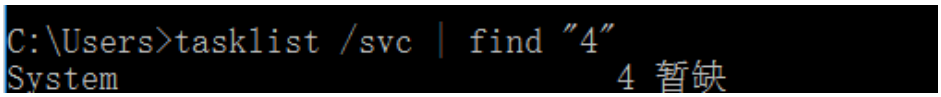
```
C:\Users>netstat -ano | find ":80"
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
```

2. 执行**tasklist /svc | find "4"** 看到的是系统进程。

   说明

   请根据实际情况修改端口。

   图 2-25 系统进程

通过查看发现80端口被系统System进程占用

处理方法

说明

此操作可能需要关闭正在运行的业务或者重启云服务器。

方法一：

1. 以管理员身份运行cmd，输入**net stop http**。
2. 若需要停止对应服务，则选择**Y**
3. 执行**sc config http start= disabled**

方法二：

1. 在cmd下运行**regedit**打开注册表
2. 找到注册表HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > services > HTTP，修改Start，将其改为0。
3. 重启云服务器。

2.7 输入法无法使用怎么办?

问题描述

- 登录云服务器后无法切换输入法，按ctrl+shift不生效，右下角不显示输入法栏。
- 想切换其他语言的输入法怎么办?

可能原因

- 因为ctfmon.exe进程没有启动导致的
- 关闭了输入指示系统图标

输入法不显示处理方法

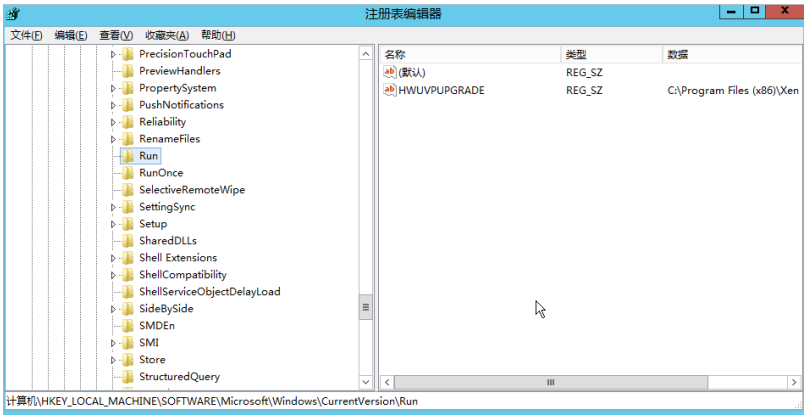
方法一：检查是否启动了ctfmon.exe进程。

1. 打开C:\Windows\System32，
2. 双击运行ctfmon.exe，查看右下角是否显示输入法栏，能否切换输入法。
3. 设置开机自启动：

a. 在运行窗口输入“regedit”回车，打开注册表编辑器。

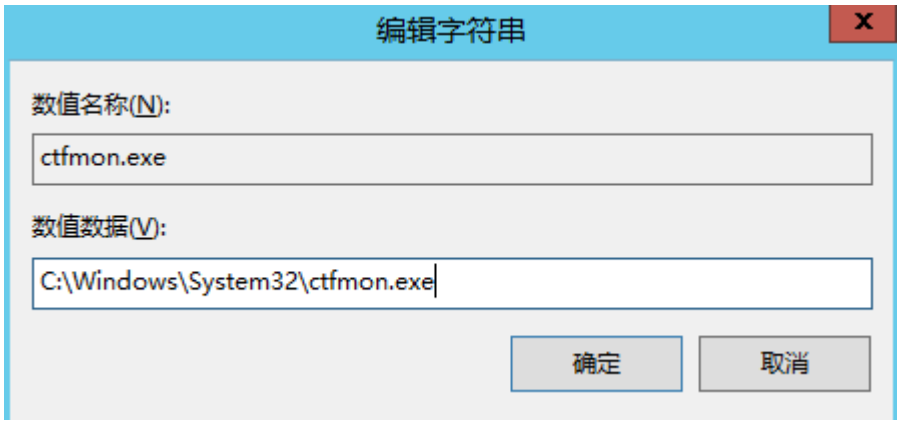
b. 在目录HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Windows > CurrentVersion > Run下，新建一个注册表文件ctfmon.exe。

图 2-26 Run 目录



c. 修改字符串的数值数据为ctfmon.exe的存储位置：C:\Windows\System32\ctfmon.exe

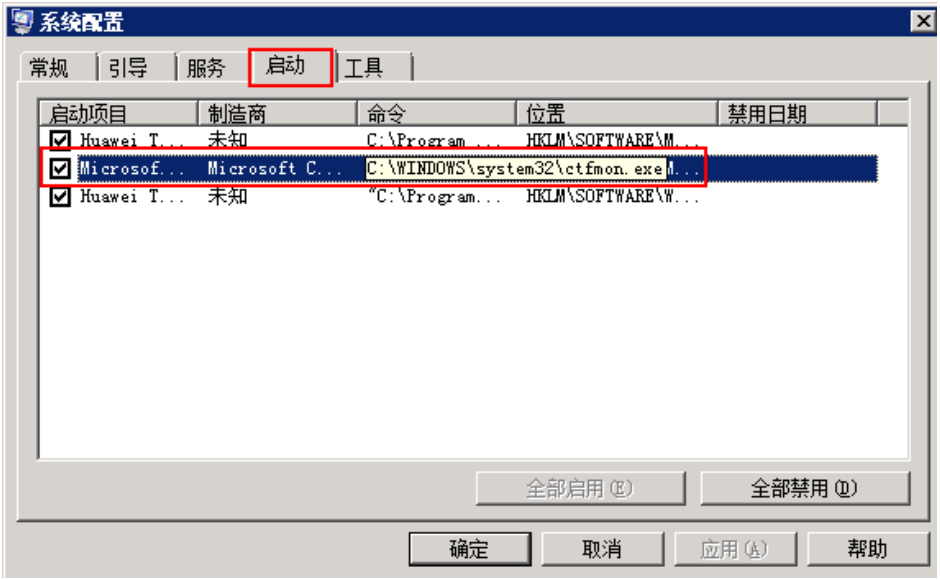
图 2-27 修改字符串的数值数据



d. 在运行窗口输入“msconfig”，打开“系统配置使用程序”。

e. 选择“启动”页，找到ctfmon项并在其前面打上钩，分别再单击“应用”和“确定”保存修改后退出，重启云服务器后即可生效。

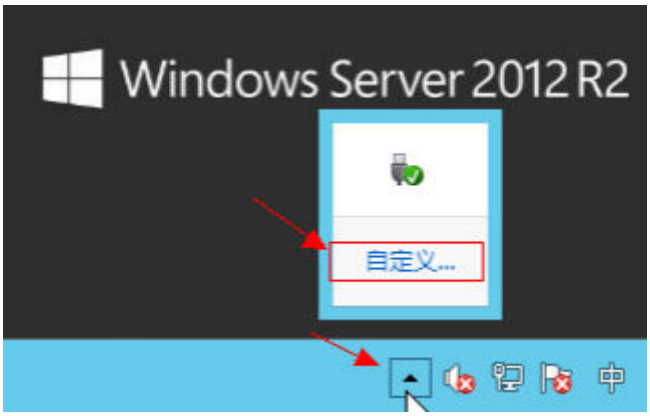
图 2-28 勾选 ctfmon 项



方法二：启用系统图标

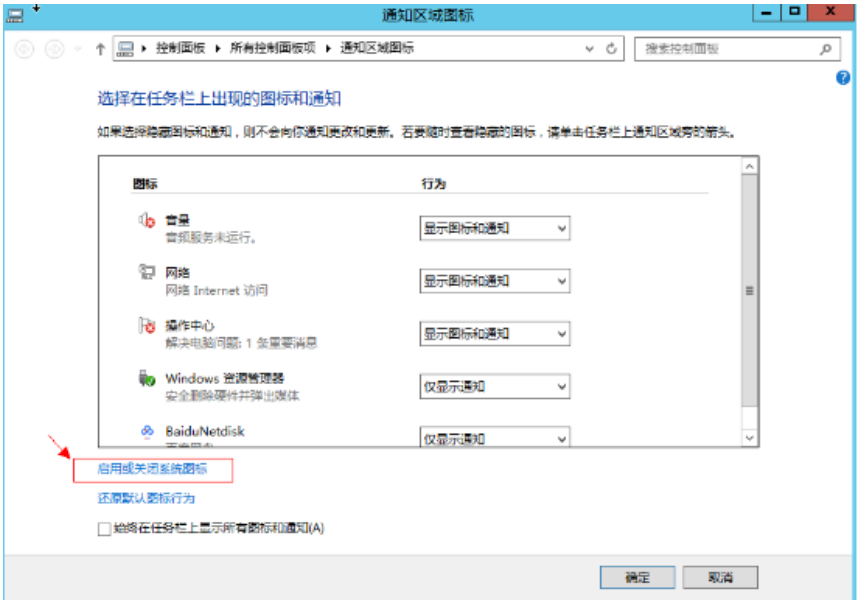
1. 登录云服务器，在云服务器右下角单击“自定义”。

图 2-29 单击“自定义”



2. 在通知区域图标页面，单击“启用或关闭系统图标”。

图 2-30 启用或关闭系统图标



3. 将输入指示选择启用，单击“确定”。

图 2-31 启用输入指示

切换其他语言的输入法

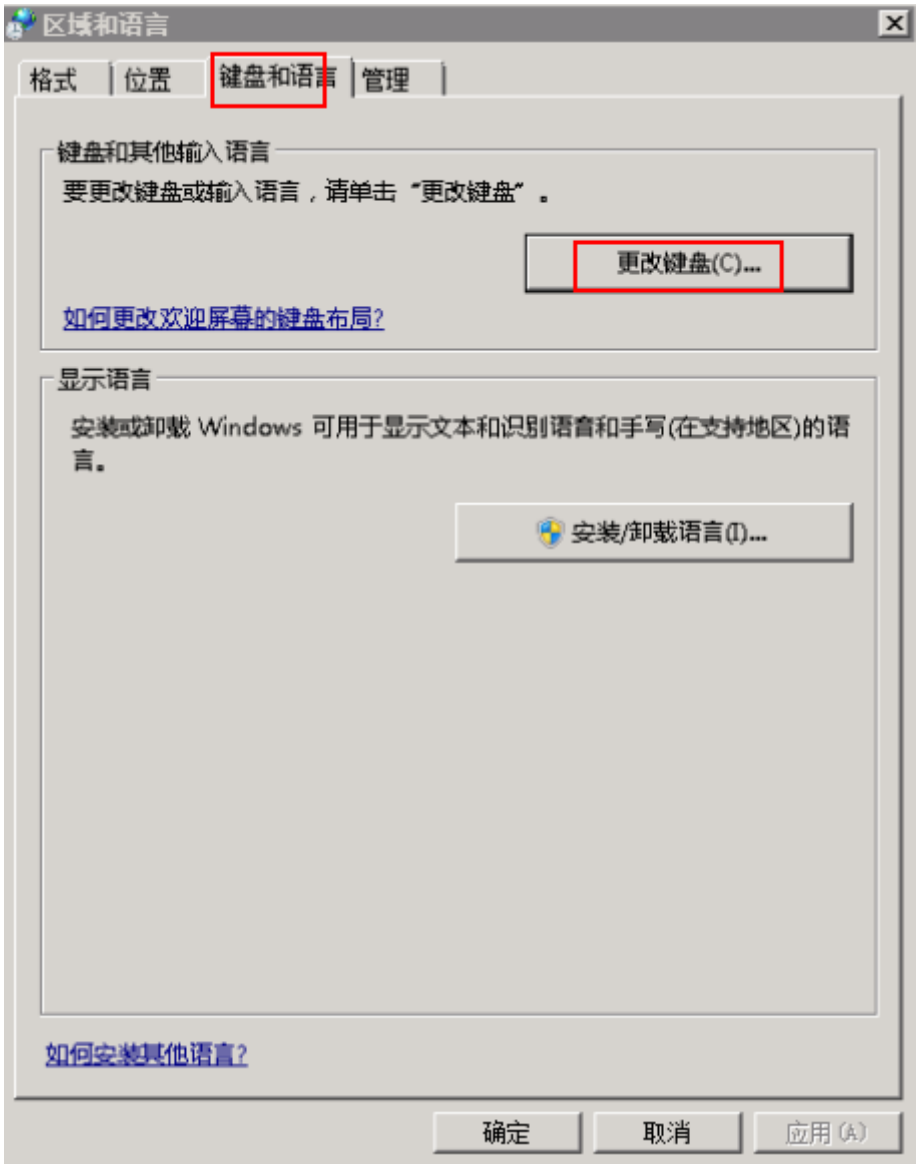
以Windows 2008操作系统云服务器，切换日语输入法为例：

1. 登录云服务器，打开“控制面板”。
2. 单击“区域和语言”选项。

图 2-32 区域和语言

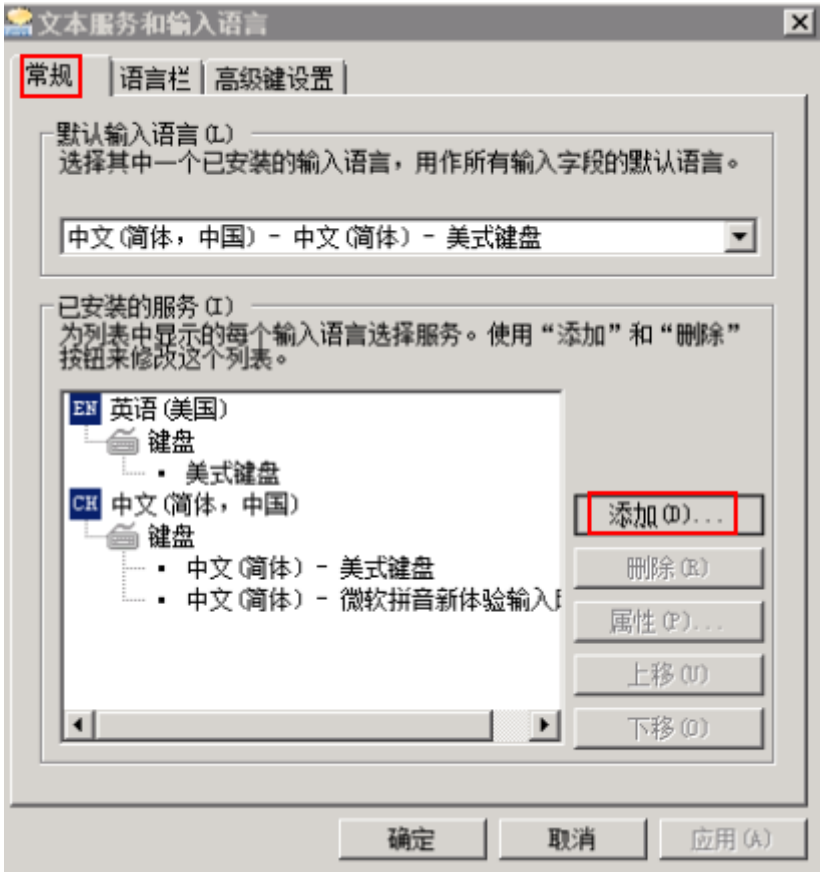
3. 选择“键盘和语言”标签，并单击“更改键盘”。

图 2-33 键盘和语言



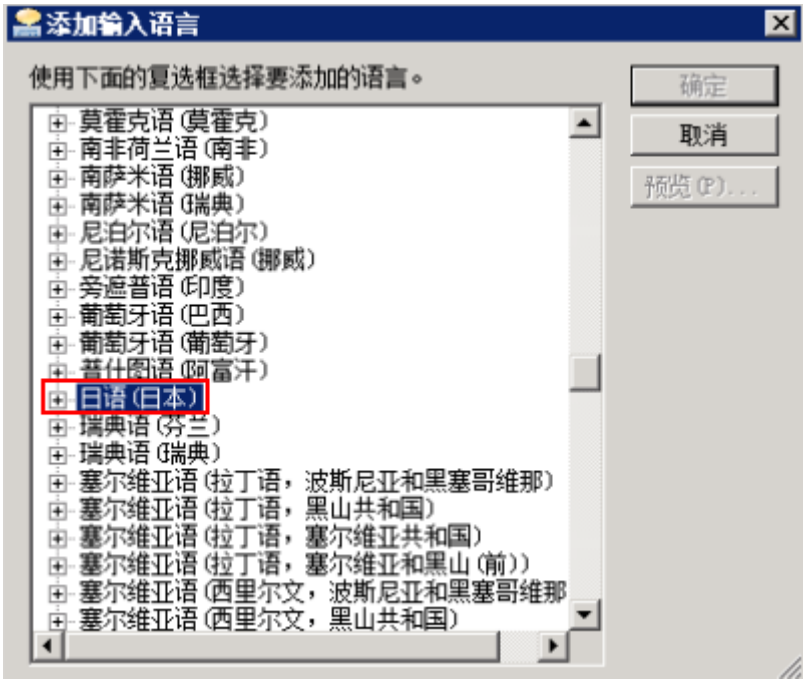
4. 打开“文本服务和输入语言”对话框，在“常规”标签中单击“添加”。

图 2-34 文本服务和输入语言



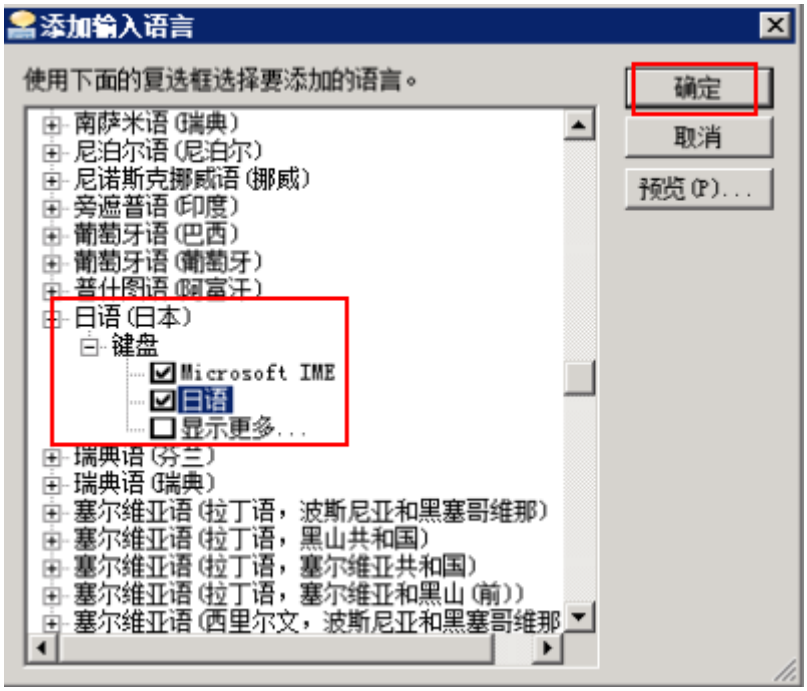
5. 在弹出的“添加输入语言”对话框中，找到“日语（日本）”。

图 2-35 添加输入语言



6. 双击“日语（日本）”展开，双击“键盘”子项展开，勾选“Microsoft IME”和“日语”，单击“确定”，分别再单击“应用”和“确定”保存修改后退出。

图 2-36 选择日语



2.8 怎样设置 Windows 云服务器输入法?

问题描述

Windows云服务器无法切换输入法的语言。

可能原因

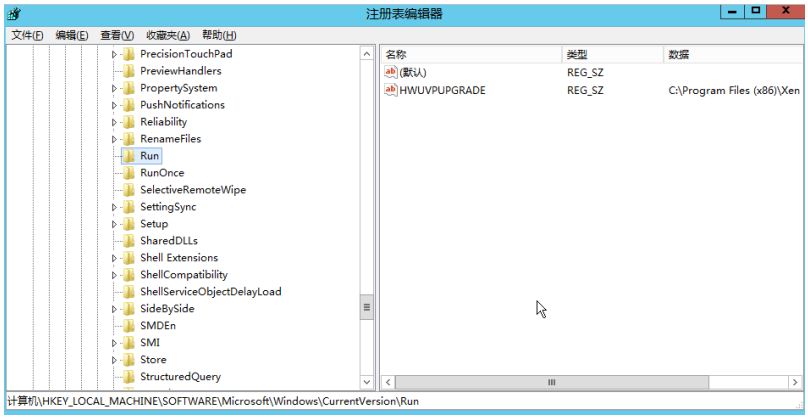
- 因为ctfmon.exe进程没有启动导致的
- 关闭了输入指示系统图标

输入法不显示处理方法

方法一：检查是否启动了ctfmon.exe进程。

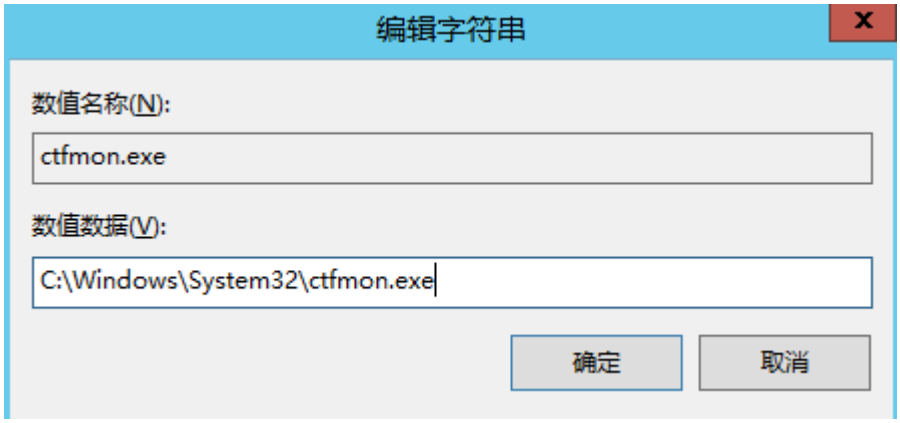
1. 打开C:\Windows\System32，
2. 双击运行ctfmon.exe，查看右下角是否显示输入法栏，能否切换输入法。
3. 设置开机自启动：
   a. 在运行窗口输入“regedit”回车，打开注册表编辑器。
   b. 在目录HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Windows > CurrentVersion > Run下，新建一个注册表文件ctfmon.exe。

图 2-37 Run 目录



c. 修改字符串的数值数据为ctfmon.exe的存储位置：C:\Windows\System32\ctfmon.exe

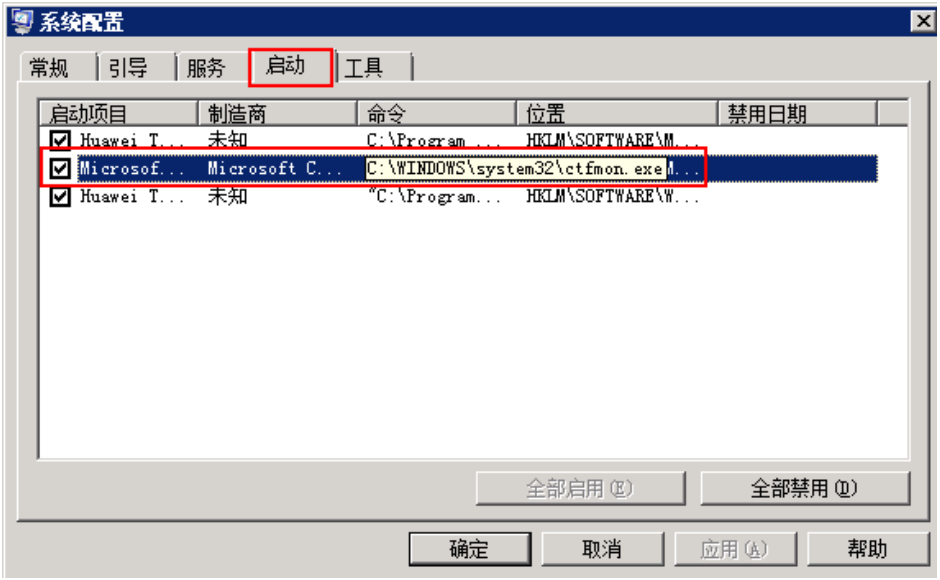
图 2-38 修改字符串的数值数据



d. 在运行窗口输入“msconfig”，打开“系统配置使用程序”。

e. 选择“启动”页，找到ctfmon项并在其前面打上钩，分别再单击“应用”和“确定”保存修改后退出，重启云服务器后即可生效。

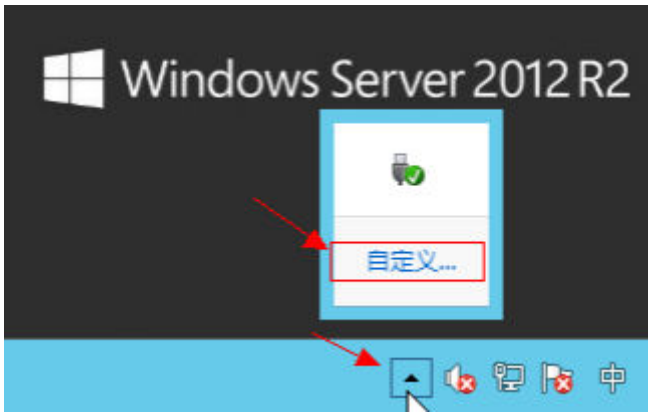
图 2-39 勾选 ctfmon 项



方法二：启用系统图标

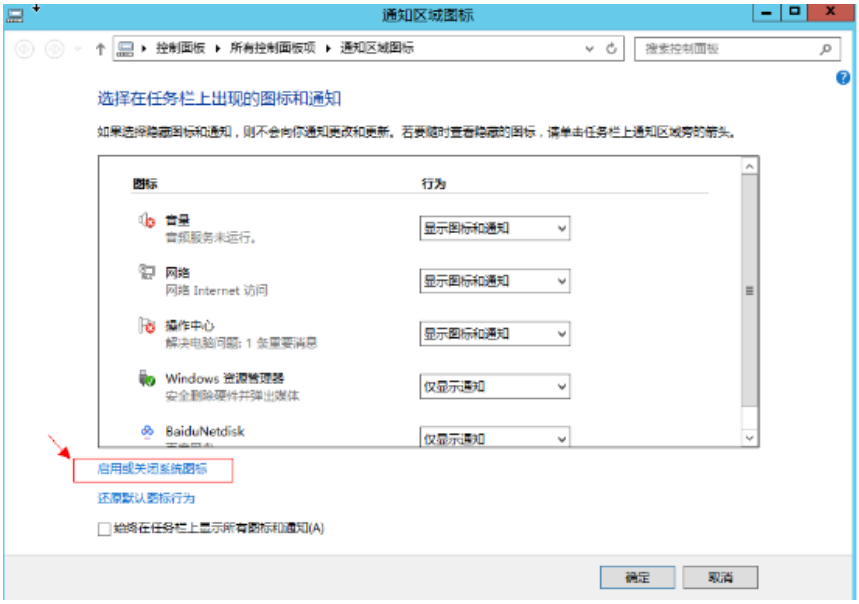
1. 登录云服务器，在云服务器右下角单击“自定义”。

图 2-40 单击“自定义”



2. 在通知区域图标页面，单击“启用或关闭系统图标”。

图 2-41 启用或关闭系统图标



3. 将输入指示选择启用，单击“确定”。

图 2-42 启用输入指示

切换其他语言的输入法

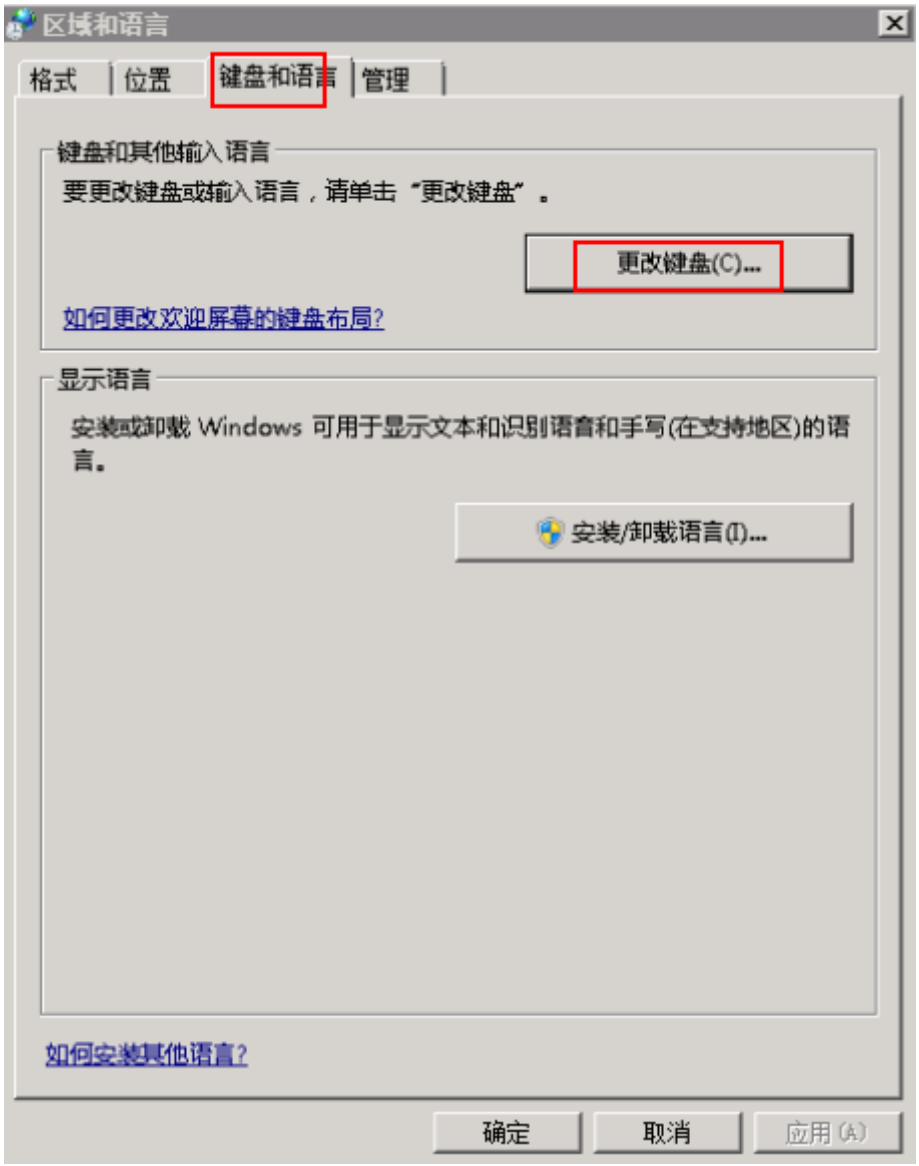
以Windows 2008操作系统云服务器，切换日语输入法为例：

1. 登录云服务器，打开“控制面板”。
2. 单击“区域和语言”选项。

图 2-43 区域和语言

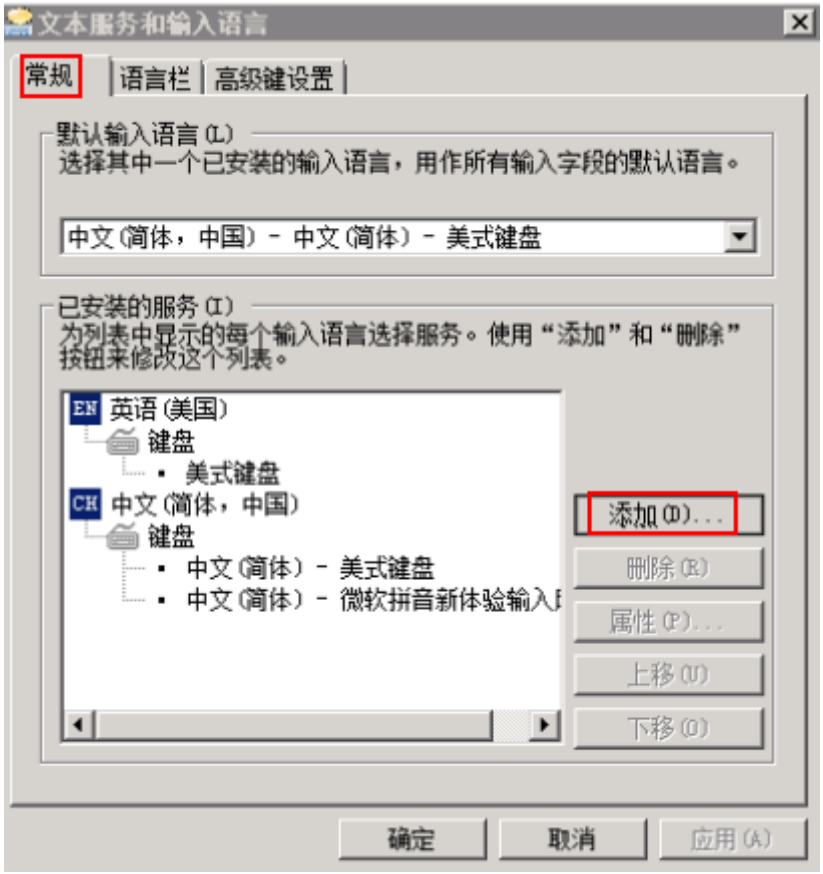
3. 选择“键盘和语言”标签，并单击“更改键盘”。

图 2-44 键盘和语言



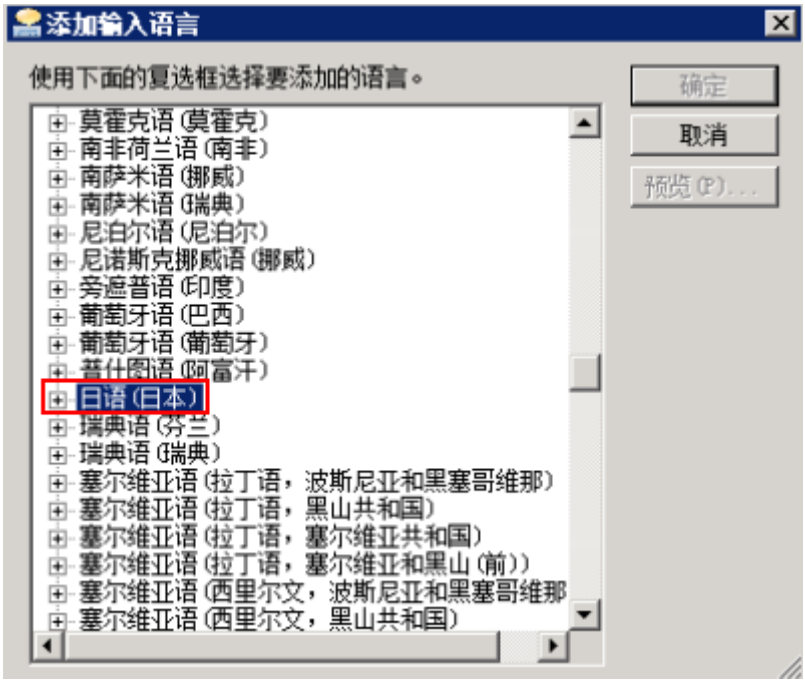
4. 打开“文本服务和输入语言”对话框，在“常规”标签中单击“添加”。

图 2-45 文本服务和输入语言



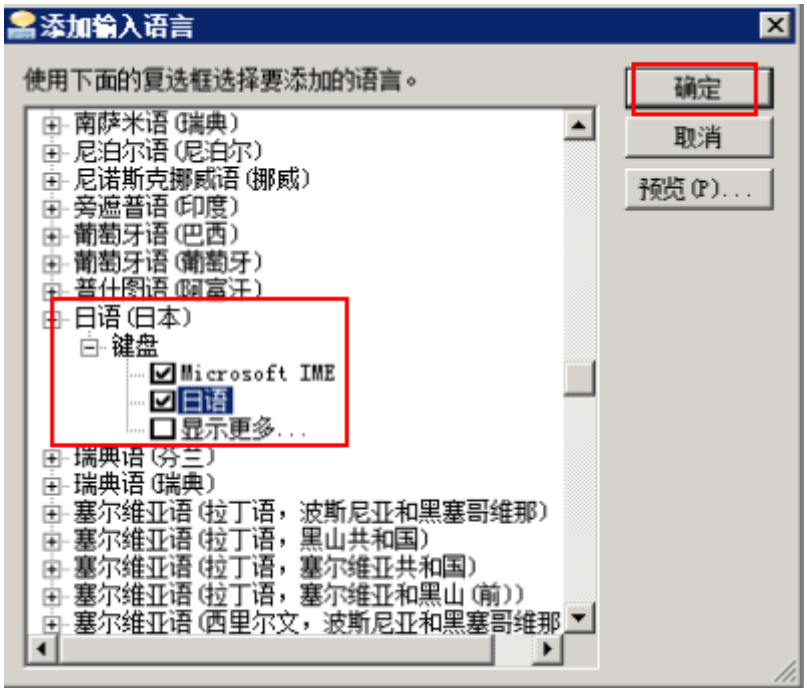
5. 在弹出的“添加输入语言”对话框中，找到“日语（日本）”。

图 2-46 添加输入语言



6. 双击“日语（日本）”展开，双击“键盘”子项展开，勾选“Microsoft IME”和“日语”，单击“确定”，分别再单击“应用”和“确定”保存修改后退出。

图 2-47 选择日语



2.9 怎样实现 Windows 云服务器文件共享?

操作场景

本节操作指导用户实现同一个子网的Windows云服务器之间文件共享。

约束与限制

共享文件的云服务器在同一个子网下，且网络互通。

操作步骤

1. 在云服务器右下方的网络图标处，右键单击“打开网络和共享中心”。

图 2-48 打开网络和共享中心

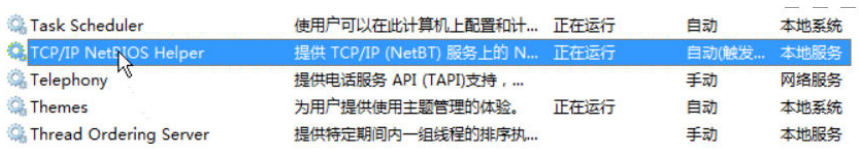
2. 单击“更改高级共享设置”分别开启“专用”和“来宾公用”的“启用文件和打印机共享”，单击“保存更改”

图 2-49 启用或关闭系统图标

3. 在cmd窗口执行命令**services.msc**，找到TCP/IP NetBIOS Helper服务，并设置为开启。

   若服务处于“禁用”状态，则右键属性，将服务设为“自动”或者“手动”，然后开启服务。

图 2-50 开启 TCP/IP NetBIOS Helper



2.10 Windows 无法正常启动时怎样恢复数据?

问题描述

登录Windows操作系统云服务器时，无法正常进入系统。自启动系统修复模式，但选择修复选项后报错，无法继续进行系统恢复。

图 2-51 自启动系统修复模式

可能原因

Windows文件已损坏。

处理方法

1. 登录管理控制台，选择“计算 > 弹性云服务器”。
2. 卸载云服务器挂载的数据盘。
   在云服务器的详情页，单击“云硬盘”页签，单击数据盘后的“卸载”。
3. 重装故障服务器的操作系统。
   在待重装操作系统的云服务器的“操作”列下，单击“更多 > 重装系统”。

   须知

   - 只有关机状态的云服务器才能重装系统。如果云服务器不是关机状态，请先关机。
   - 重装操作系统会导致系统盘数据被清除，请提前做好数据备份。

4. 将数据盘重新挂载至云服务器，重新验证云服务器是否可以正常进入系统。

2.11 如何查看 Windows 云服务器的登录日志?

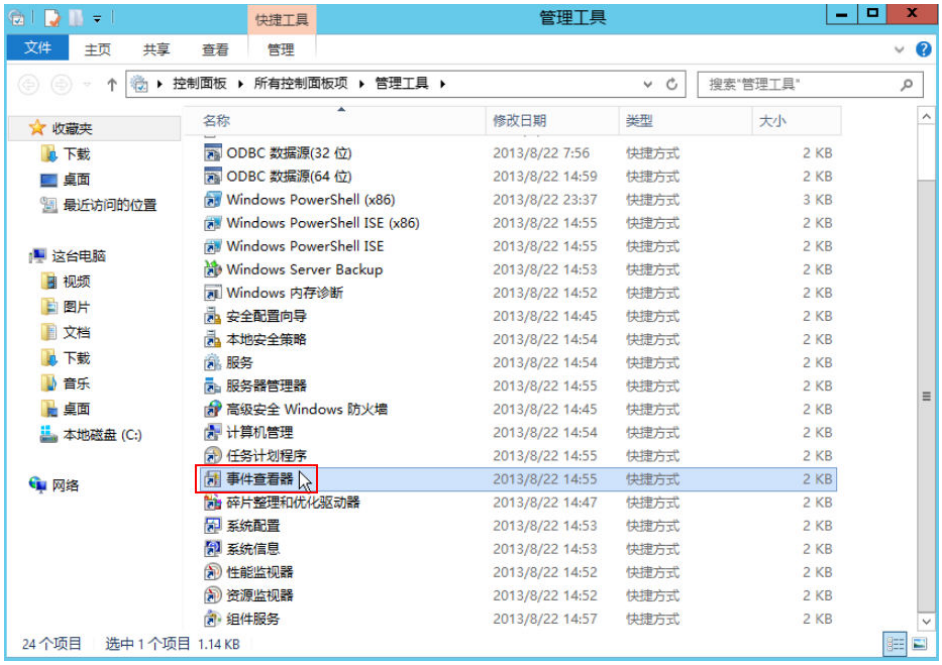
操作场景

本节操作指导用户查看Windows云服务器的登录日志。

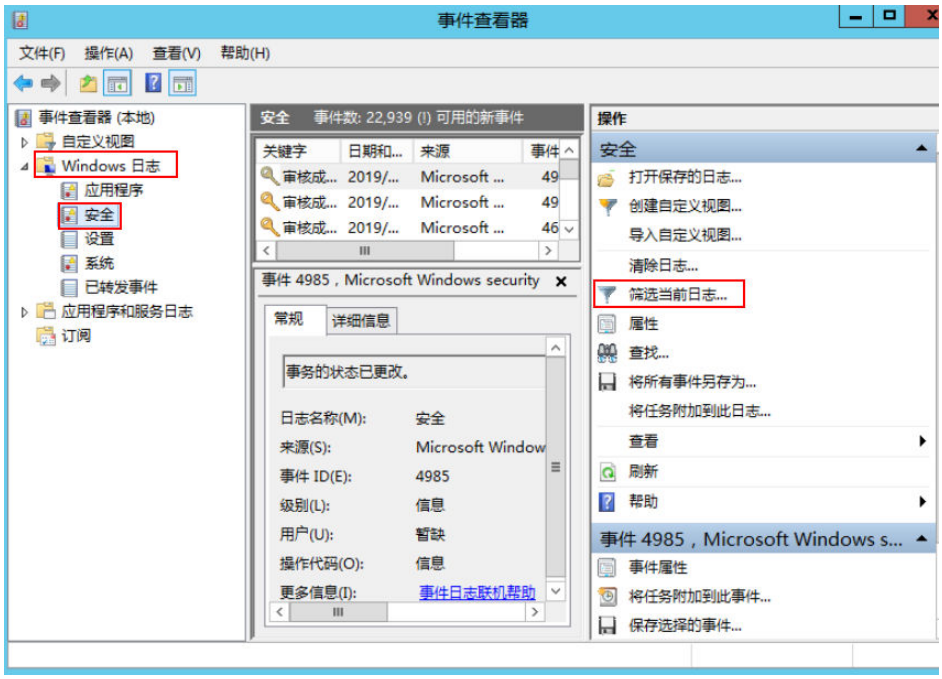
操作步骤

本节操作以2012操作系统云服务器为例。

1. 登录弹性云服务器。
2. 选择“开始 > 管理工具 > 事件查看器 ”。



3. 打开“ Windows日志 > 安全 > 筛选当前日志”。

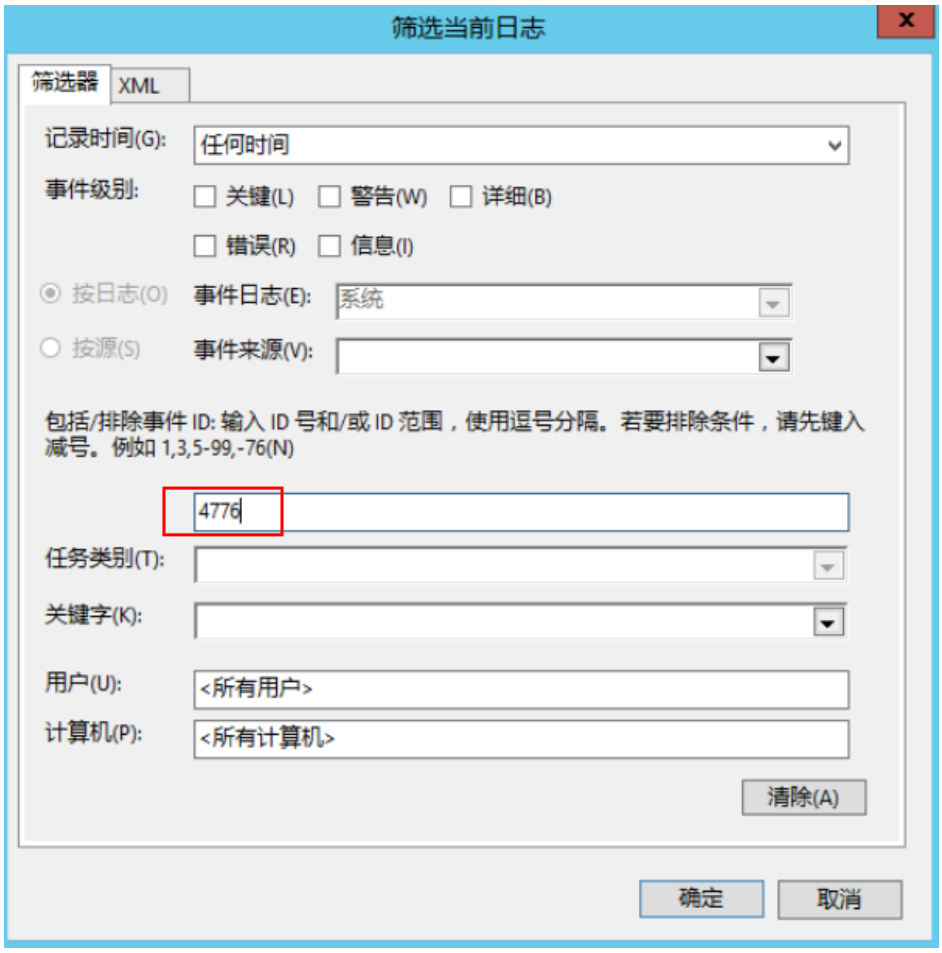


4. 筛选事件ID为4776的事件即为远程登录日志。

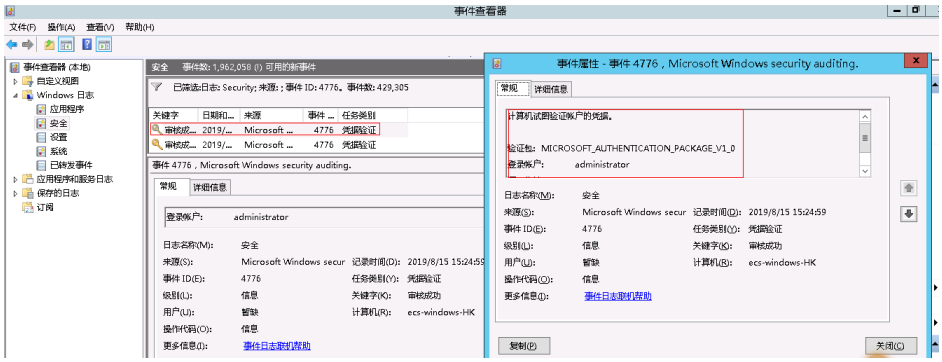
说明

您还可以使用4624和4625查看登录信息。

- 4624：Windows登录成功的事件ID。
- 4625：Windows登录失败的事件ID。



5. 单击右键查看“事件属性”，即可看到该事件的登录账户。



2.12 Windows 云服务器可以 Ping 通网站，但是无法访问怎么办?

问题描述

Windows云服务器在长时间运行后，无妨访问网站或应用。

此时，云服务器可以正常远程登录，可以Ping通外部网址，但是无法使用浏览器访问外部网站或应用。

可能原因

Windows云服务器的动态端口耗尽。

由于Windows操作系统中TCP默认的TIME_WAIT时间为4分钟，因此，当Windows操作系统云服务器在长时间使用后，可能会存在处于TIME_WAIT状态并占用大量端口的连接，从而导致Windows云服务器访问外部网站或应用出现异常。

您可以在Windows云服务器的CMD命令提示符中，执行以下命令查看处于TIME_WAIT状态的连接。

netstat -an |find "TIME_WAIT" /c

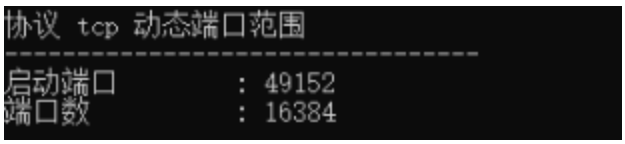
执行结果如下：

图 2-52 查看 TIME_WAIT 状态的连接数量

处理方法

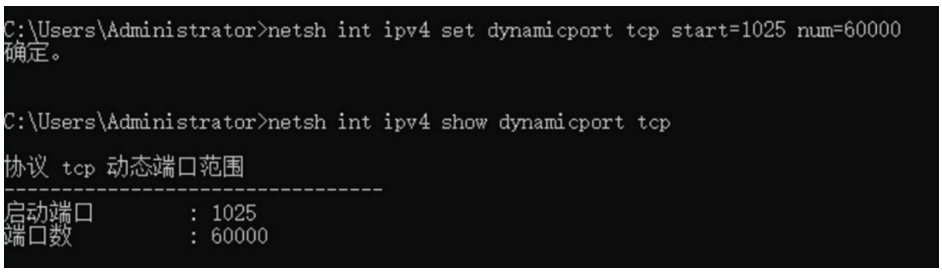
1. 登录Windows云服务器。
2. 以管理员身份运行CMD。
3. 执行以下命令，查看当前的动态端口数量。
   netsh int ipv4 show dynamicport tcp

   图 2-53 查看当前动态端口

4. 执行以下命令，增大动态端口数量并再次查看当前动态端口数量。
   netsh int ipv4 set dynamicport tcp start=1025 num=60000
   netsh int ipv4 show dynamicport tcp

   图 2-54 设置动态端口

5. 重新访问外部网站或应用。

2.13 Windows 无法打开开始菜单及搜索框

问题描述

新创建的Windows云服务器可以正常登录，但是登录进去后单击开始菜单按钮无反应，搜索框也无反应。

可能原因

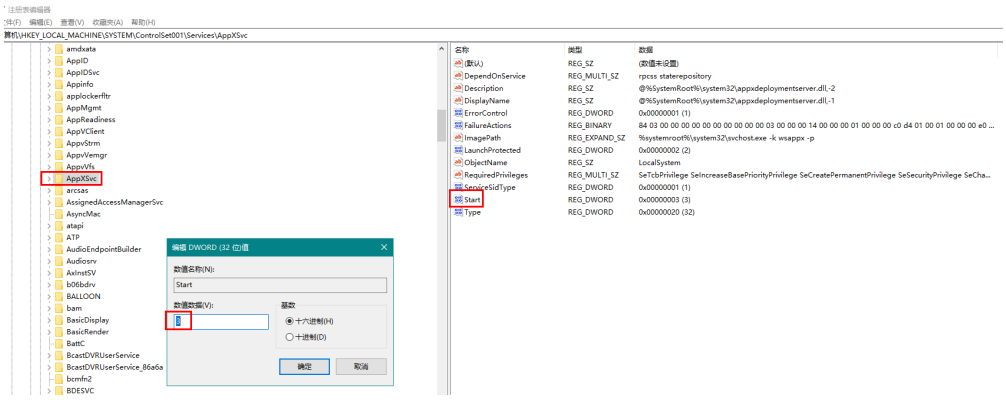
AppX Deployment Service(AppXSVC)服务大量占用系统资源，如磁盘占用率非常高，且无法关闭。AppX Deployment Service服务是Windows应用部署服务，当用户初次登录到这台电脑和添加新应用时，使应用进入就绪可用的状态。

处理方法

关闭AppX Deployment Service服务，操作步骤如下：

1. 按“Win+R”键打开运行对话框，输入regedit并按回车键，打开注册表编辑器。
2. 打开至注册表键值：“HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\AppXSvc”。
3. 双击右侧子项中的“Start”，将“数值数据”中的“3”修改为“4”。

图 2-55 修改数值数据



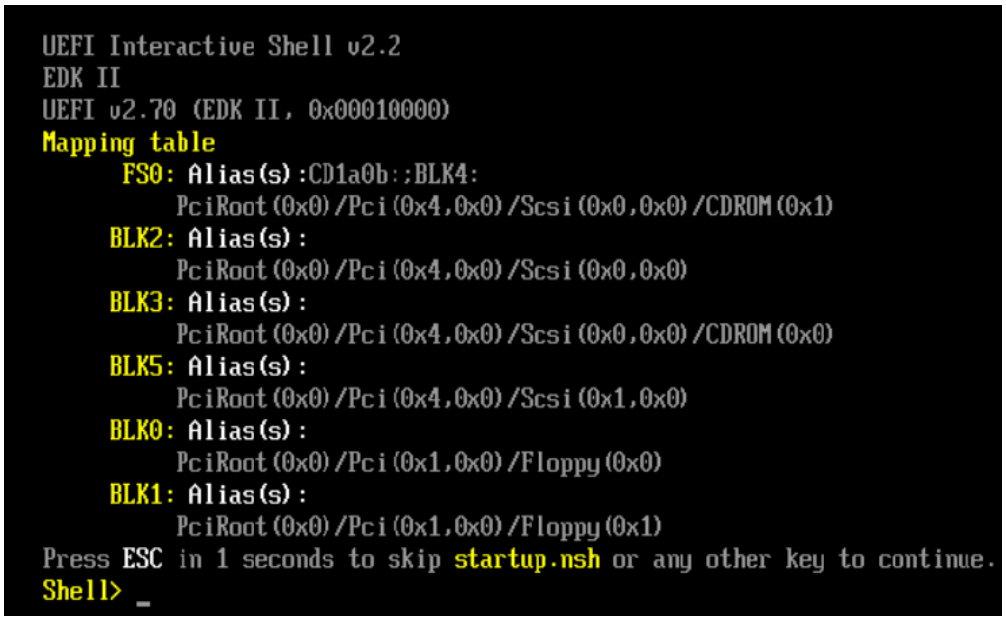
说明

如果要启用AppX Deployment Service服务，将“数值数据”由“4”改回“3”即可。

2.14 Windows Server 2016 ISO 实例 UEFI 无法启动

问题描述

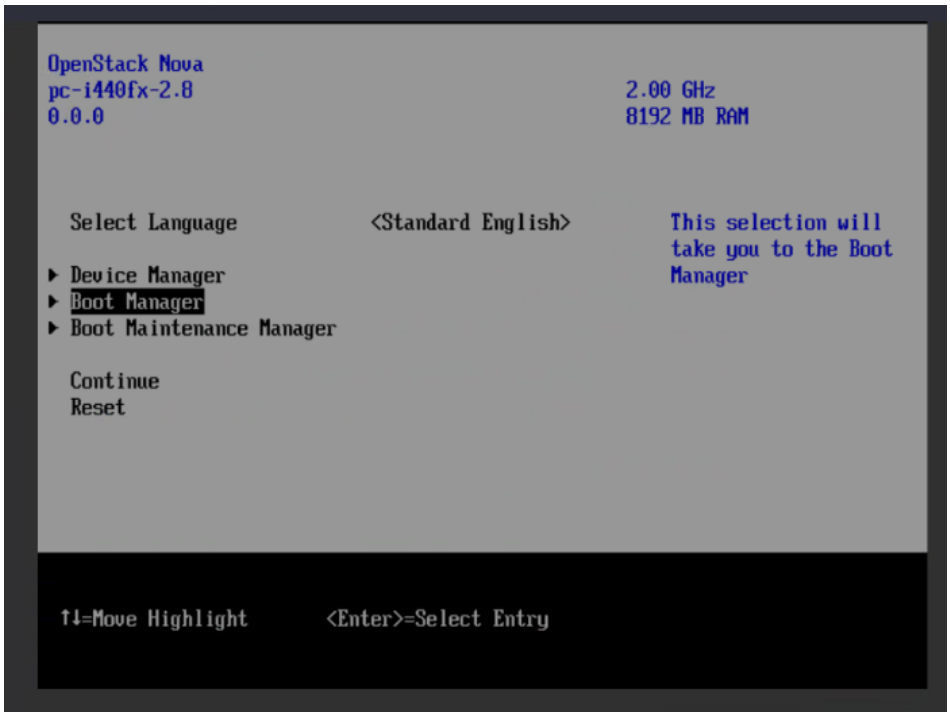
通过UEFI方式启动Windows Server 2016 ISO镜像失败，提示“UEFI Interactive Shell”。



处理方法

1. 确认镜像是否支持UEFI启动。
   - 若镜像中存在如下图所示的bootx64.efi文件，说明镜像支持UEFI启动，继续执行2。
   - 若镜像中不存在bootx64.efi文件，说明镜像不支持UEFI启动，请通过BIOS方式启动。

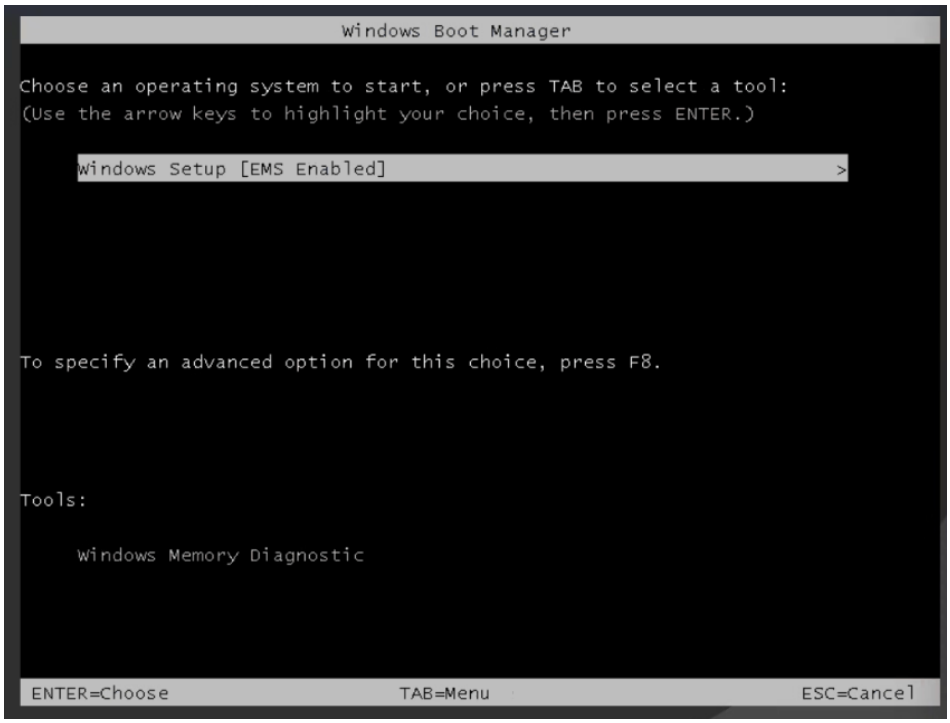
2. 手动选择启动项
   a. 输入exit，进入BIOS设置界面。
   b. 选择“**Boot Manager**”，按回车键。

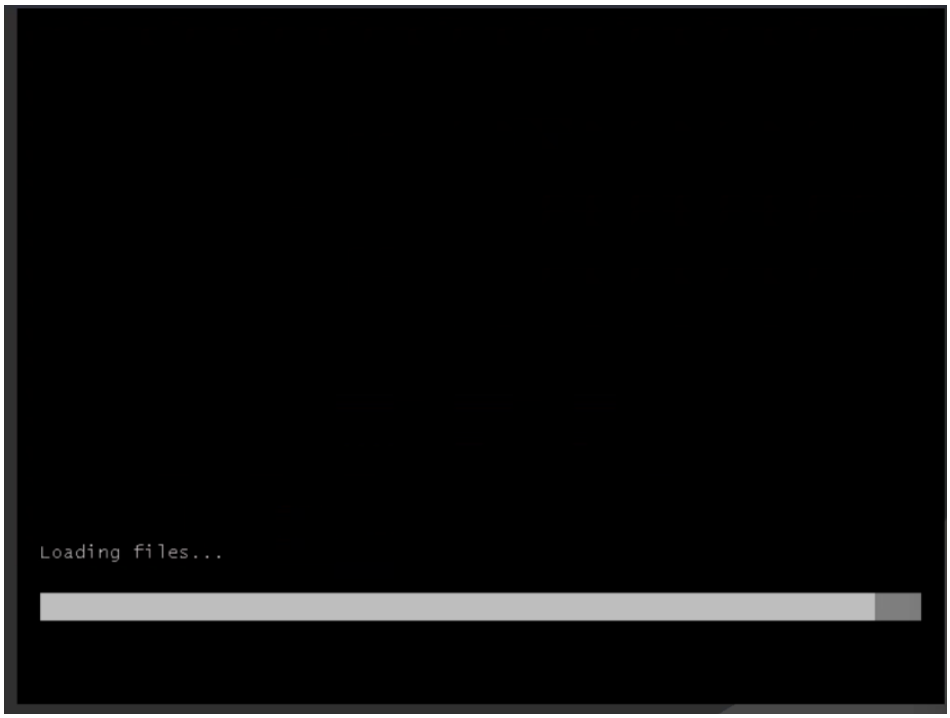


c. 选择“**UEFI QEMU DVD-ROM xxxxxx**”，按回车键。

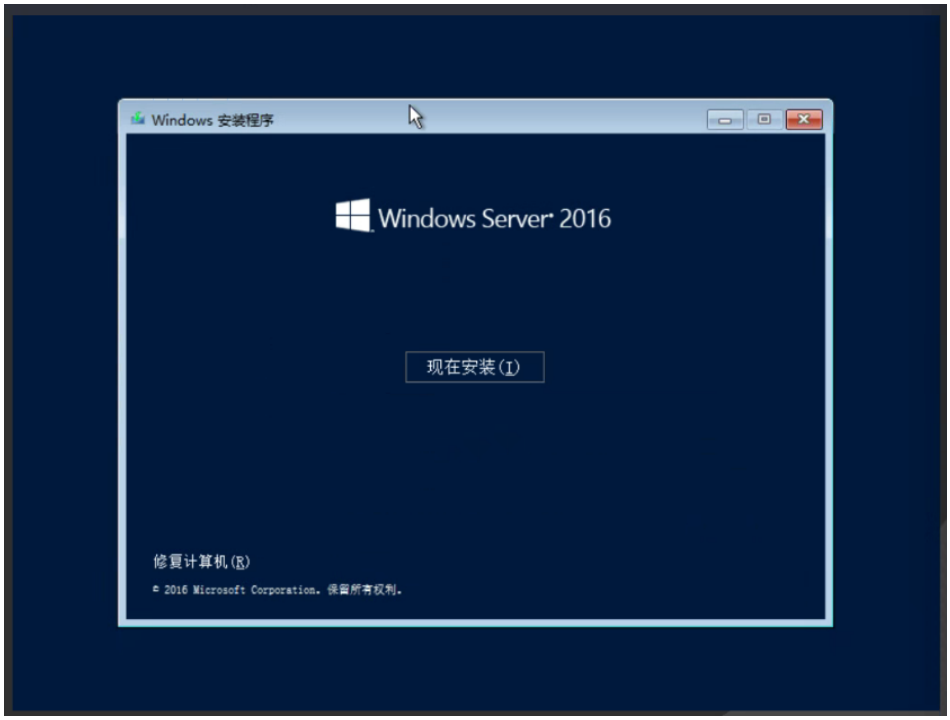
d. 按任意按键进入启动界面。

e. 单击回车键，启动文件加载中。





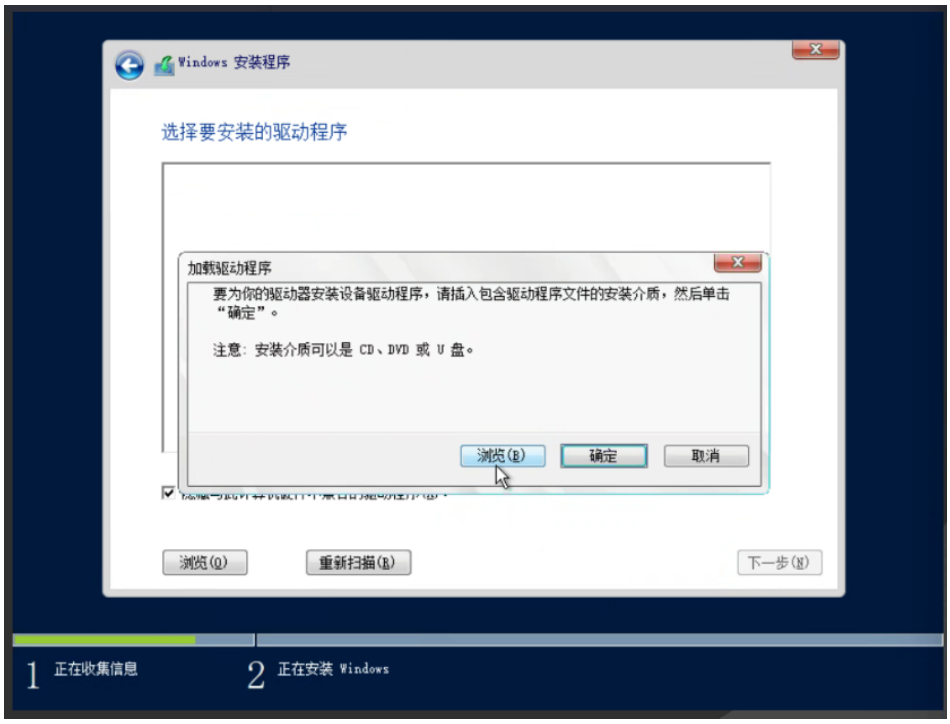
f. 进入安装界面，单击“现在安装”。



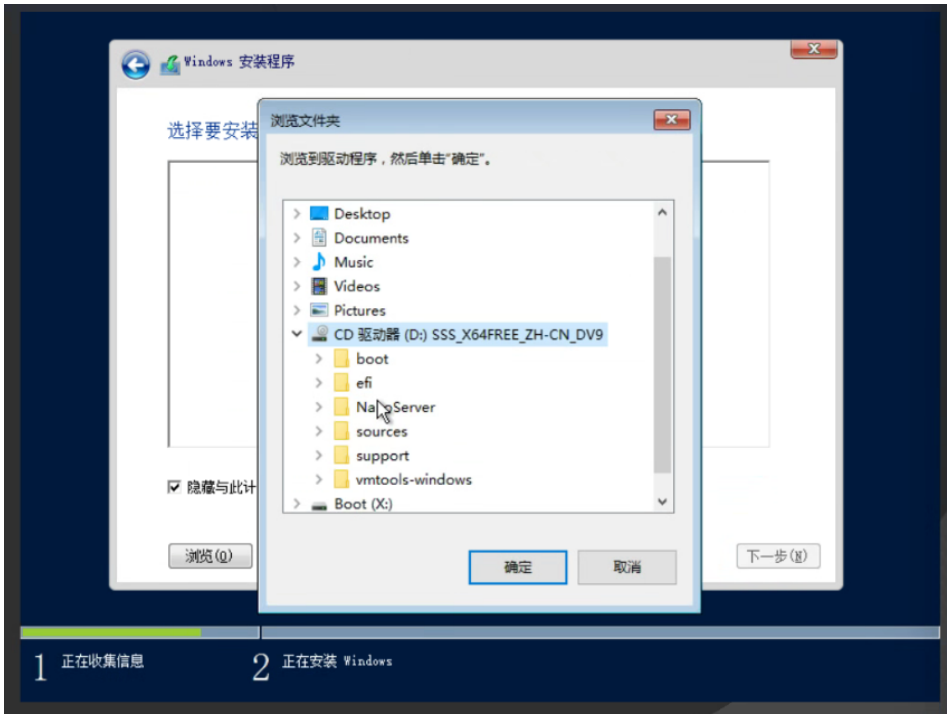
g. 在“你想执行哪种类型的安装？”界面，选择“自定义：仅安装Windows（高级）(C)”。

h. 在“你想将Windows安装在哪里？”界面，选择“加载驱动程序”。

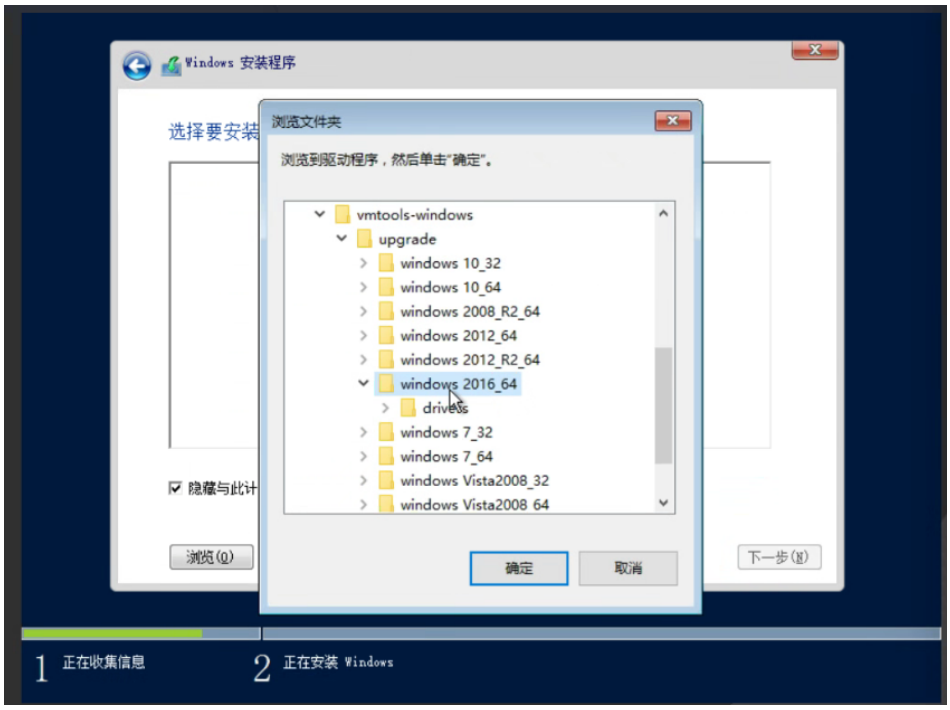
i. 在“加载驱动程序”弹窗中，单击“浏览”。



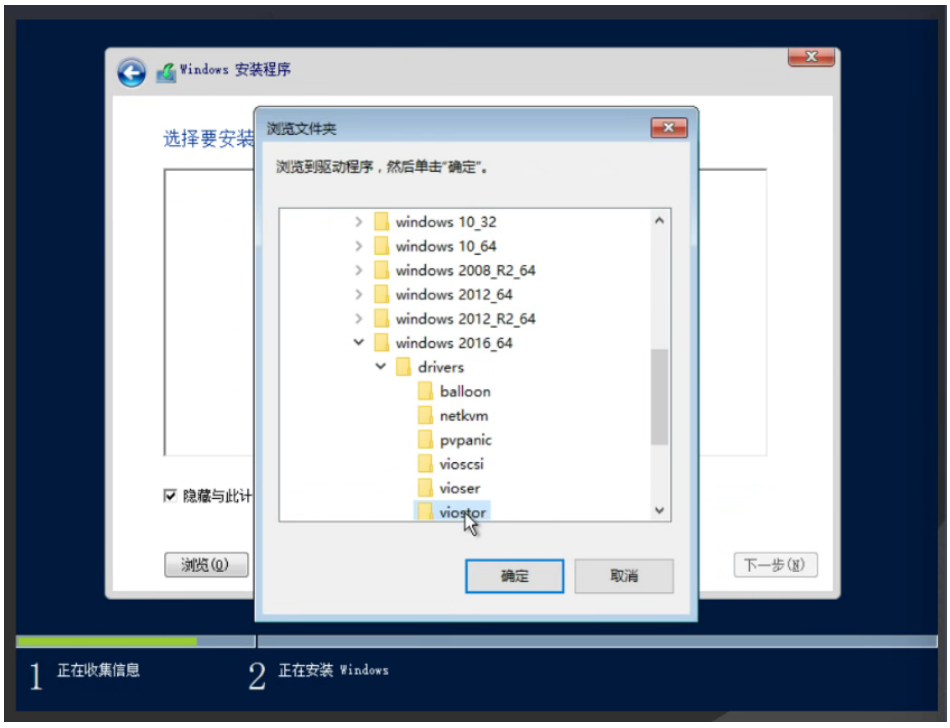
j. 选择“CD驱动器”。



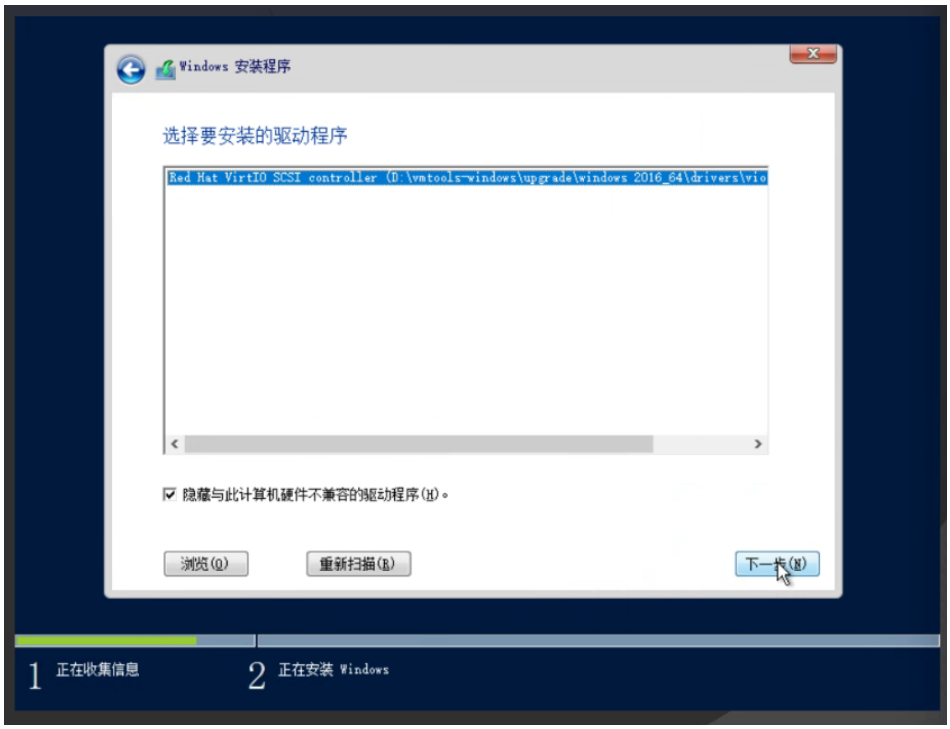
k. 根据当前的操作系统版本，选择对应的驱动目录。



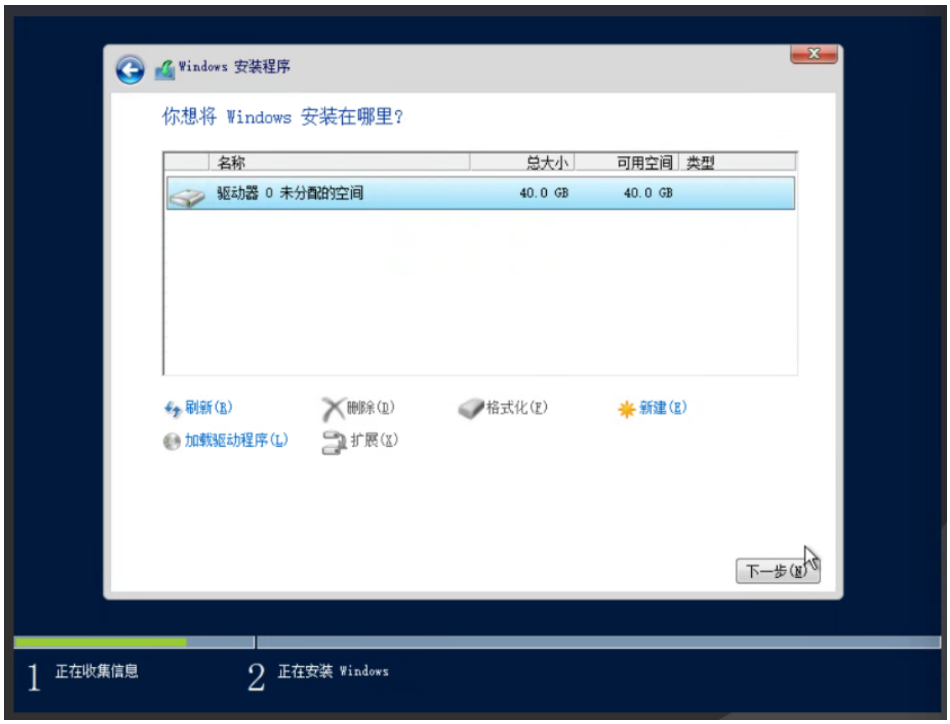
l. 选择“viostor”目录，单击“确定”。



m. 选择驱动程序，单击“下一步”。



n. 选择磁盘，单击“下一步”。

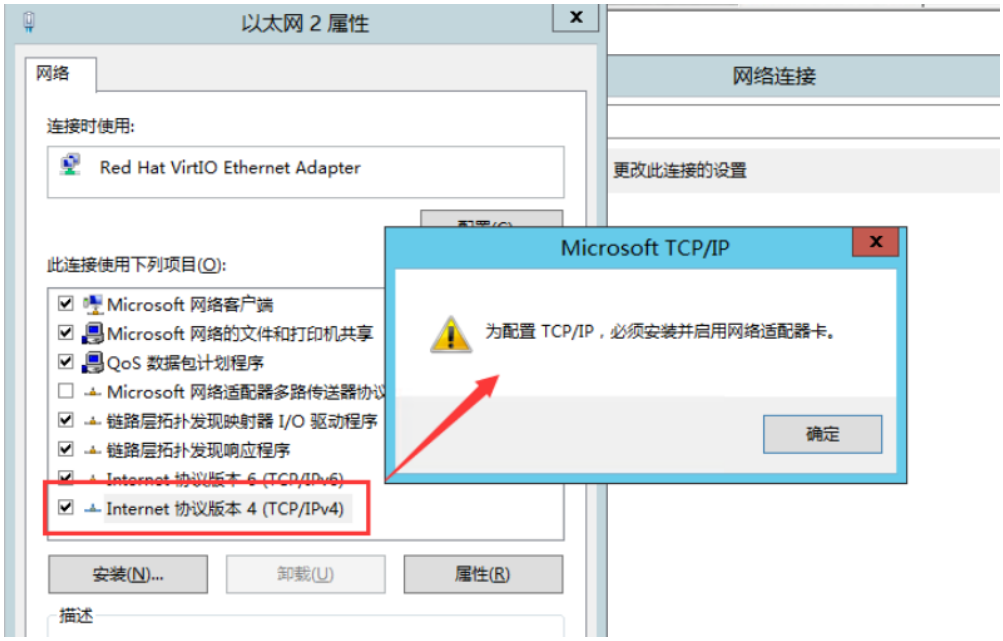


o. 进入“正在安装Windows”界面，开始安装操作系统。
安装过程大约耗时50分钟，安装完成后请重新登录弹性云服务器。

2.15 Windows 无法修改 DNS，提示为配置 TCP/IP

问题描述

Windows云服务器修改DNS时，打开Internet 协议版本4（TCP/IPV4）时报错 "为配置TCP/IP，必须安装并启用网络适配器卡"。

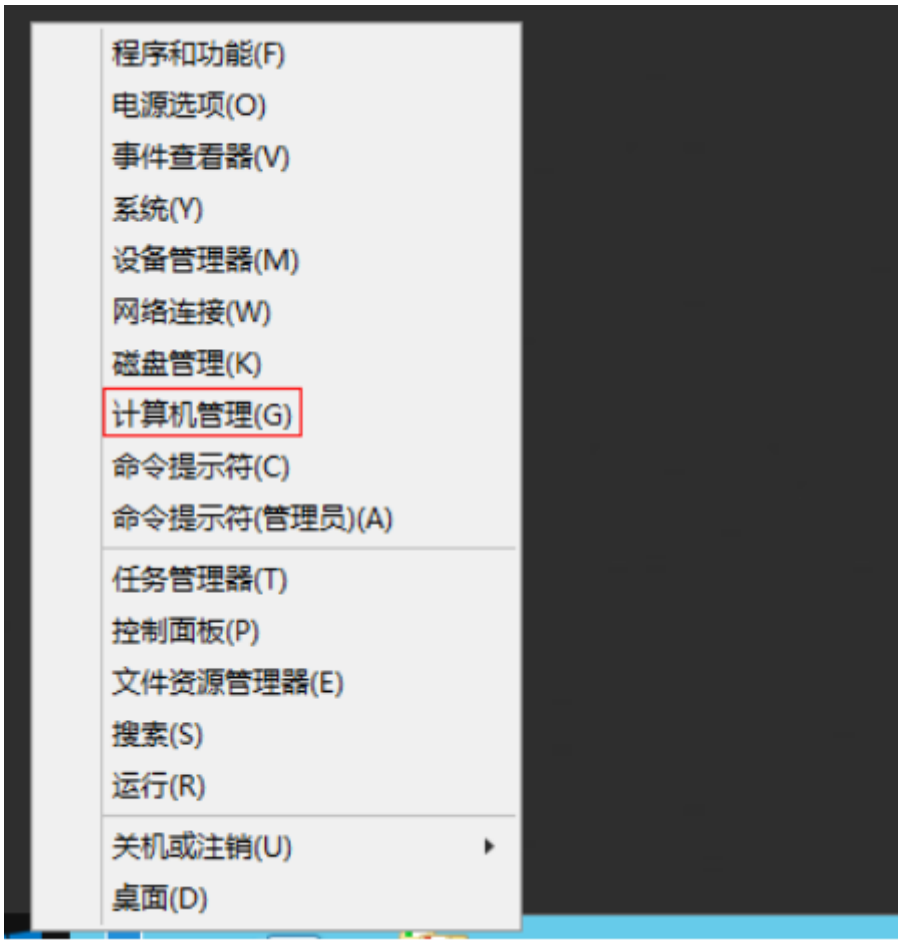


可能原因

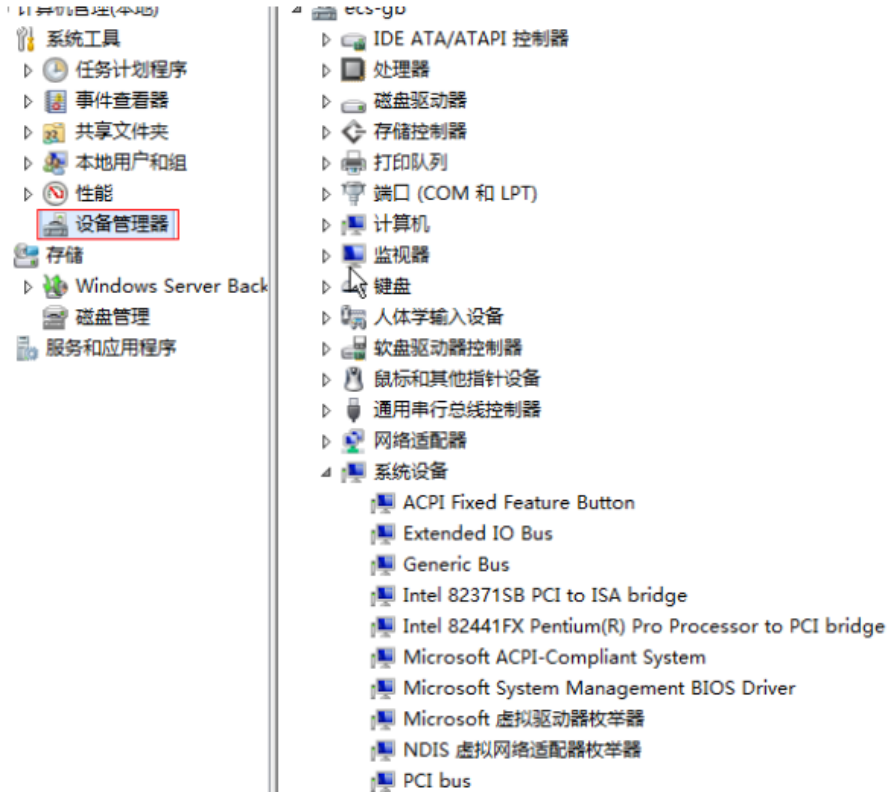
此问题是由于网卡驱动问题导致，需要重新安装网卡驱动。

处理方法

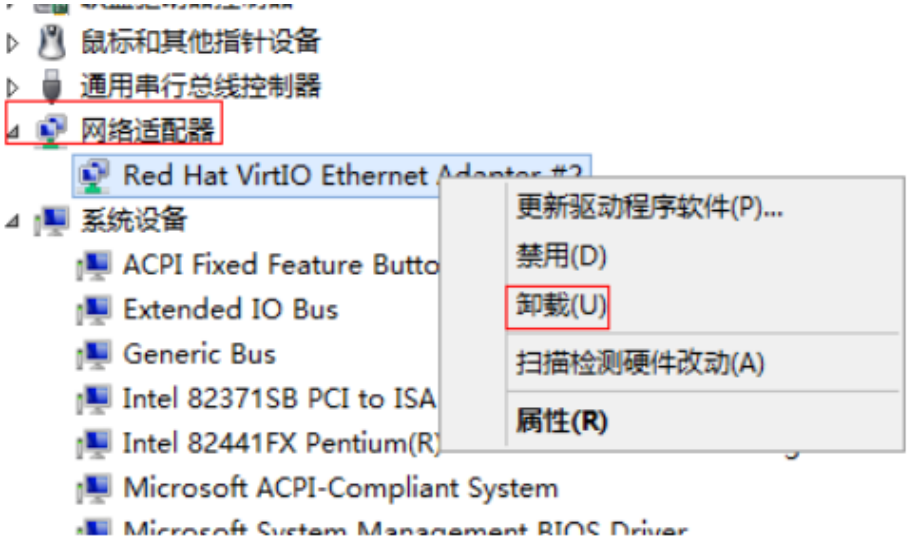
1. **通过控制台VNC登录Windows ECS**。
2. 鼠标右键单击计算机桌面左下角，选择“计算机管理(G)”。



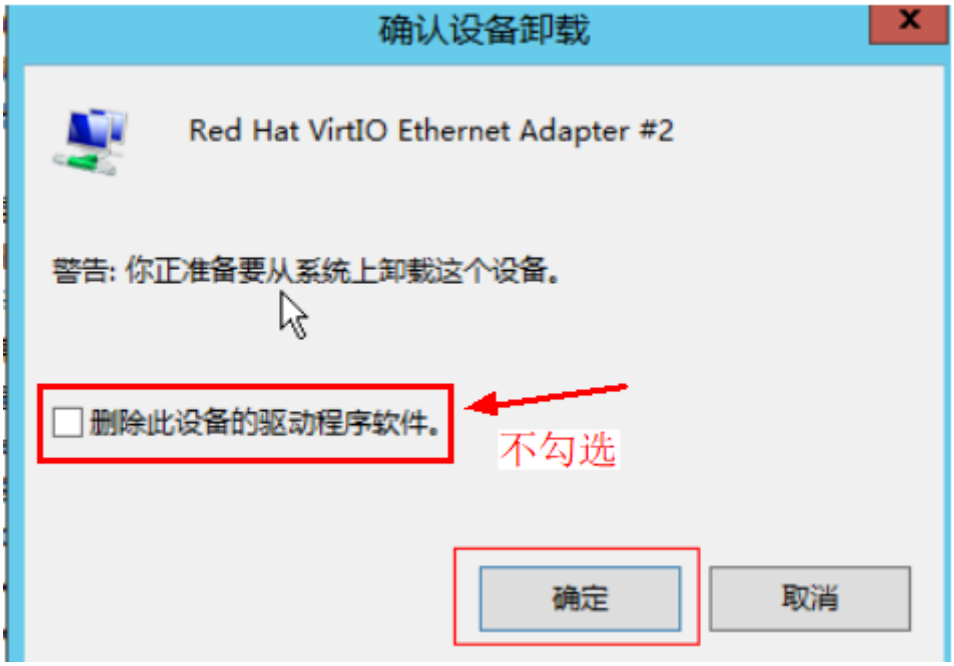
3. 单击“设备管理器”。



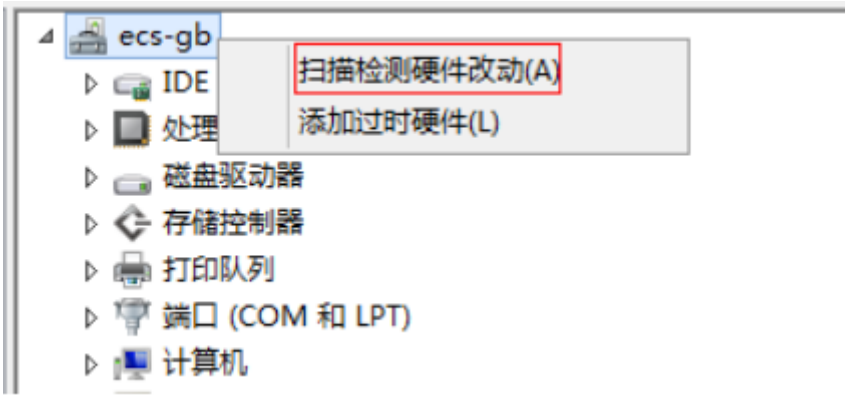
4. 选择“网络适配器”，右键单击“Red Hat VirtIO Ethernet Adapter #2”，选择“卸载(U)”。



5. 单击“确定”。
   注意：不勾选“删除此设备的驱动程序软件”。



6. 右键单击下图所示位置，单击“扫描检测硬件改动(A)”。



7. 完成扫描检查后，即可修改DNS，详细操作请参见**如何为ECS配置DNS?**。

2.16 如何处理 Windows 云服务器出现时间跳变问题

问题描述

Windows云服务器时间同步异常，系统时间跳变到未来的某一个时刻，影响业务运行。

可能原因

Windows操作系统的Secure time seeding功能可能会导致时间跳变，该功能在Windows 2016及之后版本的服务器上默认是开启的，当服务器和任何https服务器建立SSL connection的时候，在TLS交互过程中，SSL服务器会提供其当前系统时间信息， 客户端这边会将该信息写入到客户端本地， 默认存放于注册表中。服务器从某个SSL服务器那边拿到了一个有问题的时间戳，并将其缓存到注册表中， 导致服务器突然出现了异常的时间跳变问题。

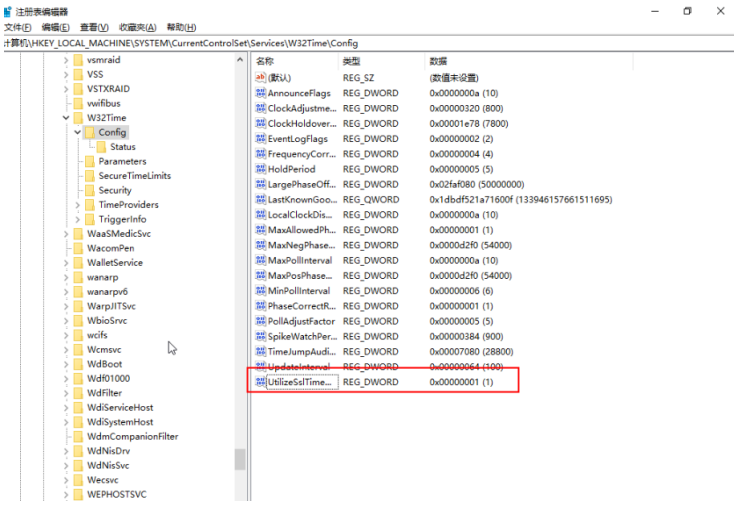
详情请参考微软文档：**https://learn.microsoft.com/zh-cn/windows-server/networking/windows-time-service/windows-server-2016-improvements**。

处理方法

建议关闭Windows云服务器的Secure time seeding功能，关闭方案如下：

1. 按“Win+R”键打开“运行”对话框，输入“regedit”并按回车键，打开注册表编辑器。
2. 依次选择HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > W32Time > Config，检查UtilizeSslTimeData参数配置。

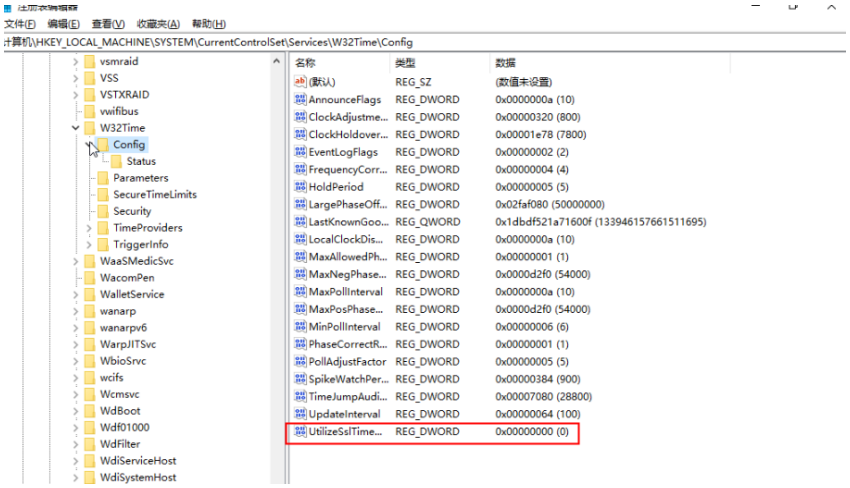
   当值为“1”时默认打开，值为“0”时默认关闭。若值为“1”，请继续以下操作。



3. 按“Win+R”键打开“运行”对话框，输入“cmd”并按回车键，打开cmd运行窗口。
4. 执行以下命令，修改UtilizeSslTimeData取值为“0”。

   ```
   reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\w32time\Config /v UtilizeSslTimeData /t REG_DWORD /d 0 /f
   ```

5. 重启云服务器，使修改生效。
6. 按“Win+R”键打开“运行”对话框，输入“regedit”并按回车键，打开注册表编辑器。
7. 依次选择HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > W32Time > Config，检查UtilizeSslTimeData参数取值是否修改成功。



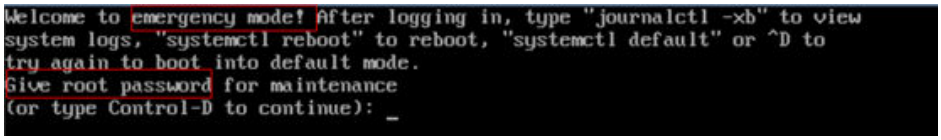
3 操作系统类（Linux）

3.1 emergency mode（紧急模式）问题处理方法

问题现象

Linux系统启动时进入紧急模式，提示：Welcome to emergency mode，如图3-1所示，并提示输入root密码进入维护。

图 3-1 紧急模式



根因分析

紧急模式提供尽可能最小的环境，即使在系统无法进入救援模式的情况下，您也可以修复系统。在紧急模式下，系统仅安装根文件系统进行读取，不尝试安装任何其他本地文件系统，不激活网络接口，只启动一些基本服务。

进入紧急模式的原因通常是：

- /etc/fstab文件存在错误导致挂载文件系统时失败。
- 文件系统存在错误导致。

约束与限制

本节操作适用于Linux操作系统emergency mode（紧急模式）问题处理。操作步骤涉及修复文件系统操作，修复文件系统存在丢失数据风险，请先备份数据后进行修复操作。

处理方法

1. 输入root密码后回车，进入修复模式。

若无法进入修复模式，可选择进入单用户模式或Debug Shell模式，详细内容，请参见**Linux云服务器如何进入单用户模式?** 和**Linux云服务器如何进入Debug Shell模式?** 。

2. 在紧急模式下根分区是以只读方式挂载，要修改根目录下的文件需要执行以下命令，以读写方式重新挂载根分区。

   mount -o rw,remount /

3. 请执行以下命令首先检查fstab文件是否存在错误，尝试挂载所有未挂载的文件系统。

   mount -a

   - 如果出现mount point does not exist为挂载点不存在，请创建对应的挂载点。
   - 如果出现no such device为不存在该文件系统设备，请注释或者删除该挂载行。
   - 如果出现an incorrect mount option was specified为挂载参数错误，请修改为正确的参数。
   - 如果出现can't find uuid为UUID不存在，请注释或者删除该挂载行。
   - 如果没有出现任何错误且提示UNEXPECTED INCONSISTENCY;RUN fsck MANUALLY，通常为文件系统错误导致，请跳至步骤7。

4. 执行以下命令，打开/etc/fstab修改相应的错误。

   vi /etc/fstab

   /etc/fstab文件包含了如下字段，通过空格分隔：

   [file system] [dir] [type] [options] [dump] [fsck]

表 3-1 /etc/fstab 参数说明

参数	说明
[file system]	要挂载的分区或存储设备。 [file system]列建议使用UUID的方式书写，执行**blkid**命令查询设备文件系统UUID。 参考格式如下： # <device> <dir> <type> <options> <dump> <fsck> UUID=b411dc99-f0a0-4c87-9e05-184977be8539 /home ext4 defaults 0 2 使用UUID的好处在于它们与磁盘顺序无关。如果您在BIOS中改变了您的存储设备顺序，或是重新拔插了存储设备，或是因为一些BIOS可能会随机地改变存储设备的顺序，那么用UUID来表示将更有效。
[dir]	[file system]的挂载位置。
[type]	挂载设备或分区的文件系统类型，支持许多种不同的文件系统：ext2，ext3，ext4，reiserfs，xfs，jfs，smbfs，iso9660，vfat，ntfs，swap及auto。 设置成auto类型，mount命令会猜测使用的文件系统类型，对CDROM和DVD等移动设备是非常有用的。

参数	说明
[options]	挂载时使用的参数，有些参数是特定文件系统才有的。例如：defaults参数使用文件系统的默认挂载参数，ext4的默认参数为:rw，suid，dev，exec，auto，nouser，async。 更多参数请执行以下命令查看man手册：**man mount**
[dump]	dump工具通过它决定何时作备份。 dump会检查其内容，并用数字来决定是否对这个文件系统进行备份。 取值为0和1 。0表示忽略，1则进行备份。大部分的用户是没有安装dump的，[dump]应设为0。
[fsck]	fsck读取[fsck]的数值来决定需要检查的文件系统的检查顺序。 取值为0，1，和2。 根目录应当获得最高的优先权1, 其它所有需要被检查的设备设置为2，0表示设备不会被fsck所检查。

5. 修改完成后，确认修改是否正确，再次执行以下命令首先检查fstab文件。
   mount -a
6. 执行以下命令，重启服务器。
   reboot
7. 如果步骤3中没有任何错误，则可能为文件系统错误导致，执行：
   dmesg |egrep "ext[2..4]|xfs" |grep -i error

   说明

   - 输出结果中如果有I/O error ... inode的错误信息则根因为文件系统错误导致。
   - 如果上述命令没有发现日志记录文件系统文件错误则通常为超级块损坏。超级块是文件系统的“头部”。它包含文件系统的状态、尺寸和空闲磁盘块等信息。
   - 如果损坏了一个文件系统的超级块（例如不小心直接将数据写到了文件系统的超级块分区中），那么系统可能会完全不识别该文件系统，系统启动时没有识别到文件系统导致进入紧急模式。ext2fs类型的文件系统将超级块的内容进行了备份，并存放于驱动程序的块组（blockgroup）边界。
8. 请执行以下命令，卸载文件系统出错的目录，
   umount *挂载点*
9. 检查并修复已损坏的文件系统。

须知

修复文件系统可能会导致数据丢失请先进行数据备份。

- ext文件系统，执行以下命令，检查文件系统是否存在错误。
  fsck -n /dev/vdb1

  说明

  如果出现The super block Cloud no be read or does not describe a correct ext2 filesystem的提示请跳转至10。

  如果需要修复，执行以下命令，修复文件系统。
  fsck /dev/vdb1

- xfs文件系统，执行以下命令，检查文件系统是否存在错误。

  xfs_repair -n /dev/vdb1

  如果需要修复，执行以下命令，修复文件系统。

  xfs_repair /dev/vdb1

10. （可选）出现The super block Cloud no be read or does not describe a correct ext2 filesystem通常为超级块损坏，如图3-2所示，请按照提示使用备份的超级块更新超级块。

    图 3-2 超级块损坏

    ```
    [root@ecs ~]# fsck -n /dev/vda2
    fsck from util-linux-ng 2.17.2
    e2fsck 1.41.12 (17-May-2010)
    fsck.ext2: No such file or directory while trying to open /dev/vda2

    The superblock could not be read or does not describe a correct ext2
    filesystem.  If the device is valid and it really contains an ext2
    filesystem (and not swap or ufs or something else), then the superblock
    is corrupt, and you might try running e2fsck with an alternate superblock:
        e2fsck -b 8193 <device>
    ```

    执行以下命令，使用备份的超级块信息更新超级块。

    e2fsck -b 8193 设备名

    如图3-3所示更新超级块完成：

    图 3-3 更新超级块

    ```
    [root@ecs ~]# e2fsck -b 8193 /dev/xvda
    e2fsck 1.41.12 (17-May-2010)
    /dev/xvda is in use.
    e2fsck: Cannot continue, aborting.
    ```

    说明

    - -b 8193选项用于显示使用存放在文件系统中的8193块的超级块的备份数据。通常在主超级块已损坏时使用。备份超级块的位置是依赖的在文件系统的blocksize上。

      对于具有1k块大小的文件系统，可以在块处找到备份超级块8193。

      对于具有2k块大小的文件系统，在块16384;对于4k块，在块32768。
    - <设备名>为磁盘名称而非分区。

11. 修复完成后执行以下命令，重启服务器。

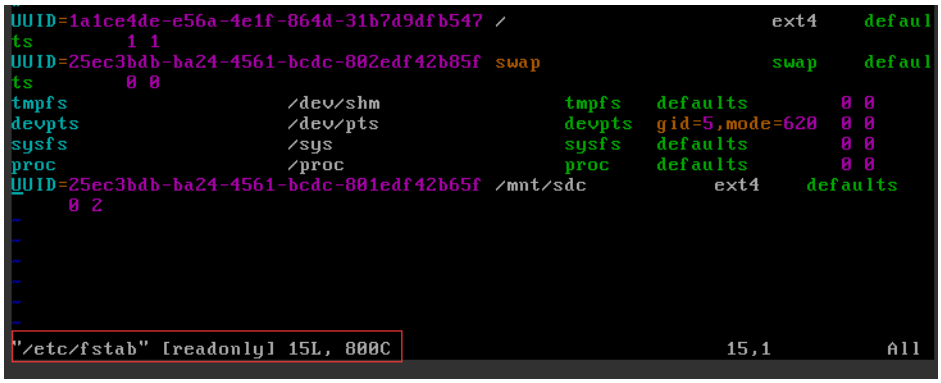
    reboot

3.2 无法编辑 fstab 文件怎么办?

