ALIBABA CLOUD

阿里云

负载均衡

通用配置

文档版本：20220401

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.WebSocket和WebSocket Secure协议概述 05
2.API Inspector 07
3.结合全局流量管理实现跨地域负载均衡 09
4.DDoS原生防护（基础版） 14

1.WebSocket和WebSocket Secure协议概述

WebSocket（WS）和WebSocket Secure（WSS）协议概述

本文介绍WebSocket和WebSocket Secure协议相关的简介。

什么是WebSocket?

WebSocket是HTML5一种新的协议，它实现了浏览器与服务器全双工（full-duplex）通信，能更好地节省服务器资源和带宽并达到实时通讯。WebSocket建立在TCP之上，同HTTP一样通过TCP来传输数据，但是它和HTTP最大不同是：WebSocket是一种双向通信协议，在建立连接后，WebSocket服务器和Browser/Client Agent都能主动地向对方发送或接收数据，就像Socket一样；WebSocket需要类似TCP的客户端和服务器端通过握手连接，连接成功后才能相互通信。

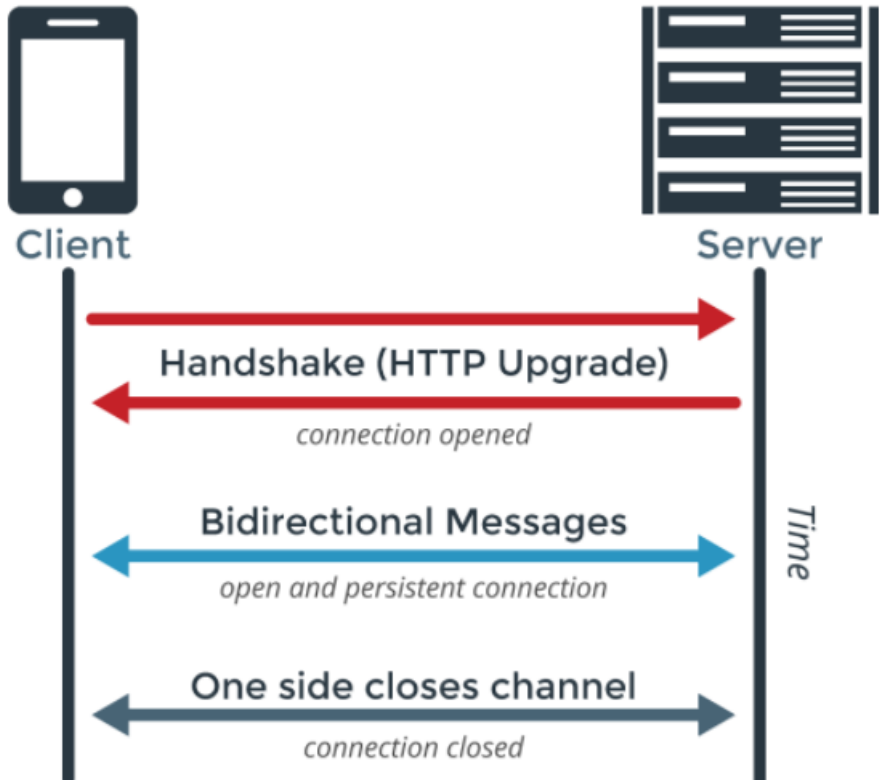
WebSocket Secure是WebSocket的加密版本。

为何使用WebSocket?

随着互联网的蓬勃发展，各种类型的Web应用层出不穷，很多应用要求服务端有能力进行实时推送（例如直播间聊天室），以往很多网站为了实现推送技术，所用的技术都是轮询。轮询是在特定的时间间隔（如每1秒），由浏览器对服务器发出HTTP请求，然后由服务器返回最新的数据给客户端的浏览器。这种传统的模式带来很明显的缺点，即浏览器需要不断地向服务器发出请求，然而HTTP请求可能包含较长的头部，其中真正有效的数据可能只是很小的一部分，显然这样会浪费很多的带宽资源。

