云服务器 ECS

故障处理

故障处理

问题描述

无法访问云服务器ECS上的网站。

解决办法

1. 先测试本地是否能 ping 通云服务器。
2. ping 测试正常再测试本地是否能够正常访问云服务器的 Web 端口。
3. telnet下服务器ip的80web端口和3306数据库端口，查看web服务器apache/nginx/iis或者数据库是否正常运行；
4. 如果本地到云服务器的 web 端口访问正常，再通过 http://ip.taobao.com/ 来测试全国范围内网站访问情况。
5. 如果全国范围内访问基本正常，仅本地无法正常访问，用 tracert 或者 traceroute 测试本地到云服务器的路由信息，并反馈到本地运营商。

如果还无法访问，考虑以下情况：

- 检查服务器 CPU、I/O、带宽、内存使用性能是否有异常。
- 查看的网站是否有报错，比如 404、502、503、504 错误，一般出现这种错误多半是服务器web内部问题。
- 检查服务器是否受攻击。
- 是否是磁盘空间占满了导致。
- 检查云服务器网站是否是用户访问量太大。
- 查看服务器是否处于运行状态。

关于 Linux 系统的连接故障排查，请参考 云服务器 ECS Linux SSH 无法远程登录问题排查指引。

关于 Windows 系统的连接故障排查，请参考 Windows 系统远程桌面无法连接的检查。

因各种因素，用户通过私网或本地公网访问云服务器 ECS 上相关业务时，可能出现访问异常的情况。本文先对整个链路上，可能引发访问异常的相关因素及症状进行说明，然后阐述了出现异常时的排查思路及处理办法。最后对工单提交时的注意事项进行了说明。

说明：本文相关说明不考虑阿里云 CDN 或第三方 CDN 网络相关因素的影响。

ECS 访问异常关联因素及症状示意图

从客户端到服务端的整个链路上，可能引发访问异常的相关因素主要如下*ECS 访问异常关联因素示意图*所示：

相关因素可能导致的症状，主要如下*ECS 访问异常症状对应图*所示：

ECS 访问异常关联因素说明

- 通过私网访问异常时关联因素说明
- 通过公网访问异常时关联因素说明

通过私网访问异常时关联因素说明

如果客户端是通过私网访问，则其链路相对简单。可能引发访问异常的因素及导致的客户端症状包括：

1. **源服务器内部配置 因素说明：**
   源服务器内部防火墙、安全软件等安全策略，或系统中毒等操作系统内部问题导致访问异常。**可能症状及原因：** ping 丢包：源服务器中毒等操作系统内部问题导致网络异常。ping 不通：源服务器系统内安全软件等安全策略禁止外 ping。所有端口 telnet 都不通：源服务器中毒等操作系统内部问题导致网络异常。只有部分端口 telnet 不通：源服务器系统内安全软件等安全策略禁止了对部分端口的访问。
2. **源服务器安全组配置 因素说明：**
   源服务器归属安全组规则阻断了对目标服务器的访问。**可能症状及原因：** ping 不通：源服务器出方向配置了禁 ping 规则。所有端口 telnet 都不通：源服务器出方向为指定端口配置了 drop 规则。只有部分端口 telnet 不通：源服务器出方向为所有端口配置了 drop 规则。
3. **负载均衡白名单 因素说明：**
   如果目标服务器是负载均衡，则相应监听端口开启白名单后，只有指定的 IP 或 IP 段地址才能对其访问。**可能症状及原因：** 只有部分端口 telnet 不通：源服务器 IP 不在白名单之内，导致无法访问相应监听端口。
4. **目标服务器安全组配置 因素说明：?**目标服务器归属安全组规则阻断了源服务器的访问。**可能症状及原因：** ping 不通：目标服务器入方向配置了禁 ping 规则。所有端口 telnet 都不通：目标服务器入方向为指定端口配置了 drop 规则。只有部分端口 telnet 不通：目标服务器入方向为所有端口配置了 drop 规则。
5. **目标服务器内部配置 因素说明：**目标服务器内部防火墙、安全软件等安全策略，或系统中毒等操作系统内部问题导致访问异常。**可能症状及原因：** ping 丢包：目标服务器中毒等操作系统内部问题导致访问异常。ping 不通：目标服务器系统内安全软件等安全策略禁 ping。所有端口 telnet 都不通：目标服务器中毒等操作系统内部问题导致访问异常。只有部分端口 telnet 不通：目标服务器系统内安全软件等安全策略禁止了对部分端口的访问。

通过公网访问异常时关联因素说明

如果客户端通过公网访问，则涉及的关联因素较多，包括：

- 客户端网络环境
- 运营商网络环境
- 阿里云网络环境
- 目标ECS服务器内部环境

客户端网络环境

对于客户端网络环境，可能引发访问异常的因素及导致的客户端症状包括：

1. **用户本地网络 因素说明：**
   如果用户本地网络存在异常，可能会导致部分 IP 或所有 IP 均无法正常访问。**可能症状及原因：** 非阿里云服务 IP 也无法访问：不仅是目标服务器无法访问，其它非阿里云 IP 也无法访问。
2. **本地 DNS 劫持 因素说明：**
   用户本地网络或当地运营商有 DNS 劫持行为，导致访问目标服务器关联业务时，出现非正常跳转或者被插入广告。**可能症状及原因：** 非正常跳转：DNS 劫持导致访问目标服务器关联业务时，跳转到了其它无关联网站。被插入广告：DNS 劫持导致访问目标服务器关联业务时，页面被插入广告。