问题描述

编辑/etc/fstab文件，提示“readonly”。

图 3-4 fstab 文件提示 readonly



处理方法

修复模式下（read-only system）文件是被保护的不能修改，运行下面命令，把系统文件权限改成可读写（rw）。

mount -o remount,rw /

执行完上述命令，重试编辑fstab文件。

3.3 CentOS/EulerOS 设置系统时区

操作场景

本节操作介绍在CentOS或EulerOS操作系统云服务器设置时区的操作步骤。

约束与限制

- 该文档已在CentOS 6.8及CentOS 7.5操作系统云服务器上验证，其他版本可能存在差异。
- 文档中以中国上海时区为例，其他时区请根据实际进行设置。

CentOS 6/RHEL 6 操作系统（以中国上海时区为例）

1. 永久修改系统时区，请执行
   cp -vf /usr/share/zoneinfo/Asia/Shanghai /etc/localtime
2. 重新登录后执行以下命令，确认当前时区是否已经为CST。
   date |awk '{print $5}'

在 CentOS 7/EulerOS 操作系统（以中国上海时区为例）

1. 使用以下命令找到所需的时区，请执行：
   timedatectl list-timezones
2. 更改时区
   timedatectl set-timezone Asia/Shanghai
3. 验证时区的状态
   timedatectl status

3.4 Web 访问超时系统日志打印：nf_conntrack:table full, dropping packet

问题现象

客户端访问web时出现time out。 服务端系统日志/var/log/messages打印kernel: nf_conntrack:table full, dropping packet。

图 3-5 系统日志

```
Aug  2 17:35:58 ecs-69dc-0002 kernel: nf_conntrack: table full, dropping packet
Aug  2 17:35:58 ecs-69dc-0002 kernel: nf_conntrack: table full, dropping packet
Aug  2 17:35:58 ecs-69dc-0002 kernel: nf_conntrack: table full, dropping packet
Aug  2 17:35:58 ecs-69dc-0002 kernel: nf_conntrack: table full, dropping packet
Aug  2 17:35:58 ecs-69dc-0002 kernel: nf_conntrack: table full, dropping packet
Aug  2 17:35:58 ecs-69dc-0002 kernel: nf_conntrack: table full, dropping packet
Aug  2 17:36:06 ecs-69dc-0002 kernel: net_ratelimit: 40 callbacks suppressed
Aug  2 17:36:06 ecs-69dc-0002 kernel: nf_conntrack: table full, dropping packet
Aug  2 17:36:06 ecs-69dc-0002 kernel: nf_conntrack: table full, dropping packet
Aug  2 17:36:06 ecs-69dc-0002 kernel: nf_conntrack: table full, dropping packet
Aug  2 17:36:06 ecs-69dc-0002 kernel: nf_conntrack: table full, dropping packet
Aug  2 17:36:06 ecs-69dc-0002 kernel: nf_conntrack: table full, dropping packet
Aug  2 17:36:06 ecs-69dc-0002 kernel: nf_conntrack: table full, dropping packet
Aug  2 17:36:06 ecs-69dc-0002 kernel: nf_conntrack: table full, dropping packet
Aug  2 17:36:06 ecs-69dc-0002 kernel: nf_conntrack: table full, dropping packet
Aug  2 17:36:06 ecs-69dc-0002 kernel: nf_conntrack: table full, dropping packet
Aug  2 17:36:06 ecs-69dc-0002 kernel: nf_conntrack: table full, dropping packet
Aug  2 17:36:22 ecs-69dc-0002 kernel: net_ratelimit: 40 callbacks suppressed
Aug  2 17:36:22 ecs-69dc-0002 kernel: nf_conntrack: table full, dropping packet
```

适用场景

本节操作适用于CentOS系统，且系统开启了主机防火墙，其他Linux系统可能存在差异。

约束与限制

本节操作涉及修改系统内核参数，在线修改内核参数会出现内核不稳定，建议修改后在合理的时间重启系统，请评估风险后操作。

根因分析

iptables的connection-tracking模块使用系统内存的一部分来跟踪表中的连接。“table full, dropping packet”表明连接跟踪表已满，不能为新连接创建新的条目，因为没有更多的空间。因此出现“dropping packet”问题。

解决方案是增加连接跟踪条目的数量。

CentOS 6 系列操作系统处理方法

1. 执行以下命令，查看nf_conntrack_max参数。

   sysctl net.netfilter.nf_conntrack_max

2. 检查当前正在跟踪的连接数。

   cat /proc/sys/net/netfilter/nf_conntrack_count

如果该值达到nf_conntrack_max值则会出现包被丢弃的现象。

3. 提高net.netfilter.nf_conntrack_max值（以内存为64G，net.netfilter.nf_conntrack_max值2097152为例）。

   执行以下命令，使配置即时生效。

   sysctl -w net.netfilter.nf_conntrack_max=2097152

   执行以下命令确保重启后配置仍然生效。

   echo "net.netfilter.nf_conntrack_max = 2097152" >> /etc/sysctl.conf

   说明

   - .net.netfilter.nf_conntrack_max不是越高越好，通常根据内存大小进行设置。
   - nf_conntrack_max计算公式（64位）

     CONNTRACK_MAX = RAMSIZE (inbytes)/16384/2

     例如您的机器是一个64GB 64bit的系统，那么最合适的值是

     CONNTRACK_MAX = 64*1024*1024*1024/16384/2 = 2097152

4. 如果conntrack表中的条目数量显著增加（例如以4倍的速度增加），则还应增加存储conntrack条目的哈希表的大小以提高效率。

   计算新的哈希值：在CentOS 6及以上版本，计算公式是hashsize = conntrack_max/4

5. 执行以下命令，设置新的哈希大小。

   echo "options nf_conntrack expect_hashsize=524288 hashsize=524288" >/etc/modprobe.conf

6. 重启iptables。

   service iptables restart

CentOS 7 系列操作系统处理方法

1. 执行以下命令，在/etc/modprobe.d/firewalld-sysctls.conf中设置conntrack条目的哈希值。

   在CentOS 6及以上版本，计算公式是hashsize = conntrack_max/4

   echo "options nf_conntrack expect_hashsize=131072 hashsize=131072" >> /etc/modprobe.d/firewalld-sysctls.conf

2. 重启firewalld。

   systemctl restart firewalld

3. 确认参数修改成功。

   sysctl -a |grep nf_conntrack_max

了解更多请参考**Red Hat Customer Portal**。

3.5 Ubuntu 操作系统如何设置默认启动内核

操作场景

本节操作适用于Ubuntu16.04操作系统与云服务器设置默认启动内核，其他Ubuntu版本可能存在差异。

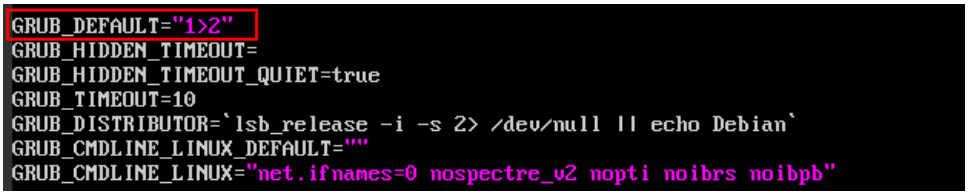
约束与限制

本操作涉及修改grub配置文件，误操作可能会导致系统无法启动。操作前，请务必对grub配置文件进行备份，以便在发生误操作时能够进行恢复。

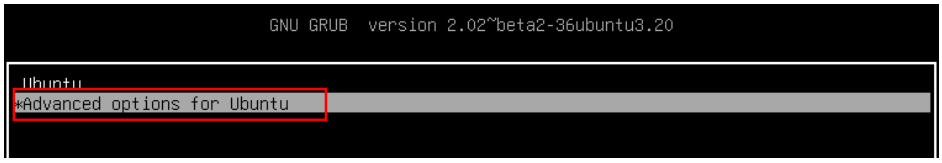
操作方法

1. 打开/etc/default/grub文件（以启动第三内核为例），修改GRUB_DEFAULT的值为"1>2"，如图3-6所示。

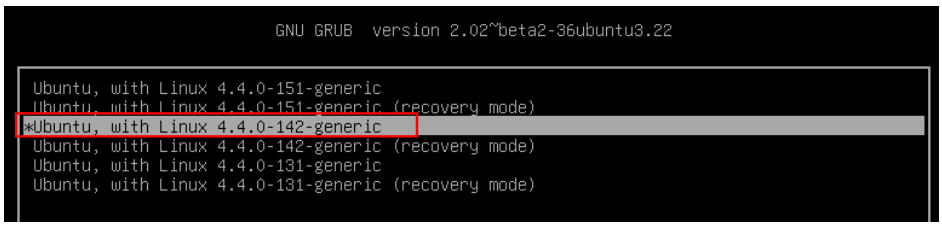
   图 3-6 修改 GRUB_DEFAULT

   - 1>2中的1指的是主菜单第二个选项。

   - 1>2中的2指的是主菜单第二个选项中的第三个启动内核选项。

   - 1>2中的>分隔符号前后不带空格。
   - 整个条目使用一组引号。

2. 执行以下命令，重新生成grub配置文件。

   update-grub

3.6 怎样配置 Linux 分析工具：atop 和 kdump

操作场景

本节操作介绍atop和kdump的配置方法。

不同的Linux版本使用的atop工具版本不同，因此配置方法稍微有所不同。

配置atop：

- **atop简介**
- **atop安装前准备**

- CentOS 6系列操作系统配置atop
- CentOS 7/8、AlmaLinux、 Rocky Linux系列操作系统配置atop
- Ubuntu 16、Debian8系列操作系统配置atop
- Ubuntu 18、Debian 9系列操作系统配置atop
- Ubuntu 20、Debian 10系列操作系统配置atop
- Ubuntu 22/24系列操作系统配置atop
- Debian 11/12系列操作系统配置atop
- SUSE 15、SUSE 12系列操作系统配置atop
- Huawei Cloud EulerOS 2.0（HCE）系列操作系统配置atop
- 使用源码方式安装（适用于CentOS Stream 8/9、openEuler、EulerOS等系列操作系统）
- 分析atop日志
- （可选）加载netatop内核模块

配置kdump：

- 配置kdump使用须知
- kdump简介
- 配置kdump操作步骤
- 检查kdump配置是否生效

atop 简介

atop是一款用于监控Linux系统资源与进程的工具，它以一定的频率记录系统的运行状态，所采集的数据包含系统资源(CPU、内存、磁盘和网络)使用情况和进程运行情况，并能以日志文件的方式保存在磁盘中，服务器出现问题后，可获取相应的atop日志文件进行分析。

atop 安装前准备

需要弹性公网IP且能访问yum软件源。

约束与限制

使用atop工具对节点资源信息监控会占用少量的CPU核和内存进行系统资源的收集并占用部分磁盘空间记录日志，日志路径为/var/log/atop。

CentOS 6 系列操作系统配置 atop

1. 执行以下命令，安装atop。

   yum install -y atop

2. 编辑配置文件，修改采样周期。

   vi /etc/sysconfig/atop

   修改如下配置参数，修改后保存并退出。

   LOGINTERVAL默认是600，可以修改成15，单位秒。

   ```
   LOGINTERVAL=15
   ```

   vi /etc/logrotate.d/atop

修改如下配置参数，修改后保存并退出。

默认atop日志保存周期为40天，可以根据实际修改“-mtime”的值为3，单位为天。

```
  postrotate
    /usr/bin/find /var/log/atop/ -maxdepth 1 -mount -name atop_\[0-9\]\[0-9\]\[0-9\]\[0-9\]\[0-9\]\[0-9\]\[0-9\]\[0-9\]\* -mtime +3 -exec /bin/rm {} \;
  endscript
```

3. 启动atop服务。

   service atop start

4. 检查是否启动成功，is running 表示运行正常。

   service atop status

   ```
   atop (pid 3170) is running
   ```

5. atop运行会占用额外的系统和磁盘资源，您可在问题排查完成后，执行以下命令停止atop。

   service atop stop

CentOS 7/8、AlmaLinux、 Rocky Linux 系列操作系统配置 atop

1. 执行以下命令，安装atop。

   yum install -y atop

2. 编辑配置文件，修改采样周期。

   vi /etc/sysconfig/atop

   修改如下配置参数，修改后保存并退出。

   - LOGINTERVAL默认是600，可以修改成15，单位秒。
   - 默认atop日志保存周期为28天，可以根据实际修改LOGGENERATIONS的值为3，单位为天。

   ```
   LOGINTERVAL=15
   LOGGENERATIONS=3
   ```

3. 启动atop服务。

   systemctl enable --now atop atopacct atop-rotate.timer

4. 检查是否启动成功，atop atopacct是 active(running)表示运行正常，atop-rotate.timer是active(waiting) 表示运行正常。

   systemctl status atop atopacct atop-rotate.timer

   ```
   atop.service - Atop advanced performance monitor
   Loaded: loaded (/usr/lib/systemd/system/atop.service; enabled; vendor preset: enabled)
   Active: active (running)

   atopacct.service - Atop process accounting daemon
   Loaded: loaded (/usr/lib/systemd/system/atopacct.service; enabled; vendor preset: enabled)
   Active: active (running)

   atop-rotate.timer - Daily atop restart
   Loaded: loaded (/usr/lib/systemd/system/atop-rotate.timer; enabled; vendor preset: enabled)
   Active: active (waiting)
   ```

5. atop运行会占用额外的系统和磁盘资源，您可在问题排查完成后，执行以下命令停止atop。

   systemctl disable atop atopacct atop-rotate.timer

   systemctl stop atop atopacct atop-rotate.timer

Ubuntu 16、Debian8 系列操作系统配置 atop

1. 执行以下命令，安装atop。

   apt-get install -y atop

2. 编辑配置文件，修改采样周期。

   vi /etc/default/atop

   修改如下配置参数，修改后保存并退出。

   - LOGINTERVAL默认是600，可以修改成15，单位秒。
   - 默认atop日志保存周期为28天，不支持修改。

   ```
   LOGINTERVAL=15
   ```

3. 启动atop服务。

   systemctl start atop

4. 检查是否启动成功，active(running) 表示运行正常。

   systemctl status atop

   ```
   atop.service - Atop advanced performance monitor
   Loaded: loaded (/etc/init.d/atop; bad; vendor preset: disabled)
   Active: active (running)
   ```

5. atop运行会占用额外的系统和磁盘资源，您可在问题排查完成后，执行以下命令停止atop。

   systemctl stop atop

Ubuntu 18、Debian 9 系列操作系统配置 atop

1. 执行以下命令，安装atop。

   apt-get install -y atop

2. 编辑配置文件，修改采样周期。

   vi /usr/share/atop/atop.daily

   修改如下配置参数，修改后保存并退出。

   - LOGINTERVAL默认是600，可以修改成15，单位秒。
   - 默认atop日志保存周期为28天，可以根据实际修改“-mtime”的值为3，单位为天。

   ```
   LOGINTERVAL=15
   ......
   ( (sleep 3; find $LOGPATH -name 'atop_*' -mtime +3 -exec rm {} \;)& )
   ```

3. atop是默认启动，需重启atop服务使配置生效。

   systemctl restart atop atopacct

4. 检查是否启动成功，active(running) 表示运行正常。

   systemctl status atop atopacct

   ```
   atop.service - Atop advanced performance monitor
   Loaded: loaded (/etc/init.d/atop; enable; vendor preset: enabled)
   Active: active (running)

   atopacct.service - Atop process accounting daemon
   Loaded: loaded (/usr/lib/systemd/system/atopacct.service; enabled; vendor preset: enabled)
   Active: active (running)
   ```

5. atop运行会占用额外的系统和磁盘资源，您可在问题排查完成后，执行以下命令停止atop。

   systemctl disable atop atopacct

systemctl stop atop atopacct

Ubuntu 20、Debian 10 系列操作系统配置 atop

1. 执行以下命令，安装atop。

   apt-get install -y atop

2. 编辑配置文件，修改采样周期。

   vi /etc/default/atop

   修改如下配置参数，修改后保存并退出。

   - LOGINTERVAL默认是600，可以修改成15，单位秒。
   - 默认atop日志保存周期为28天，可以根据实际修改LOGGENERATIONS的值为3，单位为天。

   ```
   LOGINTERVAL=15
   LOGGENERATIONS=3
   ```

3. atop是默认启动，需重启atop服务使配置生效。

   systemctl restart atop atopacct

4. 检查是否启动成功，active(running) 表示运行正常。

   systemctl status atop atopacct

   ```
   atop.service - Atop advanced performance monitor
   Loaded: loaded (/etc/init.d/atop; enable; vendor preset: enabled)
   Active: active (running)

   atopacct.service - Atop process accounting daemon
   Loaded: loaded (/usr/lib/systemd/system/atopacct.service; enabled; vendor preset: enabled)
   Active: active (running)
   ```

5. atop运行会占用额外的系统和磁盘资源，您可在问题排查完成后，执行以下命令停止atop。

   systemctl disable atop atopacct

   systemctl stop atop atopacct

Ubuntu 22/24 系列操作系统配置 atop

1. 执行以下命令，安装atop。

   apt-get install -y atop

2. 编辑配置文件，修改采样周期。

   vi /etc/default/atop

   修改如下配置参数，修改后保存并退出。

   - LOGINTERVAL默认是600，可以修改成15，单位秒。
   - 默认atop日志保存周期为28天，可以根据实际修改LOGGENERATIONS的值为3，单位为天。

   ```
   LOGINTERVAL=15
   LOGGENERATIONS=3
   ```

3. atop是默认启动，需重启atop服务使配置生效。

   systemctl restart atop atopacct atop-rotate.timer

4. 检查是否启动成功，atop atopacct是 active(running)表示运行正常，atop-rotate.timer是active(waiting) 表示运行正常。

   systemctl status atop atopacct atop-rotate.timer


```
atop.service - Atop advanced performance monitor
Loaded: loaded (/usr/lib/systemd/system/atop.service; enabled; vendor preset: enabled)
Active: active (running)

atopacct.service - Atop process accounting daemon
Loaded: loaded (/usr/lib/systemd/system/atopacct.service; enabled; vendor preset: enabled)
Active: active (running)

atop-rotate.timer - Daily atop restart
Loaded: loaded (/usr/lib/systemd/system/atop-rotate.timer; enabled; vendor preset: enabled)
Active: active (waiting)
```

5. atop运行会占用额外的系统和磁盘资源，您可在问题排查完成后，执行以下命令停止atop。

   systemctl disable atop atopacct atop-rotate.timer

   systemctl stop atop atopacct atop-rotate.timer

Debian 11/12 系列操作系统配置 atop

1. 执行以下命令，安装atop。

   apt-get install -y atop

2. 编辑配置文件，修改采样周期。

   vi /etc/default/atop

   修改如下配置参数，修改后保存并退出。

   - LOGINTERVAL默认是600，可以修改成15，单位秒。
   - 默认atop日志保存周期为28天，可以根据实际修改LOGGENERATIONS的值为3，单位为天。

   ```
   LOGINTERVAL=15
   LOGGENERATIONS=3
   ```

3. atop是默认启动，需重启atop服务使配置生效。

   systemctl restart atop atopacct atop-rotate.timer

4. 检查是否启动成功，atop atopacct是 active(running)表示运行正常，atop-rotate.timer是active(waiting) 表示运行正常。

   systemctl status atop atopacct atop-rotate.timer

   ```
   atop.service - Atop advanced performance monitor
   Loaded: loaded (/usr/lib/systemd/system/atop.service; enabled; vendor preset: enabled)
   Active: active (running)

   atopacct.service - Atop process accounting daemon
   Loaded: loaded (/usr/lib/systemd/system/atopacct.service; enabled; vendor preset: enabled)
   Active: active (running)

   atop-rotate.timer - Daily atop restart
   Loaded: loaded (/usr/lib/systemd/system/atop-rotate.timer; enabled; vendor preset: enabled)
   Active: active (waiting)
   ```

5. atop运行会占用额外的系统和磁盘资源，您可在问题排查完成后，执行以下命令停止atop。

   systemctl disable atop atopacct atop-rotate.timer

   systemctl stop atop atopacct atop-rotate.timer

SUSE 15、SUSE 12 系列操作系统配置 atop

1. 下载atop源码安装包。

   wget https://www.atoptool.nl/download/atop-2.6.0-1.src.rpm

2. 执行以下命令安装源码atop。

   rpm -ivh atop-2.6.0-1.src.rpm

3. 安装编译atop依赖软件包

   zypper -n install rpm-build ncurses-devel zlib-devel

4. 执行以下命令编译atop

   cd /usr/src/packages/SPECS

   rpmbuild -bb atop-2.6.0.spec

5. 执行以下命令安装atop

   cd /usr/src/packages/RPMS/x86_64

   rpm -ivh atop-2.6.0-1.x86_64.rpm

6. 编辑配置文件，修改采样周期。

   vi /etc/default/atop

   修改如下配置参数，修改后保存并退出。

   - LOGINTERVAL默认是600，可以修改成15，单位秒。
   - 默认atop日志保存周期为28天，可以根据实际修改LOGGENERATIONS的值为3，单位为天。

   ```
   LOGINTERVAL=15
   LOGGENERATIONS=3
   ```

7. atop是默认启动，需重启atop服务使配置生效。

   systemctl restart atop atopacct atop-rotate.timer

8. 检查是否启动成功，atop atopacct是 active(running)表示运行正常，atop-rotate.timer是active(waiting) 表示运行正常。

   systemctl status atop atopacct atop-rotate.timer

   ```
   atop.service - Atop advanced performance monitor
   Loaded: loaded (/usr/lib/systemd/system/atop.service; enabled; vendor preset: enabled)
   Active: active (running)

   atopacct.service - Atop process accounting daemon
   Loaded: loaded (/usr/lib/systemd/system/atopacct.service; enabled; vendor preset: enabled)
   Active: active (running)

   atop-rotate.timer - Daily atop restart
   Loaded: loaded (/usr/lib/systemd/system/atop-rotate.timer; enabled; vendor preset: enabled)
   Active: active (waiting)
   ```

9. atop运行会占用额外的系统和磁盘资源，您可在问题排查完成后，执行以下命令停止atop。

   systemctl disable atop atopacct atop-rotate.timer

   systemctl stop atop atopacct atop-rotate.timer

Huawei Cloud EulerOS 2.0（HCE）系列操作系统配置 atop

1. 执行以下命令，安装atop。

   yum install -y atop

2. 设置采样周期。

   HCE系统已经预设好采样周期，无需调整。默认采样周期10秒，日志保存3天。

3. 执行以下命令，启动atop服务。

   systemctl enable --now atop atopacct atop-rotate.timer

4. 检查是否启动成功，atop atopacct是active(running)表示运行正常，atop-rotate.timer是active(waiting) 表示运行正常。

   systemctl status atop atopacct atop-rotate.timer

   ```
   atop.service - Atop advanced performance monitor
   Loaded: loaded (/usr/lib/systemd/system/atop.service; enabled; vendor preset: enabled)
   Active: active (running)

   atopacct.service - Atop process accounting daemon
   Loaded: loaded (/usr/lib/systemd/system/atopacct.service; enabled; vendor preset: enabled)
   Active: active (running)

   atop-rotate.timer - Daily atop restart
   Loaded: loaded (/usr/lib/systemd/system/atop-rotate.timer; enabled; vendor preset: enabled)
   Active: active (waiting)
   ```

5. atop运行会占用额外的系统和磁盘资源，您可在问题排查完成后，执行以下命令停止atop。

   systemctl disable atop atopacct atop-rotate.timer

   systemctl stop atop atopacct atop-rotate.timer

使用源码方式安装（适用于 CentOS Stream 8/9、openEuler、EulerOS 等系列操作系统）

1. 下载atop源码。

   wget https://www.atoptool.nl/download/atop-2.6.0.tar.gz

2. 执行以下命令解压源码atop。

   tar -zxvf atop-2.6.0.tar.gz

3. 执行以下命令查看systemctl版本。

   systemctl --version

   如果版本大于等于220，直接进行下一步。

   否则需要修改atop的Makefile文件，删除--now参数。

   vi atop-2.6.0/Makefile

   删除systemctl命令后的--now参数

   ```
   then   /bin/systemctl disable  atop     2> /dev/null; \
          /bin/systemctl disable  atopacct 2> /dev/null; \
          /bin/systemctl daemon-reload;                  \
          /bin/systemctl enable   atopacct;          \
          /bin/systemctl enable   atop;              \
          /bin/systemctl enable   atop-rotate.timer; \
   ```

4. 安装编译atop依赖软件包。
   - SUSE12、SUSE15系列操作系统执行以下命令安装：

     zypper -n install make gcc zlib-devel ncurses-devel
   - EulerOS、Fedora系列操作系统执行以下命令安装：

     yum install make gcc zlib-devel ncurses-devel -y
   - Debian9、Debian10、Ubuntu系列操作系统执行以下命令安装：

     apt install make gcc zlib1g-dev libncurses5-dev libncursesw5-dev -y

5. 执行以下命令编译并安装atop。

   cd atop-2.6.0

   make systemdinstall

6. 编辑配置文件，修改采样周期。

   vi /etc/default/atop

   添加如下配置参数，修改后保存并退出。

   - LOGINTERVAL默认是600，可以修改成15，单位秒。
   - 默认atop日志保存周期为28天，可以根据实际修改LOGGENERATIONS的值为3，单位为天。

   ```
   LOGOPTS=""
   LOGINTERVAL=15
   LOGGENERATIONS=3
   LOGPATH=/var/log/atop
   ```

7. atop是默认启动，需重启atop服务使配置生效。

   systemctl restart atop atopacct atop-rotate.timer

8. 检查是否启动成功，atop atopacct是 active(running)表示运行正常，atop-rotate.timer是active(waiting) 表示运行正常。

   systemctl status atop atopacct atop-rotate.timer

   ```
   atop.service - Atop advanced performance monitor
   Loaded: loaded (/usr/lib/systemd/system/atop.service; enabled; vendor preset: enabled)
   Active: active (running)

   atopacct.service - Atop process accounting daemon
   Loaded: loaded (/usr/lib/systemd/system/atopacct.service; enabled; vendor preset: enabled)
   Active: active (running)

   atop-rotate.timer - Daily atop restart
   Loaded: loaded (/usr/lib/systemd/system/atop-rotate.timer; enabled; vendor preset: enabled)
   Active: active (waiting)
   ```

9. atop运行会占用额外的系统和磁盘资源，您可在问题排查完成后，执行以下命令停止atop。

   systemctl disable atop atopacct atop-rotate.timer

   systemctl stop atop atopacct atop-rotate.timer

分析 atop 日志

atop启动后，会将采集记录存放在/var/log/atop目录下的日志文件中。

执行如下命令，查看日志文件。

atop -r /var/log/atop/atop_2024XXXX

- **atop常用命令**

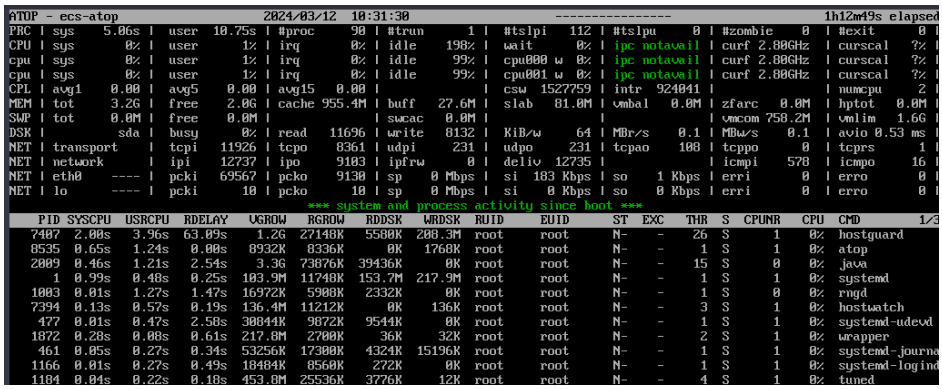
  打开日志文件后，您可以使用以下命令筛选数据。

  - c：按照进程CPU使用率进行降序筛选。
  - m：按照进程内存使用率进行降序筛选。
  - d：按照进程磁盘使用率进行降序筛选。
  - a：按照进程资源综合使用率进行降序筛选。
  - n：按照进程网络使用率进行降序筛选。
  - t：跳转到下一个监控采集点。
  - T：跳转到上一个监控采集点。
  - b：指定时间点，格式为YYYYMMDDhhmm。

- **系统资源监控字段含义**

下图为部分监控字段以及数值，具体数值根据采样周期和atop版本有所不同。下图仅供参考，具体数据以您实际数据为准。

图 3-7 系统资源监控字段



主要参数说明如下：

- ATOP 行：主机名、信息采样日期和时间点。
- PRC 行：进程整体运行情况。
- #sys 及 user：内核态和用户态所占 CPU 的时间值。
- #proc：进程总数。
- #zombie：僵死进程的数量。
- #exit：采样周期期间退出的进程数量。
- CPU 行：CPU 整体（即多核 CPU 作为一个整体 CPU 资源）的使用情况。CPU 行的各字段数值相加结果为 N*100%，N 为 CPU 核数。
- #sys 及 user：内核态和用户态所占 CPU 的时间比例。
- #irq：CPU 被用于处理中断的时间比例。
- #idle：CPU 处在完全空闲状态的时间比例。
- #wait：CPU 处在进程等待磁盘 IO ，导致 CPU 空闲状态的时间比例。
- CPL 行：CPU 负载情况。
- #avg1、avg5 和 avg15：过去1分钟、5分钟和15分钟内运行队列中的平均进程数量。
- #csw：指示上下文交换次数。
- #intr：指示中断发生次数。
- MEM 行：内存的使用情况。
- #tot：物理内存大小。
- #free：空闲的物理内存大小
- #cache ： 用于页缓存的内存大小。
- #buff：用于文件缓存的内存大小。
- #slab：系统内核占用的内存大小。
- SWP 行：交换空间的使用情况。
- #tot：交换区总量。
- #free：空闲交换空间大小。

- DSK 行：磁盘使用情况，每一个磁盘设备对应一列。如果有 sdb 设备，那么增加一行 DSK 信息。
- #sda：磁盘设备标识。
- #busy：磁盘忙时比例。
- #read 及 write：读、写请求数量。
- NET 行：多列 NET 展示了网络状况，包括传输层（TCP 和 UDP）、IP 层以及各活动的网口信息。
- #xxxxxi：各层或活动网口收包数目。
- #xxxxxo：各层或活动网口发包数目。

（可选）加载 netatop 内核模块

netatop内核模块能够监测每个进程或线程发送和接收的TCP及UDP数据包统计信息。在atop中，netatop未默认安装。如需监测网络使用率，可参考本示例进行安装。

本示例以Huawei Cloud EulerOS 2.0系统为例，为您展示如何为atop加载netatop内核模块。

如需在其他Linux操作系统加载netatop内核模块，请参考atop官方帮助文档。详细内容，请参见**Module netatop**。

1. 执行以下命令，为当前内核安装内核开发包及编译所需软件环境。

   sudo yum install -y kernel-devel dkms elfutils-libelf-devel
2. 执行以下命令，下载最新版本netatop源码至指定目录。

   cd /usr/src/ && sudo wget https://www.atoptool.nl/download/netatop-3.2.2.tar.gz --no-check-certificate
3. 执行以下命令，解压源码并进入源码目录。

   sudo tar -zxvf netatop-3.2.2.tar.gz && cd netatop-3.2.2
4. 执行以下命令，基于源码构建并安装模块和守护程序。

   sudo make && sudo make install
5. 执行以下命令，启动netatop服务。

   systemctl start netatop

配置 kdump 使用须知

配置kdump的操作适用于EulerOS以及CentOS 7系列Linux产品， 且云服务器的虚拟化类型为KVM。**了解更多**

kdump 简介

kdump是系统崩溃的时候，用来转储运行内存的一个工具。系统一旦崩溃，内核就无法正常工作了，这个时候将由kdump提供一个用于捕获当前运行信息的内核，该内核会将此时内存中的所有运行状态和数据信息收集到一个dump core文件中以便之后分析崩溃原因。

配置 kdump 操作步骤

1. 查看是否已经安装kexec-tools。

   rpm -q kexec-tools

如果没有安装，则执行下面命令安装。

yum install -y kexec-tools

2. 开启kdump默认启动。

   systemctl enable kdump

3. 设置crashkernel参数，设置这个参数的目的是预留内存给capture kernel。

   首先查看参数是否已经设置。

   grep crashkernel /proc/cmdline

   如果有显示，则表示已经设置，如果没有显示，则需要重新设置。

   设置crashkernel，编辑/etc/default/grub文件。

   ```
   GRUB_TIMEOUT=5
   GRUB_DEFAULT=saved
   GRUB_DISABLE_SUBMENU=true
   GRUB_TERMINAL_OUTPUT="console"
   GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=rhel00/root rd.lvm.lv=rhel00/swap
   rhgb quiet"
   GRUB_DISABLE_RECOVERY="true"
   ```

   找到GRUB_CMDLINE_LINUX参数，添加crashkernel=auto，其他内容不变。

4. 执行grub命令，使以上配置生效。

   grub2-mkconfig -o /boot/grub2/grub.cfg

5. 打开/etc/kdump.conf文件中找到“path”参数，添加以下内容。

   ```
   path  /var/crash
   ```

   默认是保存在/var/crash目录下，如果要保存到其他目录，则改成对应的目录，

   例如保存在/home/kdump下，则改成：

   ```
   path  /home/kdump
   ```

   说明

   要确保指定的路径有足够的空间保存vmcore，建议剩余空间不小于RAM大小；也可以保存在SAN，nfs等共享设备上。

6. 设置转存vmcore级别。

   修改/etc/kdump.conf文件，添加如下参数，如果存在则无需添加。

   ```
   core_collector makedumpfile -d 31 -c
   ```

   -c表示压缩vmcore文件，

   -d表示过滤掉部分无效的内存数据，可以根据需要调整，一般31即可，31是由如下的值与计算而成。

   ```
   zero pages   = 1
   cache pages   = 2
   cache private = 4
   user  pages   = 8
   free  pages   = 16
   ```

7. 执行如下命令重启系统，使以上配置生效。

   reboot

检查 kdump 配置是否生效

1. 执行以下命令，确认回显信息中crashkernel=auto

   cat /proc/cmdline |grep crashkernel

   ```
   BOOT_IMAGE=/boot/vmlinuz-3.10.0-514.44.5.10.h142.x86_64 root=UUID=6407d6ac-c761-43cc-
   a9dd-1383de3fc995 ro crash_kexec_post_notifiers softlockup_panic=1 panic=3
   reserve_kbox_mem=16M nmi_watchdog=1 rd.shell=0 fsck.mode=auto fsck.repair=yes net.ifnames=0
   spectre_v2=off nopti noibrs noibpb crashkernel=auto LANG=en_US.UTF-8
   ```


2. 执行以下命令，并确认回显信息中的配置信息正确。

   grep core_collector /etc/kdump.conf |grep -v ^"#"

   ```
   core_collector makedumpfile -l --message-level 1 -d 31
   ```

3. 执行以下命令，并确认回显信息中的配置信息正确。

   grep path /etc/kdump.conf |grep -v ^"#"

   ```
   path /var/crash
   ```

4. 执行以下命令，并确认回显信息中的Active的状态为active (exited)。

   systemctl status kdump

   ```
   ● kdump.service - Crash recovery kernel arming
   Loaded: loaded (/usr/lib/systemd/system/kdump.service; enabled; vendor preset: enabled)
   Active: active (exited) since Tue 2019-04-09 19:30:24 CST; 8min ago
   Process: 495 ExecStart=/usr/bin/kdumpctl start (code=exited, status=0/SUCCESS)
   Main PID: 495 (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/system-hostos.slice/kdump.service
   ```

5. 执行测试命令。

   echo c > /proc/sysrq-trigger

   这会触发kdump，重新启动，并将生成的vmcore文件保存的path参数指定的位置。

6. 检查vmcore是否生成。

   到所在环境path参数所指定的路径查看是否有vmcore文件生成，例如/var/crash/目录。

   ll /var/crash/

   可以看到生成了一个文件夹，里面有vmcore文件。

3.7 为什么操作系统实际版本与购买时镜像版本不一致?

问题现象

在云服务器执行以下命令查看系统当前版本：

/etc/redhat-release

得到当前云服务器版本为CentOS 7.6。但在控制台使用的镜像为CentOS 7.2（或者低于7.6的其他版本）。

说明

本节操作适用于CentOS、EulerOS操作系统云服务器。

根因分析

1. 问题原因对系统进行升级补丁后导致，执行以下命令查看yum操作记录。

   yum history

   回显信息如下所示：

   ```
   Loaded plugins: fastestmirror
   ID     | Login user            | Date and time    | Action(s)      | Altered
   -------------------------------------------------------------------------------
        8 | root <root>           | 2019-08-23 10:00 | I, U           |   40 EE
        7 | root <root>           | 2019-06-24 10:12 | I, U           |   55
        6 | root <root>           | 2019-02-22 11:10 | I, O, U        |  280 EE
        5 | root <root>           | 2019-02-22 11:09 | I, U           |    6
   ```

```
    4 | root <root>            | 2019-02-22 11:08 | Install       |    1
    3 | root <root>            | 2019-02-22 11:08 | Install       |    1
    2 | root <root>            | 2019-02-22 11:08 | Install       |    1
    1 | System <unset>           | 2019-02-22 10:49 | Install       |  352
history list
```

在8月23日的Action中包含I（install）和U（update）操作，该操作ID为8。

2. 执行以下命令进一步查看该操作详细信息。

   yum history info 8

   回显信息如下所示：

```
Loaded plugins: fastestmirror
Transaction ID : 8
Begin time     : Fri Aug 23 10:00:13 2019
Begin rpmdb    : 384:1c8e3df918de17e245b0dd7195f06f89656c5f27
End time       :          10:02:22 2019 (129 seconds)
End rpmdb      : 386:9a3172e7946f31d43c1268b6e1f2428125b3dfc5
User           : root <root>
Return-Code    : Success
Command Line   : update -y
```

   如上结果显示root用户执行了yum update操作，且操作成功，执行该操作后系统版本会更新为当前最新版本。

3.8 云服务器新内核启动失败如何设置使用第二内核启动

操作场景

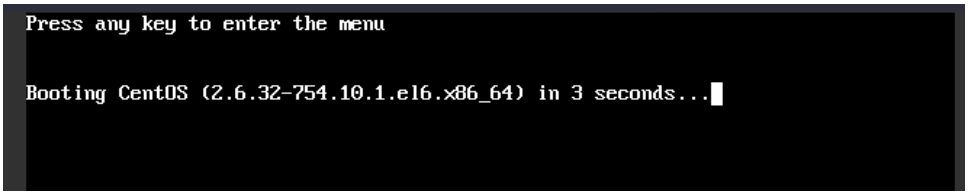
本节操作介绍云服务器新内核启动失败时如何设置使用第二内核启动。

本节操作适用于CentOS EulerOS操作系统，且系统内安装至少两个内核。

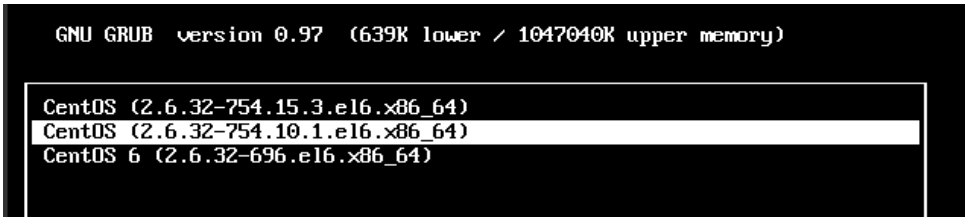
CentOS 6 操作系统

1. 登录控制台，重启云服务器，单击“远程登录”。
2. 在出现Booting CentOS界面时，按任意键，进入内核选择界面。

   图 3-8 Booting CentOS



3. 内核选择界面出现时按下键将光标移至第二内核，然后按回车键进行启动。



4. 待系统启动后，执行以下命令设置默认启动内核为第二内核。

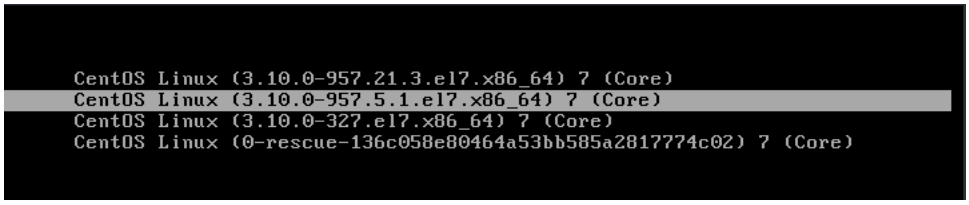
   sed 's/default=0/default=1/' /boot/grub/grub.conf -i

说明

default默认值为 0（代表从/boot/grub/grub.conf文件中kernel菜单中第一个，从上往下依次是 0，1，2 等）。

CentOS 7/EulerOS 操作系统

1. 登录控制台，重启云服务器，单击“远程登录”。
2. 在出现内核选择界面时，按下键，将光标移至第二内核，按回车键。



3. 待系统启动后，执行以下命令设置默认启动内核为第二内核。

   grub2-set-default 1

3.9 CentOS 7 中/etc/rc.local 开机启动脚本不生效怎么办?

问题现象

CentOS 7、EulerOS操作系统云服务器中，/etc/rc.local开机启动脚本不生效。

本节操作以CentOS 7操作系统为例分析根因，并介绍解决方法。

根因分析

出现该问题的可能原因如下：

- CentOS 7中/etc/rc.d/rc.local文件没有执行权限。解决方案请参考**处理方法1**。

  说明

  /etc/rc.local为/etc/rc.d/rc.local的软链接

  ```
  [root@wxf-cent7-test ~]# ll /etc/rc.d/rc.local
  -rw-r--r-- 1 root root 489 Mar 14 11:28 /etc/rc.d/rc.local
  [root@wxf-cent7-test ~]# ll /etc/rc.local
  lrwxrwxrwx. 1 root root 13 Nov  7 14:30 /etc/rc.local -> rc.d/rc.local
  ```

- /etc/rc.local配置路由重启不生效的场景，是由于添加路由依赖网络服务，而在CentOS 7系统启动过程中内核读取rc.local时网络服务尚未启动，导致添加路由失败。解决方案请参考**处理方法2**。

处理方法 1

针对/etc/rc.d/rc.local文件没有执行权限导致开机启动脚本执行失败的场景，解决方案如下。

说明

CentOS7中该文件默认没有可执行权限

1. 查看/etc/rc.d/rc.local是否有执行权限

   ls -l /etc/rc.d/rc.local

   ```
   -rw-r--r-- 1 root root 473 Sep 14 02:19 /etc/rc.d/rc.local
   ```

   如回显信息所示该文件没有执行权限，需要为/etc/rc.d/rc.local添加可执行权限。
2. 执行以下命令为/etc/rc.d/rc.local添加可执行权限

   chmod +x /etc/rc.d/rc.local

处理方法 2

针对/etc/rc.local配置路由重启不生效的场景，解决方案如下。

方法一：不使用/etc/rc.local配置路由，改为将路由写入静态路由配置文件（该方法即使重启网卡路由也不会丢失）。

1. 在/etc/sysconfig/network-scripts/目录中创建或修改route-<interface>文件。

   该目录<interface>是与路由相关的接口的名称。

   ```
   <network/prefix> via <gateway>
   ```

   其中<network/prefix>是带有前缀的远程网络，<gateway>是下一跳的IP地址。

   例如，要添加一条通过192.168.100.10到10.20.30.0/24网络的路由，以便在eth0启用时都处于活动状态：

   cat /etc/sysconfig/network-scripts/route-eth0

   ```
   10.20.30.0/24 via 192.168.100.10
   ```
2. 执行以下命令，使修改生效。

   ifup eth0

方法二：/etc/rc.d/rc.local开机启动脚本由rc-local服务引导执行，可以修改在network-online.target后启动该服务。

1. rc-local服务配置路径为/usr/lib/systemd/system/rc-local.service。

   执行以下命令，在[Unit]模块中添加或修改Requires和After项值为network-online.target。

   cat /usr/lib/systemd/system/rc-local.service |grep -v "^#"

   修改内容如下：

   ```
   [Unit]
   Description=/etc/rc.d/rc.local Compatibility
   ConditionFileIsExecutable=/etc/rc.d/rc.local
   Requires=network-online.target
   After=network-online.target

   [Service]
   Type=forking
   ExecStart=/etc/rc.d/rc.local start
   TimeoutSec=0
   RemainAfterExit=yes
   ```

   说明

   network-online.target是主动等待直到网络“启动”的target，其中“启动”的定义由网络管理软件定义。通常，它表示某种已配置的、可路由的IP地址。其主要目的是主动延迟服务的激活，直到建立网络为止。
2. 执行以下命令，确认/etc/rc.d/rc.local有执行权限。

   ls -l /etc/rc.d/rc.local

   如果显示没有可执行权限，请参考**处理方法1**处理。

3. 通知systemd重新加载配置文件。
   systemctl daemon-reload
4. 重启rc-local.service，使/etc/rc.d/rc.local脚本立即生效。
   systemctl restart rc-local.service

3.10 修改/etc/security/limits.conf 文件，重启后不生效怎么办?

问题现象

修改/etc/security/limits.conf文件，重启后配置项不生效。

可能原因

Linux操作系统云服务器中限制资源使用的配置文件是/etc/security/limits.conf和/etc/security/limits.d/目录，/etc/security/limits.d/目录中的配置优先级高于/etc/security/limits.conf的配置。

如果修改/etc/security/limits.conf文件，重启后不生效，则可能是由于limits.conf中的修改被/etc/security/limits.d/目录中配置项的值所覆盖。

解决方案

修改/etc/security/limits.d/目录中配置项或修改/etc/security/limits.conf文件。

说明

如果修改了/etc/security/limits.conf 文件没有生效，请检查/etc/security/limits.d/目录中配置项的值。

3.11 使用 taskset 命令让进程运行在指定 CPU 上

操作场景

taskset命令，可用于进程的CPU调优，可以把云服务器上运行的某个进程，指定在某个CPU上工作。

本节操作指导用户使用taskset命令让进程运行在指定CPU上。

适用范围

CentOS、EulerOS系列操作系统。

操作步骤

1. 执行如下命令，查看云服务器CPU核数。
   cat /proc/cpuinfo
   关于CPU的核心参数说明：
   - processor：指明第几个CPU处理器

- cpu cores：指明每个处理器的核心数

2. 执行以下命令，获取进程状态（以下操作以进程test.sh为例，对应的pid为23989）

   ps aux | grep test.sh

```
[root@ecs-linux-bj1 ~]# ps aux|grep test.sh
root     23989  0.0  0.2 113188  3016 pts/1    S    16:25   0:00 /bin/bash ./test.sh
```

3. 执行以下命令，查看进程当前运行在哪个CPU上。

   taskset -p *进程号*

   例如：taskset -p 23989

```
[root@ecs-linux-bj1 ~]# taskset -p 23989
pid 23989's current affinity mask: 1
```

   显示的是十六进制数字1，转换为二进制为0001。每个1对应一个CPU，所以进程运行在第0个CPU上。

4. 执行以下命令，指定进程运行在第二个CPU（CPU1）上。

   taskset -pc 1 *进程号*

   例如：**taskset -pc 1 23989**

   说明

   CPU的标号是从0开始的，所以CPU1表示第二个CPU（第一个CPU的标号是0），这样就把应用程序test.sh绑定到了CPU1上运行。

   也可以使用如下命令在启动程序时绑定CPU（启动时绑定到第二个CPU）上。

   taskset -c 1 ./test.sh&

3.12 pip 安装软件时出现错误：command ´gcc´ failed with exit status 1

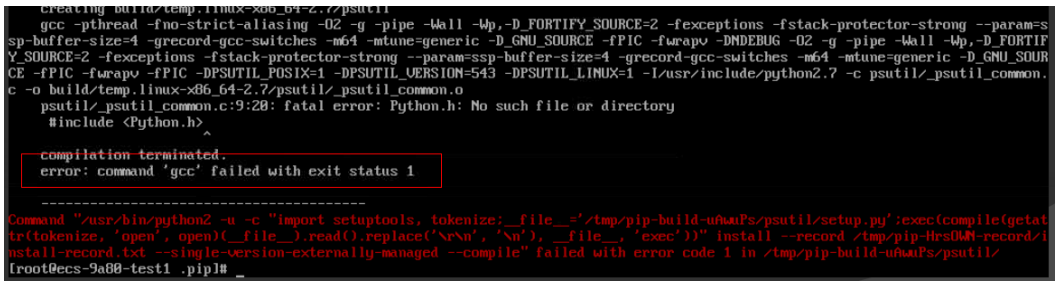
问题描述

安装Python库软件时，需配置pip源。以中国科技大学镜像源为例：

```
[root@test home]# cat /root/.pip/pip.conf
[global]
index-url = https://pypi.mirrors.ustc.edu.cn/simple/
trusted-host = pypi.mirrors.ustc.edu.cn
```

安装过程中，系统报错"command ´gcc´ failed with exit status 1"，如图3-9所示。但是，在用pip安装Python库软件之前，确认已经使用yum命令安装了gcc。

图 3-9 安装报错



问题原因

缺少openssl-devel支持。

处理方法

以安装psutil模块为例：

1. 执行以下命令，安装openssl-devel。

   yum install gcc libffi-devel python-devel openssl-devel -y

2. 再次使用pip安装python库软件，可以看到系统不再报错，如图3-10所示。

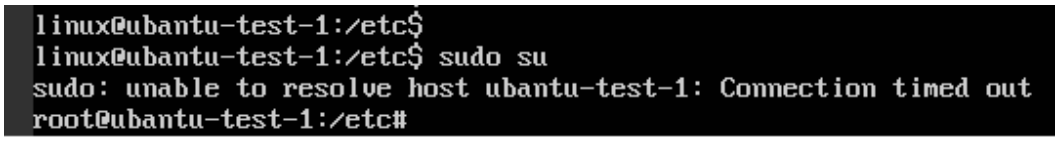
   图 3-10 安装成功

3.13 非 root 用户切 root 用户时，连接超时怎么办?

问题描述

针对镜像为Ubuntu、Debian的弹性云服务器，使用sudo命令切换root用户时，系统提示连接超时，如图3-11所示。

图 3-11 连接超时



处理方法

1. 登录弹性云服务器。
2. 执行以下命令，编辑hosts文件。

   vi /etc/hosts

3. 按“i”，进入编辑模式。
4. 在hosts文件最后添加一行内容，写入IP地址和主机名。

   私有IP地址 主机名

   示例：

   假设弹性云服务器的主机名为“hostname”，私有IP地址为“192.168.0.1”，则需添加的语句为：

   192.168.0.1 hostname

5. 按“Esc”退出编辑模式。
6. 执行以下命令，保存并退出。

   :wq

说明

针对镜像为Ubuntu、Debian的弹性云服务器，如果需要更新主机名，需将/etc/cloud/cloud.cfg中的manage_etc_hosts参数设置为false，同时将新设置的主机名更新至/etc/hosts中。编辑/etc/hosts文件时，请勿删除127.0.0.1所在行语句，否则会出现非root用户切换root超时问题。

3.14 CentOS 云服务器根目录设置成 777 权限怎么办?

问题描述

执行**chmod -R 777 /** 导致CentOS云服务器根目录权限设置成777，系统中的大部分服务以及命令无法使用。此时可通过系统自带的**getfacl**命令来拷贝和还原系统权限，本节操作介绍误操作导致根目录设置成777权限的补救措施。

说明

对文件或目录设置777权限代表它将对所有用户都是可读、可写和可执行的，根目录设置777权限后存在安全风险。本节操作是临时的补救措施，恢复目录权限后，建议您备份数据，重装操作系统，避免777权限后续带来的安全风险问题。

操作步骤

本节操作使用CentOS7.5操作系统云服务器测试验证。

1. 设置了777权限后请勿关闭或重启云服务器，在故障云服务器执行以下命令，修改ssh连接相关文件的权限。

   cd /etc

   chmod 644 passwd group shadow

   chmod 400 gshadow

   cd ssh

   chmod 600 moduli ssh_host_dsa_key ssh_host_key ssh_host_rsa_key

   chmod 644 ssh_config ssh_host_dsa_key.pub ssh_host_key.pub ssh_host_rsa_key.pub

   chmod 640 sshd_config

2. 执行完上述命令后ssh可以连接但无法使用root。

   su root

   ```
   root "su: cannot set groups:"
   ```

   执行以下命令，su必须有s权限才能读取root的相关配置。

   chmod u+s ·which su·

   完成之后就可以用root权限进入系统了。

3. 创建一台权限正常的临时云服务器：Linux操作系统，内核版本与故障云服务器相同。

4. 在临时云服务器上执行以下命令，将这个正常系统的/目录下所有文件的权限都备份保存在 systemp.bak 中。

   getfacl -R / >systemp.bak

5. 使用**scp**命令将正常的备份文件传至故障云服务器中。

- 您可以在临时云服务器上执行以下命令，上传**systemp.bak**文件到故障云服务器。

  scp systemp.bak文件地址 用户名@弹性公网IP:故障云服务器文件地址

  例如：**scp /systemp.bak root@119.**.**.**:/121.**.**.****
- 或在故障云服务器上执行以下命令，从临时云服务器上下载**systemp.bak**文件到故障云服务器。

  scp 用户名@弹性公网IP:临时云服务器systemp.bak文件地址 故障云服务器文件地址

  例如：**scp root@121.**.**.**:/systemp.bak /**

6. 在故障云服务器中执行以下命令将现在的系统权限恢复成和正常系统一样。

   setfacl --restore=systemp.bak
7. 重启系统之前新建脚本，避免ssh连接失败。

   vim sshtmp.sh

   ```
   cat sshtmp.sh
   #----------start----------
   sleep 300
   cd /etc
   chmod 644 passwd group shadow
   chmod 400 gshadow
   cd ssh
   chmod  600  moduli  ssh_host_dsa_key ssh_host_key ssh_host_rsa_key
   chmod  644 ssh_config ssh_host_dsa_key.pub ssh_host_key.pub ssh_host_rsa_key.pub
   chmod  640 sshd_config
   chmod u+s `which su`
   #-----------------end---------
   ```
8. 执行以下命令添加到Linux启动脚本rc.local中。

   echo '/sshtmp.sh &' >>/etc/rc.local
9. 执行以下命令重启操作系统。

   reboot

   重启后云服务器恢复正常，结束sshtmp.sh进程，恢复rc.local，删除sshtmp.sh，重新查看系统权限是否恢复正常。

后续操作

对文件或目录设置777权限代表它将对所有用户都是可读、可写和可执行的，根目录设置777权限后存在安全风险。

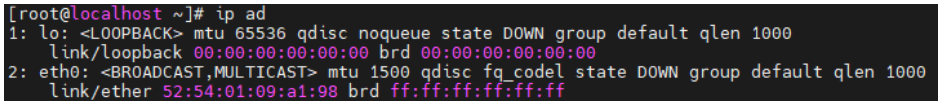
本节操作是临时的补救措施，恢复目录权限后，建议您备份数据，重装操作系统，避免777权限后续带来的安全风险问题。

3.15 Linux 实例 IP 地址丢失怎么办?

问题描述

当ECS实例在未重启的情况下连续运行超过一定时间后，出现IP丢失、实例断网、网络瘫痪的情况，如图3-12所示。

图 3-12 故障现象



可能原因

ECS实例的网络配置为DHCP（Dynamic Host Configuration Protocol，动态主机设置协议）方式。

以CentOS 7的ECS为例，如果网络配置为DHCP方式，当ECS实例启动时，Linux系统的NetworkManager服务会启动dhclient进程，dhclient进程会向DHCP服务器请求分配IP地址，并获得IP地址租约到期时间。

正常情况下，dhclient进程会定期向DHCP服务器更新租约到期时间，以确保实例IP地址的可用性，如下图：

图 3-13 正常情况

当用户误操作停止了NetworkManager服务，并清理了dhclient进程时，会导致ECS实例无法自动更新IP地址的续租到期时间。当租约到期后，ECS实例的IP地址会被释放，导致网络不通。

解决方案

1. 远程登录ECS实例。
2. 执行以下命令，重启NetworkManager服务，并设置为开启自启动。

   systemctl restart NetworkManager

   systemctl enable NetworkManager
3. 执行以下命令，查看NetworkManager服务状态。

   systemctl status NetworkManager

   图 3-14 查看 NetworkManager 服务状态

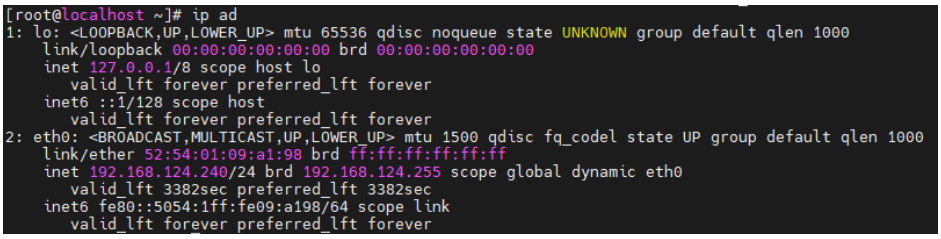
```
[root@localhost ~]# systemctl status NetworkManager
● NetworkManager.service - Network Manager
     Loaded: loaded (/usr/lib/systemd/system/NetworkManager.service; enabled; v>
    Drop-In: /usr/lib/systemd/system/NetworkManager.service.d
             └─NetworkManager-ovs.conf
     Active: active (running) since Thu 2023-03-02 15:47:17 CST; 4min 1s ago
       Docs: man:NetworkManager(8)
   Main PID: 308119 (NetworkManager)
      Tasks: 4 (limit: 21656)
     Memory: 3.8M
     CGroup: /system.slice/NetworkManager.service
             ├─ 308119 /usr/sbin/NetworkManager --no-daemon
             └─ 308129 /sbin/dhclient -d -q -sf /usr/libexec/nm-dhcp-helper -pf>

Mar 02 15:47:17 localhost NetworkManager[308119]: <info>  [1677743237.3023] dev>
Mar 02 15:47:17 localhost NetworkManager[308119]: <info>  [1677743237.3025] dev>
Mar 02 15:47:17 localhost NetworkManager[308119]: <info>  [1677743237.3032] man>
Mar 02 15:47:17 localhost NetworkManager[308119]: <info>  [1677743237.3036] man>
Mar 02 15:47:17 localhost NetworkManager[308119]: <info>  [1677743237.3037] pol>
Mar 02 15:47:17 localhost dhclient[308129]: bound to 192.168.122.59 -- renewal >
Mar 02 15:47:17 localhost NetworkManager[308119]: <info>  [1677743237.3177] dev>
Mar 02 15:47:17 localhost NetworkManager[308119]: <info>  [1677743237.3192] man>
Mar 02 15:47:17 localhost NetworkManager[308119]: <info>  [1677743237.3196] man>
Mar 02 15:47:17 localhost NetworkManager[308119]: <info>  [1677743237.3264] pol>
```

4. 执行以下命令，查看网络状态。

   ip ad

图 3-15 查看网络状态



若出现如图3-15所示结果，表示ECS实例的网络恢复正常。

附录

常见操作系统的默认网络服务配置，建议不修改，直接采用默认值。

表 3-2 常见操作系统的默认网络服务配置

操作系统	网络服务	是否内置DHCP功能
CentOS 6	Network	否，有单独的dhclient进程
CentOS 7	NetworkManager	否，有单独的dhclient进程
CentOS 8	NetworkManager	是
Ubuntu 16.04	NetworkManager	否，有单独的dhclient进程
Ubuntu 18.04	NetworkManager	否，有单独的dhclient进程
Ubuntu 20.04	NetworkManager	是
Ubuntu 22.04	NetworkManager	是

3.16 内核参数 kernel.unknown_nmi_panic 配置错误导致 Linux ECS 实例异常重启

问题描述

Linux操作系统的ECS实例发生异常重启事件，错误提示如下：

```
Kernel panic - not syncing: NMI: Not continuing
```

同时，内核日志打印如下信息：

```
[645683.754132] Uhhuh. NMI received for unknown reason 20 on CPU 1.
[645683.754133] Do you have a strange power saving mode enabled?
[645683.754133] Kernel panic - not syncing: NMI: Not continuing
```

可能原因

如果Linux操作系统ECS实例的内核参数kernel.unknown_nmi_panic配置为1，则ECS会在系统收到NMI中断时主动通过panic系统重启。

通常情况下，将内核参数kernel.unknown_nmi_panic配置为1的目的是为了在发生NMI中断时，主动触发panic，从而进行系统定位。由于个别型号的CPU会在正常业务流程中产生NMI中断，在这种情况下如果将内核参数kernel.unknown_nmi_panic配置为1，将会导致ECS产生非预期的异常重启事件。

约束与限制

本节操作涉及修改系统内核参数，在线修改内核参数会出现内核不稳定，请评估风险后操作。

解决方案

1. 远程登录ECS实例。
2. 执行以下命令，查看ECS实例内核参数kernel.unknown_nmi_panic的值。

   sysctl -n kernel.unknown_nmi_panic

   如果内核参数的取值为1，说明是由于内核参数配置错误引起的ECS实例异常重启。

   图 3-16 排查结果

   ```
   linux-JjFcyI:~ # sysctl -n kernel.unknown_nmi_panic
   1
   ```

3. 执行以下命令，查看是否存在内核参数kernel.unknown_nmi_panic相关配置。

   vim /etc/sysctl.conf

   在/etc/sysctl.conf文件中，排查是否存在kernel.unknown_nmi_panic的相关配置。

   - 如果存在kernel.unknown_nmi_panic=1的配置，将该配置改为kernel.unknown_nmi_panic=0
   - 如果不存在kernel.unknown_nmi_panic=1的配置，增加kernel.unknown_nmi_panic=0

   图 3-17 查看/etc/sysctl.conf 文件

   ```
   # sysctl settings are defined through files in
   # /usr/lib/sysctl.d/, /run/sysctl.d/, and /etc/sysctl.d/.
   #
   # Vendors settings live in /usr/lib/sysctl.d/.
   # To override a whole file, create a new file with the same in
   # /etc/sysctl.d/ and put new settings there. To override
   # only specific settings, add a file with a lexically later
   # name in /etc/sysctl.d/ and put new settings there.
   #
   # For more information, see sysctl.conf(5) and sysctl.d(5).
   #
   kernel.unknown_nmi_panic=0
   ~
   ```

4. 按“Esc”，输入**:wq**保存并退出。

5. 执行以下命令，使配置生效。
   sysctl –p

   图 3-18 配置生效

   ```
   linux-JjFcyI:~ # sysctl -p
   kernel.unknown_nmi_panic = 0
   ```

   说明

   该修复方案热生效，无需重启ECS。

结果验证

1. 执行以下命令，查看结果是否为0。
   cat /proc/sys/kernel/panic_on_unrecovered_nmi

   图 3-19 检查结果 1

   ```
   linux-JjFcyI:~ # cat /proc/sys/kernel/panic_on_unrecovered_nmi
   0
   ```

2. 执行以下命令，查看内核参数sysctl -n kernel.unknown_nmi_panic是否为0。

   图 3-20 检查结果 2

   ```
   linux-JjFcyI:~ # sysctl -n kernel.unknown_nmi_panic
   0
   ```

   如果验证结果符合预期，说明修改成功。

3.17 Linux 实例执行命令或启动服务时出现错误：Cannot allocate memory

问题描述

Linux操作系统的ECS实例内存充足，但是在执行命令或启动服务时，出现错误提示“Cannot allocate memory”。

命令及执行结果如下：

```
root@localhost:~# free -m
              total        used        free      shared  buffers/cached   available
Mem:           3890         125        3179           2         504        3463
Swap:             0           0           0
root@localhost:~# uname -a
-bash: fork: Cannot allocate memory
```

可能原因

出现该错误信息表示系统的进程ID（PID），即系统中运行的进程/线程数达到了最大限制，该限制由内核参数/proc/sys/kernel/pid_max控制。

解决方案

1. 远程登录ECS实例。
2. 执行以下命令，查看系统当前已运行的进程数。

   ps -eLf | wc -l

   结果如下：

   ```
   32753
   ```

   也可以通过执行以下命令，通过观测plist-sz列数值查看系统已运行的进程数变化情况。

   说明

   如果执行sar –q命令后提示“command not found”，请先执行以下命令安装软件包：

   - CentOS系统：**yum install sysstat**
   - Ubuntu系统：**apt install sysstat**

   sar -q

   结果如下：

   ```
   ...
   00:00:01      runq-sz  plist-sz   ldavg-1   ldavg-5  ldavg-15  blocked
   10:45:01        0     32722      0.10      0.12      0.16     0
   10:46:01        1     32730      0.21      0.15      0.17     0
   10:47:01        2     32752      0.07      0.11      0.15     0
   ```

3. 执行以下命令，查看系统配置的最大进程数。

   cat /proc/sys/kernel/pid_max

   ```
   32768
   ```

   如果系统当前已经运行的进程数接近或达到系统配置的最大进程数，则说明需要增大/proc/sys/kernel/pid_max的数值。

4. 根据业务需要，执行以下命令，调整/proc/sys/kernel/pid_max的数值。

   以调整为65530为例：

   echo "kernel.pid_max=65530" >> /etc/sysctl.conf

   sysctl -p

   结果如下：

   ```
   vm.swappiness = 0
   net.core.somaxconn = 1024
   net.ipv4.tcp_max_tw_buckets = 5000
   net.ipv4.tcp_max_syn_backlog = 1024
   kernel.pid_max = 65530
   ```

3.18 fork 失败，无法创建新的线程怎么办?

问题描述

Linux操作系统的ECS，在执行命令或者日志打印时，出现如下报错信息：

错误信息1：

```
root@localhost:~# free -g
              total        used        free      shared     buffers   cached
Mem:            94          43          51           0           0        0
Swap:           19           0          19
root@localhost:~# uname -a
-bash: fork: Cannot allocate memory
```

错误信息2：

```
xxxxsshd2[23985]: fatal: setresuid 20054: Resource temporarily unavailable
xxxxsshd2[28377]: Disconnecting: fork failed: Resource temporarily unavailable
xxxxsshd2[4484]: Disconnecting: fork failed: Resource temporarily unavailable
```

错误信息3：

```
[root@ecs-xxxx ~]$ sudo docker info
runtime/cgo: pthread_create failed: Resource temporarily unavailable
SIGABRT: abort
```

根因分析

通常情况，出现上述错误由于创建线程失败，可能原因是ECS系统内存不足，系统当前的线程数达到了配置的最大值。

处理方法

1. 登录管理控制台。
2. 通过ECS的主机监控功能的“内存使用率”指标，查看云服务器内存使用情况确认云服务器内存情况，详细操作，请参见**查看监控指标** 。
   - 如果内存不足，建议扩容内存或者优化内存的使用，扩容内存可参考**变更规格通用操作**。
   - 否则，执行步骤**3**。
3. 以root用户登录云服务器，执行以下命令，排查message和dmesg日志。

   dmesg -T

   cat /var/log/messages
   - 如果出现如**图3-21**所示的cgroup相关报错打印，执行步骤**8**。
   - 否则，执行步骤**4**。

   图 3-21 日志报错

4. 执行以下命令，查看当前系统线程总数。

   ps -efL | wc -l
5. 执行以下命令，将得到的两个值与步骤**4**查到的当前系统线程总数进行对比。

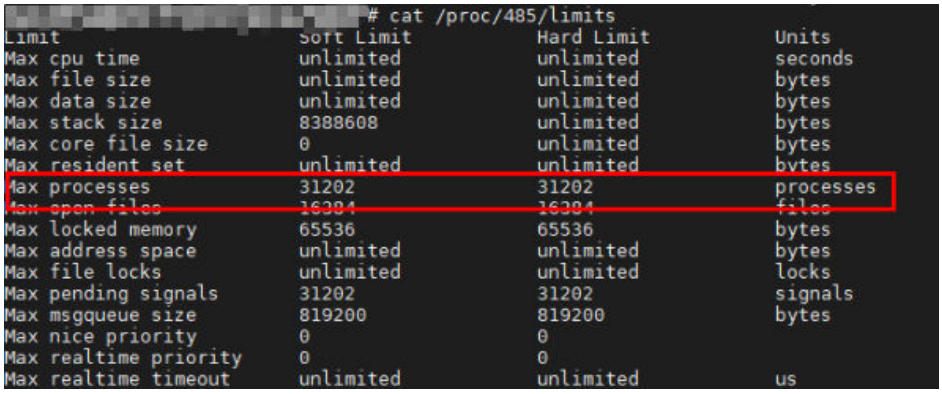
   sysctl -a | grep pid_max

   sysctl -a | grep threads-max
   - 如果当前系统线程总数接近这两个值其中一个，那么就需要对这pid_max、threads-max这两个参数进行调优。调优步骤请参考**调优pid_max、threads-max参数**。
   - 否则，执行步骤**6**。
6. 执行以下命令，确定报错进程的pid。

   ps -ef | grep 报错进程名
7. 执行以下命令，根据得到的pid检查该进程的limits配置：

cat /proc/pid/limits

图 3-22 确定进程 limits 配置



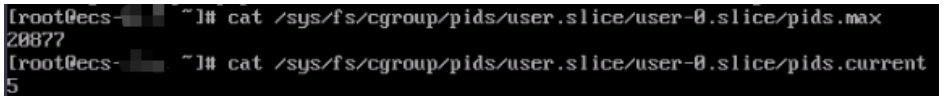
- 查看Max processes行，如果当前用户创建的所有线程数接近该值，那么需要对limits参数进行调优，调优步骤请参考**调优limits参数**。
- 否则，执行步骤**8**。

8. 执行以下命令，根据日志的cgroup报错可以得到pid_max、pids.current参数值。

   cat /sys/fs/cgroup/pids/拼接日志中报错目录/pids.max

   cat /sys/fs/cgroup/pids/拼接日志中报错目录/pids.current

   图 3-23 cgroup 目录

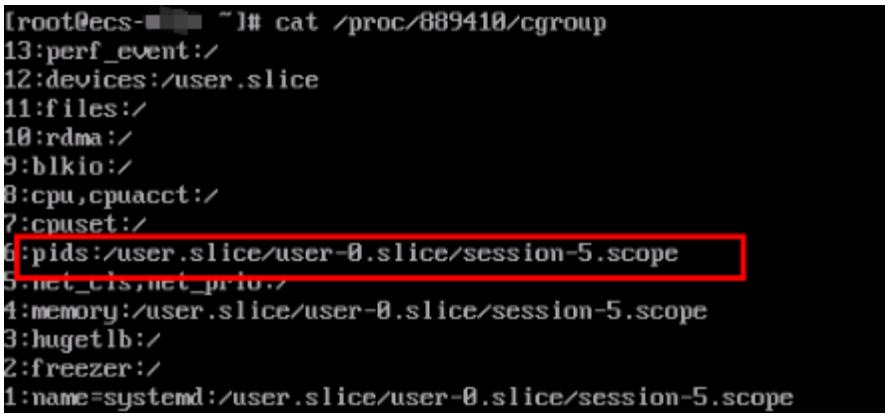
   

   示例如下：

   a. 执行以下命令，根据进程的pid查找对应的cgroup目录。

      cat /proc/pid/cgroup

      图 3-24 根据 pid 查找对应的 cgroup 目录

      返回结果中的pids行为“/user.slice/user-0.slice/session-5.scope/”，与/sys/fs/cgroup/pids/拼接，可得进程对应的cgroup目录为“/sys/fs/cgroup/pids/user.slice/user-0.slice/session-5.scope/”。

b. 执行以下命令，根据得到的cgroup目录获取pid_max、pids.current参数值。

cat /sys/fs/cgroup/pids/user.slice/user-0.slice/session-5.scope/pids.max

cat /sys/fs/cgroup/pids/user.slice/user-0.slice/session-5.scope/pids.current

- 如果pids.current接近pids.max，那么需要对cgroup参数进行调优，调优步骤请参考**调优cgroup参数**。
- 否则，请提交工单联系技术支持处理。

相关命令

- 调优pid_max、threads-max参数
  a. 由于不同操作系统发行版默认参数不一致，执行以下命令，查询当前配置参数。

  sysctl -a | grep pid_max

  sysctl -a | grep threads-max

  b. 执行以下命令，修改pid_max、threads-max参数。

  echo 'kernel.pid_max = 4194304' >> /etc/sysctl.conf

  echo 'kernel.threads-max = 4194304' >> /etc/sysctl.conf

  c. 执行以下命令，使配置生效。

  sysctl -p
- 调优limits参数
  a. 以启动报错业务进程的用户登录云服务器，执行以下命令查询当前配置参数。

  ulimit -u

  b. 执行以下命令，根据业务需求和当前值评估，配置合适的nproc上限。

  以root用户nproc配置100000为例：

  echo 'root soft nproc 100000' >> /etc/security/limits.conf

  echo 'root hard nproc 100000' >> /etc/security/limits.conf

  c. 重新登录云服务器，执行以下命令确认配置是否生效。

  ulimit -u

  - 回显值如果是步骤**b**配置的值，表示配置已经生效，在该session重启业务进程即可。
  - 否则，请提交工单联系技术支持处理。
- 调优cgroup参数
  - 临时修改方案：

    执行以下命令，以将相关cgroup临时修改上限为最大为例，修改当前超出限制的cgroup目录。

    echo max > /sys/fs/cgroup/pids/user.slice/user-0.slice/session-25.scope/pids.max
  - 永久修改方案：

执行以下命令，以将相关cgroup设置到无穷大为例，修改当前超出限制的cgroup目录。

该值可以根据需要调整，修改完成后需要重启云服务器使配置生效。

echo DefaultTasksMax=infinity >>/etc/systemd/system.conf

echo DefaultTasksMax=infinity >>/etc/systemd/user.conf

echo UserTasksMax=infinity >>/etc/systemd/logind.conf

3.19 错误的系统配置导致启动或远程登录失败

问题描述

Linux系统经常因为错误的系统配置导致系统无法启动成功或者无法登录系统，由于无法通过SSH或者VNC登录系统，导致错误的系统配置无法得到修复，需要一种通用的方法来修改该异常实例系统盘上的错误配置，使得实例或者系统能够恢复正常。本文介绍一种通用的异常恢复手段，通过卸载该异常实例的系统盘，并作为数据盘挂载到其他正常ECS实例进行修复。

问题原因

常见的可能导致系统启动失败或者无法进入系统的系统配置错误如表3-3所示。

表 3-3 常见系统配置错误

问题类型	典型问题
配置错误	/etc/fstab文件缺失或者配置错误
	SELinux配置错误
	/etc/security/limits.conf配置错误
	/etc/passwd配置格式错误
	/etc/shadow配置格式错误
	/etc/ssh/sshd_config配置格式错误
文件或目录缺失	/etc/ssh目录被误删
	/etc/security目录被误删
	/etc/passwd文件被误删
	/etc/shadow文件被误删
	/etc/ssh/sshd_config文件被误删
文件权限错误	SSH依赖的私钥权限配置过大
	SSH依赖的公钥权限配置过大
内核参数配置错误	vm.nr_hugepages配置过大

操作步骤

步骤1 准备正常实例

准备一台可以正常访问的ECS实例，操作系统与该异常实例保持一致。

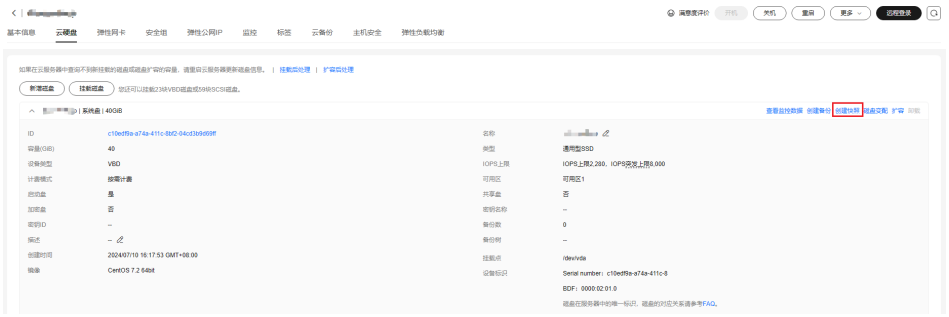
- 可以是已有ECS实例
- 可以新创建一台ECS实例，具体操作请参见**购买并登录Linux弹性云服务器**。

步骤2 创建快照

操作异常实例系统盘前，建议您对该实例系统盘创建快照，避免数据丢失。具体操作请参见**创建快照**。

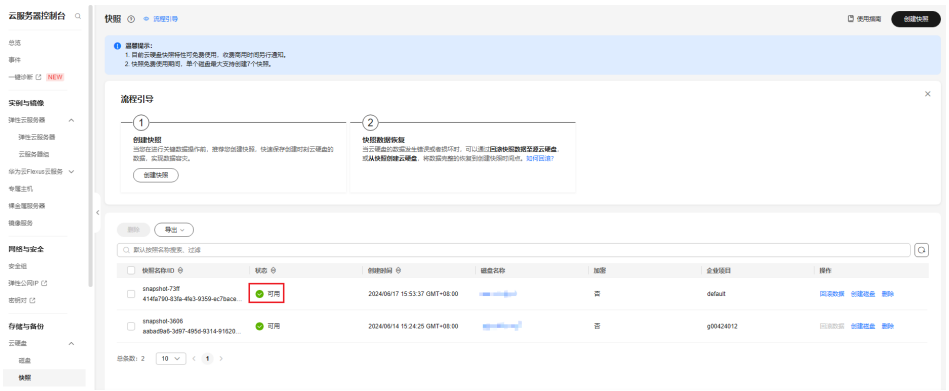
1. 登录管理控制台。
2. 单击“ ☰ ”，选择“计算 > 弹性云服务器”。
3. 在实例列表页面找到异常的实例，单击该异常实例的实例名称，进入该异常实例的详情页面。
4. 在实例详情页面，单击“云硬盘”页签。
5. 在“云硬盘”页面中，单击“创建快照”。

图 3-25 创建快照



6. 在ECS管理控制台左侧导航栏，选择“云硬盘 > 快照”，可以查看快照状态，当“状态”为“可用”时，表示快照创建成功。

图 3-26 查看快照状态



步骤3 卸载异常实例系统盘

快照创建完成后，需要停止该异常实例，然后卸载该异常实例的系统盘，具体操作请参见**卸载系统盘**。

步骤4 将异常实例的系统盘挂载为正常实例的数据盘

具体的操作步骤如下：

1. 登录管理控制台。
2. 单击“ ”，选择“计算 > 弹性云服务器”。
3. 在实例列表页面找到正常的实例，单击该正常实例的实例名称，进入该正常实例的详情页面。
4. 在实例详情页面，单击“云硬盘”页签。
5. 在“云硬盘”页面中，单击“挂载磁盘”。

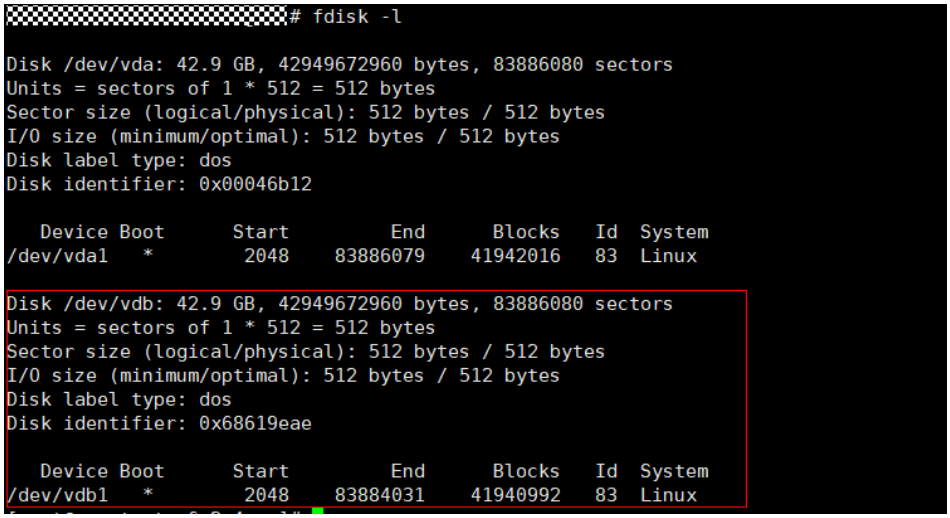
图 3-27 挂载磁盘

6. 在弹出的对话框中，选择**步骤3**已卸载的异常实例的系统盘，“磁盘属性”为“数据盘”，单击“确定”，即可完成挂载。

图 3-28 挂载数据盘

7. 等待一段时间，在ECS管理控制台左侧导航栏，选择“云硬盘 > 磁盘”，可以查看磁盘状态。当该磁盘“状态”变为“正在使用”时，表示已经成功挂载磁盘。
8. 挂载完成后，**通过SSH或VNC远程登录**正常实例，执行**fdisk -l**命令，会看到该正常实例新增一块磁盘设备/dev/vdb和分区/dev/vdb1。

图 3-29 查看新增磁盘设备



9. 执行以下命令，将异常实例的系统盘作为数据盘挂载到正常实例。

   mount <数据盘分区> <挂载点>

   - 数据盘分区：8查询到的分区为准，比如：/dev/vdb1
   - 挂载点：正常实例的本地目录，比如：/mnt

   以数据盘分区为/dev/vdb1，挂载点为/mnt为例，命令如下：

   mount /dev/vdb1 /mnt

步骤5 修复数据盘

您可以在该正常实例中进行对应操作来修复数据盘，常见的四种场景如下：

场景一：文件配置错误

以修复异常实例**/etc/fstab**文件配置错误为例，操作步骤如下：

1. 在正常实例上，对数据盘中的**/mnt/etc/fstab**文件进行修复，执行以下命令，对文件配置错误的内容进行编辑修改。

   vim /mnt/etc/fstab

2. 文件编辑修改完成后，按**Esc**键退出编辑模式，并输入**:wq**保存后退出。

   说明

   本示例以异常实例**/etc/fstab**文件修复为例，其他文件配置错误的修复请修改对应文件的目录。

   例如：/etc/ssh/sshd_config文件对应数据盘上的目录为/mnt/etc/ssh/sshd_config。

场景二：文件或目录缺失

以修复异常实例**/etc/security**目录缺失为例，操作步骤如下：

在正常实例上，执行以下命令，对数据盘中的**/mnt/etc/security**目录缺失进行修复。

cp -rfa /etc/security /mnt/etc/

说明

本示例以异常实例**/etc/security**目录缺失进行修复为例，其他文件或目录缺失的修复请修改对应文件的目录。

例如：/etc/ssh/sshd_config文件缺失则执行**cp -rfa /etc/ssh/sshd_config /mnt/etc/ssh**命令进行修复。

场景三：文件权限错误

以修复异常实例**/etc/ssh/ssh_host_ecdsa_key**文件权限配置错误为例，操作步骤如下：

在正常实例上，执行以下命令，对数据盘中的**/mnt/etc/ssh/ssh_host_ecdsa_key**文件进行权限修复。

chmod 600 /mnt/etc/ssh/ssh_host_ecdsa_key

说明

本示例以异常实例**/etc/ssh/ssh_host_ecdsa_key**文件修复为例，其他文件权限配置错误的修复请修改对应文件的目录。

例如：/etc/ssh/ssh_host_ed25519_key文件对应数据盘上的目录为/mnt/etc/ssh/ssh_host_ed25519_key。

场景四：内核参数优化

注意

修改系统内核参数可能产生内核不稳定，请评估风险后进行操作。

以配置**vm.nr_hugepages**参数为例，操作步骤如下：

1. 在正常实例上，执行以下命令，对数据盘中的/mnt/etc/sysctl.conf文件中的内核参数进行配置优化。

   vim /mnt/etc/sysctl.conf
2. 按**/**键，输入**nr_hugepages**，按回车键搜索定位到该配置项所在的位置。
3. 按**i**键，编辑该配置项，并将该配置项调低至合理的数值，如果未搜索到该配置项则新增如下配置项。

   ```
   vm.nr_hugepages=4
   ```

   该数值需要保证vm.nr_hugepages * hugepagesize < memory_total，具体值请根据实际业务需要进行计算。
4. 修改完成后，按**Esc**键退出编辑模式，并输入**:wq**保存后退出。
5. 执行如下命令，使配置生效。

   sysctl -p

步骤6 恢复异常实例系统盘

通过上述步骤，已经将异常实例系统盘上的配置错误修复完毕，可以将正常实例的ECS数据盘(即原来异常实例的系统盘)卸载，然后再挂载回原异常实例，操作步骤如下：

1. 正常实例卸载数据盘(即原异常实例的系统盘)，具体操作请参见**卸载数据盘**。

2. 将原异常实例的系统盘作为系统盘挂载回原异常实例。

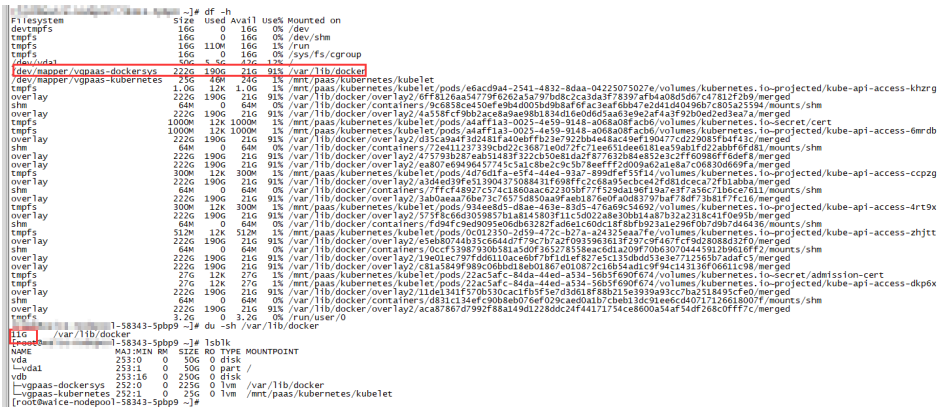
----结束

3.20 为什么 Linux 云服务器 df 和 du 统计磁盘空间的大小不一致?

