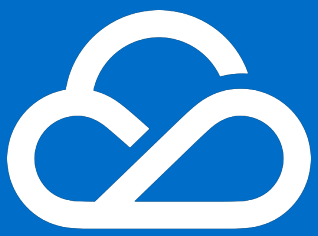
腾讯云云服务器

常见问题

产品文档



腾讯云

【版权声明】

【商标声明】

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或模式的承诺或保证。

文档目录

常见问题

无法登录云服务器

若您无法连接实例，建议按照如下原因进行排查：

端口问题

故障现象：

端口远程连接失败。

解决方法：

可能由远程访问端口非默认端口或端口设置不一致所致。

详见 端口问题导致无法远程连接 。

CPU/内存占用率高问题

故障现象：

使用云服务器时，出现无法登录、服务速度变慢、实例突然断开情况。

解决方法：

可能存在 CPU 或内存荷载过高的问题，检查资源占用情况。

Windows 云服务器详见 Windows系统CPU与内存占用率高导致无法登录 。

Linux 云服务器详见 Linux系统CPU与内存占用率高导致无法登录 。

外网被隔离问题

故障现象：

云服务器出现违规事件或风险事件时，被进行部分隔离。

解决方法：

详见 外网被隔离导致无法远程连接 。

外网带宽占用高问题

故障现象：

带宽跑满或跑高，导致无法登录。

解决方法：

详见 外网带宽占用高导致无法登录 。

安全组设置问题

故障现象：

服务器 telnet 无法连接，排查防火墙、网卡 IP 配置无误，回滚系统后仍然无法连接。

解决方法：

详见 安全组设置导致无法远程连接 。

关联密钥后无法使用密码

故障现象：

云服务器关联密钥后，无法使用密码登录，排查防火墙、网卡 IP 配置无误。

解决方法：

云服务器关联密钥后，云服务器 SSH 服务默认关闭用户名密码登录，请您使用密钥登录服务器。密钥登录方式可参见 SSH 密钥 。

远程登录网络级别身份验证

故障现象：

使用 Windows 系统自带远程桌面连接，有时出现无法连接到远程计算机的问题。

解决方法：

详见 远程登录网络级别身份验证 。

xshell 无法密码登录

故障现象：

使用 xshell 进行登录时，无法使用密码登录云服务器。

解决方法：

您在安装系统时已选择密钥登录方式，如何使用密钥可参考 SSH 密钥

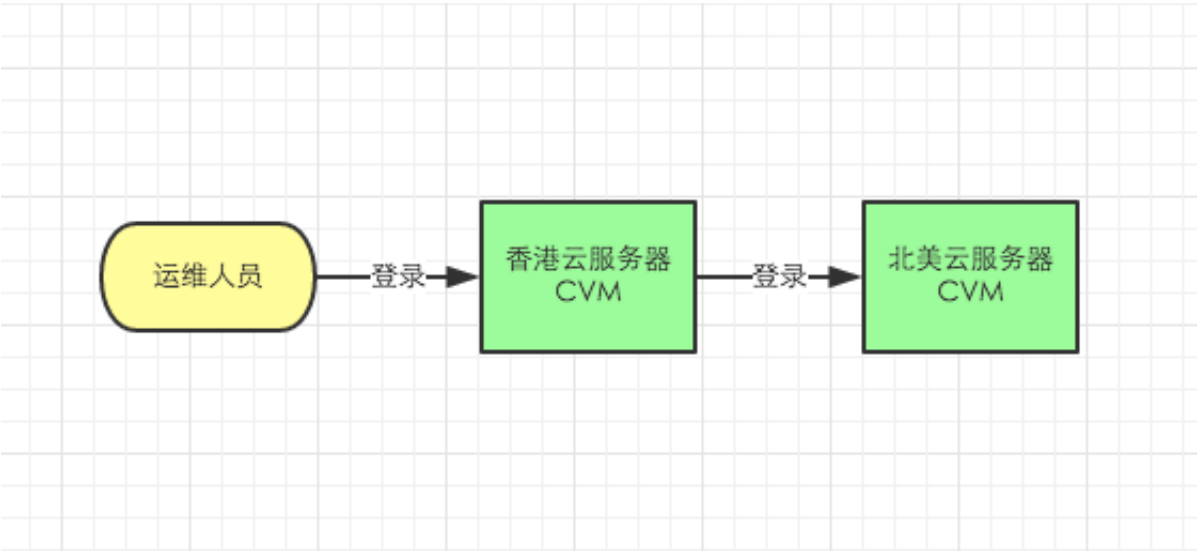
如需采用密码方式登录，可重装系统时选择密码登录，或者进入登录计算机修改 sshd 配置文件。

国际链路时延

问题描述

北美地域云服务器登录时延太长。

因全国国际路由出口较少及某些其他原因，并发数大时，国际链路会非常拥塞并导致访问不稳定，对此腾讯云已经向运营商进行反馈。目前，购买了北美地域云服务器的客户若需要在国内进行管理运维。短时间内您可使用在香港地域购买云服务器,然后通过香港地域 CVM 进行中转登录的方法解决该问题。



解决办法

1. 购买香港地域的 Windows 云服务器，在自定义配置页中 选购，（ Windows 操作系统可以支持登录北美 Windows 和 Linux 这两类云服务器，推荐选购）作为“跳板机”。

   注意：
   您需要购买至少 1 Mbps 的带宽，否则跳板机无法登录。

2. 购买成功后，登录香港地域的 Windows 云服务器：
   从 Windows 机器登录有公网 IP 的 Windows 云服务器
   控制台 VNC 登录 Windows 云服务器

3. 在香港地域的 Windows 云服务器内，登录您位于北美地域的 CVM ：

- 登录北美地域的 Linux 云服务器

  从 Windows 机器使用密码登录有公网 IP 的 Linux 云服务器

  从 Windows 机器使用密钥登录有公网 IP 的 Linux 云服务器
- 登录北美地域的 Windows 云服务器

  从 Windows 机器登录有公网 IP 的 Windows 云服务器

  控制台 VNC 登录 Windows 云服务器

云服务器配置调整

调整云服务器配置相关

问：哪里查看调整配置的记录？

控制台 右上角操作日志中可以展示您对 CVM 调整配置的记录。对于包年包月的 CVM ，在收支明细中升配和降配都会产生相应的订单。

操作日志

问：包年包月计费模式的配置降级延长时长是如何计算的？

计算截止至云服务器降级时刻，实际支付费用为剩余价值与目标配置剩余价值的应补差值。若应补差价大于零，将该差值折算为目标配置所支持的时长，延长该服务器的到期时间；若应补差价小于等于零，将不会调整您的服务器到期时间。

问：包年包月计费模式下的配置降级，可能产生配置降低了没有延长使用时长的情况吗？

可能。
例如，降配前，您的配置为 A ，官网售卖价格为 100 元/月，您购买时正好遇到官网运营活动 5 折优惠，您的购买价格为 50 元/月。使用 10 天后，此时，您需要降配，降配的配置为 B ，官网价格为 60 元，按照实际支付和官网价格折算，应补差价小于 0 ，将不会调整您的服务器到期时间。
同样的情况还可能发生在购买时使用代金券等非现金支付。遇到这种情况，在降配时会提示您如下信息：

> 该云服务器共有 1 次降配机会，还有 1 次；
> 原始配置为 2 核 8GB ，目标配置为 1 核 2GB ；
> 降低配置，按照实际支付和官网价格折算，应补差价 ** 元；
> 由于应补差价小于零，将不会调整您的服务器到期时间。

问：按量计费调整配置后如何计费？

调整配置后，即时生效，精确到秒。
例如，您的配置为 1C2G ，在 1 点 23 分 21 秒配置升级成功为 2C4G ，在 2 点整结算时，23 分 21 秒按 1C2G 配置计费，后面的 36 分 39 秒按 2C4G 配置计费，精确到秒。

调整网络相关问题

问：什么是带宽包模式？

带宽包是云主机共享公网带宽的一种网络计费方式，计费分为提前购买带宽包和超出月结两部分，您可以在本月购买未来几个月的带宽包：
当下个月实际使用小于带宽包额度时，不再额外扣费；当下个月实际使用大于带宽包额度时，将在月底根据超出部分进行额外结算。
价格如下：

	带宽包（元/Mbps）	超出部分（元/Mbps）
大陆	100	108
香港	100	108
北美	200	216

问：按流量计费和按带宽计费可以切换吗？

切换前提是云服务器为包年包月计费类型。

1. 每台主机只允许在按带宽计费与按流量计费两种模式之间转换 2 次，包年包月按带宽计费切换成按流量计费，就算转换一次。再把按流量计费切换成按带宽计费，也算一次，两次用完之后，不能切换。
2. 流量计费切换带宽计费实时生效。切换后带宽费从切换当天 0 点开始算。带宽费用按原价计算，不享受折扣。

系统盘

问：重装系统时，是否可以调整系统盘的大小？

- 系统盘为云盘的云服务器，重装系统时可以调高系统盘大小，不可以降低系统盘大小。
- 系统盘为本地盘的云服务器，重装系统时，根据当前系统盘大小的不同，默认重装后的值也不同。如，当前系统盘大小是 20GB 及以下的，将默认重装至 20GB ；如果当前系统盘大小是 20GB 以上的，将默认重装至 50GB 。

问：哪些地域可用区支持系统盘可调整至大于 50GB ？

北京、上海、广州地区支持云硬盘系统盘调整至大于 50GB，国内金融专区和其他地域暂不支持。

问：存量云盘 CVM 的系统盘容量与费用如何调整？

容量：老用户的云硬盘类型云服务器，在重装系统时会默认调整至 50GB 。
价格：包年包月类型的最终单价在大部分情况下不变，按量计费类型的最终单价将会有小幅升高。

问：系统盘是否支持扩容后再通过重装系统缩容？

系统盘不支持缩容。

问：有没有办法可以让我保存云主机当前的数据并扩容系统盘？

可以选择先制作镜像，再通过镜像重装系统，从而达到扩容系统盘的目的。

问：选择了低于 50GB 的小容量存量镜像，用来创建或重装云服务器时，系统盘是多大？

选择的小镜像，不影响系统盘大小，最低均为 50GB 。

问：老用户 Linux 云服务器系统盘支持扩容至 20GB 吗？

存量 8GB 本地系统盘可以通过重装系统实现将本地盘扩容为 20GB 。

问：已购买超过 20 GB 云硬盘类型的 Linux 云服务器，重装为 Windows 操作系统，如何计费？

若用户新购了超过 20GB 的云硬盘类型的 Linux 云服务器，在切换为 Windows 时，将根据计费方式的不同进行相应处理：

- 若该云服务器为包年包月类型，则根据支付时的情况进行相应的退费（扣除支付中使用的代金券等金额）或调低；
- 若该云服务器为按量计费类型，则在重装 Windows 成功后，停止计算之前购买的超出 20GB 部分的系统盘配置费用（即系统盘不再收费）。

问：已购买云硬盘类型的 Windows 云服务器，重装为 Linux 操作系统，如何计费？

由于目前系统盘不支持缩容，所以将容量为 50GB 的 Windows 云硬盘重装为 Linux 时，需要保留容量并支付相应的云硬盘费用（免费额度为 20GB，需支付 30GB 的硬盘费用）。详情请见 硬盘价格 。

安全组

安全组使用相关

为什么购买实例时需要选择安全组？

安全组
是一种虚拟防火墙，用于设置单台或多台云服务器进行出/入流量控制
。它是重要的网络安全隔离手段，每个云主机至少属于一个安全组。因此，在创建的时候就需要指定。
您可以在云主机 购买页 或 控制台 创建安全组（支持 模板 和 自定义 创建
），通过配置安全组规则对出入云主机的数据包进行控制。安全组模板包括：