运营商网络环境

对于运营商网络环境，可能引发访问异常的因素及导致的客户端症状包括：

1. **运营商网络策略 因素说明：**
   运营商根据其策略，可能会进行 DNS 劫持，或阻断某些 IP、域名或端口的访问。**可能症状及原因：** 被插入广告：DNS 劫持导致访问目标服务器关联业务时，页面被插入广告。域名无法访问但 IP 访问正常：运营商对某些违规域名的访问做了阻断。所有端口 telnet 都不通：运营商对某些违规 IP 的访问做了阻断。只有部分端口 telnet 不通：运营商对某些高危端口的访问做了阻断。
2. **备案 因素说明：**
   对于境内服务器，根据行政管控要求，需要进行备案。**可能症状及原因：** 非正常跳转：目标服务器关联域名未备案，导致访问关联业务时，跳转到了备案提示页面。域名无法访问但 IP 访问正常：目标服务器关联域名未备案，导致访问时，跳转到了备案提示页面，但通过 IP 访问无影响。

阿里云网络环境

对于阿里云网络环境，可能引发访问异常的因素及导致的客户端症状包括：

1. **云盾-肉鸡关停 因素说明：**
   目标服务器因肉鸡、中毒等问题，持续对外攻击，被云盾关停。**可能症状及原因：** ping 不通：服务器被关停导致无法 ping 通。所有端口 telnet 都不通：服务器被关停导致所有端口都不通。
2. **云盾-访问拦截 因素说明：**
   源服务器因持续扫描探测、攻击等行为，被云盾阻断。
   注意：如果源服务器本地网络是通过 NAT 共享方式访问公网的，则攻击源不一定是客户自身服务器，而可能是同网络内其它服务器。由于共享相同的公网 IP，导致云盾阻断相应 IP 后，源服务器的访问也受到了波及和影响。**可能症状及原因：** ping 不通：源服务器 IP 被云盾拦截，导致禁 ping。所有端口 telnet 都不通：源服务器 IP 被云盾拦截，导致所有端口都无法访问。

3. **绿网-违规屏蔽 因素说明：**
   目标服务器相关 URL 存在违规内容，访问被阻断。**可能症状及原因：** 非正常跳转：源服务器业务异常，导致相关访问跳转到了 DDos 高防或 Web 应用防火墙源站异常提示页面。部分 URL 无法访问：被 Web 应用防火墙规则命中的相应 URL，客户端无法正常访问，会跳转到了相应的阻断提示页面。
4. **DDos 高防和 Web 应用防火墙 因素说明：**
   目标服务器业务异常，或者源服务器相关访问行为被 DDos 高防或 Web 应用防火墙拦截规则命中，导致访问异常。**可能症状及原因：** ping 不通：服务器被关停导致无法 ping 通。所有端口 telnet 都不通：服务器被关停导致所有端口都不通。
5. **负载均衡白名单 因素说明：**
   如果目标服务器是负载均衡，则相应监听端口开启白名单后，只有指定的 IP 或 IP 段地址才能对其访问。**可能症状及原因：** 只有部分端口 telnet 不通：源服务器 IP 不在白名单之内，导致无法访问相应监听端口。
6. **目标服务器安全组配置 因素说明：**
   目标服务器归属安全组规则阻断了源服务器的访问。**可能症状及原因：** ping 不通：目标服务器入方向配置了禁 ping 规则。所有端口 telnet 都不通：目标服务器入方向为指定端口配置了 drop 规则。只有部分端口 telnet 不通：目标服务器入方向为所有端口配置了 drop 规则。

目标ECS服务器内部环境

对于目标 ECS 服务器自身相关环境，可能引发访问异常的因素及导致的客户端症状包括：

1. **目标服务器欠费停机 因素说明：**目标服务器欠费停机导致无法访问。**可能症状及原因：** ping 不通：目标服务器欠费停机导致无法 ping 通。所有端口 telnet 都不通：目标服务器欠费停机导致所有端口无法访问。
2. **目标服务器内部配置 因素说明：**
   目标服务器内部防火墙、安全软件等安全策略，或系统中毒等操作系统内部问题导致访问异常。**可能症状及原因：** ping 丢包：目标服务器中毒等操作系统内部问题导致访问异常。ping 不通：目标服务器系统内安全软件等安全策略禁ping。所有端口 telnet 都不通：目标服务器中毒等操作系统内部问题导致访问异常。只有部分端口 telnet 不通：目标服务器系统内安全软件等安全策略禁止了对部分端口的访问。
3. **软件源地址访问控制 因素说明：**
   目标服务器内部业务软件对源 IP 做了访问控制，导致源服务器无法访问。**可能症状及原因：** 只有部分端口 telnet 不通：相应端口对应业务软件对源 IP 做了访问控制，阻断了源服务器的访问。

