阿里云
负载均衡

用户指南

文档版本：20190218

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

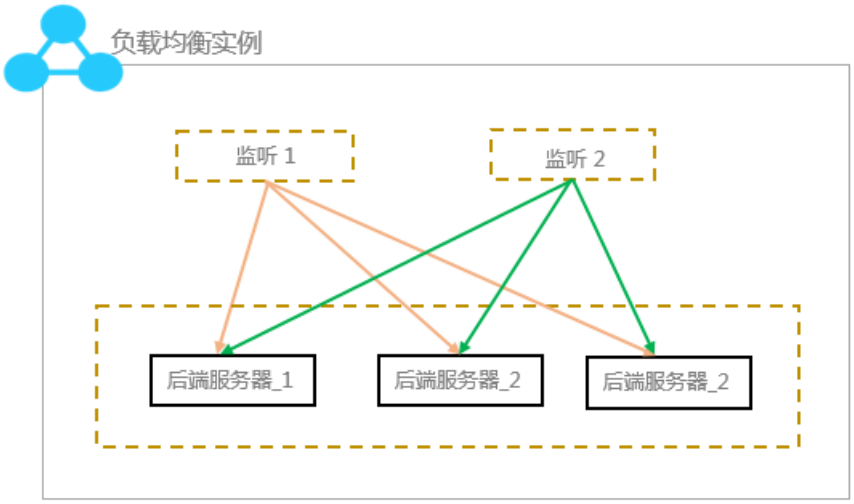
格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 确定。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	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。	`swich` *`{stand | slave}`*

目录

1 负载均衡实例

1.1 什么是负载均衡实例

负载均衡实例是一个运行的负载均衡服务实体。使用负载均衡服务，您必须创建一个负载均衡实例，在实例中添加监听和后端服务器。



阿里云提供公网和私网两种类型的负载均衡服务。您可以根据业务场景选择配置对外公开或对内私有的负载均衡，系统会根据您的选择分配公网或私网服务地址。

公网负载均衡实例

公网类型的负载均衡实例可以通过Internet将客户端请求按照您制定的监听规则分发到添加的后端服务器ECS上。

在您创建公网负载均衡实例后，系统会为其分配一个公网服务地址，您可以将您的域名和该公网服务地址进行绑定，对外提供服务。

私网负载均衡实例

私网类型的负载均衡实例只能在阿里云内部使用，可以转发的请求只能来自具有负载均衡的私网访问权限的客户端。

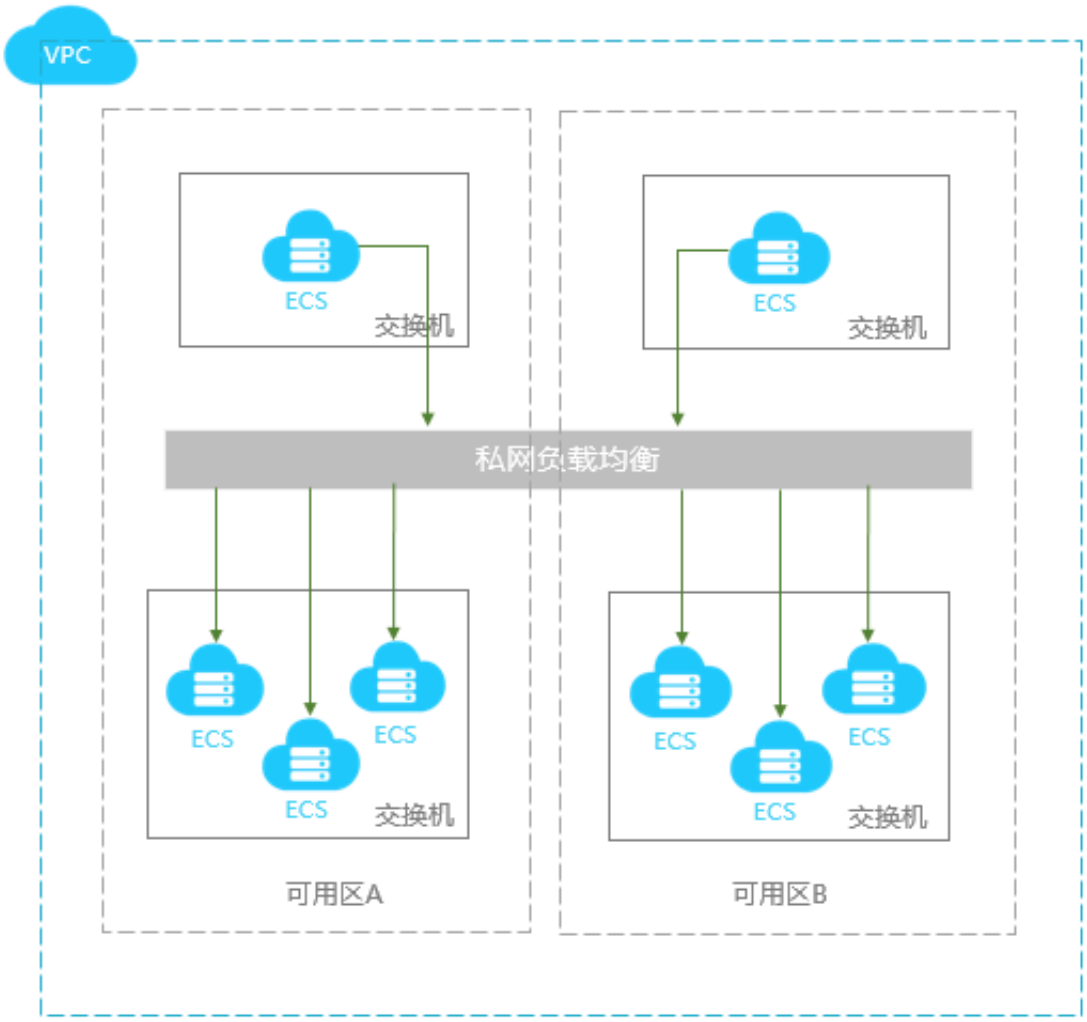
私网负载均衡实例可以进一步对网络类型进行选择：

- 经典网络

  如果您选择的私网负载均衡实例的网络类型是经典网络，那么您的私网负载均衡实例的服务地址由阿里云统一分配和管理。该私网负载均衡服务只能被经典网络ECS实例访问。

- 专有网络

  如果您选择的私网负载均衡实例的网络类型是专有网络，那么您的私网负载均衡实例的服务地址会从您指定的专有网络的交换机网段内分配。该私网负载均衡服务只能被相同VPC内的ECS实例访问。



1.2 性能保障型实例

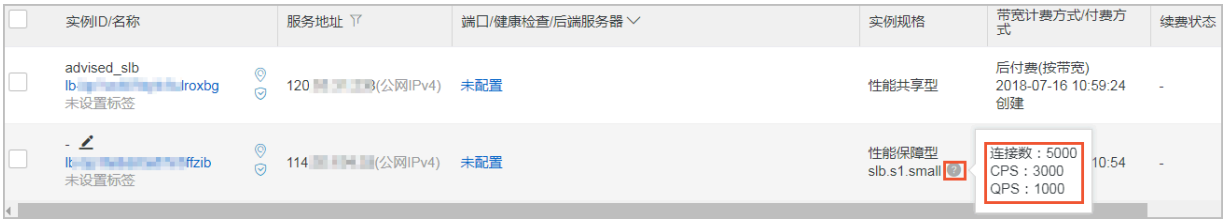
阿里云负载均衡计划将于2018年4月1日开始针对性能保障型实例收取规格费，同时继续保留性能共享型实例的售卖。

1. 什么是负载均衡性能保障型实例?