- 放通 22、80、443、3389 端口和 ICMP，放通 Windows 和 Linux 默认的登录端口和常见的 Web 服务端口到公网，内网端口全通。
- 放通全部端口：暴露全部端口到公网和内网，有一定安全风险。

选择安全组不正确，会对绑定该安全组的实例有何影响？如何解决？

问题隐患

- 远程连接(SSH) Linux 实例、远程登录桌面 Windows 实例可能失败。
- 远程 Ping 该安全组下的 CVM 实例的公网 IP 和内网 IP 可能失败。
- http 访问该安全组下的实例暴露的 Web 服务可能失败。
- 该安全组下实例可能无法访问 Internet 服务。

解决方案

- 如果发生以上问题，可以在控制台的安全组管理中重新设置安全组规则，例如：只绑定默认全通安全组
。
- 具体设置安全组规则参考 安全组操作指南 。

安全组策略的生效顺序是怎样？

从上至下。流量经过安全组时的策略匹配顺序是从上至下，一但匹配成功则策略生效。

什么是安全组的方向和策略？

安全组策略方向分为出和入，出方向是指过滤云主机的出流量，入方向是指过滤云主机的入流量。
策略分为允许和拒绝流量。

为什么安全组未允许的 IP 依然能访问云服务器 ？

- CVM 可能绑定了多个安全组，特定 IP 在其他安全组中允许。
- 特定 IP 属于审批过的腾讯云公共服务。

同时绑定多个安全组的优先级如何确定？

优先级数字越小，优先级越高。

- 安全组默认最后有deny策略。
- 当多个安全组叠加使用的时候，只有最后一个安全组的deny策略生效。

如何调整安全组优先级？

登录 控制台 - 详情页 - 安全组 - 已加入安全组 - 编辑。

云服务器已经全部退还，为何安全组无法删除?

请查看回收站内是否还有云主机。安全组绑定了回收站内的云服务器同样无法被删除。

使用了安全组是否意味着不可以使用 iptables ？

不是。安全组和 iptables 可以同时使用，您的流量会经过两次过滤，流量的走向如下：

- 出方向：实例上的进程 -> iptables -> 安全组。
- 入方向：安全组 -> iptables ->实例上的进程。

TCP 25 端口出方向被封禁？

无法使用 TCP 25 端口连接外部地址。例如，运行

Telnet smtp.***.com 25

，该命令执行失败，但是安全组并没有禁止该端口。

原因：为了提升腾讯云 IP 地址发邮件的质量，将默认限制云主机 TCP 25 端口连接外部地址 。

解封方法：登录腾讯云控制台，鼠标移动到账号，即见 25 端口解封 入口，每个客户在每个地域默认可解封 5 个云服务器。

25 端口主要用于 SMTP 邮件服务器的架设，如果您没有在云上部署邮件服务，则本次端口封堵不会对您的服务造成影响；如果您在云主机中使用 25 端口部署了邮件服务，则您的邮件服务将受到影响而暂时不可用。

我们诚挚地推荐您使用腾讯企业邮箱（exmail.qq.com）代替云上的 SMTP 邮件服务，来提高业务的整体安全性。如果您一定要保留云上的 SMTP 服务，请优先在云主机内安装相关安全工具，如 云镜，进行相风险控制。

> 注意：
> 如果您发起解封申请，腾讯云将默认您已确认并承诺：保证 TCP 25 端口仅用来连接第三方的 SMTP 服务器，并从第三方的 SMTP 服务器向外发邮件。如发现您使用申请的 IP 直接通过 SMTP 发送邮件，腾讯云有权永久性封禁 TCP 25 端口，并不再提供解封服务，如有其它问题，请提 工单申请。

云主机已经解封访问外网的 TCP 25 端口，仍无法访问外网的 TCP 25 端口？

您好，请检查：

- 云主机安全组的出站规则是否禁止了 TCP 25。
- 云主机是否处于正常运行状态。

安全组克隆相关

安全组跨项目跨地域克隆，会将安全组管理的云服务器一起复制过去吗？

不会，安全组跨地域克隆，只将原安全组出入口规则克隆，云服务器需另行关联。

安全组是否支持跨用户克隆？

暂不支持。

安全组跨项目跨地域克隆是否有云 API 支持？

目前为了方便使用控制台的客户，提供了 MC 的支持，暂无直接云 API
支持，您可通过原有的批量导入导出的安全组规则的云 API ，间接达到安全组的跨项目跨地域克隆。

安全组克隆时命名能否与目标区域的安全组相同？

不行。命名需保持与目标地域现有安全组名称不同。

镜像

镜像共享相关

问：每个镜像最多可以共享给多少个用户？

50个。

问：共享镜像能否更改名称和描述？

不能。

问：共享镜像是否占用自身镜像配额？

不占用。

问：共享镜像在创建和重装云主机时是否有地域限制？

有地域限制，共享镜像与源镜像同地域，只能在相同地域创建和重装云主机。

问：共享镜像是否能复制到其他地域？

不能。

问：共享给其他用户的自定义镜像是否可以删除？

可以删除，但需先取消该自定义镜像所有的共享。

问：其他用户共享的镜像是否能删除？

不能。

问：使用其他用户共享的自定义镜像存在什么样的风险？

使用其他用户共享的镜像，腾讯云不保证该共享镜像的完整性和安全性，请您选择选择信任的账号共享给您的镜像。

问：能否将别人共享给我的镜像再共享给其他人？

不能。

Windows系统制作自定义镜像失败

若 Windows 系统制作镜像失败，请依次做如下检查：

1. 请确保以下服务正常运行

程序名	安装位置	服务名称
QcloudService.exe	C:\Windows\	Qcloud服务
WinAgent.exe	C:\WinAgent\	WinAgent Display Name
win-agent.exe	C:\win-agent\	win-agent

   请确保以上服务以及所有腾讯云官方提供的以 Win_Agent 开头的服务运行正常。

2. 自定义镜像制作依赖微软自带的 Windows Modules Installer 服务，请确保该服务运行正常。

3. 自定义镜像制作脚本执行被一些杀毒工具或安全狗拦截，为避免制作失败，建议在制作自定义镜像前先关闭这些工具。

4. 镜像制作工具在执行时被系统弹窗中断，请远程登录云服务器查看，并调整云服务器设置，避免弹窗。

性能相关

CPU 使用率过高排查（Windows 系统）

CPU 使用率过高，容易引起服务响应速度变慢、服务器登陆不上等问题。可以使用 云监控，创建 CPU 使用率阈值告警，当 CPU 使用率超过阈值时，将及时通知到您。

CPU 使用率过高排查的步骤大致为：定位消耗 CPU 的具体进程，对 CPU 占用率高的进程进行分析。如果为异常进程，可能是病毒或木马导致，可以自行终止进程，或者使用安全软件进行查杀；如果是业务进程，则需要分析是否由于访问量变化引起，是否存在优化空间；如果是腾讯云组件进程，请 发起工单 联系我们进行进一步定位处理。

下面将介绍 Windows 系统如何定位 CPU 使用率过高的问题。

定位工具介绍

任务管理器：Windows 自带的应用程序和进程管理工具，展示有关电脑性能和运行软件的信息，包括运行进程的名称，CPU 负载，内存使用，I/O 情况，已登录的用户和 Windows 服务的信息。可以通过快捷键 CtrL+Shift+Esc，或开始菜单右键点击任务管理器，或运行中输入 taskmgr 的方式打开。

进程：系统上所有正在运行的进程的列表。

性能：有关系统性能的总体统计信息，例如总体 CPU 使用量和正在使用的内存量。

用户：当前系统上有会话的所有用户。

详细信息：进程选项卡的增强版，显示进程的 PID、状态、CPU/内存的使用情况等进程的详细信息。

服务：系统中所有的服务（包括并未运行的服务）。

问题定位及处理

CPU 使用率过高可能由硬件因素、系统进程、业务进程或者木马病毒等因素引起，下面介绍如何定位到占用 CPU 的具体进程以及对如何对进程进行分析处理。

1. 登录到 Windows 服务器。
   说明：服务器负载较高时，远程连接可能失败，建议使用 VNC 方式登录到服务器。如何使用 VNC 方式登陆Windows服务器详见登录 Windows 实例中 VNC 登录小节。

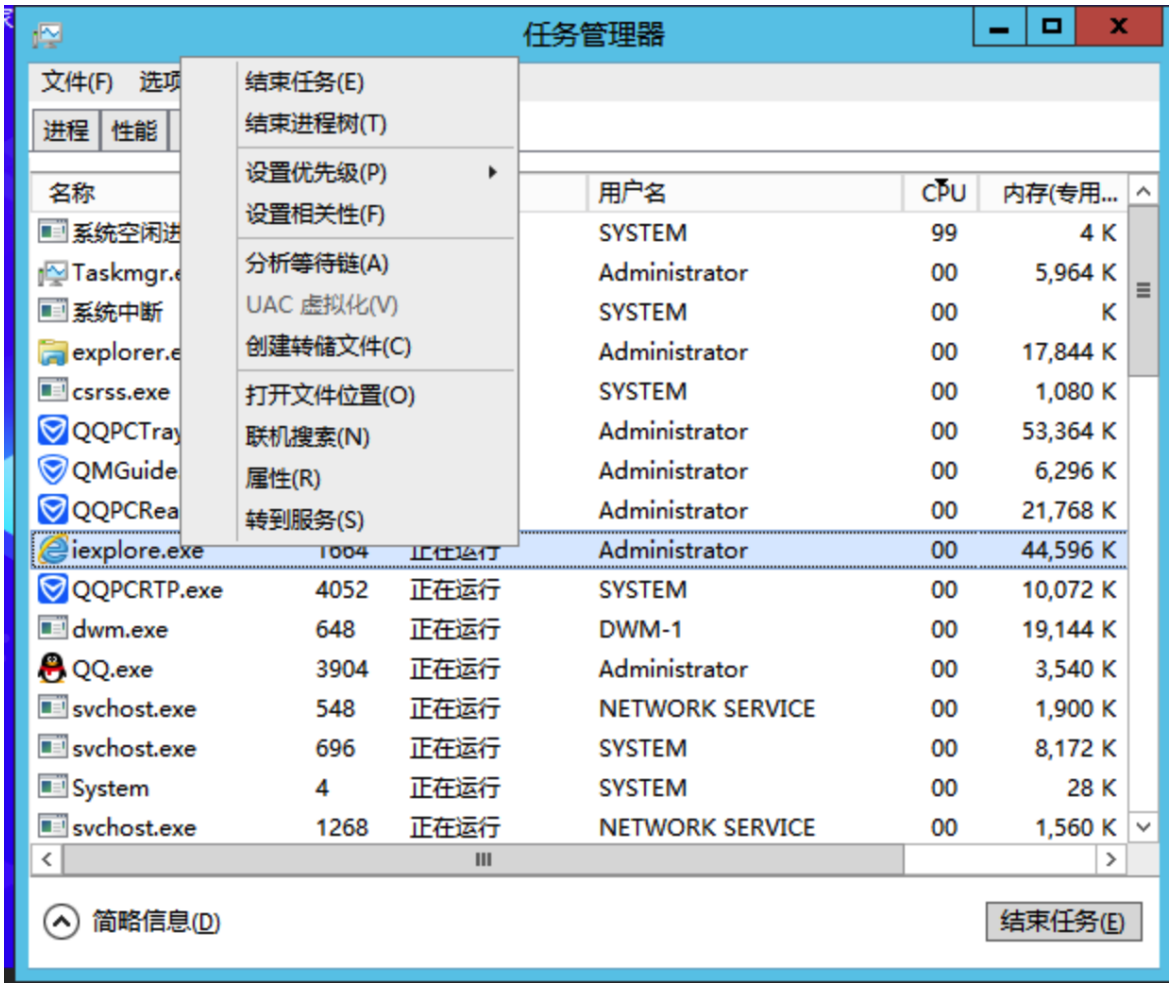
2. 使用 Ctrl+Shift+Esc 或开始菜单右键点击任务管理器打开任务管理器，切换到详细信息 tab，点击 CPU 使进程按照 CPU 使用率降序排列。