ECS 服务器访问异常问题排查流程图

对于 ECS 访问异常问题，基本排查思路如下*ECS 服务器访问异常问题排查流程图*所示：

ECS 访问异常问题排查思路及处理办法

对于 ECS 访问异常问题，参照前图，其排查思路说明如下：

- 通过私网访问异常时的排查思路
- 通过公网访问异常时的排查思路

通过私网访问异常时排查思路

如果客户端通过私网访问，则访问异常时，可通过如下步骤进行判断、排查分析和处理：

1. **所有服务器访问目标服务器均存在异常？**
   即从其它不同服务器同时访问目标服务器做对比测试。**【1-A】是（所有服务器访问目标服务器均存在异常）：**如果所有服务器访问均存在异常，则推断是目标服务器归属安全组、或服务器内部自身存在异常所致。需要做进一步排查分析。**1-A.1 服务器内部访问是否正常？**
   即通过 **管理终端** 进入服务器，在服务器内部使用 127.0.0.1 做对比访问测试，看是否正常。**【1-A.1-A】是（目标服务器内部访问也存在异常）：**
   如果目标服务器内部访问也存在异常，则需要联系业务提供商或者业务运维人员，检查代码配置、软件运行状态。**【1-A.1-B】否（目标服务器内部访问正常）：**
   如果服务器内部访问是正常的，则需要检查目标服务器归属安全组和操作系统内相关安全软件的安全配置，排查是否对源服务器做了阻断。
   安全组的常见使用问题，可以参阅*安全组使用FAQ*。
   如果排查分析安全组和操作系统内安全软件配置后，均未见明显异常，则需要参阅文档*网络异常时抓包操作说明*，在出现异常时，从客户端和服务端同时并发抓包，然后提交抓包结果，联系**售后技术支持。【1-B】否（只有源服务器访问目标服务器存在异常）：**
   如果只有源服务器访问存在异常，则推断是源服务器归属安全组、服务器内部自身存在异常或源服务器到目标服务器之间的网络存在异常所致。需要做进一步排查分析。**1-B.1 telnet 端口测试是否正常？**
   即从源服务器访问目标服务器是否只是 ping 不通而端口访问正常。**【1-B.1-A】是（源服务器 ping 不通目标服务器，但 telnet 端口测试正常）：**
   如果只是 ping 不通，但端口访问正常，则需要检查目标服务器归属安全组和操作系统内相关安全软件的安全配置，是否对源服务器做了禁 ping。
   安全组的常见使用问题，可以参阅*安全组使用FAQ*。**【1-B.1-B】否（源服务器到目标服务器，telnet 端口测试及 ping 测试均异常）：**
   如果 ping 及 telnet 端口测试均有异常，则需要进一步排查：**1-B.1-B.1 到源服务器网关 ping 是否正常?**
   即从源服务器内部 ping 自身网关，看是否正常。**【1-B.1-B.1-A】否（源服务器 ping 自身网关也异常）：**
   如果源服务器 ping 自身网关也存在异常（不通或丢包），则需要通过系统日志等检查源服务器自身运行状态，比如服务器负载、网络配置等。**【1-B.1-B.1-B】是（源服务器 ping 自身网关正常）：**
   如果源服务器 ping 自身网关正常。则需要进一步排查：**1-B.1-B.1-B.1 到目标服务器网关 ping 是否**

正常？

即从源服务器内部 ping 目标服务器网关，看是否正常。**【1-B.1-B.1-B.1-A】否（源服务器 ping 目标网关正常）：**

如果源服务器 ping 自身网关和目标服务器网关都正常，则需要通过系统日志等检查目标服务器自身运行状态，比如服务器负载、网络配置等。**【1-B.1-B.1-B.1-B】 是（源服务器 ping 目标网关也不正常）：**

如果源服务器 ping 自身网关正常，但 ping 目标服务器网关存在异常（不通或丢包），则判断可能是中间网络异常所致。则需要参阅文档*网络异常时抓包操作说明*，在出现异常时，从客户端和服务端同时并发抓包，然后提交抓包结果，联系售后技术支持。

通过公网访问异常时排查思路

如果客户端通过公网访问，则访问异常时，可通过如下步骤进行判断、排查分析和处理：

1. **URL 访问问题判断：**

   1.1 被插入广告？

   即客户端访问目标服务器业务时，是否出现了页面被插入广告的情况。 **【1.1-A】是（页面被插入广告）：**

   如果是页面被插入广告情况，则参阅如下步骤进一步排查： **1.1-A.1 系统内部访问是否正常？**

   即通过 **管理终端** 进入目标服务器，在服务器内部使用 127.0.0.1做对比访问测试看是否正常。 **【1.1-A.1-A】是（目标服务器系统内部访问也存在异常）：**

   如果目标服务器内部访问也存在异常，则需要联系业务提供商或者业务运维人员，检查代码配置、软件运行状态。**【1.1-A.1-B】 否（目标服务器系统内部访问正常）：**

   如果目标服务器内部访问正常，则判断是由于本地网络异常或者本地运营商劫持所致。用户可以尝试修改本地 DNS 服务器地址看问题能否解决。如果还有问题，建议联系本地网络部门排查分析，或向当地运营商进行问题反馈。**【1.1-B】 否（页面没有被插入广告）：**

   如果不是页面被植入广告问题，则参阅后续步骤进一步排查分析。 **1.1-B.1 页面异常跳转？**

   即客户端访问目标服务器业务时，相关 URL 是否出现了非正常跳转。 **【1.1-B.1-A】 是（页面出现了非正常跳转）：**

   如果是页面出现了非正常跳转，则参阅如下步骤进一步排查分析： **1.1-B.1-A.1 系统内部访问是否正常？**

   即通过 **管理终端** 进入目标服务器，在服务器内部使用 127.0.0.1做对比访问测试看是否正常。 **【1.1-B.1-A.1-A】 否（目标服务器系统内部访问也存在异常）：**

   如果目标服务器内部访问也存在异常，则需要联系业务提供商或者业务运维人员，检查代码配置、软件运行状态。**【1.1-B.1-A.1-B】 是（目标服务器系统内部访问正常）：**

   如果目标服务器内部访问正常，则可以根据跳转到的页面做进一步处理。比如： 未备案提醒页面处理：为什么我的网站已经备案了还是提示未备案？DDos 高防异常页面：云盾DDOS高防502,504报错绿网阻断页面：页面如何解除屏蔽？Web 应用防火墙阻断页面：云盾Web应用防火墙返回的405、502、504页面分别代表含义**【1.1-B.1-B】 否（页面没有出现非正常跳转）：**

   如果不是页面非正常跳转问题，则参阅后续步骤进一步排查分析。

2. **问题范围判断：**

   如果不是 URL 访问异常问题，则需要通过对比分析确定问题范围：

   2.1 所有网络访问都有异常？

   即通过第三方拨测平台，从全国各地做对比访问测试，判断是否所有网络访问目标服务器都存在同样

异常。**【2.1-A】是（所有网络访问均存在异常）：**
如果经过测试，所有外部网络访问均存在异常，则参阅如下步骤进一步排查分析：**2.1-A.1 系统内部访问是否正常？**
即通过 **管理终端** 进入目标服务器，在服务器内部使用 127.0.0.1做对比访问测试看是否正常。**【2.1-A.1-A】否（目标服务器系统内部访问也存在异常）：**
如果目标服务器内部访问也存在异常，则需要联系业务提供商或者业务运维人员，检查代码配置、软件运行状态。**【2.1-A.1-B】是（目标服务器系统内部访问正常）：**
如果目标服务器内部访问正常，则需要检查目标服务器安全组及系统内安全配置，是否对源服务器的访问做了限制。
安全组的常见使用问题，可以参阅*安全组使用FAQ*。**【2.1-B】否（只有源服务器访问目标服务器存在异常）**
如果只有源服务器访问存在异常，则参阅后续步骤进一步排查分析。