在这种情况下，HTML5定义了WebSocket协议，能更好地节省服务器资源和带宽，并且能够更实时地进行通讯。WebSocket实现了浏览器与服务器全双工通信，允许服务器主动发送信息给客户端。

WebSocket协议的交互过程如下图所示。



如何在阿里云负载均衡上启用WebSocket和WebSocket Secure支持？

性能保障型实例无需配置。

- HTTP监听默认支持WebSocket协议。
- HTTPS监听默认支持WebSocket Secure协议。

> **说明** 性能共享型实例需要升级为性能保障型实例才能支持WebSocket和WebSocket Secure。更多信息，请参见 性能保障型实例FAQ。

支持的地域

全部地域都已开放WebSocket和WebSocket Secure支持。

相关计费

WebSocket和WebSocket Secure协议不额外收取费用。

使用限制

WebSocket和WebSocket Secure协议的使用限制如下：

- 若负载均衡与ECS后端服务的连接采用HTTP/1.1，建议后端服务器采用支持HTTP/1.1的Web Server。
- 若负载均衡与后端服务超过60秒无消息交互，会主动断开连接，如需要维持连接一直不中断，需要主动实现保活机制，每60秒内进行一次报文交互。

2.API Inspector

API Inspector是一个实验性的功能，旨在让用户查看控制台的每一步操作背后的API调用，并自动生成各语言版本的API代码，可通过Cloud Shell和API Explorer在线调试。

功能特点

API Inspector与API Explorer、Cloud Shell集成到一起，构成阿里云用户学习和调试API的一体化解决方案，具有以下特性：

- 自动录制：根据您需要的功能，在控制台操作相应的功能即可获得相关API调用。更多信息，请参见自动录制功能。
- 一键生成：自动生成各语种的API代码片段参数预填充，可直接运行。更多信息，请参见一键生成API代码。
- 在线调试：结合API Explorer、Cloud Shell一键在线调试，免开发环境搭建。更多信息，请参见API Explorer在线调试和Cloud Shell在线调试。

开启API Inspector功能

完成以下操作，开启API Inspector功能：

1. 登录负载均衡管理控制台。
2. 单击页面右下角的  。

自动录制功能

此处以修改负载均衡实例名称为例，演示API Inspector的自动录制功能。

1. 单击实例ID，选择**实例详情**页签。
2. 在实例**基本信息**中单击**编辑**，修改实例名称。
3. 单击**确定**，完成实例名称修改。
4. 单击页面右侧的  ，可以看到上述操作所调用的API。

   您可以勾选**隐藏Describe类接口**，查看功能核心接口。

一键生成API代码

控制台操作的功能调用的API录制完成后，单击API名称，一键生成Python、Java、Go、Node.js、PHP和CLI格式的API代码片段参数预填充。

> **说明** 单击  复制对应格式的代码段，可直接运行。

API Explorer在线调试

控制台操作的功能调用的API录制完成后，单击**前往OpenApi平台**，可以转到OpenAPI开发者门户调试对应的功能。

> **说明** 单击 查看文档，可以查看调用API的详细参数设置信息。

Cloud Shell在线调试

控制台操作的功能调用的API录制完成后，展开调用API详情后，单击，可以使用Cloud Shell一键在线调试功能。

> **说明** 使用Cloud Shell一键调试功能，推荐关联并创建一个OSS Bucket保存您常用脚本和文件，但会产生少量的OSS使用费用。也可以选择暂不创建。

负载均衡使用Cloud Shell调试功能的云命令行格式如下：

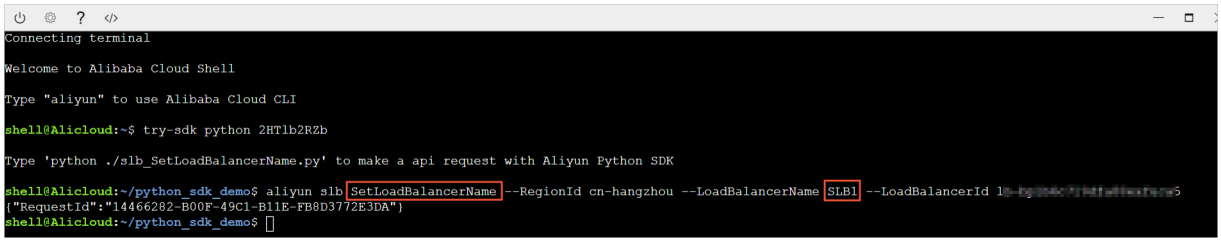
```
aliyun slb actionName --parameter1value1 --paramter2value2...
```