问题描述

Linux云服务器执行df和du命令查看磁盘使用空间的大小不一致。

如下图所示，使用**df -h**命令查看磁盘使用空间，比**du -sh**命令统计得到的要大。



可能原因

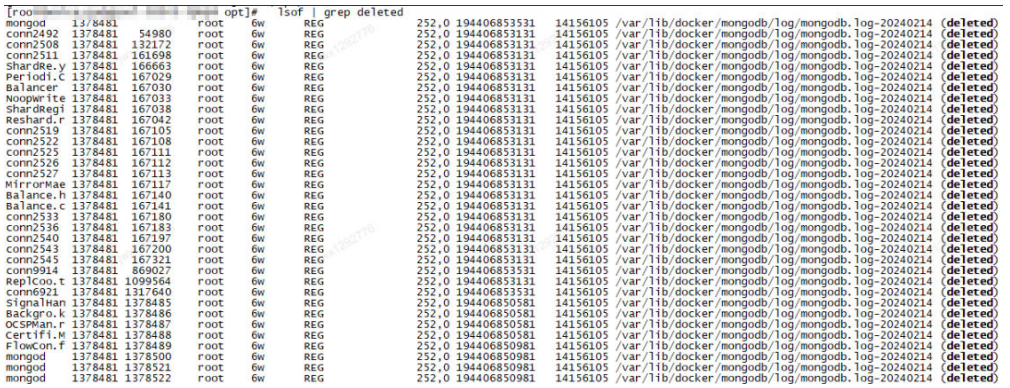
一般来说不会出现删除文件后空间不释放的情况，但是也存在例外，比如文件进程锁定，或者有进程一直在向这个文件写数据。

Linux系统中的一个文件在文件系统中存放分为两个部分：数据部分和指针部分，指针位于文件系统的meta-data中，在将数据删除后，这个指针就从meta-data中清除了，而数据部分存储在磁盘中。在将数据对应的指针从meta-data中清除后，文件数据部分占用的空间就可以被覆盖并写入新的内容，之所以出现删除文件后，空间还没有释放，就是因为进程还在一直向这个文件写入内容，导致虽然删除了文件，但是由于进程锁定，文件对应的指针部分并未从meta-data中清除，而由于指针并未删除，系统内核就认为文件并未被删除，因此通过df命令查询空间并未释放。

当一个文件被删除后，在文件系统目录中已经不可见了，所以du就不会再统计它了。然而如果此时还有运行的进程持有这个已经被删除了的文件的句柄，那么这个文件就不会真正在磁盘中被删除，分区超级块中的信息也就不会更改。这样df仍旧会统计这个被删除了的文件。

处理方法

1. 执行以下命令，切换到/opt目录。
   cd /opt
2. 执行以下命令，查看所有已被删除但还被进程占用的文件。
   lsof | grep deleted



```
[roo                    opt]#   lsof | grep deleted
mongod    13/8481           root    6w      REG              252,0 194406853531   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
conn2492  1378481   54980   root    6w      REG              252,0 194406853131   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
conn2508  1378481  132172   root    6w      REG              252,0 194406853131   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
conn2511  1378481  161698   root    6w      REG              252,0 194406853131   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
ShardRe.y 1378481  166663   root    6w      REG              252,0 194406853131   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
Periodi.C 1378481  167029   root    6w      REG              252,0 194406853131   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
Balancer  1378481  167030   root    6w      REG              252,0 194406853131   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
NoopWrite 1378481  167033   root    6w      REG              252,0 194406853131   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
ShardRegi 1378481  167038   root    6w      REG              252,0 194406853131   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
Reshard.r 1378481  167042   root    6w      REG              252,0 194406853131   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
conn2519  1378481  167105   root    6w      REG              252,0 194406853131   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
conn2522  1378481  167108   root    6w      REG              252,0 194406853131   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
conn2525  1378481  167111   root    6w      REG              252,0 194406853131   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
conn2526  1378481  167112   root    6w      REG              252,0 194406853131   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
conn2527  1378481  167113   root    6w      REG              252,0 194406853131   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
MirrorMae 1378481  167117   root    6w      REG              252,0 194406853131   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
Balance.h 1378481  167140   root    6w      REG              252,0 194406853131   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
Balance.c 1378481  167141   root    6w      REG              252,0 194406853131   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
conn2533  1378481  167180   root    6w      REG              252,0 194406853131   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
conn2536  1378481  167183   root    6w      REG              252,0 194406853131   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
conn2540  1378481  167197   root    6w      REG              252,0 194406853131   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
conn2543  1378481  167200   root    6w      REG              252,0 194406853131   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
conn2545  1378481  167321   root    6w      REG              252,0 194406853131   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
conn9914  1378481  869027   root    6w      REG              252,0 194406853531   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
ReplCoo.t 1378481 1099564   root    6w      REG              252,0 194406853131   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
conn6921  1378481 1317640   root    6w      REG              252,0 194406853531   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
SignalHan 1378481 1378485   root    6w      REG              252,0 194406850581   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
Backgro.k 1378481 1378486   root    6w      REG              252,0 194406850581   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
OCSPMan.r 1378481 1378487   root    6w      REG              252,0 194406850581   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
certifi.M 1378481 1378488   root    6w      REG              252,0 194406850581   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
FlowCon.f 1378481 1378489   root    6w      REG              252,0 194406850981   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
mongod    1378481 1378500   root    6w      REG              252,0 194406850981   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
mongod    1378481 1378521   root    6w      REG              252,0 194406850981   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
mongod    1378481 1378522   root    6w      REG              252,0 194406850981   14156105 /var/lib/docker/mongodb/log/mongodb.log-20240214 (deleted)
```

从回显结果可以看出，/var/lib/docker/mongdb/log/mongdb占用190G，“deleted”状态说明这个日志文件已经被删除，但是由于进程还在一直向此文件写入数据，因此空间并未释放。

3. 执行以下命令，清除文件。

   echo >“/var/log/docker/mongdb/log/mongdb”

   通过这种方法，磁盘空间不但可以马上释放，也可以保证进程继续向文件写入日志。

3.21 NetworkManager 服务无法启动，报错：Failed to restart NetworkManager.service: Unit NetworkManager.service is masked

问题描述

NetworkManager启动时报错：Failed to restart NetworkManager.service: Unit NetworkManager.service is masked。

可能原因

服务单元被禁用，导致NetworkManager服务无法启动。

处理方法

执行以下命令，解除服务单元mask状态。

systemctl unmask NetworkManager

3.22 修改弹性云服务器的时间后，为什么 IP 地址丢失了?

问题描述

修改弹性云服务器的时间后，IP地址丢失。

可能原因

由于时间修改跨度超过您的DHCP租约时间导致的。

当前华为云新创建的VPC子网默认DHCP租约为365天（较早创建的VPC子网DHCP租约为24小时），如果您手动修改弹性云服务器的系统时间，且修改后的系统时间距离当前时间的跨度超过24小时，则可能导致DHCP续租失败，从而使得IP地址丢失。

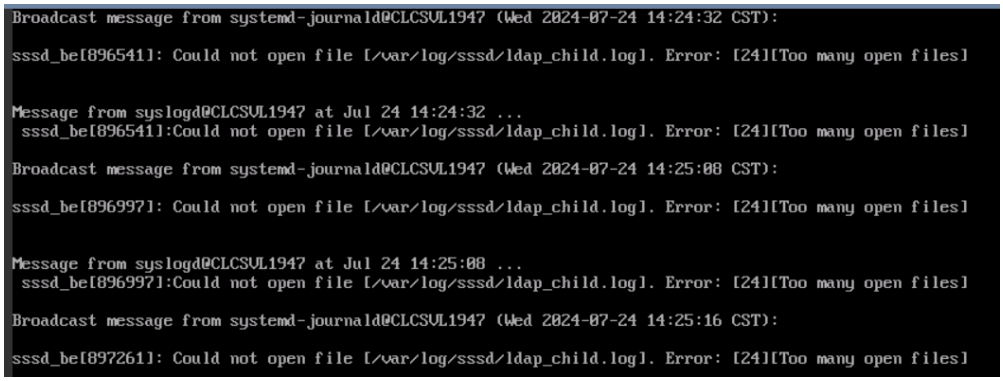
处理方法

如果必须要进行大跨度的时间更改的话，在修改时间之前请先把弹性云服务器的IP地址获取方式修改为静态配置。

3.23 如何解决 ECS 日志中出现 Too many open files 的错误?

问题描述

Linux操作系统的ECS日志中出现“Too many open files”的错误。



可能原因

too many open files（打开的文件过多），表示程序打开的文件句柄数过多，超过了某一资源的限制。一般来说这个资源的限制包含两种维度的限制，包含系统的整体限制和用户单独的限制。出现该问题时需要判断具体超出了哪一维度的限制，再对该限制参数进行调整。

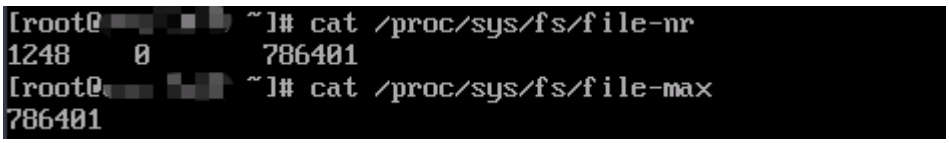
处理方法一：系统范围设置

1. 以root用户登录云服务器。
2. 执行以下命令，查看操作系统中当前打开的所有文件数和最大打开文件数设置（部分版本默认为366954）。

   cat /proc/sys/fs/file-nr

   cat /proc/sys/fs/file-max

   回显输出的第一列表示当前系统中所有打开的文件数。

3. 执行以下命令，更改系统范围的最大打开文件数。

   vim /etc/sysctl.conf

4. 按**i**键进入编辑模式。
5. 在文件末尾添加如下内容，具体的数值可以根据实际情况修改。
   ```
   fs.file-max = 495000
   ```
6. 按**ESC**键退出，并输入**:wq**保存配置。
7. 执行以下命令，使修改生效。
   sysctl -p

处理方法二：用户层面设置

1. 以root用户登录云服务器。
2. 执行以下命令，检查当前打开文件数的限制。
   ulimit -n
3. 执行以下命令，增加数量限制。
   ulimit -n <new_limit>
   该方法修改的参数值仅在当前运行中生效，重启后会还原为默认值，一般用于临时性验证。如需永久生效，请继续执行步骤**4**~**8**。
4. 执行以下命令，编辑/etc/security/limits.conf文件，增加打开文件的数量限制。
   vim /etc/security/limits.conf
5. 按**i**键进入编辑模式。
6. 在文件末尾添加如下内容，此处以655350为例，可根据具体情况修改数值。
   - 只针对特定用户
     ```
     user - nofile 655350
     ```
   - 所有用户
     ```
     * - nofile 655350
     ```
7. 按**ESC**键退出，并输入**:wq**保存配置。
8. 执行以下命令，重启服务器，使修改永久生效。
   reboot

⚠ 注意

Linux操作系统云服务器中的限制资源使用的模块首先读取**/etc/security/limits.conf**，然后读取每个匹配的文件**/etc/security/limits.d/*.conf**，您在 **/etc/security/limits.conf** 中所做的任何更改可能会被后续文件覆盖。若重启后修改未生效请参见**修改/etc/security/limits.conf文件，重启后不生效怎么办?**处理。

3.24 以非 root 用户执行程序，控制台报错：打开日志文件失败

问题背景

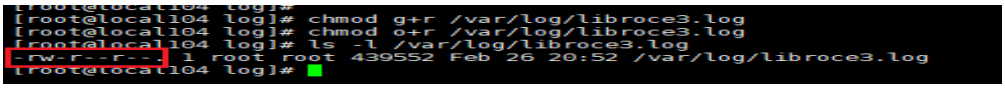
一般情况下，用户程序的日志文件保存在/var/log文件夹下，该文件夹的所有者为root，且只有文件夹所有者才能对目录进行写操作。如果出现控制台打印打开日志文件失败，一般是该用户对/var/log文件夹以及相应的日志文件没有写权限导致的，可以通过如下方式解决该问题。

处理方法

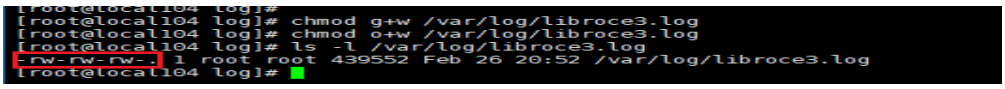
1. 执行“**su**”命令切换到**root**用户。

2. 执行“**chmod g+w /var/log**”和“**chmod o+w /var/log**”命令为文件夹添加所属组和其他用户的写权限。

3. 执行“**chmod g+r /var/log/***日志文件名*”和“**chmod o+r /var/log/***日志文件名*”命令为日志文件添加所属组和其他用户的读权限。



4. 执行“**chmod g+w /var/log/**日志文件名”和“**chmod o+w /var/log/***日志文件名*”命令为日志文件添加所属组和其他用户的写权限。



5. 执行**exit**退出**root**用户。

3.25 如何解决 Linux ECS 整机带宽性能下降的问题?

问题描述

采用Linux操作系统的ECS，其内网带宽性能下降，无法达到规格QoS中的最大带宽PPS。

可能原因

该ECS的操作系统采用Linux3.10内核版本。Linux3.10内核virtio-net驱动rq的rx buf没有实现内存复用，收包流程每个description指向的rx buf都需要申请释放，导致CPU一直处于申请释放内存，占用100%。

在进行TCP多流双向带宽时，性能差，影响多流性能带宽，导致ECS整机宽带PPS能力下降。

处理方法

合入补丁：**index : kernel/git/torvalds/linux.git**。

3.26 如何处理 Linux 实例中的 OOM 问题?

背景信息

OOM（Out of Memory）指系统内存已用完，在Linux系统中，如果内存用完会导致系统无法正常工作，触发系统panic或者OOM Killer。OOM Killer是Linux内核的一个机制，该机制会监控那些占用内存过大的进程，尤其是短时间内消耗大量内存的进程，在系统的内存即将不够用时结束这些进程从而保障系统的整体可用性。

问题现象

ECS实例在运行过程中日志中有类似于如下所示信息：

```
[  327.199955] 5202 total pagecache pages
[  327.200965] 0 pages in swap cache
[  327.201950] Swap cache stats: add 0, delete 0, find 0/0
[  327.203656] Free swap  = 0kB
[  327.204580] Total swap = 0kB
[  327.205491] 2096926 pages RAM
[  327.206375] 0 pages HighMem/MovableOnly
[  327.207509] 94837 pages reserved
[  327.208746] [ pid ]   uid  tgid total_vm      rss nr_ptes swapents oom_score_adj name
[  327.210727] [  352]     0   352     9764      616      22        0             0 systemd-journal
[  327.212897] [  372]     0   372    11370      150      23        0         -1000 systemd-udevd
[  327.214662] [  410]     0   410    13883      102      27        0         -1000 auditd
[  327.216276] [  498]    81   498    14558      164      33        0          -900 dbus-daemon
[  327.217880] [  499]     0   499     5385       62      16        0             0 irqbalance
[  327.219369] [  500]   999   500   153060     1350      63        0             0 polkitd
[  327.221158] [  502]     0   502   243884     3537      36        0             0 uniagent
[  327.222916] [  503]     0   503   137033     1033      84        0             0 NetworkManager
[  327.225002] [  505]     0   505     6596       77      19        0             0 systemd-logind
[  327.226841] [  508]   998   508    29452      105      30        0             0 chronyd
[  327.228427] [  529]     0   529    26123      488      21        0             0 uniagentd
[  327.230120] [  532]     0   532   143572     2883      96        0             0 tuned
[  327.231779] [  563]     0   563    25753      514      51        0             0 dhclient
[  327.233396] [  608]     0   608    54632      688      42        0             0 rsyslogd
[  327.235004] [  839]     0   839    39781      400      42        0             0 hostwatch
[  327.236505] [  904]     0   904   335577     1654     112        0             0 [kworker/0:0H]
[  327.237967] [ 1059]     0  1059    22452      253      45        0             0 master
[  327.239371] [ 1074]    89  1074    22478      250      44        0             0 pickup
[  327.240758] [ 1075]    89  1075    22495      252      45        0             0 qmgr
[  327.242087] [ 1416]     0  1416    28251      259      57        0         -1000 sshd
[  327.243474] [ 1418]     0  1418     6477       51      18        0             0 atd
[  327.244773] [ 1420]     0  1420    31597      152      18        0             0 crond
[  327.246133] [ 1422]     0  1422    24842      166      51        0             0 login
[  327.247893] [ 1423]     0  1423    27552       32      10        0             0 agetty
[  327.249319] [ 2359]     0  2359   197550     4903      48        0             0 containerserver
[  327.250828] [ 7726]     0  7726    63736      535      22        0             0 uniagentd
[  327.252278] [ 7727]     0  7727    98075      305      26        0             0 uniagentd
[  327.253688] [ 7773]     0  7773    28886      101      13        0             0 bash
[  327.254906] [ 7840]     0  7840   225333     3183      34        0             0 telescope
[  327.256240] [ 7922]     0  7922    39390      374      83        0             0 sshd
[  327.257496] [ 7924]     0  7924    28887      102      13        0             0 bash
[  327.258769] [ 7943]     0  7943    18088      190      39        0             0 sftp-server
[  327.260041] [ 8076]     0  8076  1958387  1904796    3739        0             0 python3
[  327.261301] Out of memory: Kill process 8076 (python3) score 924 or sacrifice child
[  327.262504] Killed process 8076 (python3), UID 0, total-vm:7833548kB, anon-rss:7619112kB, file-rss:72kB, shmem-rss:0kB
```

可能原因

如果您在Linux实例上运行程序时，频繁发生OOM，可能是以下原因。

- Linux实例的配置过低，无法满足程序运行所需的内存资源，引发OOM。
- 应用程序代码对内存的使用不当，引发OOM。

处理方法

关于OOM的问题，请参考以下步骤进行处理：

1. 执行以下命令，查看OOM相关日志。

   ```
   sudo less /var/log/messages    # CentOS
   sudo less /var/log/syslog      # Ubuntu
   ```


在日志中通过oom或者kill作为关键字进行搜索，以查看OOM问题的相关日志信息。

日志中会存在OOM Killer评估进程时的标准输出标题行如下图，其中可通过对rss列（单位4KB）进行排序，查看内存消耗最大的进程。

```
[  327.208746] [ pid ]   uid  tgid total_vm      rss nr_ptes swapents oom_score_adj name
[  327.210727] [  352]     0   352     9764      616      22        0             0 systemd-journal
[  327.212897] [  372]     0   372    11370      150      23        0         -1000 systemd-udevd
[  327.214662] [  410]     0   410    13883      102      27        0         -1000 auditd
[  327.216276] [  498]    81   498    14558      164      33        0          -900 dbus-daemon
[  327.217880] [  499]     0   499     5385       62      16        0             0 irqbalance
[  327.219369] [  500]   999   500   153060     1350      63        0             0 polkitd
```

如果是业务进程占用的内存高导致的内存OOM，建议您可以进一步通过业务应用日志定位内存占用高的原因。

2. 根据您排查的结果，可以选择对应的处理方案。

问题原因	处理建议
Linux实例的配置过低，无法满足程序运行所需的内存资源。	升级实例内存配置：**变更ECS规格**。 **注意** 更改实例规格的过程中，您需要停止并重新启动ECS实例，建议您在非业务高峰期时执行该操作，减少对您业务造成的影响。
应用程序代码对内存的使用不当。	优化应用程序代码，如对批量查询请求进行分页等。

参考信息

1. OOM Killer评估进程时的标准输出标题行，各列具体详解如**表1 OOM Killer评估进程时的标准输出标题行**所示。

表 3-4 OOM Killer 评估进程时的标准输出标题行

列名	全称	含义解释
pid	Process ID	进程的操作系统内部ID。
uid	User ID	启动该进程的用户ID。0代表root用户。
tgid	Thread Group ID	线程组ID。 • 对于单线程进程，这与pid相同。 • 对于多线程程序，所有线程共享同一个tgid。

列名	全称	含义解释
total_vm	Total Virtual Memory	进程占用的总虚拟内存大小（以4KB的页为单位）。这个值很大，因为它包括共享库、映射的文件等，不是衡量内存压力的最佳指标。
rss	Resident Set Size	驻留集大小（以4KB的页为单位）。这是进程当前在物理内存中占用的、非交换的内存总量。这是 OOM Killer 最重要的考量因素之一，它直接反映了进程对物理内存的消耗。
nr_ptes	Number of Page Table Entries	页表项数目。进程使用的虚拟内存越多，需要的页表项就越多。这项本身也消耗内存，所以也是 OOM 评分的一个因素。
swapents	Swap Entries	被换出到交换分区（Swap）的内存大小（以4KB的页为单位）。值越高，说明该进程的一些内存当前不在物理RAM中。
oom_score_adj	OOM Score Adjust	OOM调整值（范围从-1000到1000）。这是用户态可以设置的最重要的参数，用于主动影响 OOM Killer的决策。
name	Process Name	进程的可执行文件名称。

2. OOM相关参数如**表2 OOM相关参数表**所示。

表 3-5 OOM 相关参数表

参数名称	参数说明	取值	修改方式
panic_on_oom	panic_on_oom参数是控制系统遇到OOM时如何反应的。当系统遇到OOM的时候，通常会有两种选择： • 触发系统panic，可能会出现频繁宕机的情况。 • 选择一个或者几个进程，触发OOM Killer，结束选中的进程，释放内存，让系统保持整体可用。	可以通过以下命令查看参数取值： **cat /proc/sys/vm/panic_on_oom**或者 **sysctl -a | grep panic_on_oom** • 值为0：内存不足时，触发OOM Killer。 • 值为1：内存不足时，根据具体情况可能发生kernel panic，也可能触发OOM Killer。 • 值为2：内存不足时，强制触发系统panic，导致系统重启。	例如：将参数设置为0，可用以下两种方式： • 临时配置，立即生效，但重启后恢复成默认值。 **sysctl -w vm.panic_on_oom=0** • 持久化配置，系统重启仍生效。 执行命令**vim /etc/sysctl.conf**，在该文件中添加一行**vm.panic_on_oom =0**，再执行命令**sysctl –p**或重启系统后生效。

参数名称	参数说明	取值	修改方式
oom_kill_allocating_task	当系统选择触发OOM Killer，试图结束某些进程时，oom_kill_allocating_task参数会控制选择哪些进程，有以下两种选择： ● 触发OOM的进程。 ● oom_score得分最高的进程。	可以通过以下命令查看参数取值： **cat /proc/sys/vm/oom_kill_allocating_task**或者**sysctl -a | grep oom_kill_allocating_task** ● 值为0：选择oom_score得分最高的进程。 ● 值为非0：选择触发OOM的进程。	例如：将该参数设置成1，可用以下两种方式： ● 临时配置，立即生效，但重启后恢复成默认值。**sysctl -w vm.oom_kill_allocating_task=1** ● 持久化配置，系统重启仍生效。执行命令**vim /etc/sysctl.conf**，在该文件中添加一行**vm.oom_kill_allocating_task=1**，再执行命令**sysctl –p**或重启系统后生效。
oom_score	指进程的得分，主要有两部分组成： ● 系统打分，主要是根据该进程的内存使用情况由系统自动计算。 ● 用户打分，也就是oom_score_adj，可以自定义。	可以通过调整oom_score_adj的值进而调整一个进程最终的得分。通过以下命令查看参数取值： **cat /proc/*进程id*/oom_score_adj** ● 值为0：不调整oom_score。 ● 值为负值：在实际打分值上减去一个折扣。 ● 值为正值：增加该进程的oom_score。	例如：将进程id为2939的进程oom_score_adj参数值设置为1000，可用以下命令： **echo 1000 > /proc/2939/oom_score_adj**

参数名称	参数说明	取值	修改方式
oom_dump_tasks	oom_dump_tasks参数控制OOM发生时是否记录系统的进程信息和OOM Killer信息。 例如dump系统中所有的用户空间进程关于内存方面的一些信息，包括：进程标识信息、该进程使用的内存信息、该进程的页表信息等，这些信息有助于了解出现OOM的原因。	可以通过以下命令查看参数取值： **cat /proc/sys/vm/oom_dump_tasks**或者**sysctl -a | grep oom_dump_tasks** ● 值为0：OOM发生时不会打印相关信息。 ● 值为非0：以下三种情况会调用dump_tasks打印系统中所有task的内存状况。 – 由于OOM导致kernel panic。 – 没有找到需要结束的进程。 – 找到进程并将其结束的时候。	例如：将该参数设置成0，可用以下两种方式： ● 临时配置，立即生效，但重启后恢复成默认值。 **sysctl –w vm.oom_dump_tasks=0** ● 持久化配置，系统重启仍生效。 执行命令**vim /etc/sysctl.conf**，在该文件中添加一行**vm.oom_dump_tasks=0**，再执行命令**sysctl –p**或重启系统后生效。

3.27 如何处理 Linux 实例中的 page allocation failure 问题?

问题描述

在系统的dmesg日志或者message日志中显示page allocation failure报错，如下图所示。此时系统可能处于网络不通、丢包或者IO异常的异常状态。

```
[39151723.910890] wrapper: page allocation failure: order:0, mode:0x20
[39151723.912006] CPU: 22 PID: 997 Comm: wrapper Kdump: loaded Not tainted 3.10.0-1160.15.2.el7.x86_64 #1
[39151723.913204] Hardware name: OpenStack Foundation OpenStack Nova, BIOS rel-1.10.2-0-g5f4c7b1-20200515_170850-szxrtoscil0000 04/01/2014
[39151723.914919] Call Trace:
[39151723.915459]  <IRQ>  [<ffffffffbab81fba>] dump_stack+0x19/0x1b
[39151723.916343]  [<ffffffffba5c48f0>] warn_alloc_failed+0x110/0x180
[39151723.917216]  [<ffffffffba4d3333>] ? __wake_up+0x13/0x20
[39151723.918009]  [<ffffffffbab7d4d7>] __alloc_pages_slowpath+0x6bb/0x729
[39151723.918925]  [<ffffffffba4e8294>] ? find_busiest_group+0x144/0x990
[39151723.919812]  [<ffffffffba5c8ee6>] __alloc_pages_nodemask+0x436/0x450
[39151723.920707]  [<ffffffffba5c9108>] page_frag_alloc+0x158/0x170
[39151723.921564]  [<ffffffffbaa43fa6>] __netdev_alloc_skb+0xa6/0x110
[39151723.922438]  [<ffffffffc021e1ee>] page_to_skb+0x4e/0x1f0 [virtio_net]
[39151723.923350]  [<ffffffffc0220509>] virtnet_poll+0x2c9/0x750 [virtio_net]
[39151723.924276]  [<ffffffffbaa561cf>] net_rx_action+0x26f/0x390
[39151723.925097]  [<ffffffffba4a4b35>] __do_softirq+0xf5/0x280
[39151723.925911]  [<ffffffffbab984ec>] call_softirq+0x1c/0x30
[39151723.926702]  [<ffffffffba42f715>] do_softirq+0x65/0xa0
[39151723.927483]  [<ffffffffba4a4eb5>] irq_exit+0x105/0x110
[39151723.928265]  [<ffffffffbab99936>] do_IRQ+0x56/0xf0
[39151723.929018]  [<ffffffffbab8b36a>] common_interrupt+0x16a/0x16a
[39151723.929879]  <EOI>  [<ffffffffba51764c>] ? __pv_queued_spin_lock_slowpath+0x23c/0x2e0
[39151723.930943]  [<ffffffffbab7bff5>] queued_spin_lock_slowpath+0xb/0xf
[39151723.931840]  [<ffffffffbab8a700>] _raw_spin_lock+0x20/0x30
[39151723.932655]  [<ffffffffc0167b9d>] mb_cache_shrink_fn+0x3d/0x140 [mbcache]
[39151723.933603]  [<ffffffffba5d192e>] shrink_slab+0xae/0x340
[39151723.934411]  [<ffffffffba642aa1>] ? vmpressure+0x21/0x90
[39151723.935214]  [<ffffffffba5d4cba>] do_try_to_free_pages+0x3ca/0x520
[39151723.936104]  [<ffffffffba5d4f0c>] try_to_free_pages+0xfc/0x180
[39151723.936956]  [<ffffffffbab7d273>] __alloc_pages_slowpath+0x457/0x729
[39151723.937859]  [<ffffffffba5c8ee6>] __alloc_pages_nodemask+0x436/0x450
[39151723.938759]  [<ffffffffba618bb8>] alloc_pages_current+0x98/0x110
[39151723.939628]  [<ffffffffba5bdd37>] __page_cache_alloc+0x97/0xb0
[39151723.940481]  [<ffffffffba5c0cd0>] filemap_fault+0x270/0x420
[39151723.941309]  [<ffffffffc0305756>] ext4_filemap_fault+0x36/0x50 [ext4]
[39151723.942220]  [<ffffffffba5edfba>] __do_fault.isra.61+0x8a/0x100
[39151723.943080]  [<ffffffffba4e6101>] ? put_prev_entity+0x31/0x400
[39151723.943932]  [<ffffffffba5ee56c>] do_read_fault.isra.63+0x4c/0x1b0
[39151723.944817]  [<ffffffffba5f5db0>] handle_mm_fault+0xa20/0xfb0
[39151723.945646]  [<ffffffffba4c9f1d>] ? hrtimer_start_range_ns+0x1fd/0x3c0
[39151723.946563]  [<ffffffffbab8f653>] __do_page_fault+0x213/0x500
```

可能原因

page allocation failure报错表示分配内存页失败。常见的原因有：

- 实例内存使用率高。
- 实例内存使用率不高（低于80%），但是业务IO（网络、存储）压力大，网络消耗的速度快于系统内存的回收速度。

处理方法

问题原因	处理建议
实例内存使用率高。	升级实例内存配置：**变更ECS规格**。 **注意** 更改实例规格的过程中，您需要停止并重新启动ECS实例，建议您在非业务高峰期时执行该操作，减少对您业务造成的影响。

实例内存使用率不高（低于80%），但是业务IO（网络、存储）压力大，网络消耗的速度快于系统内存的回收速度。	需要针对高IO场景进行内存优化：
	建议调优内核参数vm.min_free_kbytes到默认值（一般为67584）的三倍，修改步骤如下：
	1. 执行以下命令，修改内核参数。
	`echo "vm.min_free_kbytes=202752" >> /etc/sysctl.conf`
	2. 执行如下命令，使结果生效。
	`sysctl -p`
	注意
	vm.min_free_kbytes该参数如果配置过大会导致应用能够使用的内存过小，更容易触发OOM的异常，建议该参数配置的值不要超过内存的3%。

4 远程登录

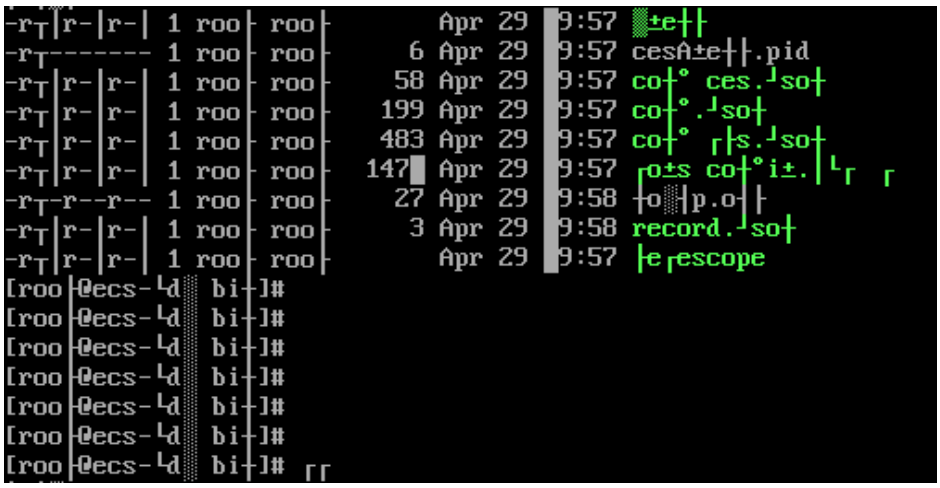
4.1 VNC 登录类

4.1.1 VNC 方式登录弹性云服务器时，登录界面显示乱码怎么办?

问题描述

使用VNC方式登录Linux云服务器，登录界面显示乱码。如图4-1所示。

图 4-1 VNC 登录界面乱码



可能原因

用户使用**cat**命令显示了一个较大二进制文件，导致云服务器登录界面显示乱码。

处理方案

使用root账号登录弹性云服务器，执行以下命令进行恢复操作。

reset

说明

reset命令是用来重新初始化终端，刷新终端屏幕。执行**reset**命令后会将混乱的显示清除掉，恢复正常显示状态。

4.1.2 VNC 方式登录弹性云服务器后，较长时间不操作，界面无响应?

用户的计算机操作系统为Windows7时，如果使用IE10或IE11浏览器通过VNC方式登录弹性云服务器，且较长时间不做任何操作，VNC登录界面会出现无响应的状况，键盘和鼠标无法正常操作。

此时，可以通过单击两次VNC页面上的“AltGr”按钮重新激活页面。

如问题未解决，请联系技术支持。

4.1.3 VNC 方式登录弹性云服务器后，查看数据失败，VNC 无法正常使用?

使用VNC方式登录弹性云服务器后，执行查看数据操作时，例如在Linux操作系统下使用**cat**命令查看大文件、播放视频，由于部分浏览器自身内存占用太大，导致VNC无法正常使用。

此时，请更换其他浏览器后重新登录弹性云服务器。

如问题未解决，请联系技术支持。

4.1.4 VNC 方式登录弹性云服务器时，系统黑屏输入无反应?

这是由于该弹性云服务器已被其他用户使用VNC方式登录。

VNC方式登录弹性云服务器时，同一时刻仅支持一个用户登录。如果多个用户同时登录，先登录的用户会断开连接，出现黑屏现象。

此时，重新进行登录操作可消除黑屏，但会导致其他用户黑屏并断开连接。

4.1.5 通过控制台登录弹性云服务器时提示 1006 或 1000 怎么办?

问题描述

VNC方式远程登录弹性云服务器时，系统报错误码“1006”，如图4-2所示。

图 4-2 VNC 远程登录报错

可能原因

- 弹性云服务器状态异常
- 其他用户正在登录
- 长时间未操作弹性云服务器，系统自动断开

排查方法

1. 再次使用VNC方式登录弹性云服务器，重试登录操作。
   - 登录成功，结束。
   - 登录报错，执行2。
2. 检查弹性云服务器的状态是否正常。

   关机、删除、主机迁移、重启、系统超时的弹性云服务器，都会引起登录报错1006。
3. 确认是否有其他用户正在登录当前弹性云服务器。

   如果有，必须等前一用户退出登录后，后一用户才能登录成功。

4.1.6 VNC 方式登录后，播放音频文件没有声音

问题描述

使用MSTSC方式登录Windows云服务器，可以正常播放音频文件。但是，使用VNC方式登录Windows云服务器时，播放音频文件没有声音。

可能原因

VNC方式不具备音频调用能力。

处理方案

通过本地PC播放Windows弹性云服务器上的音频文件。以Windows 7的本地PC为例，具体操作如下：

1. 打开本地计算机。

   说明

   不是登录Windows弹性云服务器。
2. 通过快捷键“Win+R”，打开“运行”窗口。
3. 输入“mstsc”，并单击“确定”。

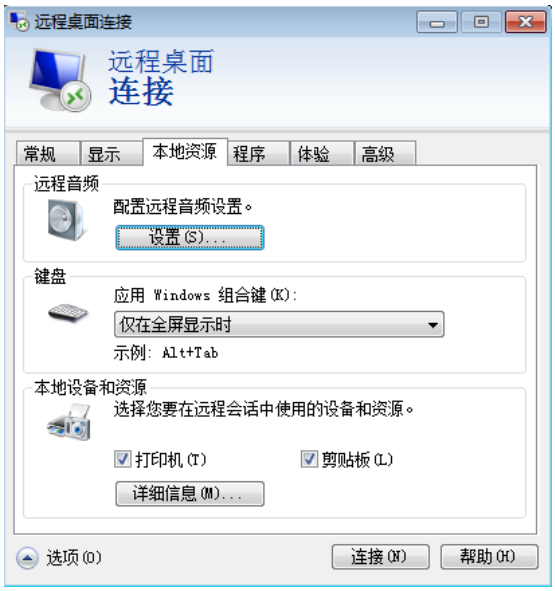
   系统打开“远程桌面连接”窗口。

   图 4-3 远程桌面连接

4. 单击左下角的“选项”，并选择“本地资源”页签。

图 4-4 远程桌面连接-本地资源



5. 在“远程音频”栏，单击“设置”，配置远程音频设置。

图 4-5 远程音频播放设置

6. 在“远程音频播放”栏，选择“在此计算机上播放”。

4.2 Windows 远程登录报错类

4.2.1 远程连接 Windows 云服务器报错：出现身份验证错误，要求的函数不受支持

问题描述

Windows操作系统的本地PC，通过RDP协议（如MSTSC方式）远程桌面连接Windows云服务器报错，报错显示出现身份验证错误，要求的函数不受支持。

- 如果报错信息中仅提示：出现身份验证错误，要求的函数不受支持。请参考**处理方法**解决该问题。

- 如果报错信息中附加提示了由于CredSSP加密Oracle修正导致该错误，如图4-6所示。可能原因是由于微软于2018年3月发布安全补丁，该安全补丁可能会影响RDP连接的CredSSP，导致通过RDP协议访问云服务器时连接失败。解决方法请参考微软官方指导文档“CredSSP updates for CVE-2018-0886”。

  图 4-6 远程桌面连接失败

处理方法

修改Windows云服务器的远程桌面连接设置：将选项“仅允许运行使用网络级别身份验证的远程桌面的计算机连接（更安全）”修改为“允许运行任意版本远程桌面的计算机连接（较不安全）”。具体操作如下：

1. 登录云服务器。
2. 打开左下角的“开始”菜单，右键单击“计算机”，并选择“属性”。
3. 在左侧导航栏，选择“远程设置”。
4. 选择“远程”页签，并在“远程桌面”栏，选择“允许远程连接到此计算机”。

图 4-7 远程设置

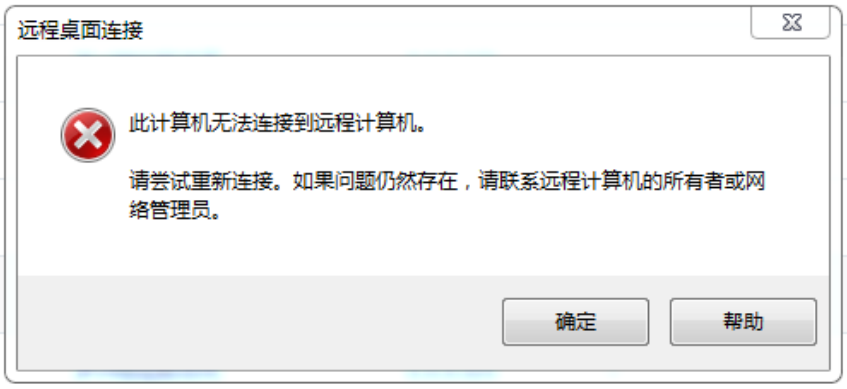
5. 单击“确定”。

4.2.2 远程连接 Windows 云服务器报错：此计算机无法连接到远程计算机

问题描述

使用远程登录方式连接登录Windows云服务器时出现如下错误：此计算机无法连接到远程计算机。

图 4-8 无法连接到远程计算机



可能原因

- 服务端安全组3389端口未开启。**检查云服务器端口配置**
- 服务端防火墙关闭。**检查防火墙配置是否正常**
- 远程桌面连接配置不正确。**检查远程桌面连接设置**
- 未开启“Remote Desktop Services”。**检查Remote Desktop Services**
- 远程桌面会话主机配置不正确。**检查远程桌面会话主机**

检查云服务器端口配置

检查云服务器的3389端口是否能够访问（默认使用3389端口）。

请确保入方向规则中已添加3389端口。

在云服务器的详情页面选择“安全组”页签，查看安全组入方向规则中已添加3389端口。

检查防火墙配置是否正常

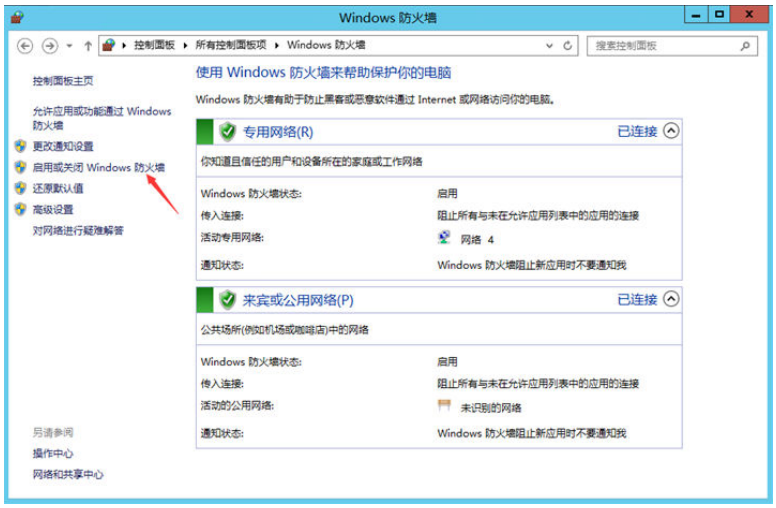
检查云服务器的防火墙是否开启。

1. 在控制台使用VNC方式登录Windows云服务器。
2. 单击桌面左下角的Windows图标，选择“控制面板 > Windows防火墙”。

图 4-9 Windows 防火墙

3. 单击“启用或关闭Windows防火墙”。
   查看并设置防火墙的具体状态：开启或关闭。

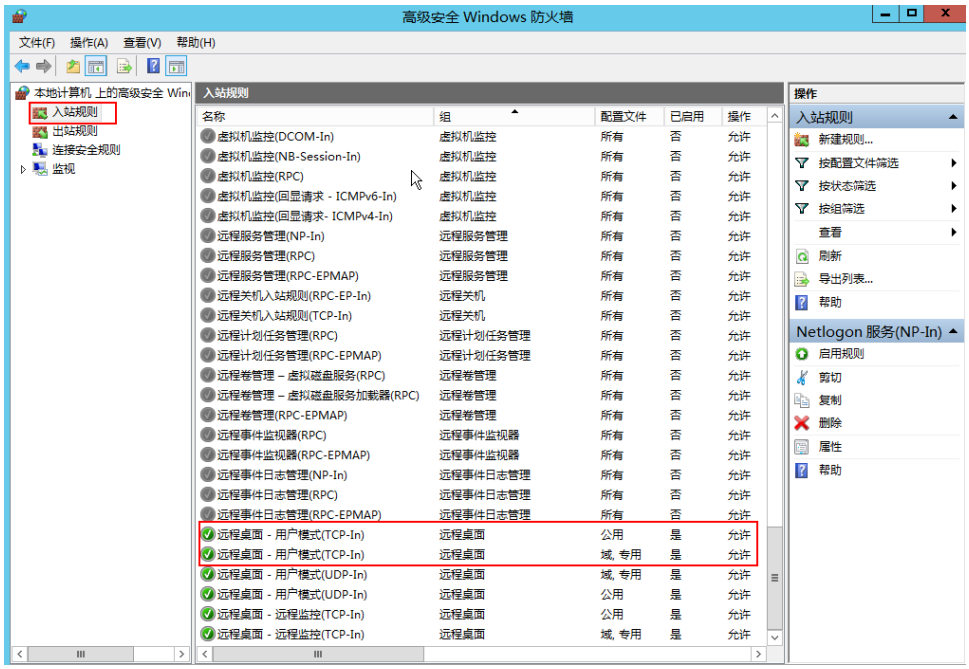
图 4-10 查看防火墙状态



如果选择开启防火墙，请继续执行以下操作步骤。

4. 单击“高级配置”。
5. 检查“入站规则”，请确保已启用如下规则。
   - 远程桌面(TCP-In)　　公用
   - 远程桌面(TCP-In)　　域，专用

图 4-11 入站规则



如果防火墙入站规则中设置的端口与远程服务器设置的端口不一致，远程访问服务器将无法成功。一旦出现这种情况，您也可以添加新的防火墙入站规则端口。

详细操作请参考：**Windows云服务器怎样关闭防火墙、添加例外端口？**。

说明

默认使用的是3389端口，如果您使用的是其他端口，可参考3389端口添加防火墙入站规则。

完成上述操作后，再次重试远程连接云服务器。

检查远程桌面连接设置

修改Windows云服务器的远程桌面连接设置：勾选“允许远程连接到此计算机”。具体操作如下：

1. 登录云服务器。
2. 打开左下角的“开始”菜单，右键单击“计算机”，并选择“属性”。
3. 在左侧导航栏，选择“远程设置”。
4. 选择“远程”页签，并在“远程桌面”栏，选择“允许远程连接到此计算机”。

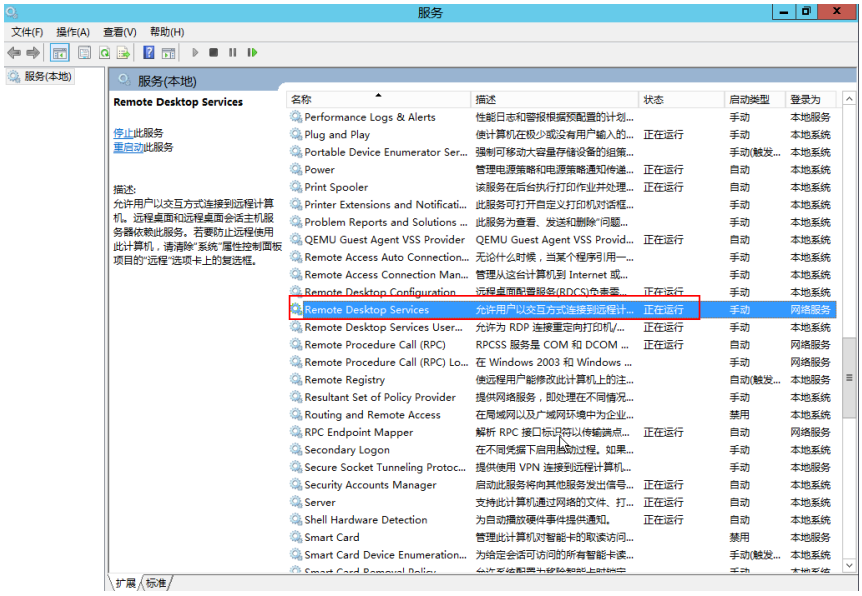
图 4-12 远程设置

5. 单击“确定”。

检查 Remote Desktop Services

1. 打开Windows搜索框，输入services，选择“服务”。
2. 在服务中选择并重启Remote Desktop Services服务，请确保Remote Desktop Services状态为“正在运行”。

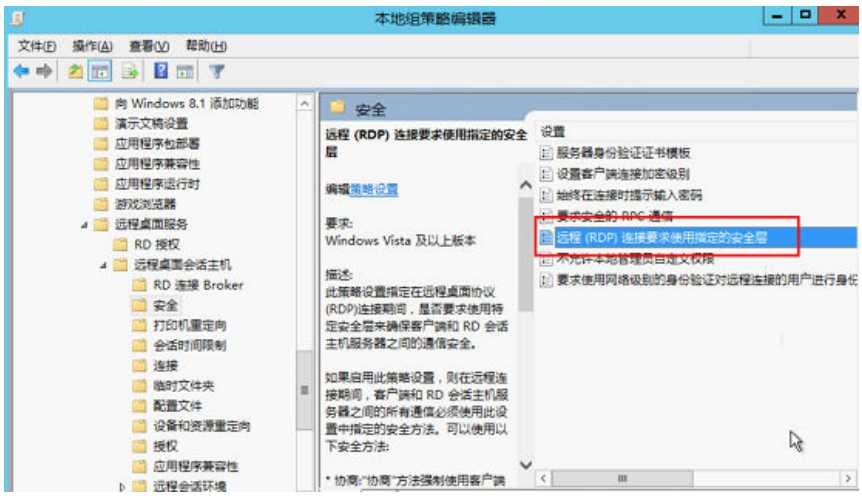
图 4-13 Remote Desktop Services



检查远程桌面会话主机

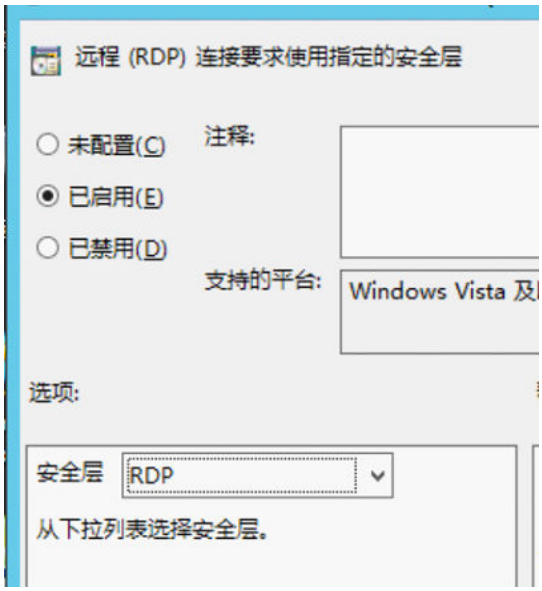
1. 打开cmd运行窗口，并输入“gpedit.msc”。
2. 单击“确定”，打开“本地组策略编辑器”。
3. 选择“计算机配置 > 管理模板 > Windows组件”，查找并双击“远程桌面服务”。
4. 选择“远程桌面会话主机 > 安全 > 远程（RDP）连接要求使用指定的安全层”。

图 4-14 远程（RDP）连接要求使用指定的安全层



5. 选择“已启用”，并将“安全层”设置为“RDP”。

图 4-15 设置安全层为 RDP

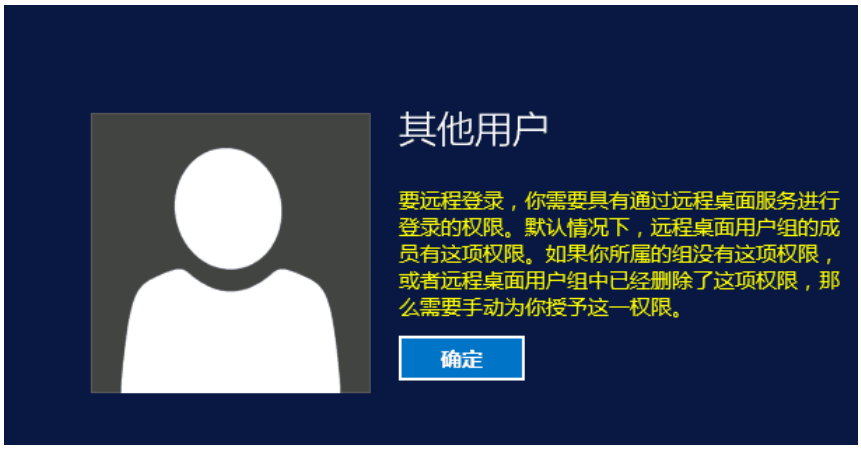


4.2.3 远程连接 Windows 云服务器报错：没有远程登录的权限

问题描述

远程桌面连接时提示需要具有通过远程桌面服务进行登录的权限。

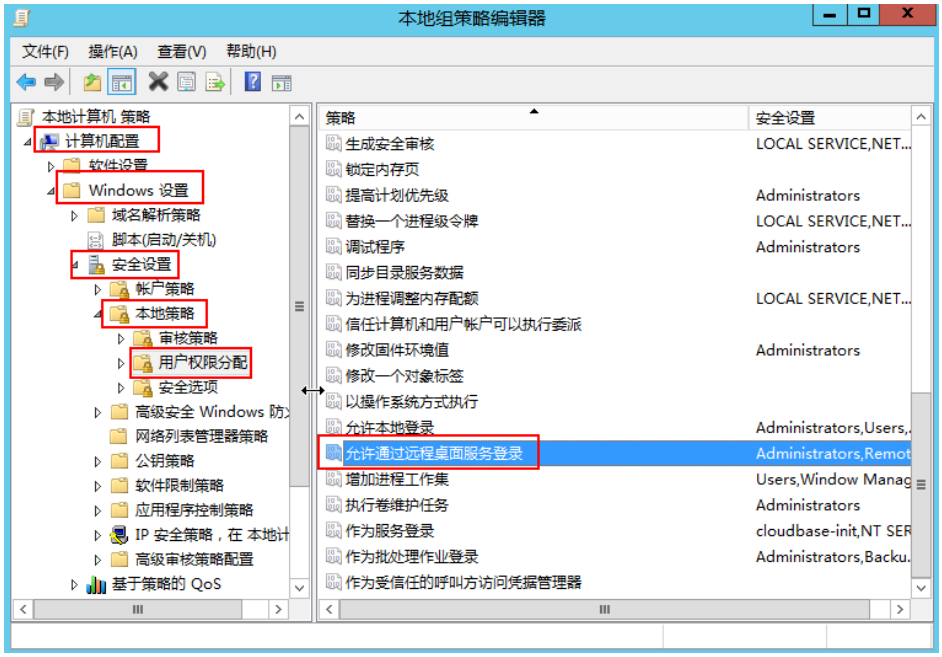
图 4-16 缺失远程登录权限



处理方法

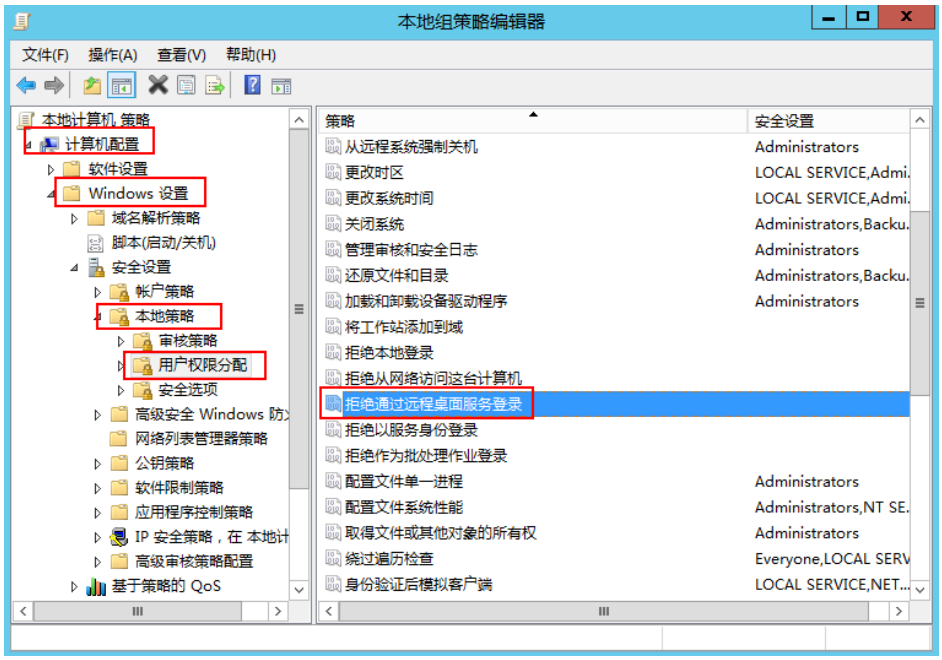
1. 打开cmd运行窗口，并输入“gpedit.msc”。
2. 单击“确定”，打开“本地组策略编辑器”。
3. 选择“计算机配置 > Windows设置 > 安全设置 > 本地策略 > 用户权限分配”。
   a. 查找并双击“允许通过远程桌面服务登录”。确保已添加“Administrators”和“Remote desktop users”。

图 4-17 允许通过远程桌面服务登录



b. 查找并双击“拒绝通过远程桌面服务登录”。如果里面有Administrator账号，请删除。

图 4-18 拒绝通过远程桌面服务登录



4.2.4 远程连接 Windows 云服务器报错：没有远程桌面授权服务器可以提供许可证

问题描述

使用远程登录方式连接登录Windows云服务器时出现如下错误：由于没有远程桌面授权服务器可以提供许可证，远程会话被中断，请跟服务器管理员联系。

图 4-19 没有远程桌面授权服务器可以提供许可证

可能原因

可能原因是由于在系统内部安装了远程桌面会话主机角色。

您可以申请免费使用 120 天，之后需要付费，如未付费会则造成远程连接失败。Windows最多仅允许两个用户连接（包含本地登录用户），若要支持更多连接数量，请安装远程桌面服务角色并取得合法授权数量。 在配置远程桌面会话主机角色后，会同时取消原有默认的2个免费连接授权。所以，在没有正确配置相关授权的时候，会导致远程桌面无法连接，并出现上述错误提示。

处理方法

- 方法一：申请多用户会话授权的license并激活云服务器。请注意申请license的步骤中需要从微软官方购买远程桌面访问许可证。

  请参考**申请多用户会话授权的license并激活云服务器**。
- 方法二：参考本节操作删除“远程桌面会话主机”（2008操作系统）或“远程桌面服务”（2012操作系统）。

  但删除该角色后，服务器最多仅允许两个用户连接（包含本地登录用户）。
- 方法三：重装/切换操作系统后重新配置多用户登录。

  当前云平台已不支持2008操作系统的公共镜像，如果您使用的2008操作系统，可以切换至2012操作系统。

  重装/切换操作系统前请做好系统盘的数据备份。

操作须知

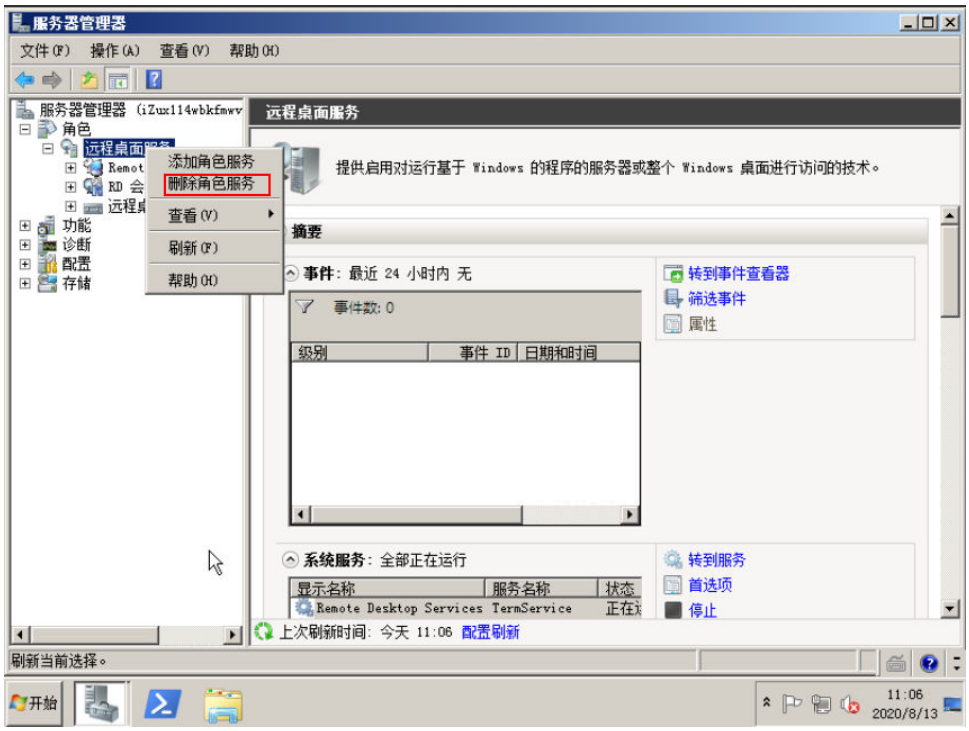
- 本文适用于Windows server 2008/2012操作系统的云服务器。
- 操作过程中需要重启云服务器，可能会造成业务中断，请提前做好数据备份。

Windows 2008 操作系统处理方法

1. 使用控制台提供的VNC连接方式登录到Windows云服务器。

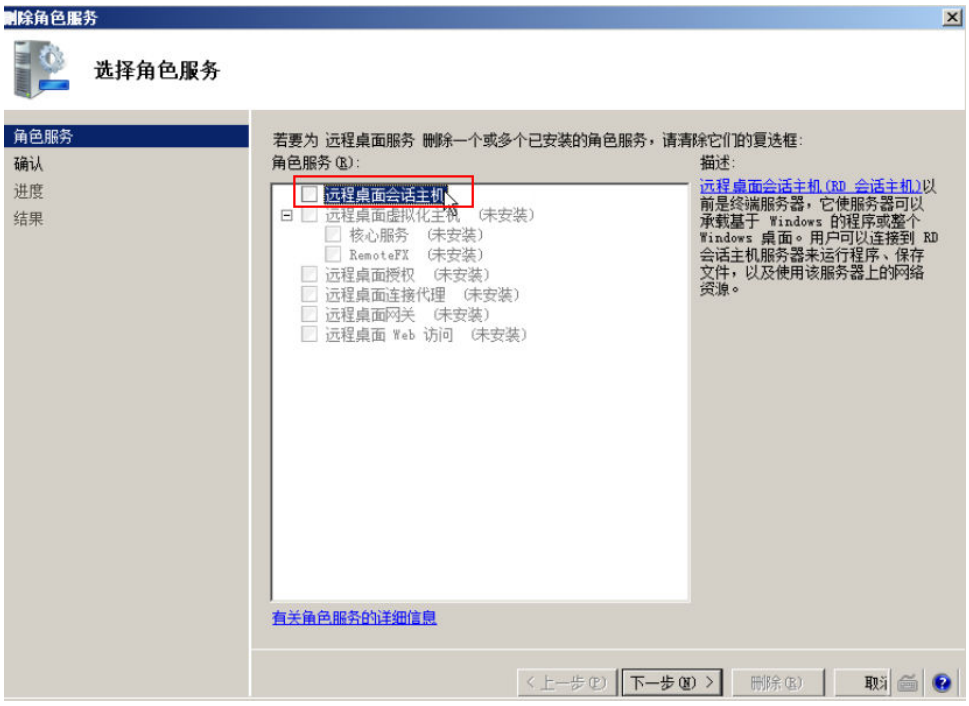
2. 打开“服务器管理器”，依次选择“角色 > 远程桌面服务 ”，右键单击“远程桌面服务”，然后选择“删除角色服务”。

图 4-20 删除角色服务



3. 在弹出窗口中，取消勾选“远程桌面会话主机”，并单击“下一步”直到完成。

图 4-21 取消勾选“远程桌面会话主机”



4. 单击“删除”。

5. 重启云服务器。

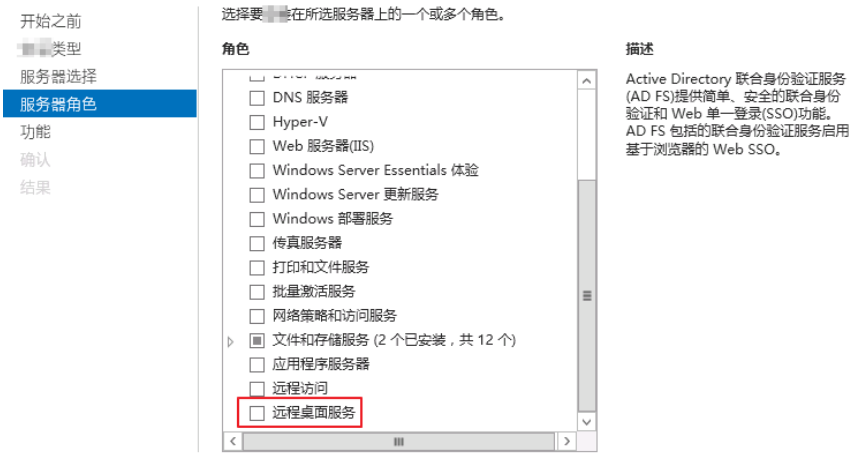
Windows 2012 操作系统处理方法

1. 使用控制台提供的VNC连接方式登录到Windows云服务器。
2. 打开“服务器管理器”，并依次选择“管理 > 删除角色和功能”，单击“下一步 ”。

图 4-22 删除角色和功能

3. 选择目标服务器，单击“下一步”。
4. 取消勾选“远程桌面服务”。

图 4-23 远程桌面服务



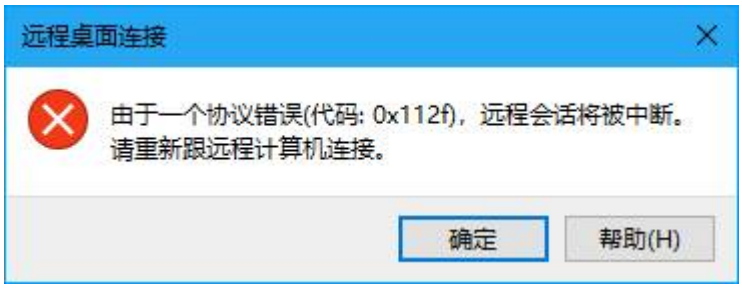
5. 单击“删除”。
6. 重启云服务器。

4.2.5 登录 Windows 云服务器时报错：0x112f

问题描述

登录Windows云服务器时，系统报错，错误代码为“0x112f”，如图4-24所示。

图 4-24 协议错误（代码 0x112f）



可能原因

云服务器内存不足。

处理方法

- 方法一（推荐）：
  变更规格，升级云服务器的CPU、内存大小。变更规格的方法，请参见**变更规格（CPU和内存）**。
- 方法二：
  开启虚拟内存，获取云服务器的空闲内存。
  开启虚拟内存的方法，请参见**怎样配置Windows弹性云服务器的虚拟内存?** 。

  说明

  该方法会导致磁盘I/O性能下降，如非必要，不推荐使用。

4.2.6 远程连接 Windows 云服务器报错：0x1104

问题描述

使用MSTSC方式登录Windows Server 2008操作系统的云服务器，系统报错：检测到一个协议错误（代码 0x1104）。

图 4-25 协议错误（代码 0x1104）

可能原因

- 服务端安全组3389端口未开启。
- 服务端防火墙关闭。
- 服务端3389端口被其他进程占用。
- 远程桌面会话主机配置不正确。

处理方法

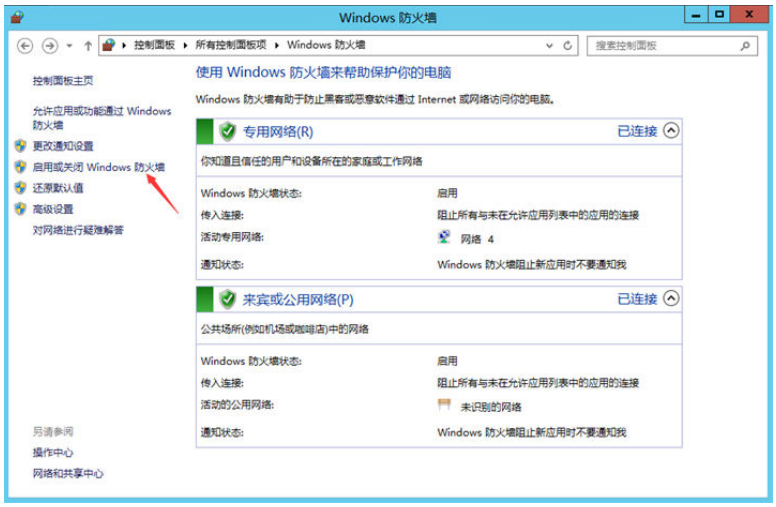
步骤1 检查安全组设置。

检查3389端口入方向是否开启，若已开启，执行**步骤2**。

步骤2 检查防火墙是否关闭。

1. 登录Windows云服务器。
2. 单击桌面左下角的Windows图标，选择“控制面板 > Windows防火墙”。

3. 单击“启用或关闭Windows防火墙”。
   查看并设置防火墙的具体状态：开启或关闭。



如果正常，请执行**步骤3**。

步骤3 使用VNC方式登录云服务器，查看端口信息。

1. 进入cmd命令窗，并执行以下命令。
   netstat -ano |findstr ： 3389

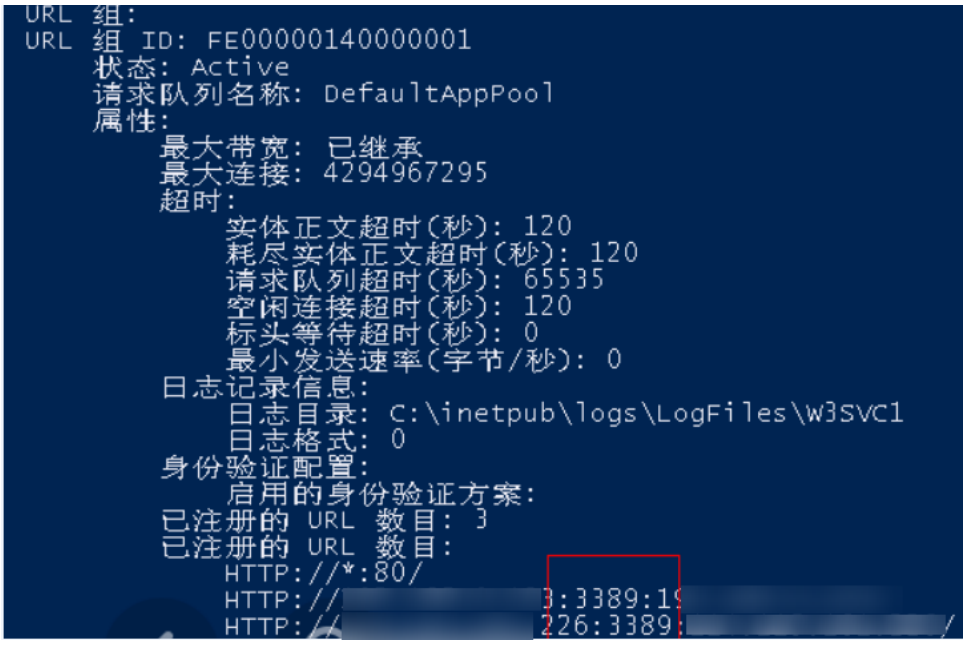
图 4-26 检查 3389 端口

如图4-26所示，3389端口被占用，进程PID为4。

2. 打开任务管理器，查看PID为4的进程为System系统进程。
3. 通常IIS服务和SQL Server会以System进程运行，执行以下HTTP命令进一步查看。

   netsh http show servicestate

图 4-27 查看系统进程



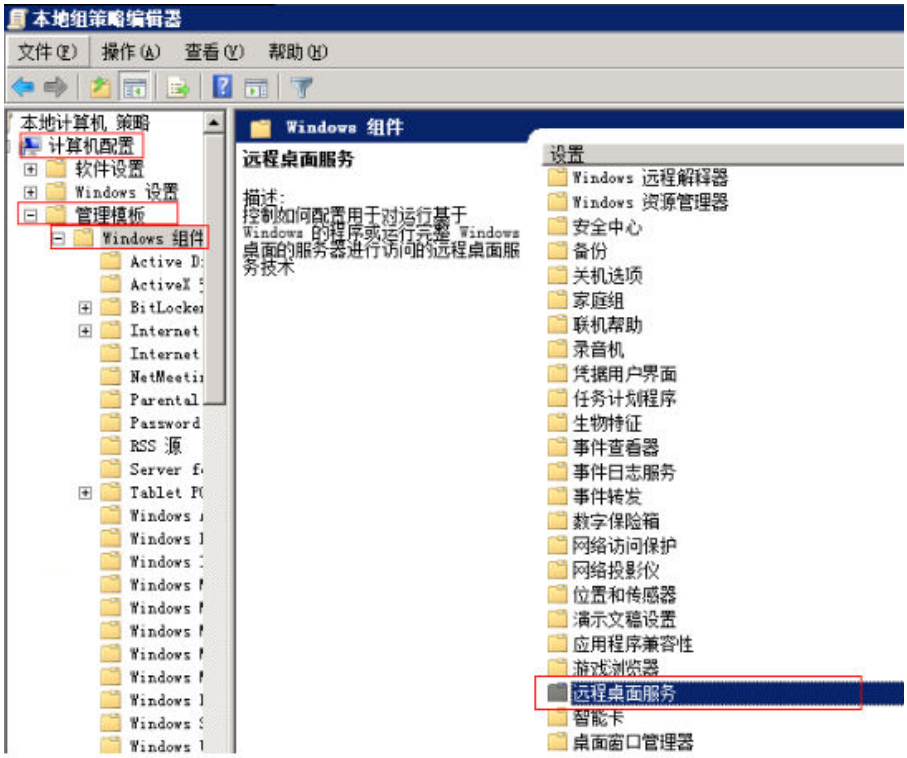
4. 如果可以看到3389端口被HTTP协议使用，可以确定是被IIS服务占用。
5. 在浏览器输入“http://127.0.0.1:3389”进行验证，网站打开正常。
6. 修改IIS使用其他端口，重启IIS服务。

步骤4 如果以上检查均没有问题，请执行步骤5，检查是否由于远程桌面会话主机配置导致。

步骤5 检查远程桌面会话主机配置。

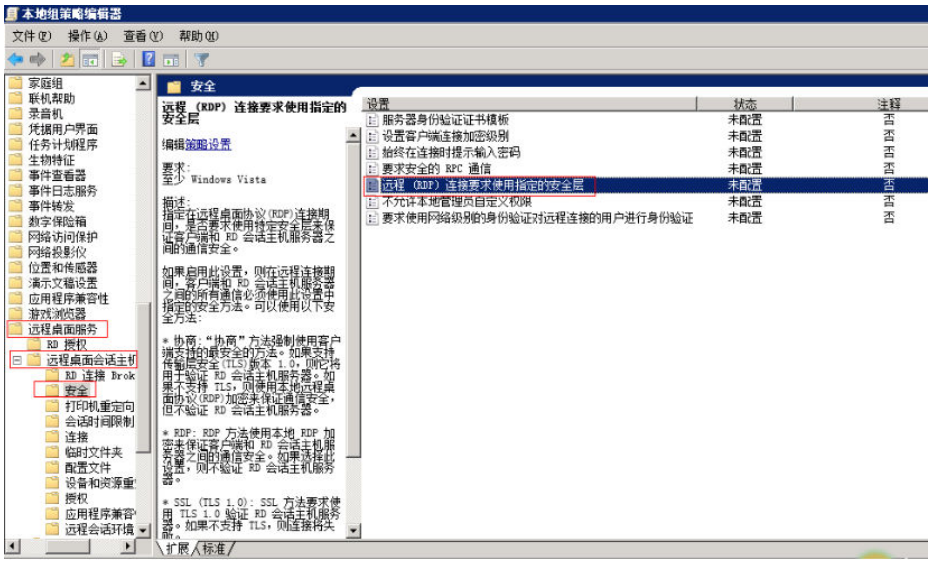
1. 通过VNC登录云服务器。
2. 打开cmd运行窗口，并输入“gpedit.msc”。
3. 单击“确定”，打开“本地组策略编辑器”。
4. 选择“计算机配置 > 管理模板 > Windows组件”，查找并双击“远程桌面服务”。

图 4-28 远程桌面服务



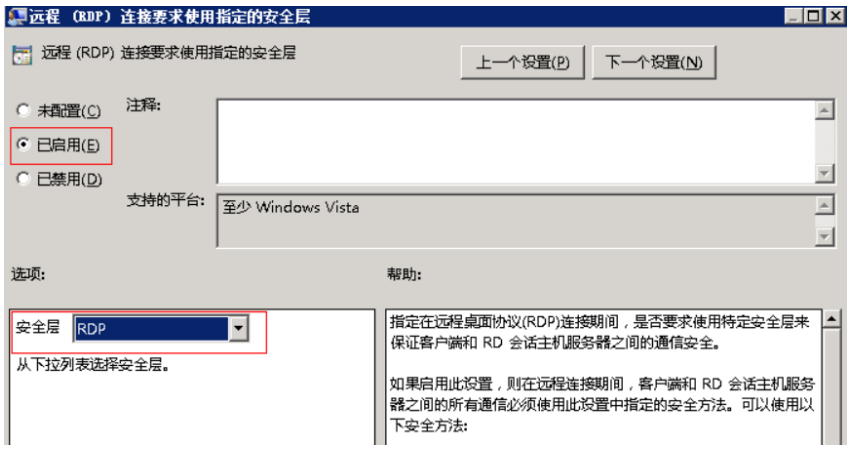
5. 选择“远程桌面会话主机 > 安全 > 远程（RDP）连接要求使用指定的安全层”。

图 4-29 远程（RDP）连接要求使用指定的安全层



6. 选择“已启用”，并将“安全层”设置为“RDP”。

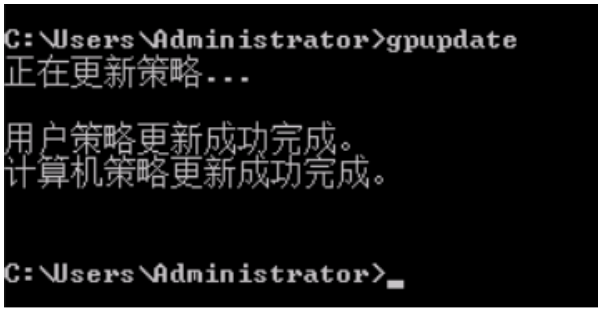
图 4-30 设置安全层



7. 单击“确定”。
8. 配置完成后，打开“cmd”命令窗。
9. 执行以下命令，刷新组策略。

   gpupdate

图 4-31 刷新组策略



----结束

4.2.7 远程连接 Windows 云服务器报错：122.112...