负载均衡性能保障型实例提供了可保障的性能指标。与之相对的是负载均衡性能共享型实例，资源是所有实例共享的，所以不保障实例的性能指标。

在推出负载均衡性能保障型实例之前，您所有购买的实例均为性能共享型实例。在控制台上，您可以查看已购实例的类型。

把鼠标移至性能保障型实例的问号图标，可查看具体的性能指标，如下图所示。



性能保障型实例的三个关键指标如下：

- 最大连接数-Max Connection

  最大连接数定义了一个负载均衡实例能够承载的最大连接数量。当实例上的连接超过规格定义的最大连接数时，新建连接请求将被丢弃。

- 每秒新建连接数-Connection Per Second (CPS)

  每秒新建连接数定义了新建连接的速率。当新建连接的速率超过规格定义的每秒新建连接数时，新建连接请求将被丢弃。

- 每秒查询数-Query Per Second (QPS)

  每秒请求数是七层监听特有的概念，指的是每秒可以完成的HTTP/HTTPS的查询（请求）的数量。当请求速率超过规格所定义的每秒查询数时，新建连接请求将被丢弃。

阿里云负载均衡性能保障型实例开放了如下六种实例规格（各地域因资源情况不同，开放的规格可能略有差异，请以控制台购买页为准）。

规格	规格	最大连接数	每秒新建连接数 (CPS)	每秒查询数(QPS)
规格 1	简约型I (slb.s1.small)	5,000	3,000	1,000
规格 2	标准型I (slb.s2.small)	50,000	5,000	5,000
规格 3	标准型II (slb.s2.medium)	100,000	10,000	10,000
规格 4	高阶型I (slb.s3.small)	200,000	20,000	20,000
规格 5	高阶型II (slb.s3.medium)	500,000	50,000	30,000
规格 6	超强型I (slb.s3.large)	1,000,000	100,000	50,000

如果需要更大规格，请联系您的客户经理申请。

2. 性能保障型实例如何收费?

负载均衡性能保障型实例需要收取规格费用，收费模型如下:

性能保障型费用 = 实例费 + 流量/带宽费 + 规格费

说明:

负载均衡私网实例也可以选择性能共享型实例或性能保障型实例，性能保障型私网实例，也需要收取规格费用，收费方式与公网性能保障型实例一致，但不收取流量费/带宽费和实例费。

负载均衡分为两种计费模式，预付费和按量付费。在不同的计费模式下，性能保障型实例的规格费收取规则不同:

- 预付费模式

  性能保障型实例规格费按照预付费模式收取，即在实例的付费周期内，实例规格费按照固定的价格收取。假设您选择的是高阶型I (slb.s3.small)规格，并且选择购买时长为3个月， 则规格费用 = slb.s3.small规格费月价 x 3月。

- 按量付费模式

  性能保障型实例规格费按使用量收取，即不论您选择的何种规格，实例规格规格费均会按照您实际使用的规格收取。

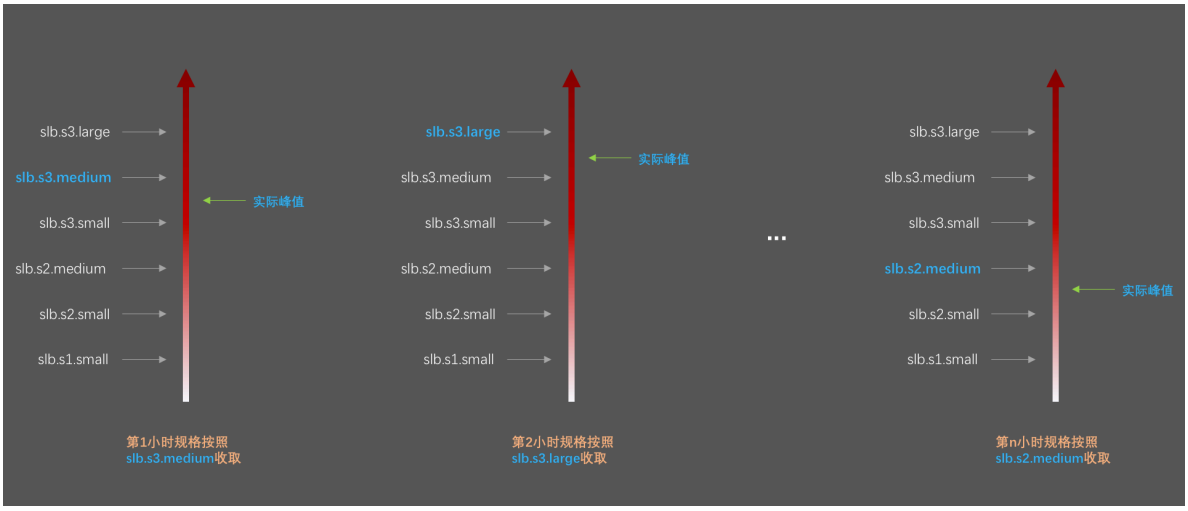
  例如，您选择了超强型I (slb.s3.large)规格（最大连接数1,000,000；CPS 500,000；QPS 50,000）。您的实例在某个小时内各项指标产生的实际峰值如下:

最大连接数	每秒新建连接数（CPS）	每秒查询数 （QPS）
90000	4000	11000

  - 从最大连接数维度看，90,000超过slb.s2.small规格中最大连接数50,000的上限，但未达到slb.s2.medium规格中最大连接数的100,000上限，因此从最大连接数维度计算，该小时规格为slb.s2.medium。
  - 从每秒新建连接数（CPS）维度看，4,000超过slb.s1.small规格中CPS 3,000的上限，但未到达slb.s2.small规格中CPS 5,000的上限，因此从CPS维度计算，该小时规格为slb.s2.small。
  - 从每秒查询数（QPS）维度看，11,000超过slb.s2.medium规格中QPS 10,000的上限，但未达到slb.s3.small中QPS 20,000的上限，因此从QPS维度计算，该小时规格为slb.s3.small。

    综合以上三个维度，QPS指标的规格（slb.s3.small）最大，因此将QPS维度的规格作为该小时实例的综合规格，该小时内该实例将按照slb.s3.small规格进行计费。

以后每小时规格费均按照上述方式计算，如下图所示：



因此，按量付费的性能保障型实例具有自动弹性伸缩（或计费）的能力。您在购买时所选的规格，是性能的上限，比如您选择高阶型II (slb.s3.medium)，那么意味着，您的实例最大可以达到的规格上限就是高阶型II (slb.s3.medium)。

3. 性能保障型实例规格费的定价

下表中所列的只是规格费用。除规格费以外，负载均衡实例的实例费和流量/带宽费正常收取。更多详细信息，参考计费说明。

地域	规格	规格	最大连接数	每秒新建连接数 (CPS)	每秒查询数(QPS)	包年包月(元/月)	按量付费(元/时)
华东1（杭州） 华北3（张家口） 华北5（呼和浩特） 华北1（青岛） 华北2（北京） 华东2（上海） 华南1（深圳）	规格 1	简约型I (slb.s1.small)	5,000	3,000	1,000	免费	免费
	规格 2	标准型I (slb.s2.small)	50,000	5,000	5,000	190.00	0.32
	规格 3	标准型II (slb.s2.medium)	100,000	10,000	10,000	380.00	0.63
	规格 4	高阶型I (slb.s3.small)	200,000	20,000	20,000	760.00	1.27
	规格 5	高阶型II (slb.s3.medium)	500,000	50,000	30,000	1,143.00	1.91

地域	规格	规格	最大连接数	每秒新建连接数 (CPS)	每秒查询数(QPS)	包年包月(元/月)	按量付费(元/时)
	规格 6	超强型I (slb.s3.large)	1,000,000	100,000	50,000	1,908.00	3.18
亚太东南1（新加坡） 亚太东南3（吉隆坡） 亚太东南5（雅加达） 亚太南部1（孟买） 美国西部1（硅谷） 美国东部1（弗吉尼亚） 香港 亚太东北1（东京） 亚太东南1（悉尼） 中东东部1（迪拜） 欧洲中部1（法兰克福） 英国（伦敦）	规格 1	简约型I (slb.s1.small)	5,000	3,000	1,000	免费	免费
	规格 2	标准型I (slb.s2.small)	50,000	5,000	5,000	228.00	0.38
	规格 3	标准型II (slb.s2.medium)	100,000	10,000	10,000	456.00	0.76
	规格 4	高阶型I (slb.s3.small)	200,000	20,000	20,000	912.00	1.52
	规格 5	高阶型II (slb.s3.medium)	500,000	50,000	30,000	1,372.00	2.29
	规格 6	超强型I (slb.s3.large)	1,000,000	100,000	50,000	2,290.00	3.82