如本次示例中调用的SetLoadBalancerName接口修改负载均衡实例名称为SLB1，运行的云命令行为：

```
aliyun slb SetLoadBalancerName --RegionId cn-hangzhou --LoadBalancerName SLB1 --LoadBalance
rId lb-bp1b6c719dfa08exfuca5
```

返回值为：

```
{"RequestId":"14466282-B00F-49C1-B11E-FB8D3772E3DA"}
```



3.结合全局流量管理实现跨地域负载均衡

结合全局流量管理，您可在本地负载均衡上层部署全局流量管理，实现跨地域容灾、不同地域访问加速和智能解析。

全局流量管理

负载均衡从其应用的地理结构上分为本地负载均衡和全局负载均衡。本地负载均衡是指对同地域的服务器群做负载均衡，全局负载均衡是指对分别部署在不同地域有不同网络结构的服务器群做负载均衡。

- 多线路智能化解析服务

  全局流量管理利用DNS智能解析和应用服务的运行状态健康检查，将用户访问定向到最合适的IP地址，使访问用户获得最快捷、最流畅的体验。

- 跨地域容灾

  全局流量支持将不同地域的IP地址添加到不同的地址池，并配置健康检查。在访问策略配置中，设置默认地址池为**地址池甲**，Failover地址池为**地址池乙**，即可以实现应用服务主备IP容灾切换。

- 不同地域访问加速

  使用全局流量管理，可以使不同地域的用户访问不同的IP地址池，实现用户分组管理，分组接入，帮助应用服务提高用户访问体验。

部署全局流量管理

本操作以一个域名为aliyundoc.com的网站为例（该网站的大多数用户分布在新加坡和中国内地），指导您如何通过全局流量管理和负载均衡实现全局负载均衡。

步骤一：购买与配置云服务器

根据您的应用服务的用户的地域分布，在相应地域下购买并配置至少两台ECS。

本操作中，在北京、深圳、新加坡这三个地域分别购买了两台ECS，并在ECS上搭建了一个简单的静态网页。

- 北京地域ECS示例
- 深圳地域ECS示例
- 新加坡地域ECS示例

步骤二：购买与配置负载均衡实例

1. 请参见创建实例，分别在北京、深圳和新加坡创建一个公网负载均衡实例。
2. 请参见配置实例，添加监听并将各个地域下配置好的ECS添加到后端服务器池。

- 北京地域负载均衡实例示例
- 深圳地域负载均衡实例示例
- 新加坡地域负载均衡实例示例

步骤三：配置全局流量管理

1. 购买全局流量管理实例。
   i. 登录云解析DNS管理控制台。
   ii. 在左侧导航栏，单击**全局流量管理**。
   iii. 在**全局流量管理**页面，单击**创建实例**。

iv. 选择套餐版本、购买数量和购买时长。

v. 单击**立即购买**。

购买成功后，系统会自动分配一个CNAME接入域名。

2. 配置全局流量实例。

i. 在**全局流量管理**页面，单击全局流量实例ID或者**操作**列的**配置**。

ii. 在左侧导航栏，单击**配置管理**。

iii. 在**全局管理**页签下，单击**修改**，配置全局管理实例参数。

设置以下参数，其他保持默认值。

- 实例名称：用于识别该实例用于某个应用服务的标识。
- 主域名：主域名是用户访问应用服务使用的域名，本操作中设置为aliyundoc.com。
- 报警通知组：选择全局流量管理服务发生异常时，通知消息发送的对象，自动读取您在云监控产品中创建的报警人联系组。

