ALIBABA CLOUD

阿里云

负载均衡

常见问题

文档版本：20220228

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.为什么无法访问负载均衡

本文主要介绍通过客户端无法访问负载均衡的可能原因和处理方法。

> **说明** 本次示例中负载均衡前端端口为80，ECS后端端口为80，ECS内网IP是10.11.192.1。排查客户端无法访问负载均衡问题时，请根据实际情况配置端口和内网IP信息。

序号	可能原因	处理方法
1	后端服务器无法访问SLB，对于四层负载均衡服务，目前不支持负载均衡后端ECS实例直接为客户端提供服务的同时，又作为负载均衡的后端服务器。	-
2	健康检查异常。	健康检查方法请参见如何排查四层监听（TCP/UDP）健康检查异常和如何排查七层监听（HTTP/HTTPS）健康检查异常。
3	不支持通过SLB搭建FTP、tftp、h323和sip等	• 如果是Linux系统，您可以尝试配置22端口的转发，使用sftp连接传输数据。 • 支持通过EIP可见模式将EIP绑定到FTP服务器上对外提供FTP服务，配置详情请参见使用EIP部署FTP服务器。

4	服务器内网防火墙设置没有放行80端口。	可以选择执行如下命令，暂时关闭防火墙进行测试。
		• Windows 服务器上运行：
		`firewall.cpl`
		• Linux 服务器上运行：
		`/etc/init.d/iptables stop`

5	后端端口异常。	• 对于四层负载均衡，使用telnet测试有响应即为正常。 示例：使用 `telnet 10.11.192.1 80` 来测试。 • 对于七层负载均衡，HTTP状态码需要是200等代表正常的状态码，检验方法如下： ◦ Windows：直接在ECS上访问ECS的内网IP测试是否正常。 示例：`http://10.11.192.1` ◦ Linux：使用 `curl -I` 命令查看状态是否为 `HTTP/1.1 200 OK` 。 示例：`curl -I 10.11.192.1`

序号	可能原因	处理方法

6	rp_filter特性和负载均衡底层LVS的策略路由产生冲突，导致访问出现异常。	1. 登录四层负载均衡后端添加的Linux系统的ECS实例。
		2. 编辑*/etc/sysctl.conf*文件，将系统配置文件中的以下三个参数值设置为0。
		`net.ipv4.conf.default.rp_filter = 0`
		`net.ipv4.conf.all.rp_filter = 0`
		`net.ipv4.conf.eth0.rp_filter = 0`
		3. 执行 `sysctl -p` 命令，使配置生效。

7	监听功能异常	在服务器上执行以下命令，如果能看到10.11.192.1:80的监听信息，或者0.0.0.0:80的监听信息，说明这部分端口的监听正常。
		• Windows 服务器上运行：
		`netstat -ano | findstr :80`
		• Linux 服务器上运行：
		`netstat -anp | grep :80`

8	创建负载均衡实例后，没有添加监听。	请配置监听，详情请参见监听概述。
9	负载均衡通过域名访问不通，可能为用户域名解析错误导致。	-
10	客户端本地网络或运营商中间链路异常。	从不同地域及不同网络环境，对负载均衡相应服务端口做访问测试。 如果只有本地网络访问时出现异常，则判定是网络异常导致的问题，此时可以继续通过持续进行ping测试或MTR路由跟踪等手段做进一步排查分析。
11	客户端IP被云盾拦截。	1. 在客户端网络环境下访问 `http://ip.taobao.com` ，获取客户端网络环境对应的公网IP。 2. 将获取的IP配置为白名单，该操作将会对来自相应IP到负载均衡的所有访问全部放行。 **说明** 该操作可能会带来安全风险，确保白名单中的IP不会对负载均衡进行恶意攻击。
12	用户使用完高防IP之后切换回普通模式，未关闭访问控制白名单功能。	关闭ACL白名单。

序号	可能原因	处理方法
如果还未能解决问题，请在提交工单时提供如下信息，以便我们更高效地协助您解决问题。 • 负载均衡实例ID或负载均衡服务IP地址。 • 访问 `ip.taobao.com` 时获取的客户端对应的公网IP。 • 公网客户端对负载均衡IP长时间ping及MTR路由跟踪测试截图。		

2.为什么请求不均衡

介绍负载均衡请求不均衡的可能原因和排查方法。

可能原因

负载均衡请求不均衡可能有以下几种原因：

- ECS实例请求连接数较少。
- 不同ECS实例的性能不同导致请求不均衡。

> **说明** ECS实例内存使用情况不能准确的判断请求转发是否均衡。

- 开启了会话保持功能 。

  配置了会话保持，当访问负载均衡实例的客户端又很少时，容易导致不均衡，尤其在使用少量客户端对负载均衡进行测试的时候。例如TCP监听，开启了会话保持（四层是基于来源地址做会话保持），使用一台客户端对负载均衡实例进行压测，就会导致不均衡。

- ECS健康检查异常 。

  后端服务器ECS的健康建状态异常会导致不均衡，尤其在压测的时候容易忽略后端服务器ECS的健康检查状态，如果有后端服务器ECS健康检查失败或者健康检查状态经常跳跃（好到坏，又从坏到好，反复变化）必然会导致不均衡。

- TCP Keepalive保持长连接 。

  后端服务器ECS有些开启了TCP Keepalive保持长连接，而有些又没有开启，则连接会在保持长连接的后端服务器上堆积，造成不均衡。

排查和解决方法

- 查看后端各台ECS的权重是否相同。
- 在相关时间段内是否有健康检查失败或波动现象，查找波动的原因；或者健康检查没有配置正确的响应码2xx和3xx，导致了健康检查显示正常，但后端服务有异常。
- 是否同时使用了加权最小连接数（WLC）调度方式和会话保持，如果是，尝试改为加权轮询（WRR）算法和会话保持。