3. 分析占用 CPU 多的进程。占用 CPU

多的可能为系统、业务抑或是异常进程，下面将例举这三种情况该如何处理：

1. 系统进程。

当发现系统进程占用大量 CPU 资源时，需要仔细检查进程名，不少病毒会通过使用跟系统进程相似的名称，迷惑用户的眼睛。例如：svch0st.exe、explore.exe、iexplorer.exe，要仔细甄别。其次要注意检查这些进程对应的可执行文件对应的位置，系统进程一般位于 c:\windows\system32，并且会有完善的签名和介绍，在任务管理器对应的进程处右键，点击打开文件位置，可以查看具体可执行文件的位置。如果进程位置也不是在 c:\windows\system32 目录下，服务器可能中了病毒，请手动或者使用安全工具进行查杀。



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

2. 异常进程。如果占用大量 CPU 资源的是一些命名很奇怪的进程，可能为木马病毒进程。建议使用搜索引擎进行搜索确认，例如xmr64.exe（挖矿病毒）等。确认后使用安全工具进行查杀。

3. 业务进程。如果发现占用 CPU 资源的是您的业务进程（iis、httpd、php、java 等），建议进一步分析，例如当前业务量是否较大，则高负载时正常情况，建议考虑升级服务器配置；否则可以考虑业务程序是否存在优化空间，进行优化。

CPU 使用率过高排查（Linux 系统）

CPU 使用率过高，容易引起服务响应速度变慢、服务器登陆不上等问题。可以使用 云监控，创建 CPU 使用率阈值告警，当 CPU 使用率超过阈值时，将及时通知到您。

CPU 使用率过高排查的步骤大致为：定位消耗 CPU 的具体进程，对 CPU 占用率高的进程进行分析。如果为异常进程，可能是病毒或木马导致，可以自行终止进程，或者使用安全软件进行查杀；如果是业务进程，则需要分析是否由于访问量变化引起，是否存在优化空间；如果是腾讯云组件进程，请 发起工单 联系我们进行进一步定位处理。

下面将介绍 Linux 系统下如何定位出 CPU 使用率过高的进程。

定位工具介绍：top 命令

top：Linux 系统下常用的监控工具，用于实时获取进程级别的 CPU 使用情况。下图是 top 命令的输出信息。

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

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

上半部分显示 CPU 和内存资源的总体使用情况：

第一行：系统当前时间，当前登陆用户个数以及系统负载。

第二行：系统总进程数、运行中进程数、休眠、睡眠和僵尸进程数量。

第三行：CPU 当前使用情况。

第四行：内存当前使用情况。

第五行：swap 空间当前使用情况。

下半部分以进程为维度显示资源的占用情况。

PID：进程 ID。

USER：进程所有者。

PR：进程优先级 NI：NICE 值，NICE 值越小，优先级越高。

VIRT：使用的虚拟内存大小，单位 KB。

RES：当前使用的内存大小，单位 KB。

SHR：使用的共享内存的大小，单位 KB。

S：进程状态。

%CPU：更新时间间隔内进程所使用的 CPU 时间的百分比。

%MEM：更新时间间隔内进程所使用的内存的百分比。

TIME+：进程使用的 CPU 时间，精确到 0.01s。

COMMAND：进程名称。

问题定位及处理

使用工具定位 CPU 使用率高的进程

前面介绍了 top 工具，下面介绍如何利用该工具定位出 CPU 使用率高的进程。

1. 通过 SSH 或者 VNC 方式登陆实例

   说明：CPU 使用率过高，容易引起服务器登陆不上，此时可以尝试使用 VNC 登陆的方式。使用 VNC 登陆实例的方法详见 登陆 Linux 实例 相关小节。

2. 输入 top 命令查看系统负载。

3. 输入大写 P，进程按 CPU 使用率降序排列；通过排序，可以方便得获得占用 CPU 资源较多的进程，进行进一步的分析。

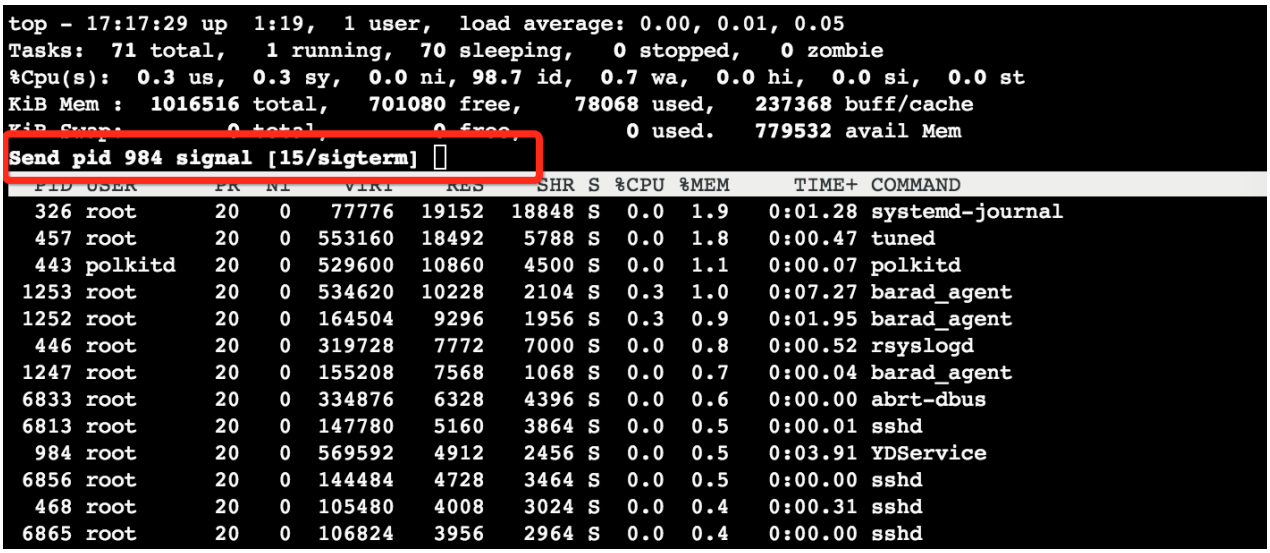
```
top - 22:16:25 up  6:18,  1 user,  load average: 0.00, 0.01, 0.05
Tasks:  68 total,   1 running,  67 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.3 sy,  0.0 ni, 99.7 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  1016516 total,   605016 free,    77224 used,   334276 buff/cache
KiB Swap: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

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

4. 分析占用 CPU 高的进程。

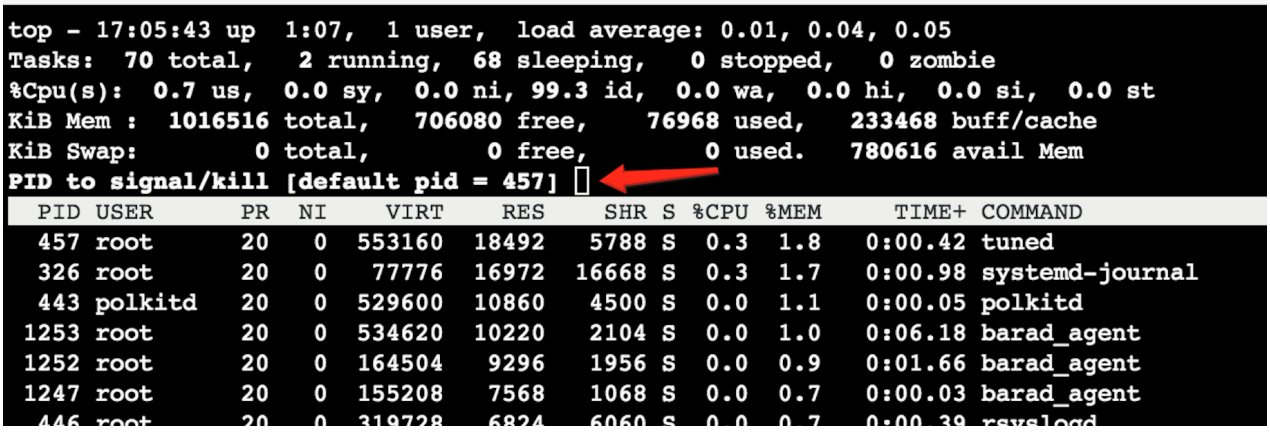
   1. 如果为业务进程，建议分析业务程序是否有优化空间，进行优化或者提升实例的资源配置。
   2. 如果为异常进程，实例可能中毒，可以自行终止进程、使用安全软件进行查杀或者进行数据备份后，重装系统。
   3. 如果为腾讯云组件进程，占用 CPU 超过 20%，请 发起工单 联系我们进行进一步定位处理。
      常见的腾讯云组件有：
      sap00x：安全组件进程
      Barad_agent：监控组件进程
      secu-tcs-agent：安全组件进程

使用 top 命令结束进程

1. 键入小写 k，输入想要结束进程的 pid（默认为排序第一的进程），回车。



2. 操作成功，界面会出现 Send pid 984 signal [15/sigterm] 的提示信息，回车确认即可。



kswapd0 进程占用 CPU 较高的处理

kswapd0 是 Linux 系统虚拟内存管理中负责换页的进程。Linux
系统通过分页机制管理内存的同时，将磁盘的一部分划出来作为虚拟内存。当系统内存不足时，kswapd0
会频繁的进行换页操作。换页操作非常消耗 CPU 资源，导致该进程持续占用高 CPU 资源。
如果使用 top 命令，看到 kswapd0 进程持续占用大量 CPU 资源，可以进一步使用
vmstat，查看系统的虚拟内存的情况，如果 si，so
也比较高，证明系统存在频繁的换页操作，当前的系统物理内存已经不能满足需要，考虑升级系统的内存。

带宽利用率过高问题处理

当发现实例带宽利用率过高时，往往希望能够具体定位出是哪一个进程占用了带宽，进而进行相应的分析处理。本文将介绍 Linux 和 Windows 系统下如何使用对应的工具进行定位处带宽使用高的进程。

Linux下查看进程的带宽使用情况

NetHogs 介绍

NetHogs 是 Linux 平台下的一个开源命令行工具，用来实时统计各进程的带宽使用情况。在 CentOS 下可以使用如下命令进行安装：

yum install nethogs

NetHogs 使用方法

终端输入以下命令可以看到 NetHogs 的可用参数以及具体用法。

nethogs -h

```
[root@VM_2_184_centos ~]# nethogs -h
usage: nethogs [-V] [-h] [-b] [-d seconds] [-v mode] [-c count] [-t] [-p] [-s] [device [device [device ...]]]
                -V : prints version.
                -h : prints this help.
                -b : bughunt mode - implies tracemode.
                -d : delay for update refresh rate in seconds. default is 1.
                -v : view mode (0 = KB/s, 1 = total KB, 2 = total B, 3 = total MB). default is 0.
                -c : number of updates. default is 0 (unlimited).
                -t : tracemode.
                -p : sniff in promiscious mode (not recommended).
                -s : sort output by sent column.
   -a : monitor all devices, even loopback/stopped ones.
                device : device(s) to monitor. default is all interfaces up and running excluding loopback