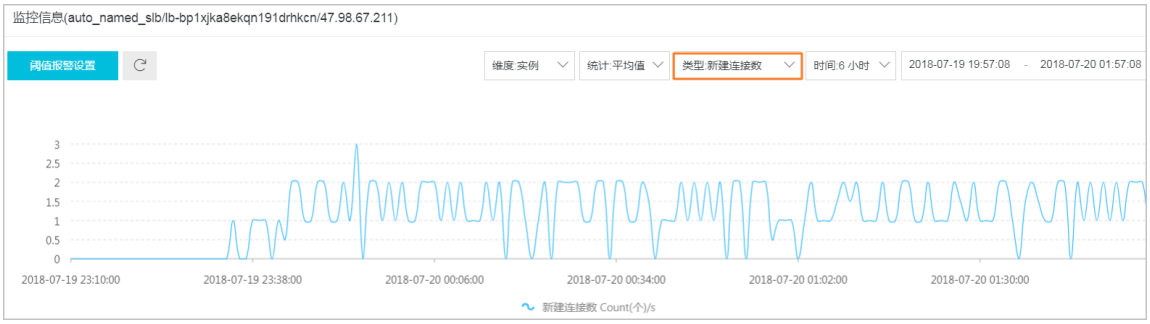
4. 如何选择性能保障型实例?

- 如果您购买的是按量付费实例，如上文所描述，规格费是按量（弹性）计费的，因此建议您直接选择您可以买到的最大规格，对于大多数用户而言，即高阶型I(slb.s3.large)，这样可以保证较好的业务灵活性（弹性），且不会让您额外多付出成本。但如果您认为您的业务量不太可能到达超强型I(slb.s3.large），也可以设置一个合理的弹性上限，比如高阶型II(slb.s3.medium)。

- 如果您购买的是预付费实例，情况会略微复杂一点。因为规格费按照固定费率恒定收取，而您不希望购买一个超出您实际业务量很多的规格，并因此付出不必要的成本，因此您需要评估您的实际业务量，并合理的考虑一些冗余，然后选择一个较合适的规格，对于业务量评估来说，主要参考下面几个原则：
  - 如果是四层监听，关注的重点是长连接的并发连接数，那么最大（并发）连接数应当作为一个关键指标来参考。根据不同的业务场景，您需要预估一个负载均衡实例需要承载的最大并发连接数，并选择相应的规格。
  - 如果是七层监听，关注的重点是QPS的性能，QPS决定了一个七层应用系统的吞吐量。同样，您也需要根据经验对QPS进行预估。在初步选定一个规格后，在业务压测和实测过程中对规格进行微调。
  - 结合与性能保障型实例一起推出的其它关键监控指标，查看实际业务流量的走势、峰值情况，对性能规格进行更加精确的选取。更多详细信息，参考监控数据。

    并发连接数监控示例

    新建连接数监控示例



    QPS监控示例

5. 是否可以调整性能保障型实例的规格?

您可在控制台对性能保障型实例进行变配，如下图所示。

按量付费的性能保障型实例的规格可以升配也可以降配，包年包月的性能保障型实例需要开通白名单才可以降配。详情参考包年包月实例变配。

因此，建议您先使用按量付费的实例进行业务测试，确认好规格后再购买所需规格的包年包月实例。

说明:

- 将性能共享型实例变更为性能保障型实例后，无法再将其变更回性能共享型。
- 变更性能保障型实例规格时，如果同时变更计费方式(按流量计费或按带宽计费)，则规格变更需要到次日零点才能生效。如果仅仅是对实例规格进行变更，变更立即生效。建议您在变更规格时，尽量不要变更计费方式。
- 由于历史存量原因，部分实例可能存在于较老的集群。此部分实例在变配到性能保障型实例时，因为需要将实例迁移，因此可能出现10-30秒的业务中断，其他变配操作均不会影响业务。因此建议在业务低谷期进行此类变配。
- 所有的变配操作都不影响负载均衡实例的IP地址。

6. 性能保障型实例何时收费?

阿里云负载均衡计划将于2018年4月1日开始针对性能保障型实例收取规格费，同时继续保留性能共享型实例的售卖。

性能保障型实例的规格费收取将按地域分批次生效:

- 第一批:

  生效时间：4月1日至4月10日陆续生效

  生效地域：亚太东南1（新加坡）、亚太东南3（吉隆坡）、亚太东南5（雅加达）、亚太南部1（孟买）、美国西部1（硅谷）、美国东部1（弗吉尼亚）

- 第二批:

生效时间：4月11日至4月20日陆续生效

生效地域：华东1（杭州）、华北3（张家口）、华北5（呼和浩特）、香港

- 第三批：

生效时间：4月21日至4月30日陆续生效

生效地域：华北1（青岛）、华北2（北京）、华东2（上海）、华南1（深圳）

7. 收取规格费以后，性能共享型实例需也会额外收取费用吗？

不会。

原有的性能共享型实例（如果您不将其变配性能保障型）将继续保持为性能共享型实例，不收取规格费。您也可以通过变配，将性能共享型实例升级成性能保障型实例。变更成性能保障型后，当性能保障型实例开始正式收费时，该实例将收取规格费。

8. 为何有时性能保障型实例看起来达不到规格中的性能指标上限？

短木板原理。

性能保障型实例并不保障三个指标（包含带宽指标）同时达到指定规格的指标上限。即规格中哪个指标先达到峰值，就以哪个指标开始限速。

同样，如果购买了按带宽付费的实例，当实例带宽达到峰值上限时，也可能会出现因为带宽限速而导致某些指标达不到规格上限的情况。

比如某用户选择高阶型I（slb.s3.small）实例，当实例的QPS已经达到20000，但并发连接数确远未达到20万，那么该实例最大连接数可能永远都不会达到规格上限，因为新建的连接请求会因为QPS达到上限而被丢弃。

9. 还可以购买性能共享型实例吗？

可以。

当前继续开放性能共享型实例的售卖，后续性能共享型实例有可能会下线，届时会通过官网公告、邮件等方式通知。

10. 私网负载均衡实例也会收取规格费吗？

如果您选择的是性能共享型私网实例，则不会收取规格费；如果您选择的是性能保障型私网实例，则需要收取规格费。规格费收取方式与公网实例规格费计费规则一致。私网实例免收实例费和流量费。