问题描述

本地使用远程桌面连接登录Windows server 2012云服务器，报错：122.112...，服务器频繁掉线，Windows登录进程意外中断。

可能原因

1. 系统资源不足或不可用。
2. 服务启动失败。

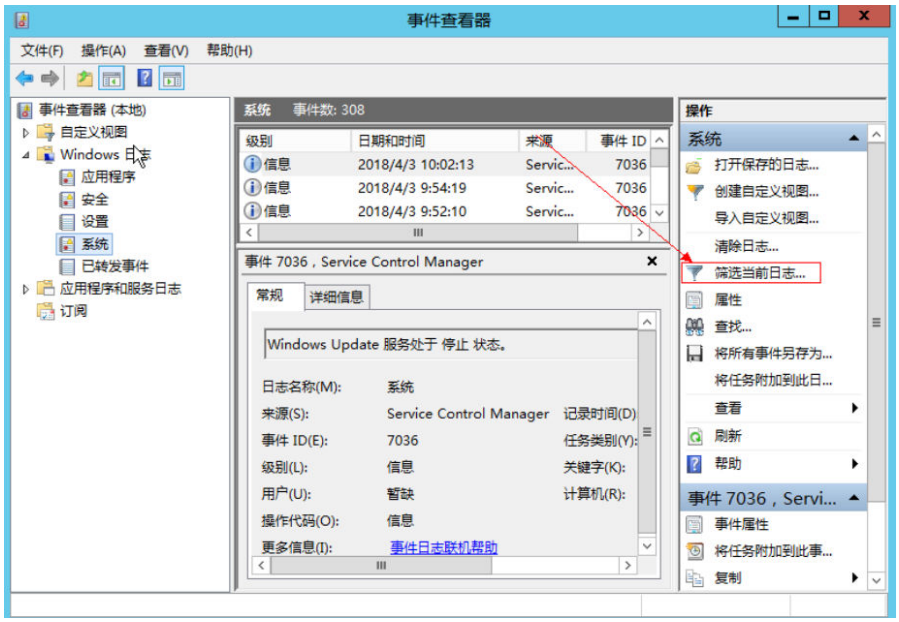
处理方法

步骤1 查看系统日志。

1. 通过VNC方式登录云服务器。

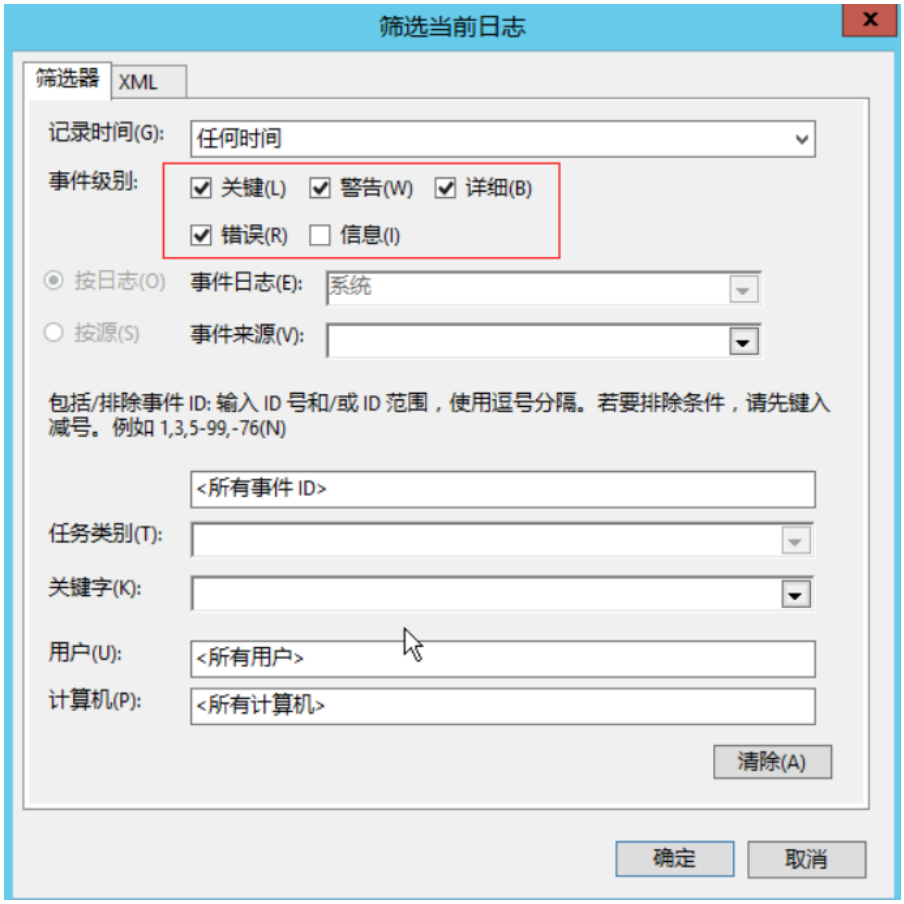
2. 单击  打开服务管理，选择“管理工具 > 事件查看器 > Windows日志 > 系统 > 筛选当前日志”。

图 4-32 事件查看器



3. 在“事件级别”栏，勾选“关键”、“警告”、“详细”、“错误”。

图 4-33 筛选日志



4. 查找登录相关的日志信息。

步骤2 查看主机系统资源使用情况。

1. 选择“开始 > 任务管理器 > 性能”。
2. 查看CPU、内存使用情况。

步骤3 检查购买的Windows云服务器规格是否为1U1GB。

如果是，建议变更规格或者停止不使用的进程。

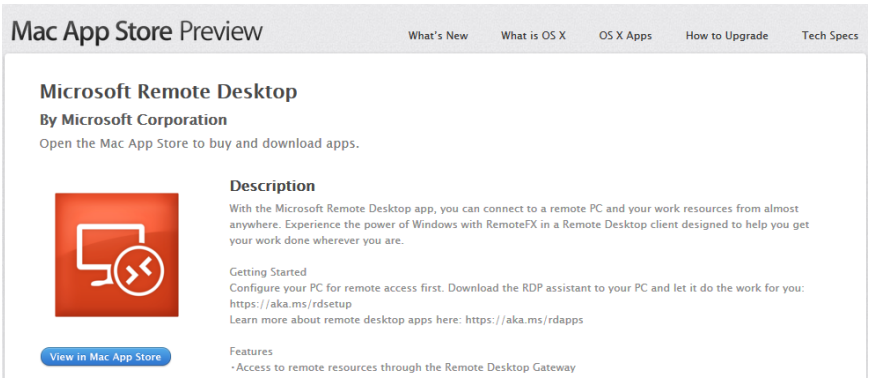
----结束

4.2.8 使用 Mac 远程连接 Windows 云服务器报错：证书或相关链无效

问题描述

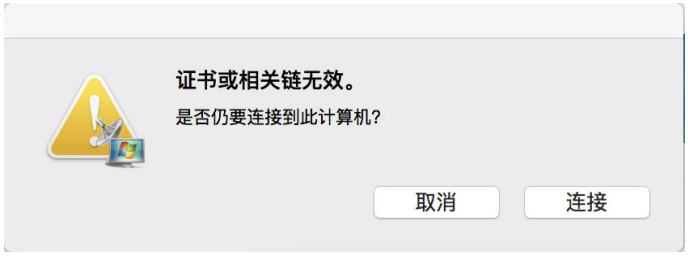
使用Mac版Microsoft Remote Desktop工具，远程连接Windows云服务器。

图 4-34 Mac 版 Microsoft Remote Desktop 工具



由于Mac系统的特殊性，在使用Mac系统远程登录Windows云服务器时，需要在Mac端和Windows云服务器内部执行相关配置，才能远程连接成功。使用Mac远程连接时，出现报错“证书或相关链无效”。

图 4-35 证书或相关链无效



可能原因

云服务器策略组设置的问题。

操作步骤

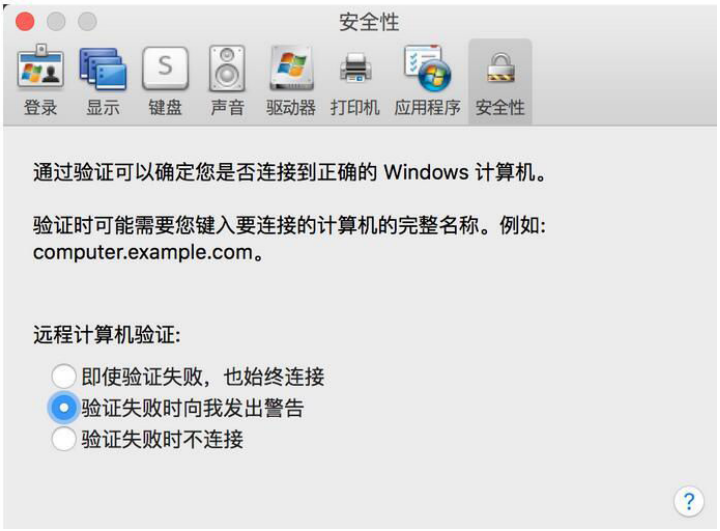
1. 在本地主机左上角的菜单栏选择“RDC > 首选项”打开Microsoft Remote Desktop的偏好设置。

   图 4-36 选择首选项

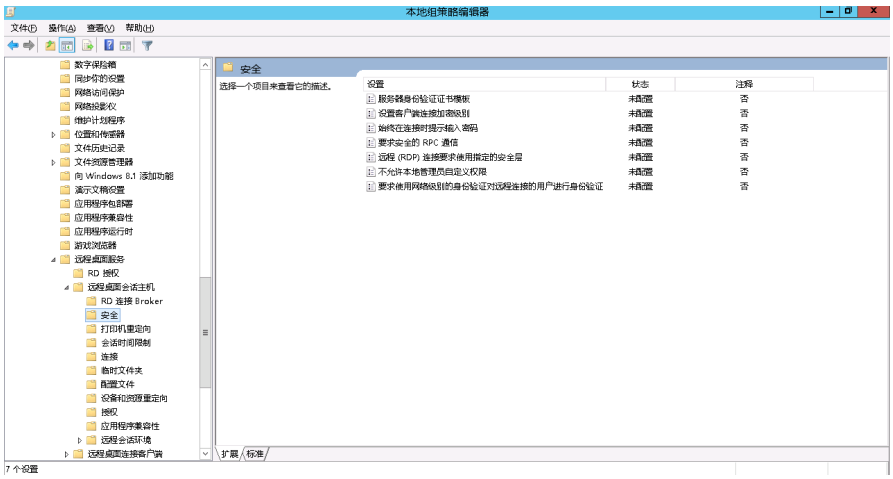
2. 选择“安全性”，并修改参数配置。

图 4-37 选择安全性



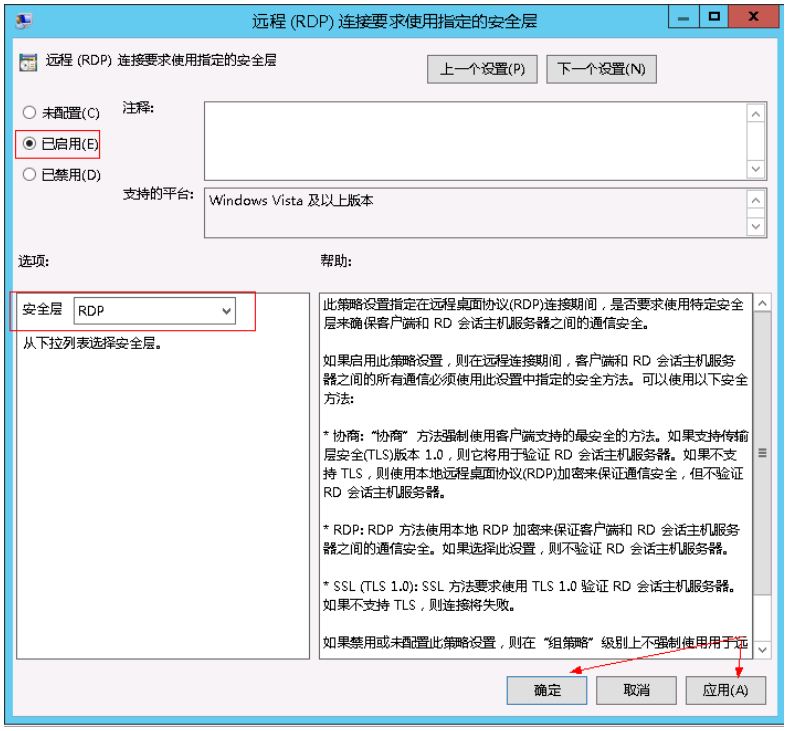
3. 再次远程连接Windows云服务器，如果仍出现报错“证书或相关链无效”，请执行4。
4. 使用控制台提供的远程连接功能（VNC方式）登录Windows云服务器。
5. 按快捷键“Win+R”打开“运行”窗口。
6. 输入“gpedit.msc”，进入“本地组策略编辑器”。
7. 在左侧导航栏，选择“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 安全”。

图 4-38 远程桌面会话主机



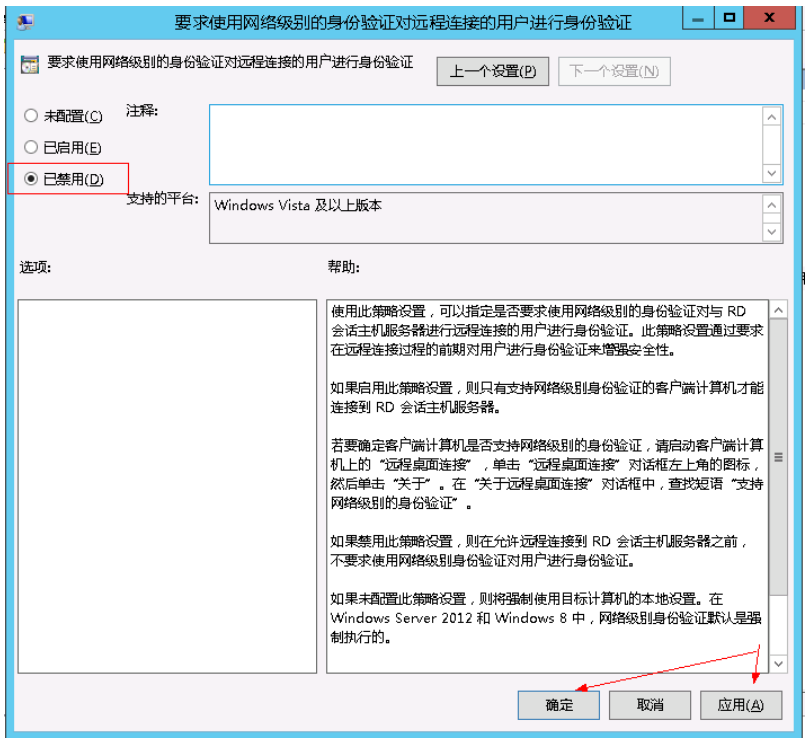
8. 根据界面提示，修改如下两项配置：
   - 启用“远程（RDP）连接要求使用指定的安全层”。

图 4-39 远程（RDP）连接要求使用指定的安全层



- 禁用“要求使用网络级别的身份验证对远程连接的用户进行身份验证”。

图 4-40 远程连接身份认证



9. 关闭组策略编辑器，然后重启云服务器。

4.2.9 使用 Mac 远程连接 Windows 云服务器出现报错 0x207

问题描述

使用“Microsoft Remote Desktop for Mac”工具远程连接Windows操作系统云服务器时出现报错0x207。

可能原因

该问题为勾选了仅允许运行使用网络级别身份验证的远程桌面的计算机连接导致。

处理方法

1. 按“Win+R”键打开运行对话框，输入“sysdm.cpl”并按回车键，打开系统属性。
2. 切换到“远程”选项卡，然后取消选中“仅允许运行使用网络级别身份验证的远程桌面的计算机连接”。

图 4-41 远程选项卡

3. 单击“确定”。

说明

该方法同样适用远程桌面时出现错误0x204。

4.2.10 远程连接 Windows 云服务器报错：您的凭据无法工作

问题描述

Windows操作系统的本地PC，通过RDP协议（如MSTSC方式）远程桌面连接Windows弹性云服务器报错，报错显示：您的凭据无法工作，之前用于连接到云主机的凭据无法工作，请输入新凭据。

处理方法

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。

步骤一：修改网络访问策略

步骤二：修改凭据分配

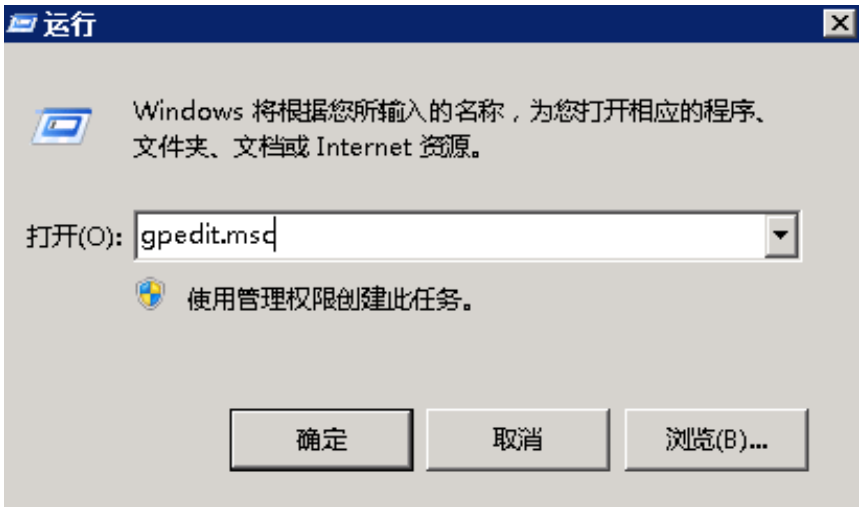
步骤三：设置本地主机的凭据

步骤四：关闭云服务器密码保护共享

步骤一：修改网络访问策略

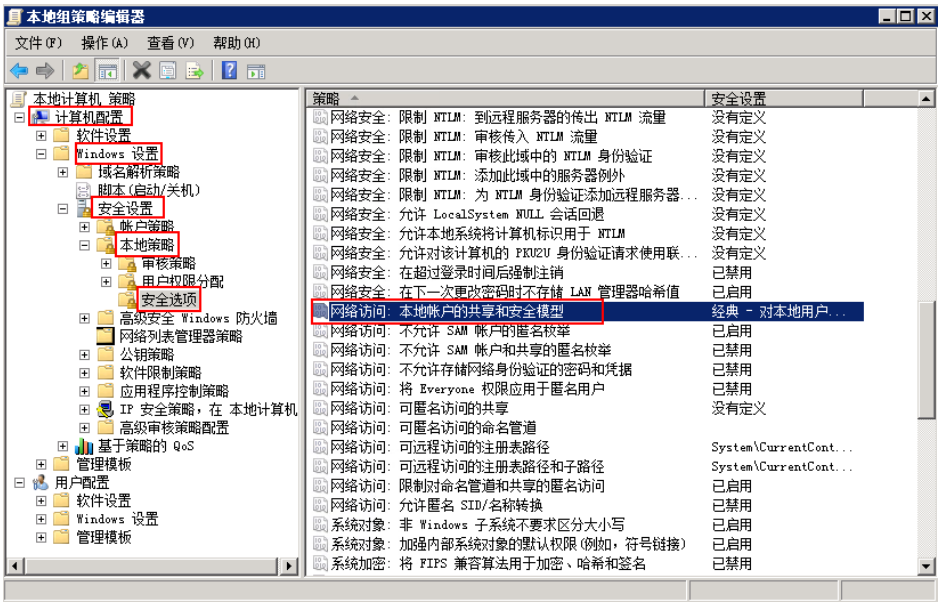
1. 使用管理控制台VNC方式登录云服务器。
2. 打开“开始 > 运行”，输入“gpedit.msc”，打开“本地组策略编辑器”。

图 4-42 gpedit.msc



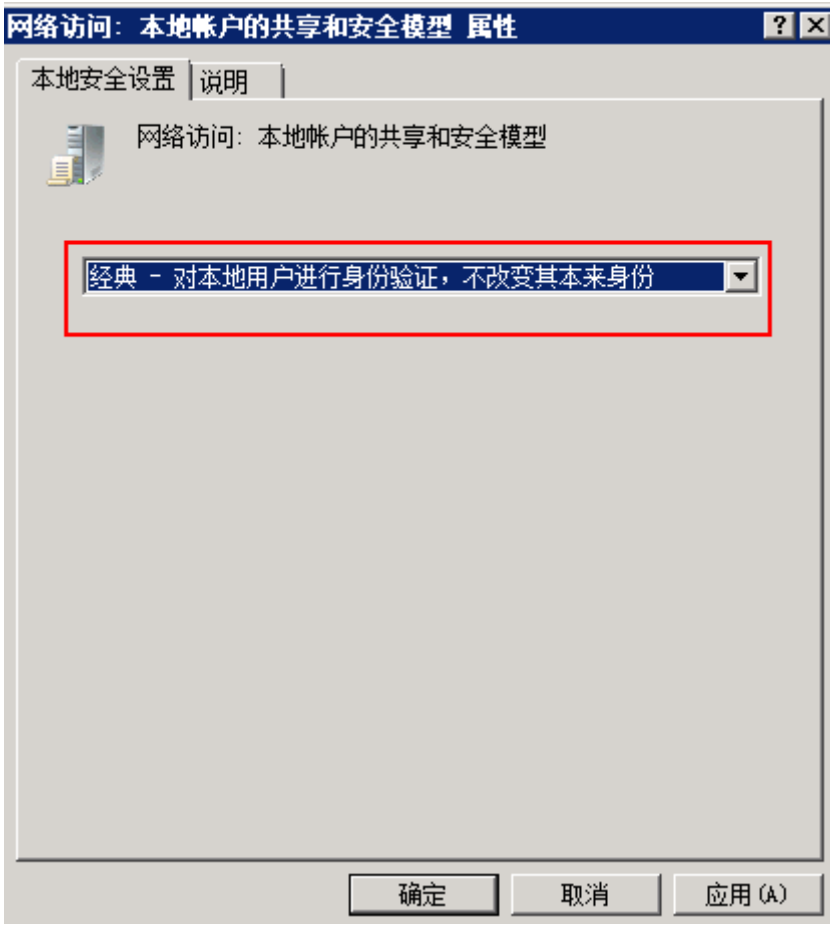
3. 选择“计算机配置 < Windows设置 < 安全设置 < 本地策略 < 安全选项”，打开“网络访问：本地账户的共享和安全模型”。

图 4-43 打开网络访问策略



4. 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”。

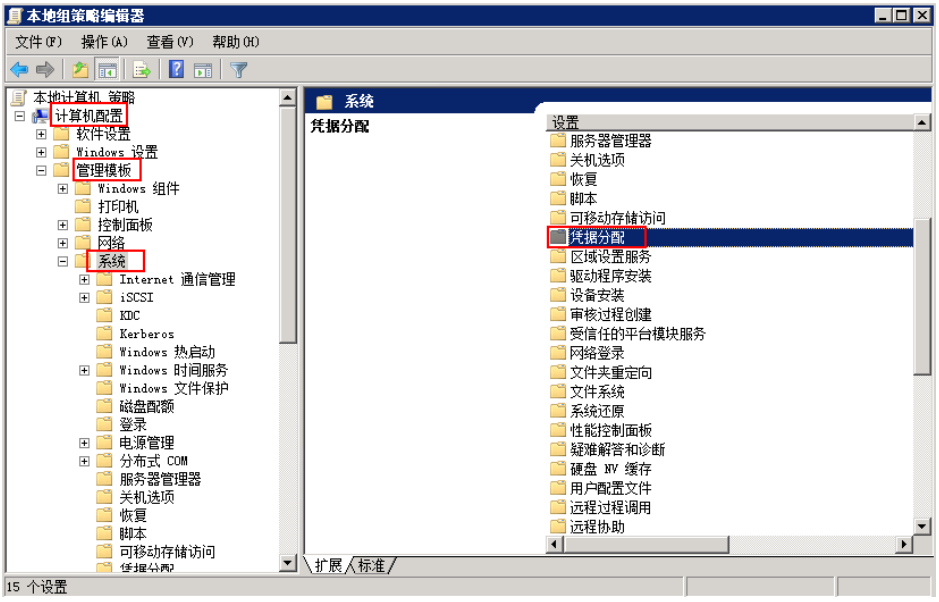
图 4-44 修改网络访问策略



步骤二：修改凭据分配

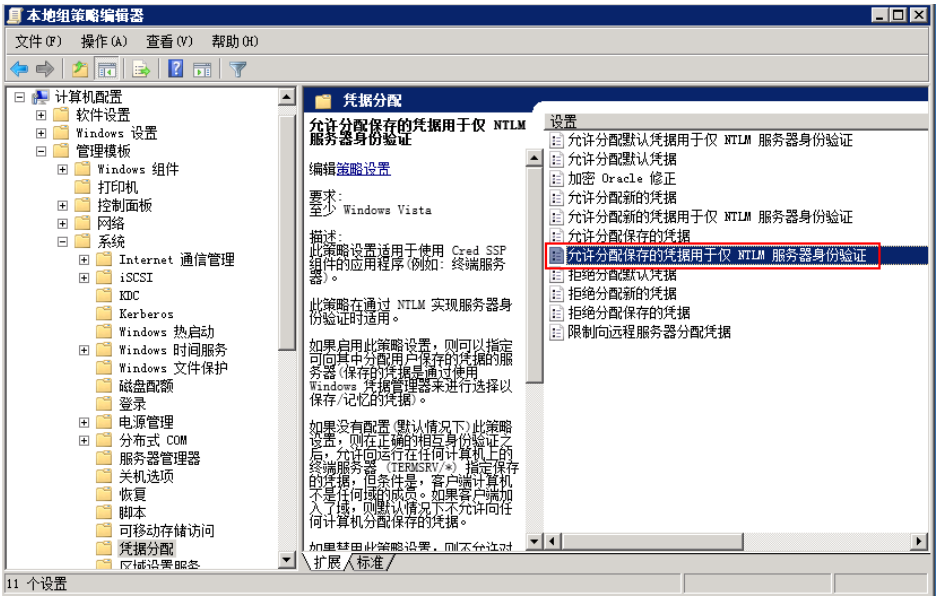
1. 使用管理控制台VNC方式登录云服务器。
2. 打开“开始 > 运行”，输入“gpedit.msc”，打开“本地组策略编辑器”。
3. 选择“计算机配置 < 管理模板 < 系统”，打开“凭据分配”。

图 4-45 打开网络访问策略



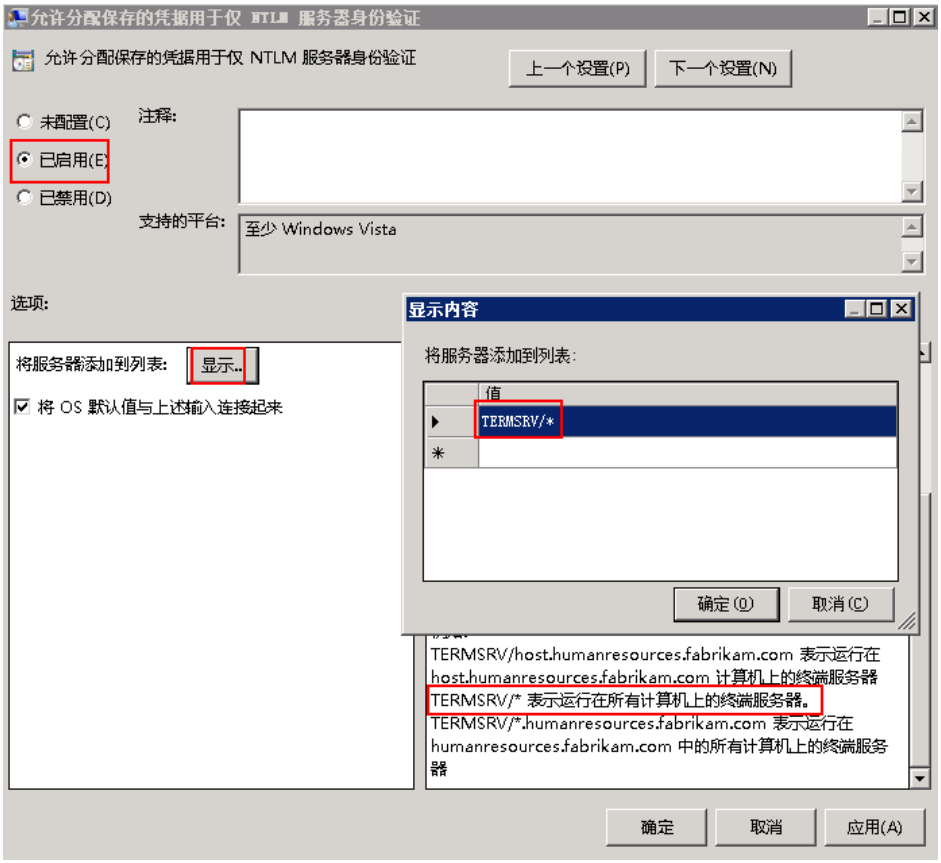
4. 双击打开“允许分配保存的凭据用于仅NTLM服务器身份验证”，单击“确定”。

图 4-46 允许分配保存的凭据用于仅 NTLM 服务器身份验证



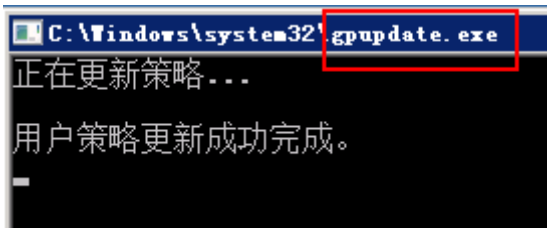
5. 选择“已启用” 在“显示”里面输入TERMSRV/*。TERMSRV/* 表示运行在所有计算机上的终端服务器。

图 4-47 配置为已启用



6. 刷新组策略，让设置生效。
7. 打开“开始 > 运行”输入**gpupdate /force**，更新组策略。

图 4-48 更新组策略



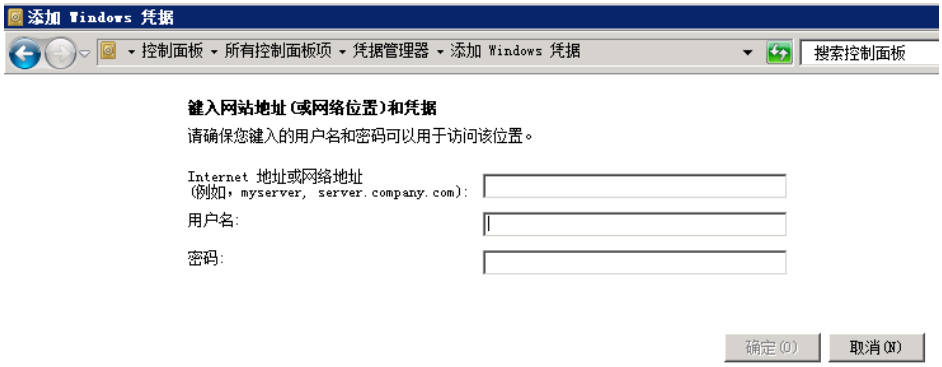
步骤三：设置本地主机的凭据

1. 打开本地主机的控制面板，选择“凭据管理器 > 管理Windows凭据”。

图 4-49 凭据管理器

2. 看Windows凭据下是否有当前登录的云服务器凭据，如果没有，添加一条凭据。
   - Internet地址或网络地址：云服务器的IP地址
   - 用户名：云服务器的登录用户名
   - 密码：云服务器的登录密码

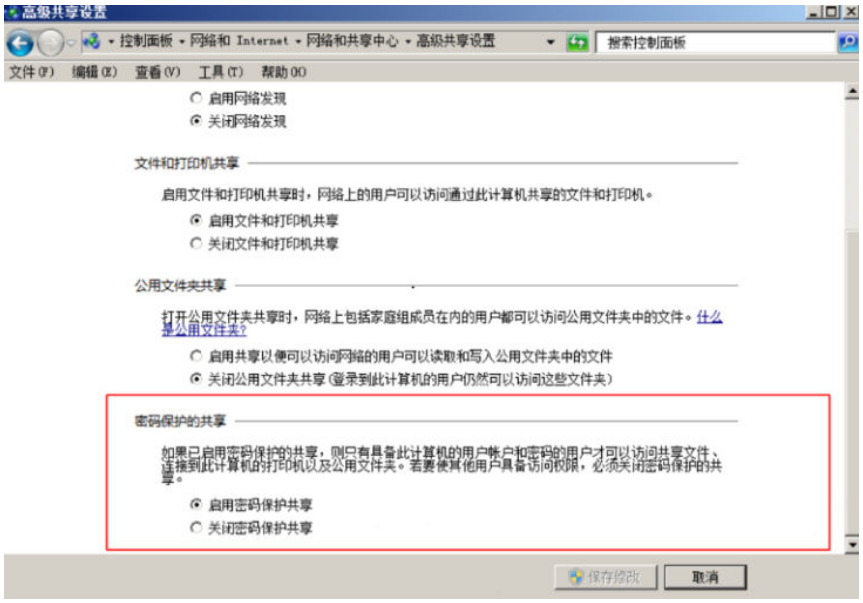
图 4-50 添加凭据



步骤四：关闭云服务器密码保护共享

1. 登录云服务器。
2. 打开左下角的“开始”菜单，选择“控制面板 > 所有控制面板项 > 网络和共享中心 > 更改高级共享配置。
3. 在“密码保护的共享”页签下选择“关闭密码保护共享”。

图 4-51 关闭密码保护共享



4. 单击“保存修改”。

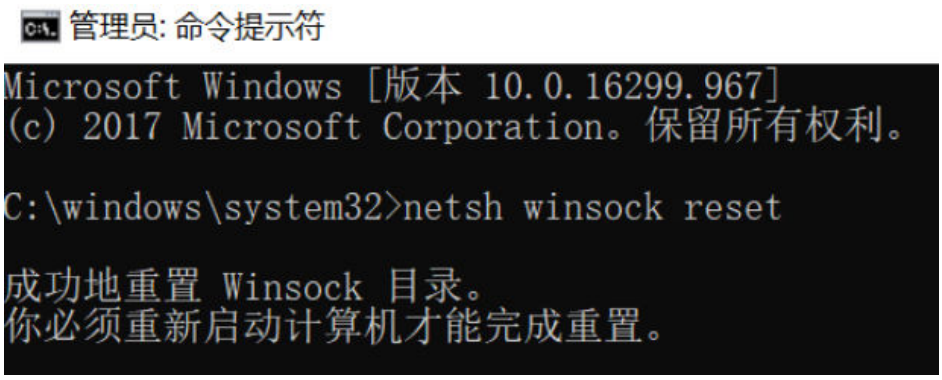
4.2.11 登录 Windows 云服务器提示“内部错误”怎么办?

问题描述

使用MSTSC方式登录Windows云服务器时，系统报错提示“内部错误”。

处理方法

1. 在本地主机以管理员身份运行cmd。
2. 执行**netsh winsock reset**



3. 重启本地主机。
4. 重试远程登录。

   如果仍无法登录云服务器，首先建议您排查本地的网络是否正常。更换网络（例如：手机热点）测试是否可以远程登录。

   如果使用手机热点的网络可以正常远程登录，说明是本地网络异常，建议重启本地网络（例如重启路由器）。

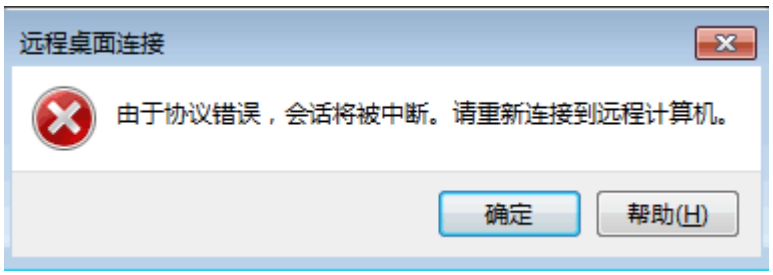
如果通过上述排查，仍然无法登录云服务器，请记录资源信息和问题时间，然后单击管理控制台右上方的“工单”，填写工单信息，获取技术支持。

4.2.12 远程连接 Windows 云服务器报错：由于协议错误会话中断

问题描述

远程桌面提示：由于协议错误，会话将会被中断，请重新连接到远程计算机。

图 4-52 协议错误



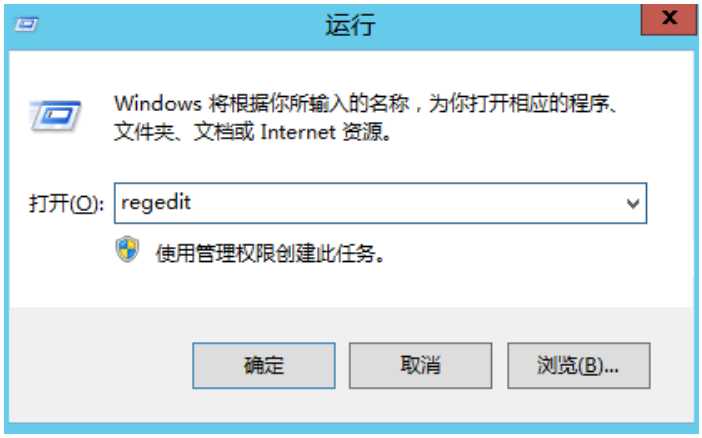
可能原因

注册表中的“Certificate”子键被损坏，导致用户无法与终端服务进行正常通信。

解决方法

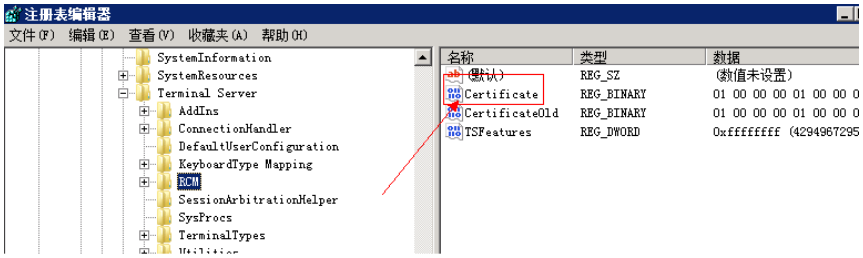
1. 在运行窗口输入“regedit”回车，打开注册表编辑器。

   图 4-53 打开注册表

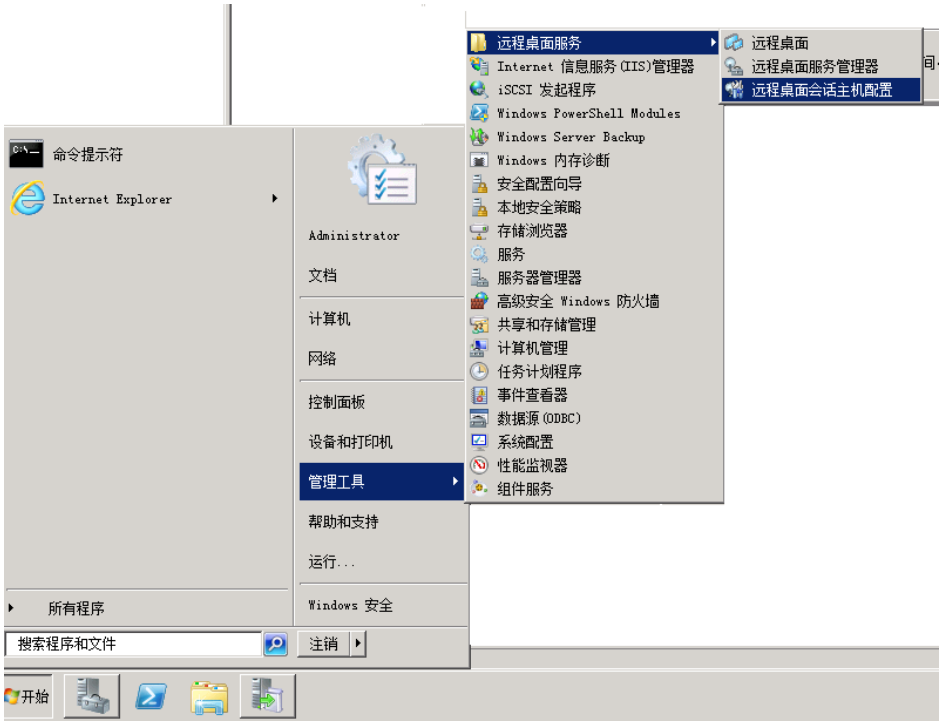
2. 找到HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Terminal Server\RCM
3. 删除Certificate。

图 4-54 删除 Certificate



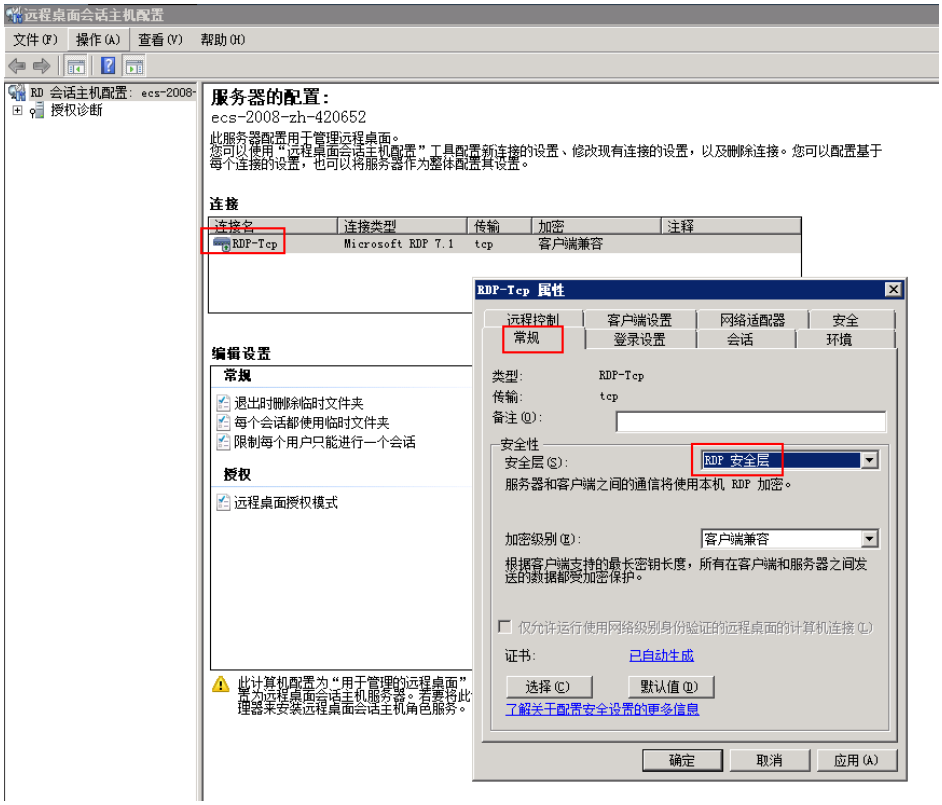
4. 重启云服务器。
5. 打开远程桌面会话主机配置。单击“开始”，打开“管理工具 > 远程桌面服务 > 远程桌面会话主机配置”

图 4-55 打开远程桌面会话主机配置



6. 右键单击RDP-TCP，选择“属性”，打开RDP-TCP属性对话框，修改安全性中的安全层为RDP安全层。

图 4-56 RDP-TCP 属性

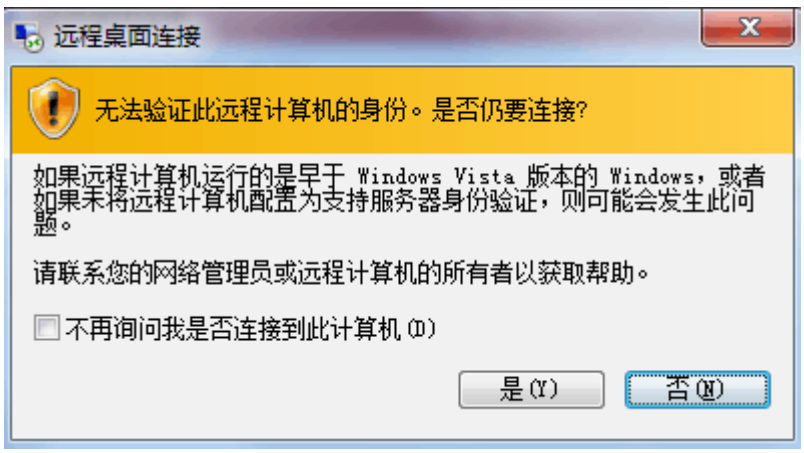


4.2.13 远程连接 Windows 云服务器报错：无法验证此远程计算机的身份

问题描述

由于在安全软件中设置了安全登录限制，导致远程桌面连接Windows云服务器报错：无法验证此远程计算机的身份。需要再次登录输入密码。

图 4-57 协议错误



可能原因

云服务器安装了安全软件，防止有未知IP登录云服务器。

解决方法

- 卸载安全软件。
- 登录安全软件，将登录安全等级修改为系统默认登录方式。

4.2.14 远程连接 Windows 云服务器报错：两台计算机无法在分配的时间内连接

问题描述

本地主机远程桌面连接云服务器时报错提示：两台计算机无法在分配的时间内连接。

图 4-58 两台计算机无法在分配的时间内连接

解决方法

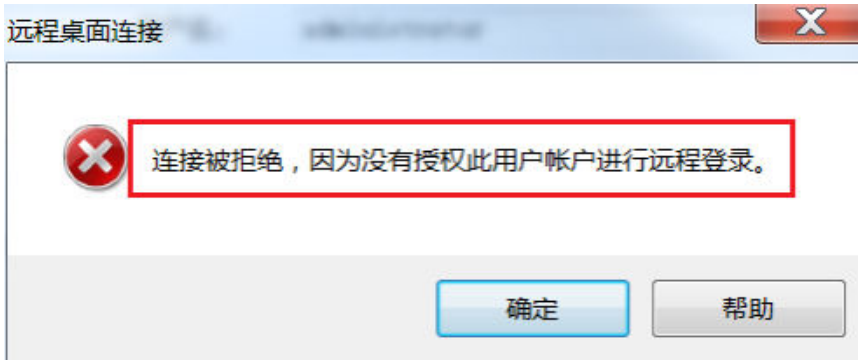
1. 在本地主机单击“开始”，运行中输入cmd，用管理员身份运行cmd。
2. 然后输入命令 **netsh winsock reset**
3. 根据提示重启本地主机后，重新连接云服务器。

4.2.15 远程连接 Windows 云服务器报错：连接被拒绝未授权此用户

问题描述

远程桌面连接Windows云服务器报错：连接被拒绝，因为没有授权此用户账户进行远程登录。

图 4-59 连接被拒绝未授权此用户



可能原因

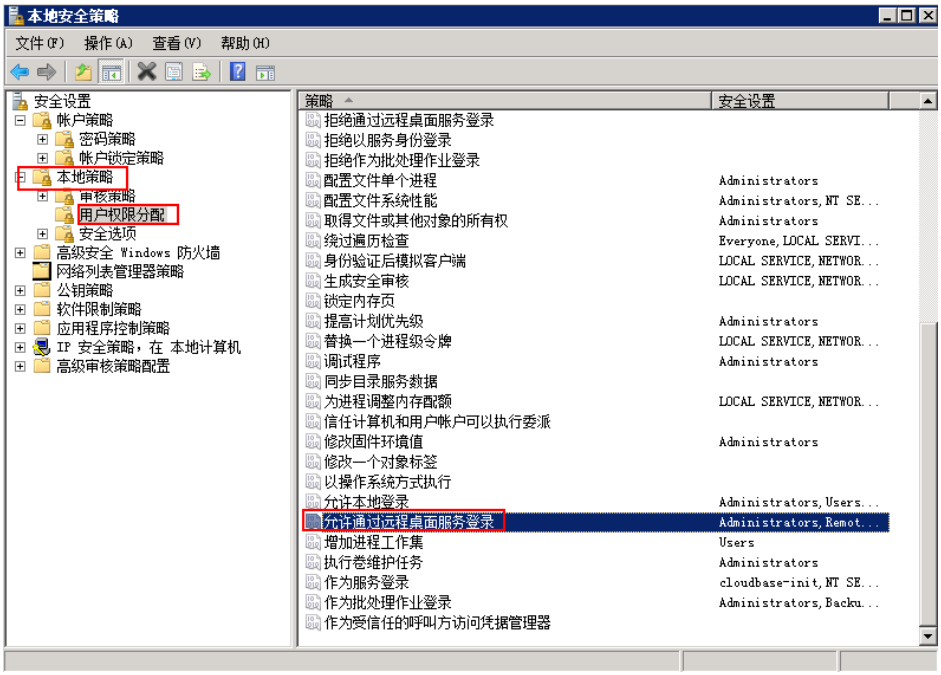
Windows远程桌面相关权限配置异常。

解决方法

步骤1 检查云服务器远程桌面权限配置。

1. 在运行窗口输入**secpol.msc**，打开组策略编辑器
2. 打开"本地策略 > 用户权限分配 > 允许通过远程桌面服务登录"。

图 4-60 本地策略



3. 包含已经被赋予远程登录服务器权限的用户组或单独的用户名。
   如果缺少上述配置，请单击“添加用户或组”进行添加。

图 4-61 允许通过远程桌面服务登录

步骤2 检查用户的用户组属性。

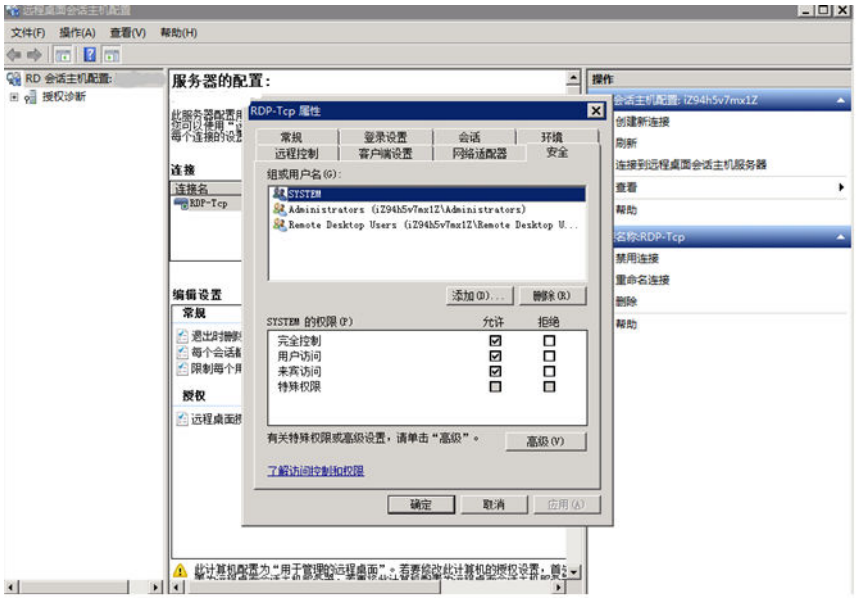
1. 在运行窗口输入**lusrmgr.msc**，打开"本地用户和组"配置管理单元。
2. 双击左侧功能树中的“用户”节点，切换到用户管理。
3. 双击出现访问异常的用户名。
4. 在弹出的用户属性对话框中，切换到“隶属于”选项卡，确保用户隶属于上述**步骤2.2**已经被赋予远程登录服务器权限的用户组。

图 4-62 检查用户的用户组属性

步骤3 检查远程桌面会话主机配置

1. 在运行窗口输入**tsconfig.msc**，打开"本远程桌面会话主机配置"。
2. 双击默认的远程桌面连接配置"RDP-Tcp"，或其他用户自己新增的连接配置，然后切换到“安全”选项卡。

图 4-63 安全选项卡



3. 确保"组或用户名"下，包含已经被赋予远程登录服务器权限的用户组或单独的用户名。

   如果缺少上述配置，请用户单击“添加”按钮进行添加。

4. 重启服务器或使用如下指令重启远程桌面服务以配置生效。
5. 在命令窗口依次输入如下命令：

   net stop TermService

   net start TermService

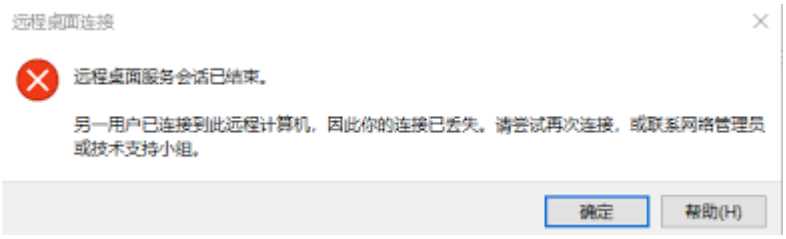
----结束

4.2.16 远程连接 Windows 云服务器报错：您的连接已丢失

问题描述

远程桌面连接Windows云服务器报错：您的远程桌面会话已结束，另一用户已连接到此远程计算机，因此您的连接已丢失。

图 4-64 远程桌面会话已结束



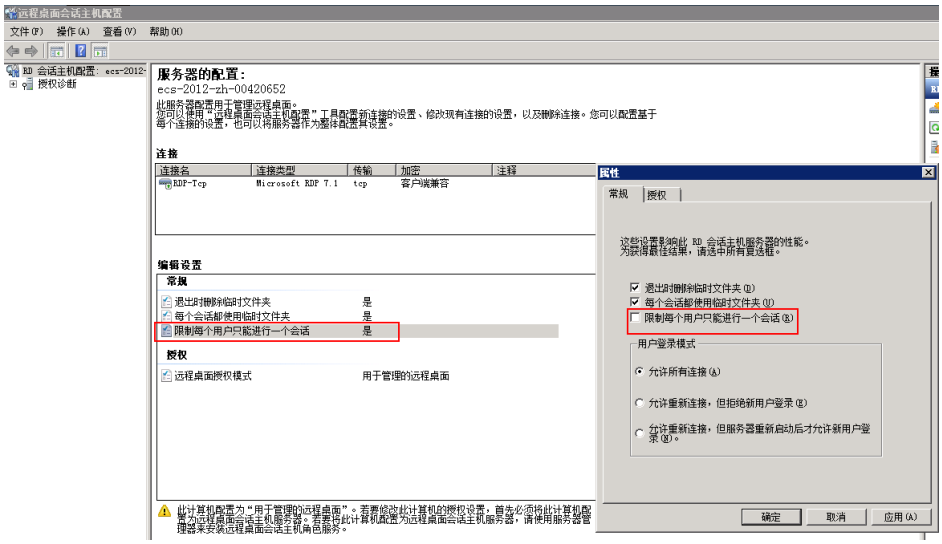
2008 操作系统处理方法

1. 打开“管理工具 > 远程桌面服务 > 远程桌面会话主机配置”，进入远程桌面会话主机配置页面。

图 4-65 远程桌面会话主机配置

2. 双击打开，取消勾选“限制每个用户只能进行一个会话”，单击“确定”。

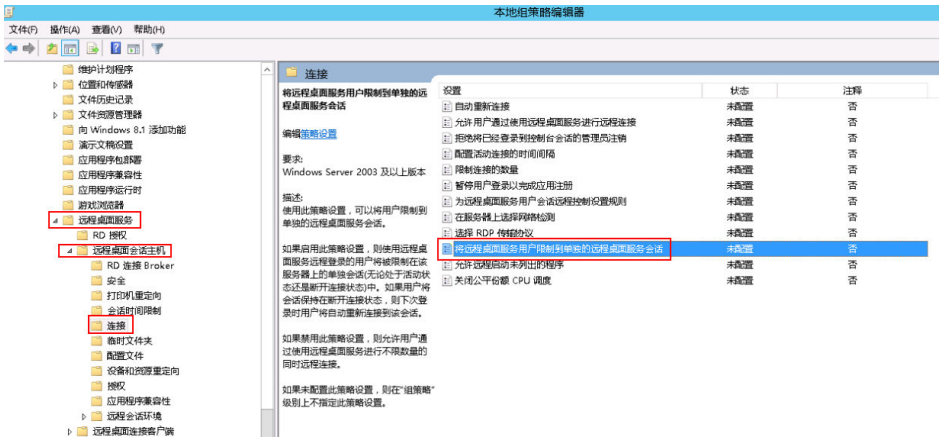
图 4-66 修改配置



2012 操作系统处理方法

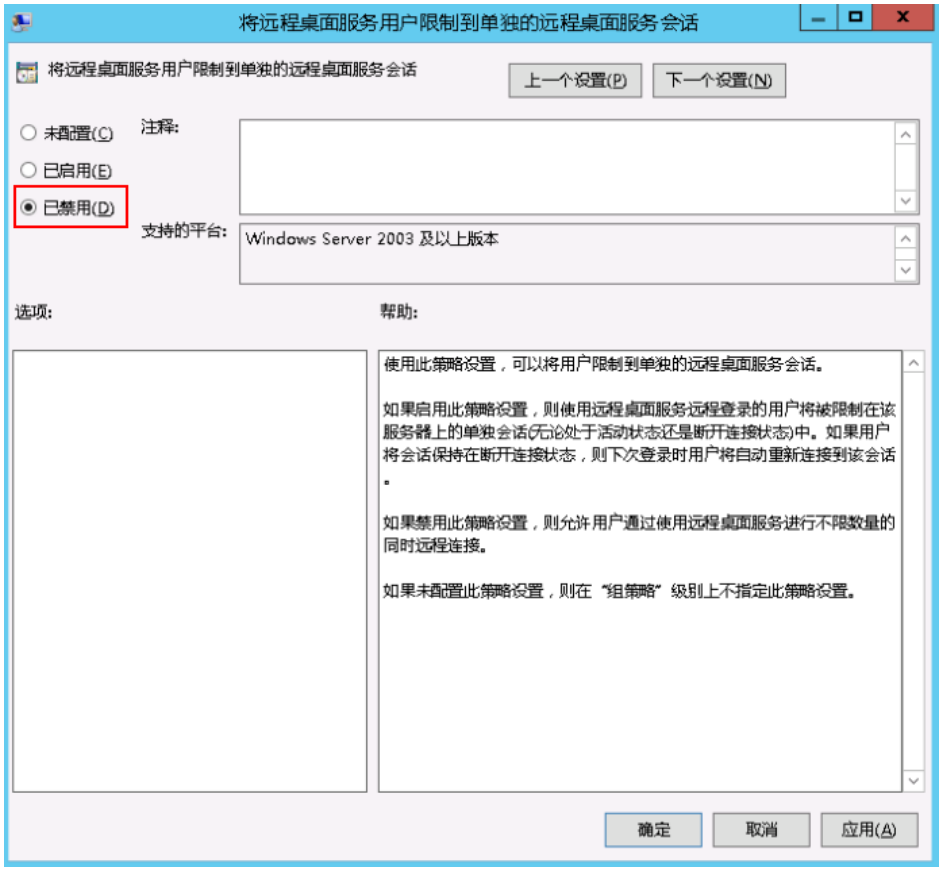
1. 打开“开始 > 运行”，输入 gpedit.msc，进入本地组策略编辑器。
2. 打开“计算机配置 > 管理模板 > Windows组件 > 远程桌面服务 > 远程桌面会话主机 > 连接”。

图 4-67 连接



3. 双击打开“将远程桌面服务用户限制到单独的远程桌面服务会话”，修改配置为“已禁用”，单击“确定”保存。

图 4-68 修改配置



4. 在命令窗口执行**gpupdate /force**，更新组策略。

4.2.17 远程连接云服务器出现蓝屏

问题描述

Windows Server 2012 R2操作系统云服务器，本地使用远程桌面连接功能连接云服务器并启用redirected drive功能时，云服务器出现蓝屏。

根本原因

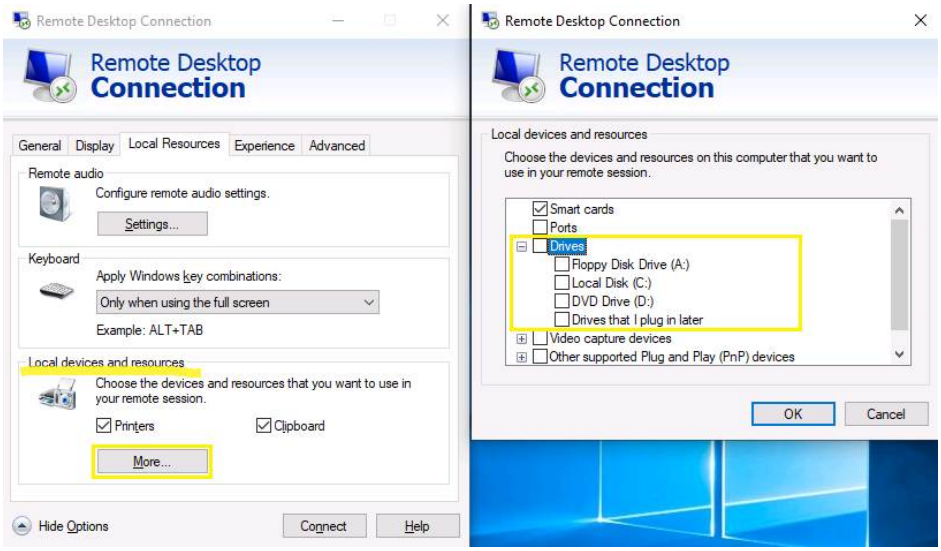
远程桌面连接启用了redirected drive功能，同时加载对应rdpdr.sys驱动，该驱动可能会导致云服务器操作系统崩溃，无法正常运作（例如错误码：0x18, 0x50, 0xa, 0x27, 0x133）导致云服务器蓝屏。

解决方法

使用远程桌面连接功能后，禁用redirect local drives功能。

1. 打开“运行”窗口。
2. 输入“mstsc”，并单击“确定”。
   系统打开“远程桌面连接”窗口。
3. 单击左下角的“选项”，并选择“本地资源”页签。
4. 在“本地设备和资源”栏，单击“详细信息”。
5. 在“本地设备和资源”窗口中，取消勾选“驱动器”。
6. 单击“确定”保存修改。

图 4-69 禁用 redirect local drives 功能



4.2.18 RDP 连接已断开，出现内部错误，错误代码 4

问题描述

Windows操作系统云服务器在登录时会遇到“出现了内部错误”提示，无法正常连接到服务器。这种情况一般都是远程服务太忙导致。

可能原因

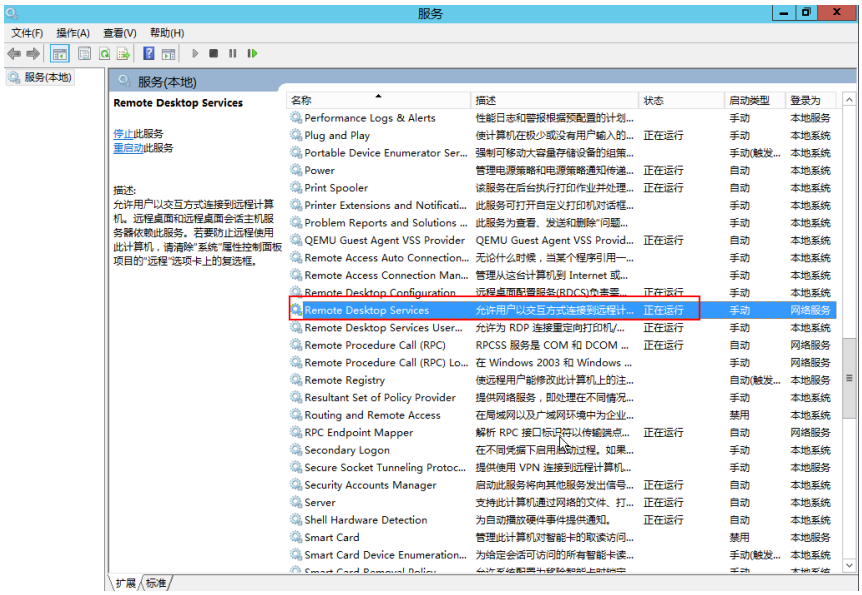
Remote Desktop Services服务忙碌导致的登录异常。

远程桌面登录后断开连接，但未注销登录也可能会出现这个提示。为了避免类似情况，建议在不需要远程连接服务器时及时注销登录。

解决方法

1. 通过控制台提供的VNC方式登录云服务器。
2. 打开Windows搜索框，输入services，选择“服务”。
3. 在服务中选择并重启Remote Desktop Services服务，请确保Remote Desktop Services状态为“正在运行”。

图 4-70 Remote Desktop Services



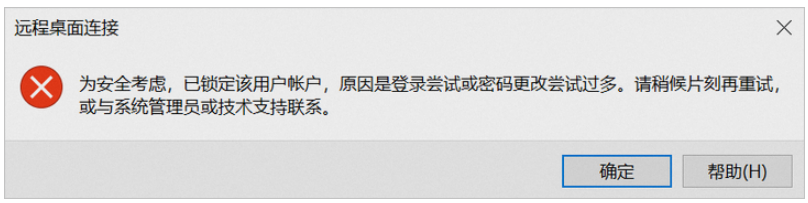
4. 重试远程连接。

   如果仍然无法连接还可以尝试在本地主机以管理员身份运行cmd，执行**netsh winsock reset**恢复网络连接的默认配置，执行后重试远程连接。

4.2.19 远程连接 Windows 云服务器报错：为安全考虑，已锁定该用户账户，原因是登录尝试或密码更改尝试过多

问题描述

使用远程登录方式连接Windows云服务器时提示“为安全考虑，已锁定该用户账户，原因是登录尝试或密码更改尝试过多”错误，具体报错信息如下图所示。



可能原因

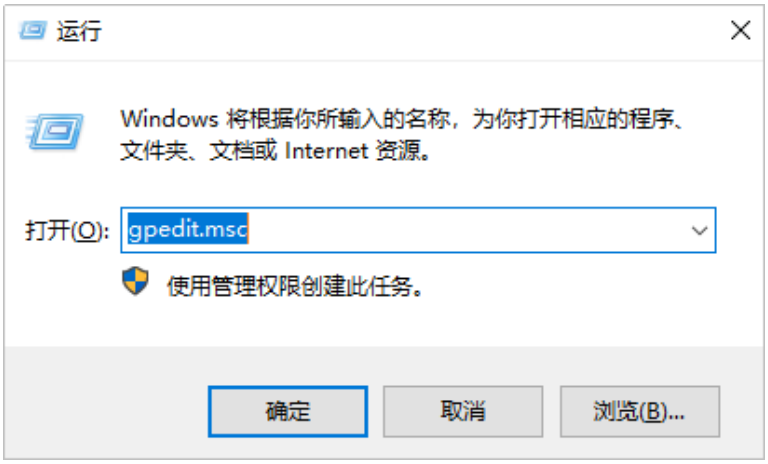
- Windows系统的系统组策略中配置了账户锁定策略，导致在登录时输入错误的密码次数过多时，该账户会被锁定，导致远程桌面无法登录。
- Windows公共镜像是Windows 2022版本，该镜像默认开启账户锁定策略。

解决方法

您可以修改Windows实例组策略账户锁定阈值为0以解决该问题。

1. 通过VNC连接Windows实例。

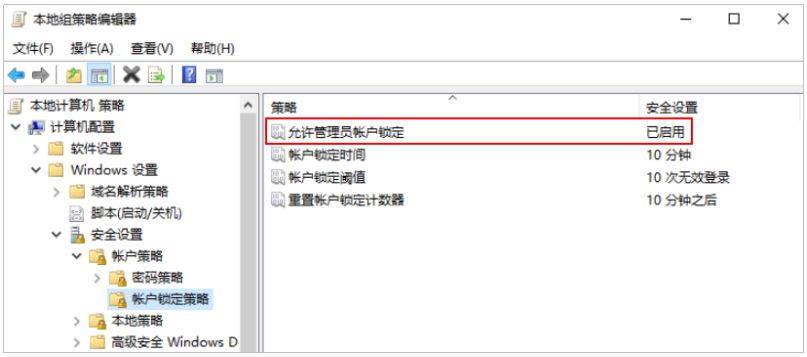
   具体操作，请参见**通过控制台VNC登录Windows ECS**。
2. 在Windows系统左下角，右键单击开始，然后单击“运行(R)”。
3. 在运行对话框中输入gpedit.msc命令，单击“确定”进入本地组策略编辑器页面。



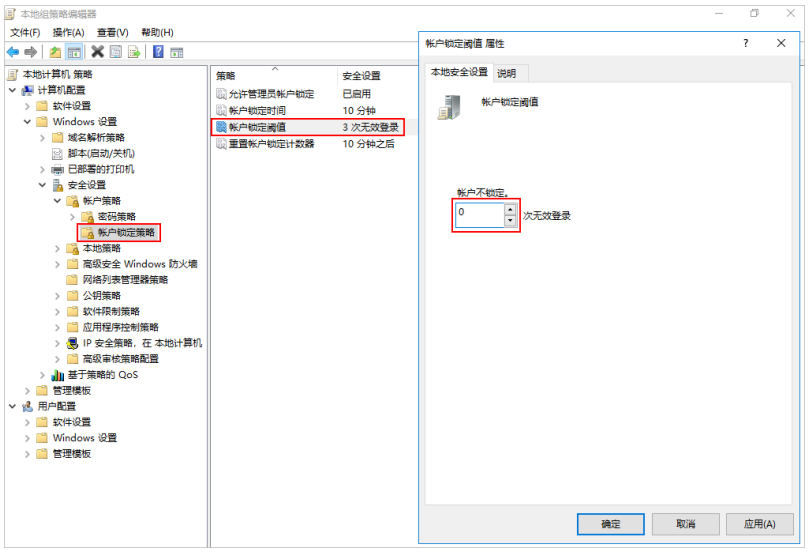
4. 在本地组策略编辑器页面中，选择“计算机配置 > Windows设置 > 安全设置 > 账户策略 > 账户锁定策略”。

   不同的Windows操作系统禁用该策略的操作略有不同，请尝试以下方式。

   - 双击“允许管理员账户锁定”，选中“已禁用”，单击“确定”。



   - 双击“账户锁定阈值”，将账户不锁定阈值修改为0，单击“确定”。



5. 重新使用远程桌面连接Windows实例，确保可以正常连接。

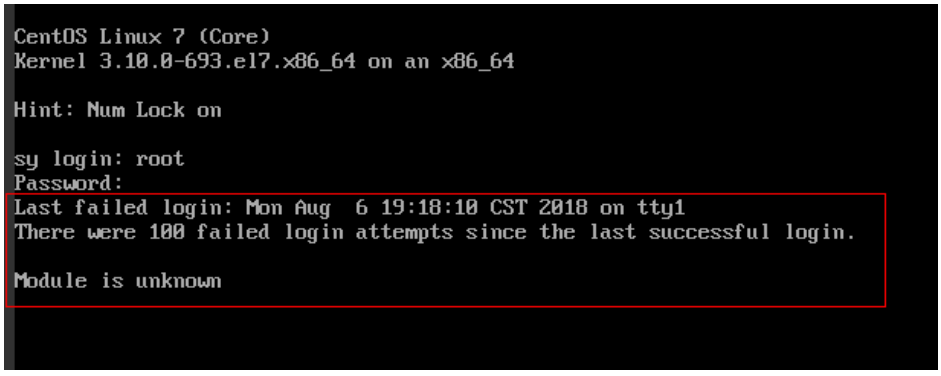
4.3 Linux 远程登录报错类

4.3.1 远程连接 Linux 云服务器报错：Module is unknown

问题描述

远程连接Linux云服务器报错：Module is unknown

图 4-71 Module is unknown



说明

- 修改此问题需要重启进入救援模式，请评估风险后进行操作。
- 本节操作涉及云服务器重启操作，可能会导致业务中断，请谨慎操作。

根因分析

由于错误修改/etc/pam.d/目录下的文件导致。

处理方法

1. 进入云服务器的单用户模式。

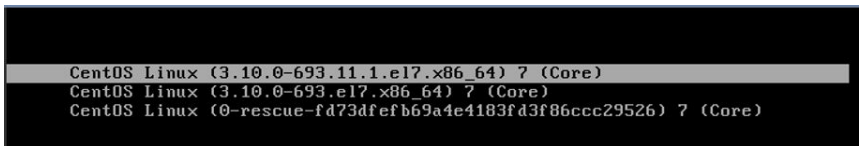
   以CentOS 7操作系统为例：

   a. 单击“远程登录”。

   b. 单击远程登录操作面板上方的“发送CtrlAltDel”按钮，重启虚拟机。

   c. 按上方向键，阻止系统自动继续，在出现内核选项时按字母键**e**进入内核编辑模式。

   图 4-72 进入内核编辑模式

   说明

   Euler镜像默认对grub文件进行了加密，进入编辑内核模式时会提示：Enter username，需要输入用户和密码，请联系客服获取。

   d. 找到linux16行末尾，删除不需要加载的参数到ro参数。

   e. 修改ro为rw，以读写方式挂载根分区。

   f. 并添加rd.break，然后执行Ctrl+X。

   图 4-73 修改前

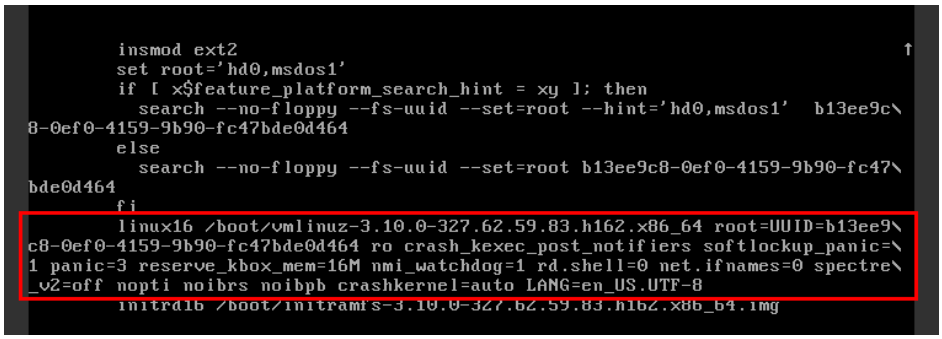
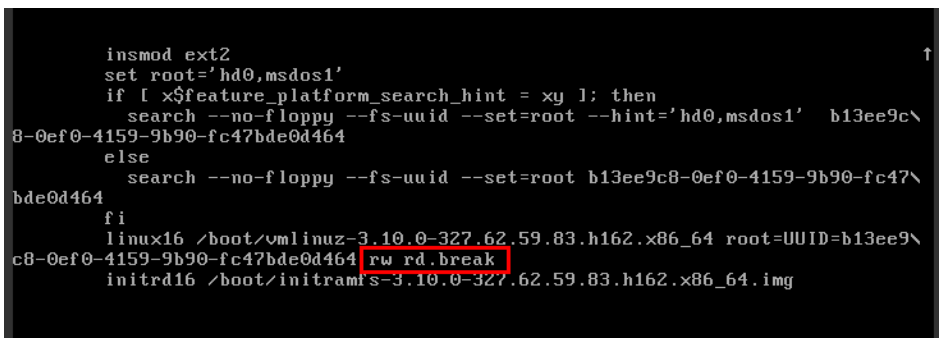
   

   图 4-74 修改后

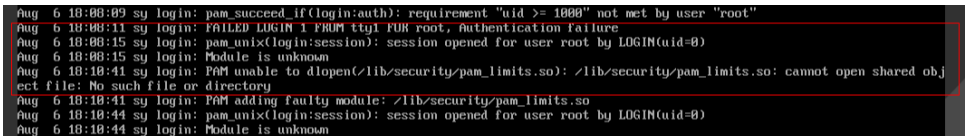
   

   g. 执行以下命令切换至/sysroot目录。

   chroot /sysroot

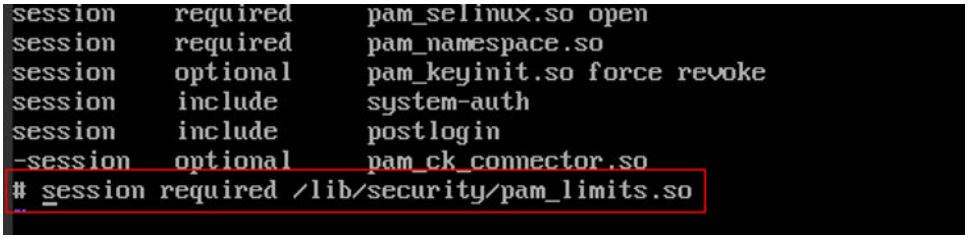
2. 执行以下命令，查看系统日志定位出错的文件
   grep Module /var/log/messages

   图 4-75 系统日志



3. 编辑系统日志中提示的错误文件，并注释或修改错误行。
   vi /etc/pam.d/login

   图 4-76 修改错误信息



4. 重启服务器，重试连接云服务器。

   说明

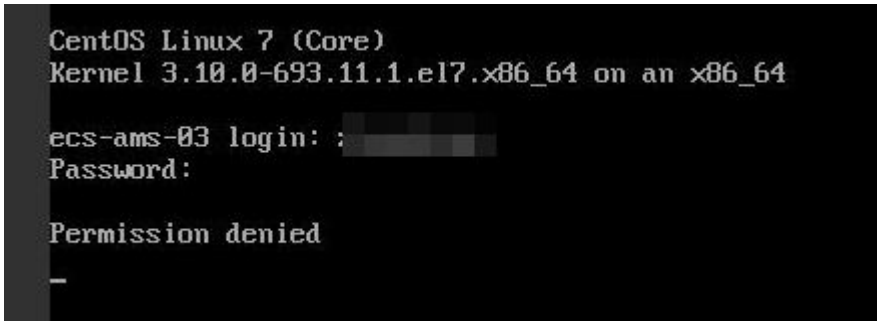
   - 如需查看修改记录，定位是否人为错误修改导致，请执行以下命令。
     vi /root/.bash_history
     搜索关键字vi或者login
   - 请勿随便修改/etc/pam.d/目录下的文件。如需对pam详细了解可查看pam.d帮助手册，在系统内执行以下命令。
     man pam.d

4.3.2 远程连接 Linux 云服务器报错：Permission denied

问题现象

远程连接Linux云服务器报错：Permission denied

图 4-77 Permission denied



说明

- 修改此问题需要重启进入救援模式，请评估风险后进行操作。
- 本节操作涉及云服务器重启操作，可能会导致业务中断，请谨慎操作。

根因分析

/etc/security/limits.conf中的nofile 用来设置系统允许打开的最大文件数目，如果nofile值大于PermissionDenied.png内核设置的fs.nr_open参数值（默认为1048576），会导致登录校验错误，导致登录云服务器时提示“Permission denied”。

处理方法

1. 进入云服务器的单用户模式。

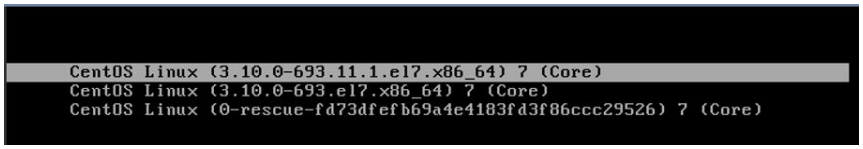
   以CentOS 7操作系统为例：

   a. 单击“远程登录”。

   b. 单击远程登录操作面板上方的“发送CtrlAltDel”按钮，重启虚拟机。

   c. 按上方向键，阻止系统自动继续，在出现内核选项时按字母键**e**进入内核编辑模式。

   图 4-78 进入内核编辑模式

   说明

   Euler镜像默认对grub文件进行了加密，进入编辑内核模式时会提示：Enter username，需要输入用户和密码，请联系客服获取。

   d. 找到linux16行末尾，删除不需要加载的参数到ro参数。

   e. 修改ro为rw，以读写方式挂载根分区。

   f. 并添加rd.break，然后执行Ctrl+X。

   图 4-79 修改前

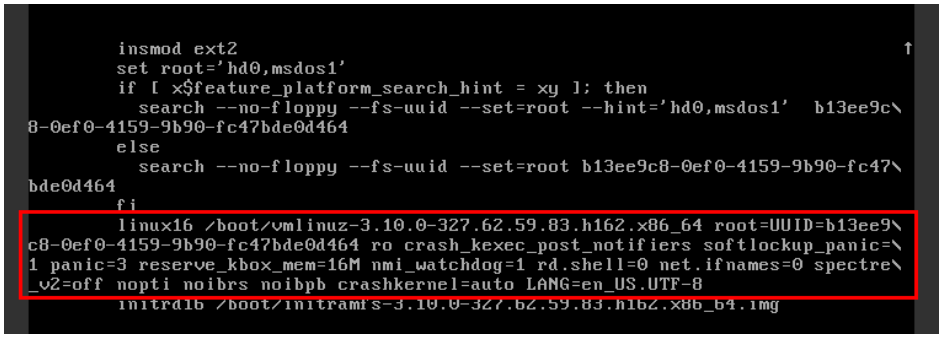
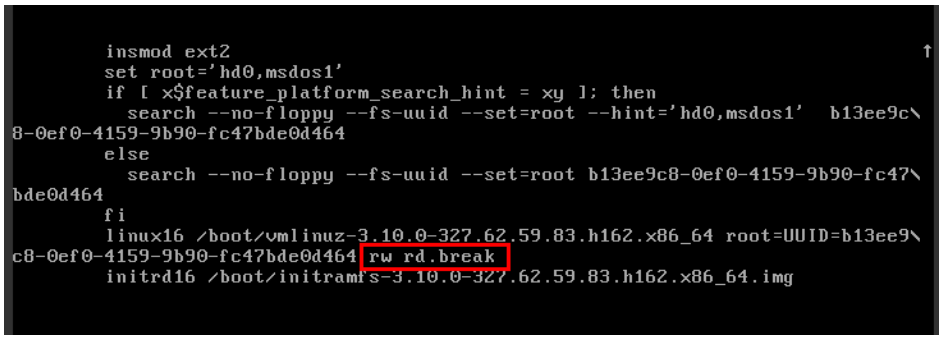
   

图 4-80 修改后



g. 执行以下命令切换至/sysroot目录。

chroot /sysroot

2. 执行以下命令，查询内核的fs.nr_open值。

sysctl fs.nr_open

3. 编辑 /etc/security/limits.conf，修改配置的nofile值为合理的值，需小于2中查询的fs.nr_open值，例如65535。

vi /etc/security/limits.conf

说明

limits.conf 文件实际是Linux PAM（插入式认证模块，Pluggable Authentication Modules）中pam_limits.so 的配置文件。更多详细配置信息请查看man手册，执行：

man limits.conf

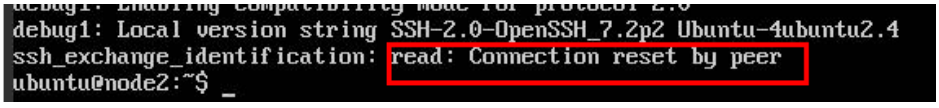
4. 重启服务器，重试连接云服务器。

4.3.3 远程连接 Linux 云服务器报错：read: Connection reset by peer

问题现象

远程连接Linux云服务器报错：read: Connection reset by peer

图 4-81 read: Connection reset by peer



可能原因

- 安全组未放通远程登录端口。
- 防火墙开启，且关闭了远程连接端口。

处理方法

针对此问题，推荐采用以下方式来排查：

- **检查安全组规则**
  - 入方向：打开远程登录端口。默认使用的22端口。

图 4-82 入方向开放 22 端口

- 出方向：出方向规则为白名单（允许），放通出方向网络流量。

图 4-83 放通出方向网络流量

- **云服务器防火墙添加端口例外**

  以Ubuntu操作系统为例：

  a. 执行以下命令检查防火墙状态：

  sudo ufw status

  回显信息如下：

  ```
  Status: active
  ```

  b. 添加端口例外，以默认使用的22端口为例。

  ufw allow 22

  Rule added

  Rule added (v6)

  c. 重新查看防火墙状态

  sudo ufw status

  ```
  Status: active
  To                         Action      From
  --                         ------      ----
  22                         ALLOW       Anywhere
  22 (v6)                    ALLOW       Anywhere (v6)
  ```

  规则添加成功，重新测试远程连接云服务器。

4.3.4 远程连接 Linux 云服务器报错：Access denied

问题现象

远程连接Linux云服务器报错：Access denied

可能原因

- 账号或密码输入错误。
- SSH服务端配置了禁止root用户登录的策略。

处理方法

- 账号或密码输入错误。

  检查输入的用户名或密码。

  Linux云服务器默认用户名root，如果密码错误，请在控制台重置密码。

  重置密码：选中待重置密码的云服务器，并选择“操作”列下的“更多 > 重置密码”。
- SSH服务端配置了禁止root用户登录的策略。
  a. 编辑 /etc/ssh/sshd_config 文件，检查如下设置，确保root用户能通过SSH登录：
  ```
  PermitRootLogin yes
  ```
  b. 重启 SSH 服务。
  - CentOS 6

    service sshd restart
  - CentOS 7

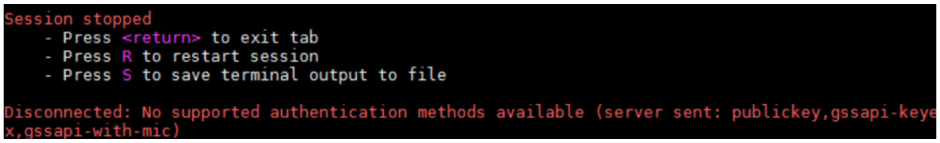
    systemctl restart sshd

4.3.5 远程连接 Linux 云服务器报错：Disconnected: No supported authentication methods available

问题现象

远程连接Linux云服务器报错：Disconnected: No supported authentication methods available.