When nethogs is running, press:
 q: quit
 s: sort by SENT traffic
 r: sort by RECEIVE traffic
 m: switch between total (KB, B, MB) and KB/s mode
```

- -d：设置刷新的时间间隔，默认为 1s。
- -t：跟踪模式。

- -c：更新次数。
- device：设置要监控的网卡，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。
- s：按发送流量进行排序。
- r：按接收流量进行排序。
- m：切换是显示各进程使用的网络速率亦或是使用的流量，或者使用流量的计量单位。切换顺序为 KB/s > KB > B > MB。

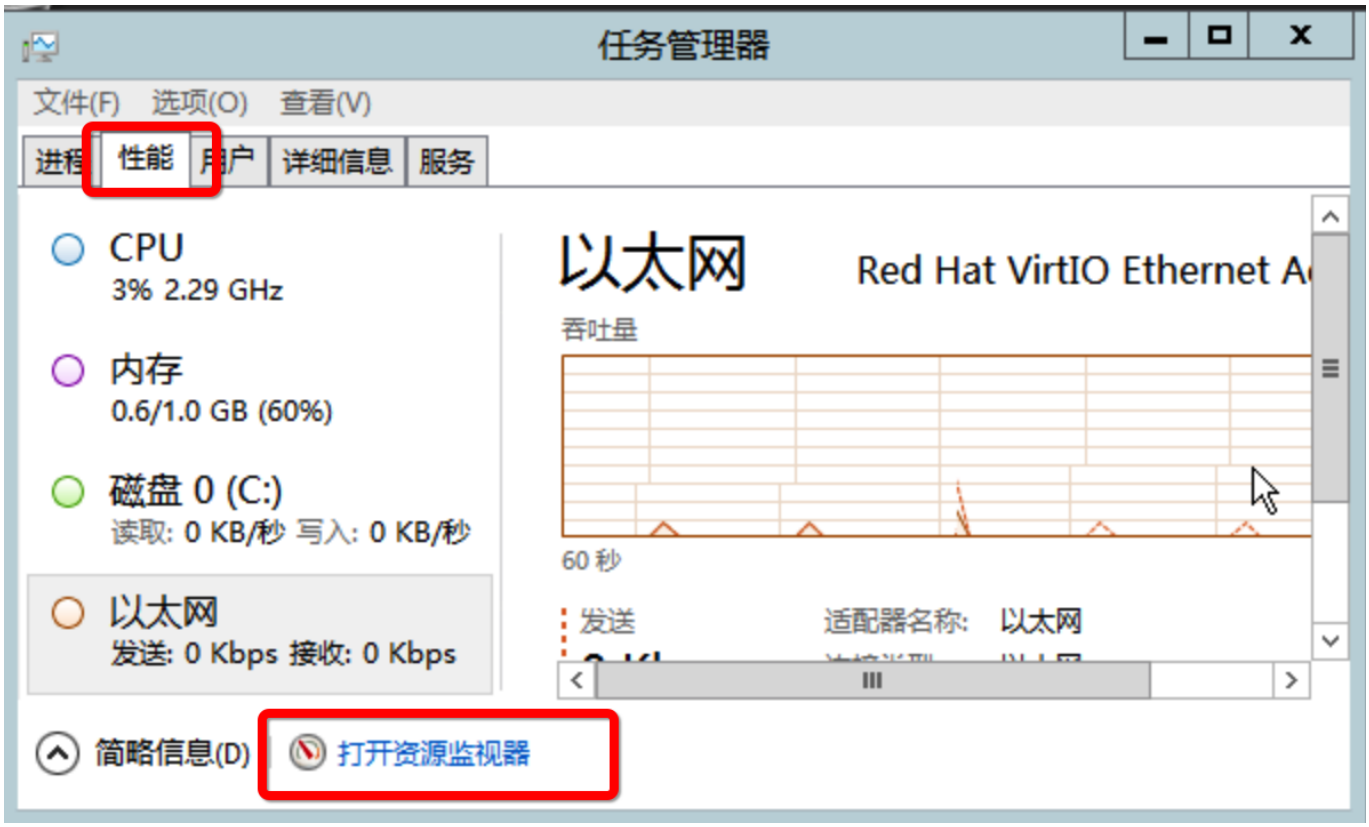
下图展示了在 Linux 实例上运行 nethogs -d 10 并按发送数据量进行排序的结果，以此为示例，介绍 NetHogs 的输出。通过切换按发送/接收流量排序，可以很方便的获取占用发送/接收流量较多的进程。

PID：进程 ID。
USER：运行该进程的用户。
PROGRAM：程序名或IP端口号。
DEV：流量要去往的网络接口。
SENT：进程每秒发送的数据量。
RECEIVED：进程每秒接收的数据量。

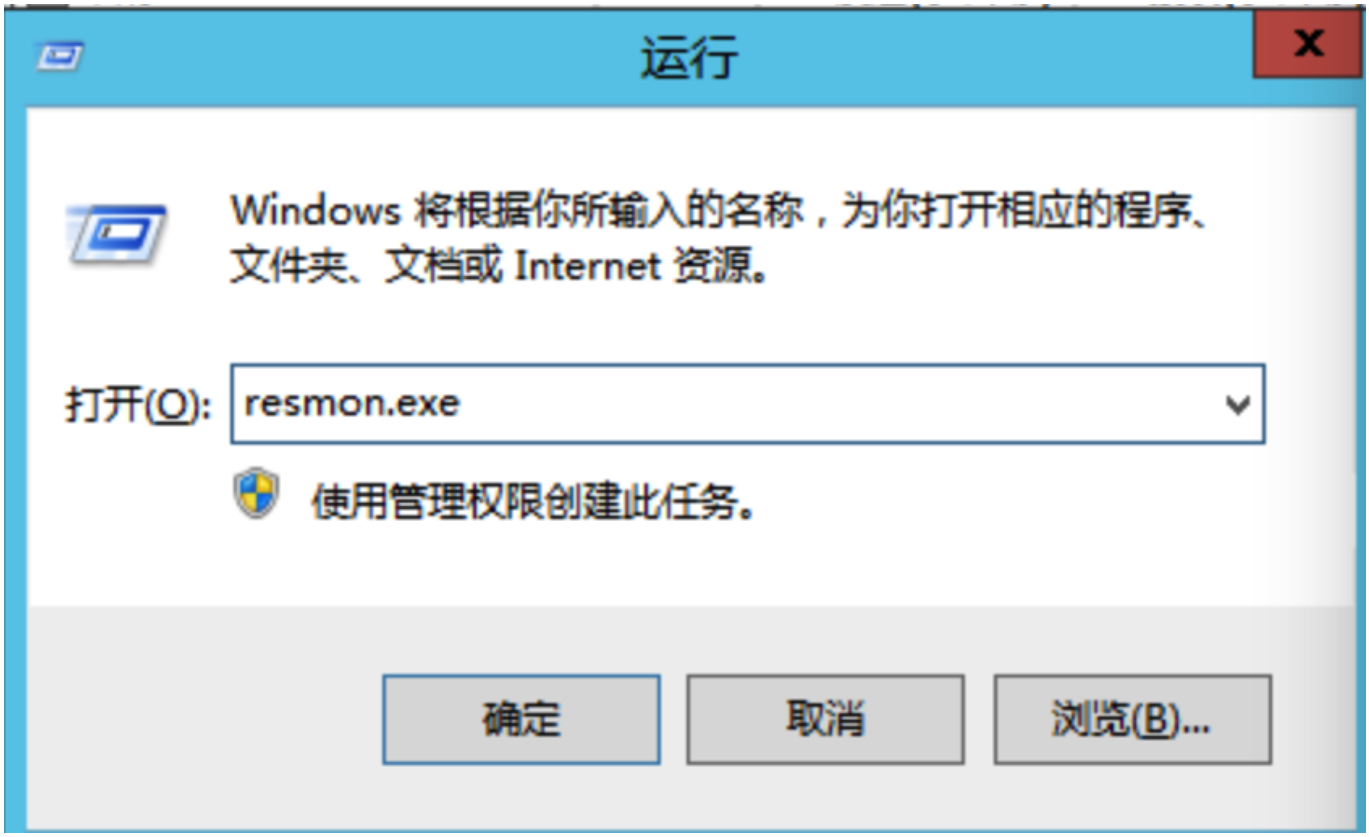
Windows下查看进程的带宽使用情况

Windows 资源监视器

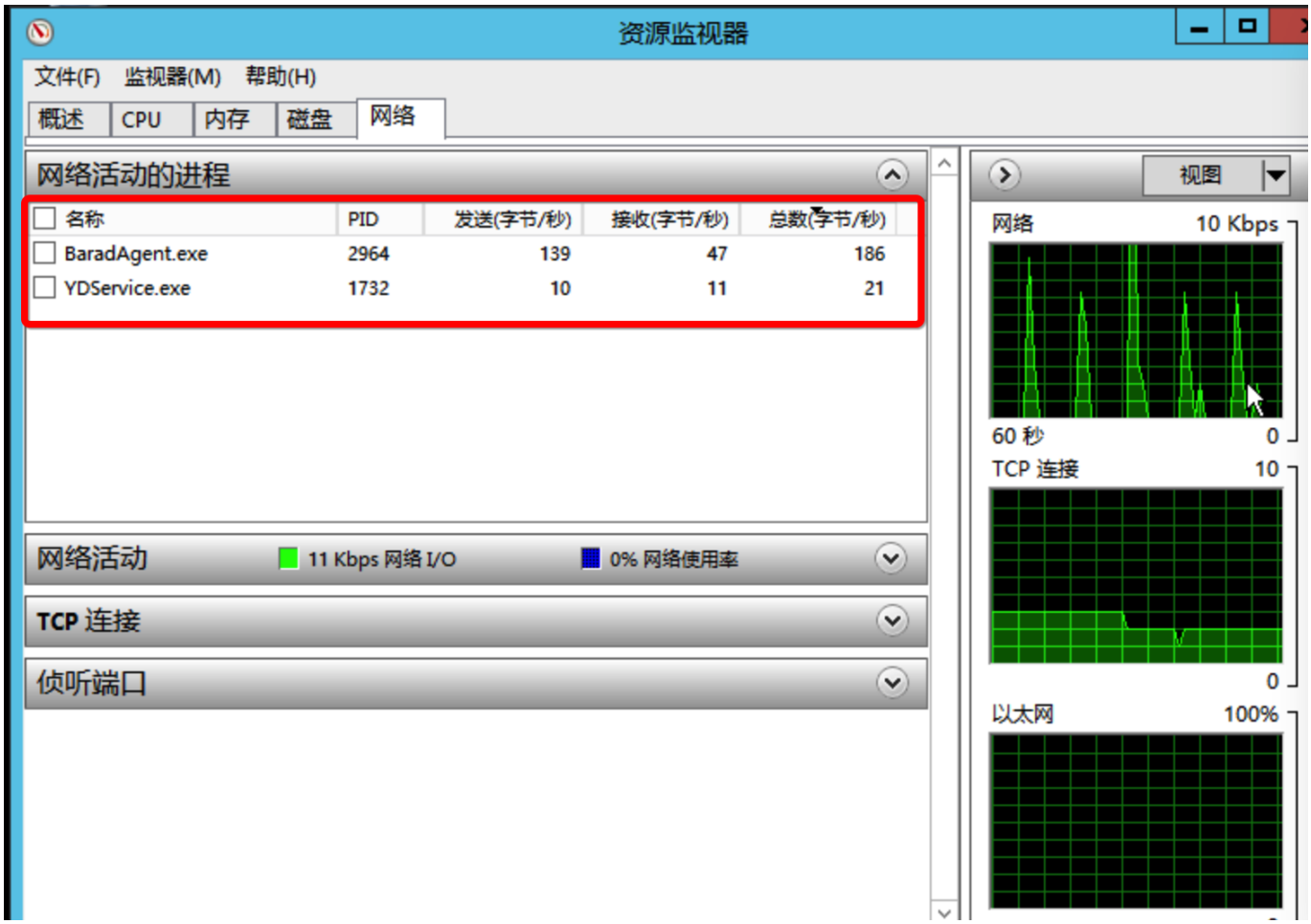
资源监视器是 Windows下以进程为单位了解 CPU、内存、磁盘、网络等资源的使用情况的工具。
可以在任务管理器，性能 tab 点击打开资源监视器打开。



或者在运行中输入 resmon.exe，确定打开



点击资源监视器的网络 tab，就可以看到每个进程的带宽使用情况。点击发送，按发送数据量进行排序，点击接收按照接收数据量进行排序。排序后，可以方便的看到具体是哪个进程占用了网络资源。



结果分析及处理

知道占用资源较多的进程后，需要分析进程所属的类型，然后进行：

1. 分析是否正常进程（系统进程/业务进程/腾讯云的常见进程）起。如果无法完全确认，建议使用进程名进程搜索确认。

2. 如果是异常进程，实例可能中毒，可以自行终止进程、使用安全软件进行查杀或者进行数据备份后，重装系统。

3. 如果为腾讯云组件进程，请 发起工单 联系我们进行进一步定位处理。
   常见的腾讯云组件有：

   - sap00x：安全组件进程
   - Barad_agent：监控组件进程

- secu-tcs-agent：安全组件进程

4. 正常的业务进程，分析是否有大量的网络访问行为，是否通过压缩文件解决网络带宽的资源瓶颈。否则建议升级实例配置。带宽配置升级详情见 变更配置。

网络与 DNS 相关

网站无法访问问题处理

网络问题、防火墙设置、服务器负载过高等都可能导致网站无法访问的问题。本文将介绍网站无法访问的问题如何一步步进行排查定位。

一. 服务器原因排查

服务器关机、硬件故障、CPU/内存/带宽使用率过高都可能造成网站无法访问，因此建议依次排查服务器的运行状态、CPU/内存/带宽的使用情况。

1. 查看服务器运行状态。登陆腾讯云的控制台，查看实例的运行情况，确认实例正常运行。如果状态非运行中，建议进行重启等相应处理。

2. 查看资源使用情况。在实例的详情页，点击监控 tab 查看CPU/内存/带宽的使用情况。如果存在 CPU 使用过高的情况，请参考 CPU 使用率过高排查（Windows 系统）和 CPU 使用率过高排查（Linux 系统）进行定位；带宽使用过高的情况，参考 带宽利用率过高问题处理。

3. 检查 Web 服务相应的端口是否被正常监听。下面以 http 服务常用的 80 端口为例，介绍 Linux 和 Windows 系统下应该如何检查：

   - Linux 系统

     使用 netstat 查看 80 端口的监听情况，具体命令如下所示，-t 显示 tcp 端口，-p 显示进程标识符和对应的程序名，-l 显示监听套接字。