3.如何处理健康检查导致的大量日志

负载均衡的日志管理功能会自动保存三天内的健康检查日志，如果健康检查日志过多，对您的运维工作造成不便，您可以选择以下方案来减少或禁止某些场景下健康日志的产生。

> **说明** 减少健康检查日志的数量可能会导致您无法及时发现负载均衡实例运行时所出现的问题，请您谨慎权衡每种方案所带来的风险，根据您的实际情况进行选择。

- 获取访问日志
- 调整健康检查频率
- 关闭7层负载均衡下的健康检查
- 将7层负载均衡切换为4层负载均衡
- 关闭健康检查页面的应用日志

获取访问日志

HTTP协议健康检查默认使用HEAD请求方法，因此过滤掉HEAD的请求，就可以获得实际的访问日志。

调整健康检查频率

通过延长健康检查的间隔时间来减少健康检查的次数，降低健康检查产生的日志数量。

方案风险说明：

延长健康检查的间隔时间后，后端ECS实例出现故障时，负载均衡发现故障ECS实例的时间也会变长。

操作步骤：

1. 登录负载均衡管理控制台。
2. 在**实例管理**页面中找到相应的负载均衡实例，单击实例ID。
3. 在**监听**页签下，找到对应监听，单击监听**操作**列的**配置**。
4. 在**配置监听**对话框中，单击**下一步**，再单击**下一步**，进入健康检查配置。
5. 调整**健康检查间隔时间**，范围为1～50秒，间隔越大，健康检查的频率就越低，后端服务器产生的日志也会相应减少。请根据您的实际情况进行修改。

6. 单击**下一步**至**确定**，完成修改。

关闭7层负载均衡下的健康检查

使用7层HTTP/HTTPS负载均衡模式时，健康检查由HTTP Head请求实现， 后端服务器的应用日志会记录相应的健康检查请求信息，可能导致大量的日志信息。

风险说明

HTTP/HTTPS模式下关闭健康检查后，负载均衡不再检查后端服务器，一旦某台后端服务器发生故障，则无法实现访问流量自动切换至其它正常的后端服务器。

操作步骤

1. 登录负载均衡管理控制台。
2. 在**实例管理**页面中找到对应的负载均衡实例，单击实例ID。
3. 在**监听**页签下，单击**操作**列的进单击**配置**。
4. 在**配置监听**对话框中单击**下一步**，再单击**下一步**，进入健康检查配置。
5. 关闭**开启健康检查**。

6. 单击**下一步**至**确定**，完成修改。

将7层负载均衡切换4层负载均衡

4层TCP模式下的健康检查仅仅使用TCP的三次握手实现，不会生成应用日志。如果您的业务可以切换为4层TCP模式，采用该方法可以减少应用日志的产生。

风险说明

将HTTP/HTTPS模式的负载均衡修改为TCP模式后，负载均衡将只检查监听端口状态，不检查HTTP状态，会导致负载均衡无法实时获知HTTP应用是否出现问题。

操作步骤

1. 登录负载均衡管理控制台。
2. 在**实例管理**页面中找到对应的负载均衡实例，单击实例ID。
3. 在**监听**页签下，找到对应监听，单击**配置**。
4. 在**配置监听**对话框中单击**下一步**，再单击**下一步**，进入健康检查配置。
5. 将**健康检查协议**修改为**TCP**。

6. 单击**下一步**至**确定**，完成修改。

关闭健康检查页面的应用日志

在业务站点之外，独立配置健康检查站点，并关闭健康检查页面的应用日志，可以减少健康检查日志的数量。例如业务站点为example.aliyundoc.com，则使用demo.aliyundoc.com作为健康检查站点，并关闭demo.aliyundoc.com站点的日志记录。

风险说明

如果健康检查的站点正常，但是业务站点出现异常时，健康检查则无法检测到业务站点的异常。

操作步骤

1. 在后端服务器上新建一个健康检查站点和健康检查页面，并关闭日志记录。本操作以nginx为例进行说明。

```
server
        {
                listen       80;
                server_name test.123.com;
                index index.php index.html index.htm default.html default.htm default.php;
                root  /home/test.123.com;
        access_log off;
        }
~
```

2. 登录负载均衡管理控制台。
3. 在**实例管理**页面中找到对应的负载均衡实例，单击实例ID。
4. 在击**监听**页签下，找到对应监听，单击**操作**列的**配置**。
5. 在**配置监听**对话框中单击**下一步**，再单击**下一步**，进入健康检查配置。

6. 在**健康检查域名（可选）**中输入健康检查站点的域名，在**健康检查路径**中输入健康检查页面的相对路径。

7. 单击**下一步**至**确定**，完成修改。

4.如何排查ECS实例异常

在负载均衡服务中开启健康检查功能后，当后端某个ECS健康检查出现问题时，会将请求转发到其他健康检查正常的ECS上。当该ECS恢复正常运行时，负载均衡会将其自动恢复到对外或对内的服务中。

针对七层负载均衡服务，当监听获取到健康检查异常的信息时，可以从以下方面对ECS实例进行健康排查：

- 确保您能够直接通过ECS访问到您的应用服务。
- 确保后端服务器开启了相应的端口，该端口必须与您在负载均衡监听配置中配置的后端端口保持一致。
- 检查后端ECS内部是否开启了防火墙或其他的安全类防护软件，这类软件很容易将负载均衡服务的本地 IP 地址屏蔽掉，导致负载均衡服务无法跟后端服务器进行通讯。
- 检查负载均衡健康检查参数设置是否正确，建议参照缺省提供的健康检查参数进行设置。
- 建议使用静态页面来进行健康检查，如果您用于健康检查的页面在后端ECS应用服务器上并不是缺省首页，需要您在健康检查配置中指定该页面的URL。健康检查指定的检测文件，建议是html形式的简单页面，只用于检查返回结果，不建议用php等动态脚本语言。
- 检查后端ECS资源是否有较高负载，降低了ECS对外提供服务的响应速度。