iv. 单击**确认**。

3. 配置地址池。

i. 在**地址池配置**页签下，单击**新增地址池**。

ii. 在**新增地址池**页面，配置地址池。

本操作中需要添加三个地址池，将三个不同地负载均衡实例地址分别放到三个地址池中。

- 地址池名称：自定义，例如华北_北京、华东_杭州、新加坡。
- 地址：加入该地域的负载均衡实例的公网地址。

iii. 单击**确认**。

4. 配置健康检查。

   本次操作，需要对三个地址池分别进行健康检查配置。

   i. 在**地址池**页签下，单击健康检查后的**修改**。

   ii. 配置健康检查参数。

   其中，**选择监控节点**表示监控节点的位置信息，不同的地域的地址池选择对应的监控节点。

5. 配置访问策略。

   本次操作，需要对三个不同地域添加不同的访问策略。

   i. 在**访问策略**页签下，单击**新增访问策略**。

ii. 在**新增访问策略**页面，配置访问策略。

- 不同访问地域的默认地址池，Failover地址池可以设置为其他区域的地址池。
- 选择访问地域的用户访问应用服务时，匹配该访问策略访问配置的对应地址池。

  必须有一个访问策略中地域选择**全局**，否则，可能会造成部分地区无法访问该应用服务。

6. 配置CNAME接入。
   i. 登录云解析DNS控制台。
   ii. 单击aliyundoc.com域名**操作**列的**解析设置**。
   iii. 在**解析设置**页面，单击**添加记录**。
   iv. 在**添加记录**页面，将最终用户访问的aliyundoc.com域名通过CNAME的形式指向全局流量管理实例的别名记录。

v. 单击**确认**。

步骤四：测试

移除北京地域负载均衡实例的后端服务器，使该负载均衡实例的服务不可用。

访问该网站，查看访问是否正常。

> **说明** 全局流量管理监控到您的IP宕机后需要1~2分钟聚合判断，假设您的监控频率设置是1分钟，那么线路异常切换生效时间在2~3分钟内。

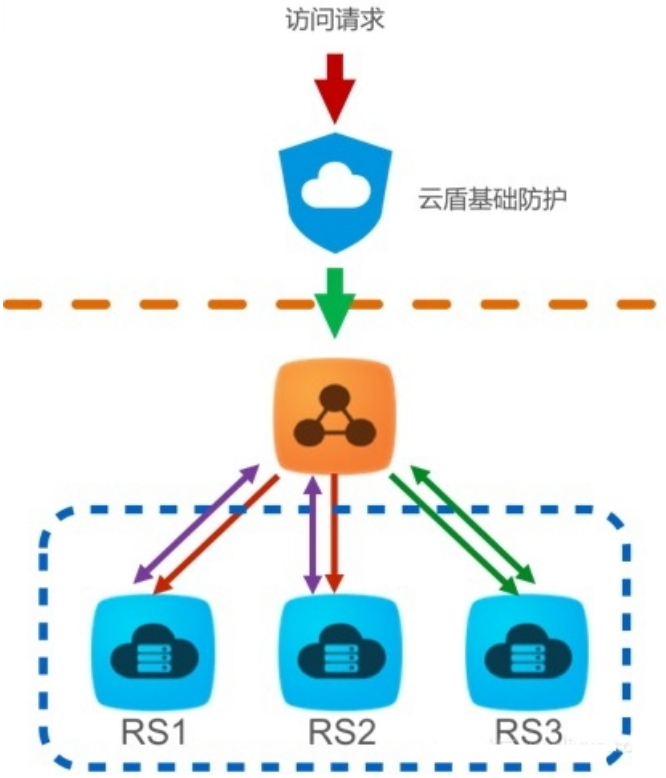
4.DDoS原生防护（基础版）

DDoS原生防护是一款针对阿里云ECS、CLB、Web应用防火墙、EIP等产品直接提升DDoS防御能力的安全产品，直接把防御能力加载到云产品上，不需要更换IP，也没有四层端口和七层域名数等限制。

DDoS原生防护（基础版）介绍

DDoS原生防护（基础版）默认为CLB等阿里云公网IP资源免费开启，提供最高5 Gbps的DDoS原生防护（基础版）。所有来自互联网的流量都要先经过云盾再到达负载均衡， 云盾会清洗过滤常见的攻击 ，例如SYN Flood、UDP Flood、ACK Flood、ICMP Flood和DNS Flood等DDoS攻击 。