3. **问题现象判断：**
如果只有源服务器访问存在异常，则需要通过 ping 或 telnet 等测试做进一步排查分析。
3.1 ping 是否正常？
即客户端 ping 目标服务器 IP 地址是否正常。**【3.1-A】否（ping 目标服务器正常）：**
如果客户端 ping 目标服务器丢包或不通，则可能是中间链路或对端服务器存在异常所致，则需要通过 MTR 链路测试做进一步排查分析。
链路测试操作说明可以参阅 *ping 丢包或不通时链路测试说明*。**【3.1-B】是（ping 目标服务器正常，但是端口访问不通）：**
如果 ping 目标服务器正常，但是端口访问不通，则需要参阅后续步骤进一步排查分析。**3.1-B.1 端口是否被目标服务器拦截？**
即目标服务器归属安全组或系统内部安全设置，是否有策略阻断了客户端对相应端口的访问。**【3.1-B.1-A】是（目标服务器阻断了客户端对某些端口的访问）：**
如果确认有对源服务器的阻断策略，则需要进行相应调整。
安全组的常见使用问题，可以参阅*安全组使用FAQ*。**【3.1-B.1-B】否（目标服务器没有阻断策略）：**
如果目标服务器没有针对源服务器的阻断策略，则可能是相应被运营商拦截所致，则需要通过 tracetcp 等工具对端口阻断情况做进一步跟踪分析。
端口可用性探测说明可以参阅 *能 ping 通但端口不通时端口可用性探测说明*。

ECS 访问异常问题工单提交须知

如果经过前述步骤还是未能成功解决问题，请参阅如下步骤依次进行测试并记录测试结果，然后提交工单。

- 客户端通过私网进行访问
- 客户端通过公网进行访问

客户端通过私网进行访问

如果客户端是通过私网进行访问的，则请参阅如下步骤依次进行测试并记录测试结果：

1. 通过不同服务器向目标服务器做相同的访问测试，看是否有同样的异常症状。
2. ping 目标服务器 IP ，看是否正常。
3. telnet 目标服务器相应端口，看是否正常。
4. 源服务器 ping 自身网关，看是否正常。
5. 目标服务器 ping 自身网关，看是否正常。
6. 源服务器 ping 目标服务器网关，看是否正常。
7. 目标服务器 ping 源服务器网关，看是否正常。
8. （按情况可选）参阅*网络异常时抓包操作说明*，出现异常时同时从源服务器和目标服务器抓包。

客户端通过公网进行访问

如果客户端是通过公网进行访问的，则请参阅如下步骤依次进行测试并记录测试结果：

1. 从不同地域不同网络环境，向目标服务器做同样的访问测试，看是否存在同样的异常症状。
2. 异常情况是否是页面被插入广告？
3. 异常情况是否是页面出现了异常跳转？
4. 客户端 ping 目标服务器，看是否正常。
5. 客户端 telnet 目标服务器相应业务端口，看是否正常。
6. 如果是 ping 存在异常（丢包或中断），则参阅 *ping 丢包或不通时链路测试说明*进行测试，并记录测试数据。
7. 如果 ping 正常，但端口无法访问，则参阅 *能 ping 通但端口不通时端口可用性探测说明* 进行测试，记录测试数据。
8. （按情况可选）参阅*网络异常时抓包操作说明*，出现异常时同时从源服务器和目标服务器抓包。

记录前述步骤的相关测试结果或数据，然后联系售后技术支持。

启动机器，看能否登陆。如果能登陆，请检查以下可能的原因:

- 应用程序导致内存溢出或泄露
- 进程过多或者不断创建，资源耗尽
- 数据库程序死锁，连接数过多
- 应用程序异常
- 流量负载过大
- 遭受黑客入侵攻击
- 误操作

如果无法查看故障现场，可以查询系统日志查看是否有异常记录。

加强云服务器的安全的措施有：

- 检查服务器应用及网站程序是否有漏洞，开启阿里的云盾相关安全功能，购买云服务器托管服务；
- 使用“Web应用防火墙”，防御Web攻击和CC攻击
- 开启服务器默认防火墙，进行防火墙的安全设置，关闭一些不必要的端口；
- 设置密码尽量使用强密码，可以将默认远程端口修改成其他端口；

- Windows 实例及时打补丁，可以根据需要适当安装一些安全防护软件。

造成服务器带宽跑满的原因有很多，大致可以归结为以下几类：

病毒

Windows 系统服务器中病毒或站点挂马，导致服务器内部有对外发包的文件。建议在服务器上安装杀毒软件，进行杀毒。可以通过任务管理器中查看是否异常进程。当前阿里云暂时没有提供杀毒软件，您可以登陆服务器根据自己的日常使用的杀毒软件进行安装即可。

网络攻击

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。可以使用“Web应用防火墙”进行防御

存在耗资源进程

服务器内部有耗资源进程。

- Windows Server 2003 系统无法直接查看到，但可以借助第三方软件查看；
- Windows Server 2008 系统可以启动 任务管理器>性能>资源监控器>网络>查看 **发送（字节/秒）** 占用较多的进程。如果不是常用进程，说明可能是病毒或异常文件；如果是常用进程，说明该进程当前有异常，需要针对该进程对应的服务进行一下分析。