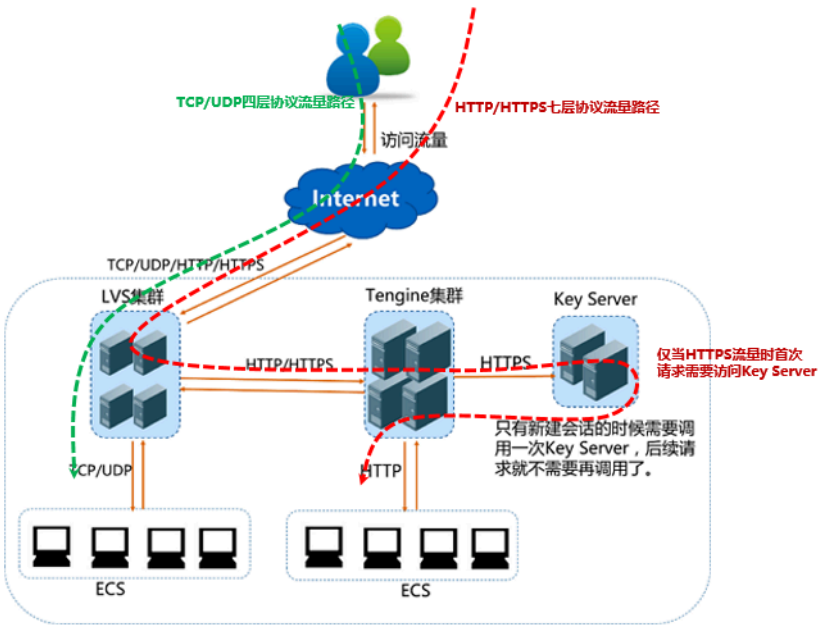
1.3 网络流量路径说明

负载均衡作为流量转发服务，将来自客户端的请求通过负载均衡集群转发至后端服务器，后端服务器再将响应通过内网返回给负载均衡。

入网流量路径

对于入网流量，负载均衡会根据用户在控制台或API上配置的转发策略，对来自前端的访问请求进行转发和处理，数据流转如图 *1-1:* 入网流量路径所示。

图 1-1: 入网流量路径



1. TCP/UDP协议和HTTP/HTTPS协议的流量都需要经过LVS集群进行转发。
2. LVS集群内的每一台节点服务器均匀地分配海量访问请求，并且每一台节点服务器之间都有会话同步策略，以保证高可用。
   - 如果相应的负载均衡实例服务端口使用的是四层协议（TCP或UDP），那么LVS集群内每个节点都会根据负载均衡实例负载均衡策略，将其承载的服务请求按策略直接分发到后端ECS服务器。
   - 如果相应的负载均衡实例服务端口使用的是七层HTTP协议，那么LVS集群内每个节点会先将其承载的服务请求均分到Tengine集群，Tengine集群内的每个节点再根据负载均衡策略，将服务请求按策略最终分发到后端ECS服务器。
   - 如果相应的负载均衡实例服务端口使用的是七层HTTPS协议，与上述HTTP处理过程类似，差别是在按策略将服务请求最终分发到后端ECS服务器前，先调用Key Server进行证书验证及数据包加解密等前置操作。

出网流量路径

负载均衡SLB和后端ECS之间是通过内网进行通信的。

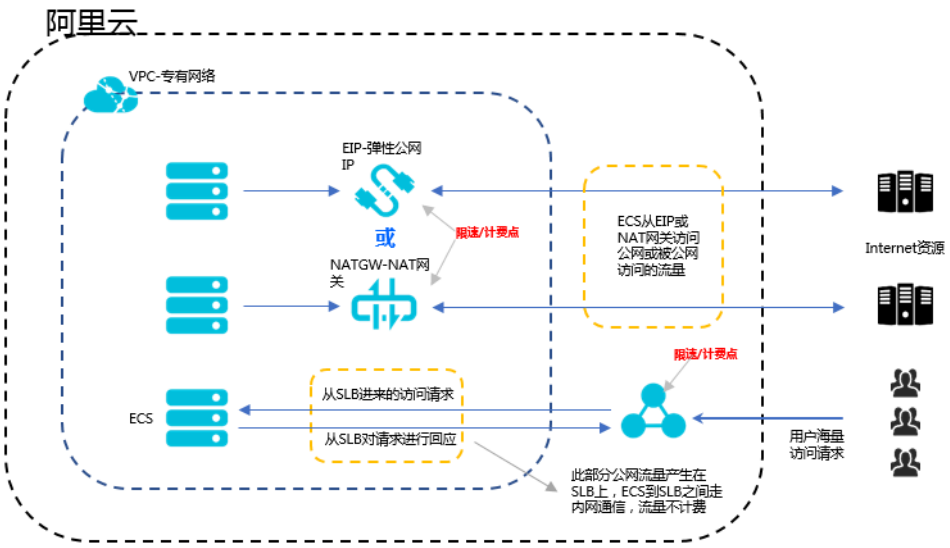
- 如果ECS仅仅处理来自负载均衡的请求，可以不购买公网带宽（ECS公网IP/弹性公网IP/NAT网关等）。

  > **说明:**
  > 早期存量ECS上直接分配了公网IP（ifconfig中可见接口上分配的公网ip地址），此类ECS如果仅通过SLB对外提供服务，即便在公网接口（网卡）上看到有流量统计，也不会产生ECS的公网费用。

- 如果需要直接通过后端ECS对外提供服务，或后端ECS有访问外网的需求，那么需要相应的配置或购买ECS公网IP/弹性公网IP/NAT网关等服务。

ECS的公网流量访问路径如图 *1-2:* 出网流量路径所示。

图 1-2: 出网流量路径



总体原则：流量从哪里进来，就从哪里出去。

1. 通过负载均衡进入的流量在负载均衡SLB上限速/计费，仅收取出方向流量费用，入方向流量不收取（在未来可能会改变），SLB到ECS之间是阿里云内网通信，不收取流量费用。
2. 来自弹性公网IP/NAT网关的流量，分别在弹性公网IP/NAT网关上进行限速/计费，如果在购买ECS时选择了公网带宽，限速/计费点在ECS上。
3. 负载均衡SLB仅提供被动访问公网的能力，即后端ECS只能在收到通过负载均衡SLB转发来的公网的请求时，才能访问公网回应该请求，如后端ECS希望主动发起公网访问，则需要配置/购买ECS公网带宽、弹性公网IP或NAT网关来实现。

4. ECS公网带宽（购买ECS时配置）、弹性公网IP、NAT网关均可以实现ECS的双向公网访问（访问或被访问），但没有流量分发和负载均衡的能力。

1.4 创建负载均衡实例

前提条件

在您创建负载均衡实例前，确保您已经做好了相关规划，详情参考规划和准备。

操作步骤

1. 登录负载均衡管理控制台。
2. 选择实例 > 实例管理，单击左上角的创建负载均衡。
3. 在购买页面选择一种付费方式。本教程选择按量付费。

   参考计费说明了解负载均衡的计费模式。
4. 根据如下信息，配置负载均衡实例。

配置	说明
地域	选择负载均衡实例的所属地域。 说明: 确保负载均衡实例的地域和后端添加的云服务器ECS的地域相同。
可用区类型	显示所选地域的可用区类型。云产品的可用区指的是一套独立的基础设施，常用数据中心IDC表示。不同的可用区之间具有基础设施（网络、电力、空调等）的独立性，就是说一个可用区的基础设施故障不影响另外一个可用区。可用区是属于某个地域的，一个地域下可能有一个或者多个可用区。负载均衡已经在大部分地域部署了多可用区。 · 单可用区：负载均衡实例只部署在一个可用区上。 · 多可用区：负载均衡实例会部署在两个可用区上。默认启用主可用区的实例。当主可用区出现故障时，将会自动切换到备可用区继续提供负载均衡服务，可以大大提升本地可用性。
主可用区	选择负载均衡实例的主可用区，主可用区是当前承载流量的可用区。
备可用区	选择负载均衡实例的备可用区。备可用区默认不承载流量，主可用区不可用时才承载流量。
实例规格	选择一个性能规格。 不同的性能规格所提供的性能指标也不同，详情查看如何使用性能保障型实例。

配置	说明
实例类型	根据业务场景选择配置对外公开或对内私有的负载均衡服务，系统会根据您的选择分配公网或私网服务地址。更多详细信息，参考什么是负载均衡实例。 · 公网：公网负载均衡实例仅提供公网IP，可以通过Internet访问负载均衡。 · 私网：私网负载均衡实例仅提供阿里云私网IP，只能通过阿里云内部网络访问该负载均衡服务，无法从Internet访问。
网络类型	如果您选择的实例类型是私网，您还需要选择该负载均衡实例的网络类型。 · 经典网络：经典网络的负载均衡实例的服务地址由阿里云统一分配和管理。 · 专有网络：专有网络的负载均衡实例的服务地址会从您指定的专有网络的交换机网段内分配。
计费方式	选择一种计费方式。
购买数量	选择购买数量。

5. 单击立即购买，完成支付。

1.5 创建IPv6实例

负载均衡支持创建IPv6实例。创建后，系统会为实例分配一个公网IPv6地址，转发来自IPv6客户端的请求。

背景信息

IPv6是Internet Protocol Version 6的缩写，其中Internet Protocol译为互联网协议。IPv6是IETF（互联网工程任务组，Internet Engineering Task Force）设计的用于替代现行版本IP协议（IPv4）的下一代IP协议，通过将IPv4中32位的地址长度扩展为128位，使得地址空间扩大了79,228,162,514,264,337,593,543,950,336倍。使用IPv6，可以让全世界的每一粒沙子都能分配到一个IP地址。