```
[root@VM_2_184_centos ~]# netstat -ntulp |grep 80
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      1309/httpd
```

   - Windows 系统

     使用 netstat -ano|findstr :80 查看 80 端口的监听情况。根据进程 id 可以查看正在监听的进程名。

```
C:\Users\Administrator>netstat -ano|findstr :80
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    10.135.182.70:53406    10.225.30.181:80       TIME_WAIT       0
  TCP    10.135.182.70:53419    10.225.30.181:80       TIME_WAIT       0
  TCP    10.135.182.70:53423    10.225.30.181:80       TIME_WAIT       0
  TCP    [::]:80                [::]:0                 LISTENING       4
```

如果端口没有被正常监听，请检查 Web 服务进程是否启动或者正常配置。

4. 检查防火墙设置，是否放行 Web 服务进程对应的端口。

   Linux 查看 iptables 是否放行 80 端口，Windows 系统则检查 Windows 防火墙设置。

二. 网络问题

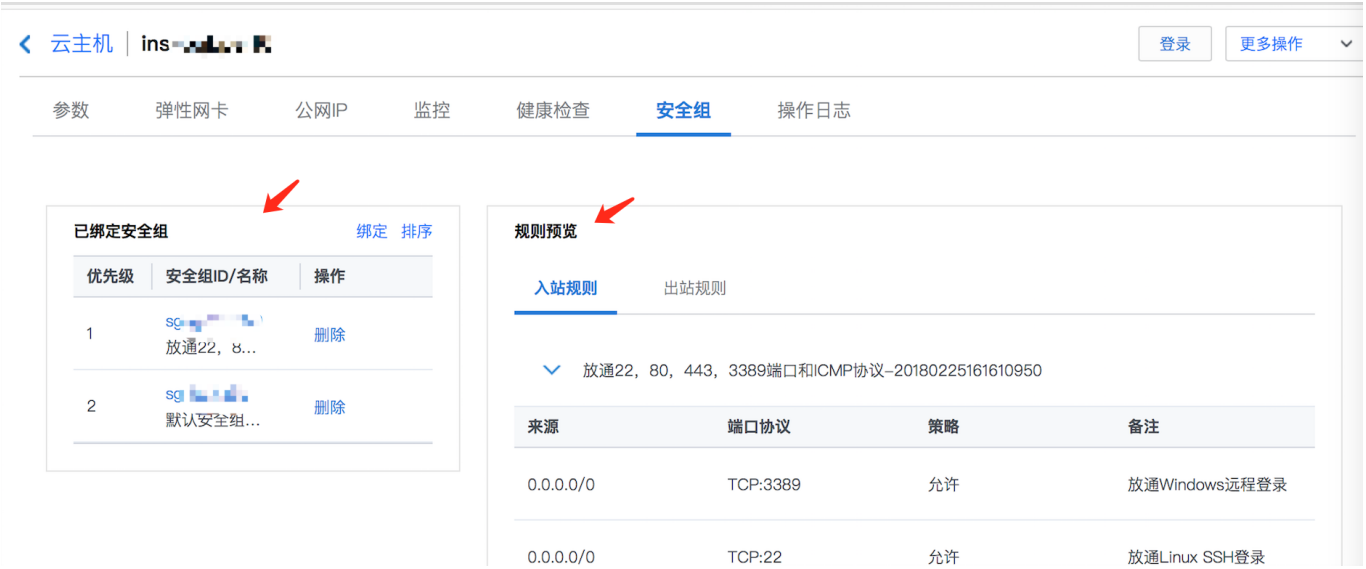
排除了服务器问题后，网站无法访问还可能是网络问题引起，这里可以使用 ping 命令 ping 目的服务器的公网 IP，确认是否有丢包或延时高的情况。如果存在，使用 MTR 进一步进行排查。具体请参考[服务器网络延迟和丢包处理](#)。