根据以往经验，曾发现过因搜狗拼音的更新，以及疑似上传本地词库导致的出网带宽跑高。

爬虫

正常网站所消耗的带宽较多，此类情况建议通过访问的日志来分析，如果日志中过多的 baiduspider 或 googlebot 。说明网页被爬虫抓取，大量来自搜索引擎的链接也容易跑高带宽，例如:windows-cmd 下找到 iis的日志，可以使用命令 type *.log | find “baidu “ 等。

Linux 的 Apache 和 nginx 可以检查 cat access.log | grep baidu 等。

同时检查站点是否存有 MP3，flv，swf 等大文件被频繁访问下载，如果此类文件较多，建议减少这些文件，可搭配使用 OSS、CDN 服务。

网站规模大

网站规模较大（比如门户网站、商城等），即网站本身访问量需求大，查看网站的 Page View 值、Hits 值、日流量都很高，建议升级带宽 。

造成流量大的原因主要有：

网站页面设计不合理

页面中包含大图片或音频、视频文件等文件，导致网站页面太大。网站提供.mp3,.rar,.zip.exe等文件的下载，或网站提供视频、音频文件的播放。

如果网站规模较大，网站的点击率很高，建议减少音频、视频文件。如果还不能满足要求，可以升级带宽。

网页内容的大小

网页文件的大小是网站是否能快速打开最重要一个因素，如果说服务器等硬件方面我们决定不了，我强烈建议从这里下手，不管是表格、还是DIV+CSS、适当的优化代码，都能减少网页大小。尽量优化代码，用最少的代码，不要将整个内容包含在一个框内。同时大量错误、冗余代码也是拖慢网站速度之一。

机器的配置

包括服务器端与客户机端的硬件配置程度，同样的网络环境下，双核的服务器的运算能力要强一些。同样的网络环境下，用一台赛扬的机器和奔四双核处理器的电脑，打开同样的网页，速度也肯定不一样。

服务器软件

软件多少、稳定和软件的正确配置，都会影响到服务器环境，以致影响到网络速度。服务器安装软件防火墙，会牺牲一些网络速度，所以 VPS、或独立服务器用户装一个防火墙即可。

网络最小带宽

这是最主要的因素，再慢的网站放在好的带宽下访问速度一样快。网络的带宽包括对网站所在服务器带宽和用户端两个位置，对接点指的是出口端与入口端（如电信对网通的对接点）。另一个就是用户本身的最小带宽，如果用户接入端办理的宽带低也会影响访问速度。

大量数据库操作

小网站在执行大量数据库操作时，也会影响网站打开速度，使用APS+Access 结构的网站尤为明显，尤其是同时有大量用户提交评论时，就操作数据库锁死，导致网站打不开。

用大量 Javascript

网站上使用大量 JS 是大忌，不仅搜索引擎无法收录，同时会不断提交请求增加服务器负担，例如鼠标特效、栏目的特效、状态栏的特效等等。这些特效的原理是先由服务器下载到本地机器，然后在本地机器上运行产生，然后你才能看到的效果。特效做的太多，在本地机器上就要运行大半天才能全部完成，而如果你的主机配置一般的话，那就更慢了。所以，建议一定要少用 Javascript 特效。

页面上用大图片和 Flash

图片是拖慢网速最重要一个因素。图片占用很多空间，又使网站打开速度变得很慢，同样FLASH也是一个道理

。建议对图片经过处理，使图片空间变小。

过多引用了其他网站的内容

包括引用其他网站的图片、视频文件等，如果直接在页面引用别的网站的东西，而那个网站的速度又慢，或者那个网站的页面已经不存在了，那么打开的速度就会非常慢。

DNS 解析时间

DNS 解析包括往返解析的次数及每次解析所花费的时间，它们两者的积就是 DNS 解析所消耗的时间，因此，很多人忽视了 DNS 的问题，其实，DNS 对 网站解析速度也是非常重要的。可以使用阿里云的云解析产品。

被CC攻击

服务器被大量HTTP Get、POST请求攻击，攻击请求占用了大量服务器资源，导致正常请求无法处理或者处理缓慢。可以使用阿里云的“Web应用防火墙”防御

如果云服务器 ECS 实例的 #CPU 跑满，考虑以下因素：

- 检查程序最大线程数不够
- 程序代码不够优化，存在死循环、死锁
- Web 配置文件的参数不够优化
- 检查 Web 和系统日志存在访问异常
- 网站被盗链
- 当时有搜索引擎爬虫大面积爬取网站
- 受到了小型网络攻击；进程有异常
- 实例中毒或中木马
- 受到了CC攻击或Web攻击

Linux 实例可以通过系统日志和 Web 日志，和一些 top，free，uptime，sar，ps 命令查询原因。Windows 实例可以通过资源监控器分析。

问题描述

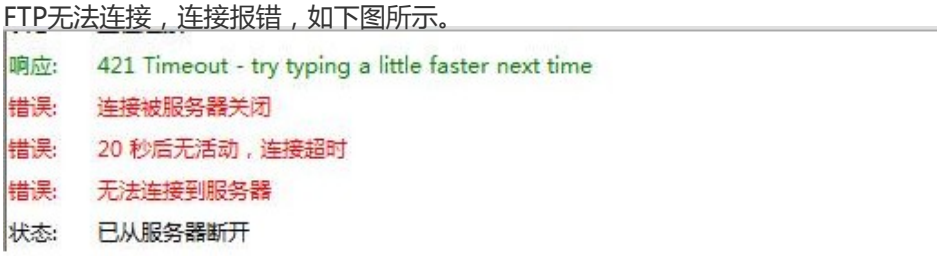
在使用 FTP 软件进行数据传输时有时会出现断开连接的情况，这种现象和网络环境、硬件环境和软件环境都可能有关系。