：

- 目前，仅有华东1地域的E、F两个可用区和华北2地域的F、G两个可用区支持创建IPv6实例且实例类型必须为性能保障型实例。
- 互联网IPv6网络大环境还处于建设初期，当前可能存在部分线路访问不通，如有请工单反馈，同时IPv6公测期间，不提供SLA保障。
- 由于IPv6的IP头部较IPv4更长，当您在SLB IPv6实例上使用UDP监听时，需要确保后端服务器（通常是ECS云服务器）与SLB通信的网卡的MTU不大于1480（有些应用程序需要根据此MTU值同步修改其配置文件），否则数据包可能会因过大被丢弃。

如果使用TCP/HTTP/HTTPS监听，TCP协议支持MSS自动协商，因此不需要额外配置。

负载均衡IPv6支持有以下特点：

- 平滑迁移IPv6，业务无感知

  IPv6 SLB后端可以直接挂载使用IPv4地址的ECS，无需对原有系统做改造，就可以平滑地将业务迁移到IPv6。

  通过新增IPv6入口，对原有IPv4业务无任何影响，仅需要在业务总量增加的情况下，适量对后端ECS进行横向扩容即可。

- IPv6访问控制让业务部署更加安全可靠

  阿里云负载均衡SLB支持IPv6访问控制，您可以根据业务需要灵活地配置访问控制策略。

  - 访问控制黑名单可有效阻断恶意地址对负载均衡业务的访问。
  - 访问控制白名单仅允许白名单中授权的地址访问负载均衡业务。

操作步骤

1. 登录负载均衡管理控制台。
2. 选择实例 > 实例管理。
3. 在实例管理页面，单击左上角的创建负载均衡。
4. 配置负载均衡实例，IP版本选择IPv6。

   其他配置和普通实例配置相同，参考*SLB*实例配置说明。

   说明：
   目前，仅有华东1地域的E、F两个可用区和华北2地域的F、G两个可用区支持创建IPv6实例且实例类型必须为性能保障型实例。


主可用区
华东 1 可用区 F
主可用区是当前承载流量的可用区，备可用区默认不承载流量，主可用区不可
备可用区
华东 1 可用区 E
实例名称
auto_named_slb
长度限制为1-80个字符，允许包含中文、字母、数字、'-'、'/'、'.'、'_'这些字符
实例规格
简约型I (slb.s1.small)
该规格最大可以支持连接数: 5000，新建连接数 (CPS): 3000，每秒查询数 (Q
性能保障型实例2018年4月起正式收取规格费
【按量付费模式下可选择最大规格，规格费将根据每小时使用的实际规格进行
点击查看具体收费详情>>
实例类型
公网
实例类型详解>>
负载均衡实例仅提供公网IP，可以通过Internet访问的负载均衡服务
IP版本
IPv4
IPv6
互联网IPv6网络大环境还处于建设初期，当前可能存在部分线路访问不通，如
计费方式
按使用流量计费
按固定带宽计费
按流量计费实例带宽峰值请查看各地域带宽峰值>>
若变更计费方式则本次变配所有参数（包括带宽）需要到次日0点才能生效，
阿里云最高提供5Gbps的恶意流量攻击防护，了解更多>>提升防护能力>>
阿里云现已开通共享流量包，可同时抵扣 ECS、EIP、SLB、NAT 产生的流量

5. 返回实例列表页面，查看已创建的IPv6实例。

预期结果

创建后，系统会为该实例分配一个IPv6地址。

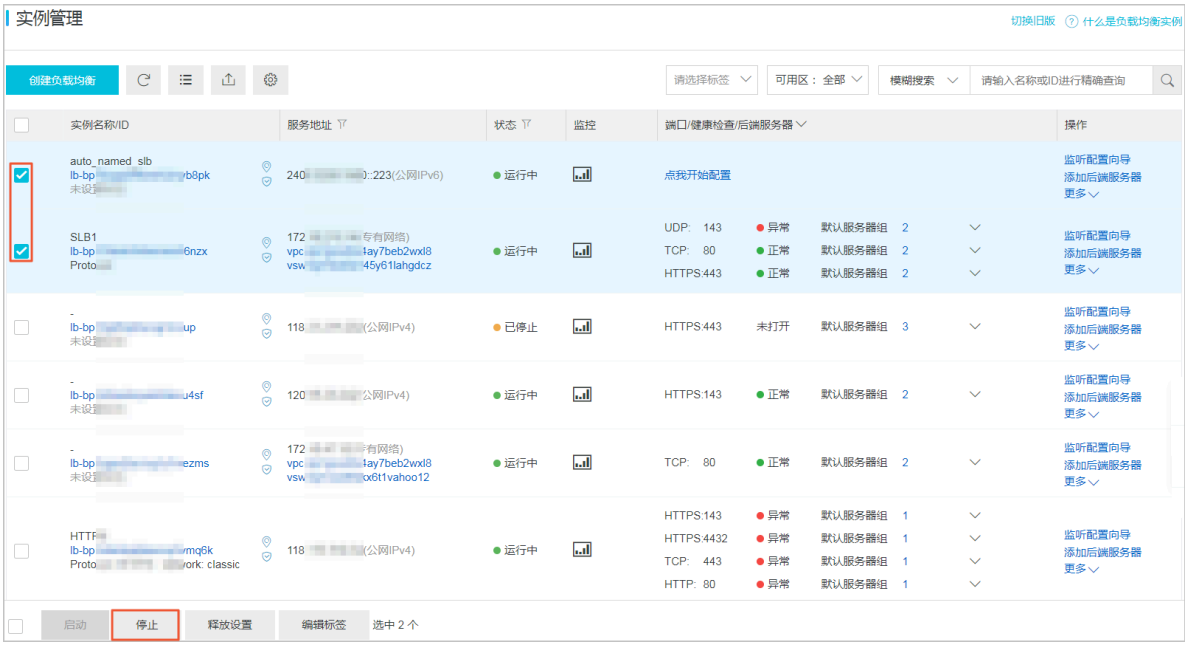
1.6 启动和暂停实例

您可以随时启动或暂停负载均衡实例。实例暂停后不再接收和转发客户端流量。

操作步骤

1. 登录负载均衡管理控制台。
2. 在左侧导航栏，单击实例 > 实例管理。
3. 选择负载均衡实例的地域，找到目标实例。
4. 在操作列下，单击更多 > 启动或更多 > 停止。

5. 如果您想批量启动或停止多个实例，选择实例后，在页面下方单击启动或停止。



1.7 绑定EIP

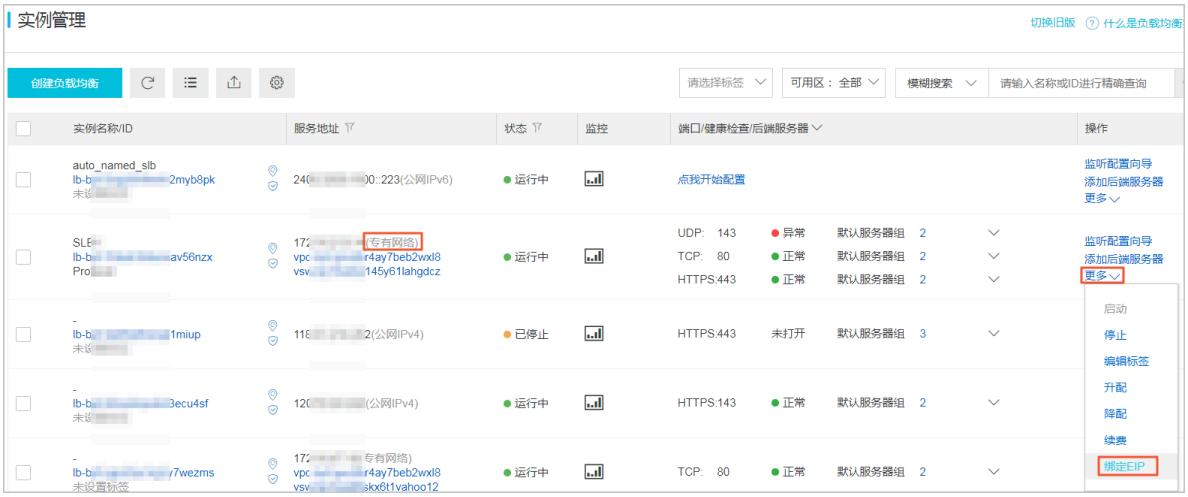
您可以为专有网络类型的SLB实例绑定一个EIP。绑定后，SLB实例便可以转发来自公网的请求。