另外，由于七层负载均衡服务跟后端ECS之间通过内网通讯，因此需要ECS监听内网或者全网端口。您可使用以下方法进行检查：

1. 检查监听功能是否正常。

   假设负载均衡前端端口是80，ECS后端端口也是80，ECS内网IP是10.11.192.1。在服务器上运行以下命令，如果能看到10.11.192.1:80的监听信息，或者0.0.0.0:80的监听信息，说明这部分端口的监听正常。

   - Windows 服务器上运行：`netstat -ano | findstr :80`
   - Linux 服务器上运行：`netstat -anp | grep :80`

2. 检查服务器内网防火墙是否放行80端口，可以暂时关闭防火墙进行测试。输入以下命令关闭防火墙。
   - Windows：`firewall.cpl`
   - Linux：`/etc/init.d/iptables stop`
3. 检查后端端口是否正常。
   - 对于四层负载均衡，使用telnet测试有响应即为正常。本例中使用`telnet 10.11.192.1 80`来测试。
   - 对于七层负载均衡，HTTP状态码需要是200等代表正常的状态码，检验方法如下：
     - Windows：直接在ECS上访问ECS的内网IP测试是否正常，本例中为：`http://10.11.192.1`。
     - Linux：使用`curl -I`命令查看状态是否为HTTP/1.1 200 OK，本例是：`curl -I 10.11.192.1`。

5.如何排查四层监听（TCP/UDP）健康检查异常

健康检查用于探测您的后端服务器是否处于正常工作状态，当健康检查出现异常时，通常说明您的后端服务器出现了异常，但也有可能是您的健康检查配置不正确导致，本文主要介绍对四层监听（TCP/UDP）健康检查异常进行排查的详细步骤。

操作步骤

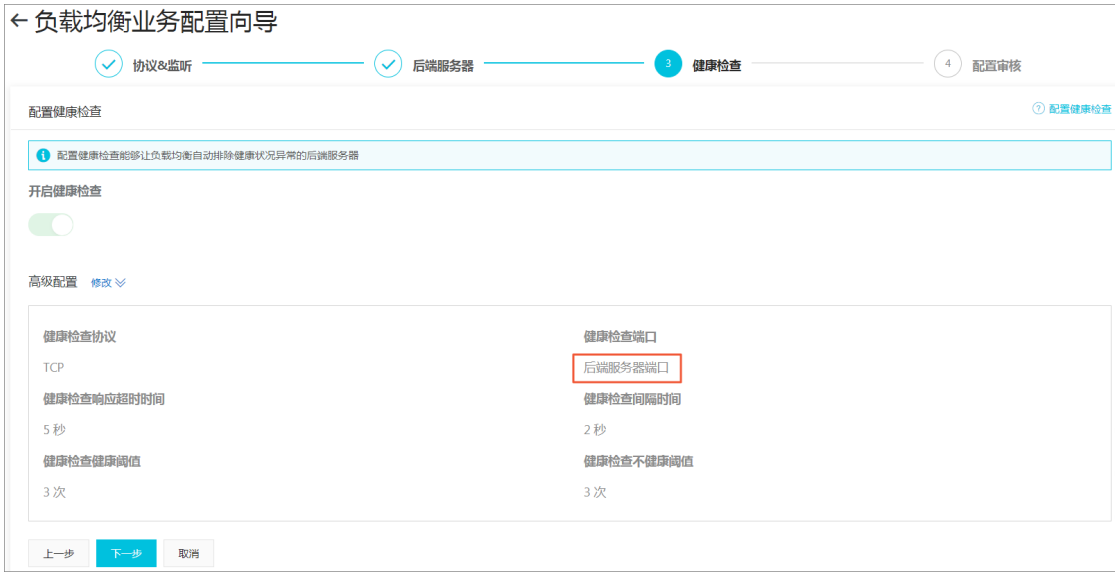
1. 确保后端服务器上没有针对100.64.0.0/10地址段进行任何形式的屏蔽，包括iptables或其他任何第三方防火墙/安全策略软件。

   负载均衡SLB通过100.64.0.0/10内部保留地址段中的IP地址与后端服务器通信，如被屏蔽则会导致健康检查异常，负载均衡无法正常工作。

2. 执行telnet命令，探测后端服务器。

   i. 登录负载均衡控制台，查看健康检查配置。

   其中，**健康检查端口**默认使用后端服务器端口，也可以手动设置端口。此处示例使用后端服务器端口，端口号为80。



ii. 执行如下命令，尝试连接健康检查端口，负载均衡上配置的健康检查端口要与后端服务器上的监听的端口保持一致。

```
telnet 172.17.58.131 80
```

此处*172.17.58.131*为后端服务器的内网IP地址，*80*为健康检查端口，如保持默认健康检查端口设置，则使用后端服务器的端口，请根据实际情况配置。

- 正常情况下，会返回类似 `Connected to xxx.xxx.xxx.xxx` 信息，表示后端服务器上指定端口处于正常工作（监听）状态，此时健康检查是正常的，如下图所示。

- 异常示例：假设负载均衡上的监听配置保持不变，但是停止后端服务器上的80端口监听进程，执行**telnet**命令后，系统提示无法连接到该主机，连接被拒绝，表示80端口监听的进程不再工作，此时健康检查会出现异常，如下图所示。

3. （可选）四层监听支持HTTP方式健康检查，如果使用HTTP方式进行健康检查，请参见如何排查七层监听（HTTP/HTTPS）健康检查异常进行排查。

6.如何排查七层监听（HTTP/HTTPS）健康检查异常

健康检查用于探测您的后端服务器是否处于正常工作状态，当健康检查出现异常时，通常说明您的后端服务器出现了异常，但也有可能是您的健康检查配置不正确导致，本文主要介绍对七层监听（HTTP/HTTPS）健康检查异常进行排查的详细步骤。