解决办法

如果在 FTP 管理里出现经常中断的情况，可以将您要上传的网站程序文件压缩，使用 FLASHFXP 等 FTP 软件进行断点续传。压缩文件上传之后再在服务器中进行解压缩操作即可。
也有小概率可能受到网络原因传输过程中压缩包损坏，需要再次上传，所以超大文件建议分割压缩。

问题描述

FTP无法连接，连接报错，如下图所示。



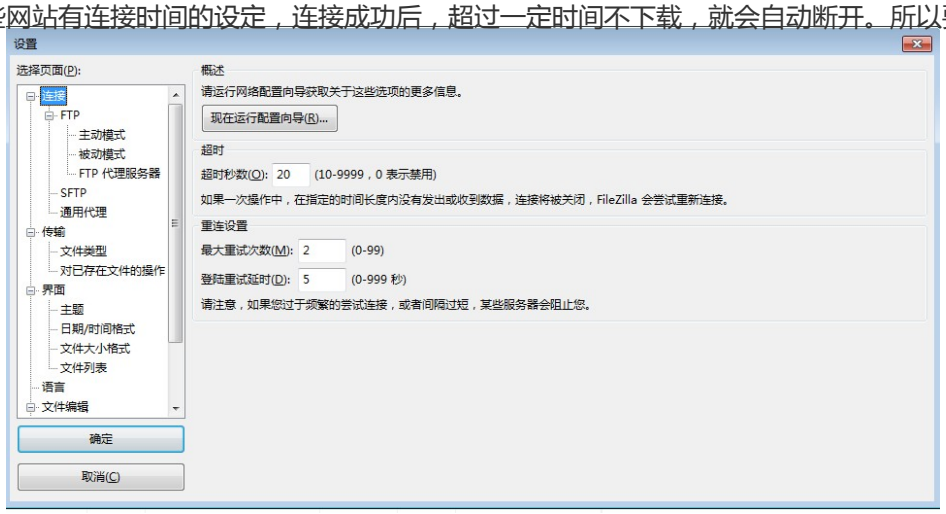
原因分析

同时连接该 FTP 的人数过多。一般 FTP 网站都有同时登陆人数的上限，超过该上限就会出现 421 错误。

问题解决

在 FTP 软件中，把重试次数改为 **999**，重试间隔改为 **60 秒**，一般几分钟到半小时就会连上。

注意：有些网站有连接时间的设定，连接成功后，超过一定时间不下载，就会自动断开。所以要经常去看看有没有连上。



遇到这类问题，请尝试：

检查服务器防护墙是否放行了 FTP 所需要的端口(默认是 20 和 21)。

尝试将本地 FTP 客户端设置为被动模式。

如果本地多次输出错误密码可能会导致本地 IP 被屏蔽，可访问http://ip.taobao.com 获取本地当前的 IP，然后将 IP 通过工单提交售后支持核查。

如问题还未解决,请联系**售后技术支持**。

需要考虑的因素有账户、恶意进程、恶意程序、Web 服务等。

账户

Windows

检查服务器内是否有异常的账户，查看下服务器内是否有非系统和用户本身创建的账户。一般黑客创建的账户账户名后会有$这个字符，有此类账户存在，请立即禁用或者删除掉。

黑客也可能在您服务器内创建隐藏用户，隐藏账户在本地用户内是查看不到的，您可以：

1. 在服务器内单击 **开始**>**运行**。
2. 输入 **regedt32.exe**。建议您在操作修改注册表前先备份，以免操作出错。
3. 依次选择 HKEY_LOCAL_MACHINE/SAM/SAM，默认是看不到里面的内容。
4. 找到 SAM，鼠标右键选择 **权限**，选择 **administrator**，将权限勾选为 **完全控制**，然后确定。
5. 单击 **开始**>**运行**，输入 **regedit**。
6. 选择 HKEY_LOCAL_MACHINE/SAM/SAM/Domains/Account，打开显示的就是您的实例所有用户名。
7. 如出现本地账户中没有的账户，即为隐藏账户，可以删除，这样就可以删除隐藏用户了。

Linux

1. 使用 last 命令查看下服务器近期登录的账户记录，或者查看/var/log/secure 日志。
2. 如果有除root外的用户登录过，检查下 /etc/passwd 这个文件，看是否有异常账户。
3. 有的话使用命令“usermod -L 用户名”禁用用户或者使用命令“userdel -r 用户名”删除用户。
4. 检查服务器内部账户，如管理员账户、mysql账户、sql server账户、ftp账户）是否密码设置的较为简单，过于简单的密码很容易被黑客破解，请将密码设置的较为复杂些。

恶意进程

Windows

1. 登录服务器，单击**开始**>**运行**。
2. 输入 cmd，然后输入 netstat –nao 查看下服务器是否有未被授权的端口被监听。
3. 检查对应的pid进程号。
4. 然后服务器单击 **开始**>**运行**，输入“msinfo32”软件环境，查看正在运行的任务，通过pid号查看下运行文件的路径，删除对应路径文件。

Linux

1. 登录服务器。

2. 使用 netstat –nap 查看下服务器是否有未被授权的端口被监听，查看下对应的pid。
3. 使用 ls -l /proc/$PID/exe ($PID为对应的pid号) 命令查看下pid对应的文件路径，删除下对应的文件。

恶意程序

Windows

检查下您服务器内部是否有异常的启动项。

1. 在服务器内单击**开始**>**所有程序**>**启动**。
2. 此目录在默认情况下是一个空目录，但是如果有启动程序或者.bat后缀的文件，核实下是否为您技术人员添加的，如果不是请删除。
3. 再次点击**开始**>**运行**，输入 **msconfig**，打开系统启动项，在启动菜单栏中查看是否存在命名异常的启动项目，例如 A.EXE、XXXXI1SU2.EXE等，有的话您将启动项目的勾选去掉，并到命令中显示的路径删除文件。
4. 点击**开始**>**运行**，输入 **regedit**，依次点击 HKEY_CURRENT_USER/software/micorsoft/windows/currentversion/run
5. 检查右侧是否有启动异常的项目，有的话也删除，并建议在服务器内安装杀毒软件对判断做下病毒查杀，清除下病毒木马。