DDoS原生防护采用被动清洗方式为主、主动压制为辅的方式，针对DDoS攻击在反向探测、黑白名单、报文合规等标准技术的基础上，保证被防护用户在攻击持续状态下，仍可对外提供业务服务。网络拓扑架构如下图所示。



DDoS原生防护（基础版）根据公网CLB实例的带宽设定清洗阈值和黑洞阈值。当入方向流量达到阈值上限时，触发清洗和黑洞：

- 清洗：当来自互联网的攻击流量较大或符合某些特定攻击流量模型特征时，云盾将会自动对攻击流量进行清洗，清洗包括攻击报文过滤、流量限速、包限速等。
- 黑洞：当来自互联网的攻击流量非常大时，为保护整个集群的安全，流量将会被黑洞处理，即所有入流量全部被丢弃。

阈值的计算遵循以下两个原则：

- 根据 CLB实例 所购买的带宽（ 即CLB的出方向带宽 ）来决定阈值的高低。当实例的带宽较高时， 阈值 较高；当实例的带宽较低时，阈值相应 地 会变低。
- 根据您的 安全信誉分 来决定黑洞阈值的高低。

> **说明** 安全信誉分仅影响黑洞阈值，不影响清洗阈值。

计算阈值

按照以下步骤计算阈值。

1. CLB后台根据 您 购买的带宽给出能够满足实例正常工作的阈值建议值。

   > **说明** 如果您购买的是按流量计费实例，出带宽为实例所在地域所支持的带宽峰值上限。目前中国内地地域带宽上限都是峰值5 Gbps。详情参见 带宽峰值限制。

   - CLB带宽与 BPS 清洗阈值之间的关系
     - 当CLB带宽<100 Mbps时，清洗BPS默认阈值 = 120 Mbps。
     - 当CLB带宽>100 Mbps时，清洗BPS默认阈值=带宽值*1.2。
   - CLB带宽与 PPS 清洗阈值之间的关系

     清洗PPS阈值=（CLB带宽值/500）*150000

     带宽值单位为Mbps。
   - CLB带宽与黑洞BPS阈值之间的关系
     - 当CLB带宽<1 Gbps时，黑洞BPS默认阈值=2 Gbps。
     - 当CLB带宽>1 Gbps时，黑洞BPS默认阈值=MAX(CLB带宽值*1.5,2G)。
2. 云盾根据CLB给出的建议值，结合您 安全信誉分 和各地域的资源情况，计算出最终的阈值。
   - 云盾评估BPS和PPS阈值的规则。

     BPS最小值为1000 M，PPS最小值为30万个。
     - 当CLB传入的参考阈值小于上述最小值时，取上述最小值。
     - 当CLB传入的参考阈值高于上述最小值时，取CLB传入的参考阈值。
   - 云盾根据您的安全信誉分来决定黑洞阈值的高低。