```
[redacted]MB0:~ chenhuiping$ ping 193.112.12.138
[redacted].12.138 (193.112.12.138): 56 data bytes
64 bytes from 193.112.12.138: icmp_seq=0 ttl=43 time=161.240 ms
64 bytes from 193.112.12.138: icmp_seq=1 ttl=43 time=161.996 ms
64 bytes from 193.112.12.138: icmp_seq=2 ttl=43 time=164.837 ms
64 bytes from 193.112.12.138: icmp_seq=3 ttl=43 time=215.650 ms
64 bytes from 193.112.12.138: icmp_seq=4 ttl=43 time=166.375 ms
64 bytes from 193.112.12.138: icmp_seq=5 ttl=43 time=160.576 ms
64 bytes from 193.112.12.138: icmp_seq=6 ttl=43 time=161.016 ms
64 bytes from 193.112.12.138: icmp_seq=7 ttl=43 time=164.129 ms
64 bytes from 193.112.12.138: icmp_seq=8 ttl=43 time=192.682 ms
64 bytes from 193.112.12.138: icmp_seq=9 ttl=43 time=163.376 ms
64 bytes from 193.112.12.138: icmp_seq=10 ttl=43 time=161.859 ms
^C
--- 193.112.12.138 ping statistics ---
11 packets transmitted, 11 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 160.576/170.340/215.650/16.765 ms
```

三. 安全组设置

安全组是一个虚拟防火墙，可以控制关联实例的入站流量和出战流量。安全组的规则可以指定协议、端口、策略等等。没有放通Web进程相关的端口也会造成网站无法访问。排除了服务器和网络问题后，需要对实例所属的安全组的规则进行检查。

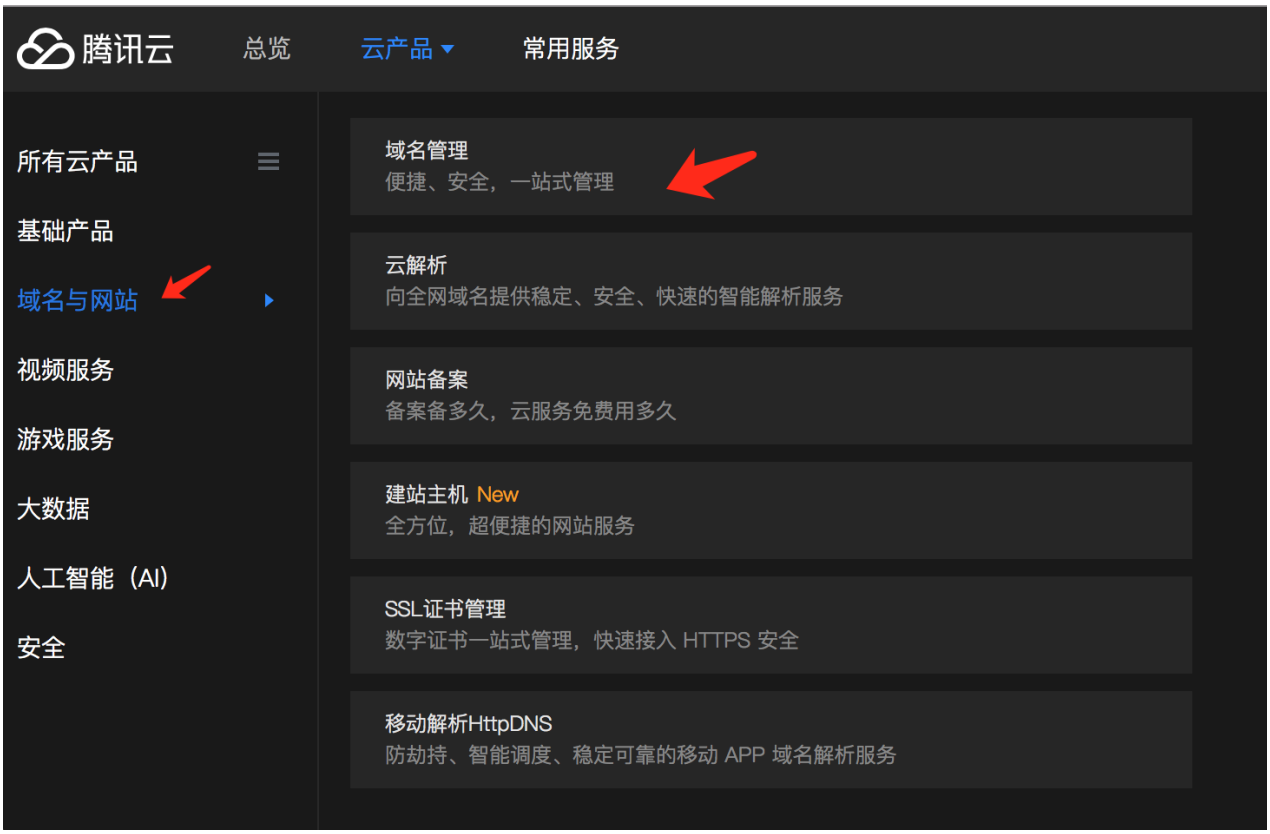
可以在实例的详情页安全组tab查看实例使用的安全组以及对应安全组具体的处长以及入站规则，确认是否放通Web进程相关的端口。如果没有放通相应的端口，请编辑绑定的安全规则，进行放通。



四. 域名备案解析问题

排除了上述三个问题后，可以尝试使用服务器公网 IP 进行访问。如果使用 IP 可以访问，而域名访问失败，则可能是域名备案或者解析的问题。

1. 国家工信部规定，对未取得许可或者未履行备案手续的网站不得从事互联网信息服务，否则就属于违法行为。为不影响网站长久正常运行，想要开办网站建议先办理网站备案，备案成功取得通信管理局下发的 ICP 备案号后才能开通访问。如果您的域名没有备案，则需先进行 域名备案。
   如果使用的是腾讯云的域名服务，可以在 控制台 > 域名与网站 > 域名管理 查看相应的域名情况。



2. 域名解析没有正确配置，导致请求没有路由到对应的 Web

服务器也会导致网站无法访问。如果您使用的是腾讯云的域名服务，可以控在 控制台 > 域名与网站 > 域名管理 ，点击对应域名的解析按钮，查看域名解析详情。

访问 CVM 实例运行的网站卡慢问题定位

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、最后对页面进行渲染呈现。这其中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，这三个环节中的任意一个出现问题，都有可能导致网站访问卡慢。

一. 本地客户端问题确认

本地客户端访问播测网站（ping.huatuo.qq.com），测试本地访问各域名的速度，确认本地网络是否存在问题。测试结果如下图，从结果中可以获知访问各个域名的延迟，以及网络是否正常。如果不正常请联系您的网络服务提供上进行协助定位解决。

以下是腾讯公司域名的测试结果	
inews.qq.com	网络正常,延迟194毫秒
www.qq.com	网络正常,延迟128毫秒
3g.qq.com	网络正常,延迟140毫秒
mail.qq.com	网络正常,延迟99毫秒
user.qzone.qq.com	网络正常,延迟98毫秒
r.qzone.qq.com	网络正常,延迟203毫秒
w.qzone.qq.com	网络正常,延迟188毫秒
ptlogin2.qq.com	网络正常,延迟96毫秒
check.ptlogin2.qq.com	网络正常,延迟189毫秒
ui.ptlogin2.qq.com	网络正常,延迟91毫秒
i.mail.qq.com	网络正常,延迟129毫秒
v.qq.com	网络正常,延迟129毫秒

以下是其他域名的测试结果	
c.3g.163.com	网络正常,延迟143毫秒
weibo.com	网络正常,延迟211毫秒
www.baidu.com	网络正常,延迟94毫秒
www.sina.com.cn	网络正常,延迟138毫秒
www.taobao.com	网络正常,延迟136毫秒

二. 网络链路问题确认

若第一步确认没有异常，请进一步确认本地客户端到服务器之前网络是否有问题。

1. 本地客户端 ping 服务器公网 IP，确认是否存在丢包或延时高的情况。
2. 若存在丢包或时延高的情况，进一步使用 MTR 进行诊断。具体参考 服务器网络延迟和丢包处理。
3. 若 ping 服务器 IP 无异常，可以使用 dig/nslookup 查看 DNS 的解析情况，排查是否 DNS 解析引起的问题。也可以通过直接使用 IP 访问对应页面，排查是否 DNS 的问题导致访问慢。

三. 服务器问题确认

如果客户端和网络链路都没有问题，进一步对 Web 服务器进行分析。是否系统资源不足、中病毒木马或者被 DDoS 攻击了。

1. 登录 云服务器控制台 ，在云主机详情页，单击 tab【监控】，可以查看实例资源使用情况。

2. 若 CPU/内存/带宽/磁盘使用率过高，可能是服务器自身负载较高或者中毒等问题导致，请参考对应的文档进行排查：
    - CPU 使用率过高排查（Linux 系统）
    - CPU 使用率过高排查（Windows 系统）
    - 带宽利用率过高问题处理

四. 业务问题确认

1. 若通过第三步定位到是服务器负载引起的资源消耗增大，则属于正常情况。可以通过优化业务程序，或升级现有的服务器配置或购买新的服务器分担现有服务器的压力解决。
2. 若上述三步都正常，则建议查看日志文件，定位具体是哪一步导致服务器响应慢，进行针对性的优化。

服务器网络延迟和丢包处理

本地访问云服务器或云服务器访问其他网络资源卡顿，Ping 发现存在丢包或时延较高，可能是骨干链路拥塞、链路节点故障、服务器负载高，系统设置问题等原因引起。在排除云服务器自身原因后，可以使用 MTR 进行进一步诊断。

MTR 是一款强大的网络诊断工具，其报告可以帮助确认网络问题的症结所在。下面将详细介绍 Linux 和 Windows 系统下 MTR 的使用方法以及如何对报告结果进行分析，其余操作系统请自行搜索。

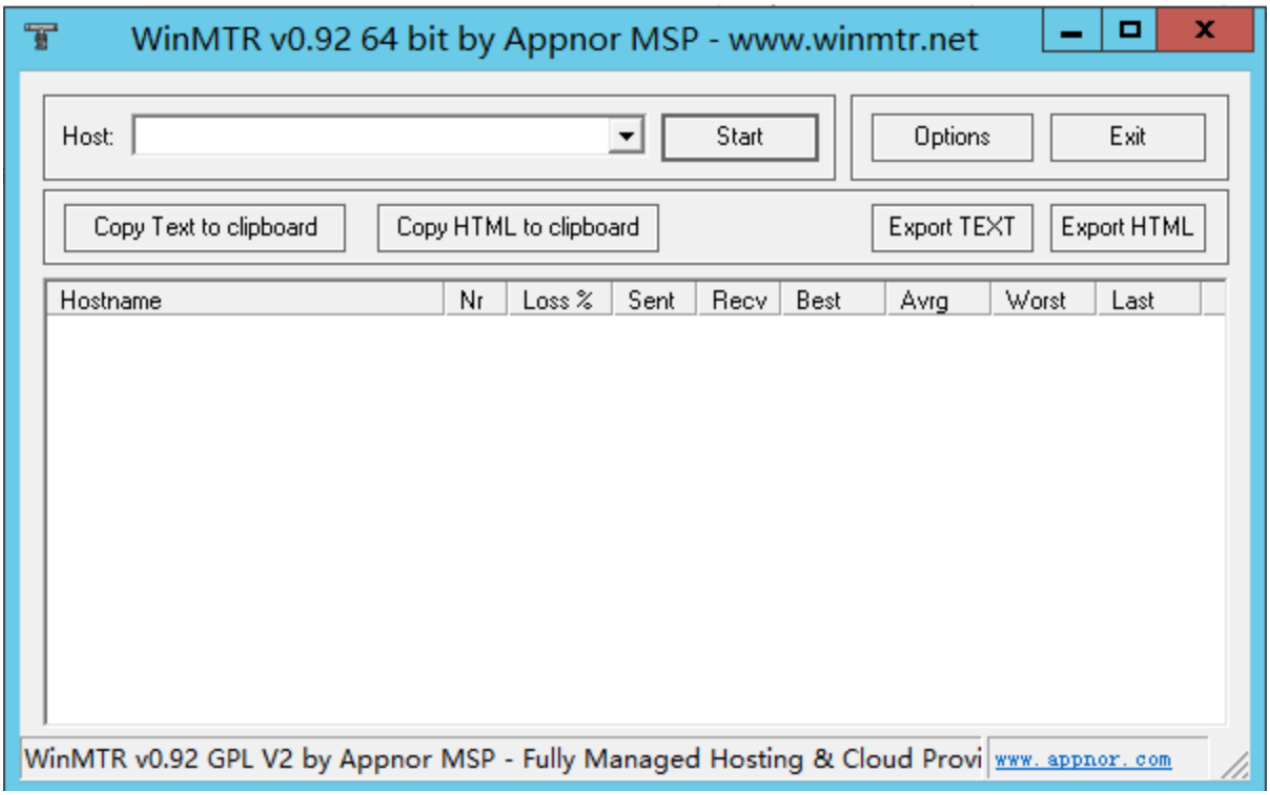
在文章中，运行 MTR 的主机称为源主机，被查询的称为目的主机，可以针对源主机的操作系统查看相关的章节。

WinMTR 介绍和使用方法（Windows）

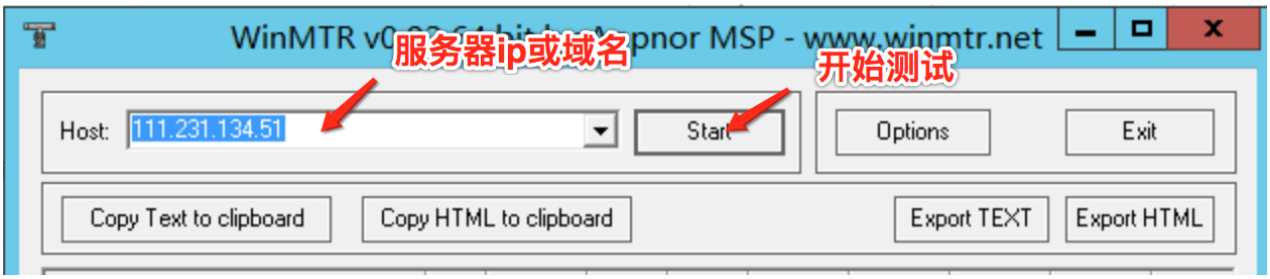
WinMTR：适用于 Windows 系统的免费网络诊断工具（官方下载地址），集成了 Ping 和 tracert 的功能，具有图形界面，可以直观地看到各个节点的响应时间和丢包情况。

WinMTR 的安装和使用

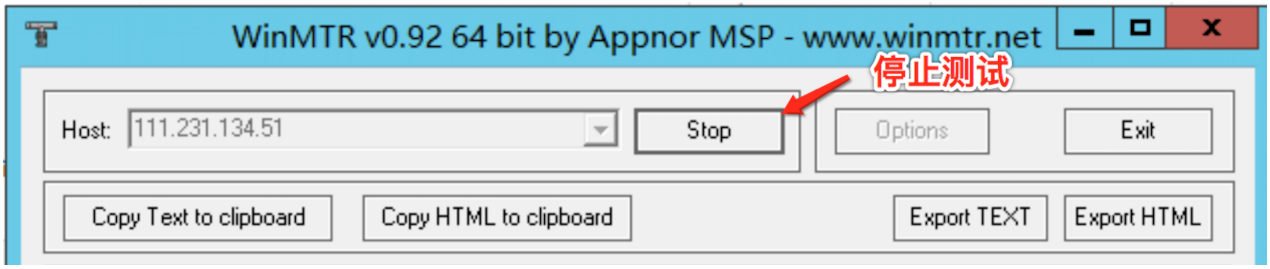
1. 根据操作系统类型下载对应的安装包，解压，双击运行其中 WinMTR.exe，界面如下图。



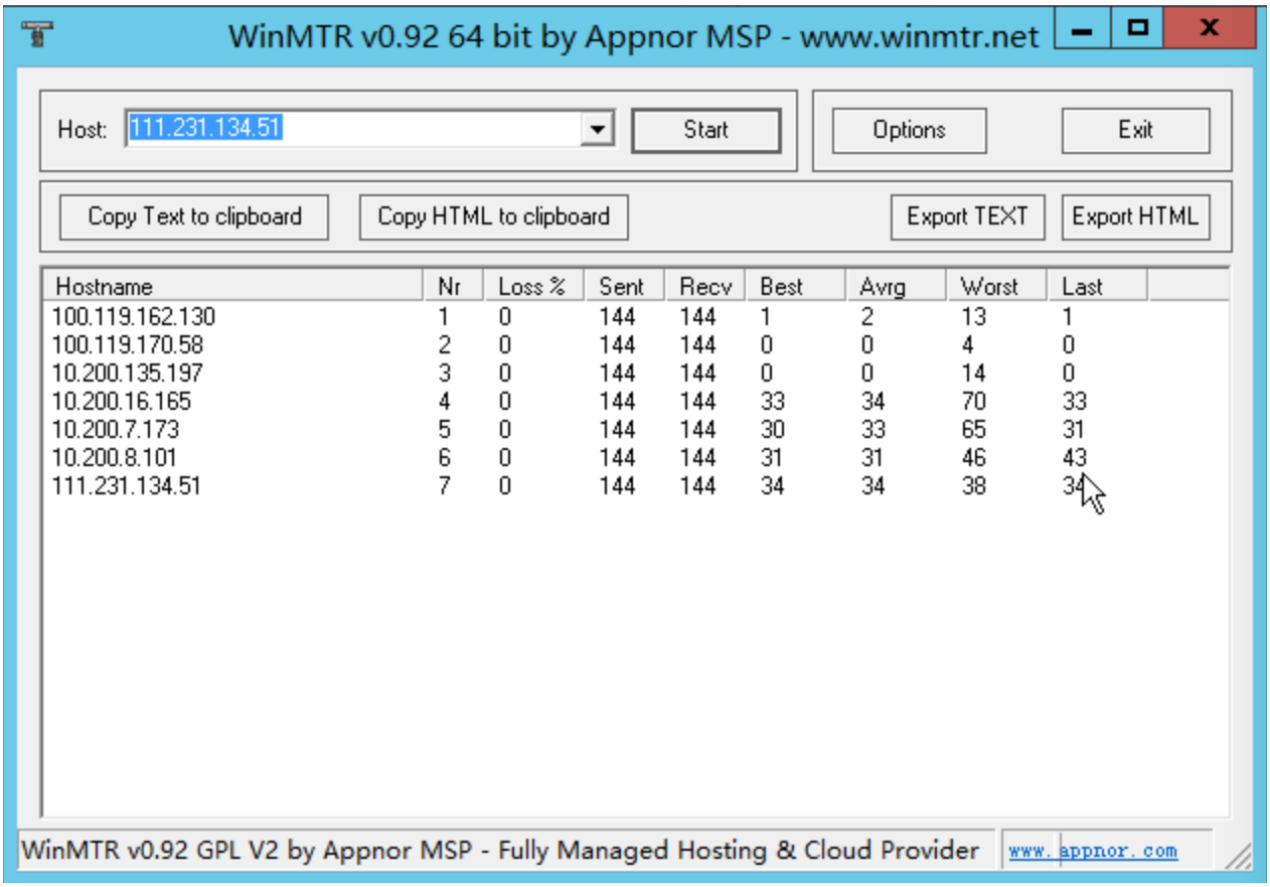
2. 在 Host 处输入目的服务器 IP 或域名，然后单击 Start，进行测试。



3. 运行一段时间后，点击 Stop 结束测试。



4. 查看测试结果。



结果各项数据简介：

Hostname：到目的服务器要经过的每个主机 IP 或名称。

Nr：经过节点的数量。

Loss%：对应节点的丢包率。

Sent：发送的数据包数量。

Recv：接收到响应的数量。

Best：最短的响应时间。
Avrg：平均响应时间。
Worst：最长的响应时间。
Last：最近一次的响应时间。

MTR 介绍和使用方法（Linux）

MTR：Linux 平台上诊断网络状态的工具，继承了 Ping、traceoute、nslookup 的功能，默认使用 ICMP 包测试两个节点之前的网络连接情况。

MTR 安装

几乎所有的 Linux 发行版本都预装了 MTR，如果没有可以通过以下命令进行安装：

- CentOS：

  yum install mtr

- Ubuntu：

  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：跟 --report 相对，每次追踪的结果分别列出来。
-c/--report-cycles：设置每秒发送的数据包数量，默认是 10。
-s/--psize：设置数据包的大小。
-n/--no-dns：不对 IP 地址做域名解析。

-a/--address：用户设置发送数据包的 IP 地址，主要用户单一主机多个 IP 地址的场景。

-4：IPv4。

-6：IPv6。

下面是一份从本机到服务器（119.28.98.39）的 MTR 报告，以此为示例，对返回结果进行说明。