Linux

1. 登录服务器。
2. 使用 ps -aux 命令查看是否有异常进程，异常进程可以使用 kill 命令关闭掉。
3. 使用 chkconfig —list 命令查看下开机启动项中是否有异常的启动服务，有的话使用 chkconfig 服务名 off 的命令关闭。同时检查 /etc/rc.local 中是否有异常的项目，如有请注释掉。

Web 服务

如果您服务器内有运行 Web 服务，请您限制 Web 运行账户对文件系统的访问权限，只开放读取的权限。

建议您可以给服务器开通使用云盾的安全网络，可以提供web攻击防护，抵御黑客利用网站应用程序的漏洞入侵服务器，防止黑客利用新漏洞入侵网站，这样能够最大程度保护您的服务器避免被入侵。

修改远程端口并限制登录IP

Windows

修改远程端口：

1. 单击**开始**>**运行**，然后输入 **regedit**。
2. 打开注册表，进入如下路径：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp
HKEY_LOCAL_MACHINE\SYSTEM\CurrentContro1Set\Control\Tenninal Server\WinStations\RDP-Tcp

3. 修改下右侧的 PortNamber 值。

限制远程登录IP：

- Windows 2003:打开防火墙点击例外，选择下远程桌面>点击编辑，更改范围，在自定义列表中填写上需要远程的 IP。
- Windows 2008/2012:依次打开控制面板>系统安全>Windows防火墙>高级设置>入站规则>远程桌面（TCP-In）>作用域，在远程 IP 处填写需要远程连接的服务器 IP。

Linux

修改远程端口：

1. 在服务器内编辑 /etc/ssh/sshd_config 文件中的 Port 22 将 22 修改为其他端口即可。
2. 修改之后需要重启 ssh 服务。可以使用 /etc/init.d/sshd restart 命令重启。

限制登录IP：

可以通过编辑/etc/hosts.deny 、/etc/hosts.allow 两个文件来限制IP。

Linux 工具：

下载地址：get_cpu_mem_info_sh.rar

使用方法：

1. 下载该文件解压后，上传到 /tmp 目录中。
2. 运行 cd 切换到/tmp目录。
3. 执行： nohup bash get_cpu_mem_info.sh &

该工具会在 /tmp 目录下生成一个日志文件，记录实时监控系统的 CPU、内存的使用情况，等到系统异常时可以用于分析日志。

Windows 工具：

下载地址：get_cpu_mem_info_bat.rar

使用方法：

1. 下载该文件解压后，上传到c:\目录中。
2. 双击打开运行后。不要关闭，最小化即可。

该工具会在 C:\ 目录下生成一个日志文件，记录实时监控系统的性能状态，等到系统异常时可以用于分析日志。

当您的云服务器存在恶意行为，例如：

- 对外 DDoS 攻击，多次通知您，但一直未处理。
- 严重的暴力破解服务器密码的行为。
- 钓鱼欺诈行为，被第三方投诉。

阿里云将封锁云服务器，您的实例的状态将变为：已锁定。

您只拥有一次解封的权限，因此解锁后，请务必停止恶意行为。

解锁步骤：

找到被锁定的云服务，找到申请解锁按钮。

2. 阅读解封承诺函，同意解封承诺函并确认。

Linux 实例挂载数据盘报错，有以下几种场景。

场景 1：

问题描述：

ECS Linux 挂载数据盘到 /mnt 目录，发现 /mnt 目录的数据不见了。

解决办法：

Linux 以 mount 方式数据盘时，是以独占目录方式挂载。即：会遮掩原目录数据，显示数据盘当前数据，不会实现数据累加效果。

原目录数据也并未丢失，而是被暂时遮掩。可通过 umount 卸载数据盘后，原目录数据可见。

场景 2：

问题描述：

umount 数据盘时无法卸载(挂载到 /mnt 目录)，提示：umount failed，Device is busy。

解决办法：

此问题一般是由于数据盘挂载的目录被占用，导致数据盘无法正常卸载，处于 busy 状态。

通过 fuser -cu /mnt 查询占用该目录的进程或用户。

确认无重要数据正在读写后，执行 fuser -ck /mnt 命令，结束占用数据盘目录的所有占用。

执行 umount 卸载。

注意： 不建议把数据盘挂载到有数据的目录上，以避免造成数据读取异常。

注意：排查前请先创建快照备份，避免误操作导致数据丢失无法还原。

建议您使用Web应用防火墙，避免黑客使用Web攻击攻陷服务器：

https://www.aliyun.com/product/waf

排查病毒木马

1. 使用 netstat 查看网络连接，分析是否有可疑发送行为，如有则停止。
2. 使用杀毒软件进行病毒查杀。

Linux常见木马清理命令:

- chattr -i /usr/bin/.sshd
- rm -f /usr/bin/.sshd
- chattr -i /usr/bin/.swhd
- rm -f /usr/bin/.swhd
- rm -f -r /usr/bin/bsd-port
- cp /usr/bin/dpkgd/ps /bin/ps
- cp /usr/bin/dpkgd/netstat /bin/netstat
- cp /usr/bin/dpkgd/lsof /usr/sbin/lsof
- cp /usr/bin/dpkgd/ss /usr/sbin/ss

- rm -r -f /root/.ssh
- rm -r -f /usr/bin/bsd-port
- find /proc/ -name exe | xargs ls -l | grep -v task |grep deleted| awk '{print $11}' | awk -F/ '{print $NF}' | xargs killall -9