图 4-84 No supported authentication methods available



可能原因

SSH服务端配置了禁止密码验证登录的策略。

处理方法

1. 编辑 /etc/ssh/sshd_config 文件，检查如下设置
   vi /etc/ssh/sshd_config
2. 修改如下配置项：
   把PasswordAuthentication no 改为 PasswordAuthentication yes
   或去掉PasswordAuthentication yes 前面的#注释掉。
3. 重启 SSH 服务。
   - CentOS 6
     service sshd restart
   - CentOS 7
     systemctl restart sshd

4.3.6 远程连接 Linux 云服务器报错：Authentication failed

问题描述

非root账号通过SSH方式远程登录Linux服务器报错：Authentication failed。

```
Your account has expired;please contact your system administrator.
Authentication failed.
```

可能原因

由于用户账号过期导致出现Authentication failed报错，重新设置过期账号密码或调整账号过期时间即可。

处理方法

方法一：

1. 以root用户登录Linux云服务器。
2. 执行以下命令，重置过期账号的密码。
   chage -l *过期账号*

方法二：

执行以下命令，调整账号过期时间。

chage -E *过期时间 过期账号*

4.3.7 使用 SSH 登录 Linux 云服务器时提示“pam_unix(sshdsession) session closed for user”错误

问题描述

当使用SSH登录Linux弹性云服务器时，即便正确输入了密码，在命令行或secure日志中也会出现类似如下错误信息，导致连接失败：

- 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

该问题通常是由于相应用户的默认Shell被修改所致。

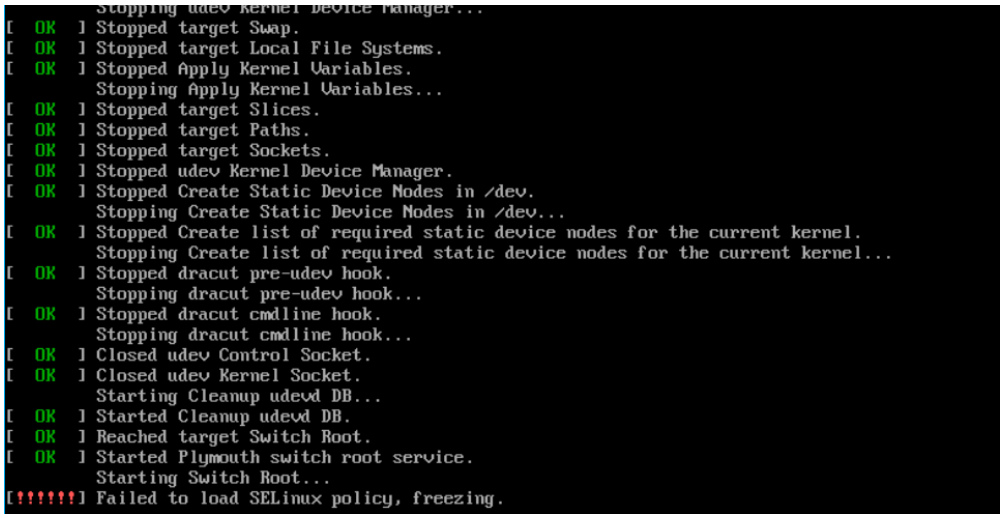
处理方法

1. 远程登录弹性云服务器。
2. 执行以下命令，查看相应用户的默认Shell。
   cat /etc/passwd | grep test
   查看相应用户的 Shell 是否被修改成了 nologin。
   test:x:1000:1000::/home/test:/sbin/nologin
3. 如果需要修改相关策略配置，在继续之前建议进行文件备份。
4. 执行以下命令，将相应用户的默认Shell修改为bash。
   vi /etc/passwd
5. 将/sbin/nologin修改为/bin/bash
6. 使用SSH客户端重新连接服务器。

4.3.8 Linux 云服务器启动时提示报错：Failed to load SELinux policy, freezing.

问题描述

Linux云服务器启动后提示“Failed to load SELinux policy, freezing. ”错误，具体报错信息如下图所示。



可能原因

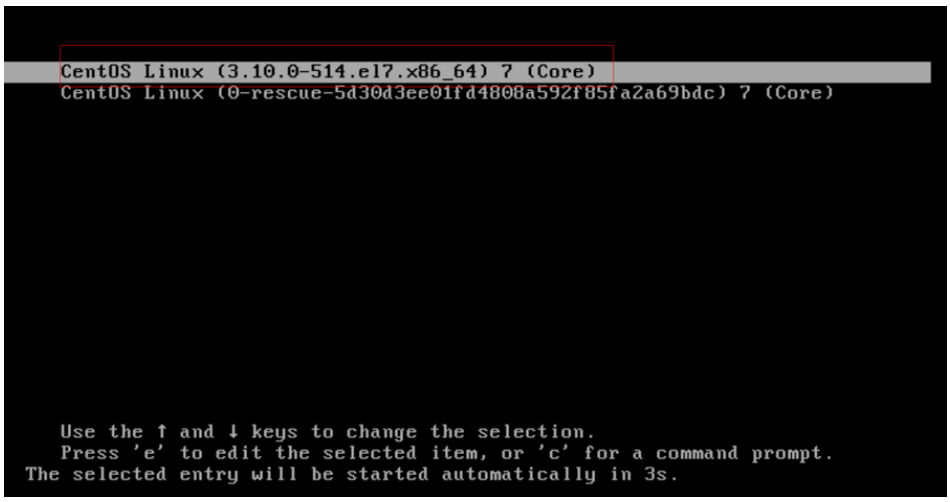
出现该报错由于当前操作系统开启了SElinux。

说明

该文档适用于CentOS系统，在该版本的系统上开启了SELinux，可能会触发该问题。

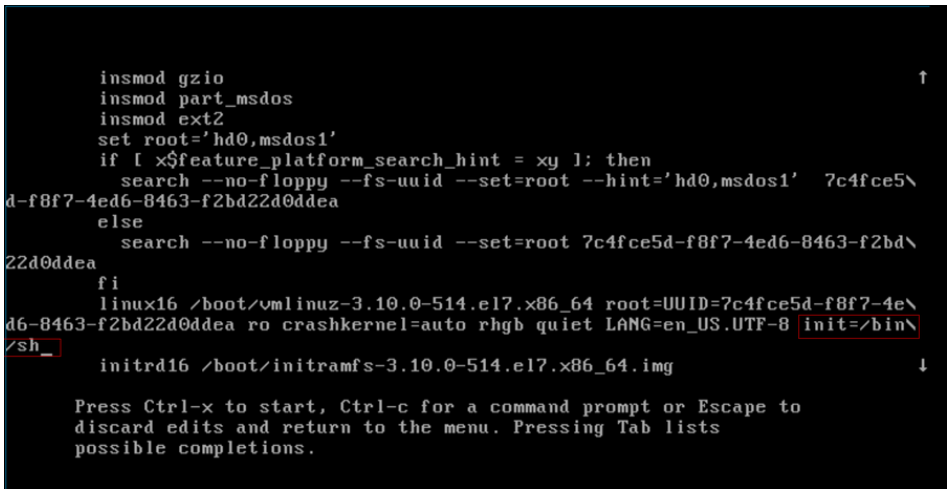
处理方法

1. Linux云服务器启动后，在出现内核选项时按字母键**e**进入内核编辑模式。



2. 找到linux16，在最后**LANG=en_US.UTF-8**字样后面添加以下内容，注意UTF-8 后面有空格。

```
init=/bin/sh
```



3. 执行以下命令启动，进入单用户模式。

   Ctrl+X

4. 执行以下命令，把系统文件权限改成可读写（rw）。

   mount -o remount,rw /

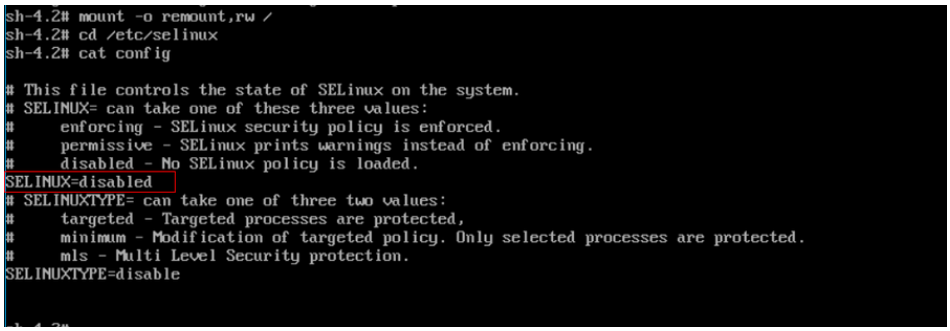
5. 执行以下命令，进入/etc/selinux目录。

   cd /etc/selinux

6. 执行以下命令，编辑config文件。

   cat config

7. 修改**SELINUX=disabled**后保存退出。



8. 重启云服务器。

4.3.9 使用 SSH 登录 Linux 云服务器时提示“requirement "uid >= 1000" not met by user "root"”错误

问题描述

登录Linux云服务器时，输入正确的用户名和密码后，也无法正常登录。该问题出现时，VNC或SSH客户端其中一种方式可以正常登录，或者两种方式均无法正常登录，执行cat /var/log/secure命令查看secure日志时提示如下错误信息。

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

可能原因

PAM相关模块的策略配置，禁止了UID小于1000的用户进行登录。

处理方法

以下操作步骤以CentOS 6.5 64位操作系统为例，其他类型及版本操作系统配置可能有所差异，具体情况请参阅相应操作系统的官方文档。

1. 通过VNC或SSH客户端登录Linux云服务器。
2. 通过cat命令查看异常登录模式，对应的PAM配置文件，请参考如下信息。

文件	功能说明
/etc/pam.d/login	控制台对应配置文件。例如密码验证、账户锁定和限制登录IP等。
/etc/pam.d/sshd	SSH远程登录的认证信息。
/etc/pam.d/system-auth	系统级别的认证信息，例如密码策略、用户信息和访问控制等。

每个启用PAM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。检查相应配置文件中，是否有类似如下配置信息。

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

3. 使用vi编辑器，修改相应配置文件中的配置，整行删除或在段落前添加#号注释。
   - 修改策略配置：

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

- 取消策略配置：

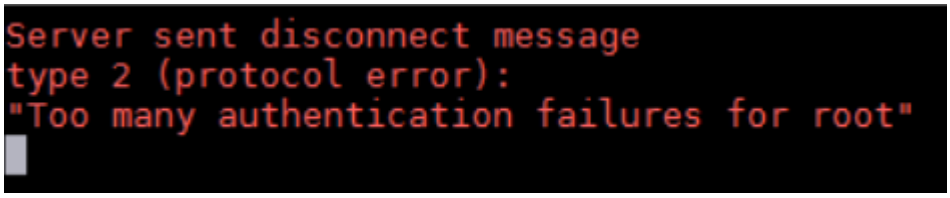
```
# auth required pam_succeed_if.so uid >= 1000
```

4. 重新登录云服务器。

4.3.10 使用 SSH 登录 Linux 云服务器时提示“Too many authentication failures for root”错误

问题描述

使用SSH客户端远程连接Linux云服务器时，连接失败，提示“Too many authentication failures”。



可能原因

SSH远程登录配置文件（/etc/ssh/sshd_config）中配置了密码重试策略，多次连续输入错误密码后，提示该错误。

处理方法

1. 远程登录弹性云服务器。
2. 执行以下命令，查看sshd_config文件中是否包含如下配置。

   cat /etc/ssh/sshd_config

   回显如下类似信息，表示连续6次输入密码错误后，会断开SSH连接。

```
MaxAuthTries 6
```

   说明

   MaxAuthTries参数默认未启用。该参数用于限制用户在每次SSH登录时，能够连续错误输入密码的次数。超过错误输入次数则会断开SSH连接，并显示相关错误信息。

3. 执行以下命令，打开SSH配置文件，修改用户登录控制参数。

   vi /etc/ssh/sshd_config

4. 按**i**键进入编辑模式。
5. 将参数MaxAuthTries设置为较大的一个数，或者在MaxAuthTries参数前添加#。
   - 修改密码重试策略：

```
MaxAuthTries 999
```

   - 取消策略配置：

```
# MaxAuthTries 6
```

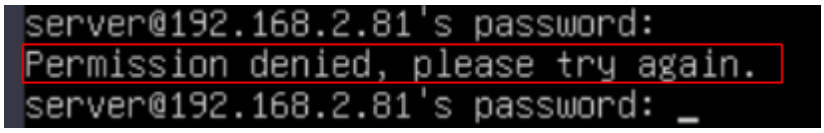
6. 按**Esc**键退出编辑模式，并输入**:wq**保存后退出。
7. 重启sshd服务。
   - CentOS 6：**service sshd restart**
   - CentOS 7：**systemctl restart sshd**

4.3.11 使用 SSH 登录 Linux 云服务器时提示“Permission denied, please try again.”错误

问题描述

使用SSH登录Linux云服务器时，提示“Permission denied, please try again.”错误。

图 4-85 报错信息



执行cat /var/log/secure命令查看登录日志，提示如下错误信息。

```
Permission denied, please try again.
User test from 192.168.xxx.xxx not allowed because not listed in AllowUsers.
User test from 192.168.xxx.xxx not allowed because listed in DenyUsers.
User root from 192.168.xxx.xxx not allowed because a group is listed in DenyGroups.
User test from 192.168.xxx.xxx not allowed because none of user's groups are listed in AllowGroups.
```

可能原因

该问题通常是由于ECS实例内SSH远程登录配置文件（/etc/ssh/sshd_config）中启用了用户登录控制参数，对可登录用户进行限制所致，用户登录控制参数说明如下：

- 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拒绝登录。

拒绝策略优先级高于允许策略，具体说明如下：

- 如果AllowUsers和DenyUsers参数包含了同一个用户，因拒绝策略优先，所以该用户无法登录。
- 如果AllowUsers中的用户在DenyGroups用户组中，因拒绝策略优先，所以该用户无法登录。

处理方法

您可以修改SSH远程登录配置文件（/etc/ssh/sshd_config）中用户登录控制参数，以解决该问题。

1. 通过VNC方式登录Linux实例。
   详细操作，请参见**通过VNC登录Linux ECS**。
2. 执行以下命令，查看sshd_config文件。
   cat /etc/ssh/sshd_config
   系统显示类似如下，表示拒绝test用户登录。

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

3. 修改用户登录控制参数。
   a. 执行以下命令，打开SSH配置文件。
      vi /etc/ssh/sshd_config
   b. 根据业务需要，修改用户登录控制参数。
      如下所示，在策略配置前添加#，取消用户访问控制，以确保相关用户能够正常登录。

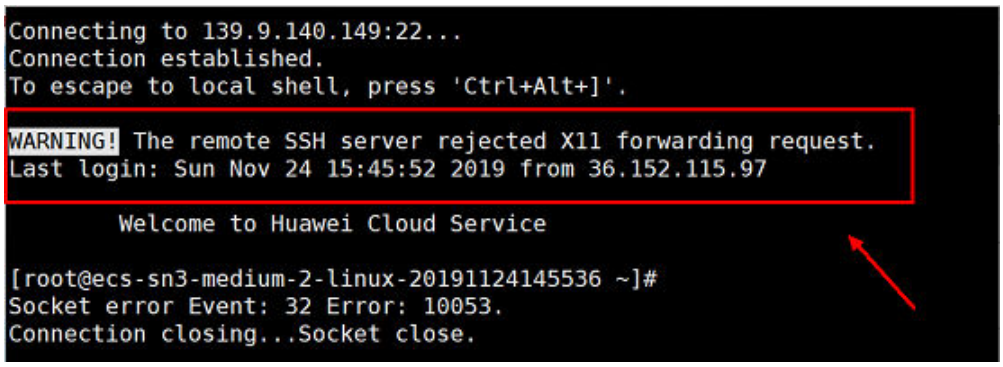
```
#AllowUsers root test
#DenyUsers test
#DenyGroups test
#AllowGroups root
```

   c. 按Esc键，输入:wq保存修改。
4. 重新登录Linux实例，确保可以正常登录。

4.3.12 使用 Xshell 连接不上云服务器，提示“WARNING! The remote SSH server rejected X11 forwarding request.”报错

问题描述

使用Xshell连接不上云服务器，提示“WARNING!The remote SSH server rejected X11 forwarding request.”报错，具体报错信息如下图所示。



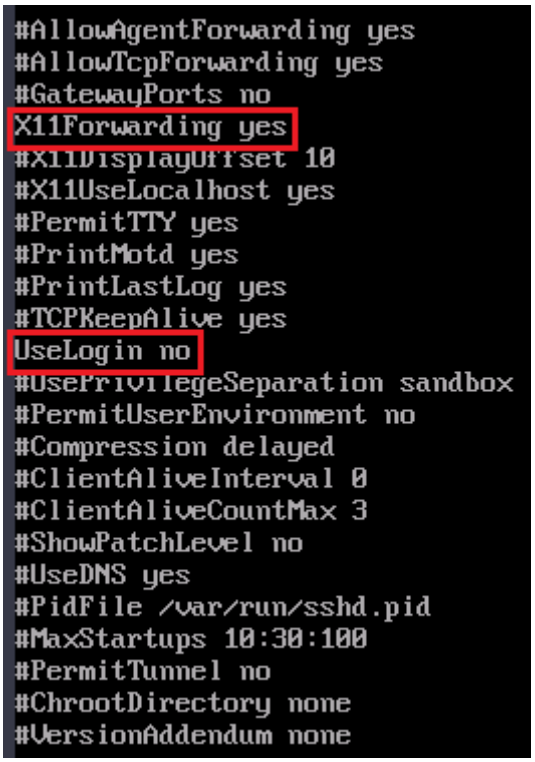
可能原因

openssh版本进行了升级。

处理方法

1. 登录弹性云服务器。
2. 执行以下命令，编辑/etc/ssh/sshd_config文件。
   vi /etc/ssh/sshd_config
3. 修改如下配置项：
   - X11Forwarding参数修改为：yes
   - UseLogin参数去掉前面的注释，并修改取值为no

   修改结果如下图所示：



4. 执行以下命令，重启ssh服务。

   systemctl restart sshd

5. 执行以下命令，安装xorg-x11-xauth软件包。

   yum install xorg-x11-xauth

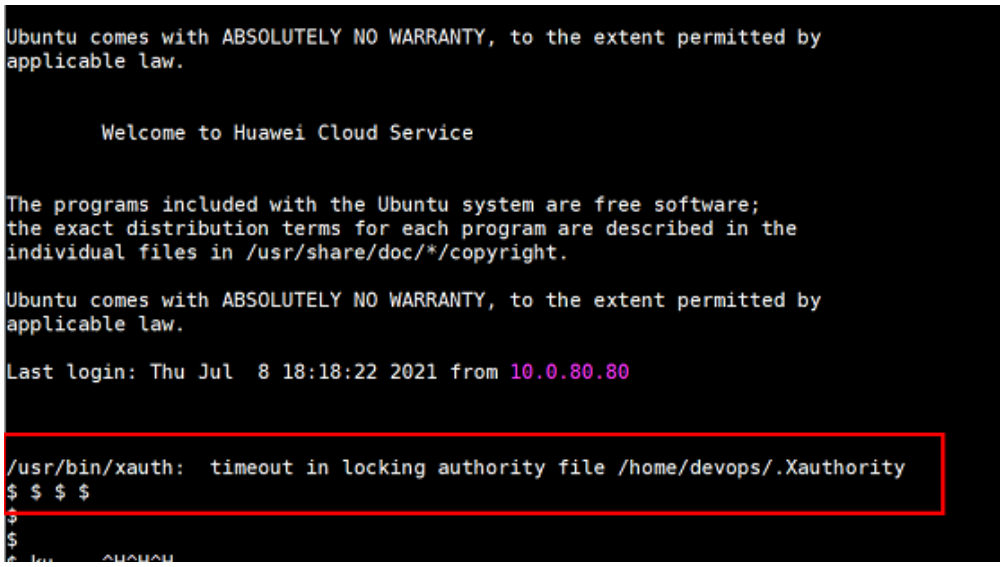
6. 重启云服务器。

   reboot

4.3.13 SSH 登录 Linux 云服务器时提示“/usr/bin/xauth: timeout in locking authority file /home/user/.Xauthority”报错

问题描述

SSH登录Linux云服务器时提示“/usr/bin/xauth: timeout in locking authority file /home/user/.Xauthority”报错，具体报错信息如下图所示。



可能原因

通常是因为在创建用户时，用户家目录属组和属主不对导致。

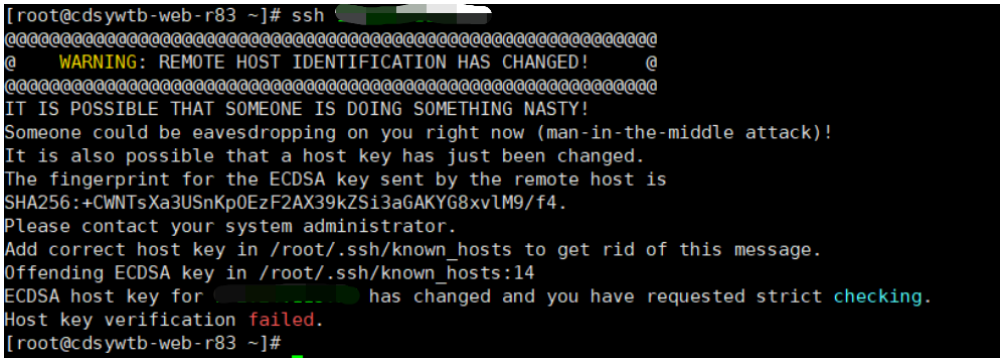
处理方法

1. 登录弹性云服务器。
2. 执行以下命令，给用户家目录赋予用户的所有权限。
   chown -R devops:devops /home/devops
3. 重启云服务器。
   reboot

4.3.14 SSH 远程登录 Linux 云服务器时提示报错：WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!

问题描述

使用SSH登录Linux云服务器时，提示“WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!”错误，具体报错信息如下图所示。


[root@cdsywtb-web-r83 ~]# ssh
@@@

可能原因

第一次进行SSH连接时，会将服务器的公钥信息保存在客户端中的~/.ssh/known_hosts中。但如果服务器重新安装过或认证信息发生变化，这时候服务器和客户端的公钥信息不匹配时，就会出现以上错误。

处理方法

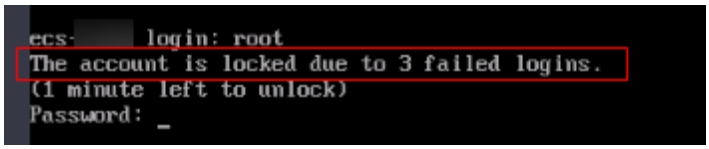
1. 登录弹性云服务器。
2. 执行以下命令，清除旧的公钥信息。
   ssh-keygen -R 服务器IP地址

4.3.15 远程连接 Linux 云服务器报错：The account is locked due to 3 failed logins

问题描述

远程连接Linux云服务器时，提示：The account is locked due to 3 failed logins。

图 4-86 报错信息



可能原因

远程登录Linux云服务器时，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，无法成功登录。

排查思路

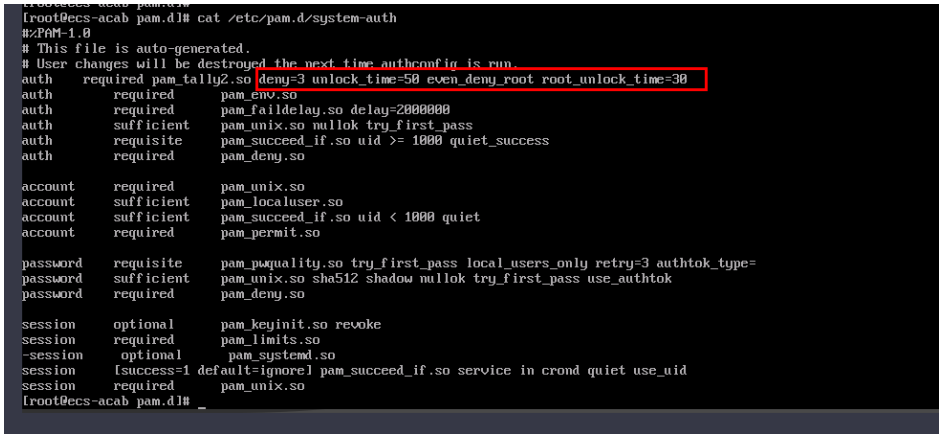
1. （可选）解锁root用户。
   若root用户被锁定，则需参考本步骤解锁root用户。否则跳过本步骤。
   a. 使用单用户模式登录ECS。
      具体操作，请参见**Linux云服务器如何进入单用户模式?** 。
   b. 依次执行以下命令，解锁root用户。
      pam_tally2 -u root #查看root用户登录密码连续输入错误次数。
      pam_tally2 -u root -r #清除root用户密码连续输入错误次数。
      authconfig --disableldap --update #更新PAM安全认证记录。
   c. 执行以下命令，重启ECS，使修改生效。
      reboot -f
2. 使用root用户登录弹性云服务器。
   详细操作，请参见**通过VNC登录Linux ECS**。
3. 执行以下命令，查看PAM配置文件中是否存在认证限制。
   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。

例如，当系统返回如下信息时，表示普通用户和root用户连续三次输入错误密码，30秒后才能再次登录Linux实例。

图 4-87 返回结果



处理方法

- 方法一：等待PAM设置的冻结时长（例如50秒），待系统解冻账户后，再重新登录实例。
- 方法二：修改配置文件。

  下文以修改“/etc/pam.d/system-auth”为例进行说明，其他配置文件修改方法类似。

  a. 执行以下命令，打开“/etc/pam.d/system-auth”配置文件。

  vim /etc/pam.d/system-auth

  b. 按“i”进入编辑模式。

  c. 根据业务需要，注释、修改或删除该配置。

  配置文件中，该配置信息表示普通用户和root用户连续三次输入错误密码会被锁定，30秒后才能解锁：

  ```
  auth required pam_tally2.so deny=3 unlock_time=30 even_deny_root root_unlock_time=30
  ```

  注释该配置信息：

  ```
  #auth required pam_tally2.so deny=3 unlock_time=30 even_deny_root root_unlock_time=30    #注释后代码
  ```

  配置解释：

  - deny=3：表示设置普通用户和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=30：表示设定普通用户锁定后，多少时间后解锁，单位是秒。
  - even_deny_root：表示也限制root用户。
  - root_unlock_time=30：表示设定root用户锁定后，多少时间后解锁，单位是秒。

说明

本示例使用的是pam_tally2模块，不同的PAM版本，设置可能有所不同，详情请参见**Linux PAM SAG**。

5 网络配置

5.1 CentOS 7 重启后 dhclient 未运行，导致无法获取 IP

问题描述

云服务器启动后dhclient未运行导致IP无法获取。

问题分析

重启后dhclient进程未运行的根因通常为：

1. NetworkManager未开启自启动导致dhclient进程未运行。
2. 网卡设备未纳入NetworkManager管理导致。

约束与限制

本节操作适用于CentOS 7系列、EulerOS 2系列、Ubuntu18.04操作系统的云服务器，并使用DHCP获取IP。

处理方法

1. 执行以下命令，确认dhclient是否运行。

   ps -ef |grep dhclient |grep -v grep

2. 如果未找到dhclient进程，则确认dhclient进程未运行，执行以下命令，继续排查NetworkManager是否运行。

   systemctl status NetworkManager

   - 如果NetworkManager的状态为Active: inactive (dead)，则NetworkManager未启动，执行以下命令，检查该服务是否开机自启。

     systemctl is-enabled NetworkManager

     结果为disabled则确认为NetworkManager未设置开机自启导致，执行以下命令进行恢复。

     systemctl enable NetworkManager && systemctl start NetworkManager

- 如果NetworkManager的状态为Active: active (running)，执行以下命令查看网卡设备是否被NetworkManager管理。

  nmcli device status

  如果显示该网卡为的STATE为unmanaged，则该网卡设备未被NetworkManager管理，执行以下命令进行恢复。

  nmcli device set eth0 managed yes

3. 执行以下命令重启NetworkManager。

   systemctl restart NetworkManager

4. 执行以下命令查看ip是否已经获取。

   ip add

5.2 Linux 私有镜像网卡漂移问题处理

适用场景

使用CentOS 6操作系统的私有镜像创建的云服务器启动后第一个网卡不是eth0而是eth1。

本节的处理方法中有重启云服务器的操作，重启云服务器会造成业务中断，请谨慎操作。

根因分析

/etc/udev/rules.d/70-persistent-net.rules文件记录的为旧的网卡IP与MAC地址对应关系，因此需禁用该规则。

处理方法

1. 禁用udev网卡生成器的正确方法是使用空文件覆盖它， /etc/udev/rules.d中的任何规则都将优先于/lib/udev/rules.d中的规则，因此只需创建一个空文件即可。

   touch /etc/udev/rules.d/75-persistent-net-generator.rules

2. 重启服务器。

   reboot

5.3 Linux 系统重启后/etc/hosts 自动添加主机名解析

问题现象

云服务器/etc/hosts文件中在重启后自动添加hostname和127.0.0.1的解析，导致自行添加的本地解析出现问题。

根因分析

/etc/cloud/cloud.cfg中对/etc/hosts文件影响的配置如下：

```
manage_etc_hosts: localhost
```

此配置为自动生成hostname和本地回环地址的解析，用于在未配置内网DNS情况下的启动加速，如果该配置影响到业务可以取消该配置。

解决方法

1. 打开/etc/cloud/cloud.cfg文件
   注释掉manage_etc_hosts配置项，如下：
   原文：
   ```
   manage_etc_hosts:localhost
   ```
   修改后：
   ```
   #manage_etc_hosts:localhost
   ```

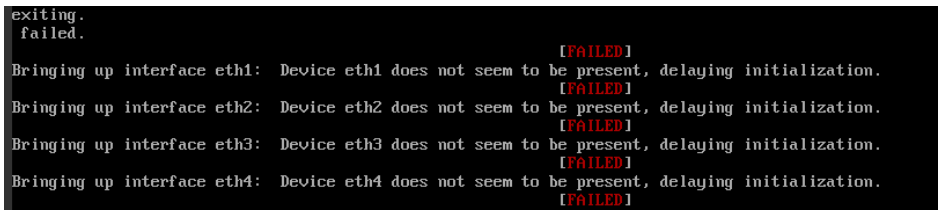
2.删除/etc/hosts中的127.0.0.1 hostname hostname的解析。

5.4 多网卡配置文件导致 network 启动失败处理

问题现象

重启或启动network后出现报错：Device eth1 does not seem to be present，或no suitable device found for this connection

图 5-1 network 启动失败



适用场景

CentOS、RedHat、Euleros系列操作系统。

约束与限制

该文档中涉及重启网卡的操作，重启网卡会出现网络暂时断开，请谨慎操作。

根因分析

启动network时会读取/etc/sysconfig/network-scripts目录下的网卡配置文件，如果系统存在多网卡配置文件，会因为找不到对应的网卡设备导致network启动失败。

处理方法

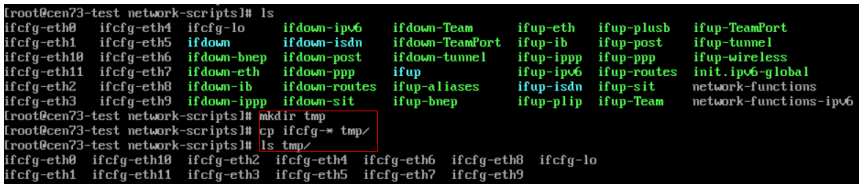
备份多余的网卡，然后删除/etc/sysconfig/network-scripts目录下多余的网卡配置文件。

1. 执行以下命令，进入该网卡配置文件目录。
   本例中查看云服务器内部包含11个网卡配置文件。
   cd /etc/sysconfig/network-scripts
2. 执行以下命令备份网卡文件。
   mkdir tmp

cp ifcfg-* tmp/

ls tmp/

图 5-2 查看网卡配置文件

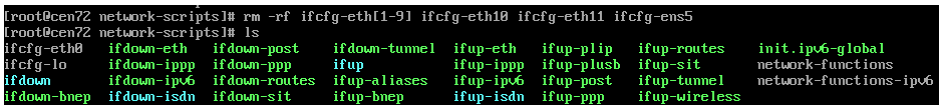


3. 如果只使用一张网卡，则删除ifcfg-eth0外多余的网卡配置文件，如果有ifcfg-ens5配置文件也需要删除。

   本例以删除ifcfg-eth1到ifcfg-eth11，和ifcfg-ens5为例，请根据实际网卡配置情况更新命令。

   rm -rf ifcfg-eth[1-9] ifcfg-eth10 ifcfg-eth11 ifcfg-ens5

   图 5-3 删除多余的配置文件



4. 结束多余的dhclient进程。

   a. 查询dhclient进程

      ps -ef | grep dhclient

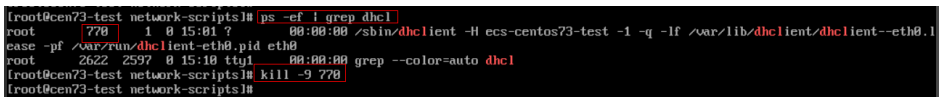
   b. 以PID为770 为例，执行以下命令结束该进程。

      kill -9 770

   注意

   - 请注意正确拼写服务的PID。
   - **kill -9 PID**表示强制结束进程。

   图 5-4 结束 dhclient 进程



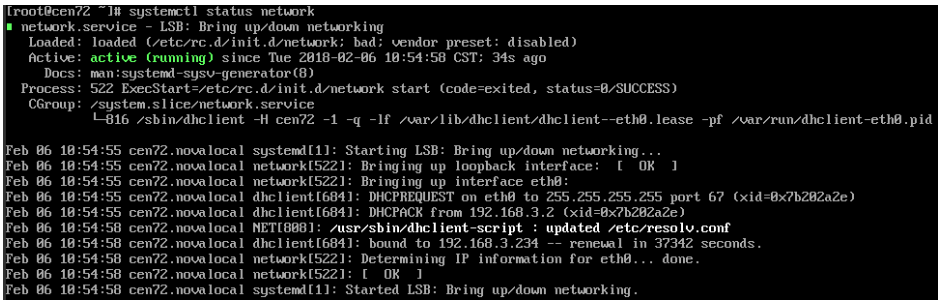
5. 重启network服务。

   systemctl restart network

6. 查看network网络状态恢复正常。

   systemctl status network

图 5-5 查看 network 网络状态



5.5 Linux 系统 ping 域名失败，提示 Name or service not known

问题现象

ping公网域名失败，提示Name or service not known，但可以ping通弹性公网IP。

根因分析

出现该问题通常有三个原因：

- /etc/resolv.conf未配置DNS地址或者DNS地址错误导致。
- /etc/nsswitch.conf文件删除DNS解析记录导致。
- /lib64/libnss_dns.so.2库文件丢失导致无法解析域名。

说明

执行以下命令，查看解析域名打开的所有文件。

strace -e trace=open ping www.baidu.com -c 1

该结果中出现的所有文件都会影响域名解析。

适用场景

CentOS、EulerOS系列操作系统。

处理方法

- 场景一：/etc/resolv.conf未配置DNS地址或者DNS地址错误导致。

  /etc/resolv.conf中最关键的是nameserver项，如果没指定nameserver就找不到DNS服务器，其它关键字是可选的。

  nameserver表示解析域名时使用该地址指定的主机为域名服务器。其中域名服务器是按照文件中出现的顺序来查询的，且只有当第一个nameserver没有反应时才查询下一个的nameserver。

  请检查/etc/resolv.conf中配置的DNS地址。

- 场景二：/etc/nsswitch.conf文件删除DNS解析记录导致。

  a. 检查/etc/nsswitch.conf是否有DNS解析配置。

  grep hosts /etc/nsswitch.conf

回显信息如下所示，hosts行中未配置DNS选项，导致解析域名时不会读取/etc/resolv.conf，导致域名解析失败。

```
#hosts:     db files nisplus nis dns
hosts:      files myhostname
```

b. 打开/etc/nsswitch.conf找到hosts行添加DNS解析。

```
#hosts:     db files nisplus nis dns
hosts:      files dns myhostname
```

说明

hosts项的值代表按优先级顺序列出服务，这些服务用于查找域名的IP地址。

“file”表示使用/etc/hosts文件，“ dns”表示使用域名服务。如果“file”位于“ dns”之前，则意味着系统将首先尝试在/etc/hosts中查找域名，然后才通过DNS查找（这是默认配置）。如果未配置dns则不会使用DNS查找。

- 场景三：/lib64/libnss_dns.so.2库文件丢失导致无法解析域名。

a. /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

说明

在正常的Linux系统执行 **rpm -qf /lib64/libnss_dns.so.2**生成库文件。

回显信息如下所示，说明/lib64/libnss_dns.so.2文件缺失。

```
missing     /lib64/libnss_dns.so.2
```

b. 执行以下命令，重新建立软链接。

说明

在正常的云服务器上执行ls -l /lib64/libnss_dns.so.2可知/lib64/libnss_dns.so.2的源文件为/usr/lib64/libnss_dns-2.17.so。

ln -s /usr/lib64/libnss_dns-2.17.so /usr/lib64/libnss_dns.so.2

5.6 同一子网的两块网卡均绑定弹性公网 IP

问题描述

云服务器上两块相同子网的网卡，均绑定了弹性公网IP。其中，主网卡绑定的弹性公网IP可以正常访问，但是扩展网卡的弹性公网IP无法访问。

可能原因

CentOS操作系统的弹性云服务器默认开启了反向过滤技术（rpfilter），云服务器的默认路由是指向eth0的，而扩展网卡弹性公网IP的流量从eth1进入。系统此时判断，这个报文在发送时应该从eth0口送出，而报文实际是从eth1进入，即从错误的网卡收到报文，故判定非法而被系统丢弃。

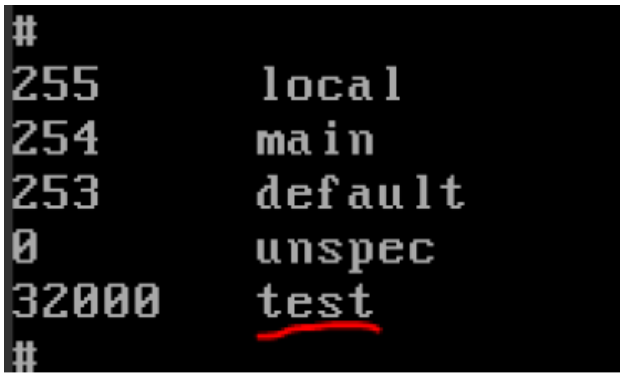
处理方法

通过策略路由让访问扩展网卡的流量从扩展网卡发出，方法如下：

1. 执行以下命令，编辑文件rt_tables。

   vi /etc/iproute2/rt_tables

添加一个route table的别名，如test。



2. 保存后退出。
3. 执行以下命令，在test表中添加路由。

   ip route add default via *扩展网卡网关* dev eth1 table *步骤1中添加的表名*

   例如：

   ip route add default via 192.168.166.1 dev eth1 table test
4. 执行以下命令，添加策略路由。

   ip rule add from *扩展网卡IP地址* lookup *步骤1中添加的表名* prio *低于32766，优先级高于main表*

   例如：

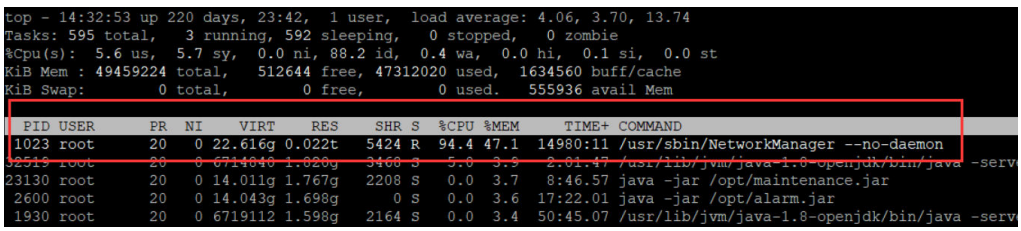
   ip rule add from 192.168.166.22 lookup test prio 32000

   至此，两块网卡上的公网IP应该都可以访问了。如果要持久化这个规则，可以将上述语句添加到开机脚本“/etc/rc.local”中。

5.7 NetworkManager 在运行 docker 容器时占用大量内存怎么办?

问题现象

在运行多个docker容器的环境下NetworkManager服务占用内存很大，导致内存使用率过高。



说明

- 本节操作适用于CentOS 7、Ubuntu 16.04操作系统。
- 该文档涉及重启网络服务，可能会造成业务中断，请谨慎操作。

问题分析

NetworkManager消耗的内存量随着容器启动/停止的每次迭代而增加，即使在所有容器已被停止和删除之后也不会减少。

处理方法

短期处理方法：

执行以下命令重启NetworkManager服务。

systemctl restart NetworkManager

长期处理方法：

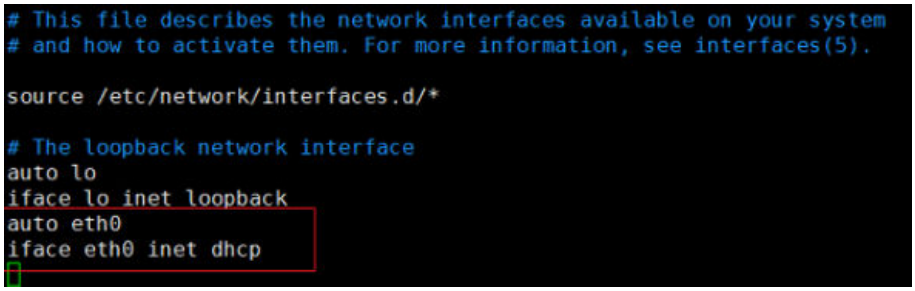
- CentOS 7操作系统云服务器
  执行以下命令停止NetworkManager服务，改用network管理网络
  systemctl disable NetworkManager
  /sbin/chkconfig network on
  kill `pgrep -o dhclient`
  systemctl stop NetworkManager
  systemctl start network

  说明

  出现network启动失败可能为系统内置多网卡配置文件导致，处理方法参考**多网卡配置文件导致network启动失败处理**。
- Ubuntu16.04操作系统
  a. 执行以下命令使用networking管理网络。
     systemctl disable NetworkManager
     systemctl disable network-manager
     systemctl enable networking
     kill `pgrep -o dhclient`
     systemctl stop NetworkManager
     systemctl start networking
  b. 启用networking服务，一定要检查interfaces文件中是否设置网络配置为DHCP模式。
     vi /etc/network/interfaces
     若只有一个网卡eth0则可以检查或增加：

```
auto eth0
iface eth0 inet dhcp
```

图 5-6 设置网络配置为 DHCP 模式



5.8 系统时间跳变导致 IP 丢失怎么办?

问题描述

修改系统时间后服务器网卡出现感叹号，无法连接网络。

适用场景

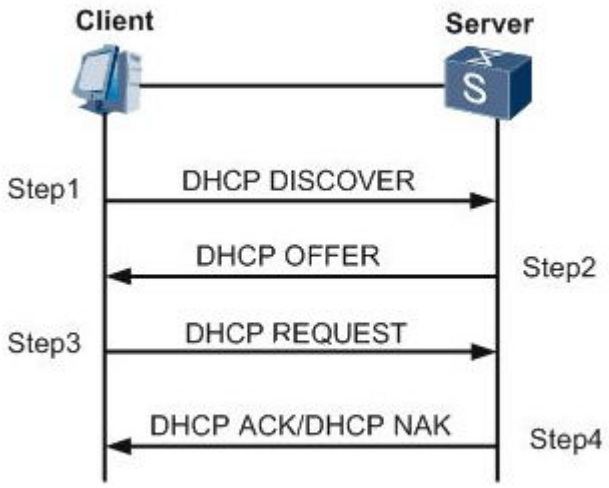
- 该文档适用于CentOS 7、EulerOS，并使用DHCP协议获取IP场景。
- DHCP租约通常默认为24小时，具体以实际场景为例。

根因分析

DHCP会话过程：

DHCP典型会话过程包括：DHCP发现、DHCP提供、DHCP请求、DHCP确认，如图1所示

图 5-7 DHCP 会话过



- DHCP发现（DISCOVER）

  客户在物理子网上发送广播来寻找可用的服务器。网络管理员可以配置一个本地路由来转发DHCP包给另一个子网上的DHCP服务器。该客户实现生成一个目的地址为255.255.255.255或者一个子网广播地址的UDP包。

- DHCP提供（OFFER）

  当DHCP服务器收到一个来自客户的IP租约请求时，它会提供一个IP租约。DHCP为客户保留一个IP地址，然后通过网络单播一个DHCPOFFER消息给客户。该消息包含客户的MAC地址、服务器提供的IP地址、子网掩码、租期以及提供IP的DHCP服务器的IP。

- DHCP请求（REQUEST）

当客户PC收到一个IP租约提供时，它必须告诉所有其他的DHCP服务器它已经接受了一个租约提供。因此，该客户会发送一个DHCPREQUEST消息，其中包含提供租约的服务器的IP。当其他DHCP服务器收到了该消息后，它们会收回所有可能已提供给客户的租约。然后它们把曾经给客户保留的那个地址重新放回到可用地址池中，这样，它们就可以为其他计算机分配这个地址。任意数量的DHCP服务器都可以响应同一个IP租约请求，但是每一个客户网卡只能接受一个租约提供。

- DHCP确认（Acknowledge，ACK）

  当DHCP服务器收到来自客户的REQUEST消息后，它就开始了配置过程的最后阶段。这个响应阶段包括发送一个DHCPACK包给客户。这个包包含租期和客户可能请求的其他所有配置信息。这时候，TCP/IP配置过程就完成了。

定位过程

1. 查看客户端DHCP请求记录

   grep -E "dhclient|DHCP" /var/log/messages

   图 5-8 DHCP 请求记录

   ```
   May 12 11:59:39 yth5_test_sl dhclient[7376]: DHCPREQUEST on eth0 to 10.10.3.254 port 67 (xid=0x1880414e)
   May 12 11:59:39 yth5_test_sl dhclient[7376]: DHCPACK from 10.10.3.254 (xid=0x1880414e)
   May 12 11:59:39 yth5_test_sl dhclient[7376]: bound to 10.10.3.240 -- renewal in 33696 seconds.
   ```

   - dhclient续租记录显示在5月12日重新续租成功（当时正确的时间为4月26日，系统时间是被手动修改过）。
   - dhclient记录下一次续租发生在33696秒后（约9小时21分，通常为租约的1/2时发出续租请求），即下次续租发生在5月12日21点21分左右。

   须知

   也可以通过查询dhclient租约信息记录文件，每一次续租成功都会记录在该文件中。执行以下命令查询文件的保存路径（文件以.lease结尾）。

   ps -ef |grep dhclient

2. 继续查看系统日志（messages）发现在续租后的5小时14分后系统时间发生跳变，回退至4月26日，但是由于下次续租请求发生在16天后，但是在9小时后未发出续租请求，租约到期后ip被DHCP服务端回收，导致ip丢失。

   grep "Time has been changed" /var/log/messages

   图 5-9 系统日志

   ```
   May 12 17:05:32 yth5_test_sl systemd-logind: Removed session 2508.
   May 12 17:13:16 yth5_test_sl systemd-logind: New session 2509 of user root.
   May 12 17:13:16 yth5_test_sl systemd: Started Session 2509 of user root.
   May 12 17:13:16 yth5_test_sl systemd: Starting Session 2509 of user root.
   Apr 26 17:49:38 yth5_test_sl systemd: Time has been changed
   Apr 26 17:53:50 yth5_test_sl systemd-logind: Removed session 2509.
   Apr 26 17:58:59 yth5_test_sl systemd-logind: New session 2510 of user rundeck.
   Apr 26 17:58:59 yth5_test_sl systemd: Started Session 2510 of user rundeck.
   ```

处理方法

1. 手动执行dhclient，获取私有ip地址。

   dhclient -r eth0

   ifconfig eth0 down

ifconfig eth0 up
dhclient eth0

⚠ 注意

该操作可能会导致网络短暂中断，请谨慎操作。

2. 重启服务器，系统时间会恢复正常，系统会重新获取IP地址。
3. 参考**NTP服务器配置**做ntp时间同步。

5.9 resolv 文件被重置怎么办?

问题现象

修改resolv.conf文件，当服务器重启后，resolv.conf文件被重置。

解决方法

执行以下命令，给resolv文件添加i属性，该命令修改文件属性为只有 root 用户才能修改该文件。

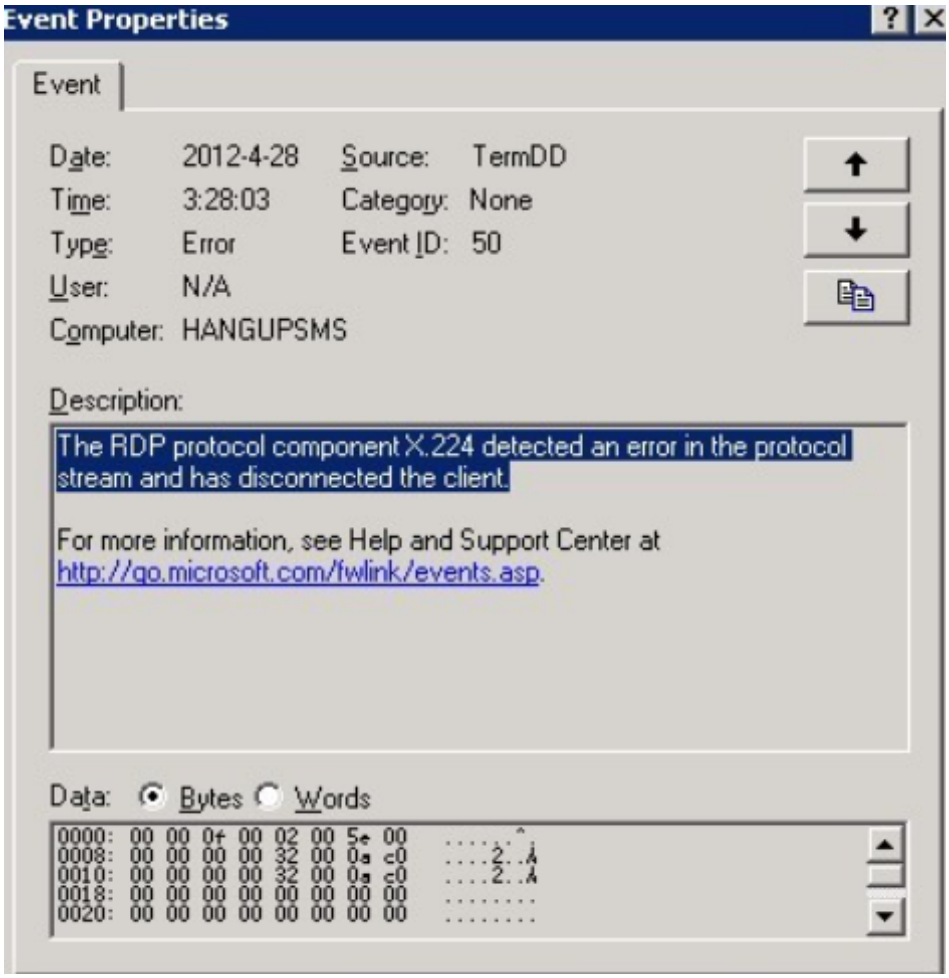
chattr +i /etc/resolv.conf

5.10 为什么弹性云服务器可以 ping 通，但是无法远程连接?

问题描述

弹性云服务器可以ping通，但是无法远程连接。

具体报错信息如下图所示。



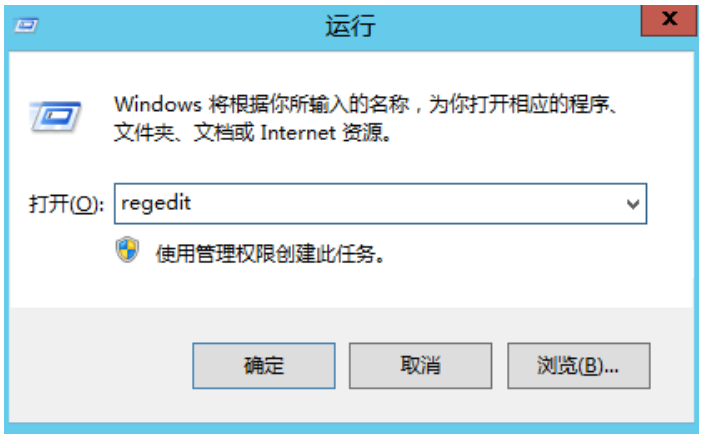
可能原因

注册表中的“Certificate”子键被损坏，导致用户无法与终端服务进行正常通信。Certificate子键负责终端服务通信中数据信息的认证和加密，它一旦被损坏，终端服务的协议组件就会检测到错误，中断客户机与终端服务器之间的通信。

处理方法

1. 在运行窗口输入“regedit”回车，打开注册表编辑器。

图 5-10 打开注册表



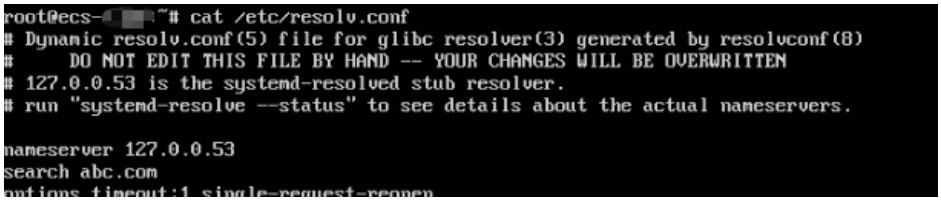
2. 找到HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TermService\Parameters键值。
3. 删除Certificate键值。
4. 重启云服务器。服务器在重新启动后会自动创建该键。

5.11 Ubuntu 系统 ECS 重启后“/etc/resolv.conf”被还原怎么办?

问题描述

在重启Ubuntu系统的ECS或者重启网络相关服务后，手动修改的/etc/resolv.conf文件被刷新，nameserver字段被还原成127.0.0.53。

图 5-11 问题现象



根因分析

Ubuntu系统相关版本默认使用systemd-resolved服务维护DNS，重启云服务器或者重启网络相关服务会导致/etc/resolv.conf文件被刷新成systemd-resolved服务维护的127.0.0.53地址。

处理方法

说明

在处理前，建议先禁用systemd-resolved服务。

方法一：手动修改/etc/resolv.conf文件。

1. 以root用户登录ECS。

2. 关闭并禁用systemd-resolved服务。

   systemctl stop systemd-resolved

   systemctl disable systemd-resolved

3. 默认的/etc/resolv.conf是软链接，删除重建为普通文件。

   rm -rf /etc/resolv.conf

4. 编辑/etc/resolv.conf，增加相关DNS配置。

   vim /etc/resolv.conf

   通过添加自定义的nameserver参数增加DNS配置，如下所示：

   ```
   nameserver 100.125.1.250
   nameserver 100.125.129.250
   ```

5. 将/etc/resolv.conf配置文件加锁，防止被dhcp或者其他服务更改。

   chattr +i /etc/resolv.conf

方法二：使用NetworkManager根据dhcp获取的DNS信息（vpc子网中配置的DNS信息）维护/etc/resolv.conf文件。

1. 关闭并禁用systemd-resolved服务。

   systemctl stop systemd-resolved

   systemctl disable systemd-resolved

2. 编辑NetworkManager配置文件，增加dns=default配置。

   vim /etc/NetworkManager/NetworkManager.conf

   ```
   [main]
   plugins=ifupdown,keyfile
   dns=default

   [ifupdown]
   managed=true

   [device]
   wifi.scan-rand-mac-address=no
   ```

3. 默认的/etc/resolv.conf是软链接，删除重建为普通文件。

   rm -rf /etc/resolv.conf

4. 重启NetworkManager，刷新/etc/resolv.conf文件。

   systemctl restart NetworkManager

5. 检查/etc/resolv.conf中的dns相关配置。
   - 如果与云服务器所属子网下的DNS配置一致，代表修改成功。

     您可以登录控制台，在弹性云服务器详情页，单击网卡区域的主网卡名称，即可跳转至子网控制台，切换至“基本信息”页签，即可查看到“DNS服务器地址”信息。
   - 如果不一致，请提交工单联系技术支持处理。

6 磁盘空间管理

6.1 CentOS 7 中修改 fstab 无法挂载怎么办?

问题现象

添加新硬盘修改/etc/fstab以将新硬盘安装到旧挂载点，然后umount旧磁盘，执行**mount -a**后使用**df**查看没有挂载成功。

本节操作适用于CentOS、EulerOS操作系统。

根因分析

1. 执行以下命令，查询有问题的mount unit。

   systemctl list-units --type=mount |grep failed

   ```
   test1.mount           loaded failed failed  /test1
   ```

2. 执行以下命令，查询该unit的状态。

   systemctl status test1.mount

   回显信息如下所示：

   ```
   ● test1.mount - /test1
   Loaded: loaded (/etc/fstab; bad; vendor preset: disabled)
   Active: failed (Result: exit-code) since Wed 2019-08-28 15:32:53 CST; 3min 27s ago
   Where: /test1
   What: /dev/vdb1
   Docs: man:fstab(5)
   man:systemd-fstab-generator(8)
   Process: 4601 ExecUnmount=/bin/umount /test1 (code=exited, status=0/SUCCESS)
   Process: 3129 ExecMount=/bin/mount /dev/vdb1 /test1 -t ext4 (code=exited, status=0/SUCCESS)
   ... ...
   Warning: test1.mount changed on disk. Run 'systemctl daemon-reload' to reload units.
   ```

   如回显信息所示test1.mount磁盘发生了改变，需要运行**systemctl daemon-reload**重新加载units。

   更改/etc/fstab时，必须执行**systemctl daemon-reload**。在运行该命令之前，systemd不读取fstab并生成装载单元。

处理方法

执行以下命令，重新加载systemd管理的unit配置。

systemctl daemon-reload

6.2 Linux 如何创建 swap 分区/swap 文件

适用场景

本节操作以CentOS 6.8操作系统云服务器为例，指导用户创建swap分区。

约束与限制

操作过程中涉及创建指定大小的文件，请确认系统磁盘空间有足够的空余空间。

场景一：使用块设备创建 swap

1. 执行以下命令，新建一个分区（以2G为例）。

   fdisk /dev/vdb

   回显信息如下：

   ```
   Command (m for help): n
   Partition type:
     p   primary (0 primary, 0 extended, 4 free)
     e   extended
   Select (default p):
   Using default response p
   Partition number (1-4, default 1):
   First sector (2048-20971519, default 2048):
   Using default value 2048
   Last sector, +sectors or +size{K,M,G} (2048-20971519, default 20971519): +2G
   Partition 1 of type Linux and of size 2 GiB is set
   Command (m for help): p

   Disk /dev/vdb: 10.7 GB, 10737418240 bytes, 20971520 sectors
   Units = sectors of 1 * 512 = 512 bytes
   Sector size (logical/physical): 512 bytes / 512 bytes
   I/O size (minimum/optimal): 512 bytes / 512 bytes
   Disk label type: dos
   Disk identifier: 0x1f02f438

     Device Boot      Start         End      Blocks   Id  System
       /dev/vdb1       2048     4196351     2097152   83   Linux

   Command (m for help): w
   The partition table has been altered!

   Calling ioctl() to re-read partition table.
   Syncing disks.
   ```

2. 执行以下命令，将新建的分区创建为swap。

   mkswap /dev/vdb1

3. 执行以下命令，激活swap分区。

   swapon /dev/vdb1

4. 执行以下命令，查询已启动的swap。

   swapon -s

5. 执行以下命令，查询swap分区UUID。

   blkid |grep swap |awk '{print $2}'

   ```
   UUID="1ee90e3c-1538-453b-9240-ad430f835f6f"
   ```

6. 执行以下命令，实现swap开机自动挂载，将挂载信息写入/etc/fstab。

   swap的UUID从步骤**4.执行以下命令，查询swap分区UUID。**获取。本例中执行命令如下。

   echo "UUID=*1ee90e3c-1538-453b-9240-ad430f835f6f* swap swap defaults 0 0" >>/etc/fstab

7. 执行以下命令，挂载swap。

   mount -a

场景二：使用文件模拟的块设备做 swap 分区

说明

使用文件模拟的块设备做swap性能较之直接使用块设备性能较差。

1. 执行以下命令，创建1G的swap文件。

   dd if=/dev/zero of=/swapfile bs=1M count=1000

2. 执行以下命令，更改文件为swap。

   chmod 600 /swapfile

3. 执行以下命令，更改文件属性为swap。

   mkswap /swapfile

4. 执行以下命令，启用swap。

   swapon /swapfile

5. 执行以下命令，实现swap开机自动挂载，将swap文件挂载写入/etc/fstab。

   echo "/swapfile swap swap defaults 0 0" >>/etc/fstab

6. 执行以下命令，挂载swap。

   mount -a

6.3 文件已经删除，但空间未释放怎么办?

问题现象

Linux操作系统云服务器根目录空间占用率过高。例如，以**图6-1**为例，根目录空间占用率为96%。

图 6-1 根目录空间占用率过高

```
[root@host1 /]#df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda2        49G   47G   2G   96%   /
tmpfs            16G     0   16G    0%   /dev/shm
```

查询当前系统存在一个约42G大小的文件access_log，这个文件是apache产生的访问日志文件，从日志大小判断是很久没有清理的apache日志文件了。

1. 执行以下命令删除access_log。

   rm /tmp/access_log

2. 执行以下命令查看文件系统使用率。
   df -h

删除该文件后使用df查看文件系统使用率仍是96%。

根因分析

通常不会出现删除文件后空间不释放的情况，特殊情况是文件进程锁定，或有进程一直在向这个文件写数据。

为了分析根因，首先需要了解Linux文件的存储机制和存储结构。

一个文件在文件系统中存放分为两个部分：

- 指针部分：指针位于文件系统的meta-data中，在将数据删除后，这个指针就从meta-data中清除了。
- 数据部分：而数据部分存储在磁盘中。

将数据对应的指针从meta-data中清除后，文件数据部分占用的空间就可以被覆盖并写入新的内容。出现删除access_log文件后，空间还没有释放的原因，是因为httpd进程还在一直向这个文件写入内容，导致删除了access_log文件后，进程锁定，文件对应的指针部分并未从meta-data中清除，由于指针并未删除，系统内核就默认文件并未被删除，因此查询文件系统使用率时，显示空间并未释放。

处理方法

1. 使用lsof命令查看是否有进程一直在向access_log文件中写入数据。
   lsof -n |grep delete

   图 6-2 查看写入进程

   ```
   [root@host1 /]#lsof -n|grep delete
   COMMAND  PID  USER   FD  TYPE  DEVICE  SIZE     NODE       NAME
   httpd   2660  root   4u  REG     8,2   43289765 /access_log (deleted)
   ```

   如回显信息所示，/tmp/access_log 文件被进程httpd锁定，而httpd进程还一直向这个文件写入日志数据，最后一列的“deleted”状态说明这个日志文件已经被删除，但是由于进程还在一直向此文件写入数据，因此空间并未释放。
2. 可以选择关闭或者重启httpd进程，或重启操作系统。推荐在线清空**access_log**。
   执行以下命令清空**access_log**。
   echo ">/access_log
   通过这种方法，磁盘空间不但可以马上释放，也可以保证进程继续向文件写入日志，再次执行**df -h**查看根分区空间已经释放。

   图 6-3 查看根目录空间占用率

   ```
   [root@host1 /]#df -h
   Filesystem      Size  Used  Avail  Use%  Mounted on
   /dev/sda2        49G   5G    44G   10%   /
   tmpfs            16G   0     16G   0%    /dev/shm
   ```


6.4 Linux 文件系统提示：Read-only file system

问题现象

Linux操作系统云服务器删除或者修改文件时提示文件系统只读：Read-only file system，导致操作失败。

```
[root@oss-vpc-network-om-elk-20 logstash]# rm -rf *2019*
rm: cannot remove ‘ logstash-plain-2019-01-18-1.log.gz’ : Read-only file system
rm: cannot remove ‘ logstash-plain-2019-01-19-1.log.gz’ : Read-only file system
rm: cannot remove ‘ logstash-plain-2019-01-20-1.log.gz’ : Read-only file system
rm: cannot remove ‘ logstash-plain-2019-01-21-1.log.gz’ : Read-only file system
rm: cannot remove ‘ logstash-plain-2019-01-22-1.log.gz’ : Read-only file system
rm: cannot remove ‘ logstash-plain-2019-01-23-1.log.gz’ : Read-only file system
rm: cannot remove ‘ logstash-plain-2019-01-23-2.log.gz’ : Read-only file system
rm: cannot remove ‘ logstash-plain-2019-01-23-3.log.gz’ : Read-only file system
rm: cannot remove ‘ logstash-plain-2019-01-23-4.log.gz’ : Read-only file system
rm: cannot remove ‘ logstash-plain-2019-01-23-5.log.gz’ : Read-only file system
```

根因分析

文件系统只读的原因可能有：

- 文件系统错误导致文件系统进入只读模式。
- 文件系统是以只读方式进行的挂载。
- 硬件故障，包括磁盘有坏道或者Raid卡故障等硬件问题。

操作须知

- 修复文件系统，可能会产生数据丢失，请先备份数据后进行操作。
- 如以下场景均不符合，请检查存储或者磁盘硬件是否存在故障。

场景一：文件系统以只读方式挂载导致删除或者修改类操作失败

1. 执行以下命令，查看删除文件所在目录的挂载方式：

   mount |grep 挂载点

   如果结果显示挂载方式为ro，则根因为挂载方式为只读导致。
2. 在不重启的情况下可以以读写方式重新进行挂载，执行：

   mount -o remount,rw 挂载点

   说明

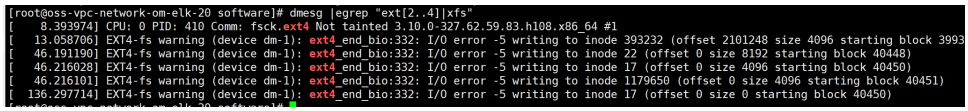
   如需在下次启动时也以读写方式挂载，需修改/etc/fstab文件中第四列参数。

场景二：如果结果显示挂载方式 rw，则确认是否为文件系统错误导致

1. 执行以下命令，检查内核中关于文件系统的信息。

   dmesg |egrep "ext[2..4]|xfs"

   输出结果中如果有I/O error ... inode 的错误信息则根因为文件系统错误导致进入只读模式。



如图所示，需要修复文件系统，请先备份数据后操作，由于文件系统在使用中无法修复，需要通过单用户模式（在该模式下磁盘未挂载）修复文件系统。

2. 重启进入**单用户模式**尝试修复文件系统。
3. 查询当前设备及文件系统

   blkid
4. 检查文件系统（以vdb1为例）。
   - ext系列文件系统执行以下命令

     fsck -n /dev/vdb1
   - xfs系列文件系统执行以下命令

     xfs_check /dev/vdb1

   说明

   如果遇到提示当前文件系统为mounted，需要先umount文件系统。

   1. 执行以下命令，查看当前挂载信息执行

      mount
   2. 卸载设备

      umount 挂载点
5. 修复文件系统（以vdb1为例）。
   - ext系列文件系统执行以下命令

     fsck /dev/vdb1
   - xfs系列文件执行以下命令

     xfs_repair /dev/vdb1

6.5 Inode 节点耗尽导致无法创建新文件问题处理

问题现象

创建文件或者目录时失败，提示没有可用空间：No space left on device，cannot create directory，Cloudn't create temporary archive name。

根因分析

Linux系统中对磁盘空间的占用分为以下两个方面：

- 物理磁盘空间。
- inode节点所占用的磁盘空间。

说明

inode（索引节点）保存了文件系统中的一个文件系统对象（包括文件、目录、设备文件、socket、管道等）的元信息数据，但不包括数据内容或者文件名。

处理方法

1. 执行以下命令，排查磁盘的物理空间是否已满。

   df -h

   图 6-4 检查磁盘物理空间

   ```
   mkdir: cannot create directory 'test': No space left on device
   [root@ecs-bbec data]# df -TH
   Filesystem     Type      Size  Used Avail Use% Mounted on
   /dev/vda2      ext4       42G  4.5G   35G  12% /
   devtmpfs       devtmpfs   17G     0   17G   0% /dev
   tmpfs          tmpfs      17G  4.1k   17G   1% /dev/shm
   tmpfs          tmpfs      17G  9.0M   17G   1% /run
   tmpfs          tmpfs      17G     0   17G   0% /sys/fs/cgroup
   /dev/vda1      ext4      1.1G  153M  801M  16% /boot
   tmpfs          tmpfs     3.4G     0  3.4G   0% /run/user/0
   /dev/vdb1      ext4      106G  990M  100G   1% /home/qis
   /dev/vdc1      ext4      106G   37G   64G  37% /home/data
   tmpfs          tmpfs     3.4G     0  3.4G   0% /run/user/1000
   ```

   如图6-4所示，磁盘空间还有剩余，排除物理磁盘空间已满的情形

2. 执行以下命令，查看系统可用的inode节点使用率。

   df -i

   当结果中的Use%为100%时则为inode耗尽，可以执行以下的操作步骤释放inode。

   a. 执行以下命令，将所有在目录文件进行归档。

      tar czvf /tmp/backup.tar.gz /home/data

   b. 删除对应目录下确认不需要的文件释放inode。

6.6 Linux 操作系统云服务器磁盘分区提示空间不足怎么办?

问题描述

在Linux操作系统云服务器中创建文件时提示空间不足：No space left on device

可能原因

- 磁盘分区block空间使用率达到100%。
- 磁盘分区inode空间使用率达到100%。
- 已删除文件因句柄被占用未释放导致相应空间未释放。
- fs.inotify.max_user_watches值耗尽

磁盘分区 block 空间使用率达到 100%

执行以下命令查看磁盘空间。

df -h

如回显信息如下所示说明block空间使用率100%。

解决方案：扩容云硬盘。

```
[root@ecs-linux-bj1 data1]# echo aaa > a
-bash: echo: write error: No space left on device
[root@ecs-linux-bj1 data1]# df -h .
Filesystem      Size  Used Avail Use% Mounted on
/dev/vdb1        89M   87M     0 100% /data1
[root@ecs-linux-bj1 data1]# df -i .
Filesystem     Inodes IUsed IFree IUse% Mounted on
/dev/vdb1       24480    13 24467    1% /data1
[root@ecs-linux-bj1 data1]#
```

磁盘分区 inode 空间使用率达到 100%

执行以下命令查看磁盘空间。

df -i

如回显信息如下所示说明inode空间使用率100%。

解决方案：扩容云硬盘。

```
[root@ecs-linux-bj1 data1]# touch bbb
touch: cannot touch 'bbb': No space left on device
[root@ecs-linux-bj1 data1]# df -i .
Filesystem     Inodes IUsed IFree IUse% Mounted on
/dev/vdb1       24480 24480     0  100% /data1
[root@ecs-linux-bj1 data1]# df -h .
Filesystem      Size  Used Avail Use% Mounted on
/dev/vdb1        89M   26M   56M  32% /data1
```

已删除文件因句柄被占用未释放导致相应空间未释放

1. 登录服务器，执行**df -h**查看磁盘block空间使用率为100%。
2. 执行**df -i**查看磁盘inode空间使用率较低，如下截图所示，本例inode空间使用率为1%。
3. 执行**du -sh**查看文件占用空间和磁盘可用空间相差较大。

```
[root@ecs-linux-bj1 data1]# echo aaaa >> a
-bash: echo: write error: No space left on device
[root@ecs-linux-bj1 data1]# df -h .
Filesystem      Size  Used Avail Use% Mounted on
/dev/vdb1        89M   87M     0 100% /data1
[root@ecs-linux-bj1 data1]# df -i .
Filesystem     Inodes IUsed IFree IUse% Mounted on
/dev/vdb1       24480    16 24464    1% /data1
[root@ecs-linux-bj1 data1]# du -sh .
6.9M    .
```

解决方案：

1. 执行以下命令，查找当前分区是否存在未被清除句柄的文件。

   lsof |grep delete

```
[root@ecs-linux-bj1 data1]# lsof |grep delete
cat       12803         root    1w      REG              253,17  81920030        11 /data1/testfile (deleted)
cat       13156         root    1w      REG              253,17  81920030        11 /data1/testfile (deleted)
[root@ecs-linux-bj1 data1]#
```

2. 执行以下命令，结束进程释放磁盘空间。
   kill -9 *进程编号*

```
[root@ecs-linux-bj1 data1]# kill -9 12803
[root@ecs-linux-bj1 data1]# kill -9 13156
[root@ecs-linux-bj1 data1]# df -h .
Filesystem      Size  Used Avail Use% Mounted on
/dev/vdb1        89M  8.4M   74M  11% /data1
[root@ecs-linux-bj1 data1]# echo aaaa >> a
```

fs.inotify.max_user_watches 值耗尽

Linux操作系统云服务器提示空间不足：No space left on device

```
ubuntu@VM-0-11-ubuntu:~/work$ sudo service docker start
Failed to add /run/systemd/ask-password to directory watch: No space left on device
Failed to add /run/systemd/ask-password to directory watch: No space left on device
ubuntu@VM-0-11-ubuntu:~/work$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            414M     0  414M   0% /dev
tmpfs            87M  9.3M   78M  11% /run
/dev/vda1        50G  3.1G   44G   7% /
tmpfs           433M   24K  433M   1% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           433M     0  433M   0% /sys/fs/cgroup
tmpfs            87M     0   87M   0% /run/user/500
```

解决方案：

1. 执行以下命令，编辑/etc/sysctl.conf文件。
   vi /etc/sysctl.conf
2. 补充如下信息：
   fs.inotify.max_user_watches = 524288
3. 执行以下命令使修改生效。
   sysctl -p
   Inotify用于监视文件系统事件， 默认情况下可监视的每个真实用户ID创建的文件数量 上限为8192，可以通过执行以下命令获取当前的inotify文件监视限制。
   cat /proc/sys/fs/inotify/max_user_watches

```
[root@ecs-linux-bj1 data1]# cat /proc/sys/fs/inotify/max_user_watches
8192
[root@ecs-linux-bj1 data1]#
```

如果此限制不足以监视所有文件，必须增加限制以使正常工作。

6.7 Linux 操作系统云服务器中 buffer 和 cache 占用内存怎么办?

问题描述

系统长期运行后，free命令查看系统内存，发现剩余内存不足，大部分是buffers和cached。

```
linux-nnkx:/home/yb/test # free -m
             total       used       free     shared    buffers     cached
Mem:         48183      47343        840          0       4754      41996
-/+ buffers/cache:        592      47591
Swap:            0          0          0
```


问题分析

在 Linux 的内存管理中，buffer是Linux内存中的Buffer cache。cache是Linux内存中的Page cache。

- Buffer cache：主要是当系统对块设备进行读写的时候，对块进行数据缓存的系统来使用，即对块的操作会使用buffer cache进行缓存。

  例如：当对一个文件进行写操作的时候，page cache 的内容会被改变，而buffer cache则可以用来将page标记为不同的缓冲区，并记录是哪一个缓冲区被修改了。内核在后续执行脏数据的回写writeback时，就不用将整个page写回，而只需要写回修改的部分即可。
- Page cache：主要用来作为文件系统上的文件数据的缓存来用，尤其是针对当进程对文件有read/write操作的时候。Linux默认会将读取的文件内容缓存在内存中，方便后续使用。

Linux默认使用的是lazy模式，即内存如果还够用，则不会主动释放当前的占用的buffer和cache，如果需要内存，则会自动释放buffer和cache，所以正常情况下，cache占用高不会对系统造成影响。

处理方法

buffer和cache是Linux对系统设备的正常环境，占用内存并不会影响系统的运行，反而强制清除cache会导致读取磁盘数据时需要重新通过IO从磁盘读取，影响系统运行速度。

说明

如需清理系统buffer和cache，可以执行以下命令：

echo 3 > /proc/sys/vm/drop_caches

根据内存大小可能需要几秒钟，执行完后响应内存被释。

6.8 扩容云硬盘后使用 growpart 扩容分区失败怎么办?

问题描述

扩容云硬盘后，使用growpart命令扩容分区时失败，报错信息例如：

图 6-5 报错信息 1

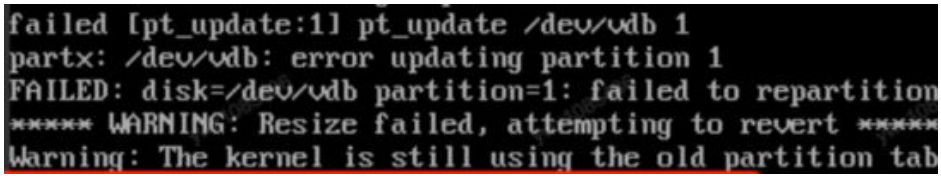
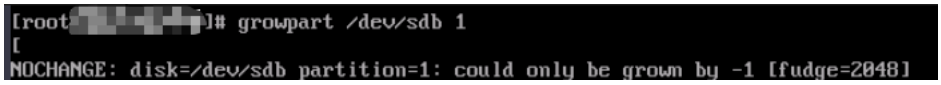


图 6-6 报错信息 2

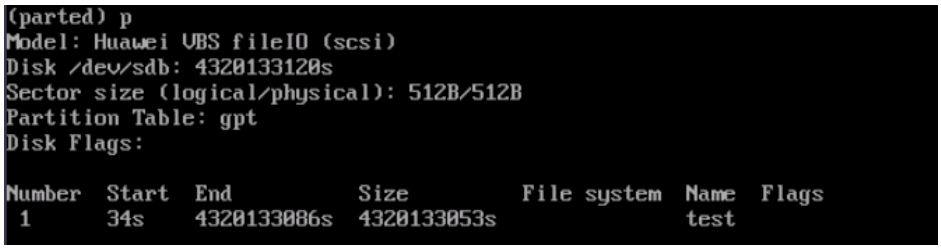


问题分析

扩容云硬盘后还需要扩容分区和文件系统，如果在初始化分区时未对齐分区，可能导致使用growpart命令扩容分区失败。

执行**parted -l**命令，如果start列显示的不是2048s或者1049KB，则表示分区未对齐。

图 6-7 分区未对齐



处理方法

如果出现分区未对齐的情况，则磁盘分区无法自动扩容，需选择手动扩容或者重新分区。

本文介绍手动扩容的方法。

说明

重新分区会导致磁盘数据丢失，请谨慎选择。

手动扩容可能存在风险，请在操作前对进行数据备份，详细内容，请参见**创建快照**或**备份磁盘** 。

1. 登录Linux云服务器。
2. 停止与挂载目录相关的进程。
3. 执行以下命令，执行卸载操作（以sdb1为例）。

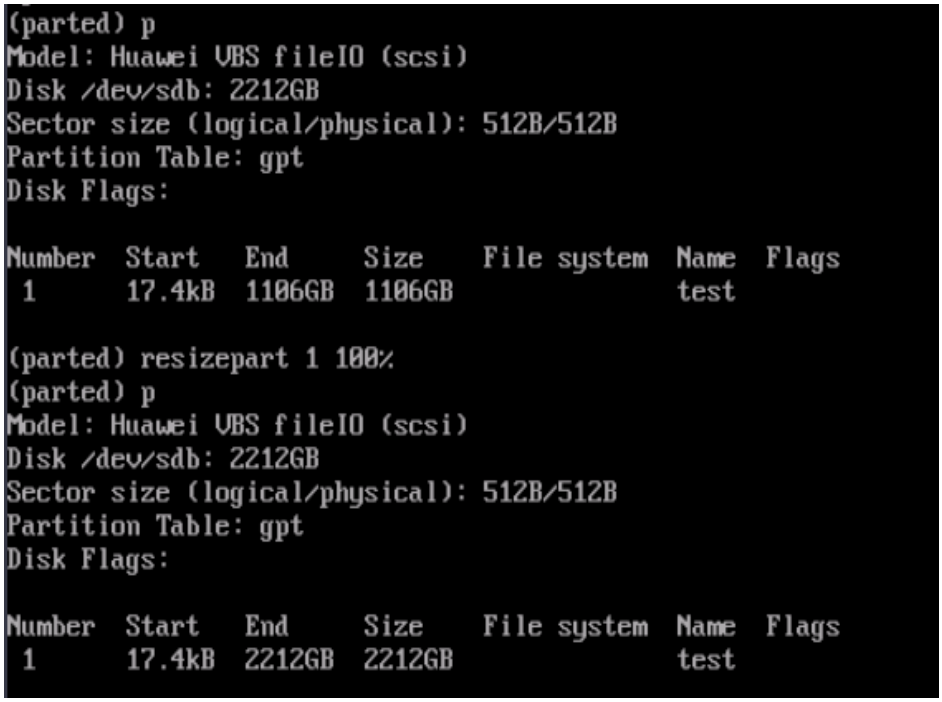
   umount /dev/sdb1
4. 执行以下命令，进行手动扩容。

   parted /dev/sdb
5. 执行**p**，检查当前分区。
6. 执行以下命令，在命令中需要选取一个分区进行扩容。

   由于只有最后一个分区可以扩容，因此，必须选择最后一个分区。

   resizepart 1*（分区号，该命令以分区1为例）*100%
7. 执行**p**，确认分区是否扩容成功。

图 6-8 扩容分区结果



8. 执行**q**，退出parted交互，手动扩容分区成功。

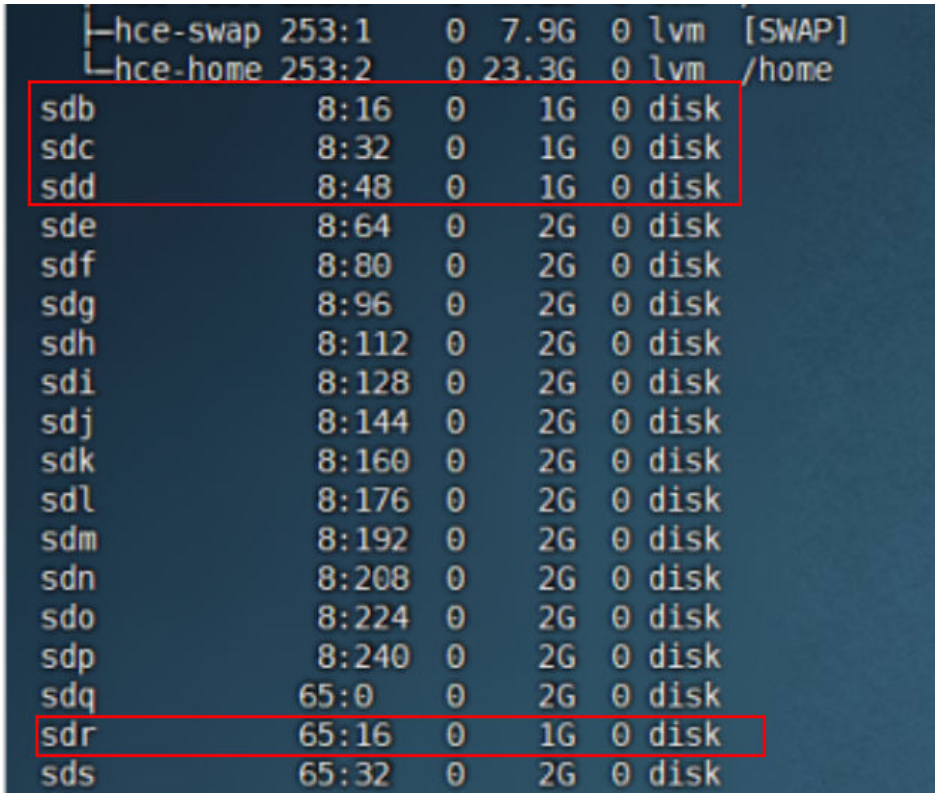
6.9 SCSI 磁盘 IO 压力大时，在线并发扩容失败怎么办?

问题描述

Linux系统、SCSI类型磁盘的云服务器进行在线并发（大于10个）扩容，扩容之后部分磁盘容量实际未发生变化。

例如，将磁盘容量由1G在线并发扩容到2G后，执行lsblk命令查看磁盘容量，发现sdb/sdc/sdd/sdr的磁盘容量没有发生变化。

图 6-9 报错信息



问题分析

当SCSI磁盘IO压力大时，磁盘队列无法及时处理扩容请求下发的请求事件，导致部分磁盘的容量增加未及时生效。

如果触发磁盘的写IO操作，云服务器会重新校验容量信息，使磁盘扩容生效。

处理方法

在Linux云服务器内，对容量未生效的磁盘进行一次写IO操作，使磁盘扩容生效，例如：

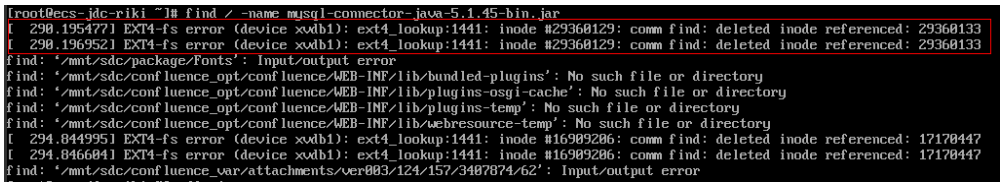
执行以下命令，在磁盘的挂载点目录创建一个空文件，进行写IO操作。

touch file

6.10 Linux 系统执行 find 命令时出现 EXT4-fs error 错误

问题描述

Linux系统执行find命令时出现EXT4-fs error错误。



可能原因

该错误由于磁盘分区文件系统损坏导致，需要卸载磁盘进行修复，建议对数据盘做备份后进行操作。

操作须知

修复文件系统，可能会产生数据丢失，请先备份数据后进行操作。

处理方法

本文以修复ext4文件系统为例，其他文件系统错误会有差异。

1. 登录弹性云服务器。
2. 执行以下命令，卸载已经挂载的分区（此处以xvdb1的挂载点为/mnt/sdc为例）。
   umount /mnt/sdc
3. 执行以下命令，修复已损坏的文件系统。
   fsck -y /mnt/sdc

   注意

   修复需要较长时间，在此期间请勿做其他操作。
4. 待磁盘修复完毕后，执行以下命令将分区重新挂载。
   mount -a
5. 执行以下命令，重启服务器。
   reboot

6.11 如何清理 Windows 云服务云硬盘空间

操作场景

当云服务器的云硬盘空间不足时，会影响云服务器的运行速度，降低使用体验。此时您可以通过以下两种途径来清理云硬盘空间。

- **使用系统自带云硬盘清理工具清理云硬盘空间**

本文以操作系统Windows 2016的云服务器为例，介绍了清理云硬盘空间的常用操作。同时建议在日常使用中养成良好的云硬盘使用习惯，定期清理冗余文件，有助于您节省云硬盘空间。

- 定期将不常用的文件压缩保存，节省云硬盘空间。
- 定期使用云硬盘清理工具清理云硬盘空间，删除不需要的文件，并定期清理回收箱。
- 卸载不需要的程序，释放云硬盘空间。

使用系统自带云硬盘清理工具清理云硬盘空间

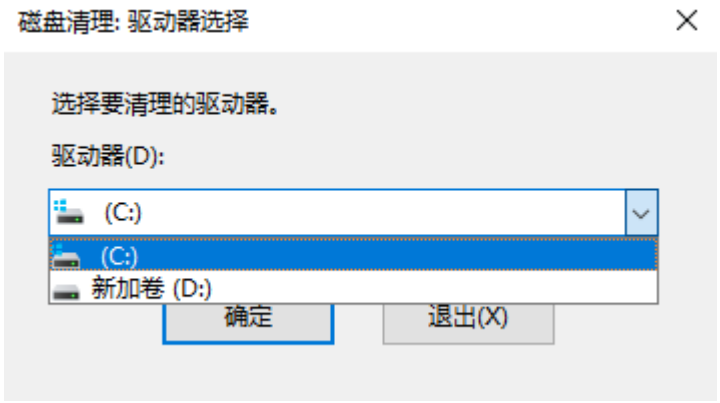
步骤1 在云服务器桌面，单击左下方开始图标。

弹出常用程序窗口。

步骤2 在左侧导航栏中，选择“Windows管理工具 > 磁盘清理”。

弹出“磁盘清理：驱动器选择”窗口。

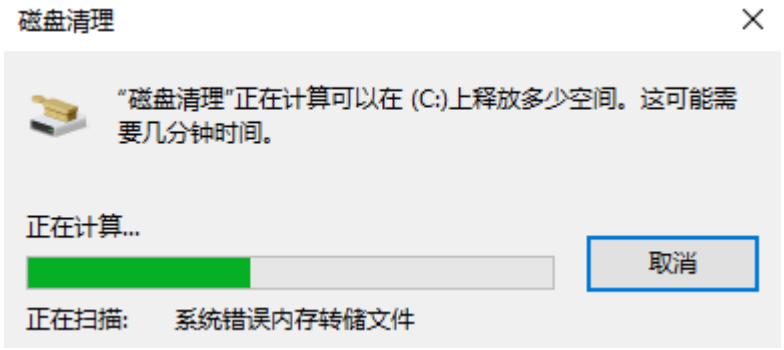
图 6-10 磁盘清理：驱动器选择



步骤3 在下拉框中，选择待清理的磁盘，以“C盘”为例。

弹出“磁盘清理”窗口，此时系统自动计算可在C盘上释放的空间。

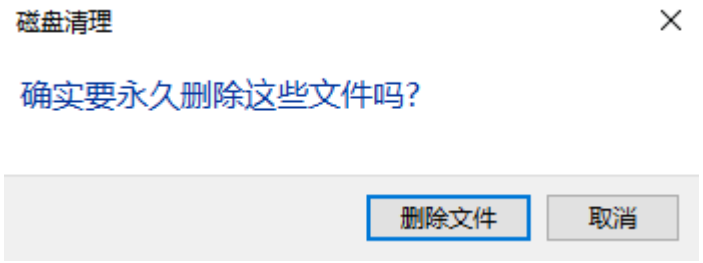
图 6-11 磁盘清理



步骤4 自动计算完成后，在弹窗中勾选要删除的文件，并单击“确定”。

弹出确认删除对话框。

图 6-12 确认删除



步骤5 单击“删除文件”，开始清理磁盘，释放磁盘空间。

----结束

使用控制面板卸载不需要的程序

步骤1 在云服务器桌面，单击左下方开始图标。

弹出常用程序窗口。

步骤2 在左侧导航栏中，选择“Windows系统 > 控制面板”。

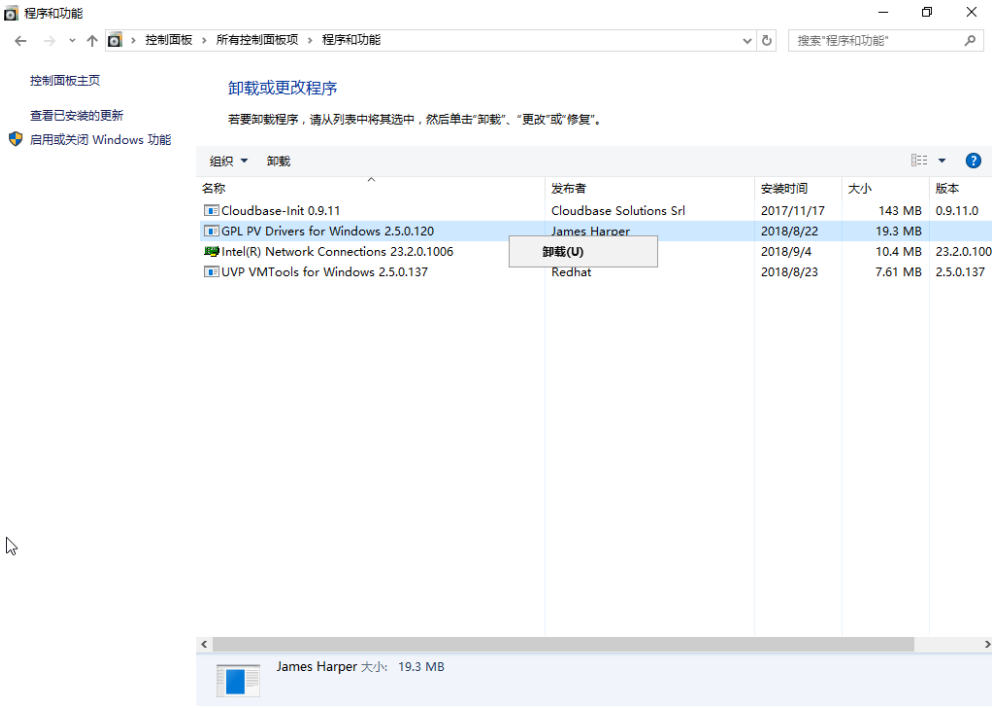
弹出“所有控制面板项”窗口。

图 6-13 所有控制面板项

步骤3 在导航列表中，选择“程序和功能”。

进入“程序和功能”窗口。

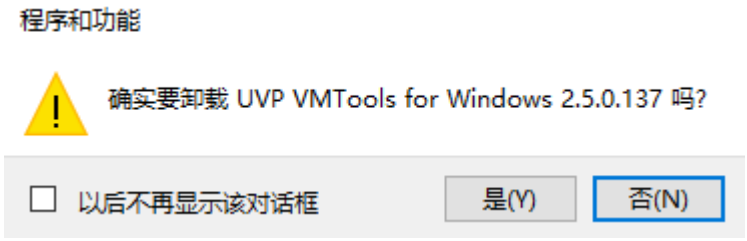
图 6-14 程序和功能



步骤4 在程序列表中，单击待卸载的程序，并右键单击“卸载”。

弹出确认卸载对话框。

图 6-15 确认卸载



步骤5 单击“是”，开始卸载程序，释放磁盘空间。

----结束

7 GPU 实例故障自诊断

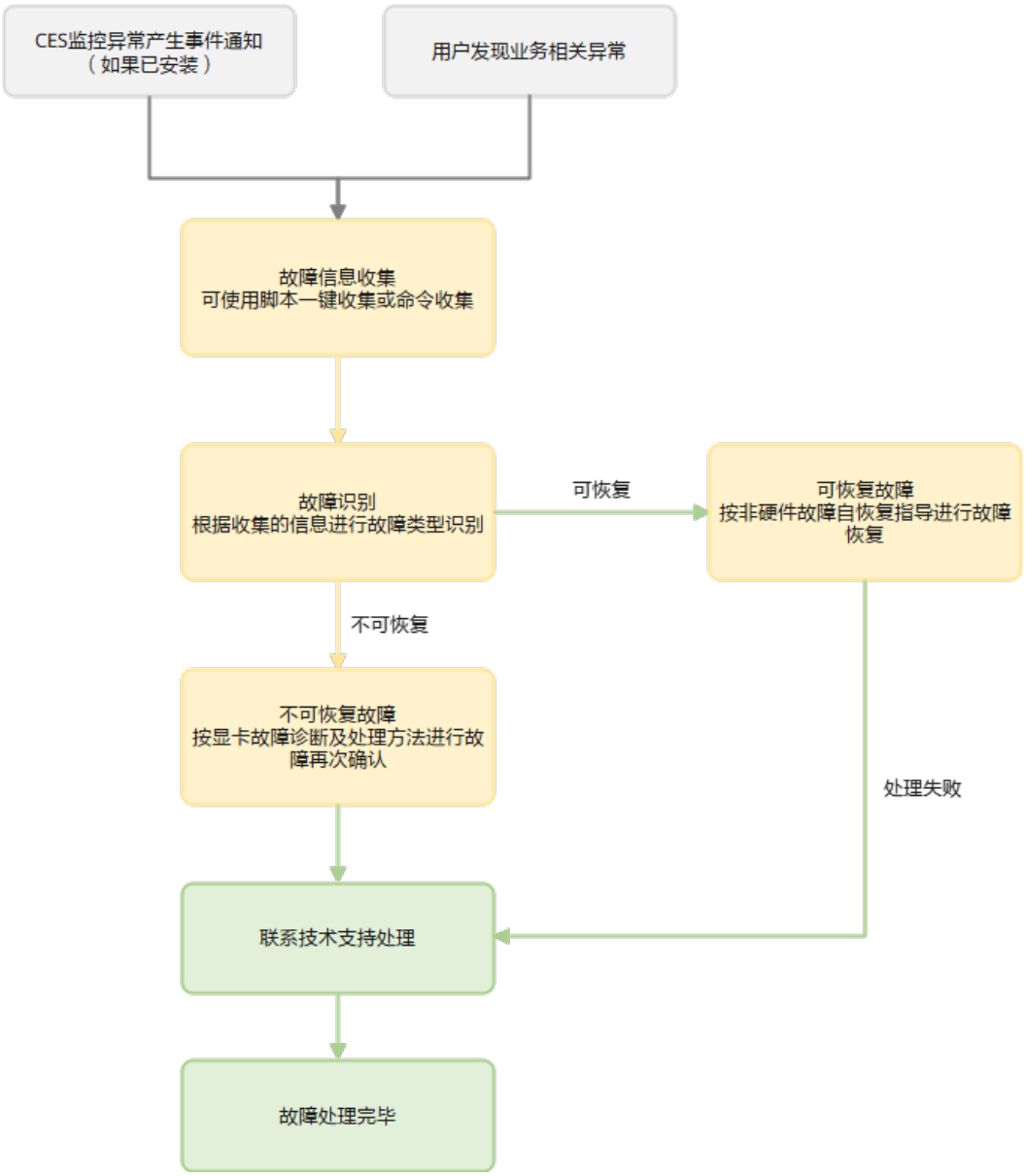
GPU实例故障，如果已安装**GPU监控的CES Agent**，当GPU服务器出现异常时则会产生事件通知，可以及时发现问题避免造成用户损失。如果没有安装CES Agent，只能依赖用户对故障的监控情况，发现故障后及时联系技术支持处理。

7.1 GPU 实例故障处理流程

GPU实例故障处理流程如**图7-1**所示，对应的操作方法如下：

- **CES监控事件通知**：配置GPU的CES监控后会产生故障事件通知。
- **故障信息收集**：可使用GPU故障信息收集脚本一键收集，也可参考**故障信息收集**执行命令行收集。
- **GPU实例故障分类列表**：根据错误信息在故障分类列表中识别故障类型。
- **非硬件故障自恢复处理方法**：这类问题可以根据指导自行排查恢复。
- **显卡故障诊断及处理方法**：这类问题可以根据指导确认后联系技术支持。
- **联系技术支持人员**：无法自恢复请提交工单联系技术支持人员获取帮助。

图 7-1 GPU 实例故障处理流程



7.2 GPU 实例故障分类列表

GPU实例故障的分类列表如**表7-1**所示。

表 7-1 GPU 实例故障分类列表

是否可恢复故障	故障类型	相关文档
可恢复故障，可按照相关文档自行恢复	镜像配置问题	如何处理Nouveau驱动未禁用导致的问题
	ECC错误	如何处理ECC ERROR：存在待隔离页问题