操作步骤

1. 确保后端服务器上没有针对100.64.0.0/10地址段进行任何形式的屏蔽，包括iptables或其他任何第三方防火墙/安全策略软件。

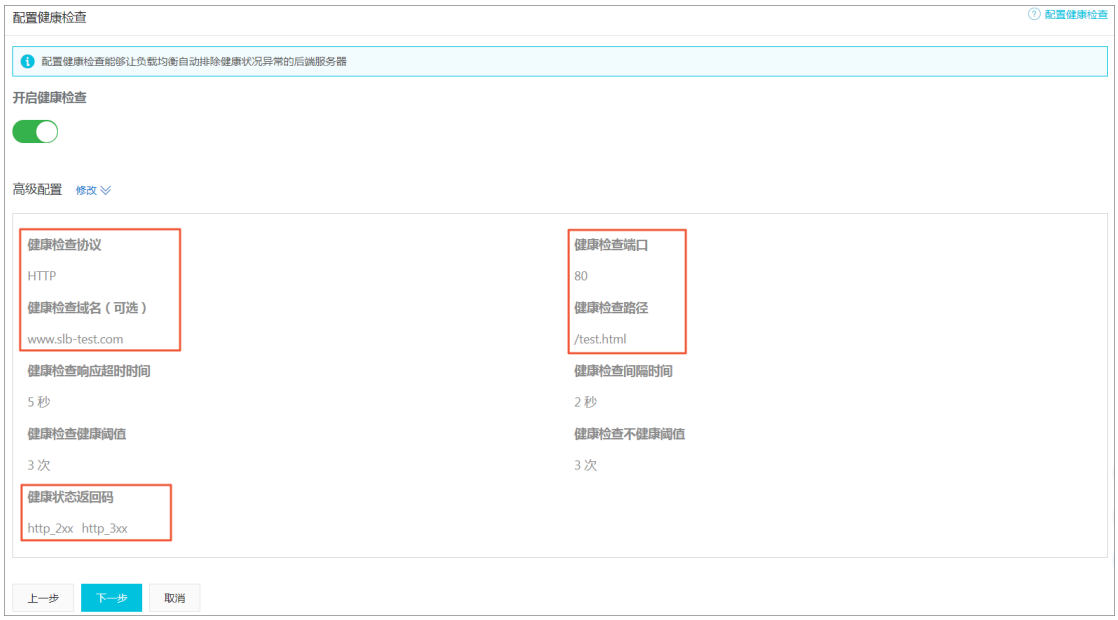
   负载均衡SLB通过100.64.0.0/10内部保留地址段中的IP地址与后端服务器通信，如被屏蔽则会导致健康检查异常，负载均衡无法正常工作。

2. 从后端服务器本地发起访问，确保后端服务器上的HTTP服务正常工作。

   i. 登录负载均衡控制台，在监听实例详情页中，查看健康检查配置。

   本次示例使用HTTP监听，出现健康检查异常的后端服务器内网IP为10.0.0.2，其他健康检查配置信息如下：

   - **健康检查端口**：80
   - **健康检查域名**：`www.slb-test.com`
   - **健康检查路径**：`/test.html`

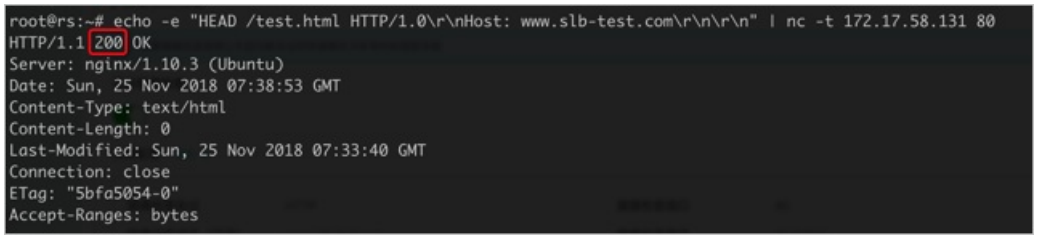


ii. 以Linux系统为例，执行nc或curl命令对后端服务器上的HTTP服务进行探测，健康检查路径、健康检查端口和健康检查域名配置必须与后端服务器上配置保持一致，否则会产生健康检查异常。

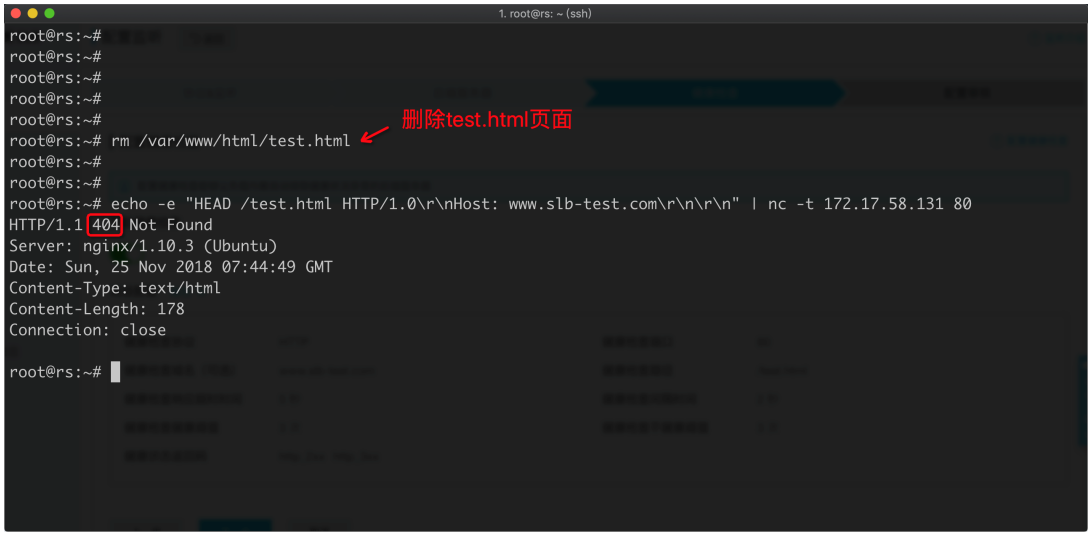
此处使用nc命令为例，请根据实际情况配置健康检查路径、健康检查域名、健康检查内网地址和健康检查端口：

```
echo -e "HEAD /test.html HTTP/1.0\r\nHost: www.slb-test.com\r\n\r\n" | nc -t 172.17
.58.131 80
```