操作步骤

1. **登录负载均衡管理控制台。**
2. **在左侧导航栏，单击实例 > 实例管理。**
3. **选择负载均衡实例的地域，找到目标实例。**

> **说明:**
> **确保负载均衡实例的网络类型为专有网络。**

4. **单击更多 > 绑定EIP。**



5. 选择一个EIP，然后单击确认。

1.8 释放实例

背景信息

您可以根据需求设置立即或者定时释放按量付费实例。

包年包月负载均衡实例不支持主动释放，如果需要释放，请提工单申请退款，负载均衡SLB支持5天无理由退款。

操作步骤

1. 登录负载均衡管理控制台。
2. 选择需要释放实例操作列的更多 > 释放设置。

   支持勾选多个负载均衡实例，单击页面下方的释放设置，批量释放按量付费实例。

3. 在释放设置页面，选择释放方式，立即释放或者在某个特定时刻释放实例。

> **说明:**
> 系统执行释放时间是每个整点和半点，但系统会按照您设置的释放时间停止计费。

4. 单击下一步。
5. 单击确定，输入验证信息，确认释放实例。

1.9 管理标签

负载均衡提供标签管理功能，方便您通过标签对负载均衡实例进行分类。

每个标签都由一对键值对组成，负载均衡标签的使用限制如下：

- 不支持未绑定实例的空标签存在，标签必须绑定在某个负载均衡实例上。

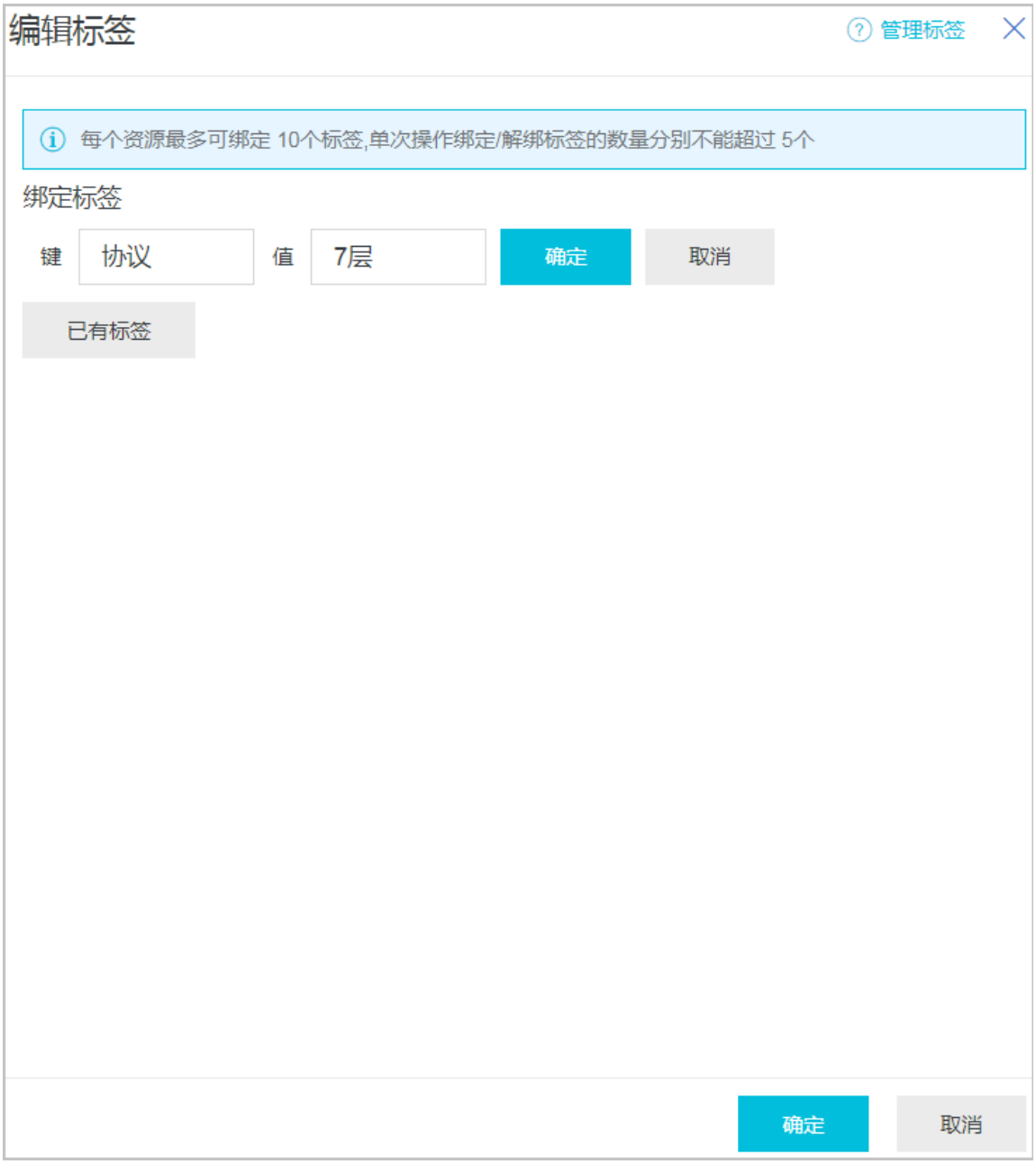
- 一个实例最多可以绑定10个标签。
- 一个实例上的每个标签的标签键必须唯一，相同标签键的标签会被覆盖。
- 每个地域中的的标签信息不互通，例如在华东1地域创建的标签在华东2地域不可见。

添加标签

完成以下操作，添加标签：

1. 登录负载均衡管理控制台。
2. 在左侧导航栏，选择实例 > 实例管理。
3. 选择一个地域，找到目标实例。
4. 在操作列下，选择更多 > 编辑标签。

5. 在编辑标签页面，完成以下操作：
   a. 如果已有可用的标签，单击已有标签，然后选择要添加的标签。
   b. 如果您需要新建标签，在编辑标签页面，单击新建，然后输入新建标签的标签键和值，单击确定。



c. 单击确定。

搜索实例

完成以下操作，搜索指定标签关联的实例：

1. 登录负载均衡管理控制台。
2. 在左侧导航栏，单击实例 > 实例管理。
3. 选择一个地域，找到目标实例。
4. 单击请选择标签，然后选择要搜索的实例绑定的标签。