```
[root@VM_103_80_centos ~]# mtr  119.28.98.39 --report
Start: Mon Feb  5 11:33:34 2018
HOST: VM_103_80_centos            Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- 100.119.162.130            0.0%    10    6.5   8.4   4.6  13.7   2.9
  2.|-- 100.119.170.58             0.0%    10    0.8   0.8   0.6   1.1   0.0
  3.|-- 10.200.135.213             0.0%    10    0.4   0.6   0.4   2.5   0.6
  4.|-- 10.200.16.173              0.0%    10    1.6   1.5   1.4   1.6   0.0
  5.|-- 14.18.199.58               0.0%    10    1.0   1.3   1.0   4.1   0.9
  6.|-- 14.18.199.25               0.0%    10    4.1   4.7   3.3  10.2   1.9
  7.|-- 113.96.7.214               0.0%    10    5.8   7.3   3.1  10.1   2.1
  8.|-- 113.96.0.106               0.0%    10    3.9   7.8   3.9  11.0   2.5
  9.|-- 202.97.90.206             30.0%    10    2.4   2.4   2.4   2.5   0.0
 10.|-- 202.97.94.77               0.0%    10    3.5   4.8   3.5   7.0   1.2
 11.|-- 202.97.51.142              0.0%    10  164.7 163.4 161.3 165.3   1.2
 12.|-- 202.97.49.106              0.0%    10  162.3 164.9 161.7 167.8   2.0
 13.|-- ix-xe-10-2-6-0.tcore2.LVW 10.0%    10  168.4 167.9 161.5 168.9   2.3
 14.|-- 180.87.15.25              10.0%    10  348.1 348.3 347.7 350.2   0.7
 15.|-- 180.87.96.21               0.0%    10  345.0 343.9 343.4 345.0   0.3
 16.|-- 180.87.96.142              0.0%    10  187.4 187.5 187.3 187.6   0.0
 17.|-- ???                      100.0    10    0.0   0.0   0.0   0.0   0.0
 18.|-- 100.78.119.231             0.0%    10  187.7 190.2 187.3 194.0   2.5
 19.|-- 119.28.98.39               0.0%    10  186.5 186.5 186.4 186.5   0.0
```

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。

报告结果分析及处理

上面已经介绍了不同操作系统下，网络诊断工具的使用。下面介绍如何对报告进行分析。

由于网络状况的非对称性，遇到本地到服务器的网络问题时，建议收集双向的 MTR 数据(从本地到云服务器以及云服务器到本地)。

MTR 结果分析步骤

1. 查看目的地 IP 是否丢包，目的地没有丢包基本证明网络正常。中间节点丢包可能是链路节点的 ICMP 限制或其他策略引起，但事实上并未丢包。因此查看 WinMTR/MTR 的结果时，首先查看最后的目的地是否有丢包，如果没有丢包，这证明网络没有问题。
2. 目的地发生丢包，这继续往上看，定位出第一次丢包的节点。
3. 如果丢包发生在目的服务器，则可能是目的服务器网络配置不当引起，请检查目的服务器的防火墙配置。

   如果丢包开始于前三跳，一般为本地运营商网络问题，建议检查访问其他网址是否存在相同情况，存在则反馈给您的运营商进行处理。相反如果丢包发生在接近目的服务器的几跳，则可能为目的服务器运营商的网络问题，请 提交工单 进行反馈处理，工单上请附上本地到目的服务器，以及目的服务器到本地的 MTR 测试截图，以便工程师进行定位。

ping 不通问题定位指引

本地主机 ping 不通实例可能由于目标服务器的设置不正确、域名没有正确解析、链路故障等等问题引起。在确保本地网络正常（可以正常 ping 通其他网站）的前提下，下文将就如何进行排查进行详细的说明：

一. 确认实例是否有公网 IP

实例必须具备公网 IP 才能跟 Internet 上的其他计算机相互访问。实例没有公网 IP，内网 IP 外部是无法直接 ping 通的。可以在 控制台实例详情页 查看公网 IP 的信息，如下图。如无公网 IP 可以绑定弹性公网 IP。

二. 安全组设置确认

安全组是一个虚拟防火墙，可以控制关联实例的入站流量和出站流量。安全组的规则可以指定协议、端口、策略等等。由于 ping 使用的是 ICMP 协议，这里要注意实例关联的安全组是否允许 ICMP。实例使用的安全组以及详细的入站和出站规则可以在实例详情页的安全组 tab 查看。

三. 系统设置检查

Linux 内核参数和防火墙设置检查

Linux 系统是否允许 ping 由内核和防火墙设置两个共同决定，任何一个禁止，都会造成 ping 包“Request timeout”。

内核参数icmp_echo_ignore_all

icmp_echo_ignore_all 代表系统是否忽略所有的 ICMP Echo 请求，1 禁止，0允许。使用如下指令查看系统 icmp_echo_ignore_all 设置。

cat /proc/sys/net/ipv4/icmp_echo_ignore_all

```
[root@VM_103_80_centos ~]# cat /proc/sys/net/ipv4/icmp_echo_ignore_all
0
```

echo "1" >/proc/sys/net/ipv4/icmp_echo_ignore_all