是否可恢复故障	故障类型	相关文档
	内核升级问题	如何处理升级内核后，驱动不可用问题
	GPU掉卡问题	如何处理GPU掉卡问题
	显卡ERR!	如何处理显卡ERR！问题
	软件安装问题	如何处理用户自行安装NVIDIA驱动、CUDA软件，安装过程出错问题
	驱动兼容性问题	如何处理驱动兼容性问题
	Xid问题	如何处理可恢复的Xid故障问题
	显卡被禁用	如何处理用户的虚拟机报错：“由于该设备有问题，Windows已将其停止”问题
	镜像问题	如何处理用户使用场景与其选择的驱动、镜像不配套问题
	License问题	如何处理用户安装了GRID驱动，但未购买、配置License问题
不可恢复故障，需联系技术支持处理	InfoROM错误	如何处理infoROM错误
	ECC错误	如何处理ECC ERROR：执行nvidia-smi -q存在double bit ecc error错误，并无待隔离页
		如何处理ECC ERROR：执行nvidia-smi存在SRAM的ECC错误（V100显卡）
	GPU掉卡	如何处理GPU掉卡，执行lspci | grep -i nvidia命令找不到显卡或显卡显示rev ff
	温度过高问题	如何处理GPU散热异常，执行nvidia-smi命令发现温度过高
	驱动安装报错	如何处理驱动安装报错“Unable to load the kernel module 'nvidia.ko'”
	Xid报错	如何处理GPU虚拟机故障，在message日志中发现存在Xid报错

7.3 故障信息收集

7.3.1 故障信息收集方法

用户可使用故障信息收集脚本一键收集所有信息或使用命令进行获取相应信息。

- 故障信息一键收集脚本使用方法如下：
  a. 故障信息一键收集脚本下载地址：https://hgcs-drivers-cn-north-4.obs.cn-north-4.myhuaweicloud.com/release/script/diagnose_gpu.sh

b. 执行**bash diagnose_gpu.sh**命令，将信息收集到信息文件diagnose_gpu_xxxxx.tar.gz进行自排查或工单联系技术支持。

- 使用命令获取信息请参考**表7-2**。

表 7-2 获取信息方法

信息分类	相关文档
显卡基本信息	**如何获取显卡ID**
	如何查询显卡详细信息
	如何查询显卡在位信息
显卡故障信息(Linux)	**如何查询NVIDIA的错误信息**
	如何查询XID报错信息
NVIDIA日志收集(Linux)	**如何收集NVIDIA日志**
镜像内核信息收集(Linux)	**如何查询内核信息**
驱动安装信息收集(Linux)	**如何收集驱动安装信息**

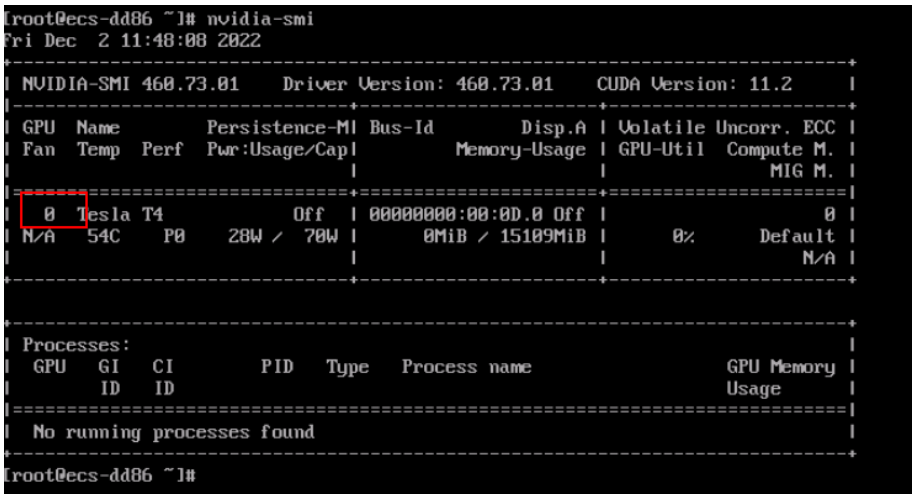
7.3.2 如何获取显卡 ID

- Linux操作系统获取显卡ID的方法如下：
  a. 登录弹性云服务器。
  b. 在任意路径下执行**nvidia-smi**命令。（CCE集群场景为*/opt/cloud/cce/nvidia/bin目录下*）

```
[root@ecs-dd86 ~]# nvidia-smi
Fri Dec  2 11:48:08 2022
+-----------------------------------------------------------------------------+
| NVIDIA-SMI 460.73.01    Driver Version: 460.73.01    CUDA Version: 11.2     |
|-------------------------------+----------------------+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute M. |
|                               |                      |               MIG M. |
|===============================+======================+======================|
|   0  Tesla T4            Off  | 00000000:00:0D.0 Off |                    0 |
| N/A   54C    P0    28W /  70W |      0MiB / 15109MiB |      0%      Default |
|                               |                      |                  N/A |
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                                  |
|  GPU   GI   CI        PID   Type   Process name                  GPU Memory |
|        ID   ID                                                   Usage      |
|=============================================================================|
|  No running processes found                                                 |
+-----------------------------------------------------------------------------+
[root@ecs-dd86 ~]#
```

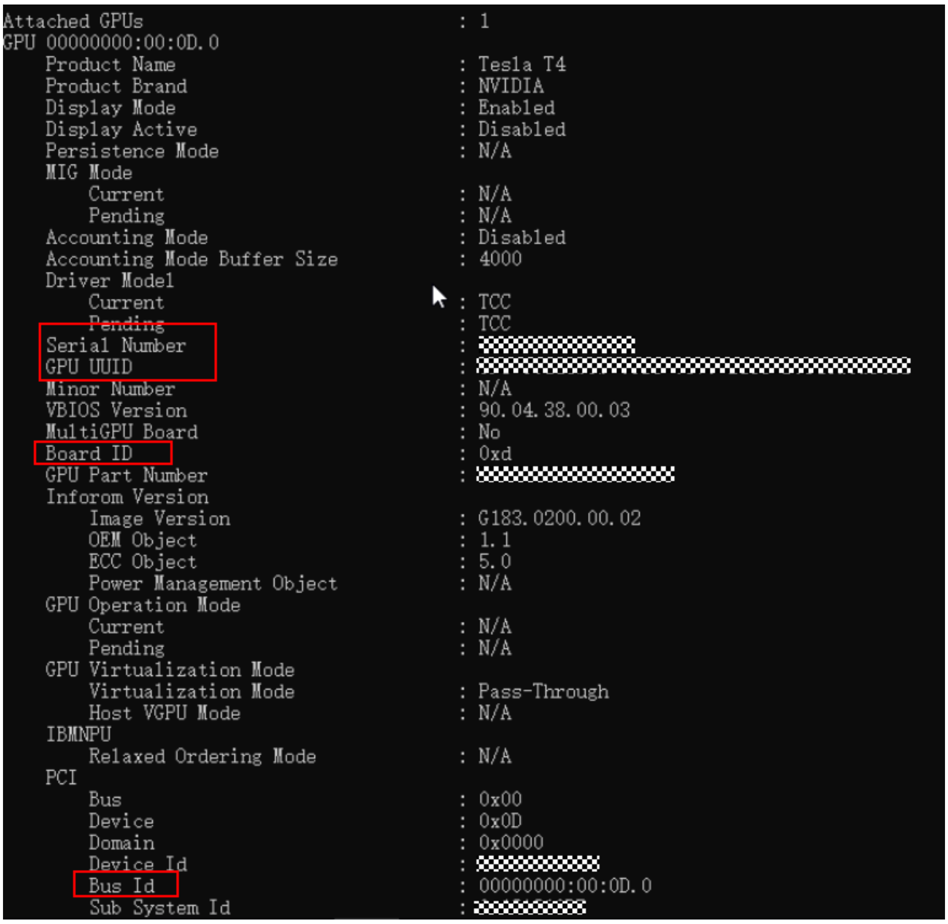
- Windows操作系统获取显卡ID的方法如下：
  a. 进入到*C:|Program Files|NVIDIA Corporation|NVSM*路径。
  b. 执行**nvidia-smi**命令。



7.3.3 如何查询显卡详细信息

- 查询指定显卡的详细信息
  a. 登录弹性云服务器。
  b. 执行以下命令，查询指定显卡的详细信息。
     nvidia-smi –q –i ${显卡ID}
- 查询所有显卡的详细信息
  a. 登录弹性云服务器。
  b. 执行以下命令，所有显卡的详细信息。
     nvidia-smi -q

执行结果示例如下：



```
Attached GPUs                           : 1
GPU 00000000:00:0D.0
    Product Name                        : Tesla T4
    Product Brand                       : NVIDIA
    Display Mode                        : Enabled
    Display Active                      : Disabled
    Persistence Mode                    : N/A
    MIG Mode
        Current                         : N/A
        Pending                         : N/A
    Accounting Mode                     : Disabled
    Accounting Mode Buffer Size         : 4000
    Driver Model
        Current                         : TCC
        Pending                         : TCC
    Serial Number                       : [redacted]
    GPU UUID                            : [redacted]
    Minor Number                        : N/A
    VBIOS Version                       : 90.04.38.00.03
    MultiGPU Board                      : No
    Board ID                            : 0xd
    GPU Part Number                     : [redacted]
    Inforom Version
        Image Version                   : G183.0200.00.02
        OEM Object                      : 1.1
        ECC Object                      : 5.0
        Power Management Object         : N/A
    GPU Operation Mode
        Current                         : N/A
        Pending                         : N/A
    GPU Virtualization Mode
        Virtualization Mode             : Pass-Through
        Host VGPU Mode                  : N/A
    IBMNPU
        Relaxed Ordering Mode           : N/A
    PCI
        Bus                             : 0x00
        Device                          : 0x0D
        Domain                          : 0x0000
        Device Id                       : [redacted]
        Bus Id                          : 00000000:00:0D.0
        Sub System Id                   : [redacted]
```

7.3.4 如何查询显卡在位信息

查询显卡在位信息方法如下：

1. 登录弹性云服务器。
2. 执行以下命令，查看显卡在位情况，确认是否和服务器规格显卡数一致，保存回显结果。

   lspci | grep NV

如下图所示，可以看到有一张GPU显卡，且显卡是rev a1，状态正常；如果为rev ff或其他状态，则显卡可能故障。

```
[[redacted]]# lspci | grep NV
00:0d.0 3D controller: NVIDIA Corporation TU104GL [Tesla T4] (rev a1)
```

7.3.5 如何查询 NVIDIA 的错误信息

查询NVDIA错误信息的方法如下：

1. 登录弹性云服务器。
2. 执行以下命令，查看是否存在error信息，保存回显结果。

   dmesg | grep -i nvidia

   也可过滤关键字后保存结果，例如：NVRM、nouveau、nvidia、nv字样等。

7.3.6 如何查询 XID 报错信息

XID消息是NVIDIA驱动程序向操作系统的内核日志或事件日志打印的错误报告，用于标识GPU错误事件，提供GPU硬件、NVIDIA软件或您应用程序中的错误类型、错误位置、错误代码等信息。

查询XID报错信息方法如下：

1. 登录弹性云服务器。
2. 执行以下命令，查看是否存在xid相关报错，保存回显结果。

   dmesg | grep -i xid

- 若检查项GPU节点上的XID异常为空，说明无XID消息。
- 若检查项GPU节点上的XID异常不为空，您可按照**GPU实例故障分类列表**自助诊断并解决问题，或联系技术支持人员获取帮助。

7.3.7 如何收集 NVIDIA 日志

收集NVIDIA日志方法如下：

1. 登录弹性云服务器。
2. 在任意目录下执行以下命令。（如果是CCE场景，进入到/opt/cloud/cce/nvidia/bin目录后执行）

   sh nvidia-bug-report.sh

   或

   ./nvidia-bug-report.sh
3. 执行完成后会在当前执行目录下生成nvidia-bug-report.log.gz，转储该日志。

```
[root@ecs-dd86 ~]# sh nvidia-bug-report.sh

nvidia-bug-report.sh will now collect information about your
system and create the file 'nvidia-bug-report.log.gz' in the current
directory.  It may take several seconds to run.  In some
cases, it may hang trying to capture data generated dynamically
by the Linux kernel and/or the NVIDIA kernel module.  While
the bug report log file will be incomplete if this happens, it
may still contain enough data to diagnose your problem.

If nvidia-bug-report.sh hangs, consider running with the --safe-mode
and --extra-system-data command line arguments.

Please include the 'nvidia-bug-report.log.gz' log file when reporting
your bug via the NVIDIA Linux forum (see forums.developer.nvidia.com)
or by sending email to 'linux-bugs@nvidia.com'.

By delivering 'nvidia-bug-report.log.gz' to NVIDIA, you acknowledge
and agree that personal information may inadvertently be included in
the output.  Notwithstanding the foregoing, NVIDIA will use the
output only for the purpose of investigating your reported issue.

Running nvidia-bug-report.sh... complete.

[root@ecs-dd86 ~]# ll
total 1252
-rw-r--r-- 1 root root 1279051 Dec  2 11:50 nvidia-bug-report.log.gz
[root@ecs-dd86 ~]# _
```

7.3.8 如何查询内核信息

查询内核信息的方法如下：

1. 登录弹性云服务器。
2. 执行以下命令，查看内核版本。

   uname -r

   ```
   [root@ecs-dd86 ~]# uname -r
   4.18.0-240.10.1.el8_3.x86_64
   [root@ecs-dd86 ~]#
   ```

3. 执行以下命令，查看安装驱动时的内核版本。

   Ubuntu：**find /lib/modules -name nvidia.ko**

   CentOS：**find /usr/lib/modules -name nvidia.ko**

   ```
   [root@ecs-6711 ~]# find /usr/lib/modules -name nvidia.ko
   /usr/lib/modules/3.10.0-957.21.3.el7.x86_64/kernel/drivers/video/nvidia.ko
   [root@ecs-6711 ~]#
   ```

4. 执行以下命令，查看gcc版本。

   rpm -qa | grep gcc

5. 执行以下命令，查看kernel-devel版本。

   rpm -qa | grep kernel-devel

7.3.9 如何收集驱动安装信息

收集驱动安装信息的方法如下：

1. 登录弹性云服务器。
2. 执行以下命令，检查是否禁用了nouveau驱动。

   lsmod | grep nouveau

如果是驱动安装失败类问题，收集/var/log/nvidia-installer.log 驱动安装日志，并转储日志信息。

7.4 非硬件故障自恢复处理方法

7.4.1 如何处理 Nouveau 驱动未禁用导致的问题

问题描述

Nouveau驱动未禁用可能导致Linux系统卡死、虚拟机无法远程登录等问题。一般常见于客户使用自己的私有镜像（从ECS普通虚拟机导出的镜像或其他来源的私有镜像）。

判断方式

1. 执行以下命令，查看Linux内核环缓冲区中的错误关键字信息。

   dmesg | grep error

   - 如果回显信息中包含nouveau关键字样，说明Nouveau驱动可能未禁用，可执行2进一步确认。
   - 如果回显信息中未包含nouveau关键字样，继续执行2。

   ```
   root[redacted]:/home/ops# dmesg |grep -i error
   [   18.603210] nouveau: probe of 0000:21:01.0 failed with error -12
   [   18.622555] nouveau: probe of 0000:21:02.0 failed with error -12
   [   18.641799] nouveau: probe of 0000:21:03.0 failed with error -12
   [   18.661004] nouveau: probe of 0000:21:04.0 failed with error -12
   [   21.558220] EXT4-fs (vda1): re-mounted. Opts: errors=remount-ro
   ```

2. 执行以下命令，查看是否安装Nouveau驱动。

   lsmod | grep nouveau

   - 如果不存在回显内容或回显中不包含nouveau关键字样，说明Nouveau驱动已禁用。
   - 如果回显信息中包含nouveau关键字样，说明Nouveau驱动已安装，则需要禁用Nouveau驱动。

   ```
   [root@ecs-dd86 ~]# lsmod | grep nouveau
   nouveau              2281472  0
   video                  49152  1 nouveau
   mxm_wmi                16384  1 nouveau
   wmi                    32768  2 mxm_wmi,nouveau
   i2c_algo_bit           16384  1 nouveau
   drm_kms_helper        217088  5 cirrus,nvidia_drm,nouveau
   ttm                   110592  1 nouveau
   drm                   557056  6 drm_kms_helper,cirrus,nvidia_drm,ttm,nouveau
   [root@ecs-dd86 ~]#
   ```

处理方法

1. 执行如下命令编辑blacklist.conf文件。

   如果没有“/etc/modprobe.d/blacklist.conf”文件，请新建一个。

   vi /etc/modprobe.d/blacklist.conf

   添加如下语句添加至文件结尾。

   ```
   blacklist nouveau
   options nouveau modeset=0
   ```

2. 执行以下命令，备份并新建一个initramfs。

   - Ubuntu系统：

     sudo update-initramfs -u

   - CentOS系统：

     mv /boot/initramfs-$(uname -r).img /boot/initramfs-$(uname -r).img.bak

     dracut -v /boot/initramfs-$(uname -r).img $(uname -r)

3. 执行以下命令，重启云服务器。

   reboot

7.4.2 如何处理 ECC ERROR：存在待隔离页问题

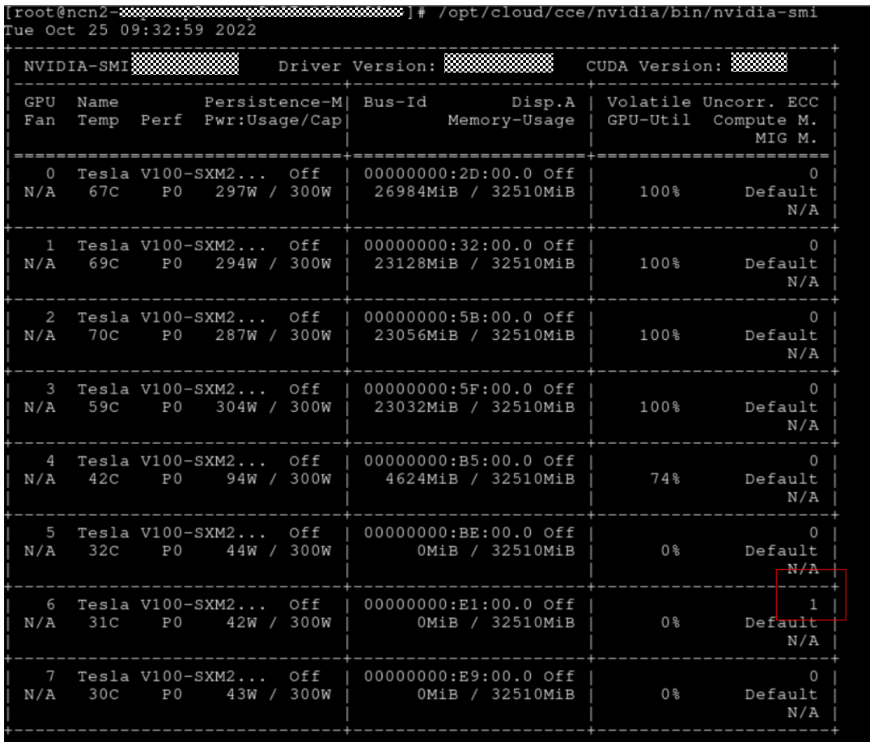
问题描述

- 业务调度到某个GPU节点后，发现业务异常，调度到其他节点时正常。
- 某台虚拟机显存使用率突然降低。

判断方式

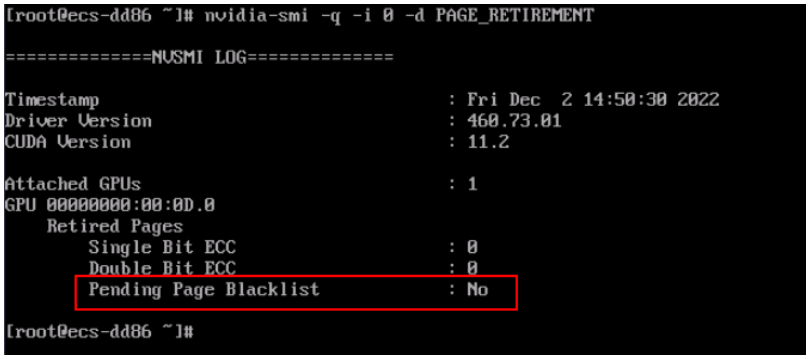
1. 执行以下命令，查看显卡是否存在ecc error。

   nvidia-smi



2. 如果1的回显结果中volatile Uncorr. ECC下ecc error > 0，执行以下命令，查看该GPU卡是否存在待隔离页。

   nvidia-smi -q -i *&{gpu_id}* -d PAGE_RETIREMEN

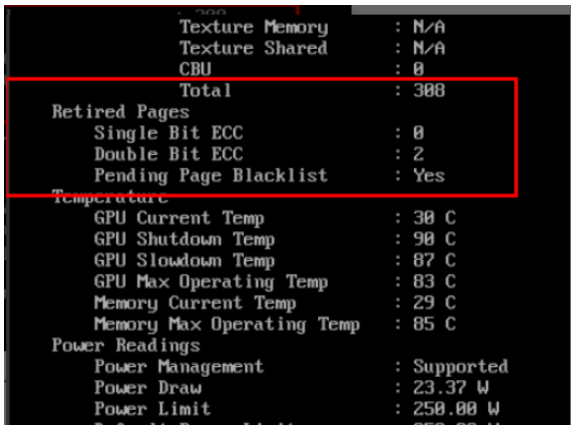


   回显结果中出现No表示不存在待隔离页。

3. 如果1的回显结果中volatile Uncorr. ECC下ecc error = 0，执行以下命令，查看所有的卡是否存在待隔离页。

   nvidia-smi -q -d PAGE_RETIREMENT

4. 如果3的回显结果中Pending Page Blacklist为Yes，说明存在待隔离页，需要重新加载驱动去隔离。



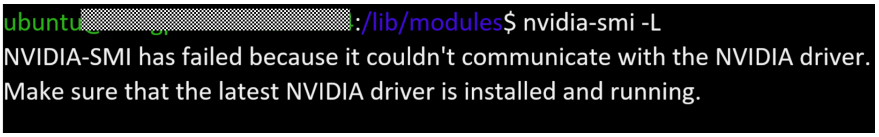
处理方法

- 方法一：
  a. 执行以下命令，查看GPU使用情况并停掉所有占用GPU的进程。
  nvidia-smi
  b. 执行以下命令，重置GPU。
  nvidia-smi -r
  c. 执行以下命令，查看是否存在待隔离页。
  nvidia-smi -q -d PAGE_RETIREMENT
  如果Pending Page Blacklist 为No，说明当前已无待隔离页。
- 方法二：
  a. 执行以下命令，重启云服务器。
  reboot
  b. 执行以下命令，查看是否存在待隔离页。
  nvidia-smi -q -d PAGE_RETIREMENT
  如果Pending Page Blacklist 为No，说明当前已无待隔离页。

7.4.3 如何处理升级内核后，驱动不可用问题

问题描述

- 客户执行**nvidia-smi**，报错failded to initialize NVML: Driver/library version mismatch。
- 客户执行**nvidia-smi**，报错NVIDIA-SMI has failed because it couldn't communicate with the NVIDIA diver。



判断方式

1. 执行以下命令，查看当前内核版本。
   uname -r

2. 根据不同的系统在云服务器中执行以下命令，查看安装驱动时的内核版本。
   - CentOS：**find /usr/lib/modules -name nvidia.ko**
   - Ubuntu：**find /lib/modules -name nvidia.ko**

   如果当前内核版本与安装驱动时的内核版本不一致，则确认为内核升级后导致的驱动不可用。

处理方法

1. 依次执行以下命令，移除NVIDIA的驱动。

   rmmod nvidia_drm

   rmmod nvidia_modeset

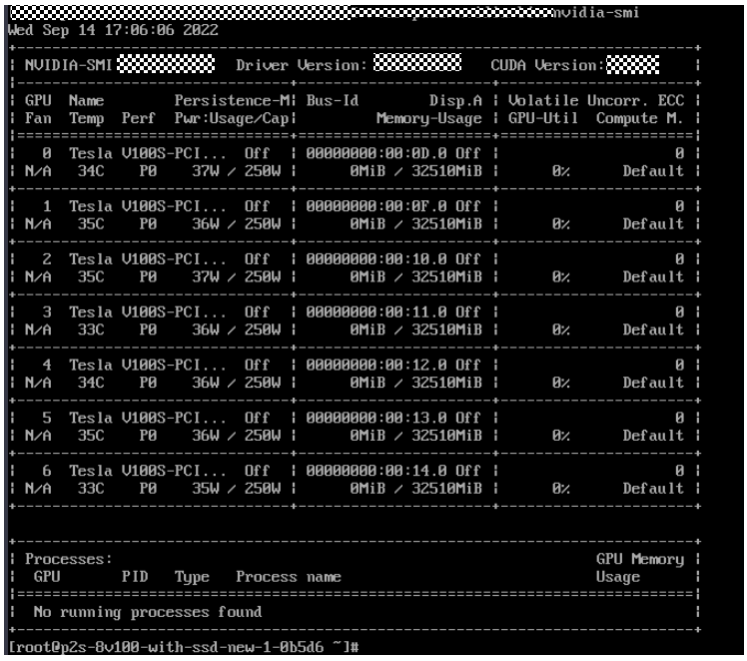
   rmmod nvidia
2. 执行以下命令，查看GPU信息。

   nvidia-smi
   - 如果回显正常，则问题已修复。
   - 如果回显仍报错，请参考**GPU驱动不可用**中的处理方法进行操作。

7.4.4 如何处理 GPU 掉卡问题

问题描述

执行**nvidia-smi**命令查询到的显卡的数量较实际规格对应的显卡数量少。



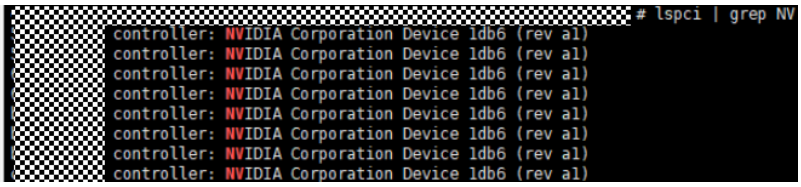
如上图所示，执行**nvidia-smi**命令查询到7张显卡，实际该机型应有8张显卡。

判断方式

执行以下命令，显卡的数量与实际规格对应的显卡数量一致，且显卡在位状态正常（rev a1），请继续按照**处理方法**处理；如果查找不到显卡或者显示状态为rev ff，请

根据**显卡故障诊断及处理方法**进行故障诊断。规格对应显卡数量可以通过**GPU加速型**查询。

lspci | grep -i nvidia



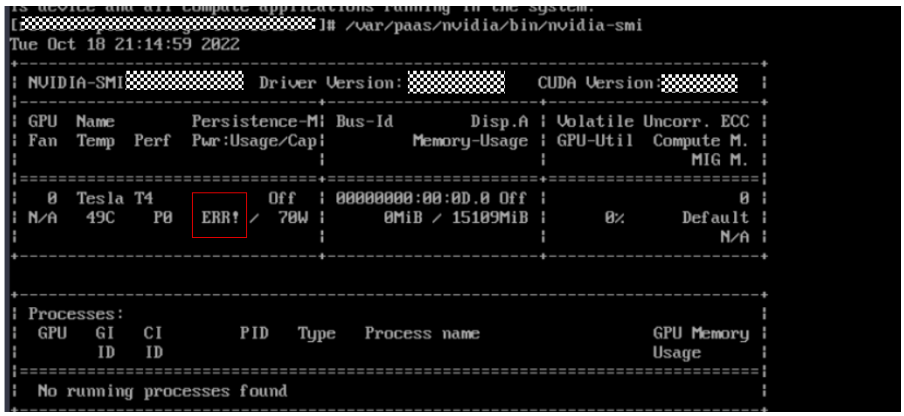
处理方法

- 非CCE集群场景，建议尝试自行重装驱动，或升级驱动版本后执行**nvidia-smi**，查看是否还存在少卡现象；若仍显示少卡，请根据**故障信息收集**收集故障信息后联系技术支持处理。
- CCE集群场景，请根据**故障信息收集**收集故障信息后联系技术支持处理。

7.4.5 如何处理显卡 ERR！问题

问题描述

执行**nvidia-smi**命令，仅Pwr:Usage/Cap（能耗）显示ERR!



处理方法

1. 如果当前用户业务正常，仅**nvidia-smi**执行后存在ERR!显示问题，无需处理。
2. 如果当前业务已经受到影响，迁移虚拟机，再根据**故障信息收集**收集故障信息后联系技术支持处理。

7.4.6 如何处理用户自行安装 NVIDIA 驱动、CUDA 软件，安装过程出错问题

问题描述

用户使用不带驱动的公共镜像或私有镜像，自行安装NVIDIA驱动软件包、CUDA软件包，在安装过程中脚本执行报错。

```
[root@ecs-8692 ~]# sudo sh cuda_10.1.105_418.39_linux.run
cuda_10.1.105_418.39_linux.run: line 1: syntax error near unexpected token `newline'
cuda_10.1.105_418.39_linux.run: line 1: `<html>'
[root@ecs-8692 ~]# sudo sh cuda_10.1.105_418.39_linux.run
cuda_10.1.105_418.39_linux.run: line 1: syntax error near unexpected token `newline'
cuda_10.1.105_418.39_linux.run: line 1: `<html>'
[root@ecs-8692 ~]# sh cuda_10.1.243_418.87.00_linux.run
sh: cuda_10.1.243_418.87.00_linux.run: No such file or directory
[root@ecs-8692 ~]# sh cuda_10.1.105_418.39_linux.run
cuda_10.1.105_418.39_linux.run: line 1: syntax error near unexpected token `newline'
cuda_10.1.105_418.39_linux.run: line 1: `<html>'
[root@ecs-8692 ~]#
```

判断方式

1. 确认用户使用的镜像文件。
2. 确认用户的NVIDIA软件包来源。
3. 确认用户想要的目标NVIDIA软件包版本以及CUDA软件版本。

处理方法

- 推荐客户使用自动安装驱动脚本。根据当前华为云驱动自动安装脚本中提供的CUDA版本，按需安装。
  - **（推荐）自动安装GPU加速型ECS的GPU驱动（Linux）**
  - **（推荐）自动安装GPU加速型ECS的GPU驱动（Windows）**
- 如果自动安装驱动脚本中无用户需要的目标软件版本，请联系技术支持处理。

7.4.7 如何处理驱动兼容性问题

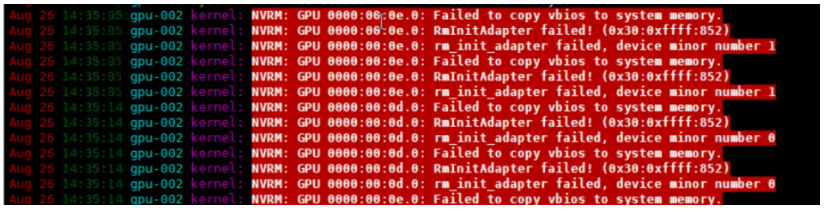
问题描述

用户执行**nvidia-smi**命令回显报错“No devices were found”。

```
No devices were found
```

处理方法

1. 查看云服务器的实例规格，确认用户使用的镜像信息。
   - 如果使用NVIDIA Tesla T4 GPU（例如，Pi2或G6规格），请参见**T4 GPU设备显示异常** 进行处理。
   - 如果使用其他规格的GPU云服务器，执行下一步。
2. 查看系统日志“/var/log/message”，是否存在驱动相关报错。
   - 如果存在报错“Failed to copy vbios to system memory”，可能是由于频繁加载/卸载驱动导致，建议开启驱动持久化模式，保持驱动处于加载状态。



     i. 执行以下命令，开启驱动持久化模式。

        nvidia-smi -pm 1

     ii. 执行以下命令，打开并编辑“**/etc/rc.local**”文件。

        vim /etc/rc.local

iii. 配置开机自启动，将命令“**nvidia-smi -pm 1**”写入“**/etc/rc.local**”文件中。

iv. 按“Esc”，输入**:wq**保存并退出。

v. 执行以下命令，添加启动权限。

chmod +x /etc/rc.d/rc.local

- 若未查到相关报错，执行下一步。

3. 查看实例的Tesla驱动版本是否为510.xx.xx。
   - 是，该驱动版本与所用镜像可能存在兼容性问题，建议更换驱动版本，请参考**安装GPU驱动**。
   - 否，请执行下一步。
4. 如果仍未确认根因，请根据**故障信息收集**操作后联系技术支持处理。

7.4.8 如何处理可恢复的 Xid 故障问题

问题原因

Xid	说明
13	Graphics Engine Exception，非硬件故障，可能是指令错误等。
31	GPU memory page fault，非硬件故障，可能访问了非法地址等。
43	GPU stopped processing， 非硬件故障，可能是自身软件错误。

详情可以参考NVIDIA的Xid描述文档：**https://docs.nvidia.com/deploy/xid-errors/index.html**。

处理方法

1. 尝试重新运行作业并观察Xid错误是否消失。
2. 若错误持续存在，尝试检查代码或分析日志，确认是否为程序引入的Xid故障。
3. 若确认不是程序引入，请联系技术支持处理。

7.4.9 如何处理用户的虚拟机报错：“由于该设备有问题，Windows已将其停止”问题

问题描述

用户在Windows设备管理器显示适配器中查询显卡属性，发现设备状态中存在错误“由于该设备有问题，Windows已将其停止”。

判断方式

1. 确认用户发生问题时的操作，是否有出现显存OOM。
2. 如果用户使用的是vGPU实例，确认实例安装的驱动与主机的驱动版本是否匹配。
   a. 登录实例所在主机。
   b. 执行**nvidia-smi**命令，查看驱动版本，并对照版本配套关系。
      版本配套关系：**https://docs.nvidia.com/grid/index.html**

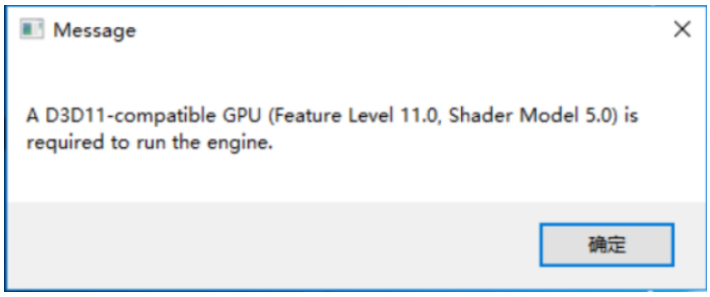
处理方法

1. 重启GPU弹性云服务器。
   - 若显示适配器恢复正常，则恢复完成。
   - 若仍异常，则执行下一步。
2. 请尝试重装GPU驱动或升级驱动版本。请参考**安装GPU驱动**。
3. 如果用户使用的是vGPU实例，且实例驱动版本与主机版本不匹配，请重装版本匹配的驱动软件。

7.4.10 如何处理用户使用场景与其选择的驱动、镜像不配套问题

问题描述

1. 用户业务是做渲染（推理）的，但用户选择了带Tesla驱动（GRID驱动）的公共镜像，运行软件时出错。
   例如：用户使用场景为做渲染，但选错公共镜像，运行软件时报错“A D3D11-compatible GPU (Feature Level 11.0,Shader Model 5.0) is required to run the engine”。



2. 用户业务是做渲染（推理）的，但用户选择了不带驱动的公共镜像，且未单独安装驱动，导致GPU能力不可用，执行**nvidia-smi**命令报错“command not found”。

判断方式

1. 确认用户业务使用场景。
2. 用户使用的镜像是否带驱动、是否已经自行安装驱动、驱动是否与使用场景匹配。
   - 如果用户使用的是异构发布的公共镜像，可通过镜像名称区分驱动类型与驱动版本。镜像名称中如带有with tesla字样，则选择该镜像会安装tesla驱动；如带有with grid字样，则选择该镜像会安装GRID驱动（不包括License）。
   - 如果用户使用的是私有镜像或其他镜像，可通过**nvidia-smi**命令查询是否安装了驱动以及确认驱动类型、驱动版本。
   - 如客户选择自行安装Tesla驱动，请务必告知客户确保Tesla驱动与CUDA软件的版本配套关系，可参考**Tesla驱动及CUDA工具包获取方式**。

处理方法

1. 如果用户未安装驱动，请自行安装驱动，或切换带驱动的公共镜像，或使用驱动自动安装脚本安装驱动。
   - **（推荐）自动安装GPU加速型ECS的GPU驱动（Linux）**
   - **（推荐）自动安装GPU加速型ECS的GPU驱动（Windows）**
2. 如果用户已安装驱动，但驱动不匹配使用场景，请卸载驱动后重新安装。请参考**安装GPU驱动**。

7.4.11 如何处理用户安装了 GRID 驱动，但未购买、配置 License 问题

问题描述

用户业务是做图形处理的，且用户已经安装了GRID驱动，但用户的GPU使用率很低或渲染性能达不到预期。

例：运行图像识别任务，任务会突然卡住无法继续运行，GPU的性能表现差；查看/var/log/messages日志发现有如下报错，询问用户后确认用户购买了License但是未配置License。

```
nvidia-gridd: Valid GRID license not found. GPU features and performance are restricted. To enable full functionality please configure licensing details.
```

处理方法

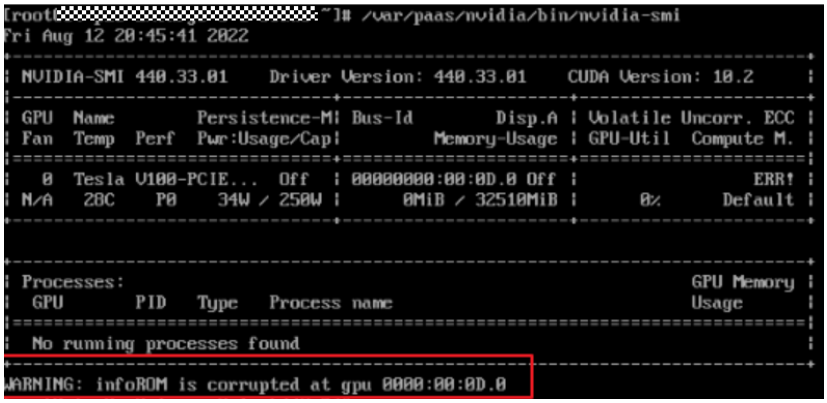
1. 确认用户业务使用场景是否是做图形处理，用户使用的实例规格是否满足图形处理要求。
2. 用户是否安装GRID驱动，执行**nvidia-smi**命令查询回显是否正常。
   - 如果回显正常，且能查询到驱动版本，驱动版本是GRID驱动的版本，则说明已安装GRID驱动。
3. 用户是否购买了License，如果已购买License是否已经配置了License。
   a. 如果用户未购买License，请参考**手动安装GPU加速型ECS的GRID驱动**购买License后再根据指导配置License。
   b. 如果用户已购买过License，但是未配置License，请参考**手动安装GPU加速型ECS的GRID驱动**配置License服务器与License文件。

7.5 显卡故障诊断及处理方法

7.5.1 如何处理 infoROM 错误

问题描述

Linux操作系统的云服务器在执行**nvidia-smi**命令报错“WARNING:infoROM is corrupted at gpu 0000:00:0D.0”，并且用户业务已经受到影响。



问题原因

健全性检查没有通过，GPU驱动程序不会使用或信任其内容（某些内容未被使用）。

问题影响

可能影响ECC相关非易失数据的记录，导致本该隔离的GPU内存页面继续使用。

处理方法

1. 如果用户业务暂未受损，则无需处理。
2. 通知用户停止业务，执行虚拟机迁移，并根据**故障信息收集**章节收集故障信息后，联系技术支持处理。

7.5.2 如何处理 ECC ERROR：执行 nvidia-smi -q 存在 double bit ecc error 错误，并无待隔离页

问题原因

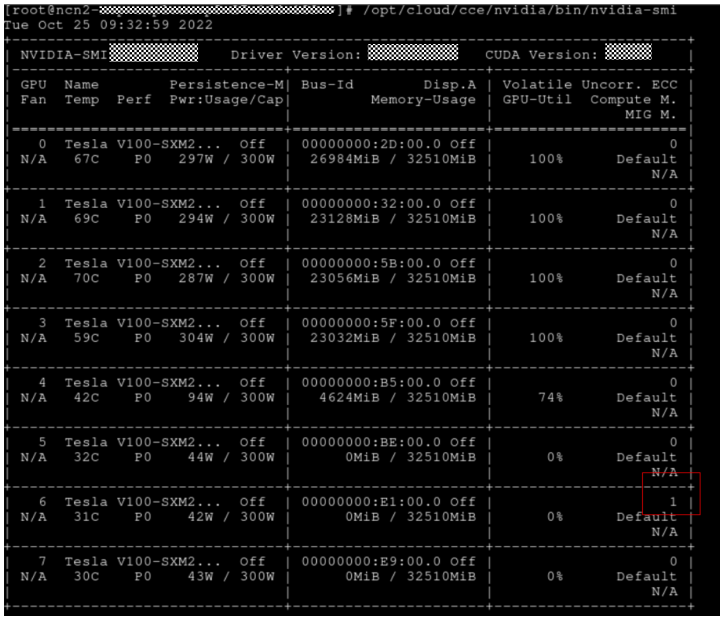
显存可能某个地方存在异常。

问题影响

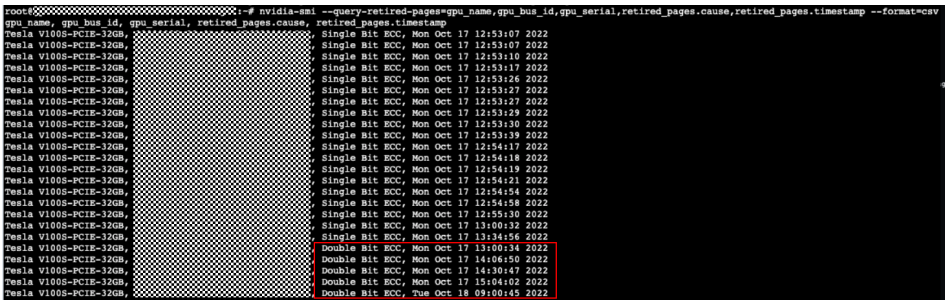
可能影响一个或多个GPU的相关应用程序。

处理方法

执行**nvidia-smi**命令，查看显卡信息。



- 如果在volatile Uncorr. ECC下ecc error > 0，执行**nvidia-smi -q -i *&.{gpu_id}***查看卡的详细信息。
- 如果在volatile Uncorr. ECC下ecc error = 0，可以执行**nvidia-smi -q**查看所有的卡。
- 如果Pending Page Blacklist 为No，且double bit ecc error较多，继续诊断是否达到换卡条件：
  a. 执行**nvidia-smi –r**命令，重置GPU。
  b. 执行**nvidia-smi --query-retired-pages=gpu_name,gpu_bus_id,gpu_serial,retired_pages.cause,retired_pages.timestamp --format=csv**，如果连续5次出现了double bit ecc错误，则联系技术支持换卡处理；否则，重置GPU后检查用户业务是否恢复正常，如果恢复正常则显卡可以继续使用。



7.5.3 如何处理 ECC ERROR：执行 nvidia-smi 存在 SRAM 的 ECC 错误（V100 显卡）

问题原因

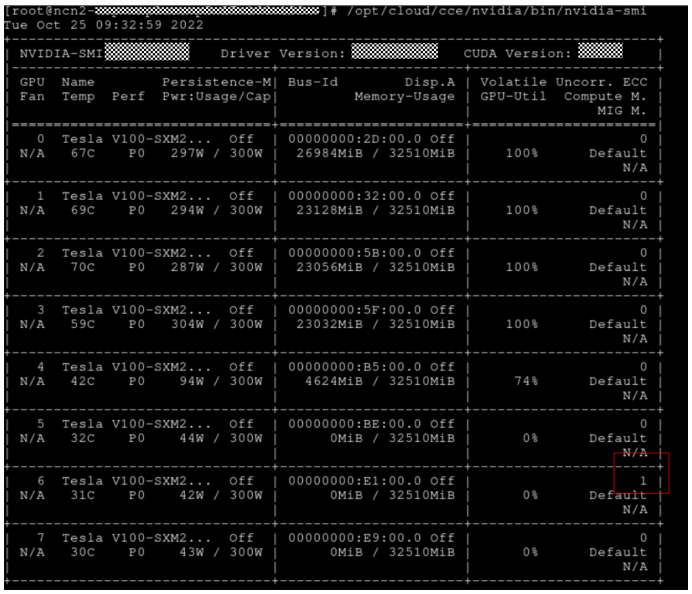
显存可能某个地方存在异常。

问题影响

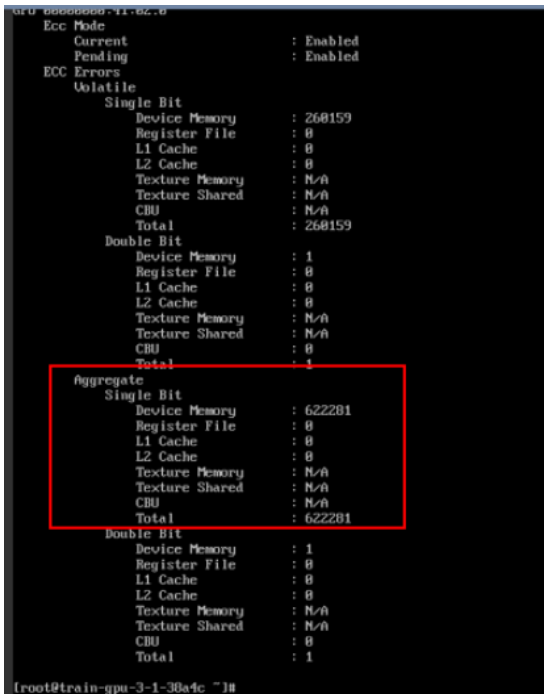
可能影响一个或多个GPU的相关应用程序。

处理方法

执行**nvidia-smi**命令查看显卡信息。



- 如果在volatile Uncorr. ECC下发现存在ecc error，执行**nvidia-smi -q -i *&{gpu_id}***查看卡的详细信息。
- 如果在volatile Uncorr. ECC下未发现ecc error，可以执行**nvidia-smi -q**查看所有的卡。
- 如果volatile下Single Bit或Aggregate下的Single Bit仅有Device Memory项有数值增加，不影响使用，无需处理。
- 如果volatile下Single Bit、Double bit或Aggregate下的Single Bit、Double bit存在Register File+L1 Cach +L2 Cache+Texture Memory+Texture Shared+CBU > 0，则根据**故障信息收集**收集故障信息后联系技术支持处理。



7.5.4 如何处理 GPU 掉卡，执行 lspci | grep -i nvidia 命令找不到显卡或显卡显示 rev ff

问题原因

某种健全性检查没有通过，GPU驱动程序不会使用或信任其内容（某些内容未被使用）。

问题影响

可能影响ECC相关非易失数据的记录，从而导致本该隔离的GPU内存页面继续使用。

处理方法

1. 用户停止业务并执行业务迁移。
2. 执行业务迁移后，根据**故障信息收集**收集故障信息后联系技术支持处理。

7.5.5 如何处理 GPU 散热异常，执行 nvidia-smi 命令发现温度过高

问题原因

显卡散热异常、风扇损坏。

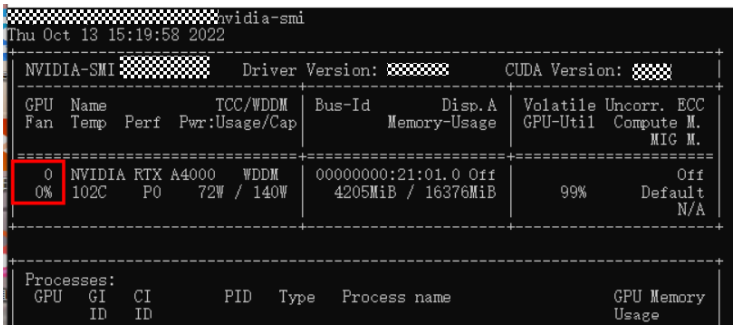
问题影响

显卡温度过高，影响用户业务。

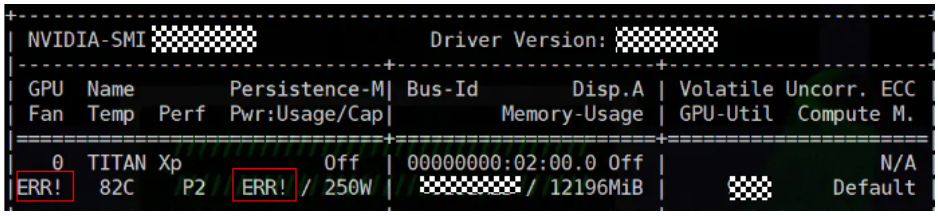
处理方法

执行**nvidia-smi**命令，查看风扇是否正常。

- 如果风扇转速为0，说明风扇可能存在损坏，用户停止业务，执行业务迁移后，根据**故障信息收集**收集故障信息后联系技术支持检查硬件是否存在问题。



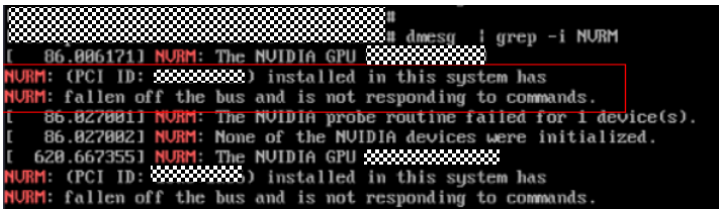
- 如果风扇显示ERR!，可能是因为显卡过热，用户先停止业务，待显卡缓解过热后再执行**nvidia-smi**命令，查看ERR!是否消失。
  - 如果回显正常，建议用户调整下业务，限制显卡运行的最大功率。
  - 如果仍未恢复正常，根据**故障信息收集**收集故障信息后联系技术支持处理。



7.5.6 如何处理驱动安装报错“Unable to load the kernel module 'nvidia.ko'”

问题原因

1. 总线脱落。



2. 内核版本不一致。

问题影响

显卡驱动安装失败，显卡无法使用。

处理方法

1. 执行以下命令，查看内核版本，检查内核版本是否一致。

   rpm -qa | grep gcc #查看gcc版本

   rpm -qa | grep kernel-devel #查看kernel-devel版本
   - 如果内核版本不一致，请重装驱动。
   - 如果内核版本一致，则执行下一步。

2. 查看dmesg日志，检查是否存在NVRM报错。
   - 如果报错“NVRM: fallen off the bus and is not responding to commands”，说明是总线脱落，请联系技术支持人员换卡。
   - 如果仍未确认问题，请根据**故障信息收集**收集GPU故障后联系技术支持处理。

7.5.7 如何处理 GPU 虚拟机故障，在 message 日志中发现存在 Xid 报错

问题原因

XID	说明
32	Invalid or corrupted push buffer stream，推送缓冲区流无效或损坏
74	NVLINK Error. NVLink异常产生的XID，表明GPU硬件故障需要下线维修。
79	GPU has fallen off the bus。总线脱落，需要下线维修

详情可以参考NVIDIA的Xid描述文档：**https://docs.nvidia.com/deploy/xid-errors/index.html**。

处理方法

1. 执行**dmesg | grep –i xid**命令，查看是否存在xid报错。

2. 通知用户停止业务，执行业务迁移，并根据**故障信息收集**章节收集故障信息后，联系技术支持处理。

8 GPU 驱动故障

8.1 G 系列弹性云服务器 GPU 驱动故障

问题描述

在Windows系统的G系列弹性云服务器中，无法打开NVIDIA 控制面板，GPU驱动无法使用或GPU驱动显示异常。

可能原因

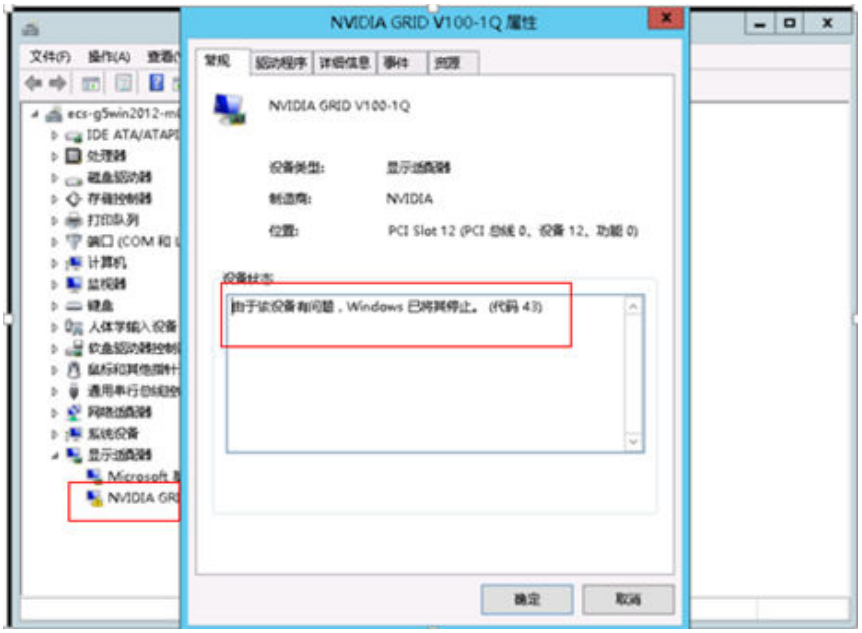
GPU驱动状态异常。

处理方法

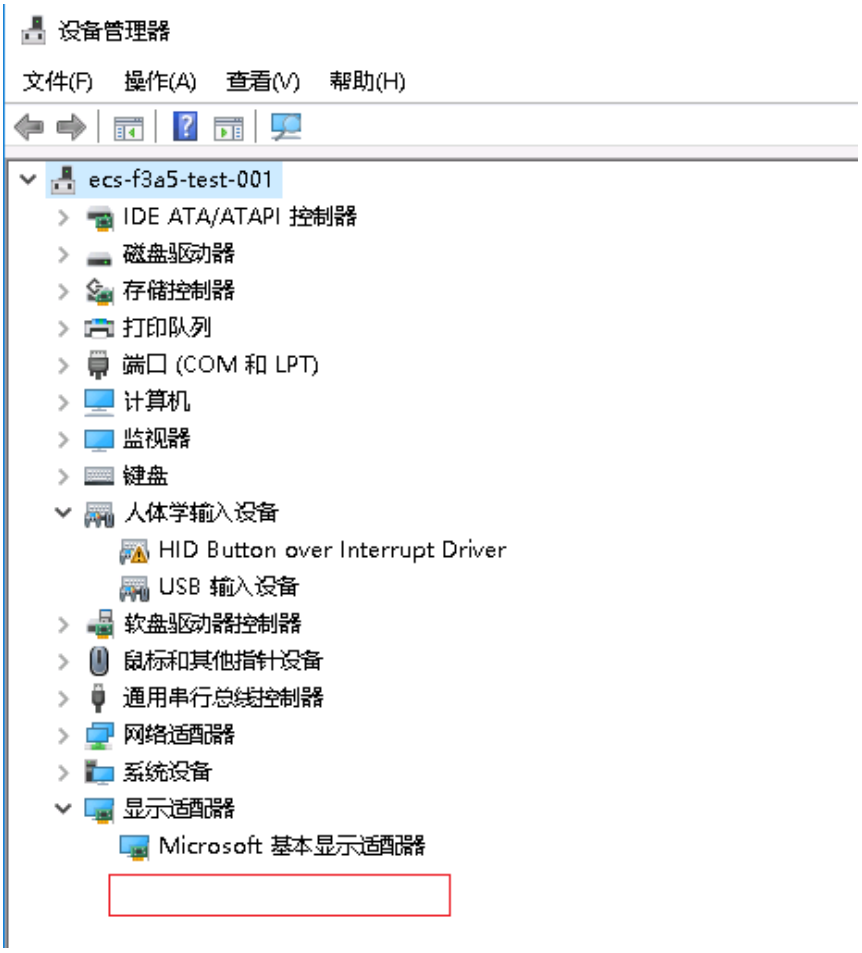
步骤1 打开Windows设备管理器，在显示适配器中查看GPU驱动状态。

- GPU驱动显示正常，查看属性，提示需要重新启动计算机后生效，如下图所示，执行步骤**步骤2**。

- GPU驱动有黄色感叹号，查看属性，显示设备有问题，如下图所示，执行步骤**步骤2**。



- 显示适配器中无GPU显卡驱动（GPU驱动未生效），如下图所示，执行步骤**步骤2**。



步骤2 重启弹性云服务器。

查看设备管理器 > 显示适配器，如果驱动生效并且状态正常，任务结束。

否则请重新安装GPU驱动。

以驱动安装包位置为C盘为例：在服务器中进入C:\ NVIDIA\xxx.xx，其中xxx.xx表示NVIDIA驱动的版本，双击“setup”安装驱动，如下图所示。

详细操作指导请参考：**安装GPU驱动**

----结束

8.2 GPU 驱动异常怎么办?

问题描述

在GPU实例中，执行以下命令查看GPU使用情况，提示系统无法执行指定的程序、或文件路径不存在。

nvidia-smi

回显信息如下所示：

```
-bash: /bin/nvidia-smi: No such file or directory
```

或

```
nvidia-smi: command not found
```

可能原因

云服务器驱动异常、没有安装驱动或者驱动被卸载。

处理方法

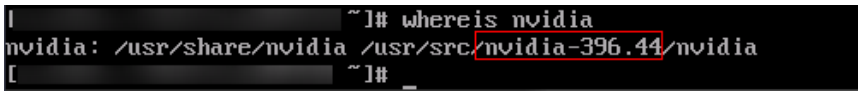
- 如果未安装GPU驱动，请重新安装GPU驱动。
  操作指导请参考：**安装GPU驱动**
- 如果已安装驱动，但是驱动被卸载。
  执行**history**，查看是否执行过卸载操作。
  进入/var/log目录，查看是否有nvidia-uninstall.log日志，如果有说明GPU驱动已被卸载，请重新安装GPU驱动。
- 如果已安装驱动，但是驱动状态异常。
  a. 卸载驱动。

- 方法1：执行**nvidia-uninstall**命令，卸载驱动。

  如果提示命令不存在可以执行 **查询云服务器安装的驱动版本：whereis n...**卸载驱动。

- 方法2：查询云服务器安装的驱动版本：whereis nvidia

  图 8-1 查询安装的驱动版本

  根据查询的驱动版本从**NVIDIA官网**下载驱动包（此处重新下载驱动包是为了执行卸载动作，且后续重新安装驱动时需要此安装包）。

  以驱动版本nvidia-396.44为例，执行**sh NVIDIA-Linux-x86_64-396.44.run --uninstall**，卸载驱动

b. 重装驱动。

   操作指导请参考：**安装GPU驱动**

8.3 GPU 驱动不可用

问题描述

执行**nvidia-smi**查看GPU使用情况，显示如下：

```
NVIDIA-SMI has failed because it couldn't communicate with the NVIDIA driver. Make sure that the latest NVIDIA driver is installed and running.
```

图 8-2 GPU 驱动不可用

可能原因

系统内核进行了升级，导致在新内核上，GPU驱动不可用。

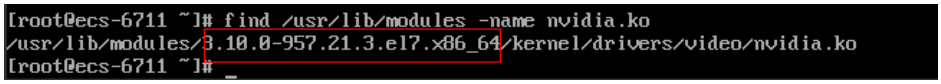
问题排查

根据不同的系统在服务器中执行如下命令，查看安装驱动时的内核版本：

- CentOS：**find /usr/lib/modules -name nvidia.ko**
- Ubuntu：**find /lib/modules -name nvidia.ko**

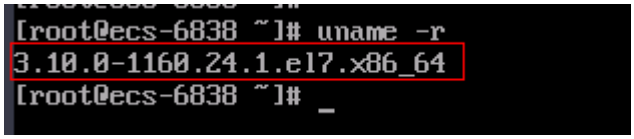
示例：以CentOS为例，执行上述命令，回显信息如图8-3所示可以看出GPU驱动是基于3.10.0-957.5.1.el7.x86_64版本的内核安装的。

图 8-3 安装驱动时的内核版本



执行**uname –r**，如图8-4所示，查看当前内核版本是3.10.0-1160.24.1.el7.x86_64。

图 8-4 当前内核版本

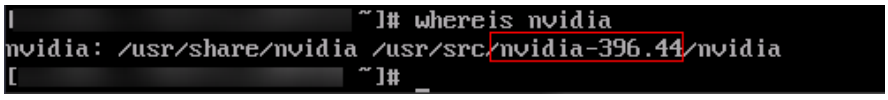


说明安装驱动的内核版本跟当前内核版本不一致。

处理方法

- 方法一：重新启动，选择安装GPU驱动时的内核版本，即可使用GPU驱动。
  a. 在云服务器操作列下单击“远程登录 > 立即登录”。
  b. 单击远程登录操作面板上方的“发送CtrlAltDel”按钮，重启虚拟机。
  c. 然后快速刷新页面，按上下键，阻止系统继续启动，选择安装GPU驱动时的内核版本进入系统。在当前内核版本下GPU驱动即可正常使用。
- 方法二：基于新的内核版本，重新安装驱动。
  a. 卸载驱动。
     - 方法1：执行**nvidia-uninstall**命令，卸载驱动。
       如果提示命令不存在可以执行**•查询云服务器安装的驱动版本：whereis n...**卸载驱动。
     - 方法2：查询云服务器安装的驱动版本：whereis nvidia

       图 8-5 查询安装的驱动版本

       根据查询的驱动版本从**NVIDIA官网**下载驱动包（此处重新下载驱动包是为了执行卸载动作，且后续重新安装驱动时需要此安装包）。
       以驱动版本nvidia-396.44为例，执行**sh NVIDIA-Linux-x86_64-396.44.run --uninstall**，卸载驱动
  b. 重装驱动。
     操作指导请参考：**安装GPU驱动**

8.4 GPU 设备显示异常

问题描述

执行**nvidia-smi**查看GPU使用情况，显示如下：

- 单卡机器显示
  No devices were found
- 多卡机器上显示卡数目不全

执行**lspci | grep -i nvidia**，显示卡数目正常。

处理方法

1. 查看实例是否使用NVIDIA Tesla T4 GPU（例如，Pi2或G6规格）。
   - 是，请参见**T4 GPU设备显示异常**进行处理。
   - 否，请执行下一步。
2. 查看系统日志“/var/log/message”，是否存在驱动相关报错。
   - 如果出现“Failed to copy vbios to system memory”，可能是由于频繁加载/卸载驱动导致，建议开启驱动持久化模式，保持驱动处于加载状态。

     图 8-6 系统日志

     i. 执行以下命令，开启驱动持久化模式。

     nvidia-smi -pm 1

     ii. 执行以下命令，打开并编辑“**/etc/rc.local**”文件。

     vim /etc/rc.local

     iii. 配置开机自启动，将命令“**nvidia-smi -pm 1**”写入“**/etc/rc.local**”文件中。

     iv. 按“Esc”，输入**:wq**保存并退出。

     v. 执行以下命令，添加启动权限。

     chmod +x /etc/rc.d/rc.local

   - 否，请执行下一步。
3. 查看实例的Tesla驱动版本是否为510.xx.xx。
   - 是，该驱动版本与镜像可能存在兼容性问题，建议更换驱动版本，操作指导，请参考**安装GPU驱动**。
   - 否，请执行下一步。
4. 请尝试重启云服务器，再执行nvidia-smi查看GPU使用情况，确认是否正常。

   如果问题依然存在，请联系客服。

8.5 T4 GPU 设备显示异常

问题描述

使用NVIDIA Tesla T4 GPU的云服务器，例如Pi2或G6规格，执行**nvidia-smi**命令查看GPU使用情况时，显示如下：

```
No devices were found
```

原因分析

NVIDIA Tesla T4 GPU是NVIDIA的新版本，默认使用并开启GSP Firmware，导致GPU无法识别。

处理方法一

说明

该处理方法在重启云服务器后失效。

1. 执行以下命令，移除NVIDIA内核模块。
   rmmod nvidia_drm
   rmmod nvidia_modeset
   rmmod nvidia
2. 执行以下命令，关闭GSP Firmware开关，并载入NVIDIA内核模块。
   modprobe nvidia NVreg_EnableGpuFirmware=0
   modprobe nvidia_drm
   modprobe nvidia_modeset
3. 如果问题依然存在，请联系客服。

处理方法二

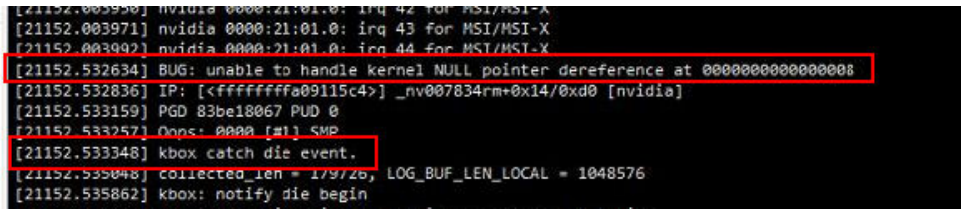
1. 执行以下命令，打开文件/etc/modprobe.d/nvidia.conf。
   vim /etc/modprobe.d/nvidia.conf
   单击“i”进入编辑模式。
2. 在文件中添加以下内容。
   ```
   options nvidia NVreg_EnableGpuFirmware=0
   ```
   编辑完成后，单击**Esc**键，并输入 **:wq!** 退出。
3. 执行以下命令，重启云服务器。
   reboot
4. 如果问题依然存在，请联系客服。

8.6 GPU 实例启动异常，查看系统日志发现 NVIDIA 驱动空指针访问怎么办?

问题描述

GPU实例启动异常，检查系统日志，发现NVIDIA驱动空指针访问。如图8-7所示。

图 8-7 NVIDIA 驱动空指针访问



可能原因

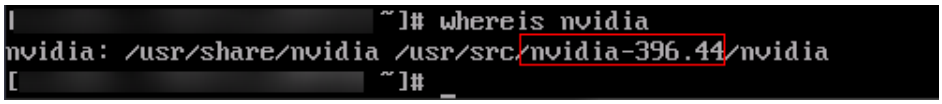
GPU驱动异常。

处理方法

1. 卸载驱动。
   - 方法1：执行**nvidia-uninstall**命令，卸载驱动。

     如果提示命令不存在可以执行 **查询云服务器安装的驱动版本：whereis n...** 卸载驱动。
   - 方法2：查询云服务器安装的驱动版本：whereis nvidia

     图 8-8 查询安装的驱动版本

     根据查询的驱动版本从**NVIDIA官网**下载驱动包（此处重新下载驱动包是为了执行卸载动作，且后续重新安装驱动时需要此安装包）。

     以驱动版本nvidia-396.44为例，执行**sh NVIDIA-Linux-x86_64-396.44.run --uninstall**，卸载驱动
2. 重装驱动。

   操作指导请参考：**安装GPU驱动**

9 SSH 连接

9.1 怎样长时间保持 SSH 会话连接不断开?

操作场景

使用SSH方式登录CentOS 6.5操作系统的云服务器时，过一段时间就会自动断开连接。本节操作介绍如何保持SSH会话持续连接不断开

该文档适用于CentOS/EulerOS系统。

说明

本节操作涉及重启sshd服务，会造成sshd断开。

操作方法

编辑/etc/ssh/sshd_config文件设置心跳，保持连接。

1. 编辑/etc/ssh/sshd_config，添加配置项：
   ```
   ClientAliveInterval 600
   ClientAliveCountMax 10
   ```
   ClientAliveInterval 600 表示每600秒发送一次请求， 从而保持连接。

   ClientAliveCountMax 10 表示服务器发出请求后客户端没有响应的次数达到10次，就自动断开连接。

   则无响应的SSH客户端将在大约600x10=6000秒后断开连接。

   说明

   ClientAliveInterval设置超时间隔（以秒为单位），在此间隔之后，如果尚未从客户端接收到任何数据，则sshd将通过加密的通道发送消息以请求客户端的响应。默认值为0，表示这些消息将不会发送到客户端。此选项仅适用于协议版本2。

   ClientAliveCountMax设置客户端活动消息的数量，该消息可以在sshd接收不到来自客户端的任何消息的情况下发送。如果在发送客户端活动消息时达到此阈值，则sshd将断开客户端连接，从而终止会话。

   客户端活动消息的使用与TCPKeepAlive有很大不同。客户端活动消息是通过加密通道发送的，因此不会被欺骗。由TCPKeepAlive启用的TCP keepalive选项是可欺骗的。
2. 执行以下命令，重启sshd服务，使配置生效。

- CentOS6操作系统
  service sshd restart
- CentOS7/EulerOS操作系统
  systemctl restart sshd

9.2 怎样设置允许或禁止用户/IP 通过 SSH 方式连接云服务器

操作场景

本节操作指导用户设置允许或禁止用户/IP通过SSH方式连接云服务器。

约束与限制

- 已安装Denyhosts插件。
- 该文档中操作涉及重启sshd服务，请在合理的时间进行操作。

方法一：通过编辑 sshd 配置文件实现允许或者禁止指定用户/用户组或者 IP 登录

1. 允许指定用户进行登录（白名单）
   在/etc/ssh/sshd_config 配置文件中设置AllowUsers选项，在配置文件末尾添加行格式如下（例如允许用户test通过192.168.1.2登录）。
   ```
   AllowUsers test@192.168.1.2
   ```
   说明
   配置了指定用户或者用户组允许登录后，默认拒绝其他所有用户或者用户组。
2. 禁止指定用户登录（黑名单）
   在 /etc/ssh/sshd_config 配置文件中设置DenyUsers选项，在配置文件末尾添加行格式如下（例如禁止用户testuser登录）。
   ```
   DenyUsers testuser
   ```
   上述修改需要重启sshd服务。
   CentOS 6系列执行以下命令进行重启：
   service sshd restart
   Centos 7/EulerOS系列执行以下命令进行重启：
   systemctl restart sshd

方法二：使用 DenyHosts 允许或者禁止指定 IP 通过 SSH 登录

linux 服务器通过设置 /etc/hosts.allow 和 /etc/hosts.deny 这个两个文件，可以限制或者允许某个或者某段IP地址远程SSH登录服务器.方法比较简单，具体如下：

1. 允许192.168.1.3 这个IP地址ssh登录，打开/etc/hosts.allow，添加如下行：
   ```
   sshd: 192.168.1.3
   ```
2. 禁止所有ip通过ssh登录，打开/etc/hosts.deny，添加如下行：
   ```
   sshd：ALL
   ```
   说明
   hosts.allow 和hosts.deny 两个文件同时设置规则的时候，hosts.allow 文件中的规则优先级高，假设按照上述方法设置后服务器只允许192.168.1.3这个IP地址的SSH登录，其它的IP 都会拒绝。

9.3 CentOS 7 修改 SSH 默认端口后无法连接怎么办?

问题现象

修改SSH服务的默认端口后，安全组入方向也放通了该端口，但无法SSH连接云服务器 。

约束与限制

本节操作适用于CentOS 7系列操作系统。

根因分析

1. 登录管理控制台，并通过**VNC方式**登录云服务器。
2. 执行以下命令，查看是否开启了firewalld。

   systemctl status firewalld

   图 9-1 开启 firewalld

   ```
   [root@ecs-test ~]# systemctl status firewalld
   ● firewalld.service - firewalld - dynamic firewall daemon
     Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor preset: enabled)
     Active: active (running) since Wed 2019-06-19 11:41:21 CST; 44s ago
       Docs: man:firewalld(1)
   Main PID: 5059 (firewalld)
     CGroup: /system.slice/firewalld.service
             └─5059 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid

   Jun 19 11:41:20 ecs-test systemd[1]: Starting firewalld - dynamic firewall daemon...
   Jun 19 11:41:21 ecs-test systemd[1]: Started firewalld - dynamic firewall daemon.
   ```

   如图9-1所示，系统已开启firewalld。
3. 执行以下命令，查看firewalld中的规则。

   firewall-cmd --list-all

   图 9-2 查看 firewalld 规则

   ```
   [root@ecs-test ~]# firewall-cmd --list-all
   public (active)
     target: default
     icmp-block-inversion: no
     interfaces: eth0
     sources:
     services: ssh dhcpv6-client
     ports:
     protocols:
     masquerade: no
     forward-ports:
     source-ports:
     icmp-blocks:
     rich rules:
   ```

   如图9-2所示，firewall当前的zone为public，该zone默认只放通ssh和dhcpv6-client服务。其中ssh服务为默认的22端口，当ssh修改为非22端口时就无法访问。

处理方法

- 方法1：执行以下命令，停止firewalld服务并取消开机自启。

  建议通过安全组和ACL进行访问控制，如业务需要开启firewalld请参考**•方法2：执行以下命令，在firewalld服务...**

  systemctl stop firewalld

  systemctl disable firewalld

- 方法2：执行以下命令，在firewalld服务中添加新的端口55660。

  firewall-cmd --add-port=55660/tcp --permanent --zone=public

  firewall-cmd --reload

9.4 /etc/passwd 文件损坏导致云服务器登录失败怎么办?

操作场景

本节操作适用于Linux操作系统云服务器/etc/passwd文件损坏导致云服务器无法登录的问题。

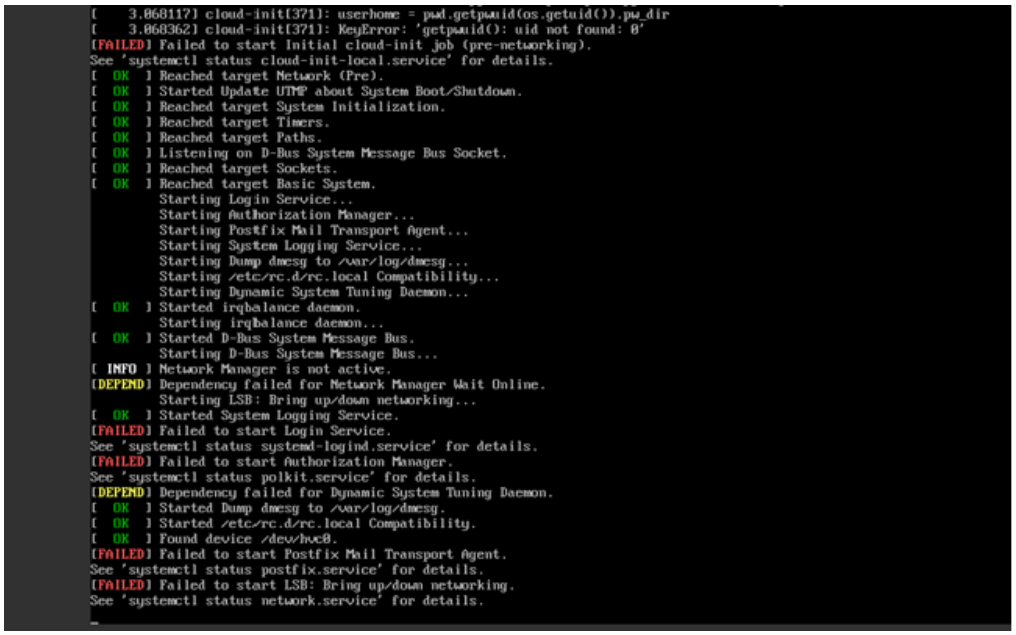
说明

- 本节操作为紧急恢复系统方法，需要在单用户模式下会将系统备份初始备份/etc/passwd-文件替换已损坏的/etc/passwd文件，该操作会造成自行添加的用户丢失（包括应用运行的用户，可以参考/etc/shadow文件添加其他账号）。
- 本节操作涉及重启云服务器操作，重启云服务器会造成业务中断，请谨慎操作。

问题描述

Linux系统中多个服务启动失败：Failed to start Login service 、Failed to start Authorization service。

待系统启动后登录，提示密码错误。



根因分析

/etc/passwd和/etc/shadow文件记录所有的用户信息，每个用户都有一个对应的记录行，如果该文件损坏或者误删除会导致登录服务（systemd-logind.service）启动失败，因此用户无法登录。

处理方法

1. 在控制台重启主机，进入单用户模式。

   详细操作，请参见**Linux云服务器如何进入单用户模式?**

2. 执行以下命令检查/etc/passwd文件 。

   cat /etc/passwd

3. 确认passwd文件已被破坏，执行以下命令使用系统初始的备份passwd-文件替换损坏的passwd文件 。

   cp /etc/passwd- /etc/passwd

   说明

   该操作会造成自行添加的用户丢失，如果为应用运行的用户会导致应用启动失败，待修复后请自行添加用户。

4. 执行以下命令退出当前根目录至initramfs的根目录。

   exit

5. 重启云服务器。

6. （可选）待系统启动，添加丢失的用户，例如执行以下命令添加Nginx运行用户nobody并指定该用户shell为/sbin/nologin（请根据场景添加用户，需要登录系统的用户需要指定shell为/bin/bash）。

   useradd nobody -s /sbin/nologin

9.5 开启 UseDNS 导致 SSH 连接缓慢怎么办?

问题现象

SSH方式连接云服务器，出现卡顿，需要较长时间才可以连接。

根因分析

服务端sshd服务开启UseDNS选项状态下，当客户端试图使用SSH连接服务器时，服务器端先根据客户端的IP地址进行DNS PTR反向查询出客户端的主机名，然后根据查询出的客户端主机名进行DNS正向A记录查询，验证与其原始IP地址是否一致，这是防止客户端欺骗的一种措施，但一般我们的是动态IP不会有PTR记录，建议关闭该选项。

执行如下命令确认是否开启了UseDNS选项。

grep UseDNS /etc/ssh/sshd_config

如果该选项值为“yes”或者为注释行则说明已开启该选项。建议参考本节操作修改UseDNS。

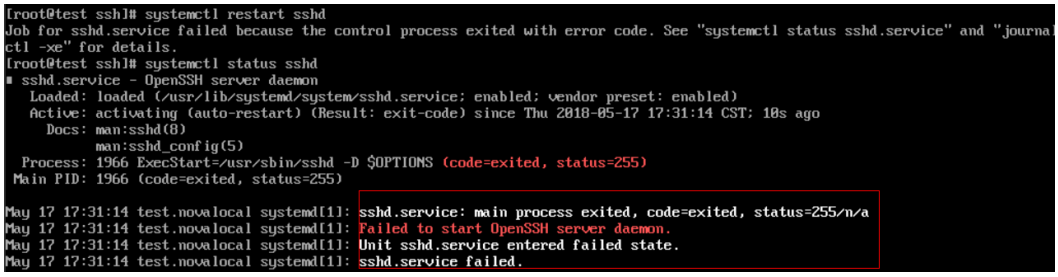
处理方法

1. 执行以下命令，编辑/etc/ssh/sshd_config文件。
   vi /etc/ssh/sshd_config
2. 修改UseDNS选项值为no。
   ```
   UseDNS no
   ```
3. 重启sshd服务。
   - CentOS6执行
     service sshd restart
   - CentOS7/EulerOS执行
     systemctl restart sshd

9.6 Linux 启动 sshd 服务出现/var/empty/sshd 无法访问的解决方案

问题现象

Linux云服务器启动sshd服务失败，出现/var/empty/sshd无法访问的问题。

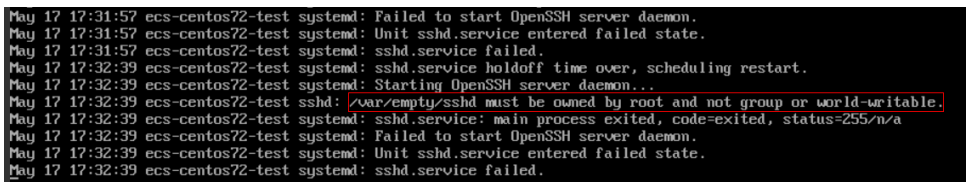


适用场景

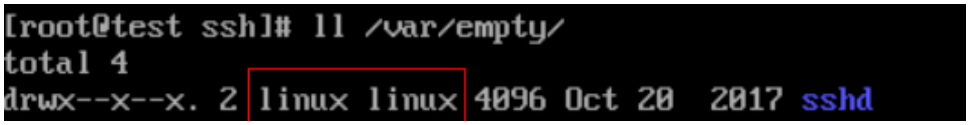
本节操作适用于CentOS7/EulerOS系统，其他Linux系统可能存在差异。

场景一：/var/empty/sshd 属主非 root 导致 sshd 启动失败

1. sshd启动失败，查看journal日志，提示/var/empty/sshd must be owned by root。
   journalctl -xe



2. 查看/var/empty/sshd文件属主信息
   ll /var/empty/sshd



如上图所示，由于/var/empty/sshd目录属主非root用户导致sshd服务启动失败。

3. 修改/var/empty/sshd属主，及其权限。

   chown -R root.root /var/empty/sshd

   chmod -R 711 /var/empty/sshd

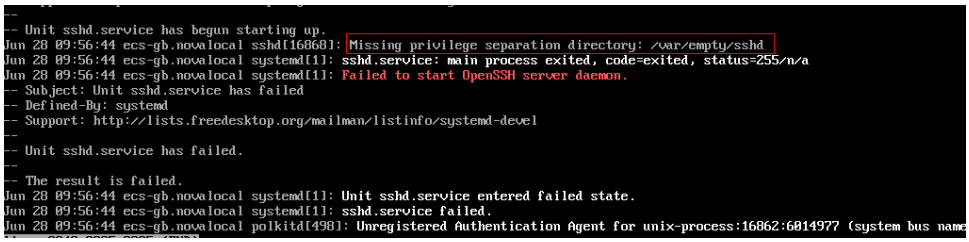
4. 重启sshd服务，执行：

   systemctl restart sshd

场景二：/var/empty/sshd 文件缺失导致 sshd 启动失败

1. 执行以下命令，查看服务失败原因。

   journalctl -xe



2. 从上图可知由于/var/empty/sshd缺失导致sshd启动失败，执行以下命令，手动创建该目录。

   mkdir -p /var/empty/sshd

3. 重启sshd服务。

   systemctl restart sshd

9.7 怎样禁用 SSH 密码方式连接云服务器?