- 正常情况下，返回 `200` 或其他 `2xx/3xx` 返回码，如下图所示。



- 异常示例：假设负载均衡上的监听配置保持不变，但是删除后端服务器上/test.html页面，执行nc命令后，得到404错误码，该错误码与负载均衡SLB监听中设置的2xx或者3xx状态码不符，此时会出现健康检查异常结果，如下图所示。



7.如何排查500/502/504错误

配置负载均衡之后，访问网站出现500 Internal Server Error、502 Bad Gateway和504 Gateway Timeout等错误，有可能由多种原因导致，例如运营商拦截、客户端异常行为导致云盾封堵、负载均衡配置错误、健康检查失败或者后端ECS Web应用访问问题。

本文档列举了此类问题的可能原因、解决方案以及排查步骤。

可能原因以及解决方案

1. 源站域名没有备案或者域名没有在高防或者安全网络中配置七层转发规则。

   解决方案：请将域名备案。如果负载均衡在高防或者安全网络中，请配置对应的域名规则。

2. 客户端源IP地址被云盾拦截。

   测试其他ISP运营商的客户端是否有相同问题，如果仅仅是某个固定运营商网络的客户端访问有问题，一般是运营商封堵导致。

   解决方案：通过提交工单反馈给阿里云售后技术支持，抓包确认是否有封堵行为。如果有，请联系运营商解决该问题。

3. 后端ECS安全防护软件阻挡。

   100.64.0.0/10（100.64.0.0/10 是阿里云保留地址，其他用户无法分配到该网段内，不会存在安全风险）是负载均衡服务器IP段，主要用于健康检查和转发请求。例如安装安全软件或者开启系统内部防火墙，可以将此IP加入白名单，避免出现500或502错误。

   解决方案：配置杀毒、防火墙软件白名单，或者卸载此类软件快速测试。

4. 后端ECS Linux内核参数配置错误。

   对于后端ECS为Linux系统，改成TCP模式时需要注意关闭系统内核参数中rp_filter相关设置。

   解决方案：将系统配置文件*/etc/sysctl.conf*的以下三个配置的值设为0，然后执行 `sysctl -p` 。

   ```
   net.ipv4.conf.default.rp_filter = 0
   net.ipv4.conf.all.rp_filter = 0
   net.ipv4.conf.eth0.rp_filter = 0
   ```

5. 后端ECS性能瓶颈。

例如CPU高，外网带宽跑满均可能导致访问异常。

解决方案：检查后端ECS性能，解决性能瓶颈问题，如果是整体系统容量不够，可以通过扩容后端ECS的数量消除问题。

6. 健康检查失败导致负载均衡出现502错误 。

   健康检查失败，请参见健康检查异常排查进行排查。

   此外，未开启负载均衡的健康检查，同时服务器中Web服务无法正常处理HTTP请求，例如Web服务未运行，也会出现502错误。

7. 健康检查正常但Web应用报502错误 。

   502 Bad Gateway错误提示表明负载均衡可以将来自客户端的请求转发到后端服务器中，但是服务器中Web应用处理异常抛出该提示，所以排错的方向是针对服务器中Web应用的配置以及运行情况进行分析。例如Web应用处理HTTP请求的时间超过了负载均衡的timeout时间。

   在七层HTTP模式下，后端对PHP请求的处理时间超过proxy_read_timeout设置的60秒，此时会出现负载均衡抛出的504 Gateway Time-out。对于四层监听，超时时间为900秒。

   解决方案：确保Web服务以及依赖正常运行，检查PHP请求处理情况，优化后端PHP请求处理。下面以Nginx+php-fpm为例进行分析说明：

   i. 处理PHP请求的进程数达到上限。

      当前服务器中PHP请求总数已经达到了php-fpm中max_children设置的上限，如果后续有新的PHP请求到达服务器中，这种情况下通常502与504的错误码会随机出现：

      - 如果已有的请求被处理完成，新请求被继续处理，一切正常。
      - 如果已有的PHP请求处理较慢，新的PHP一直处于等待状态，直至超过Nginx的fastcgi_read_timeout的值，就会出现504 Gateway timeout的错误。
      - 如果已有的PHP请求处理较慢，新的PHP处于等待状态，超过了Nginx的request_terminate_timeout的值，就会出现502 Bad Gateway的错误。

   ii. PHP脚本执行时间处理超时，即如果php-fpm处理PHP脚本的时长超过了Nginx中request_terminate_timeout设置的值，就会出现502 Bad Gateway的错误，同时在Nginx日志中可以查看到如下错误记录：