5. 单击已选标签键的删除图标，清除标签过滤条件。

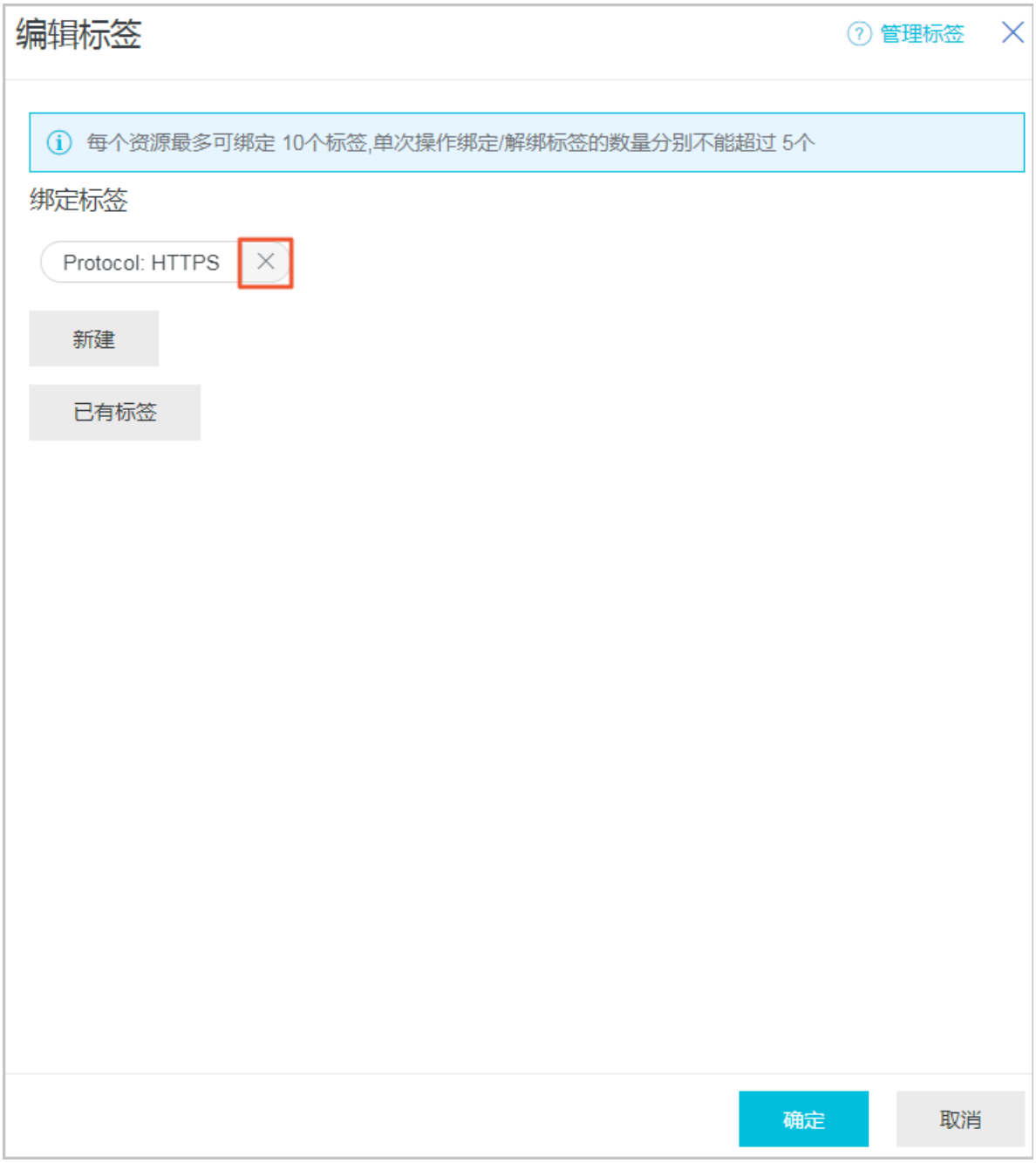
删除标签

负载均衡不支持批量删除多个实例的标签，您只能单独对某一个实例进行标签移除。

完成以下操作，删除标签：

1. 登录负载均衡管理控制台。
2. 在左侧导航栏，单击实例 > 实例管理。
3. 选择一个地域，找到目标实例。
4. 在操作列下，单击更多 > 编辑标签。
5. 在编辑标签页面，单击要移除的标签的删除图标，然后单击确定。

> **说明：**
> 当一个标签从一个实例上移除后，如果该标签没有和其他实例绑定，系统会将该标签删除。



1.10 回收站

支持将到期的预付费实例和欠费账户中的后付费实例，加入回收站管理。

背景信息

回收站的实例逾期不续费后，将自动释放。

- 预付费实例：到期后，锁定实例，进入回收站，保留七天，七天后不续费自动释放。
- 后付费实例：欠费后，实例继续运行24小时后会被锁定，停止服务，进入回收站。若7天后仍旧欠费，实例会被释放。

操作步骤

1. 登录负载均衡管理控制台。
2. 选择实例管理 > 回收站。
3. 查看即将到期的预付费实例和欠费账号中的后付费实例详细信息。
4. 单击负载均衡实例操作列的续费，对实例进行续费操作，续费成功后，实例从回收站转移到实例管理列表中。

1.11 按量付费实例变配

您可以更改后付费实例的带宽、实例规格和计费方式（按流量计费或按带宽计费）。

背景信息

在变更前，请注意：

- 性能共享型实例变更为性能保障型实例会有10-30秒业务中断，其他变配操作均不会影响业务，也不会变更负载均衡实例IP。

  建议您在业务低谷期进行变配，或者使用DNS将业务调度至其他的SLB实例后，再进行变配。
- 将性能共享型实例变更为性能保障型实例后，无法再将其变更回性能共享型。

  您可以选择使用简约型I (slb.s1.small)规格，该规格免收规格费。
- 后付费实例支持按流量计费和按带宽计费。您可以变更后付费实例的计费方式，计费方式的变更会在次日零点生效。
- 如果您更改实例规格时，也变更了计费方式（按带宽计费和按流量计费的变更），那么规格的变更会同计费方式的变更一起在次日零点生效。

操作步骤

1. 登录负载均衡管理控制台。
2. 选择目标实例的所属地域。
3. 找到目标实例，选择更多 > 升配降配。
4. 在配置变更区域，选择新的带宽值、实例规格或计费方式后，完成支付。

- 您可以更改按固定带宽计费实例的带宽。

  在变更带宽时，您还可以为实例中的每个监听指定一个带宽峰值，监听带宽峰值总和不能大于实例的带宽值。如果不开启带宽峰值限定，那么该实例下的所有监听共享指定的带宽。
- 后付费实例支持按流量计费和按带宽计费。您可以变更后付费实例的计费方式，计费方式的变更会在次日零点生效。
- 您可以更改性能保障型实例的规格，变更实时生效。

1.12 包年包月实例变配

背景信息

在变配前，请注意：

- 将性能共享型实例变更为性能保障型实例后，无法再将其变更回性能共享型。
- 将性能共享型实例变更为性能保障型实例时，可能会出现10-30秒的业务中断（其他变配操作均不会影响业务）。因此建议在业务低谷期进行此类变配，或通过DNS实现实例间的负载均衡后，再进行变配。
- 所有的变配操作都不影响负载均衡实例的IP地址。

操作步骤

1. 登录负载均衡管理控制台。
2. 选择目标实例的所属地域。
3. 找到目标实例，选择管理 > 升配。

4. 在配置变更区域，选择新的带宽值或实例规格，完成支付。

   在变更配置时，您可以为实例下的监听配置带宽，若不配置则所有监听共享实例的带宽。详情参见共享实例带宽。

> **说明:**
> 将性能共享型实例变更为性能保障型实例后，无法再将其变更回性能共享型。

1.13 包年包月实例短时升配

性能保障型负载均衡实例针对预付费实例提供短时升配功能，灵活应对业务带宽峰值波动。

背景信息

您可以通过短时升配功能，临时的提升预付费实例的带宽和规格，在短时升配到期后，实例自动恢复原有带宽和规格。

短时升配支持的最短升级间隔为2小时，按小时单价计费，支付完成后带宽立即生效，升级过程不中断业务。

当负载均衡到达指定的还原时间时，带宽将自动恢复到升级前的大小。恢复过程中不中断业务，但带宽从高变低有可能会出现闪断，建议后端应用具备重连机制。

短时升配适用于大促或者节假日线上运营活动等场景。

> 说明:
>
> - 仅性能保障型负载均衡实例支持短时升配。
> - 在使用短时升配提升实例带宽后， 如果配置了监听带宽限速且调高了监听的带宽限速，在短时升配到期时，系统会自动删除监听上的带宽限制，所有监听共享实例带宽。
> - 在短时升配状态中，不可进行升配（或降配）操作，可以多次短时升配，但是第二次短时升配结束时间需要晚于第一次短时升配时间，建议短时升配时长不超过一个月。
> - 您的实例在短时升配到期后恢复到原有实例带宽/规格时，如果此时实例上业务流量超过实例原有带宽/规格的限制，可能出现限速从而导致流量被丢弃，请合理规划短时升配的到期时间，确保实例带宽/规格和业务需求匹配。
> - 仅负载均衡新版控制台支持短时升配功能。