```
[root@VM_103_80_centos ~]# echo "1" >/proc/sys/net/ipv4/icmp_echo_ignore_all
```

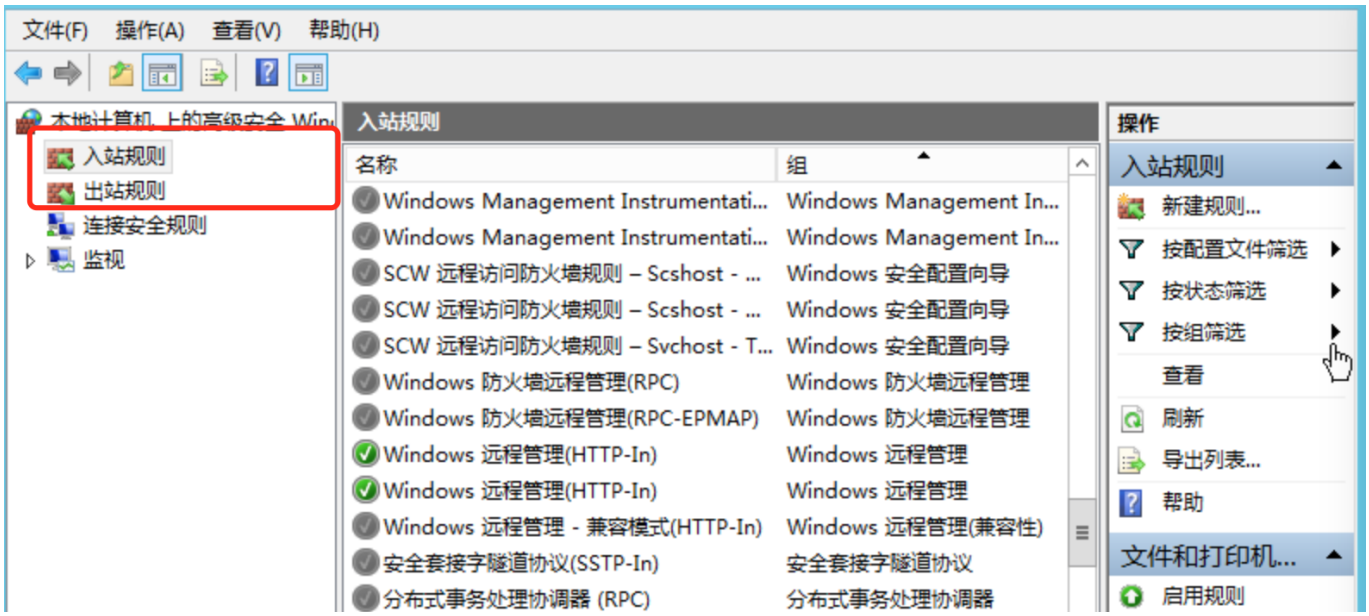
防火墙设置

使用 iptables -L 查看当前服务器的防火墙规则，查看 ICMP 对应规则，看是否被禁止。

```
[root@VM_103_80_centos ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
[root@VM_103_80_centos ~]# iptables -F
```

Windows 防火墙设置

控制面板 > Windows 防火墙设置 > 高级设置 > 查看 ICMP 有关的出入站规则，是否被禁止。



四. 域名是否备案

如果是可以 ping 通公网 IP，而域名 ping 不通，此时可能是域名没有备案，或者域名解析的问题。

国家工信部规定，对未取得许可或者未履行备案手续的网站不得从事互联网信息服务，否则就属于违法行为。

为不影响网站长久正常运行，想要开办网站建议先办理网站备案，备案成功取得通信管理局下发的 ICP 备案号后才能开通访问。如果您的域名没有备案，则需先进行域名备案。

如果使用的是腾讯云的域名服务，可以在 控制台 > 域名与网站 > 域名管理 查看相应的域名情况。

五. 域名解析

域名 ping 不通的另外一个原因是域名解析没有正确地配置。如果用户使用的是腾讯云的域名服务可以在控制台 > 域名与网站 > 域名管理，点击对应域名的解析按钮，查看域名解析详情。

若上述步骤无法解决问题，请参考：

- 域名 ping 不通，请检查您网站配置。
- 公网 IP ping 不通，请附上实例的相关信息和双向 MTR 数据（从本地到云服务器以及云服务器到本地），提交工单 联系工程师协助定位。MTR 的使用方法请参考 服务器网络延迟和丢包处理。

大数据型 D1 实例常见问题

什么是大数据型 D1 实例？

大数据型 D1 实例是专为 Hadoop 分布式计算、海量日志处理、分布式文件系统和大型数据仓库等业务场景设计的云服务器实例，主要解决大数据时代下海量业务数据云上计算和存储难题。

大数据型 D1 实例适用于哪些行业客户和业务场景？

适用于互联网行业、游戏行业、金融行业等有大数据计算与存储分析需求的行业客户，进行海量数据存储和离线计算的业务场景，充分满足以 Hadoop
为代表的分布式计算业务类型对实例存储性能、容量和内网带宽的多方面要求。
同时，结合以 Hadoop 为代表的分布式计算业务的高可用架构设计，大数据型 D1
实例采用本地存储的设计，在保证海量存储空间、高存储性能的前提下，实现与线下 IDC 自建 Hadoop 集群相近的总拥有成本。

大数据型 D1 实例的产品特点

- 单实例高达 2.3 GB/s 吞吐能力。吞吐密集型 HDD 本地盘是吞吐密集型最优选，专为 Hadoop 分布式计算、海量日志处理和大型数据仓库等业务场景设计，提供稳定的高顺序读写吞吐能力。
- 本地存储单价低至 1/10，大数据场景最优性价比，在保证海量存储空间、高存储性能的前提下，与 IDC 自建 Hadoop 集群拥有相近的总成本。
- 低至 2-5 ms 读写延时，高性能企业级机型，面向成熟的企业开发者定义的机型。
- 支持『包年包月』和『按量付费』两种计费模式，低至4.17元/小时。

大数据型 D1 实例规格

机型	vCPU（核）	内存（GB）	本地数据盘	内网带宽	备注
D1.2XLARGE32	8	32	2 × 3720 GB	1.5 Gbps	-
D1.4XLARGE64	16	64	4× 3720 GB	3 Gbps	-
D1.6XLARGE96	24	96	6× 3720 GB	4.5 Gbps	-
D1.8XLARGE128	32	128	8× 3720 GB	6 Gbps	-
D1.14XLARGE22	56	224	12× 3720 GB	10 Gbps	宿主机机专享独占

机型	vCPU（核）	内存（GB）	本地数据盘	内网带宽	备注
4					

大数据型 D1 本地数据存储的注意事项

大数据型 D1
实例的数据盘是本地硬盘，有丢失数据的风险
（比如宿主机宕机时），如果您的应用不能做到数据可靠性的架构，我们强烈建议您使用可以选择云硬盘作为数据盘的实例。

操作带本地硬盘的实例和数据保留关系如下表所示。

操作	本地硬盘数据状态	说明
操作系统重启/控制台重启/强制重启	保留	本地硬盘存储保留，数据保留。
操作系统关机/控制台关机/强制关机	保留	本地硬盘存储保留，数据保留。
控制台上销毁（实例）	擦除	本地硬盘存储擦除，数据不保留。

注意：
请勿在本地硬盘上存储需要长期保存的业务数据，并及时做好数据备份和采用高可用架构。如需长期保存，建议将数据存储在云硬盘上。

如何购买大数据型 D1 本地硬盘？

不能单独购买本地硬盘，只能在创建 D1
实例时同时购买本地硬盘。本地硬盘的数量和容量由选择的实例规格决定。

大数据型 D1 实例本机存储是否支持快照？

不支持。

大数据型 D1 实例是否支持升降配置和故障迁移？

不支持调整配置。

大数据型 D1 实例目前数据盘是基于本地HDD硬盘的海量数据存储型实例，目前不支持数据盘故障后的迁移（如宿主机宕机、本地硬盘损坏），为了防止数据丢失风险，建议使用冗余策略，例如支持冗余容错的文件系统（如 HDFS、Mapr-FS 等），另外，也建议定期将数据备份至更持久的存储系统中，例如腾讯云对象存储 COS，详情参见 对象存储COS。

本地硬盘损坏后，需要您进行云服务器实例关闭操作后，我们才能够进行本地硬盘替换；若云服务器实例已经宕机，我们会告知您并进行维修操作。

哪些地域可以购买大数据型 D1 实例？

目前可以购买可用区为：

- 上海二区
- 北京二区
- 广州三区

后续将开放更多地域可用区购买，敬请期待！

购买大数据型 D1 实例后，为什么没有看见数据盘？

大数据型 D1实例对应的本地硬盘不会自动挂载，可以按需进行挂载。

大数据型 D1 与高 IO 型 I2 的区别？

高 IO 型 I2 是专门为低延时、高随机 I/O 的业务场景设计的云服务器实例，拥有超高的 IOPS 性能，一般使用场景为高性能数据库（关系型、NoSQL 等）。大数据型 D1 实例是专门为高顺序读/写、低成本海量数据存储的业务场景设计的云服务器实例，拥有超高的存储性价比及良好的内网带宽。

大数据型 D1 实例的硬盘吞吐能力怎么样？

大数据型 D1 实例本地硬盘在顺序读写吞吐能力表现为（以D1.14XLARGE224 为例）：

- 单盘顺序读 190+ MB/s，顺序写 190+ MB/s（128 KB 块大小，32深度）。
- 12 块盘同时顺序读 2.3+ GB/s，顺序写 2.3+ GB/s（128 KB 块大小，32 深度）。

大数据型 D1 实例的本地硬盘与云硬盘有何不同？

云硬盘 CBS 为云服务器实例提供高效可靠的存储设备，CBS 是一种高可用、高可靠、低成本、可定制化的块存储设备，可以作为云服务器的独立可扩展硬盘使用。它提供数据块级别的数据存储，采用三副本的分布式机制，为云服务器实例提供数据可靠性保证，适用于各类应用场景的需求。大数据型 D1 实例的本地硬盘是专门为对本地海量数据集有高顺序读写性能需要的业务场景设计的，例如: Hadoop 分布式计算、大规模并行计算以及数据仓库等。

关机和重启失败原因排查和处理

对云服务进行关机，重启的操作时候，有非常少的概率出现失败的情况，失败的情况下可以对云服务进行如下情况的排查和处理。

可能导致关机/重启失败的原因

1. 请排查云服务器的CPU/内存的使用情况，当出现CPU使用率过高，或者内存耗尽的情况下，可能会导致在控制台关机/重启失败。

2. Linux操作系统可以检查是否安装 ACPI 管理程序，命令

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

   查看是否有进程存在，如果不存在请安装 apcid 模块。

3. Windows操作系统可以排查是否存在 WindowsUpdate 过长导致关机失败，因为 Windows 在做某些补丁操作时，会在关闭系统的时候做一些处理，这个时候可能存在更新时间过长导致关机/重启失败。

4. 初次购买 Windows 时，由于系统使用 Sysprep
   的方式分发镜像，初始化过程稍长。在初始化完成之前，Windows
   会忽略关机/重启的操作而导致关机/重启失败。

5. 操作系统安装某些了软件，或者中了木马，病毒后，系统本身遭破坏，也可能导致关机/重启失败。

强制关机/重启功能

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

云服务器控制台关机操作中选中强制关机

云服务器控制台重启操作中选中强制重启

Centos 6.x 系统 initscripts 缺陷导致 DNS 信息被清空解决办法

问题描述

centos 6.x 系统中由于 initscripts 部分版本存在缺陷，对操作系统进行重启或者执行命令

service network restart

之后

/etc/resolv.conf

配置文件中的 DNS 信息被清空，导致无法解析域名。

如何排查

存在的缺陷版本

因为系统 grep 版本的不同, initscripts 低于

initscripts-9.03.49-1

的版本存在缺陷。

查看initscripts版本

可以登录云服务器查看 initscripts 的版本情况确认是否存在该问题。

查看的方式：

$rpm -q initscripts
initscripts-9.03.40-2.e16.centos.x86_64

当前例子输出的 initscripts 版本

initscripts-9.03.40-2

低于存在的问题版本

initscripts-9.03.49-1

，存在DNS被清空的风险。

解决方法

升级版本

推荐升级 initscripts 到最新的版本，并重新生成 DNS 信息，命令如下：

```
cat /dev/null > /etc/resolv.conf
service network restart
yum makecache
yum -y update initscripts
```

等待升级完成后，可以再次检查 initscripts 的版本信息，确认升级是否成功，执行命令：

```
$rpm -q initscripts
initscripts-9.03.58-1.el6.centos.2.x86_64
```

例子打印的版本不同于之前版本，且高于

initscripts-9.03.49-1

，操作升级成功。