   ```
   [error] 1760#0: *251777 recv() failed (104: Connection reset by peer) while reading response header from upstream, client: xxx.xxx.xxx.xxx, server: localhost, request: "GET /timeoutmore.php HTTP/1.1", upstream: "fastcgi://127.0.0.1:9000"
   ```

   iii. 健康检查针对的是静态页面，实际处理动态请求的进程异常，例如php-fpm未启动运行。

8. HTTP头部过大。

   Head头信息过大可能导致负载均衡无法正确处理相关数据，进而引发502错误。

   解决方案：减少通过Head头传递的数据量或者换成TCP监听。

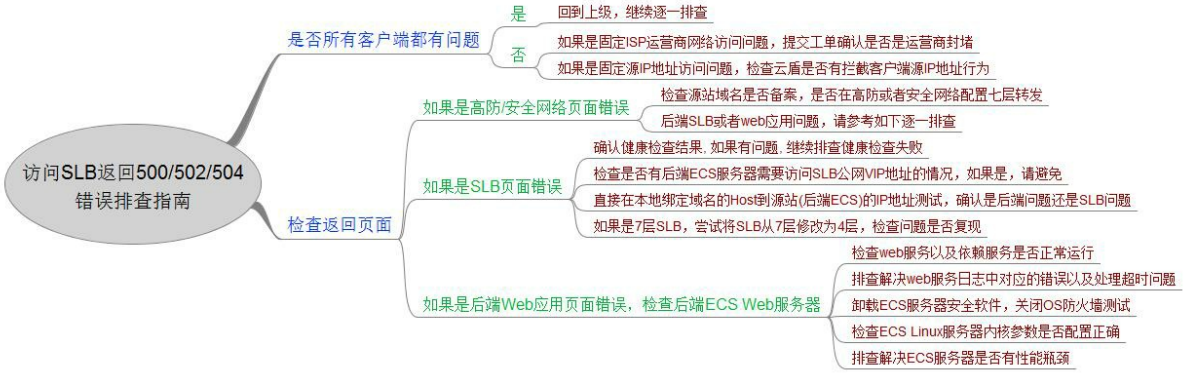
9. 业务访问逻辑问题。

   确保不存在负载均衡后端ECS实例在服务器内部通过负载均衡公网IP地址访问SLB的情况。该情况下，后端业务服务器通过负载均衡地址访问自身所监控的端口后，根据负载均衡调度策略的不同，可能会将相应的请求调度到自身服务器上。导致出现自己访问自己的情况，造成死循环，进而导致相应的请求出现500或502错误。

   解决方案：确保负载均衡场景应用正确，避免后端ECS服务器需要访问负载均衡公网IP地址的情况。

排查步骤

- 检查500/502/504错误截图，判断是负载均衡问题，高防/安全网络配置问题，还是后端ECS配置问题。
- 如果有高防/安全网络，请确认高防/安全网络的七层转发配置正确。
- 请确认是所有客户端都有问题，还仅仅是部分客户端有问题。如果仅仅是部分客户端问题，排查该客户端是否被云盾阻挡，或者负载均衡域名或者IP是否被ISP运营商拦截。
- 检查负载均衡状态，是否有后端ECS健康检查失败的情况，如果有健康检查失败，解决健康检查失败问题。
- 在客户端用hosts文件将负载均衡的服务地址绑定到后端服务器的IP地址上，确认是否是后端问题。如果5XX错误间断发生，很可能是后端某一台ECS服务器的配置问题。
- 尝试将七层负载均衡切换为四层负载均衡，查看问题是否会复现。
- 检查后端ECS服务器是否存在CPU、内存、磁盘或网络等性能瓶颈。
- 如果确认是后端服务器问题，请检查后端ECS Web服务器日志是否有相关错误，Web服务是否正常运行，确认Web访问逻辑是否有问题，卸载服务器上杀毒软件重启测试。
- 检查后端ECS Linux操作系统的TCP内核参数是否配置正确。



提交工单

请根据上述排查步骤中的指导逐条排查，详细记录排查测试结果。提交工单时，请您提供上述信息以便售后支持尽快协助您解决问题。

如果问题还未解决，请联系售后技术支持。

8.配置服务器Cookie

负载均衡服务提供会话保持功能。开启会话保持功能后，负载均衡会将会话期间内来自同一客户端的访问请求分发到同一台后端服务器上进行处理。

四层监听的会话保持是基于IP地址的会话保持，负载均衡监听器会将来自同一IP地址的请求转发到同一个后端ECS上；而七层监听是基于Cookie的会话保持。

如果您选择使用重写Cookie的方式，需要在后端服务器上配置Cookie。假如您的负载均衡服务地址下有两个域名：vip.a.com和img.a.com，当您想为vip.a.com配置会话保持时，您可以设置Cookie名称为name，然后在后端服务器上为域名vip.a.com设置key为name的Cookie。

本文档介绍了如何在Apache、Nginx和Lighttpd应用服务器上配置Cookie。

Apache

1. 打开*httpd.conf*配置文件，确保如下配置没有被注释。

```
LoadModule usertrack_module modules/mod_usertrack.so
```

2. 在virtual host中添加以下配置。

```
CookieName name
CookieExpires "1 days"
CookieStyle Cookie
CookieTracking on
```

Nginx

参考以下配置，设置Cookie。

```
server {
    listen 8080;
    server_name wqwq.example.com;
    location / {
      add_header Set-Cookie name=xxxx;
        root   html;
        index  index.html index.htm;
    }
}
```

Lighttpd

参考以下配置，设置Cookie。

```
server.modules  = ( "mod_setenv" )
$HTTP["host"] == "test.example.com" {
      server.document-root = "/var/www/html/"
      setenv.add-response-header = ( "Set-Cookie" => "name=XXXXXX"       }
}
```