授权云盾基础防护只读权限

按照以下步骤 为RAM账号授予云盾DDoS原生防护（基础版）Anti-DDoS Basic的只读权限。

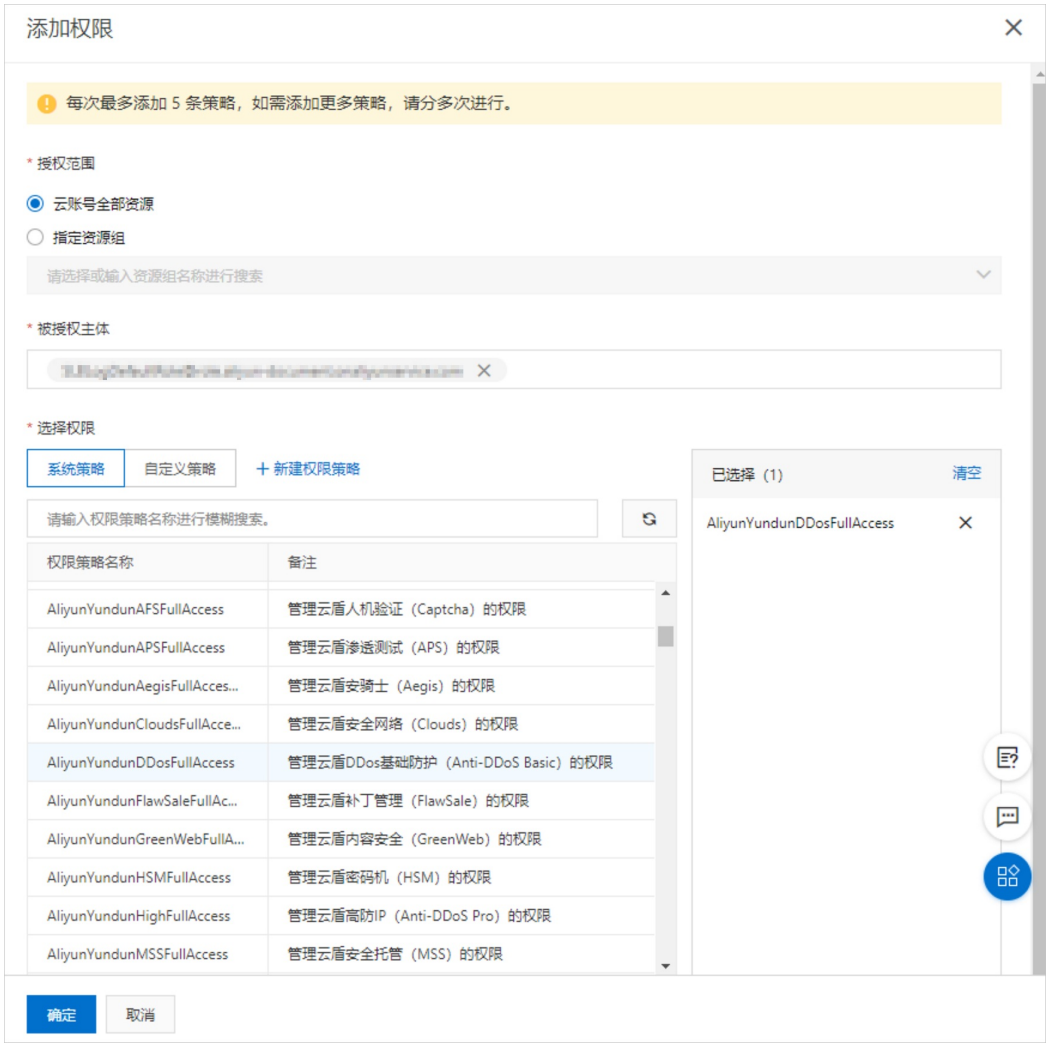
> **说明** 使用主账号进行授权。

1. 使用主账号登录RAM访问控制台。
2. 在左侧导航栏，单击**身份管理 > 用户**。
3. 在**用户**页面，找到目标RAM用户，然后在**操作**列单击**添加权限**。
4. 在**添加权限**面板，为RAM角色添加权限。
   i. 选择授权应用范围。
      - **整个云账号**：权限在当前阿里云账号内生效。
      - **指定资源组**：权限在指定的资源组内生效。

   ii. 输入授权主体。

   iii. 选择权限策略。

   单击**系统策略**页签，选择**权限策略名称**列中的AliyunYundunDDosFullAccess，将其加入到已选择的权限策略列表中，然后单击**确定**。



查看防护阈值

1. 登录传统型负载均衡CLB控制台。
2. 在顶部菜单栏，选择

   CLB

   实例的所属地域。
3. 在**实例管理**页面，找到目标

   CLB

   实例，将鼠标移至目标实例的云盾图标，查看BPS清洗阈值、PPS清洗阈值和黑洞阈值。更多信息，请参见详情请见云盾DDoS防护控制台。

- BPS清洗阈值：入方向流量超过了BPS清洗阈值时，触发清洗。
- PPS清洗阈值：入方向数据包数超过了PPS清洗阈值时，触发清洗。
- 黑洞阈值：入方向流量超过黑洞阈值时将触发黑洞。