排查并修复服务器漏洞

1. 查看服务器账号是否有异常，如有则停止删除掉。
2. 查看服务器是否有异地登录情况，如有则修改密码为强密码（字每+数字+特殊符号）大小写，10 位及以上。
3. 查看 Jenkins、Tomcat、PhpMyadmin、WDCP、Weblogic 后台密码，提高密码强度（字每+数字+特殊符号）大小写，10 位及以上，不使用建议关闭 8080 管理端口。
4. 查看WEB应用是否有漏洞，如 struts, ElasticSearch 等，如有则请升级。
5. Jenkins管理员无密码远程执行命令漏洞，如有请设置密码或关闭 8080端口管理页面。
6. 查看 Redis 无密码可远程写入文件漏洞，检查 /root/ 下黑客创建的SSH 登录密钥文件，删除掉，修改 Redis 为有密码访问并使用强密码，不需要公网访问最好 bind 127.0.0.1 本地访问。
7. 查看 MySQL、SQLServer、FTP、WEB 管理后台等其它有设置密码的地方，提高密码强度（字每+数字+特殊符号）大小写，10 位及以上。
8. 如果有安装第三方软件，请按官网指引进行修复。

开启云盾服务

1.购买Web应用防火墙防范Web攻击:

https://www.aliyun.com/product/waf

2.使用安骑士，对主机扫描杀木马，并修复漏洞

https://www.aliyun.com/product/aegis

如果问题仍未解决

经过以上处理还不能解决问题，强烈建议您执行下列操作：

1. 将系统盘和数据盘的数据完全下载备份到本地保存。
2. 重置全盘。登陆 云服务器ECS控制台。
3. 单击进行您需要进行初始化的实例，备份完服务器数据。
4. 关闭实例。
5. 单击 **重置磁盘**，按您的实际情况选择系统盘和数据盘重置即可。6. 重新部署程序应用并对数据进行杀毒后上传，并重新进行前述的 3 步处理。

如果问题还未能解决，请联系售后技术支持。

可尝试用下面的方法处理：

首先看下服务器是否由于攻击进入我方安全清洗。

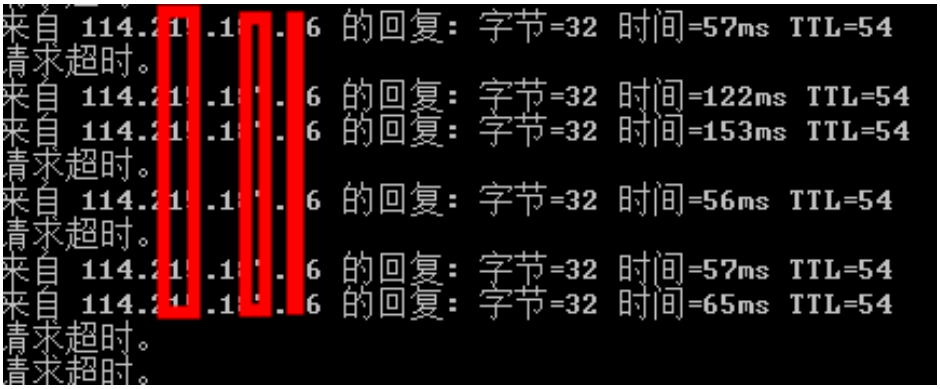
如果不再受到 DDOS 攻击，但攻击流量不大，没自动触发清洗的，建议调整触发清洗的阈值，默认阈值是 300M，可以尝试调整到较小的阈值。

同时需要检查下是否有恶意的 IP 地址连接到服务器，可以防火墙将其屏蔽掉；服务器内部也可以安装一些安全防护软件。

如果需要，请手工提工单，售后工程师会将用户 IP 加入清洗。

问题描述

服务器远程访问异常卡顿，Ping ECS 服务器 IP 出现较大延迟或丢包。



分析排查

服务器出现 Ping 延迟或丢包，一般由于本地网络、业务高峰（带宽峰值）、遭受攻击、被云盾屏蔽导致。可参考以下排查方法：

1. 检查是否为本地运营商线路问题，测试本地网络是否流畅，Ping 其他服务器是否延迟较高。

   使用阿里测或站长工具进行多次全国采点测速，判断是否国内大面积出现延迟，还是只有本地出现此问题。

监测点	响应IP	IP归属地	响应时间	TTL
江苏[电信]	114.[redacted]	浙江省杭州市 阿里云BGP数据中心	10毫秒	52
广西[电信]	114.[redacted]	浙江省杭州市 阿里云BGP数据中心	37毫秒	53
广州[电信]	114.[redacted]	浙江省杭州市 阿里云BGP数据中心	29毫秒	51
河南[电信]	114.[redacted]	浙江省杭州市 阿里云BGP数据中心	25毫秒	52
台湾[电信]	114.[redacted]	浙江省杭州市 阿里云BGP数据中心	81毫秒	48
江苏扬州[电信]	114.[redacted]	浙江省杭州市 阿里云BGP数据中心	10毫秒	53
浙江[电信]	114.[redacted]	浙江省杭州市 阿里云BGP数据中心	3毫秒	51
浙江[电信]	114.[redacted]	浙江省杭州市 阿里云BGP数据中心	7毫秒	53

如果进行全国采点测速，发现服务器网络响应异常，如国内大面积出现Ping 响应延迟或超时，排查是否达到网络峰值或出现业务高峰，此时可考虑临时升级服务器带宽。

4. 如果判断为服务器遭受外部攻击，可提交工单申请售后排查或考虑使用阿里云高防 IP 业务。
5. 本地 Ping 服务器返回：请求超时。但其他网络或全国采点测速均能正常 Ping 通服务器。这种情况一般是由于本地 IP 被云盾屏蔽导致，可通过工单申请售后排查，或在云盾中添加 IP 白名单，操作方法点此查看。
6. 多地节点或全国采点均无法 Ping 通服务器 IP，此时可通过管理终端登陆服务器，检查防火墙及网卡配置，或提交工单申请售后查询服务器IP是否被黑洞处理。