9.会话保持常见问题

会话保持的作用是什么？

将同一客户端的会话请求转发给指定的一个后端服务器处理。

如何开启会话保持？

在您进行

传统型负载均衡CLB

监听配置时就可以选择是否开启会话保持。您可以针对不同的监听配置不同的会话保持策略。会话保持的最长时间是86400秒（24小时）。

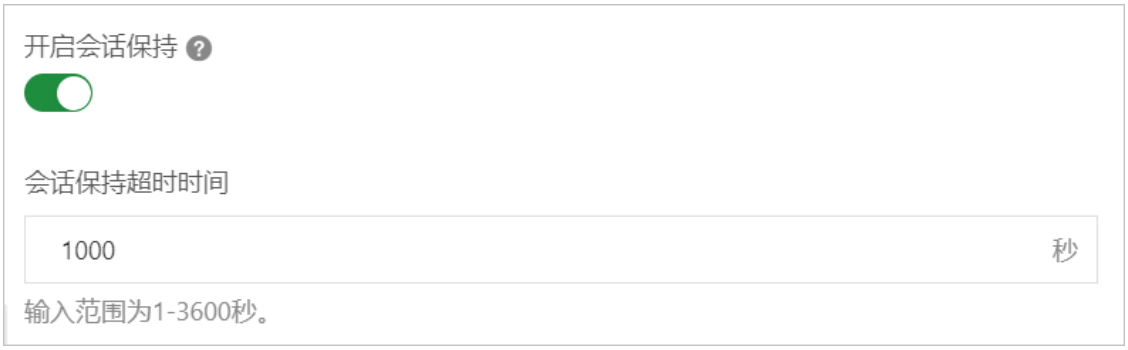
CLB

支持什么类型的会话保持？

- 四层（TCP或UDP协议）服务，

  CLB

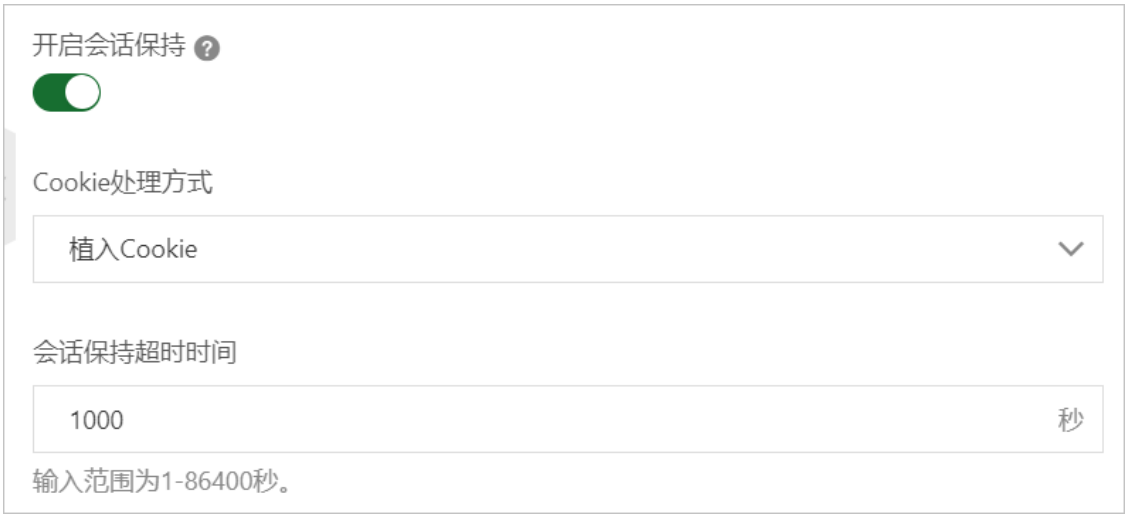
  系统是基于源IP的会话保持。四层会话保持的最长时间是3600秒。

- 七层（HTTP或HTTPS协议）服务，

  CLB

  系统是基于Cookie的会话保持。植入Cookie的会话保持的最长时间是86400秒（24小时）。



会话保持可设置哪种类型的Cookie?

HTTP/HTTPS监听可使用**植入Cookie**和**重写Cookie**来进行会话保持。

- **植入Cookie**: 此种方法下，您只需要指定Cookie的过期时间。客户端第一次访问时，

  CLB

  在返回请求中植入Cookie（即在HTTP/HTTPS响应报文中插入SERVERID字串），下次客户端携带此Cookie访问，

  CLB

  会将请求定向转发给之前记录到的ECS实例上。
- **重写Cookie**：此种方式下，您可以根据需要指定HTTPS/HTTP响应中插入的Cookie。您需要在后端ECS上维护该Cookie的过期时间和生存时间。

  CLB

  发现用户自定义了Cookie，将会对原来的Cookie进行重写，下次客户端携带新的Cookie访问，

  CLB

  会将请求定向转发给之前记录到的ECS实例上。服务器配置参考配置会话保持规则。

是否支持针对不同的域名配置不同的会话保持规则?