操作场景

基于云服务器访问安全的考虑，云服务器的访问密钥需定期更换，有时需要禁用SSH密码登录方式。

本节操作介绍禁用SSH密码方式连接云服务器的操作步骤。

说明

- 该设置方法仅对SSH连接方式有效，控制台仍然可以使用密码登录方式，请务必保存好云服务器登录密码。
- 该设置方法不适用于Ubuntu 22.04操作系统的云服务器。

操作步骤

1. 登录Linux云服务器，执行以下命令编辑云服务器SSH连接方式。

   vi /etc/ssh/sshd_config

   修改如下配置项：

   把PasswordAuthentication yes改为PasswordAuthentication no

2. 重启sshd使修改生效。

   service sshd restart

3. 重启云服务器。
4. 通过SSH密码方式连接云服务器。
   具体操作步骤，请参见**SSH密码方式登录**。
   如果提示连接失败，说明已成功禁用SSH密码访问方式。

9.8 SSH 连接或者服务偶发性断开问题处理

适用场景

该文档适用于在SSH连接Linux云服务器或者访问该服务器上的应用时偶现连接断开。

约束与限制

1. 修改系统内核参数可能产生内核不稳定，请评估风险后进行操作。
2. 为了确保系统稳定运行，修改内核参数后建议在合理的时间重启系统。

根因分析

1. 执行以下命令，查看系统内核是否开启了TIME_WAIT快速回收和重利用策略
   sysctl -a |grep tcp_tw
   如图9-3所示，确认已开启该策略。

   图 9-3 TIME_WAIT

   ```
   [root@ecs-feilsystemd-test ~]# sysctl -a |grep tcp_tw
   sysctl: reading key "net.ipv6.conf.all.stable_secret"
   sysctl: reading key "net.ipv6.conf.default.stable_secret"
   sysctl: reading key "net.ipv6.conf.eth0.stable_secret"
   sysctl: reading key "net.ipv6.conf.lo.stable_secret"
   net.ipv4.tcp_tw_recycle = 1
   net.ipv4.tcp_tw_reuse = 1
   ```

2. 由于服务端开启了TIME_WAIT快速回收和重利用策略导致，即启用了net.ipv4.tcp_tw_recycle或者net.ipv4.tcp_tw_reuse。系统默认是不启用该功能。

   说明

   客户端通常在NAT环境下，多台终端使用同一个公网ip，无法实现服务端与客户端的一对一连接。如果开启此参数服务端会回收处于TIME_WAIT状态的TCP连接，导致连接断开。

操作方法：

1. 关闭上述两个内核参数，打开/etc/sysctl.conf，添加或者修改下列两行。
   ```
   net.ipv4.tcp_tw_recycle = 0
   net.ipv4.tcp_tw_reuse = 0
   ```
2. 执行以下命令，使修改的配置生效。
   sysctl -p

   说明

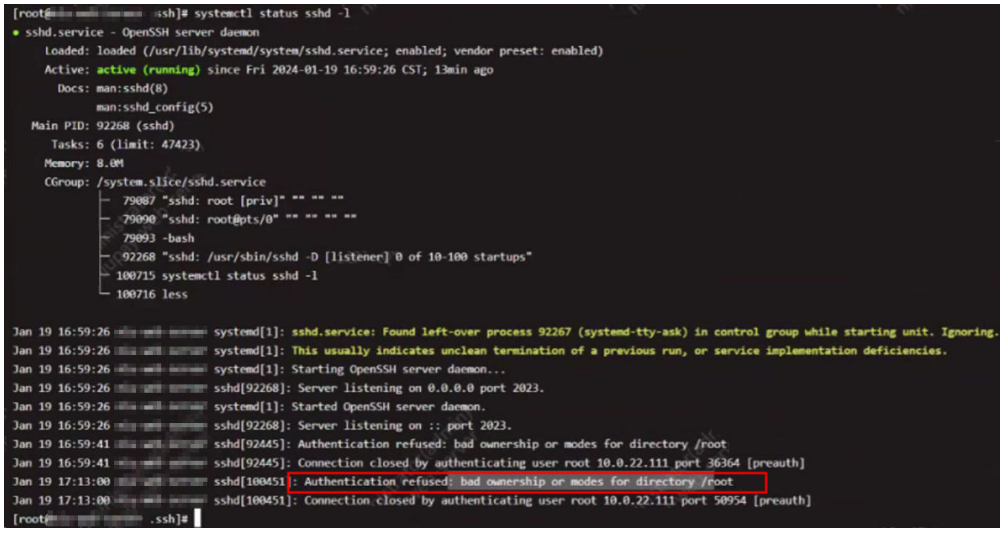
   启动中修改内核参数可能存在内核加载该参数不稳定的情况，建议在合适的时间进行重启。

9.9 SSH 密钥无法登录，报错 Authentication refused: bad ownership or modes for directory /root

问题描述

SSH密钥无法登录，报错Authentication refused: bad ownership or modes for directory /root

图 9-4 SSH 密钥无法登录

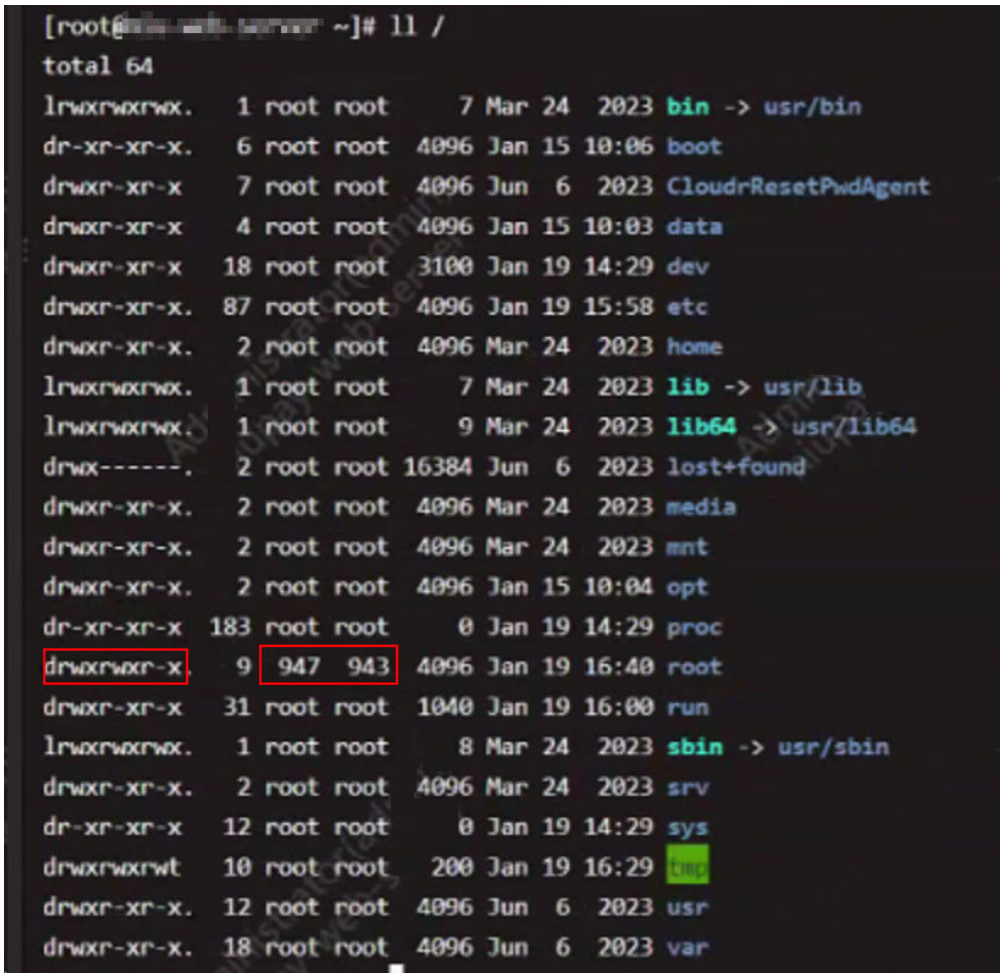


可能原因

根据日志报错，提示/root这个目录权限问题，排查/root目录，以及目录内的.ssh，.ssh目录内authorized_keys的权限以及属主属组。

处理方法

修改/root目录的权限以及属主属组后，SSH恢复正常。



9.10 如何解决 Ubuntu 16.04 云服务器可以通过 SSH 成功登录，但 VNC 界面无法到达登录界面的问题

问题描述

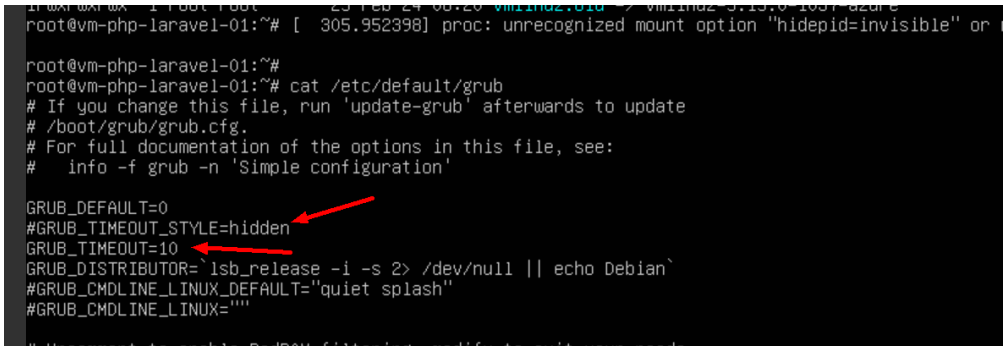
用户Ubuntu16.04系统通过SSH连接成功，但是VNC方式登录时到不了login界面。

约束与限制

本操作涉及修改grub配置文件，误操作可能会导致系统无法启动。操作前，请务必对grub配置文件进行备份，以便在发生误操作时能够进行恢复。

处理方法

1. Ubuntu 16.04云服务器通过SSH连接后，执行以下命令，修改grub配置。
   cat /etc/default/grub
   如下图所示，注释GRUB_TIMEOUT_STYLE=hidden，修改GRUB_TIMEOUT=10。



2. 删除/etc/default/grub.d/目录下以“50”开头的所有文件。

   rm -rf /etc/default/grub.d/50*

3. 执行以下命令，刷新配置。

   update-grub2

4. 执行以下命令，修改yum源用来安装公版内核。

   sed -i 's/azure.archive.ubuntu.com/repo.huaweicloud.com/g' /etc/apt/sources.list

   apt autoclean

   apt update

5. 执行以下命令，安装ubuntu16.04公版内核。

   apt install linux-image-generic

6. 安装完成重启后在grub页面选择generic内核启动系统。
7. （可选）执行以下命令，删除azurelinuxagent，因为agent会一直打印日志到VNC控制台，影响VNC的使用。

   sudo apt -y remove walinuxagent

9.11 SSH 服务启动时出现“main process exited, code=exited”错误

问题描述

在Linux系统的ECS实例中，使用service或systemctl命令启动SSH服务时，命令行没有返回任何报错信息，但服务没有正常运行。

执行cat /var/log/secure查看secure日志，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

通常是因为PATH环境变量配置异常，或SSH软件包相关文件被移除。

处理方法

1. 远程登录弹性云服务器。
2. 执行以下命令，检查环境变量配置。

echo $PATH

系统正常返回信息如下，该值为PATH环境变量的默认值。

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

若返回其他信息，表示环境变量的默认值被改变，则需执行以下命令，重置环境变量。

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

3. 执行以下命令，查找并确认SSH服务指令。

   find / -name sshd

   确保包含如下默认路径程序文件：

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

4. 如果相应文件不存在，则尝试通过 FTP 等方式从外部上传正常文件，或者重新安装SSH服务。
5. 执行以下命令，重启SSH服务。

   service sshd restart

6. 重新连接云服务器。

10 多用户登录

10.1 Windows 云服务器如何配置多用户登录？（Windows 2008）

操作场景

本节操作以Windows Server 2008操作系统的云服务器为例介绍实现多用户登录的操作步骤。

Windows server2008服务器默认能够支持两个用户同时远程登录，而通过配置远程桌面会话主机和远程桌面授权，即可实现多用户远程登录。

操作须知

- 请确保云服务器带宽资源充足，避免由于多用户同时操作负载过高导致云服务器卡顿或登录异常。
- 所在安全组入方向已开放云服务器登录使用的端口，默认使用3389端口。
- 云服务器已经绑定弹性公网IP。
- 配置多用户登录后，不同的用户登录云服务器操作互相之间无影响。
- Windows Server 2012版本操作系统安装桌面会话主机和远程桌面授权时操作步骤与Windows Server 2008版本不同，如果您使用的是Windows Server 2012操作系统请参考**Windows云服务器如何配置多用户登录？（Windows 2012）**。
- 完成本节操作的配置后可以实现多个用户同时远程登录或同一用户多个远程登录。但是远程桌面授权仅支持120天，过期后将因缺失远程桌面授权服务器许可证而导致多用户登录无法使用。如需激活远程桌面授权请参考**申请多用户会话授权的license并激活云服务器**。
- 远程桌面授权仅支持120天，过期后远程连接服务器时会提示“没有远程桌面授权服务器可以提供许可证”，请参考**远程连接Windows云服务器云主机报错：没有远程桌面授权服务器可以提供许可证**，删除远程桌面服务。
- 配置多用户登录后，可能会出现多用户登录Windows主机时无法打开浏览器的问题，解决方法请参考**多用户登录Windows主机时无法打开浏览器**。

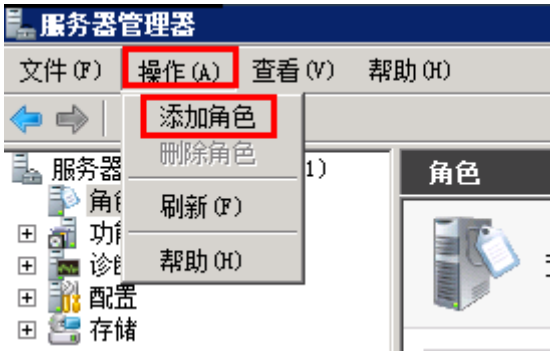
操作步骤

1. 安装桌面会话主机和远程桌面授权
2. 允许多用户远程连接云服务器
3. 配置新用户并加入远程桌面用户组

安装桌面会话主机和远程桌面授权

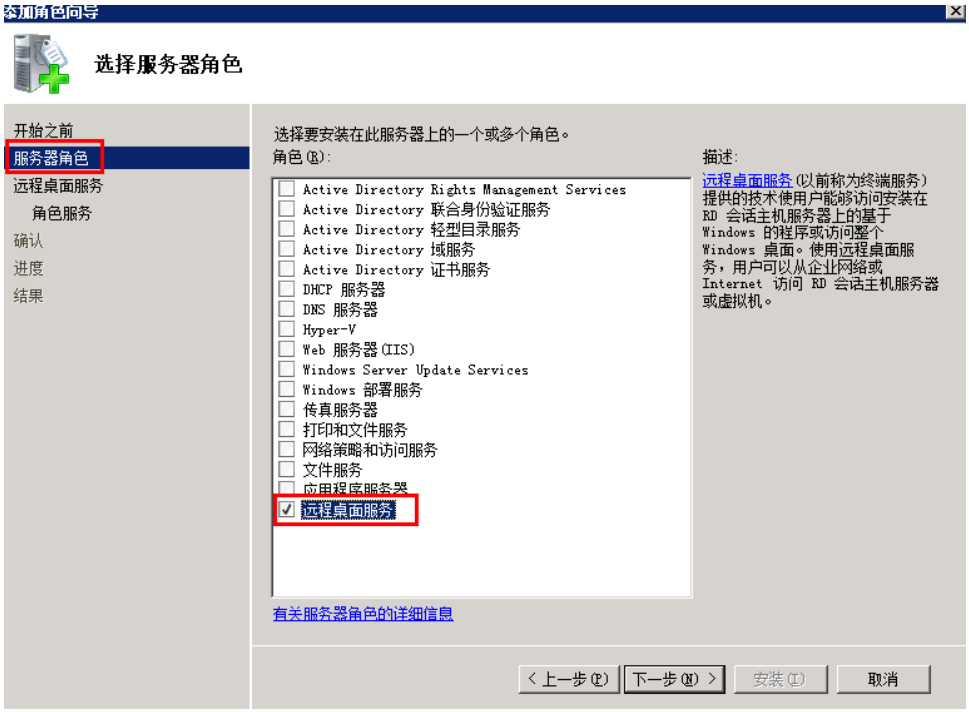
1. 登录Windows云服务器。
2. 在操作系统界面，单击  打开“服务器管理器”，单击“角色 > 操作 > 添加角色”。

图 10-1 添加角色



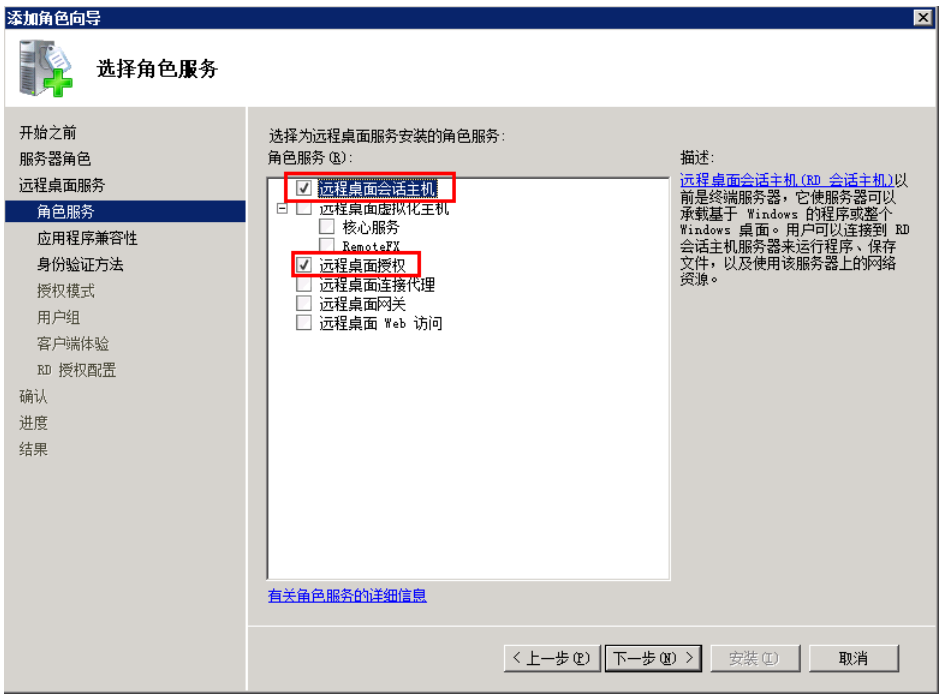
3. 单击“服务器角色”，选择“远程桌面服务”，单击“下一步”。

图 10-2 选择远程桌面服务



4. 保持默认参数，单击“下一步”，出现如下安装界面，选择“远程桌面会话主机”和“远程桌面授权”，单击“下一步”。

图 10-3 安装远程桌面角色

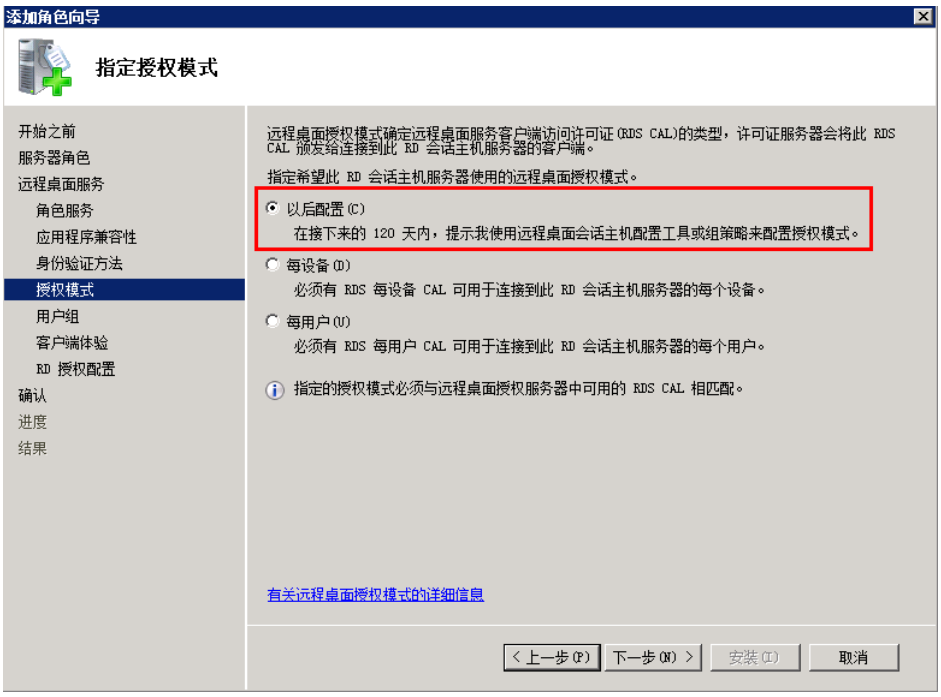


5. 保持默认参数，单击“下一步”。
6. 指定远程桌面会话主机的身份验证方法，单击“下一步”。本例中选择“需要使用网络级别身份验证”。

图 10-4 指定远程桌面会话主机的身份验证方法

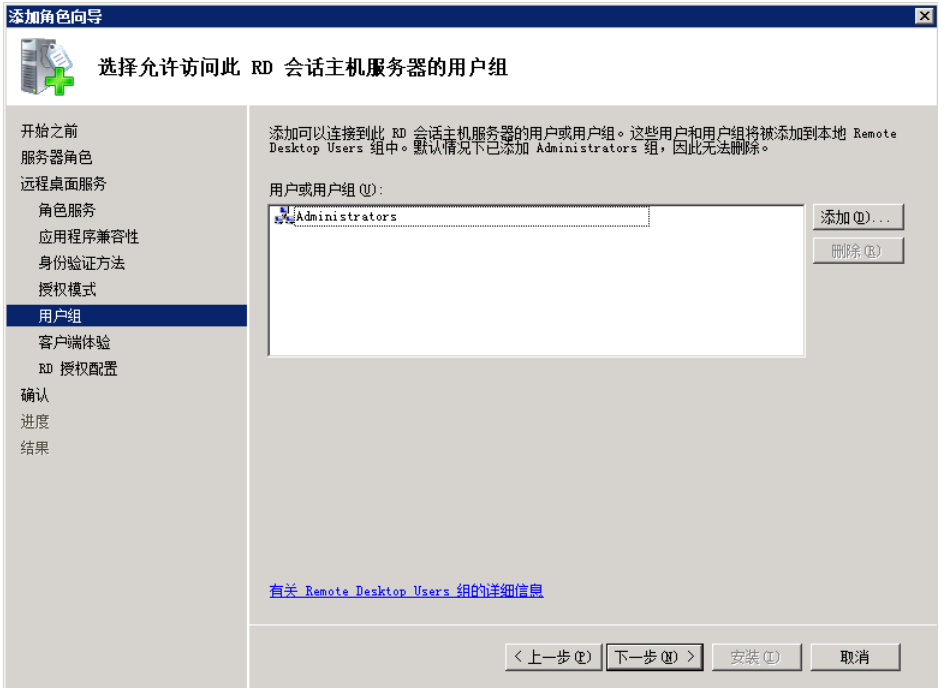
7. 指定授权模式。本例中选择“以后配置”。

图 10-5 指定授权模式。



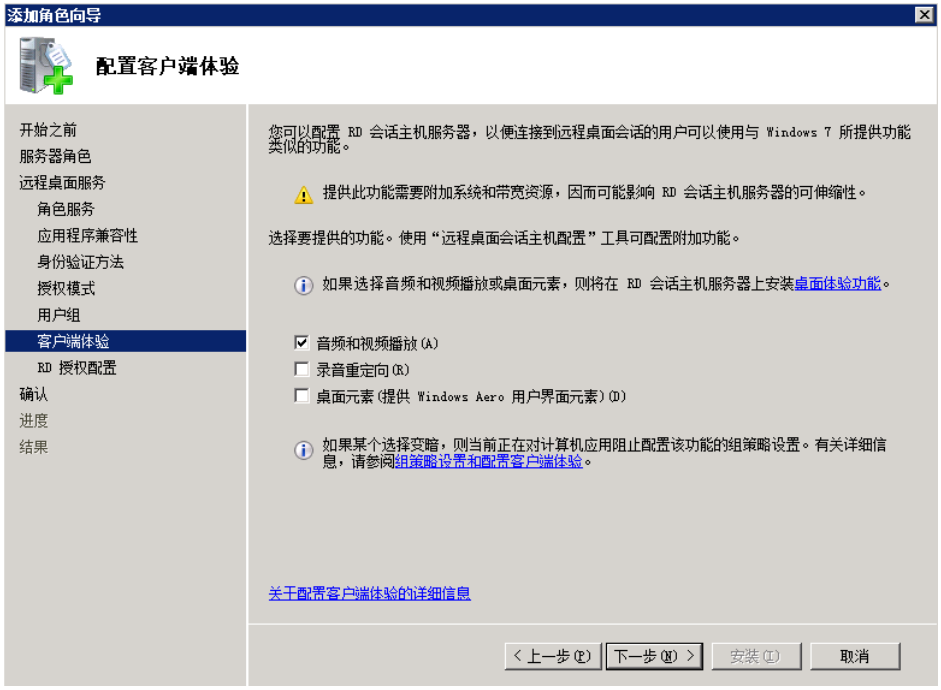
8. 选择允许访问此RD会话主机服务器的用户组。

图 10-6 选择用户组



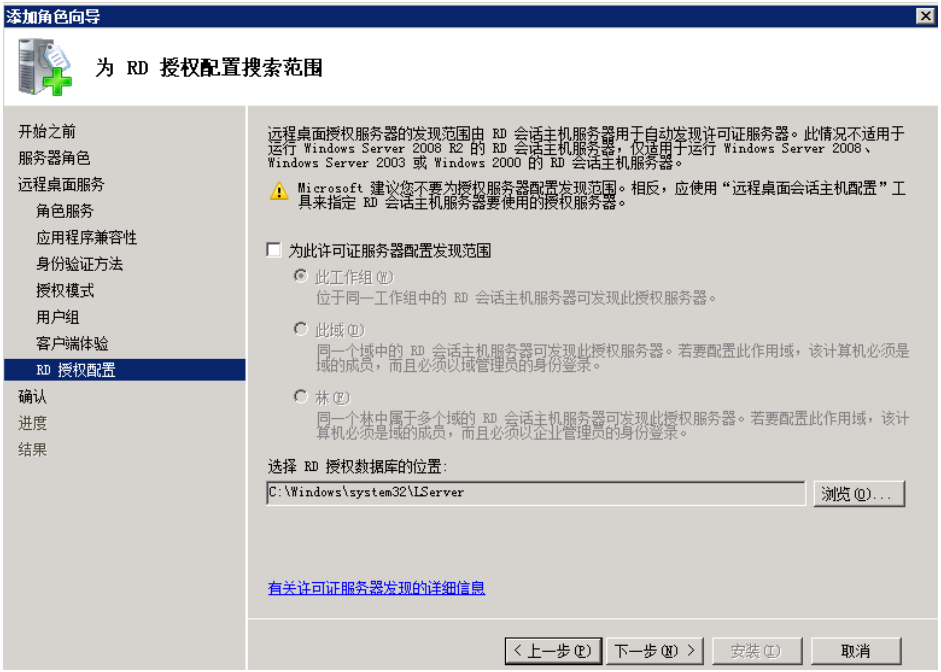
9. 配置客户端体验。本例中选择“音频和视频播放”。

图 10-7 配置客户端体验



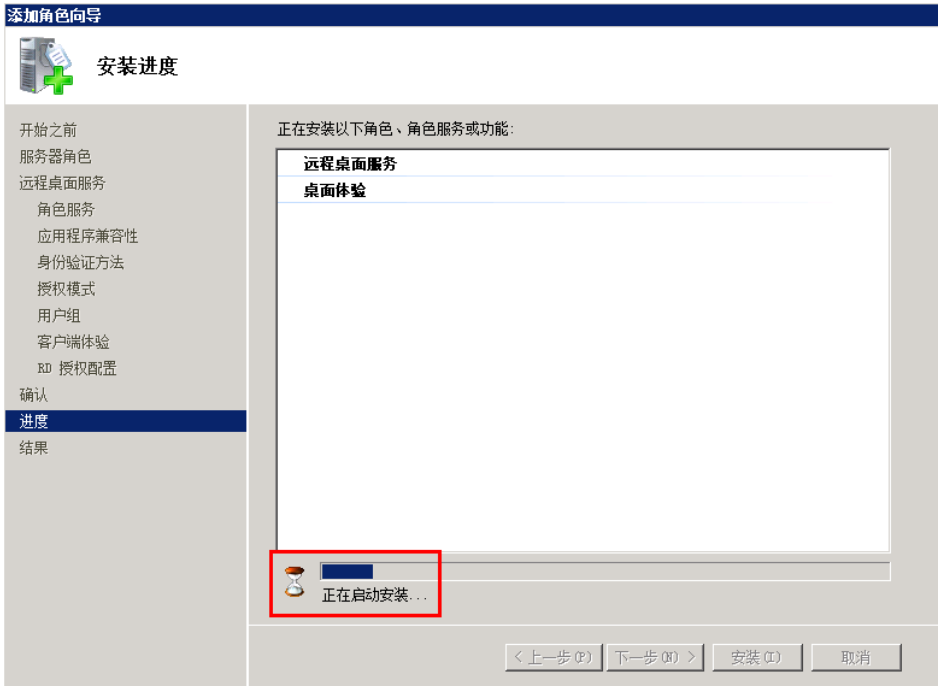
10. 为RD授权配置搜索范围。

图 10-8 为 RD 授权配置搜索范围



11. 确认安装选择，单击“安装”。

图 10-9 安装远程桌面服务



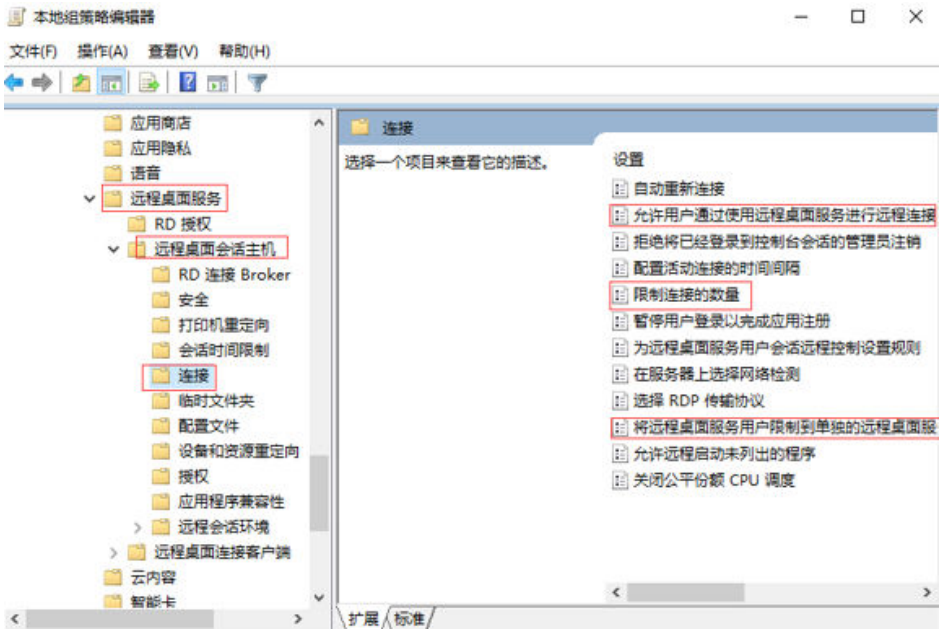
允许多用户远程连接云服务器

1. 在运行里输入“gpedit.msc”，打开计算机本地组策略。

图 10-10 gpedit.msc

2. 在计算机本地组策略里选择“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 > 连接”。如下图所示设置“允许用户通过使用远程桌面服务进行远程连接”、“限制连接数量（可根据具体数量设置）”和“将远程桌面服务用户限制到单独的远程桌面”。

图 10-11 设置“连接”

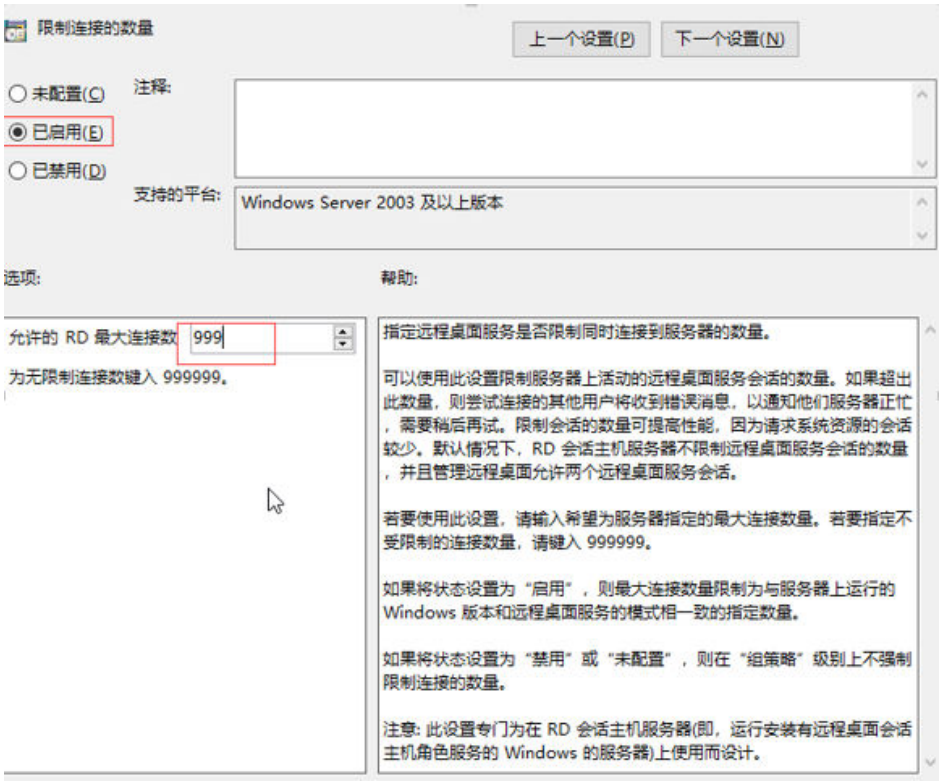


3. 右键单击“编辑”，设置“允许用户通过使用远程桌面服务进行远程连接”为已启用。

图 10-12 允许用户通过使用远程桌面服务进行远程连接

4. “限制连接数量”选择已启用，可根据具体数量设置。

图 10-13 限制连接数量

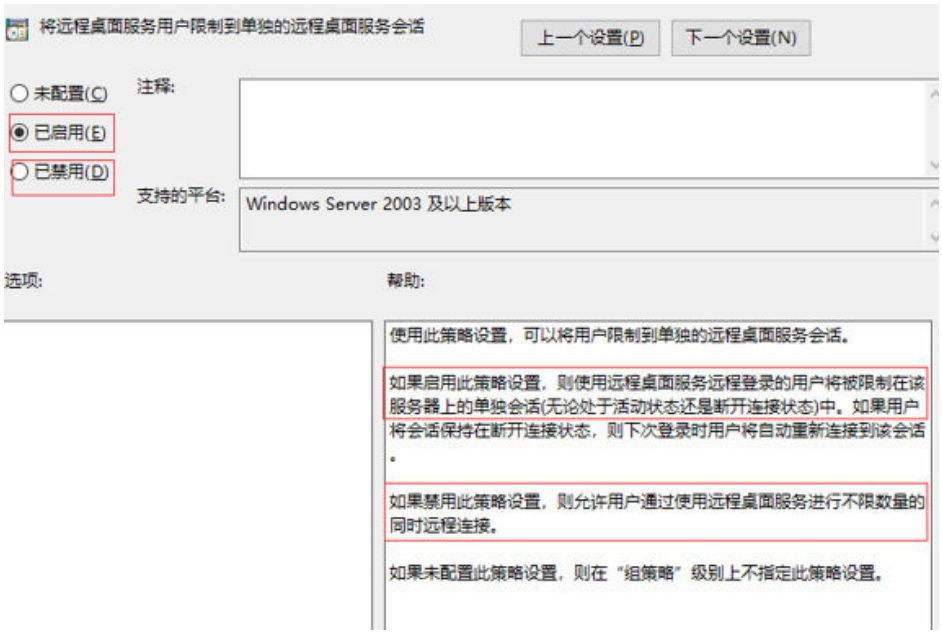


5. “将远程桌面服务用户限制到单独的远程桌面”选择已启用，或者已禁用，请注意此处已启用和已禁用的区别。本例以勾选“已启用”为例。
   - 已启用：多个用户同时登录的多用户登录，不能单个用户多登录。

     例如：配置为已启用，用户A、用户B、用户C可以分别使用账号A、账号B、账号C同时登录云服务器，但是不支持用户A、用户B、用户C使用同一个账号同时登录云服务器。
   - 已禁用：单个用户同时多个登录的多用户登录。

     例如：配置为已禁用，用户A、用户B、用户C可以使用同一个账号同时登录云服务器。

图 10-14 将远程桌面服务用户限制到单独的远程桌面



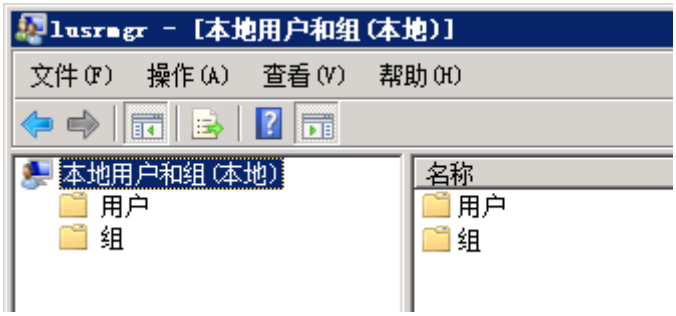
6. 运行cmd，输入”gpupdate /force”，强制执行本地组策略，重启服务器，整个配置过程完成。

配置新用户并加入远程桌面用户组

如果配置“多个用户同时登录的多用户登录”，那么在创建完新用户后需要将其加入远程桌面用户组。本小节操作介绍创建新用户并添加用户到远程桌面用户组的操作步骤。

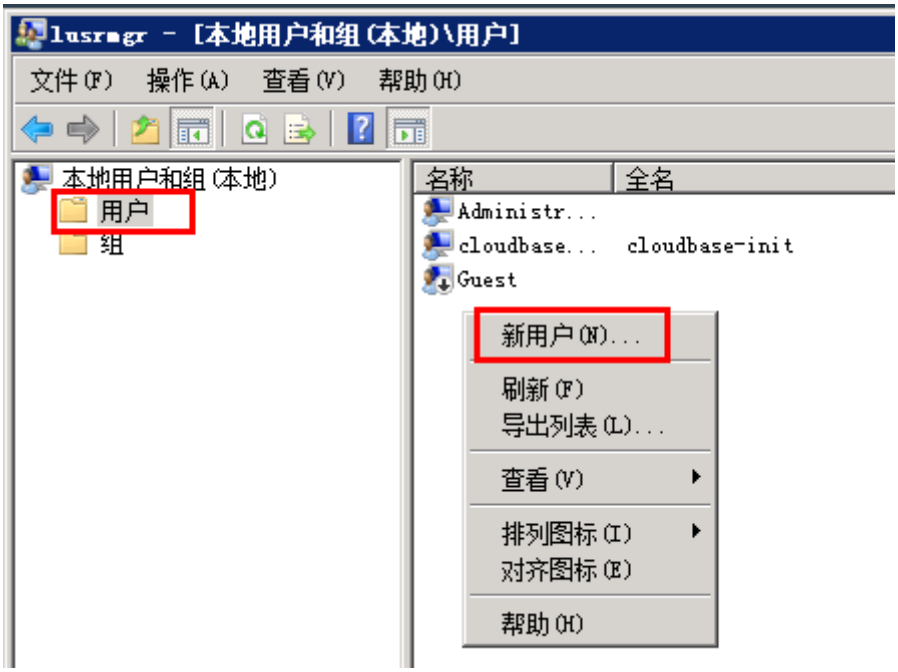
1. 在运行中输入**lusrmgr.msc**，打开本地用户和组，进行新用户创建。

图 10-15 lusrmgr.msc



2. 单击“用户”，在空白处右键选择新用户。

图 10-16 选择新用户

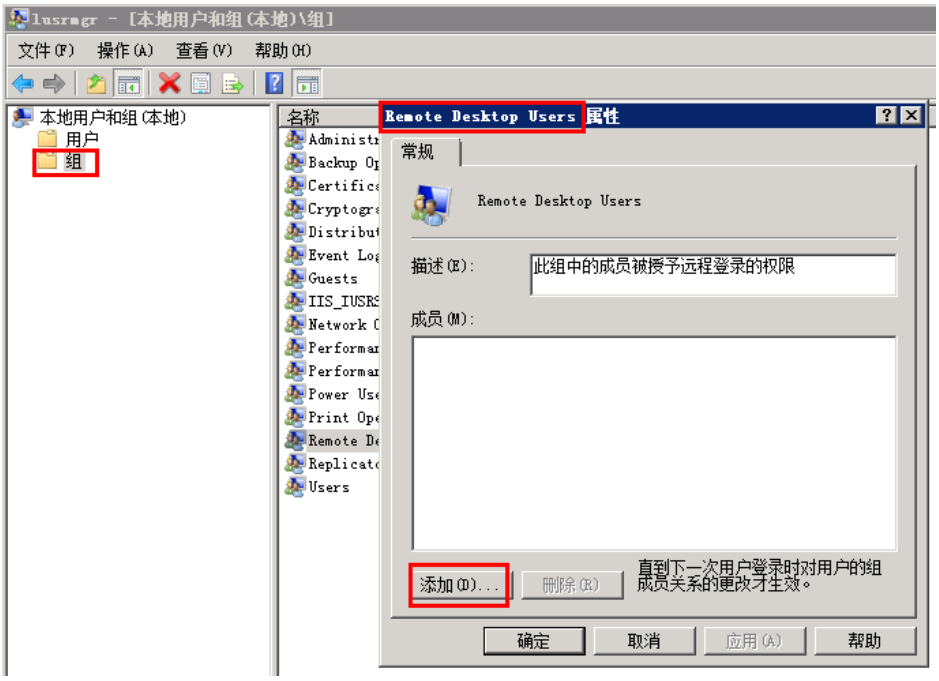


3. 填写新用户信息，单击“创建”。

图 10-17 填写新用户信息

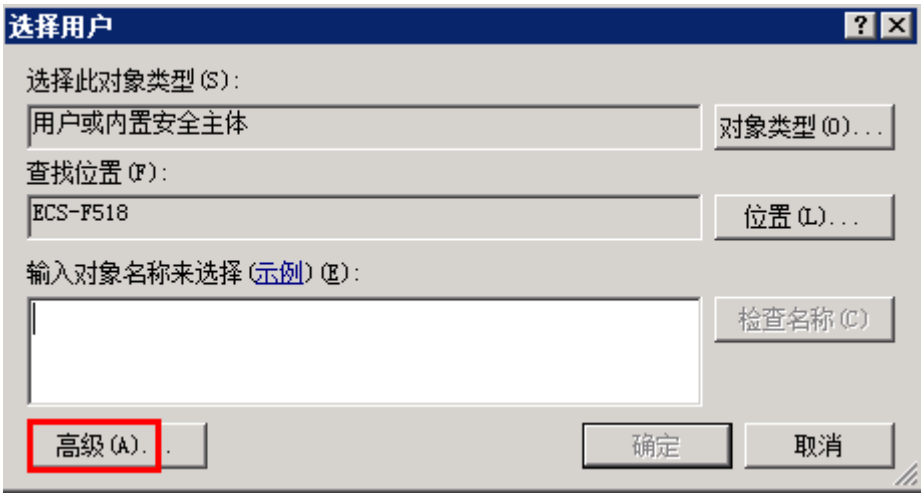
4. 单击“组”，双击打开Remote Desktop Users组，单击“添加”。

图 10-18 Remote Desktop Users 组



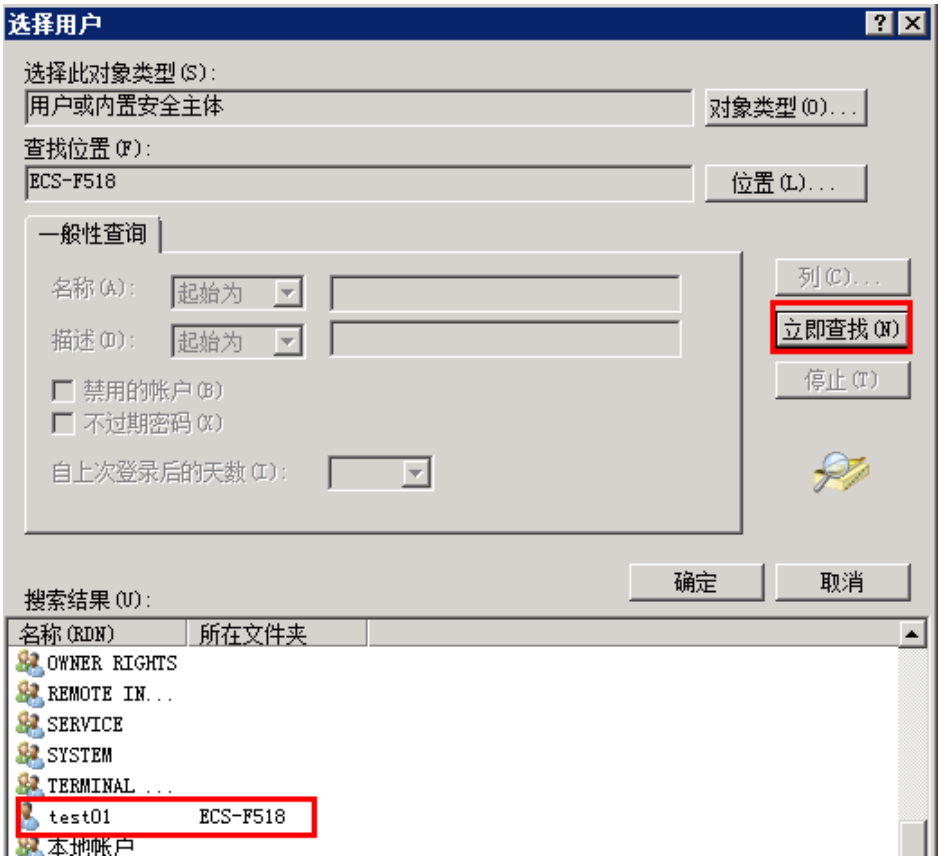
5. 进入选择用户界面，单击“高级”。

图 10-19 选择用户界面



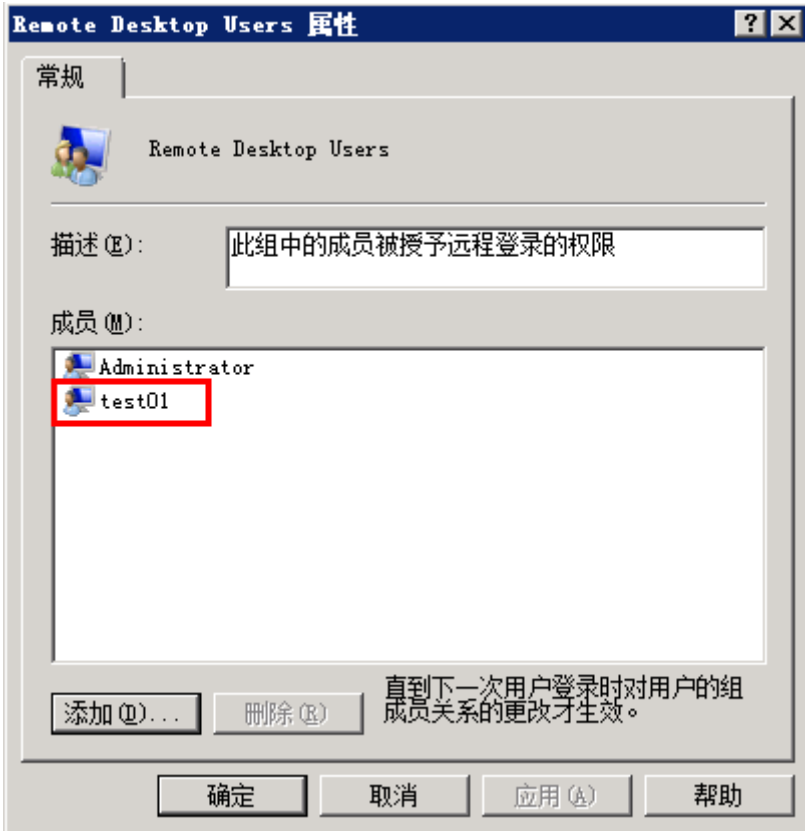
6. 在新的选择用户界面，单击“立即查找”，在下方搜索结果中选中需要远程登录的用户，并单击“确定”，完成添加，即可远程登录。

图 10-20 选择用户



7. 单击“确定”，添加用户到Remote Desktop Users组。

图 10-21 确认成员信息



后续操作

如需激活远程桌面授权请参考**申请多用户会话授权的license并激活云服务器**。

10.2 Windows 云服务器如何配置多用户登录？（Windows 2012）

操作场景

本节操作以Windows Server 2012操作系统的云服务器为例介绍实现多用户登录的操作步骤。

Windows server2012服务器默认能够支持两个用户同时远程登录，而通过配置远程桌面会话主机和远程桌面授权，即可实现多用户远程登录。

操作须知

- 请确保云服务器带宽资源充足，避免由于多用户同时操作负载过高导致云服务器卡顿或登录异常。
- 所在安全组入方向已开放云服务器登录使用的端口，默认使用3389端口。
- 云服务器已经绑定弹性公网IP。
- 配置多用户登录后，不同的用户登录云服务器操作互相之间无影响。

- Windows Server 2008版本操作系统安装桌面会话主机和远程桌面授权时操作步骤与Windows Server 2012版本不同，如果您使用的是Windows Server 2008操作系统请参考**Windows云服务器如何配置多用户登录？（Windows 2008）**。
- 完成本节操作的配置后可以实现多个用户同时远程登录或同一用户多个远程登录。但是远程桌面授权仅支持120天，过期后将因缺失远程桌面授权服务器许可证而导致多用户登录无法使用。如需激活远程桌面授权请参考**申请多用户会话授权的license并激活云服务器**。
- 远程桌面授权仅支持120天，过期后远程连接服务器时会提示“没有远程桌面授权服务器可以提供许可证”，请参考**远程连接Windows云服务器云主机报错：没有远程桌面授权服务器可以提供许可证**，删除远程桌面服务。
- 配置多用户登录后，可能会出现多用户登录Windows主机时无法打开浏览器的问题，解决方法请参考**多用户登录Windows主机时无法打开浏览器**。

操作步骤

1. **安装桌面会话主机和远程桌面授权**
2. **允许多用户远程连接云服务器**
3. **配置新用户并加入远程桌面用户组**

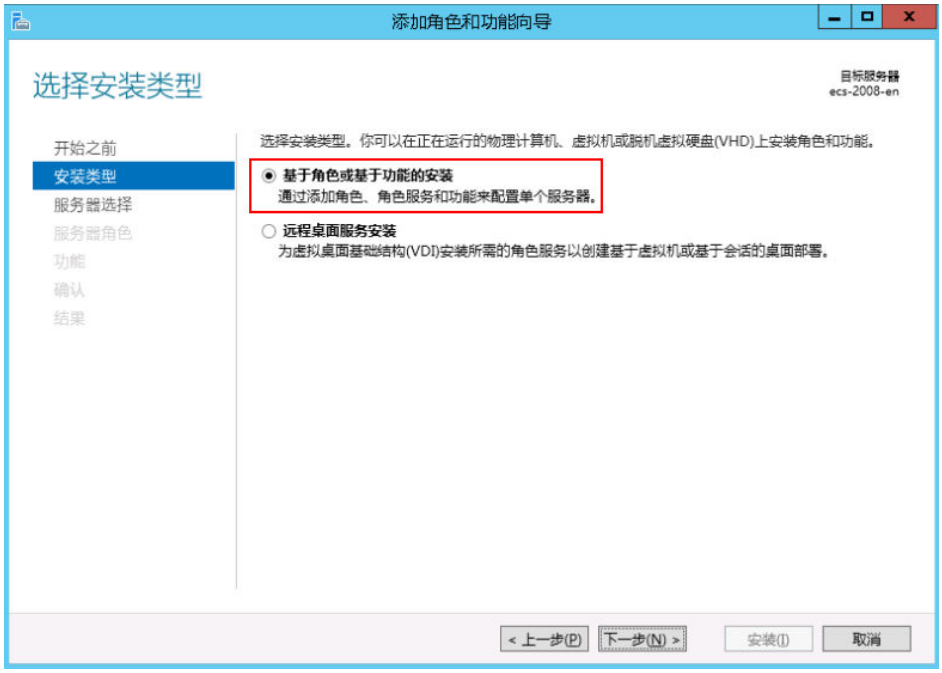
安装桌面会话主机和远程桌面授权

1. 登录Windows云服务器。
2. 在操作系统界面，单击  打开“服务器管理器”，单击“添加角色和功能”。

图 10-22 添加角色和功能

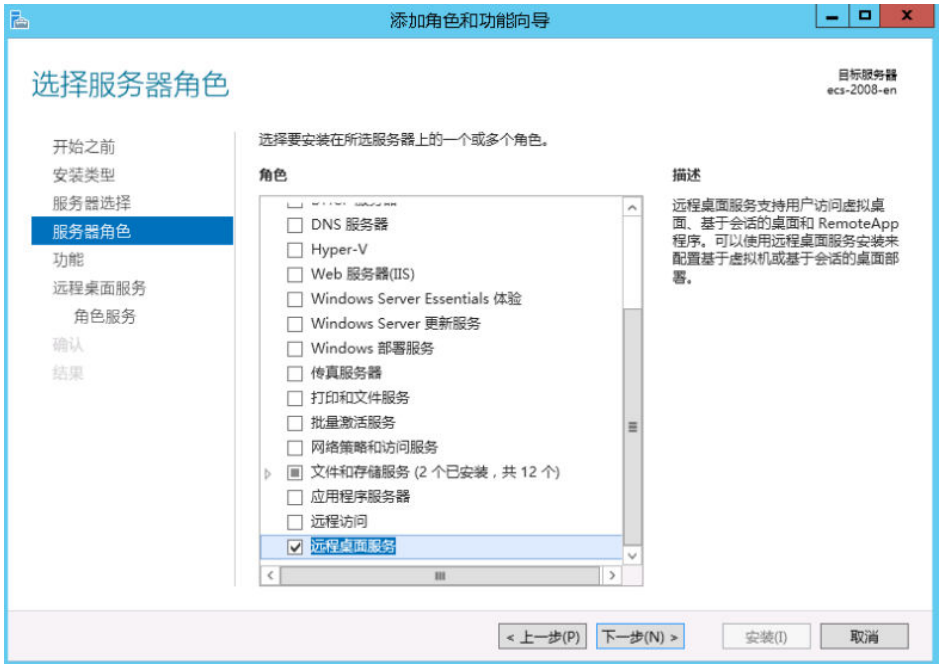
3. 保持默认参数，单击“下一步”，出现如下安装界面，选择“基于角色或基于功能的安装”，单击“下一步”。

图 10-23 添加角色和功能向导



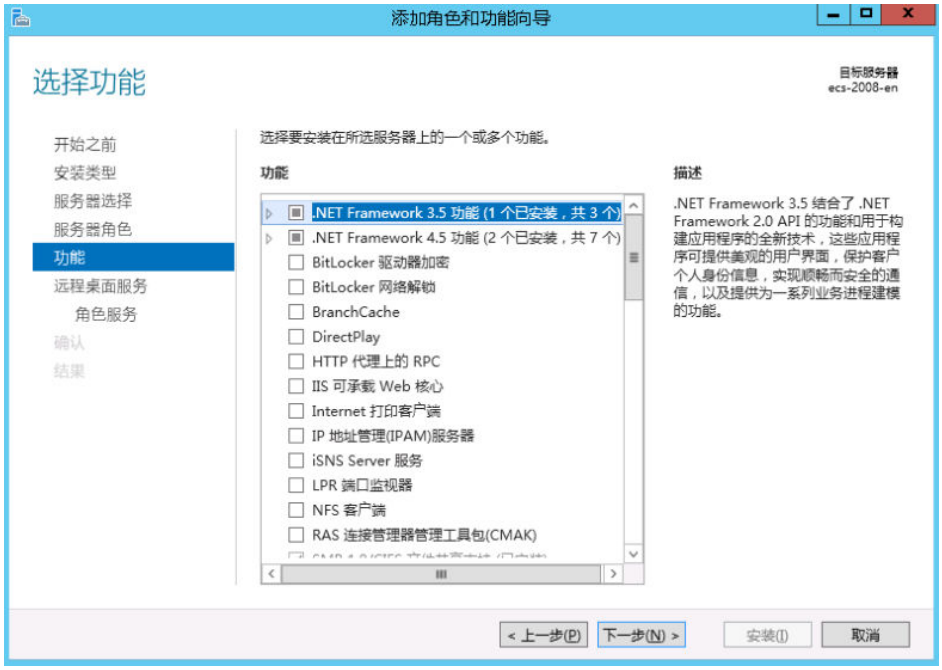
4. 选择“从服务器池中选择服务器”，单击“下一步”。
5. 选择“远程桌面服务”，单击“下一步”。

图 10-24 远程桌面服务



6. 在“功能”页面保持默认参数，单击两次“下一步”。

图 10-25 功能页面



7. 在 “选择角色服务” 界面，依次勾选“远程桌面会话主机”和“远程桌面授权 ”，在弹出的窗口中单击“添加功能”，单击“下一步”。

图 10-26 添加功能

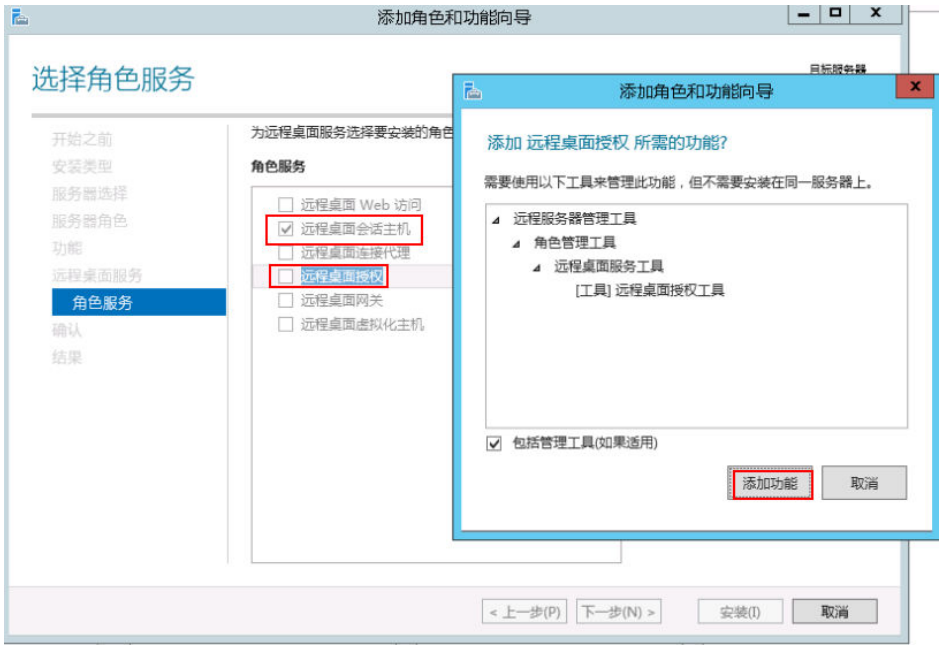
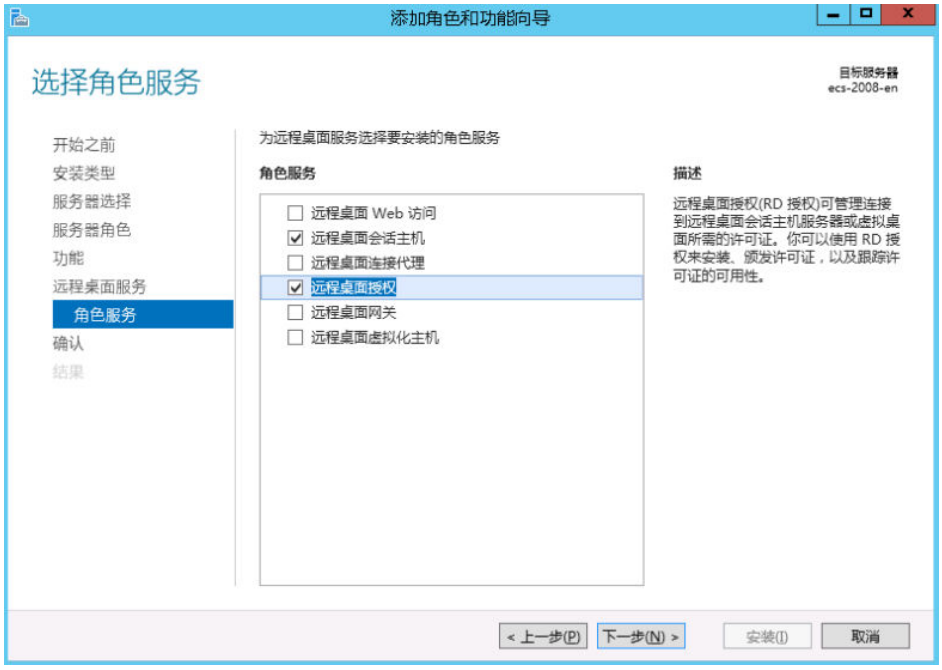


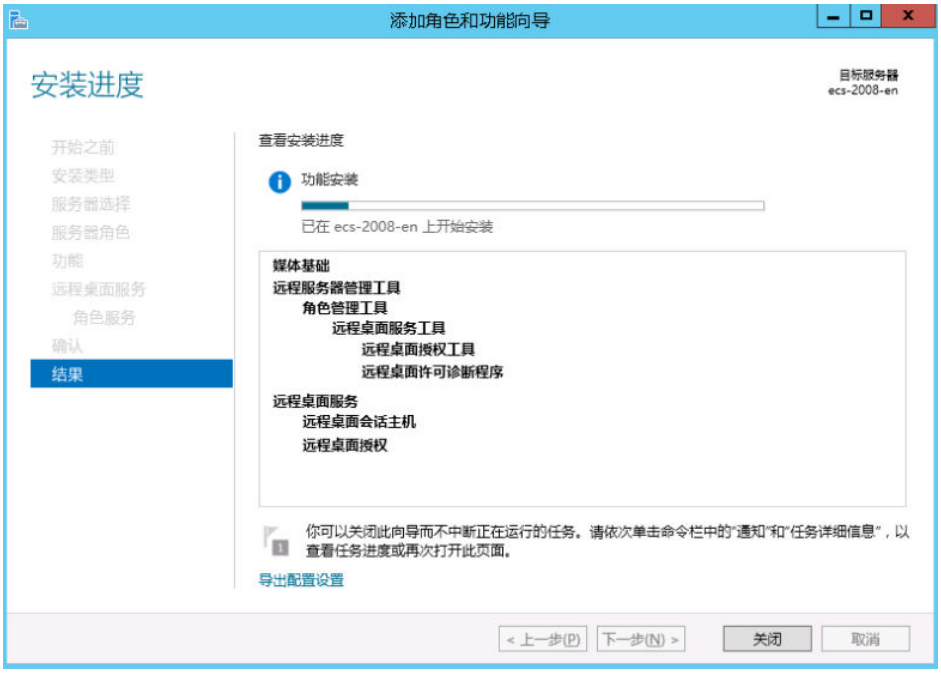
图 10-27 远程桌面授权



8. 确认在云服务器上安装的角色，单击“安装”。

图 10-28 安装

图 10-29 功能安装



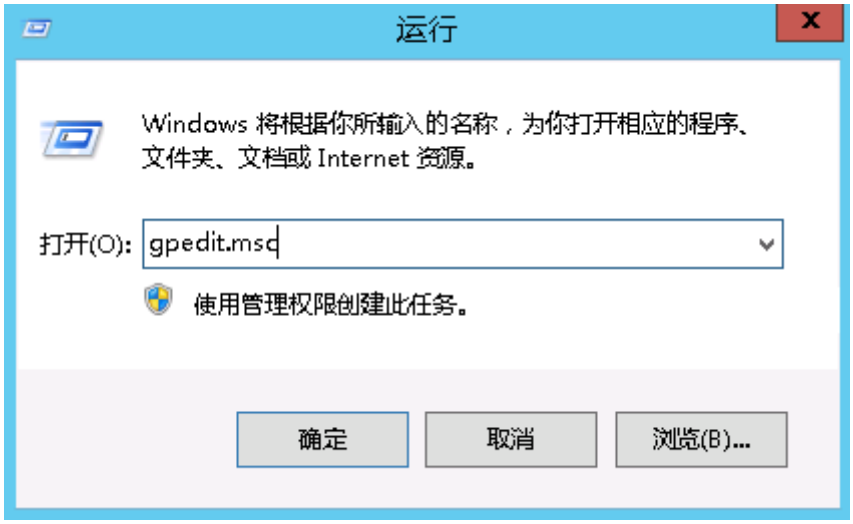
9. 安装完成后，重启服务器。

图 10-30 重启服务器

允许多用户远程连接云服务器

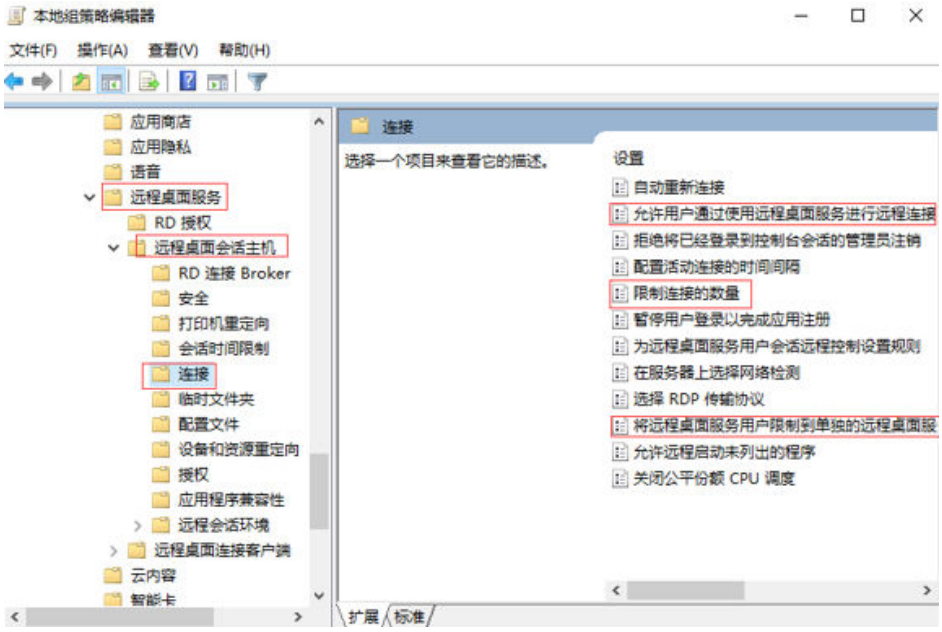
1. 在运行里输入“gpedit.msc”，打开计算机本地组策略。

图 10-31 gpedit.msc



2. 在计算机本地组策略里选择“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 > 连接”。如下图所示设置“允许用户通过使用远程桌面服务进行远程连接”、“限制连接数量（可根据具体数量设置）”和“将远程桌面服务用户限制到单独的远程桌面”。

图 10-32 设置“连接”



3. 右键单击“编辑”，设置“允许用户通过使用远程桌面服务进行远程连接”为已启用。

图 10-33 允许用户通过使用远程桌面服务进行远程连接

4. “限制连接数量”选择已启用，可根据具体数量设置。

图 10-34 限制连接数量

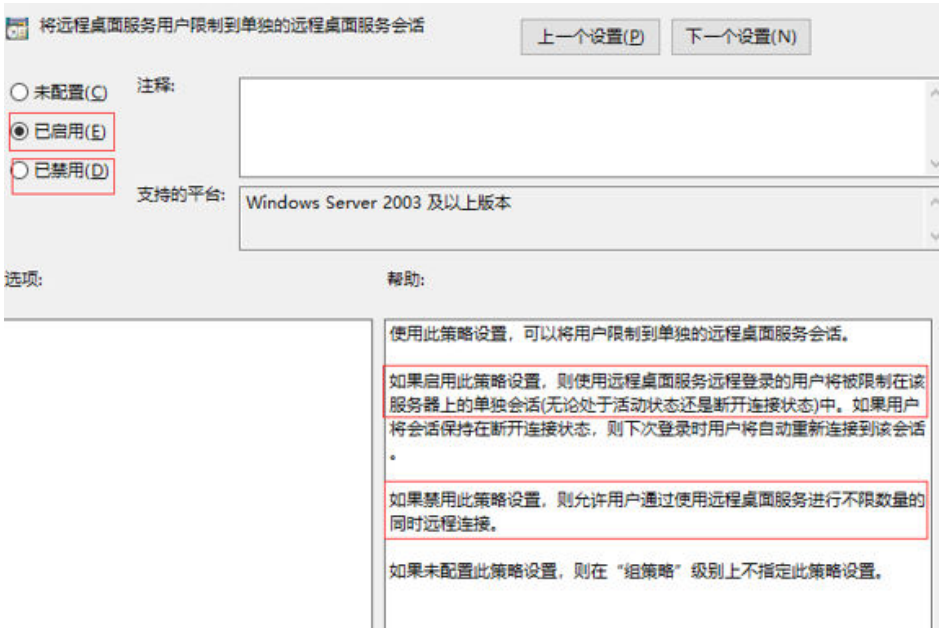
5. “将远程桌面服务用户限制到单独的远程桌面”选择已启用，或者已禁用，请注意此处已启用和已禁用的区别。本例以勾选“已启用”为例。
   - 已启用：多个用户同时登录的多用户登录，不能单个用户多登录。

例如：配置为已启用，用户A、用户B、用户C可以分别使用账号A、账号B、账号C同时登录云服务器，但是不支持用户A、用户B、用户C使用同一个账号同时登录云服务器。

- 已禁用：单个用户同时多个登录的多用户登录。

  例如：配置为已禁用，用户A、用户B、用户C可以使用同一个账号同时登录云服务器。

图 10-35 将远程桌面服务用户限制到单独的远程桌面



6. 运行cmd，输入”gpupdate /force”，强制执行本地组策略，重启服务器，整个配置过程完成。

配置新用户并加入远程桌面用户组

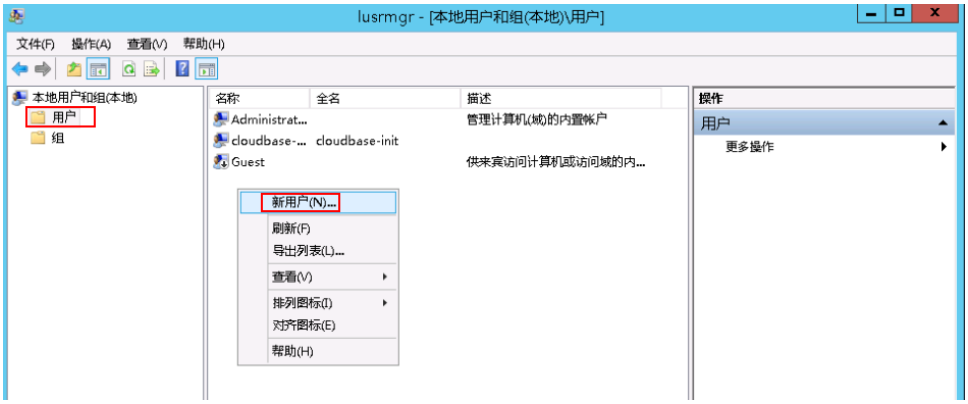
如果配置“多个用户同时登录的多用户登录”，那么在创建完新用户后需要将其加入远程桌面用户组。本小节操作介绍创建新用户并添加用户到远程桌面用户组的操作步骤。

1. 在运行中输入**lusrmgr.msc**，打开本地用户和组，进行新用户创建。

图 10-36 lusrmgr.msc

2. 单击“用户”，在空白处右键选择新用户。

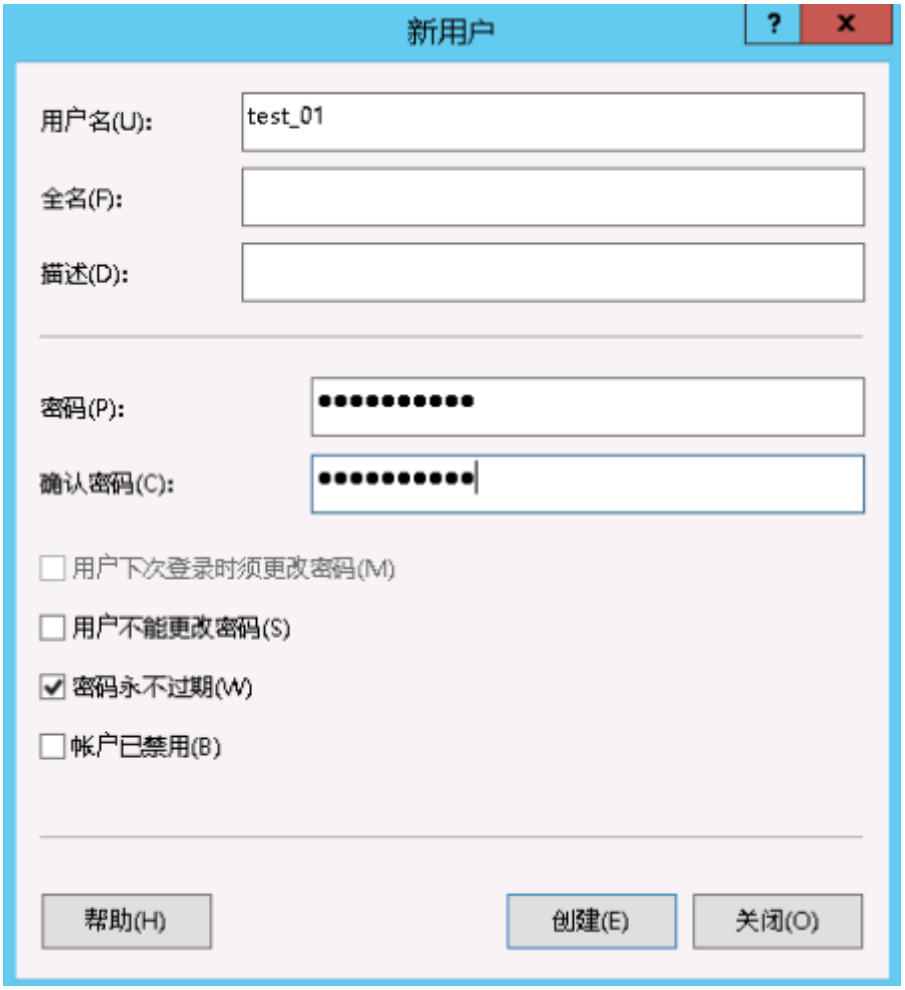
图 10-37 选择新用户



3. 填写新用户的“用户名”和“密码”信息，单击“创建”。

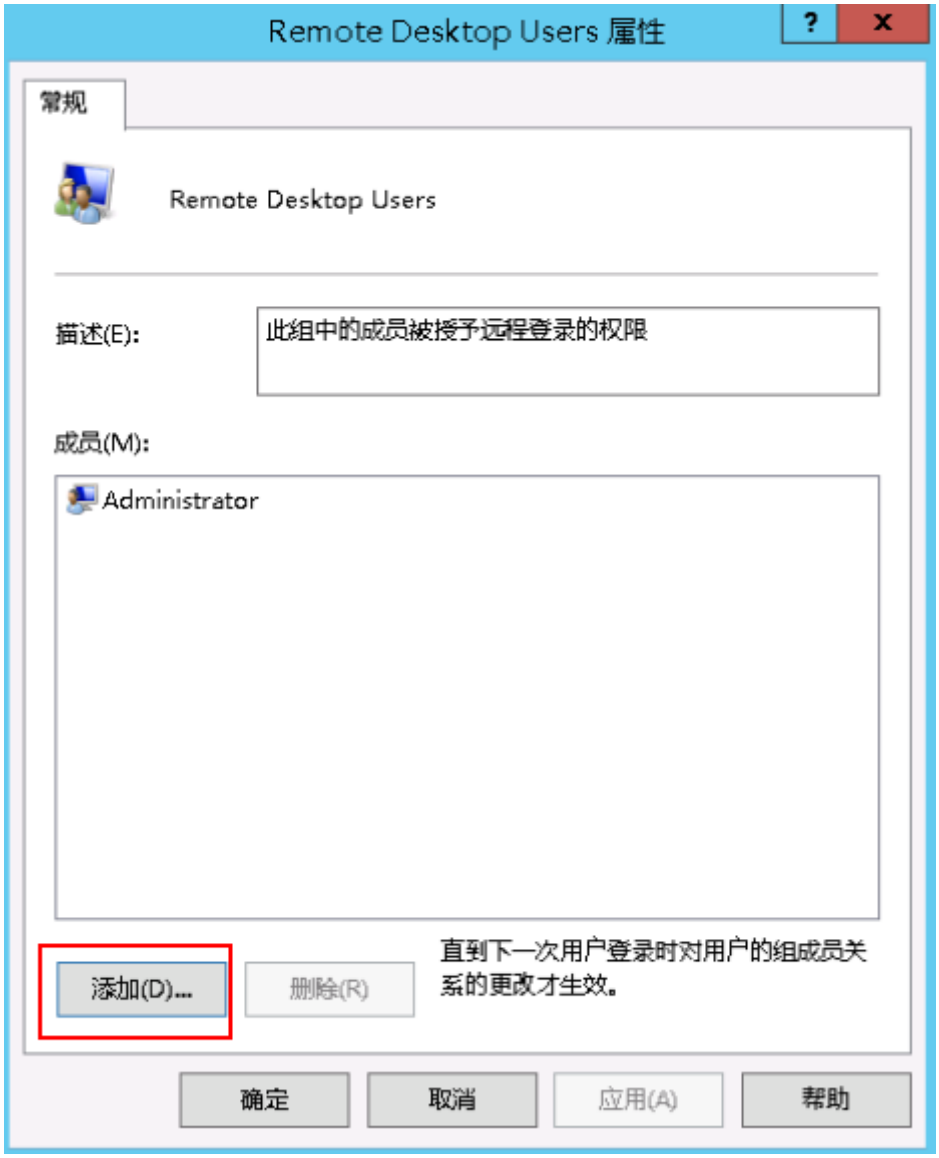
   “密码”和“确认密码”需完全一致。同时，建议您根据业务需要设置密码相关安全性属性。

图 10-38 填写新用户信息



4. 单击“组”，双击打开Remote Desktop Users组，单击“添加”。

图 10-39 Remote Desktop Users 组



5. 进入选择用户界面，单击“高级”。

图 10-40 选择用户界面

6. 在新的选择用户界面，单击“立即查找”，在下方搜索结果中选中需要远程登录的用户，并单击“确定”，完成添加，即可远程登录。

图 10-41 选择用户

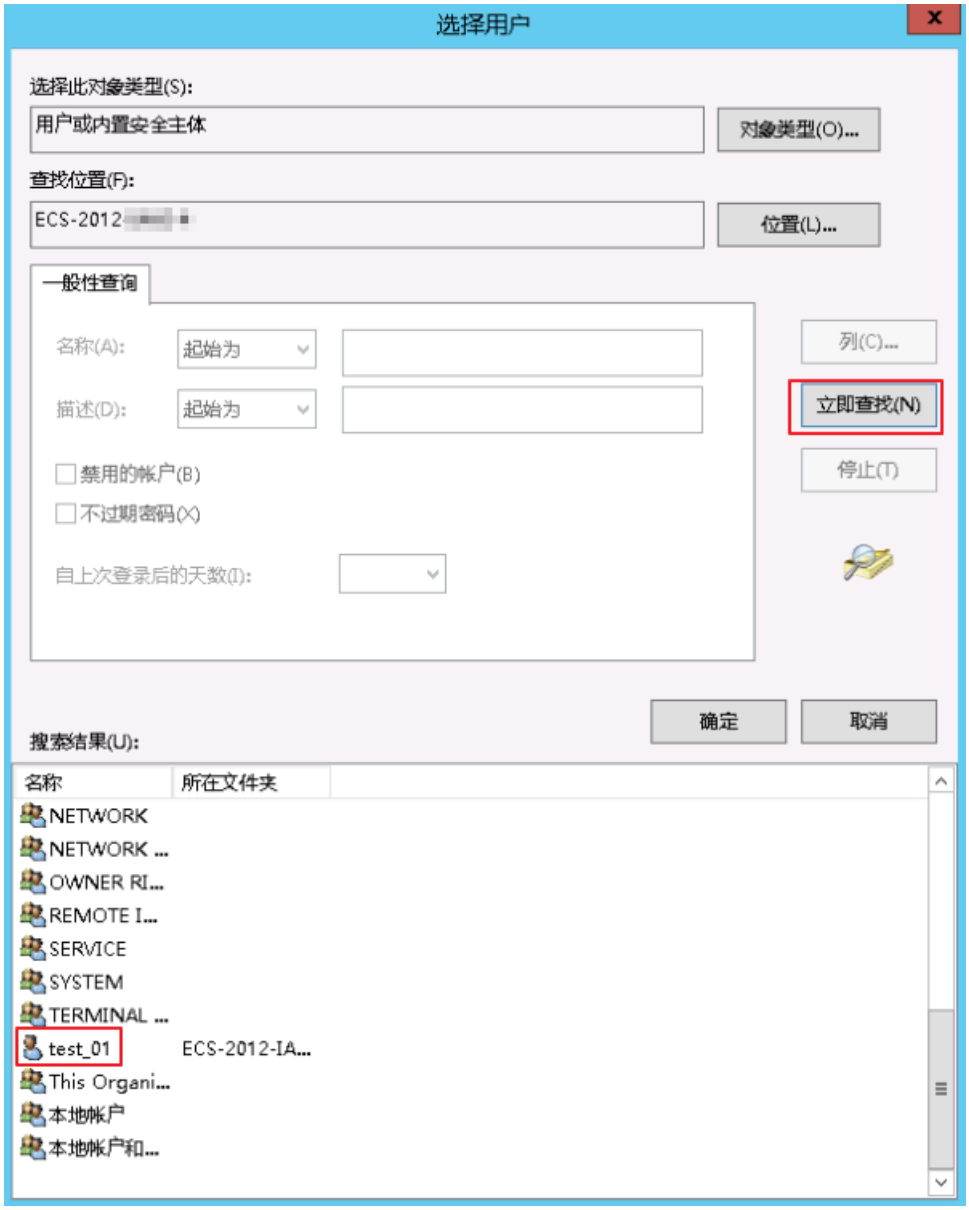
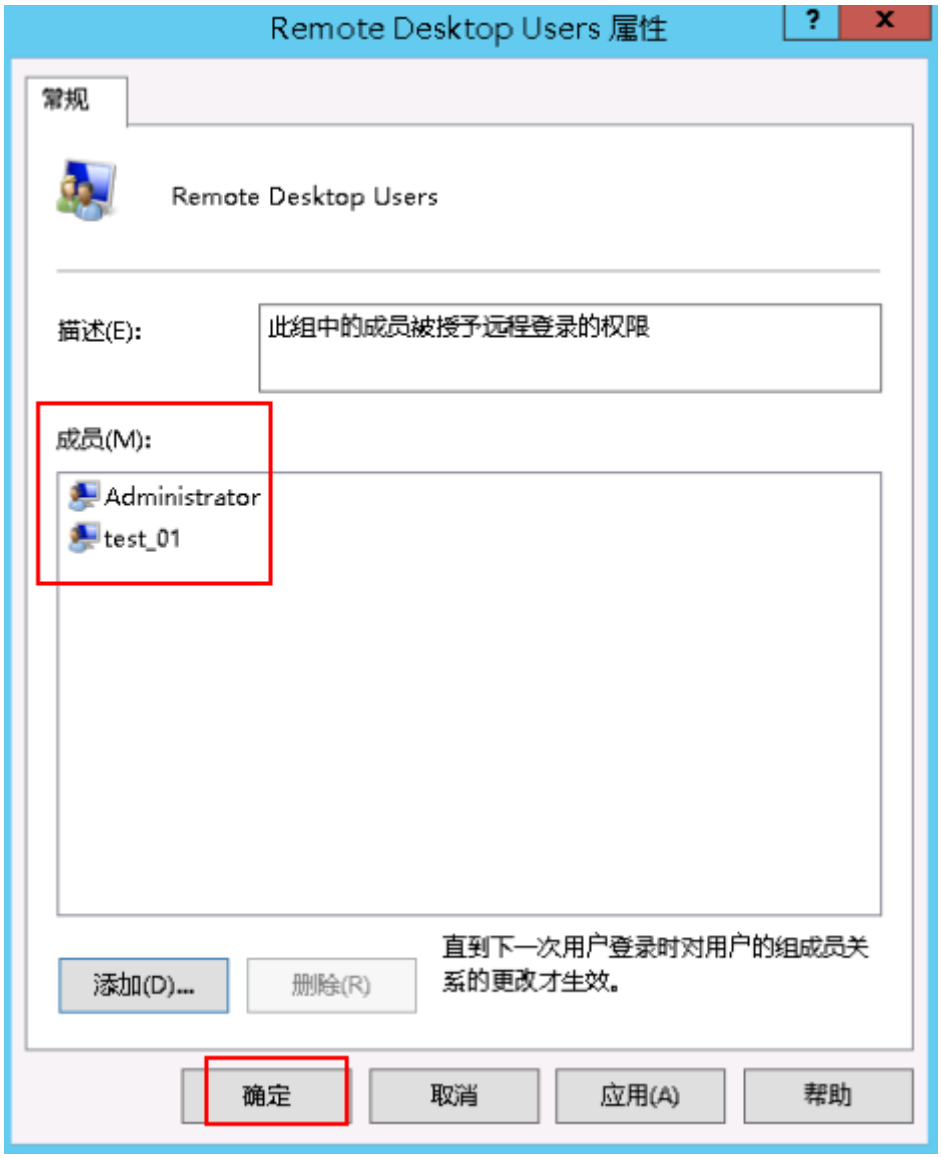


图 10-42 添加用户

7. 单击“确定”，添加用户到Remote Desktop Users组。

图 10-43 确认成员信息



后续操作

如需激活远程桌面授权请参考**申请多用户会话授权的license并激活云服务器**。

10.3 多用户登录 Windows 主机时无法打开浏览器

问题描述

Windows2008、Windows2012和Windows2016操作系统在多用户登录Windows云服务器时，如果已经有用户打开了浏览器，第二个用户打开浏览器失败。

处理方法

本节操作以IE浏览器为例。

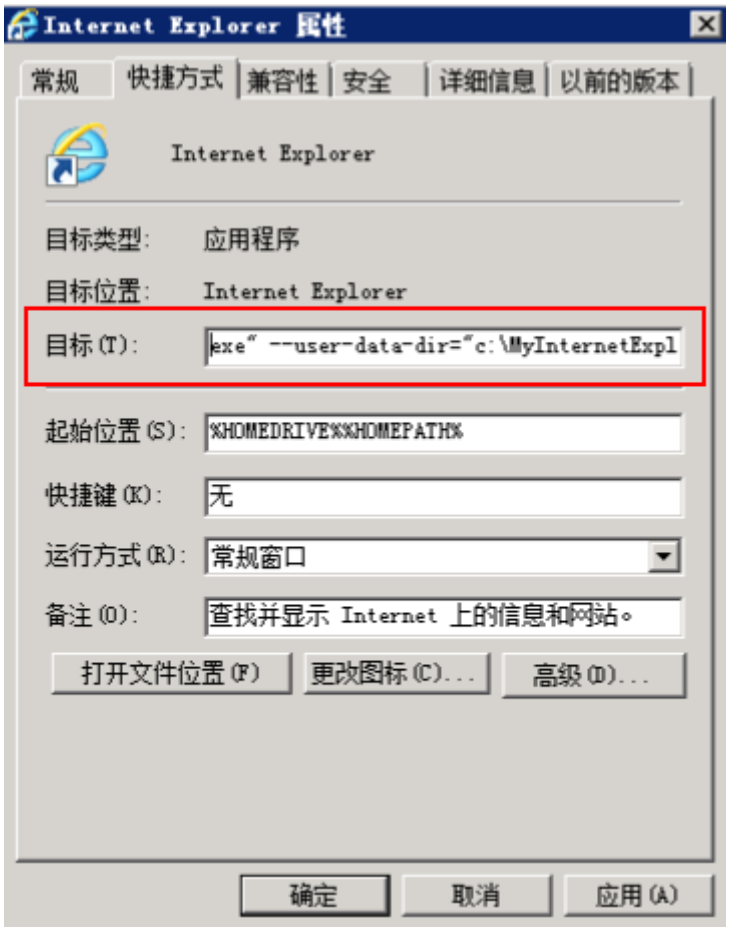
1. 在桌面选择浏览器图标，单击右键选择“创建快捷方式”。
2. 选择新创建的快捷方式，单击右键选择“属性”。
3. 选择“快捷方式”页签，找到目标选项，在末尾添加如下内容。

   --user-data-dir="c:\MyInternetExplorerData"

   说明

   - .exe"和--user中间有空格。
   - c:\MyInternetExplorerData表示Internet Explorer的数据文件存放位置，可以设置为任何有效的文件夹路径，如果此文件夹不存在，Internet Explorer浏览器会自动创建。

图 10-44 浏览器属性



4. 保存修改后就可以多个用户同时打开浏览器。

10.4 申请多用户会话授权的 license 并激活云服务器

操作场景

本节操作介绍云服务器远程桌面服务配置和授权激活的操作步骤。

本节操作以Windows 2012操作系统为例。

操作步骤

1. 申请多用户会话授权的license
2. 激活服务器
3. 配置远程桌面会话主机授权服务器

申请多用户会话授权的 license

1. 登录Windows云服务器。
2. 在操作系统界面，单击  打开“服务器管理器”
3. 在服务器管理器上单击“所有服务器 >选择服务器名称”，右键选择“RD授权管理器”。

图 10-45 选择服务器名称

4. 选择未激活的服务器，单击鼠标右键，选择“属性”。

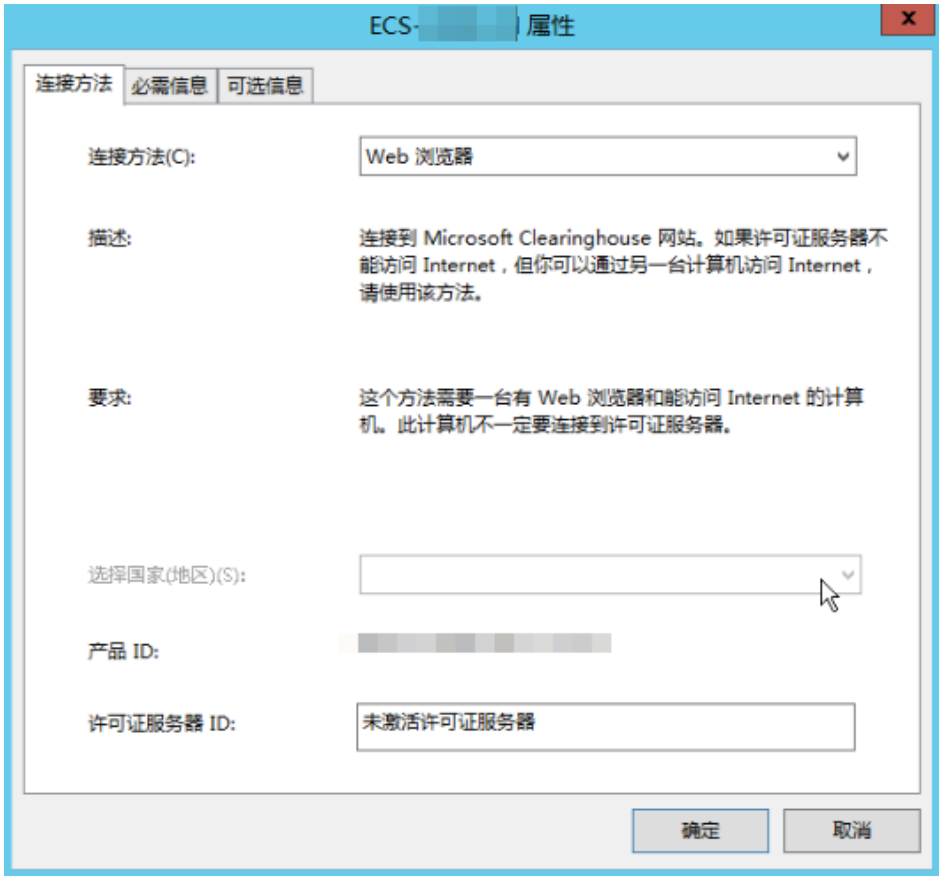
图 10-46 选择未激活的服务器

5. 在属性对话框中，连接方法选择“Web浏览器”，记下对话框中出现的产品ID，在获取服务器许可证时，需在网页上注册此ID。

须知

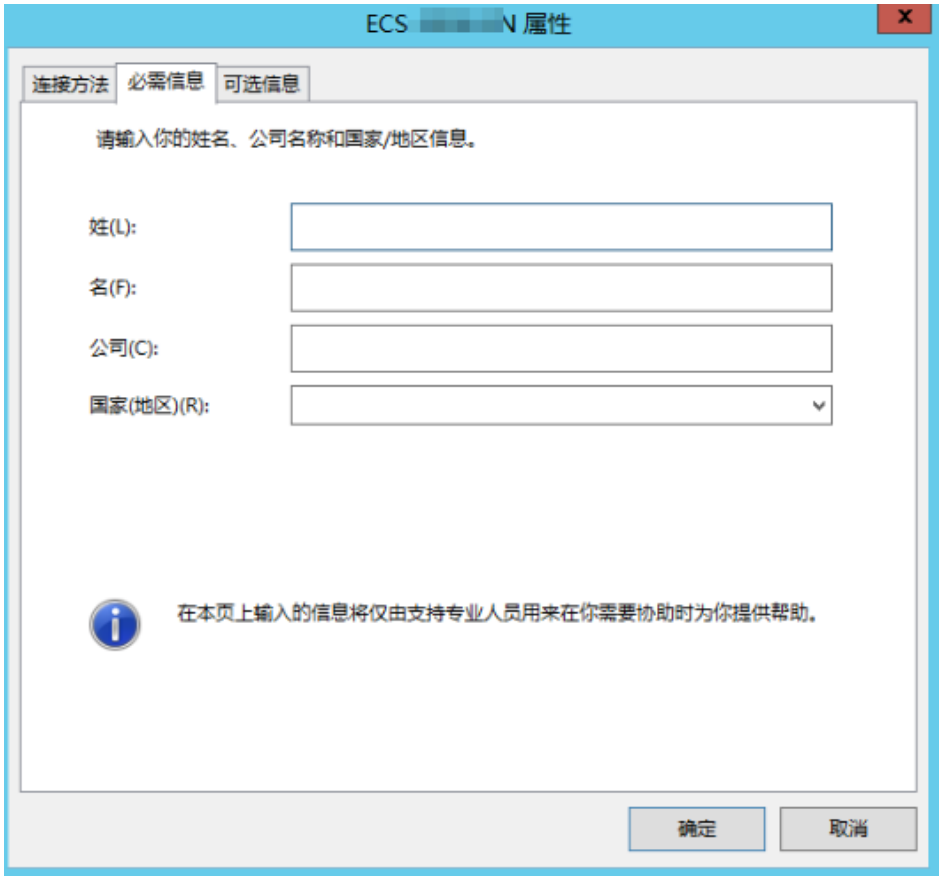
如果RD授权管理器中没有服务器，请选择“操作 > 连接”，然后输入本机服务器IP地址。

图 10-47 Web 浏览器



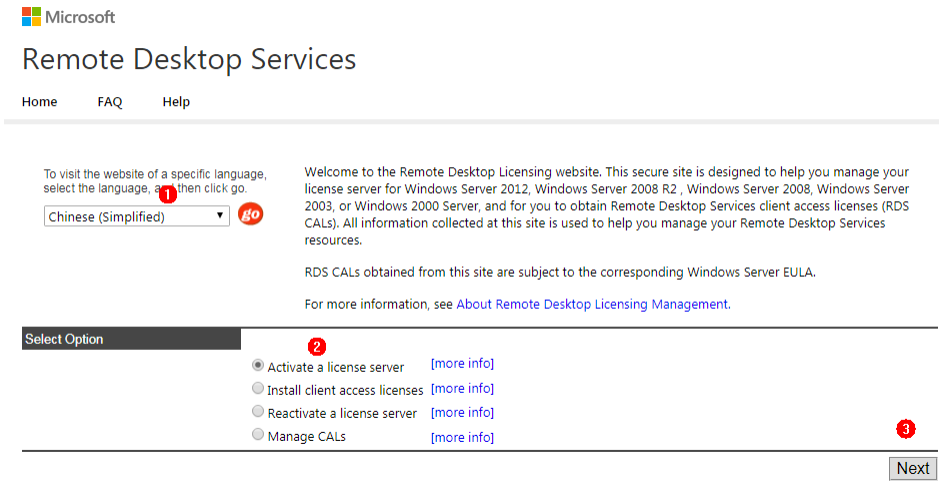
6. 选择“必需信息”，填写信息后单击“确定”。

图 10-48 填写属性信息



7. 用Internet Explorer浏览器打开**https://activate.microsoft.com** ，开始注册并获取服务器许可密码向导。
   选择“启用许可证服务器”项后单击“Next”。

图 10-49 启用许可证服务器



8. 输入“产品ID：xxxxx-xxxxx-xxxxx-xxxxx”，填写所需信息后，单击“下一步”确认产品信息无误后再次单击“下一步”。

图 10-50 填写服务器信息

9. 根据页面提示，记录服务器ID。在“需要此时获取客户机许可证吗”中选择”是” 。

图 10-51 记录服务器 ID 号

10. 如果没有许可证，在许可证程序选择“企业协议”，确定信息无误后，单击”下一步” 。

图 10-52 企业协议

11. 填写配置信息。
    - 产品类型：我们以选择“Windows Server 2012 Remote Desktop Services Per User client access license”为例。
    - 最大用户数：例如999。
    - 注册号码：请联系微软官方购买七位许可证注册号码，单击“下一步”。