支持。

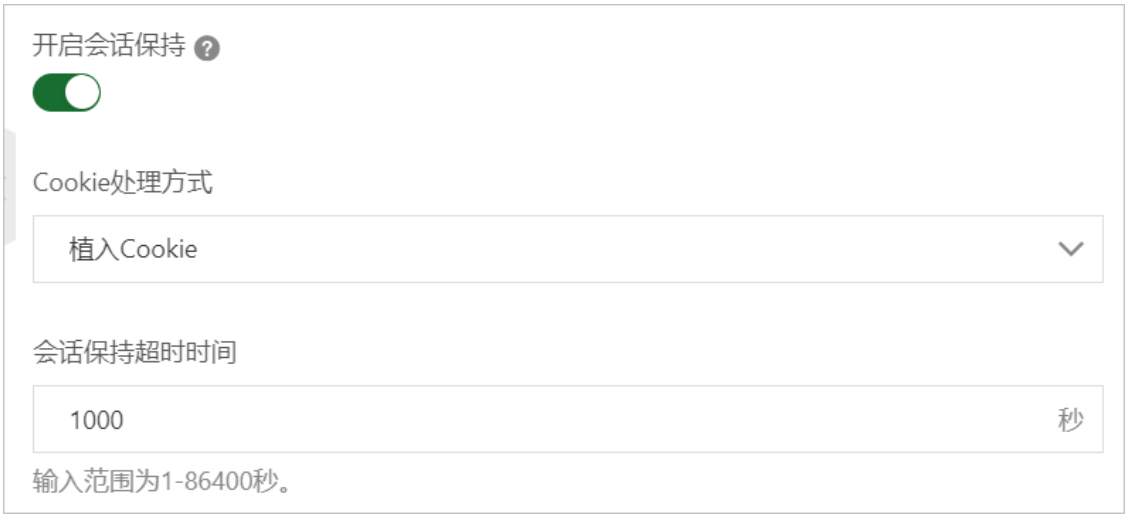
您可以通过

CLB

提供的重写Cookie的会话保持方式来实现这一需求。

Cookie的超时时间应设置为多少?

- 植入Cookie可在控制台上配置1~86400秒。



- 重写Cookie需要您在后端ECS上维护超时时间。

如何查看会话保持字符串？

可以在浏览器中用F12查看回应报文中是否含有SERVERID字符串或用户指定的关键字，或者运行 `curl www.example.com -c /tmp/cookie123` 保存一下Cookie，再用 `curl www.example.com -b /tmp/cookie123` 访问。

为什么有时候会话保持会失败？

- 查看是否在监听配置中已经开启了会话保持功能。
- HTTP或HTTPS监听在后端服务器返回4xx响应码的报文中无法插入会话保持所需Cookie。

  解决方案：改用TCP监听，因为TCP监听是以源客户端的IP来做会话保持的，另外后端ECS上也可以插入Cookie，并增加Cookie的判断来多重保障。
- 302重定向会改变会话保持中的SERVERID字串。

  负载均衡植入Cookie时，如果后端ECS中有回复302重定向的报文，将改变会话保持中的SERVERID字串，导致会话保持失效。

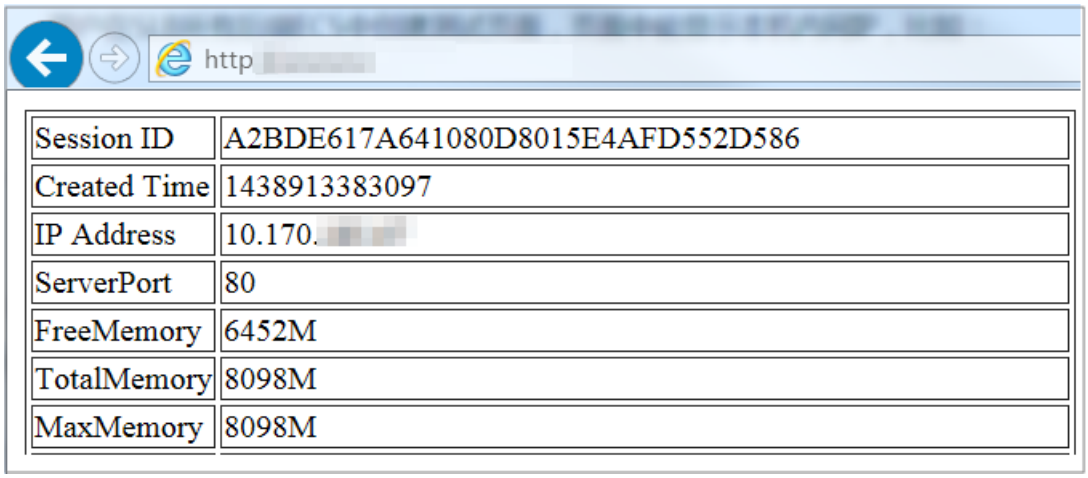
  排查方法：在浏览器端捕抓请求与响应的回复，或用抓包软件抓包后分析是否存在302的响应报文，对比前后报文的Cookie中的SERVERID字串是否不同了。

  解决方案：改用TCP监听，因为TCP监听是以源客户端的IP来做会话保持的，另外后端ECS上也可以插入Cookie，并增加Cookie的判断来多重保障。
- 会话保持时间设置过小，会话保持时间过小也会导致会话保持失败。

如何使用Linux curl测试负载均衡会话保持？

1. 创建测试页面。

   在负载均衡所有后端ECS中创建测试页面，如下图所示页面中能显示本机内网IP。内网IP用于判断相应请求被指派到的物理服务器。通过观察该IP的一致性，来判断负载均衡会话保持的有效性。



2. Linux系统内执行curl命令。

   假设负载均衡服务IP地址是 10.170.XX.XX，创建的测试页面URL为： `http://10.170.XX.XX/check.jsp` 。

   i. 登录用来测试的Linux服务器。

   ii. 执行以下命令查询负载均衡服务器Cookie值。

   ```
   curl -c test.cookie http://10.170.XX.XX/check.jsp
   ```

   > **说明** 阿里云负载均衡会话保持默认模式是植入Cookie，而curl测试默认不会保存和发送Cookie，所以必须先保存相应的Cookie，用于Cookie测试。否则，curl测试结果是随机的，会误认为负载均衡会话保持无效。

   iii. 执行以下命令持续测试。

   ```
   for ((a=1;a<=30;a++));
       do curl  -b test.cookie http://10.170.XX.XX/check.jsp  | grep '10.170.XX.XX';
       sleep 1;
   done
   ```

   > **说明** a≤30是重复测试次数，可以按需修改。 `grep '10.170.XX.XX'` 是筛选显示的IP信息，根据后端ECS内网IP情况进行相应修改。

   iv. 观察上述测试返回的IP，如果是同一台ECS内网IP，则证明负载均衡会话保持有效；反之则证明负载均衡会话保持有问题。