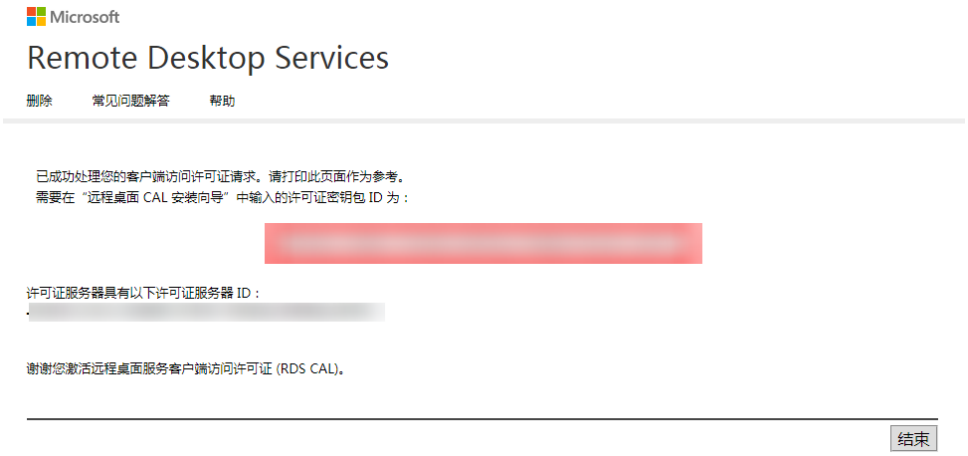
    说明

    华为云不提供远程桌面访问许可证，请从微软官方购买远程桌面访问许可证。

图 10-53 产品类型

12. 记录许可证服务器ID和许可证密钥包ID，然后单击“结束”。

图 10-54 密钥包 ID



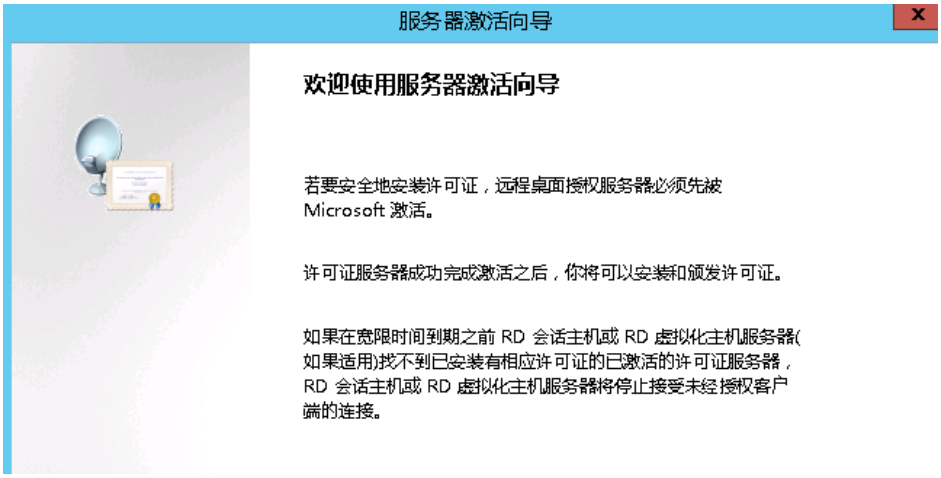
激活服务器

1. 登录云服务器，打开RD授权管理器选择服务器，单击右键选择“激活服务器”。

图 10-55 激活服务器

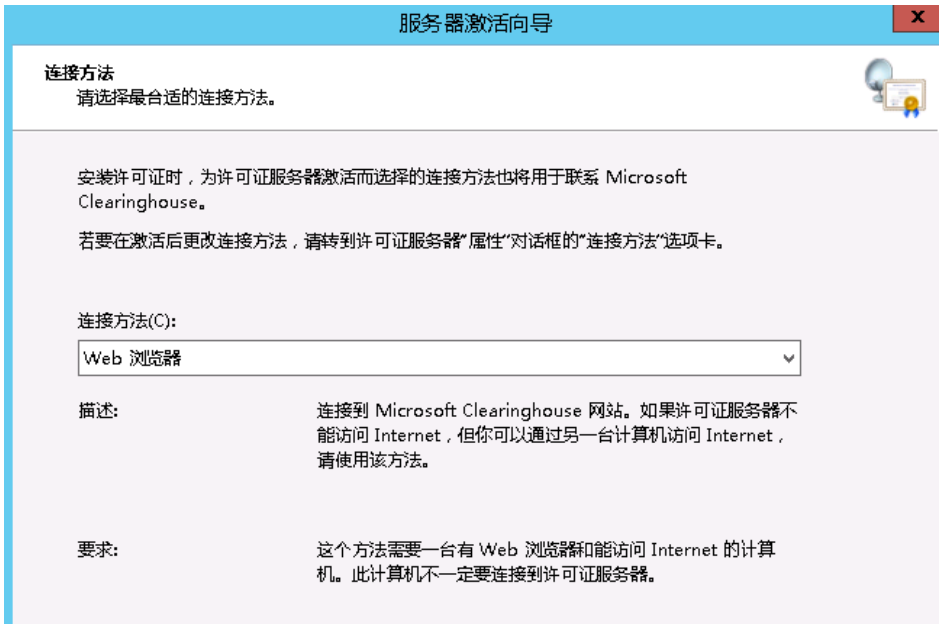
2. 在激活服务器向导中单击“下一步”。

图 10-56 激活服务器向导



3. 在连接方法处选择Web浏览器，然后单击“下一步”。

图 10-57 选择 Web 浏览器

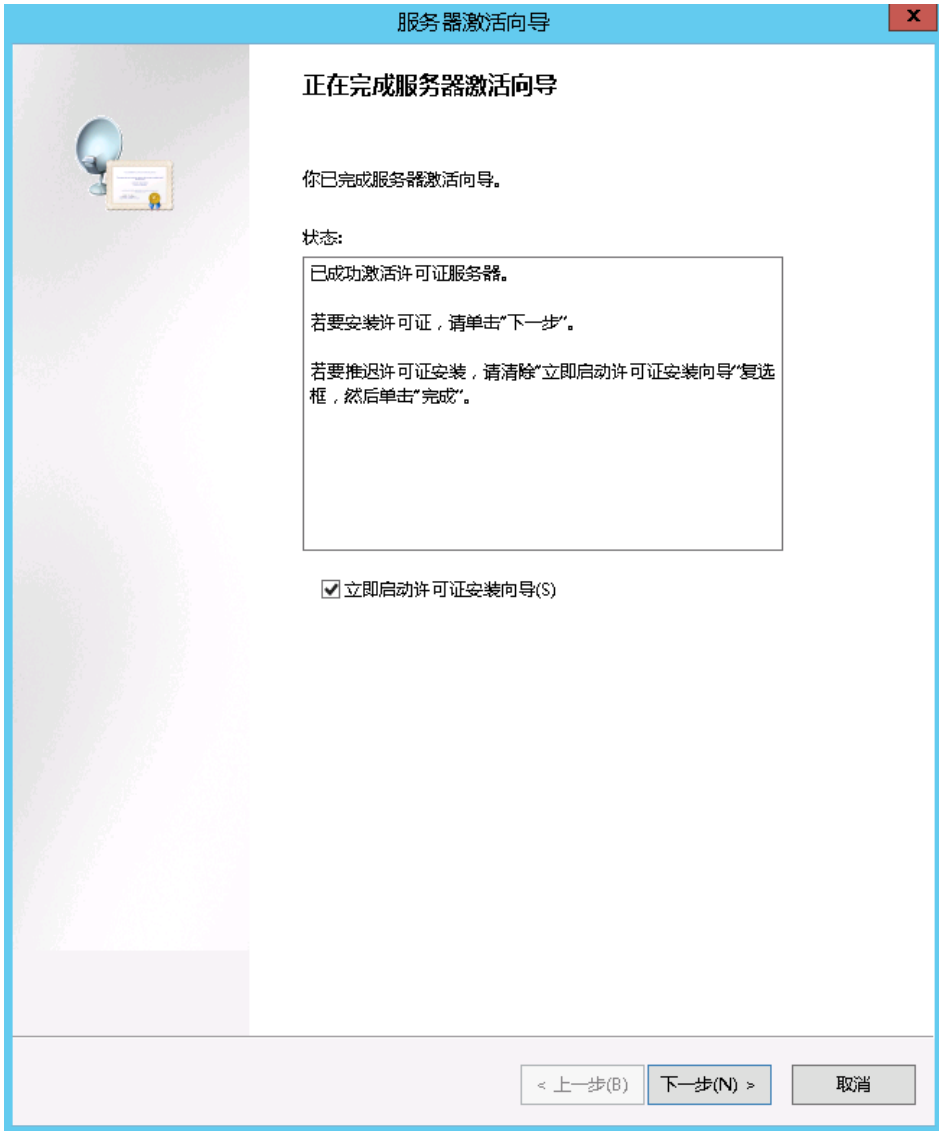


4. 输入许可服务器ID，然后单击“下一步”。
许可服务器ID为步骤9中获取的ID。

图 10-58 输入许可服务器 ID

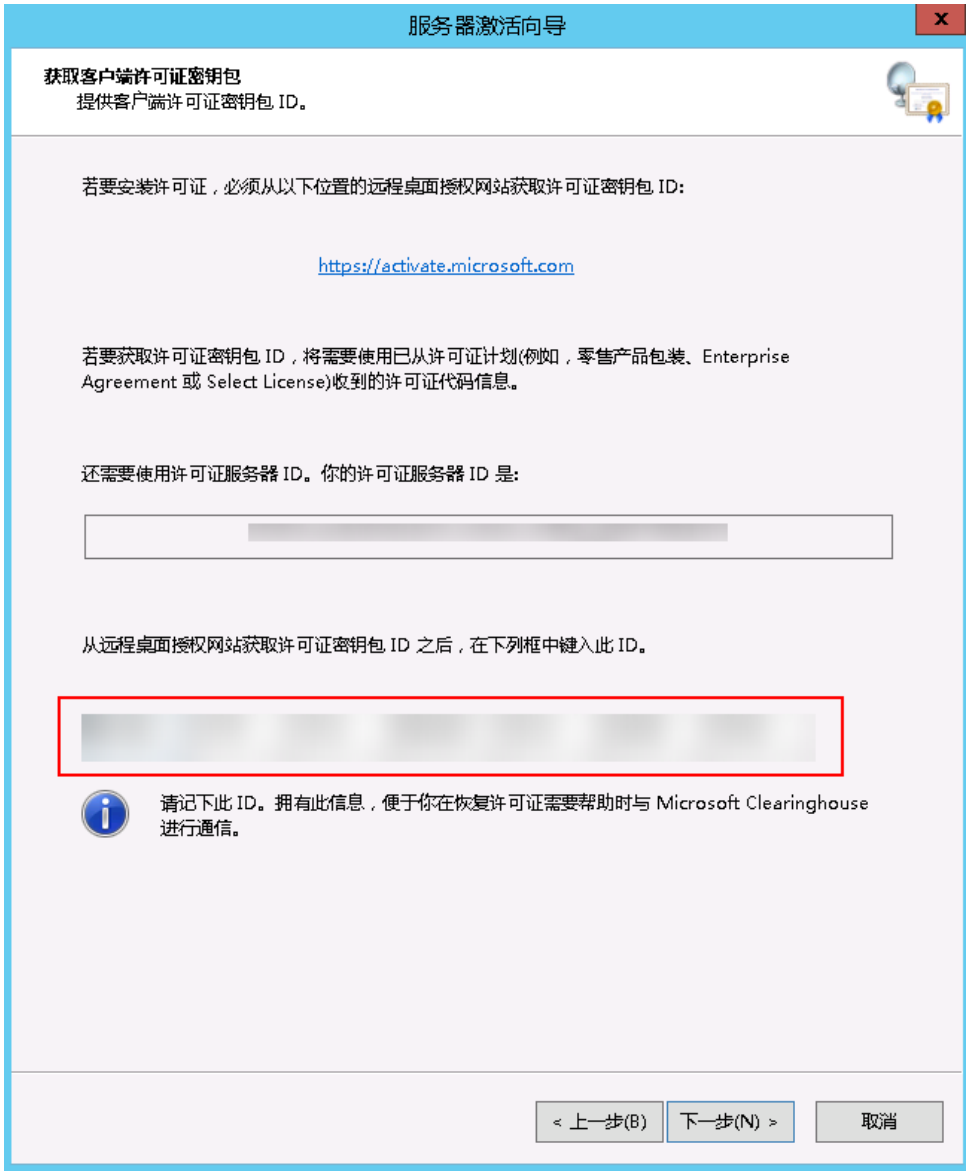
5. 选择立即启动许可安装向导，单击“下一步”。

图 10-59 启动许可安装向导



6. 输入许可密钥包ID，单击“下一步”。
   密钥包ID为步骤12中获取的密钥包ID。

图 10-60 许可密钥包 ID



7. 服务器许可证激活向导完成，单击“完成”。

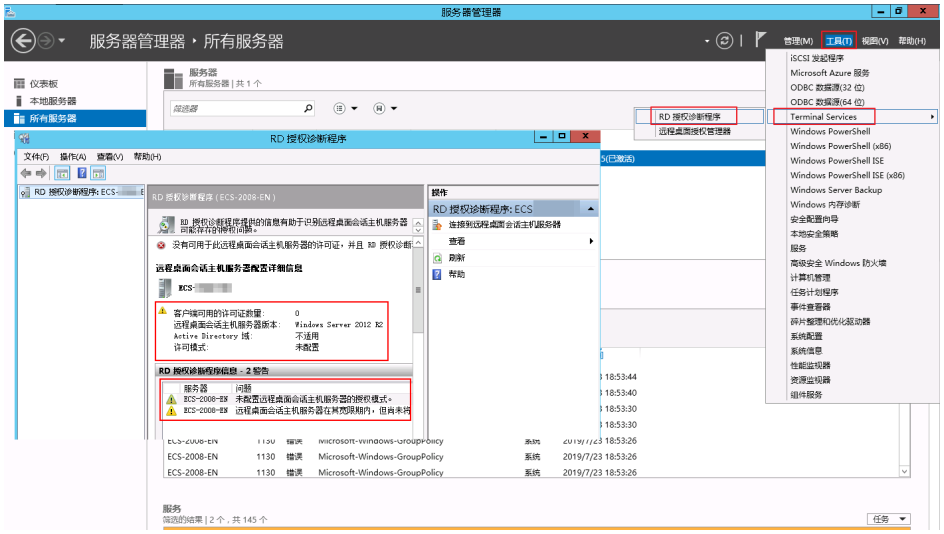
配置远程桌面会话主机授权服务器

1. 登录Windows云服务器。
2. 在操作系统界面，单击  打开“服务器管理器”，单击“工具 > Terminal Service > RD授权诊断程序”，查看当前服务器授权状态。

   2019操作系统，请单击“工具 > Remote Desktop Services > 远程桌面授权诊断程序”，查看当前服务器授权状态。

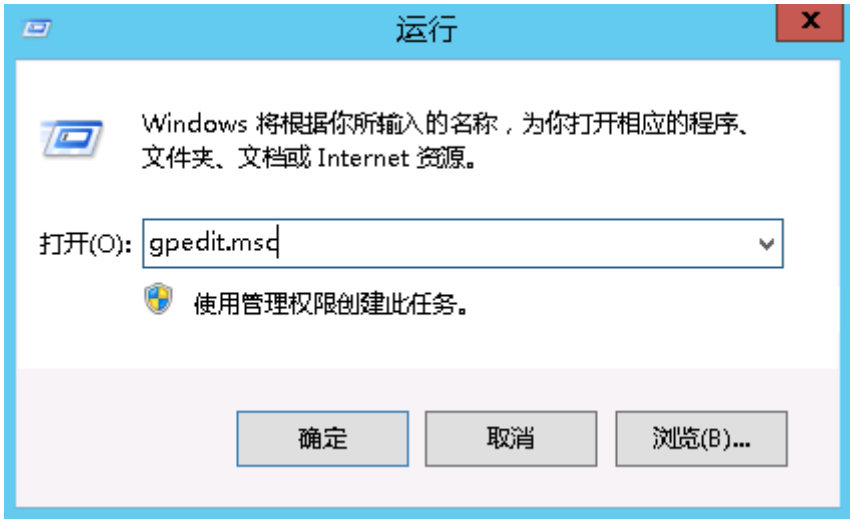
   如下图所示，提示未配置远程桌面会话主机服务器的授权模式。

图 10-61 查看服务器授权状态。



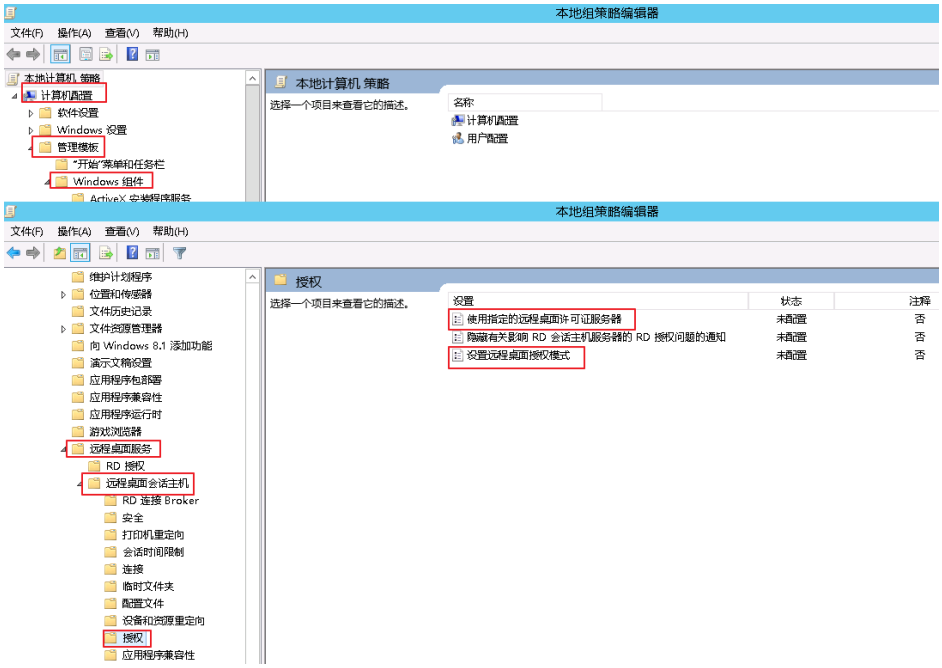
3. 在运行里输入“gpedit.msc”，打开计算机本地组策略。

图 10-62 gpedit.msc



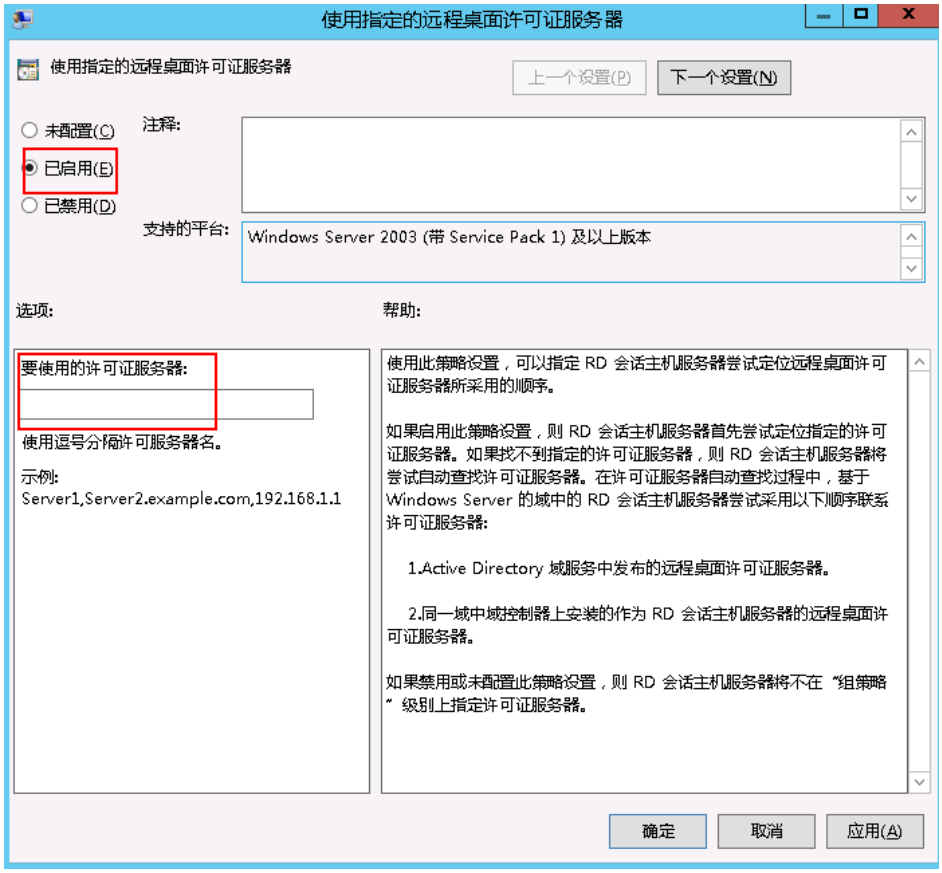
4. 在计算机本地组策略里选择“计算机配置 > 管理模板 > windows组件 > 远程桌面服务 > 远程桌面会话主机 > 授权”，找到 “使用指定的远程桌面许可服务器”和“设置远程桌面授权模式”。

图 10-63 修改授权项



5. 设置“使用指定的远程桌面许可证服务器”为启用，并在“要使用的许可证服务器”中，设置当前服务器的私有IP或者主机名。

图 10-64 使用指定的远程桌面许可证服务器

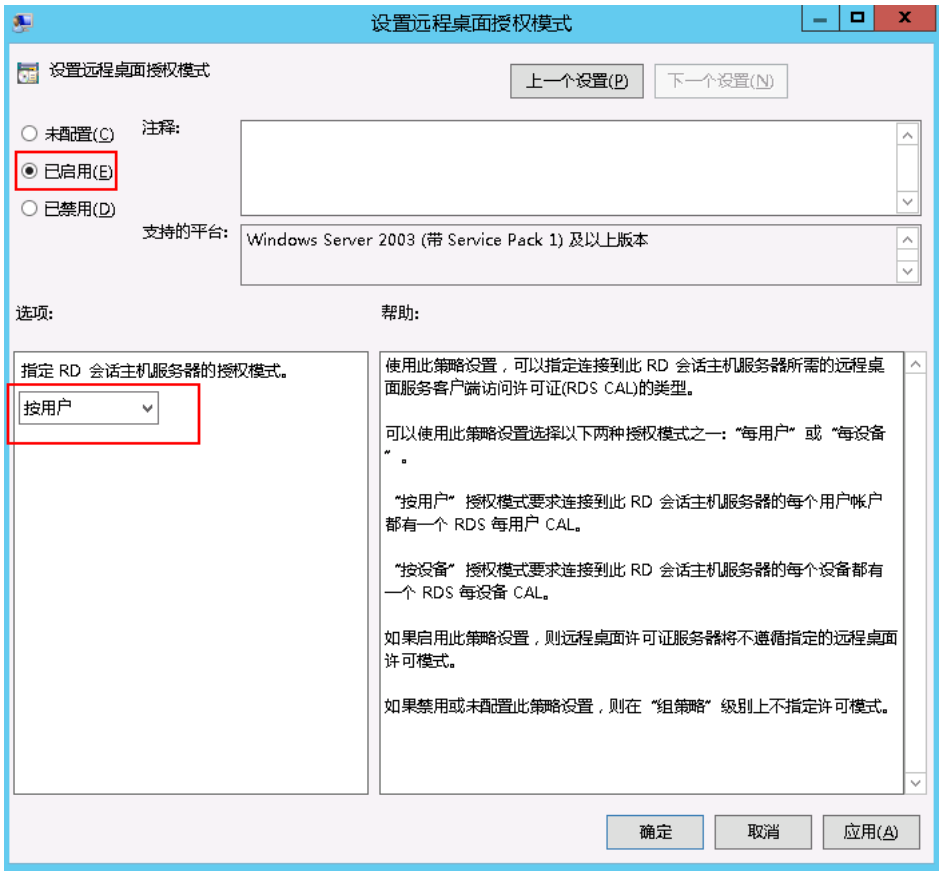


6. 启用“设置远程桌面授权模式”，设置授权模式为“按用户”。

   说明

   如果出现提示“远程桌面许可证问题”，请将授权模式为“按设备”。

   图 10-65 设置远程桌面授权模式



7. 运行cmd，输入”gpupdate /force”，强制执行本地组策略，重启服务器，整个配置过程完成。

10.5 配置多用户登录后，普通用户登录闪屏怎么办?

问题描述

Windows服务器配置多用户登录后，Administrator登录正常，普通用户登录后出现闪屏，或者打开"我的电脑"出现自动关闭，不能正常使用。

处理方法

1. 使Administrator用户登录服务器，查看系统日志及应用日志，查找异常模板，本例发现Mglayout64.dll模块出现异常
2. 打开C:\Windows\进行搜索模块名称，找到对应模块文件。本例中查看发现此模块为某一壁纸文件。
3. 打开“运行 > cmd”，进入到错误文件所在目录。

本例执行如下命令：

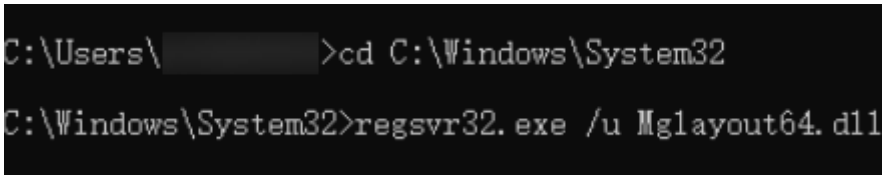
cd C:\Windows\System32

4. 通过命令**regsvr32.exe /u 文件名**，进行移除，移除后恢复正常。

   本例执行如下命令：

   regsvr32.exe /u Mglayout64.dll

   图 10-66 移除异常文件



11 密码与密钥对

11.1 Linux 操作系统执行 passwd 命令失败，提示：Authentication token manipulation error

问题现象

root用户用passwd命令修改管理员用户以及普通用户的密码时失败，提示passwd:Authentication token manipulation error。

```
[root@xiaoyao-test ~]# passwd
Changing password for user root.
New password:
Retype new password:
passwd: Authentication token manipulation error
```

根因分析

出现该问题通常是密码文件的属性的问题导致，也有可能是根目录空间满。

执行以下命令查看存放用户和密码的文件（/etc/passwd和/etc/shadow）属性。

lsattr /etc/passwd /etc/shadow

```
[root@xiaoyao-test ~]# lsattr /etc/passwd /etc/shadow
----i---------e-- /etc/passwd
----i---------e-- /etc/shadow
```

如上图所示，/etc/passwd和/etc/shadow文件中有i属性，"i"的文件属性表示该文件不能修改：它不能被删除或重命名，无法为此创建任何链接文件，不能将任何数据写入该文件。只有管理员用户可以设置或清除此属性。

说明

1.如果设置了'a'属性的文件只能在append（只允许增加记录）写作模式。只有管理员用户可以设置或清除此属性。

CAP_LINUX_IMMUTABLE功能可以设置或清除这个属性。

其他文件属性可以执行以下命令查看chattr使用手册。

chattr

2.如果lsattr结果中没有限制增加或者修改的属性，则可能为根分区空间不足，可以查询根分区使用率。

df -h

处理方法则为删除根分区下不需要的文件。

处理方法

1. 用chattr命令将i权限撤销，然后再修改密码。
   - 如果文件属性为"i"，执行以下命令。
     chattr -i /etc/passwd /etc/shadow
   - 如果文件属性为"a"，执行以下命令。
     chattr -a /etc/passwd /etc/shadow
2. （可选）如果对修改过属性的文件有安全要求需要设置相应的属性，请重新设置相应的属性。
   - 如果设置文件属性为"i"，执行以下命令。
     chattr +i /etc/passwd /etc/shadow
   - 如果设置文件属性为"a"，执行以下命令。
     chattr +a /etc/passwd /etc/shadow

   查看修改后的文件属性，执行以下命令。

   lsattr /etc/passwd /etc/shadow

11.2 如何更换我的密钥对?

问题描述

更换云服务器密钥对，删除旧的密钥对时，无法使用新的密钥对登录云服务器。

处理方法

1. 登录Linux云服务器上制作密钥对，首先用密码或旧的密钥登录到待更换密钥对的云服务器，然后执行以下命令：

```
[root@host ~]$ ssh-keygen  <== 建立密钥对
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa): <== 按 Enter
Created directory ´/root/.ssh´.
Enter passphrase (empty for no passphrase): <== 输入密钥锁码，或直接按 Enter 留空
Enter same passphrase again: <== 再输入一遍密钥锁码
Your identification has been saved in /root/.ssh/id_rsa. <== 私钥
Your public key has been saved in /root/.ssh/id_rsa.pub. <== 公钥
The key fingerprint is:
0f:d3:e7:1a:1c:bd:5c:03:f1:19:f1:22:df:9b:cc:08 root@host
```

2. 密钥锁码在使用私钥时必须输入，这样就可以保护私钥不被盗用。

现在，在 root 用户的家目录中生成了一个 .ssh 的隐藏目录，内含两个密钥文件：id_rsa 为私钥，id_rsa.pub 为公钥。

3. 在Linux云服务器上执行以下命令安装公钥。
```
[root@host ~]$ cd .ssh
[root@host .ssh]$ cat id_rsa.pub >> authorized_keys
```
4. 为了确保连接成功，请保证以下文件权限正确。
```
[root@host .ssh]$ chmod 600 authorized_keys
[root@host .ssh]$ chmod 700 ~/.ssh
```
5. （可选）设置 SSH，打开密钥登录功能（使用公共镜像创建的Linux云服务器默认是开启的），编辑 /etc/ssh/sshd_config 文件，进行如下设置：
```
RSAAuthentication yes
PubkeyAuthentication yes
```
6. 检查如下配置项，确保 root 用户能通过 SSH 登录：
```
PermitRootLogin yes
```
7. 完成上述配置后，并以密钥方式登录成功后，再禁用密码登录：

   PasswordAuthentication no
8. 重启 SSH 服务。

   service sshd restart

后续操作

1. 将私钥下载到客户端，然后转换为 PuTTY 能使用的格式。

   使用 WinSCP、SFTP 等工具将私钥文件 id_rsa 下载到客户端机器上，请谨慎保管好以防丢失。
2. 然后打开 PuTTYGen，单击 Actions 中的 “Load”，载入下载私钥文件。

   如果您刚才设置了密钥锁码，这时则需要输入。
3. 载入成功后，PuTTYGen 会显示密钥相关的信息。
4. 在 Key comment 中键入对密钥的说明信息，然后单击“ Save private key”即可将私钥文件存放为 PuTTY 能使用的格式。
5. 当再次使用 PuTTY 登录时，可在左侧导航栏选择“ Connection > SSH > Auth”中的 Private key file for authentication：选择私钥文件，输入密钥锁码即可登录。

11.3 Linux 云服务器怎样切换密钥登录为密码登录?

操作场景

本节操作介绍Linux云服务器切换密钥登录为密码登录的操作步骤。

操作步骤

1. 使用密钥登录Linux云服务器，设置root密码。

   sudo passwd root

   若密钥文件丢失或损坏，请参考**在操作系统内部修改ECS密码**，重置root密码。
2. 使用root身份编辑云服务器的ssh登录方式。

   su root

   vi /etc/ssh/sshd_config

   修改如下配置项：

- 把PasswordAuthentication no 改为 PasswordAuthentication yes
  或去掉PasswordAuthentication yes 前面的#注释掉。
- 把PermitRootLogin no 改为 PermitRootLogin yes
  或去掉PermitRootLogin yes 前面的#注释掉。

3. 重启sshd使修改生效。

   service sshd restart

4. 重启云服务器就可以使用root用户和新设置的密码登录了。

   说明

   防止非授权用户使用原来的密钥文件访问Linux云服务器，请将/root/.ssh/authorized_keys文件删除或清空authorized_keys文件内容。

12 防火墙设置

12.1 Windows 云服务器怎样开启或关闭防火墙、添加例外端口?

操作场景

本节操作指导用户开启或关闭Windows操作系统云服务器的防火墙，以及防火墙添加例外端口的操作。

本节操作以2012操作系统云服务器为例。

⚠ 注意

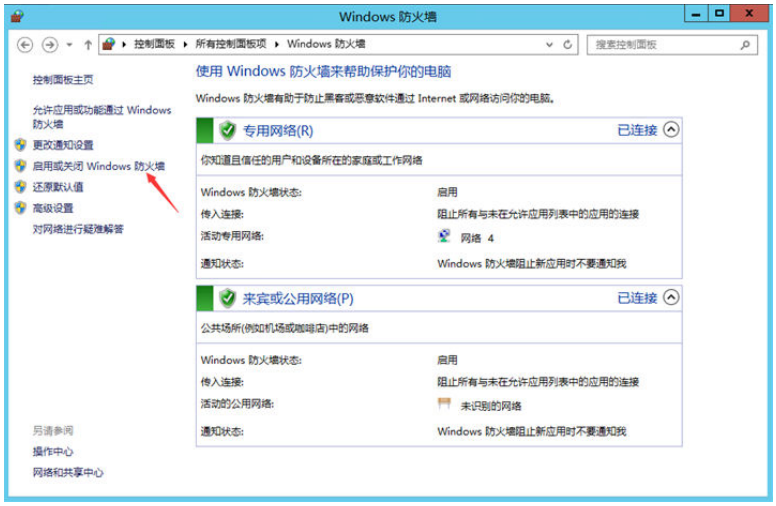
防火墙开启和设置安全组是对云服务器的双重保护，如果选择关闭防火墙或添加例外端口，建议安全组谨慎开放端口。

开启或关闭防火墙

方法一：系统界面操作

1. 登录Windows云服务器。
2. 单击桌面左下角的Windows图标，选择“控制面板 > Windows防火墙”。

3. 单击“启用或关闭Windows防火墙”。
   查看并设置防火墙的具体状态：开启或关闭。



方法二：命令行操作

1. 登录Windows云服务器。
2. 以管理员身份运行cmd。
3. 参考**表12-1**，执行命令。

表 12-1 防火墙操作相关命令

操作	命令	云运维中心
查看防火墙状态	**netsh advfirewall show currentprofile state**	1. 登录管理控制台。 2. 打开**HWC.ECS.OSOps-switch-windows-firewall.bat**脚本，获取脚本内容。 **说明** 也可在云运维中心**HWC.ECS.OSOps-switch-windows-firewall.bat**的执行脚本页面设置参数后，直接运行。
开启防火墙	**netsh advfirewall set currentprofile state on**	
关闭防火墙	**netsh advfirewall set currentprofile state off**	

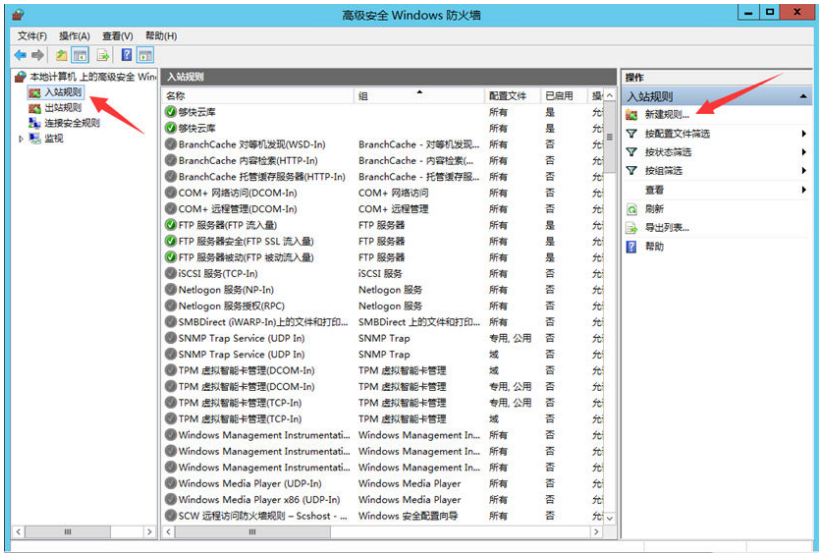
说明

适用版本：Windows XP之后的发行版本均可用，例如Windows 7/Vista/10/11/2012等。

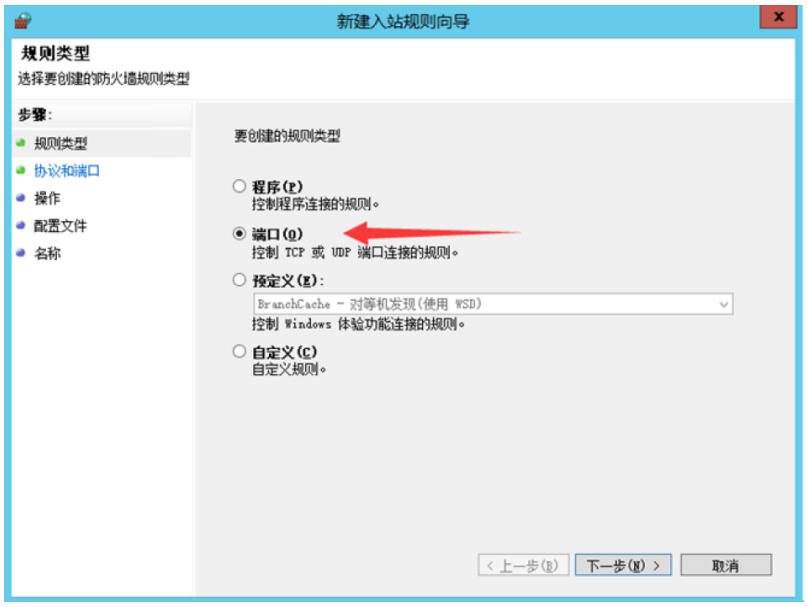
防火墙添加例外端口

1. 登录Windows云服务器。
2. 单击桌面左下角的Windows图标，选择“控制面板 > Windows防火墙”。

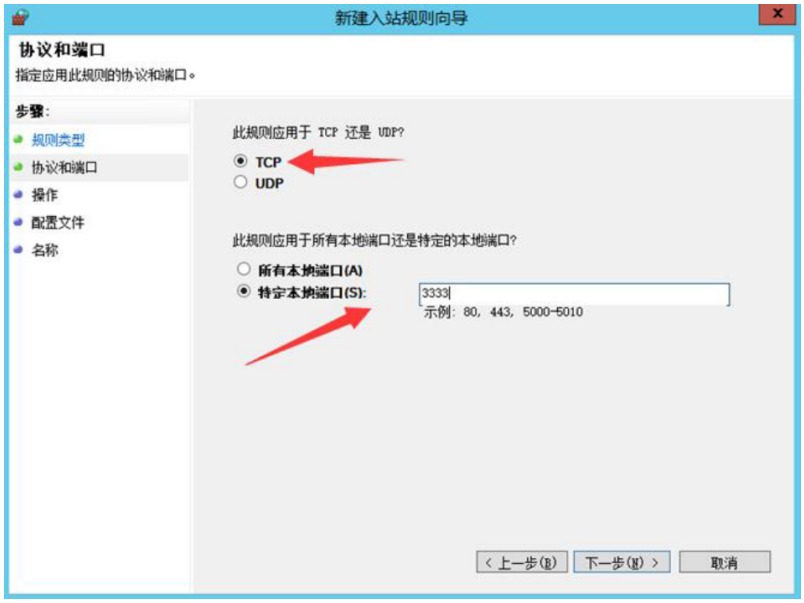
3. 在“Windows防火墙”页面，在左侧导航栏选择“高级设置 > 入站规则”。
   您可以查看云服务器允许连接的程序、端口规则等详细信息。



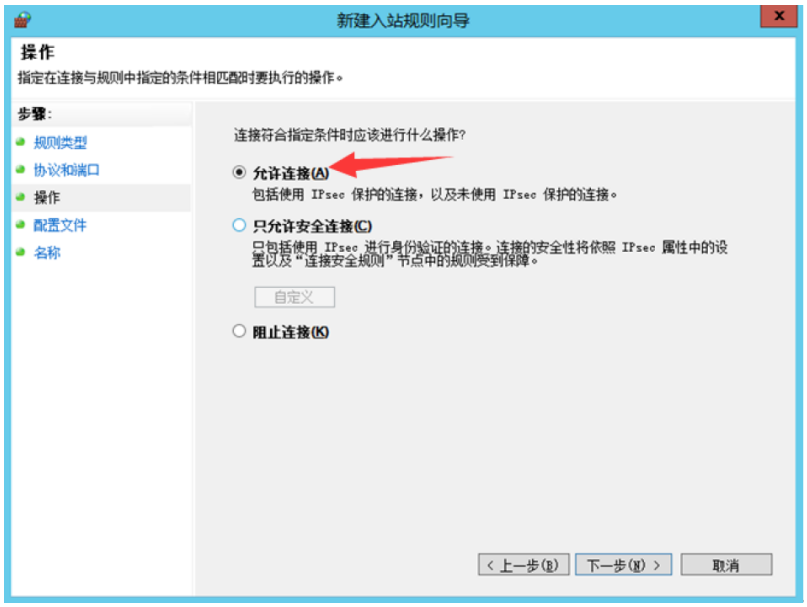
4. 单击“操作”栏的“新建规则”。
   请根据界面提示，开放具体的端口。本文以开放3333端口为例，具体操作如下：
   选择“端口”。



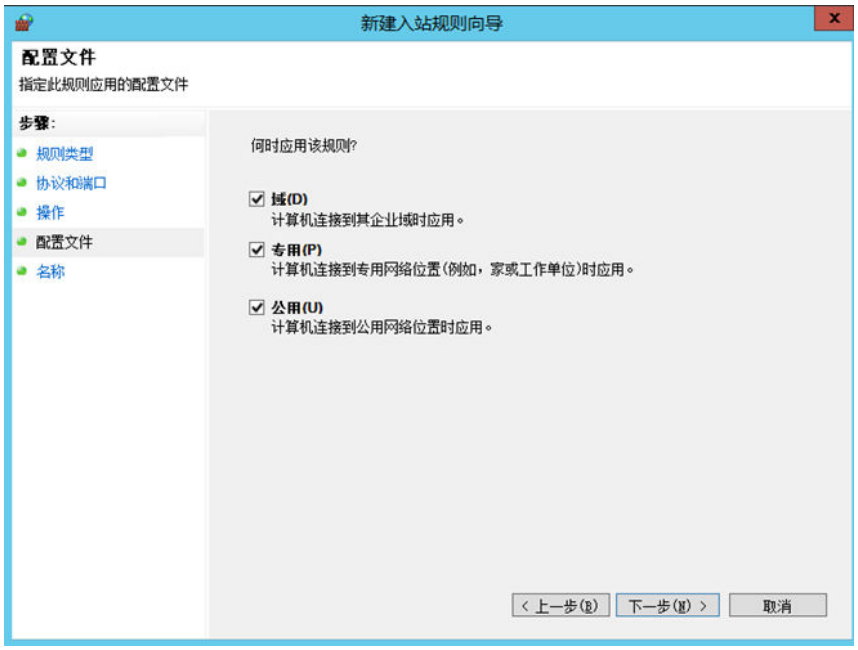
选择协议类型，并设置开放的端口。



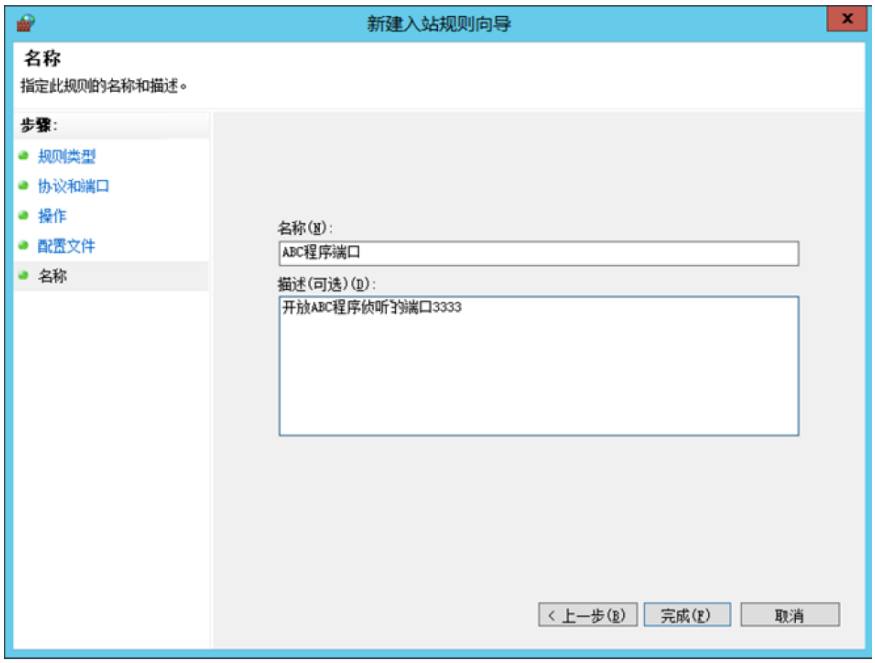
设置连接规则。



设置规则的应用场景。



自定义新建规则的名称。



5. 规则添加完成后，新端口即开放，云服务器的防火墙会自动放行。
   您可以通过单击新添加的规则，查看详细信息，设置详细的计算机连接、作用域的IP连接、协议类型等。

12.2 Linux 云服务器怎样开启或关闭防火墙、添加例外端口?

操作场景

本节操作指导用户开启或关闭Linux操作系统云服务器的防火墙，以及防火墙添加例外端口的操作。

⚠ 注意

防火墙开启和设置安全组是对云服务器的双重保护，如果选择关闭防火墙或添加例外端口，建议安全组谨慎开放端口。

开启或关闭防火墙

根据操作系统不同，分别执行以下命令开启或关闭防火墙。

操作系统	开启	关闭	云运维中心
CentOS 6	**service iptables start**	**service iptables stop**	1. 登录管理控制台。 2. 打开**HWC.ECS.OSOps-switch-linux-firewall.sh**脚本，获取脚本内容。 **说明** 也可在云运维中心**HWC.ECS.OSOps-switch-windows-firewall.bat**的执行脚本页面设置参数后，直接运行。
CentOS 7	**systemctl start firewalld.service**	**systemctl stop firewalld.service**	
Ubuntu	**ufw enable**	**ufw disable**	
Debian	**/etc/init.d/iptables start**	**/etc/init.d/ iptables stop**	

防火墙添加例外端口

- CentOS 6添加防火墙例外端口。
  a. 以添加23端口为例，执行以下命令，添加防火墙例外端口：tcp协议23端口。
     iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 23 -j ACCEPT
  b. 保存新配置。
     service iptables save
  c. （可选）设置防火墙开机自启动。
     chkconfig iptables on

     说明

     - 可执行以下命令关闭防火墙开机自启动。
       chkconfig iptables off
     - CentOS 6启动防火墙时可能会出现"iptables"no config file"错误，原因是未找到配置文件iptables。解决方法如下：
       1. 新建一条规则。
          iptables -P OUTPUT ACCEPT
       2. 保存配置。
          service iptables save
       3. 再次启动防火墙。
          service iptables start
- 以CentOS 7添加防火墙例外端口及防火墙常用操作。
  a. 查看防火墙状态。
     systemctl status firewalld
     或
     firewall-cmd --state
  b. 如果防火墙关闭可以执行以下命令开启。
     systemctl start firewalld
     如果开启命令执行后提示“Failed to start firewalld.service: Unit is masked.”请执行以下命令后再重新执行开启防火墙的命令。**systemctl unmask firewalld**

c. 重新检查防火墙状态是否打开。

firewall-cmd --state

回显信息：

```
[root@ecs-centos7 ~]# firewall-cmd --state
running
```

d. 以添加23端口为例，执行以下命令，添加防火墙例外端口：tcp协议23端口。

firewall-cmd --zone=public --add-port=23/tcp --permanent

回显信息如下说明设置成功：

```
[root@ecs-centos7 ~]# firewall-cmd --zone=public --add-port=23/tcp --permanent
success
```

e. 重新加载策略配置，使新配置生效。

firewall-cmd --reload

f. 可以执行以下命令查看开启的所有端口。

firewall-cmd --list-ports

```
[root@ecs-centos7 ~]# firewall-cmd --list-ports
23/tcp
```

g. （可选）设置防火墙开机自启动。

systemctl enable firewalld.service

查看防火墙设置开机自启是否成功。

systemctl is-enabled firewalld.service;echo $?

回显信息如下说明已设置成功：

```
[root@ecs-centos7 ~]# systemctl is-enabled firewalld.service;echo $?
enabled
0
```

说明

可执行以下命令关闭防火墙开机自启动。

systemctl disable firewalld.service

相关链接

- **远程连接Linux云服务器报错：read: Connection reset by peer**

12.3 Linux 云服务器防火墙开放 80 端口后无法访问公网

问题描述

Linux云服务器开启了防火墙并在配置中开放了80端口，但是无法访问公网，关闭防火墙后，可以正常访问网站。

原因分析

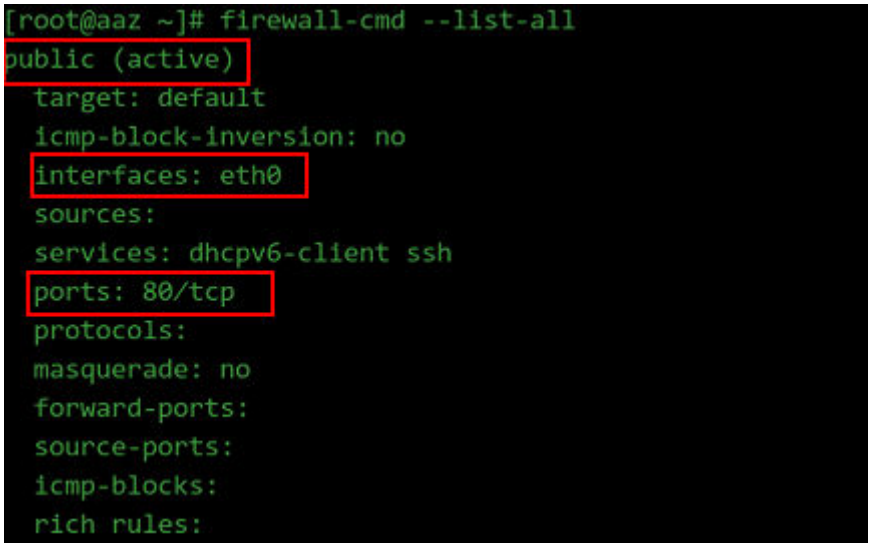
出现该问题的原因可能是防火墙规则与网卡接口不在同一区域zone。您可以按照以下步骤查看：

1. 执行如下命令，查看防火墙规则指定区域及开放端口。

```
firewall-cmd --list-all
```

下图示例中防火墙规则指定区域为public，开放端口为80，网卡接口为eth0。

图 12-1 查看防火墙信息

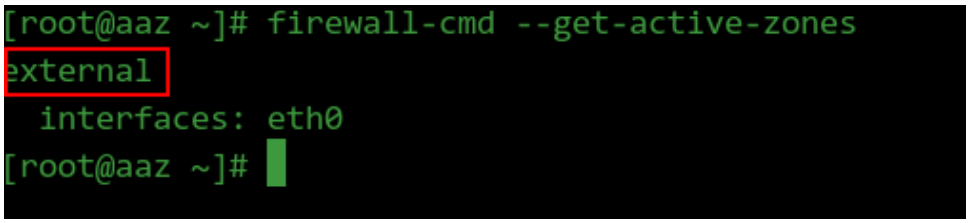


2. 执行如下命令，查看网卡接口所在区域。

```
firewall-cmd --get-active-zones
```

下图示例中网卡接口指定区域为external。

图 12-2 查看网卡接口所在区域



3. 执行如下命令，查看external区域下是否开放了80端口，具体示例如图12-3所示。

```
firewall-cmd --zone=external --list-ports
```

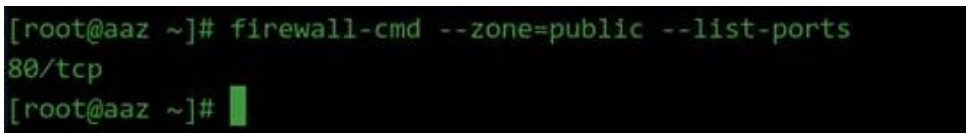
图 12-3 external 区域未开放端口

external区域下暂未开放80端口。

4. 执行如下命令，查看public区域下是否开放了80端口，具体示例如图12-4所示。

```
firewall-cmd --zone=public --list-ports
```

图 12-4 public 区域已开放端口



public区域下开放了80端口。

由此可知，防火墙规则与网卡接口不在同一区域，导致无法访问网站。

解决方法

方案一

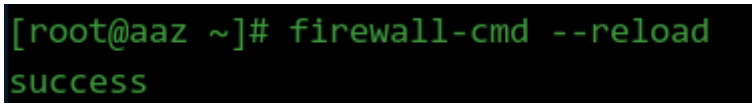
在网卡接口指定区域增加防火墙规则，开放80端口，具体操作如下。

1. 执行如下命令，开放80端口。
```
firewall-cmd --zone=external --add-port=80/tcp --permanent
```

图 12-5 开放 80 端口

2. 执行如下命令，更新防火墙规则。
```
firewall-cmd --reload
```

图 12-6 更新防火墙规则



3. 执行如下命令，查看防火墙规则。
```
firewall-cmd --zone=external --list-ports
```

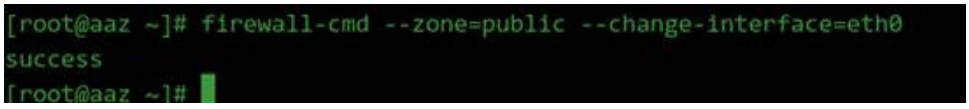
图 12-7 查看防火墙规则

方案二

修改网卡接口指定区域，使其与防火墙规则处于同一区域，具体操作如下。

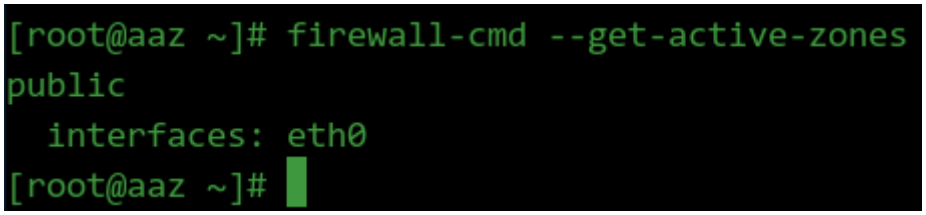
1. 执行如下命令，修改网卡接口指定区域。
```
firewall-cmd --zone=public --change-interface=eht0
```

图 12-8 修改网卡接口指定区域



2. 执行如下命令，查看网卡接口指定区域。
```
firewall-cmd --get-active-zones
```

图 12-9 查看网卡接口指定区域



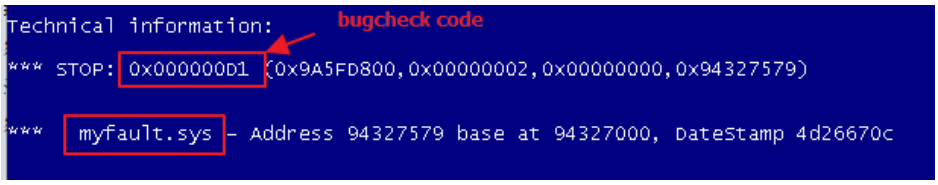
13 云服务器蓝屏

13.1 Windows 云服务器蓝屏如何处理?

问题描述

Windows操作系统云服务器蓝屏，如图13-1所示。

图 13-1 bugcheck code 以及可能的导致蓝屏的模块



可能原因

1. 使用了来源不明的第三方软件。
2. CPU占用过高导致。
3. 因为误操作或者病毒引起的系统文件、注册表损坏。

操作系统在蓝屏的情况下，会显示对应的bugcheck code以及可能的导致蓝屏的模块来大概说明问题发生的原因。

单击**Bug Check Code Reference** ，了解微软官方列举的bugcheck code解决方案。

处理方法

1. 建议不要安装来源不明的软件，使用正版软件，推荐使用Windows2012操作系统。
2. 如果是通过外部镜像创建的服务器，请参考《镜像服务用户指南》中“优化Windows私有镜像”章节优化私有镜像。
3. 排查是否是因为CPU占用过高导致的蓝屏，如果是请参考以下操作降低CPU使用率：
   - 可以通过把一些暂时不使用的进程关掉后再尝试。

- 或者可以尝试重启云服务器。
- 如果重装系统，请先备份重要数据。
- 如果服务器有重要数据不能重装，可以通过挂载磁盘方式拷贝数据，需要先备份，再卸载磁盘，然后挂载盘拷贝数据。

4. 如果需要分析蓝屏原因，需要确认是否有配置内存转储文件(crash dump)的收集，系统会自动生成蓝屏dump日志到指定的目录。

   由于蓝屏日志的分析非常耗时，建议客户在遇到蓝屏的情况，重启云服务器后，参考如上的可能原因进行排查。一般第三方杀毒软件、系统故障和CPU占用过高是导致云服务器蓝屏最常见的原因。

13.2 云服务器开机后蓝屏或黑屏不显示桌面怎么办?

问题描述

远程登录服务器出现蓝屏或黑屏，可能是由于explorer.exe进程异常导致的桌面无法显示。

根本原因

这是由于Windows服务器的explorer.exe进程异常导致的。explorer.exe是Windows程序管理器或者文件资源管理器，它用于管理Windows图形壳，包括桌面和文件管理，删除该程序会导致Windows图形界面无法使用。

解决方法

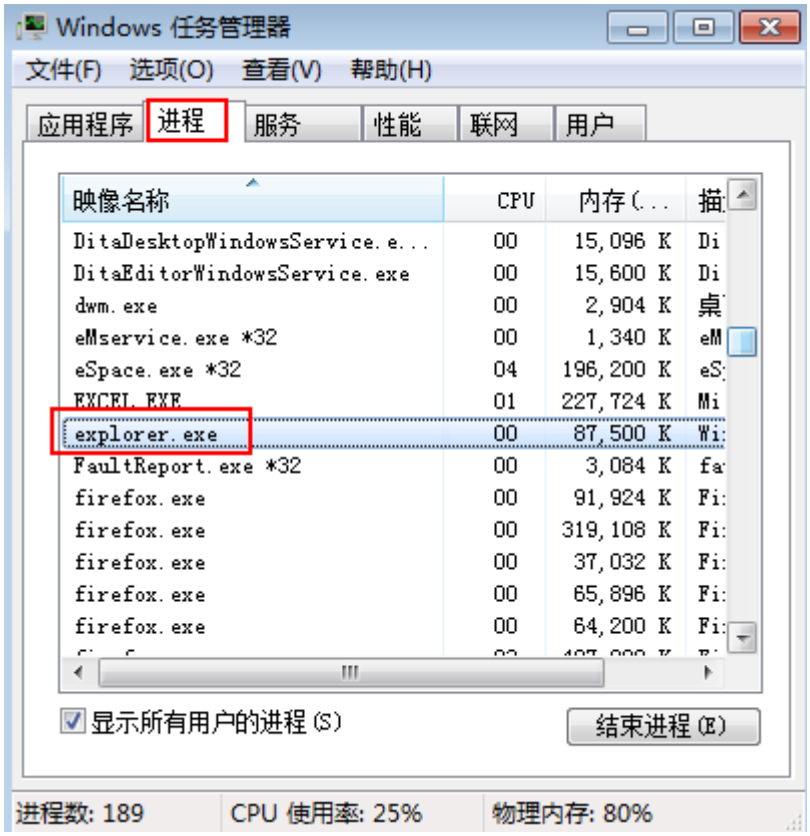
1. 打开云服务器的任务管理器。

   VNC登录页面，单击 

，可打开任务管理器。

2. 查看 “任务管理器 > 进程”是否有explorer.exe或是Windows资源管理器进程。
   - 如果有：结束掉该进程。
   - 如果在任务管理中未找到该进程。直接执行下面的操作启动该进程即可。

图 13-2 explorer.exe



3. 启动 explorer.exe 进程：

   单击“文件 > 新建任务”，在弹出的创建新任务对话框中输入“explorer.exe”，单击“确定”。

   说明

   如果还未出现正常界面，请重启云服务器。

图 13-3 新建任务

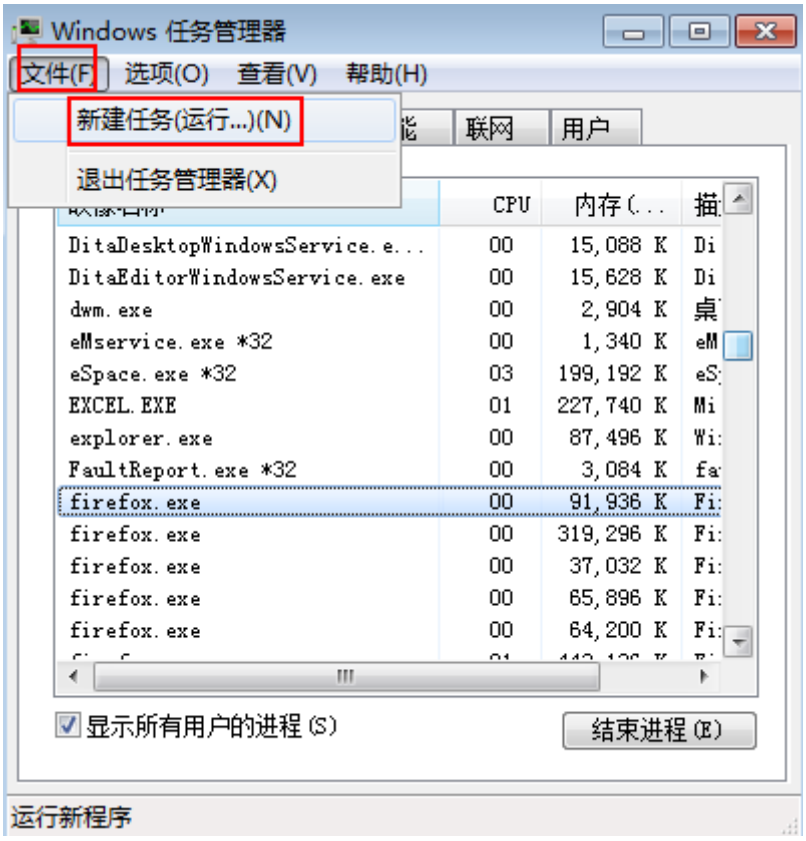
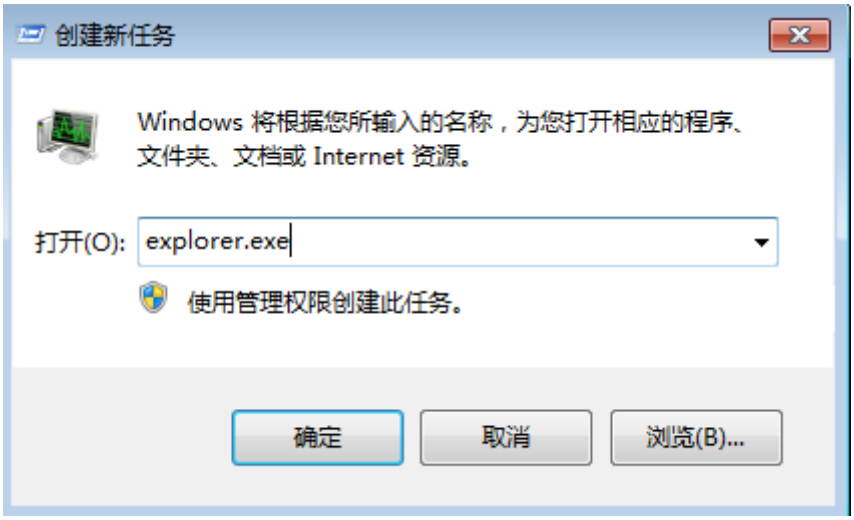


图 13-4 运行 explorer.exe



13.3 远程连接云服务器出现蓝屏

问题描述

Windows Server 2012 R2操作系统云服务器，本地使用远程桌面连接功能连接云服务器并启用redirected drive功能时，云服务器出现蓝屏。

根本原因

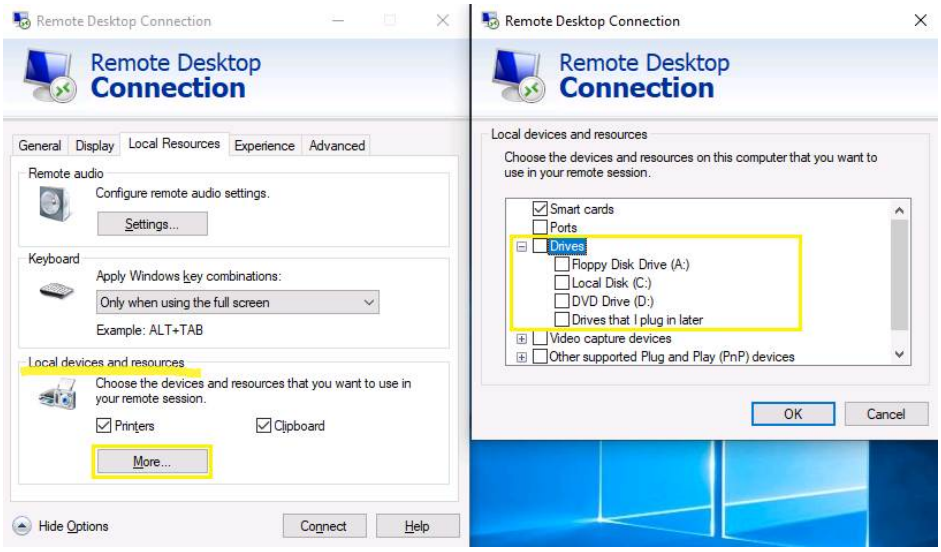
远程桌面连接启用了redirected drive功能，同时加载对应rdpdr.sys驱动，该驱动可能会导致云服务器操作系统崩溃，无法正常运作（例如错误码：0x18, 0x50, 0xa, 0x27, 0x133）导致云服务器蓝屏。

解决方法

使用远程桌面连接功能后，禁用redirect local drives功能。

1. 打开“运行”窗口。
2. 输入“mstsc”，并单击“确定”。
   系统打开“远程桌面连接”窗口。
3. 单击左下角的“选项”，并选择“本地资源”页签。
4. 在“本地设备和资源”栏，单击“详细信息”。
5. 在“本地设备和资源”窗口中，取消勾选“驱动器”。
6. 单击“确定”保存修改。

图 13-5 禁用 redirect local drives 功能



14 安装 IIS 服务

14.1 Windows 云服务器上安装 IIS 服务

操作场景

本节操作以Windows Server 2012 R2 标准版操作系统的云服务器为例，介绍安装IIS服务的操作步骤。

说明

本节操作仅是安装IIS服务的操作步骤，后续搭建具体应用的操作步骤请根据业务实际情况进行配置。

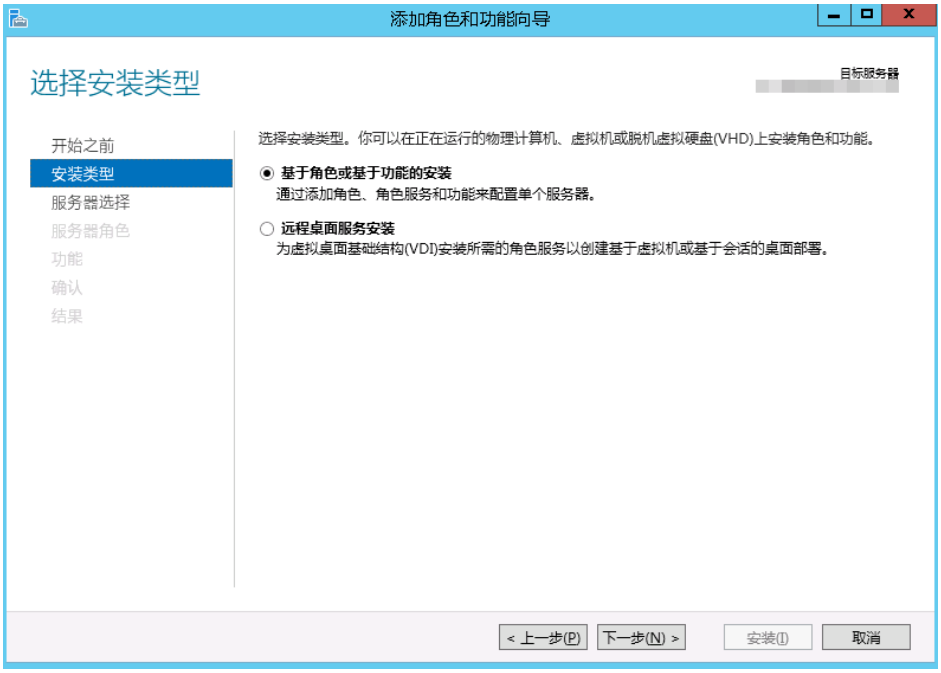
操作步骤

1. 打开服务器管理器。
2. 在“快速启动”栏，单击“添加角色和功能”。

图 14-1 添加角色和功能

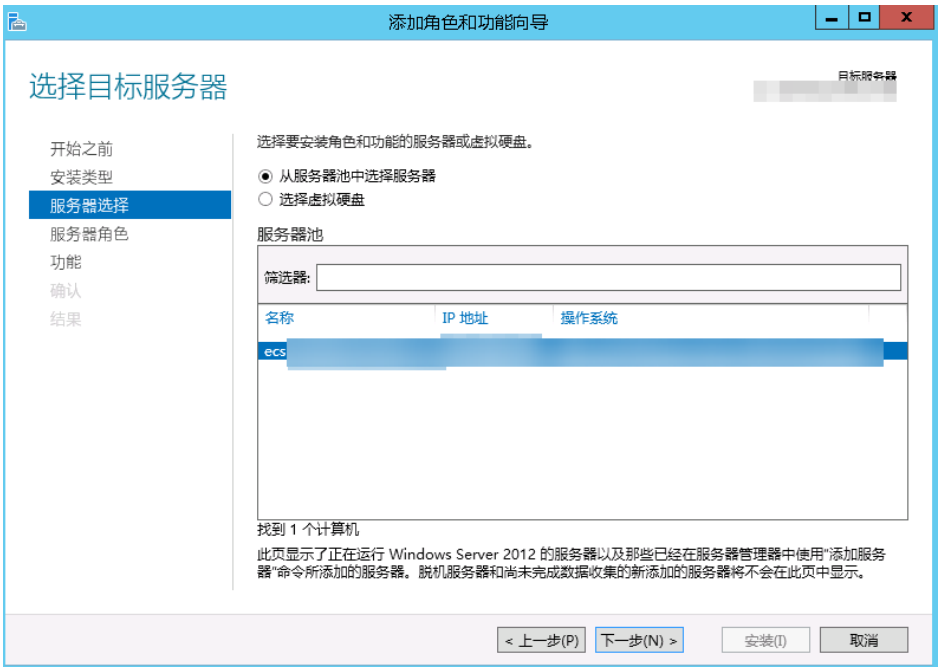
3. 在左侧导航栏，选择“安装类型”。

图 14-2 安装类型



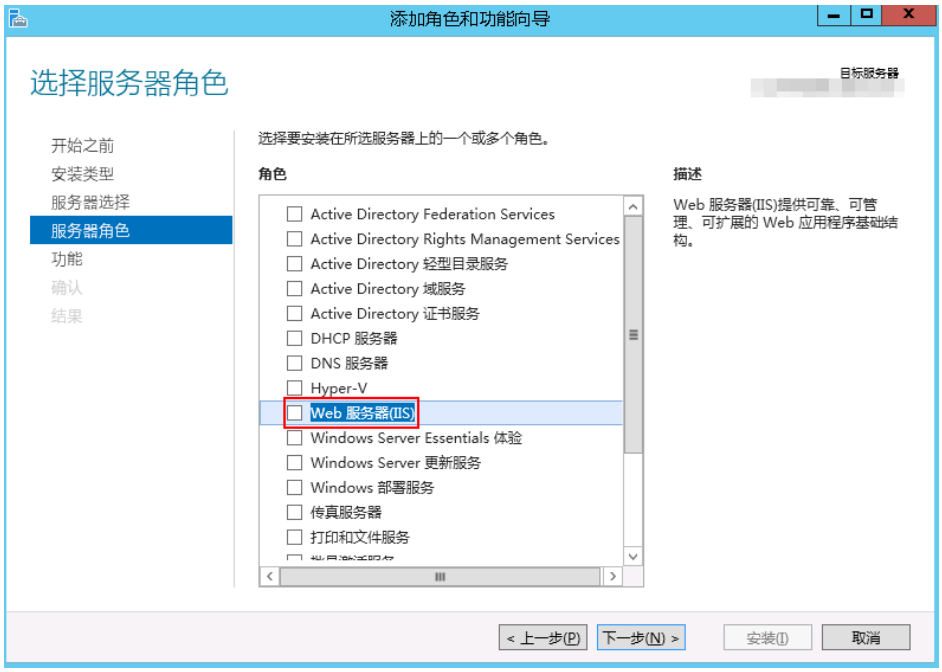
4. 单击“基于角色或基于功能的安装”，并单击“下一步”。
5. 在左侧导航栏，选择“服务器选择”。
6. 勾选“从服务器池中选择服务器”，并在“服务器池”中选择服务器的计算机名。

图 14-3 服务器选择



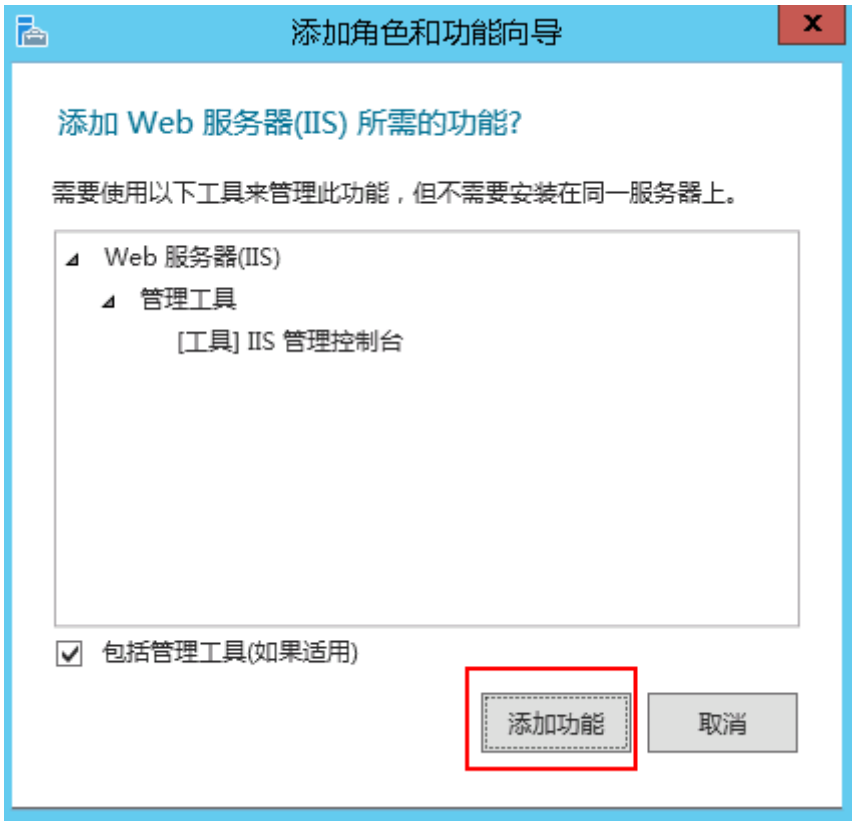
7. 单击“下一步”。
8. 在左侧导航栏，选择“服务器角色”。
9. 在角色列表内找到“Web服务器(IIS)”并勾选。

图 14-4 Web 服务器(IIS)



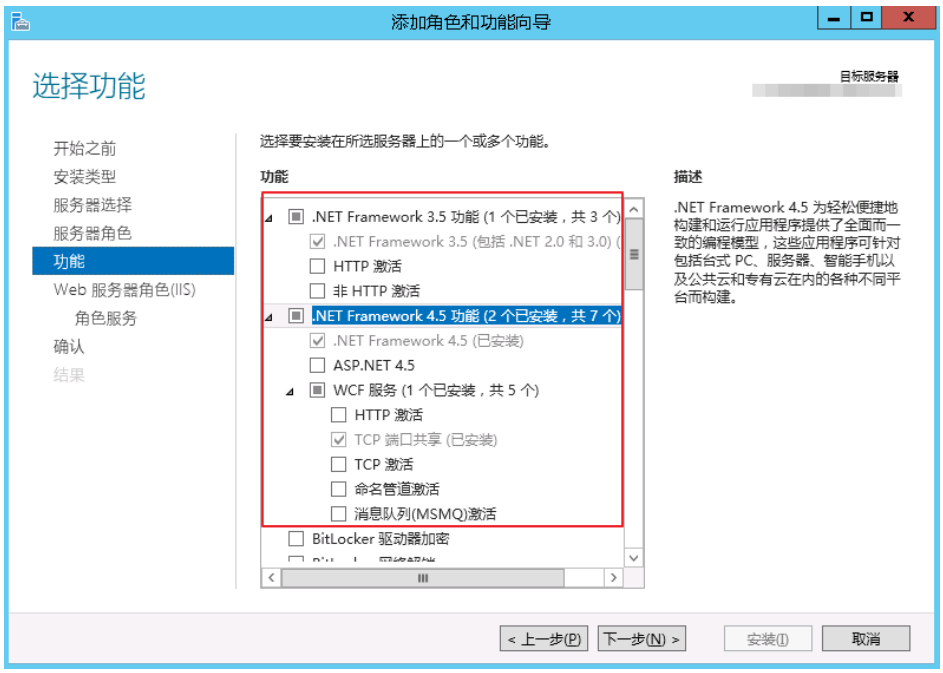
10. 在弹窗“添加角色和功能向导”中，单击“添加功能”。

图 14-5 添加功能



11. 在左侧导航栏选择“功能”，并勾选“.Net Framework 3.5”和“.Net Framework 4.5”。

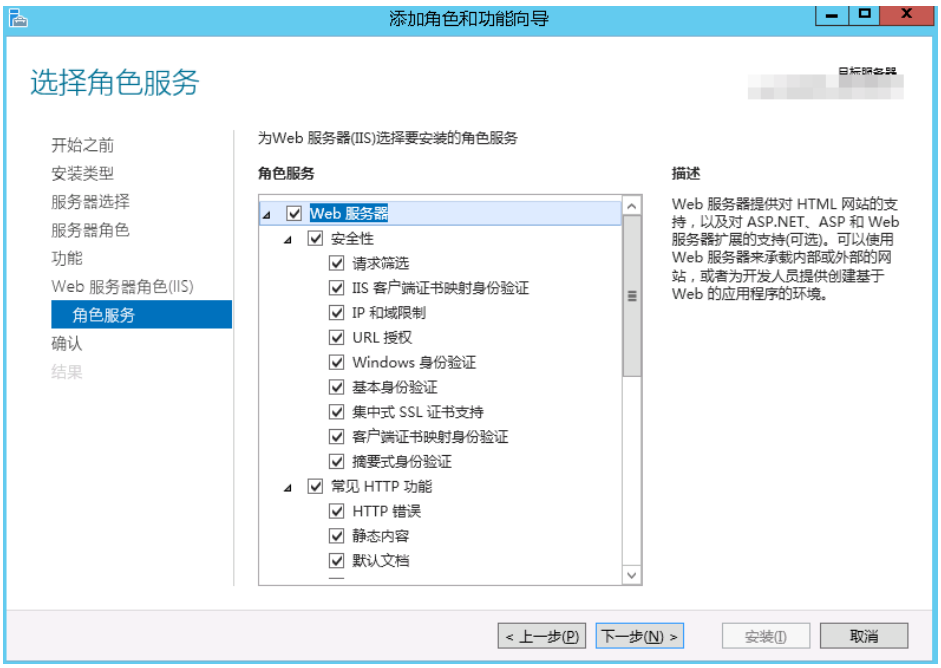
图 14-6 功能



12. 在左侧导航栏选择“Web服务器角色(IIS) > 角色服务”，并在角色服务列勾选需要安装的项目。

如果您不清楚需要安装哪些项目，除了FTP服务器，其他建议全部勾选。

图 14-7 角色服务



13. 单击“下一步”，确认安装的角色，然后单击“安装(I)”。

相关操作

IIS服务绑定域名请参考**IIS服务修改已绑定的网站域名**。

14.2 IIS 服务修改已绑定的网站域名

问题描述

访问IIS搭建的网站不通，报错404。

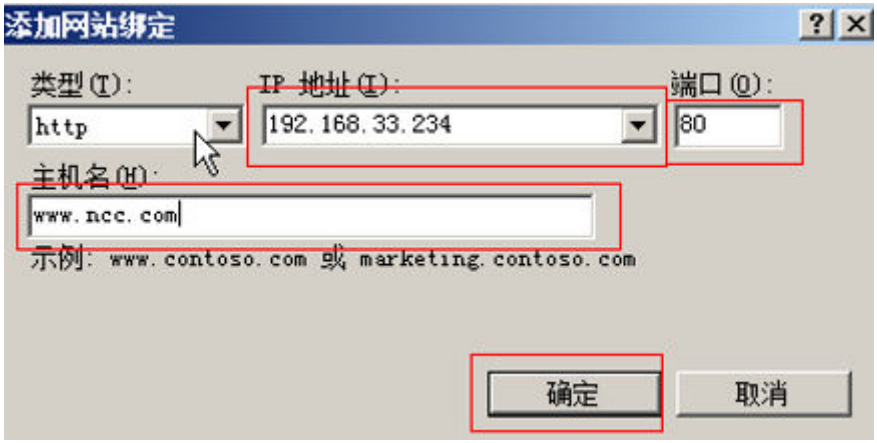
原因分析

IIS上绑定的域名只填写了主机名，没有指定IP地址。

操作步骤

本节操作指导用户修改IIS上绑定的域名，以Windows Server 2008 R2操作系统云服务器为例。

1. 登录服务器，选择“开始 >管理工具 > 信息服务（ IIS ）管理器。”
2. 在IIS管理器界面，选择自己需要编辑的网站。
3. 选择待修改的网站，单击右键选择“编辑绑定”。
   选择相应的域名，单击“编辑”，添加指定云服务器的私有IP地址。



14.3 怎样做网页定向?

操作场景

本指导适用于用户做网页301重定向时参考使用。

操作步骤

装有IIS的服务器做301重定向

1. 在IIS里把网站正常发布，例如域名为www.aaa.com。
2. 在硬盘上建一个空文件夹。
3. 在IIS里建一个网站，例如域名为aaa.com，指向新建的空文件夹。
4. 在网站的主页，选择“HTTP重定向”，具体参数设置如下：
   - 勾选“将请求重定向到此目标”。
   - 重定向地址：www.aaa.com$S$Q

     说明

     在网址后添加“SQ”的作用是：支持带“？”的网址可以正常跳转。如果未添加“SQ”，带“？”的网址跳转时会出现异常。
   - 勾选“将所有请求重定向到确切的目标(而不是相对于目标)”。
   - 状态代码：永久(301)。

图 14-8 HTTP 重定向

相关操作

除了通过IIS实现重定向外，您还可以通过代码实现301重定向，以下为在PHP和Apache下实现301重定向的代码示例：

- PHP下的301重定向

```
<?php
Header("HTTP/1.1 301 Moved Permanently");
Header("Location: http://www.***.cn"); //跳转到带www的网址
?>
```

- Apache服务器实现301重定向

  WWW域名的重定向。参考代码如下：

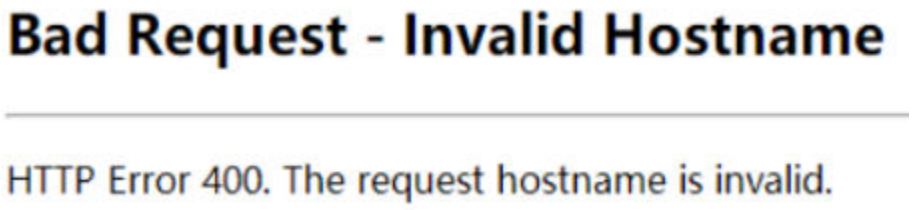
```
deny from all
RewriteEngine on
RewriteCond %{HTTP_HOST}^(****\.com)(:80)?[NC]
RewriteRule ^(.*) http://www.****.com/$1[R=301,L]
order deny,allow
```

14.4 Windows 云服务器访问使用 IIS 创建的 Web 站点时，提示“Bad Request - Invalid Hostname”错误

问题描述

在Windows云服务器访问使用IIS创建web站点时，提示“Bad Request - Invalid Hostname”错误，如**图 访问报错**图所示。

图 14-9 访问报错



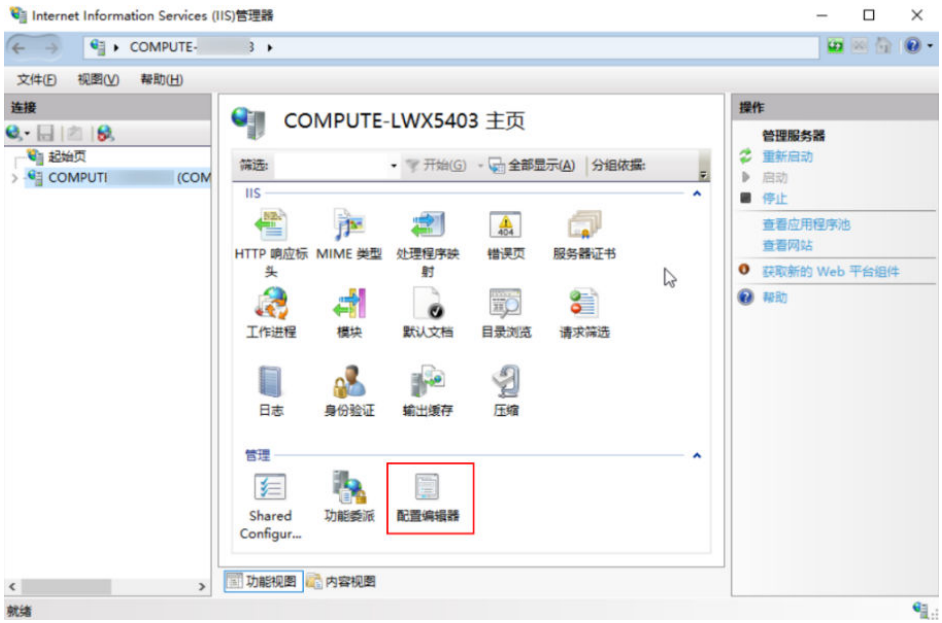
可能原因

在IIS管理器中，如果配置Web站点大于等于100个时，启动IIS服务时不会激活任何站点并且提示“Bad Request - Invalid Hostname”错误。

处理方法

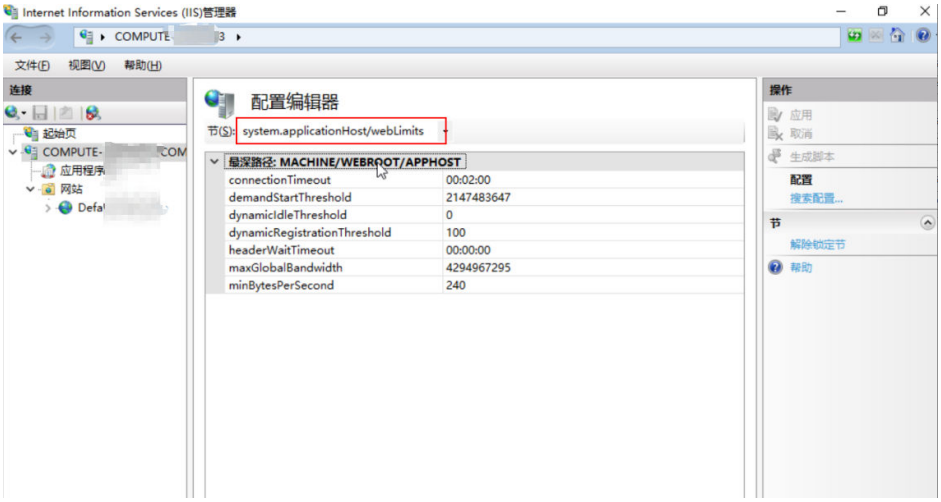
1. 登录Windows云服务器。
2. 选择“开始 > Windows管理工具 > Internet Information Services (IIS)管理器。”
3. 在IIS管理器页面，选中目标服务器，然后双击 “配置编辑器”。

图 14-10 IIS 管理器页面



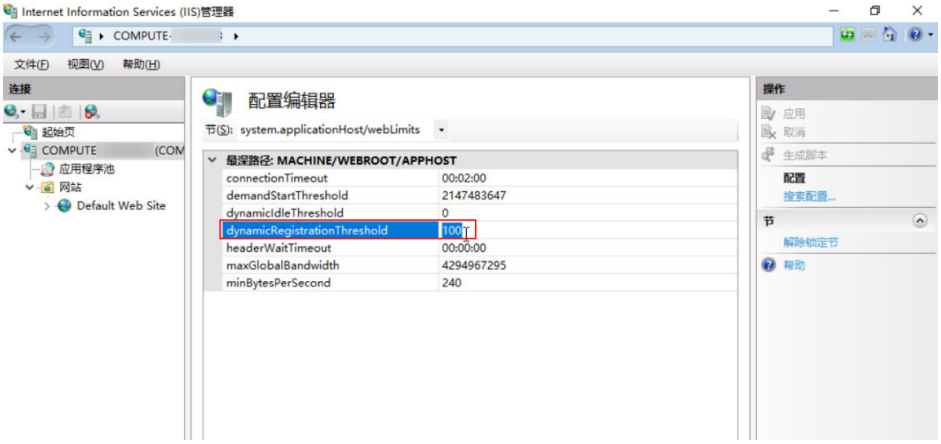
4. 选择“system.applicationHost/webLimits ”节。

图 14-11 配置编辑器界面



5. 将“dynamicRegistrationThreshold”的值设置为100。

图 14-12 设置新阈值



6. 重新访问网站。