操作步骤

1. 登录负载均衡管理控制台。
2. 在左侧导航栏，单击实例管理。
3. 在实例管理页面，选择需要短时升配的实例操作列的更多 > 短时升配。

4. 在临时升配页面，修改实例规格、带宽值和还原时间，并完成支付。

1.14 管理闲置实例

闲置实例向您展示超过7天未投入使用的后付费实例，保持关注闲置实例，有助于您更好的管理成本。

操作步骤

1. **登录负载均衡管理控制台。**
2. **在左侧导航栏，选择SLB 实验室 > 闲置实例。**
3. **在闲置实例页面，查看所有超过七天未投入使用的后付费实例，单击  ，可以自定义显示实例的服务地址和闲置原因。**
4. **如果确认闲置实例是无用的，可以单击操作列的释放设置，立即释放闲置的后付费实例。**

> **说明:**
> **由于闲置实例数据存在一天缓存期，请您确保需要释放的实例处于未使用状态，以防产生实例误释放。**


闲置实例
闲置实例向您展示超过7天未投入使用的后付费实例，保持关注闲置实例，有助于您更好的管理成本
实例名称/ID
服务地址
闲置原因
操作
auto_named_slb
没有监听
释放设置
所有监听都没有后端
释放设置

2 监听

2.1 监听介绍

创建负载均衡实例后，您需要为实例配置监听。负载均衡实例监听负责检查连接请求，然后根据调度算法定义的转发策略将请求流量分发至后端服务器。

负载均衡提供四层（TCP/UDP协议）和七层（HTTP/HTTPS协议）监听，您可根据应用场景选择监听协议：

协议	说明	使用场景
TCP	· 面向连接的协议，在正式收发数据前，必须和对方建立可靠的连接 · 基于源地址的会话保持 · 在网络层可直接看到来源地址 · 数据传输快	· 适用于注重可靠性，对数据准确性要求高，速度可以相对较慢的场景，如文件传输、发送或接收邮件、远程登录 · 无特殊要求的Web应用 详情参见添加*TCP*监听。
UDP	· 面向非连接的协议，在数据发送前不与对方进行三次握手，直接进行数据包发送，不提供差错恢复和数据重传 · 可靠性相对低；数据传输快	关注实时性而相对不注重可靠性的场景，如视频聊天、金融实时行情推送。 详情参见添加*UDP*监听。
HTTP	· 应用层协议，主要解决如何包装数据 · 基于Cookie的会话保持 · 使用X-Forward-For获取源地址	需要对数据内容进行识别的应用，如Web应用、小的手机游戏等。 详情参见添加*HTTP*监听。
HTTPS	· 加密传输数据，可以阻止未经授权的访问 · 统一的证书管理服务，用户可以将证书上传到负载均衡，解密操作直接在负载均衡上完成	需要加密传输的应用。 详情参见添加*HTTPS*监听。

说明:

负载均衡已在全部地域支持HTTP/2和WSS/WS协议，详情参见*HTTP/2*协议支持常见问题和*WS/WSS*协议支持常见问题。

2.2 添加TCP监听

TCP协议适用于注重可靠性，对数据准确性要求高，速度可以相对较慢的场景，如文件传输、发送或接收邮件、远程登录等。您可以添加一个TCP监听转发来自TCP协议的请求。

前提条件

创建负载均衡实例。

步骤一 打开监听配置向导

完成以下操作，打开监听配置向导：

1. 登录负载均衡管理控制台。
2. 在左侧导航栏，选择实例 > 实例管理。
3. 选择实例的地域。
4. 选择以下一种方法，打开监听配置向导：
   - 在实例管理页面，找到目标实例，然后单击添加配置向导。

   - 在实例管理页面，单击目标实例ID。在监听页面，单击添加监听。

步骤二 配置协议监听

完成以下操作， 配置协议监听：

1. 在协议&监听页面，根据以下信息配置TCP监听。

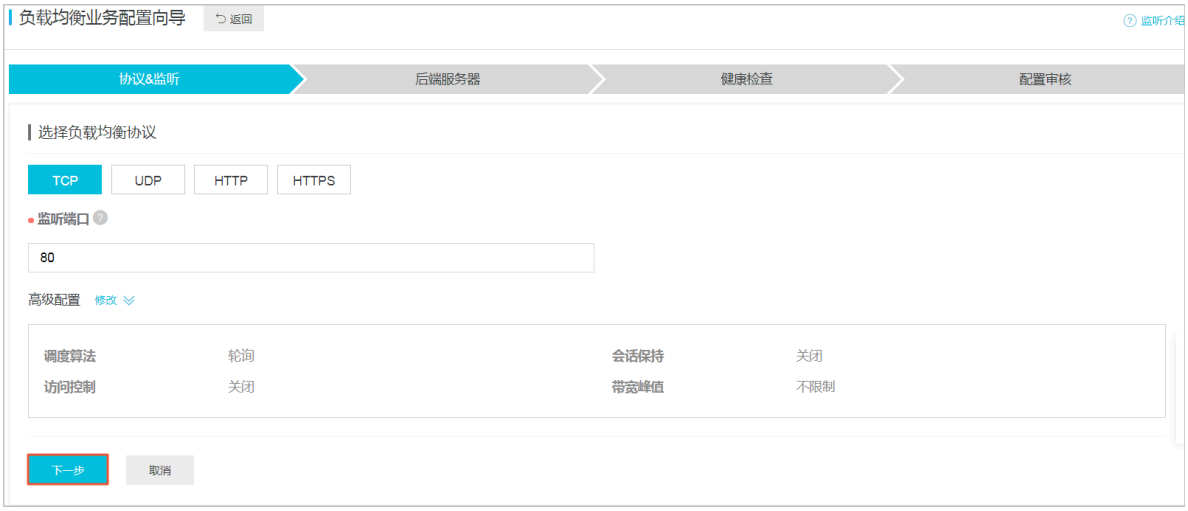
监听配置	说明
选择负载均衡协议	选择监听的协议类型。 本操作，选择TCP。

监听配置	说明
监听端口	用来接收请求并向后端服务器进行请求转发的监听端口。 端口范围为1-65535。 说明: 在同一个负载均衡实例内，监听端口不可重复。
高级配置	
调度算法	负载均衡支持轮询、加权轮询（WRR）、加权最小连接数（WLC）三种调度算法。 · 加权轮询：权重值越高的后端服务器，被轮询到的次数（概率）也越高。 · 轮询：按照访问顺序依次将外部请求依序分发到后端服务器。 · 加权最小连接数：除了根据每台后端服务器设定的权重值来进行轮询，同时还考虑后端服务器的实际负载（即连接数）。当权重值相同时，当前连接数越小的后端服务器被轮询到的次数（概率）也越高。 · 一致性哈希（CH）： - 源IP：基于源IP地址的一致性hash，相同的源地址会调度到相同的后端服务器。 - 四元组：基于四元组的一致性hash（源IP+目的IP+源端口+目的端口），相同的流会调度到相同的后端服务器。 说明: 一致性哈希（CH）算法目前仅支持以下地域： - 日本（东京） - 澳大利亚（悉尼） - 马来西亚（吉隆坡） - 印度尼西亚（雅加达） - 德国（法兰克福） - 美国（硅谷） - 美国（弗吉利亚） - 阿联酋（迪拜） - 华北5（呼和浩特）

监听配置	说明
开启会话保持	是否开启会话保持。 开启会话保持后，负载均衡监听会把来自同一客户端的访问请求分发到同一台后端服务器上。 TCP协议是基于IP地址的会话保持，即来自同一IP地址的访问请求转发到同一台后端服务器上。
启用访问控制	选择是否启用访问控制。
访问控制方式	开启访问控制后，选择一种访问控制方式： · 白名单：仅转发来自所选访问控制策略组中设置的IP地址或地址段的请求，白名单适用于应用只允许特定IP访问的场景。 设置白名单存在一定业务风险。一旦设置白名单，就只有白名单中的IP可以访问负载均衡监听。如果开启了白名单访问，但访问策略组中没有添加任何IP，则负载均衡监听会转发全部请求。 · 黑名单：来自所选访问控制策略组中设置的IP地址或地址段的所有请求都不会转发，黑名单适用于应用只限制某些特定IP访问的场景。 如果开启了黑名单访问，但访问策略组中没有添加任何IP，则负载均衡监听会转发全部请求。
选择访问控制策略组	选择访问控制策略组，作为该监听的白名单或黑名单。 说明: IPv6实例只能绑定IPv6访问控制策略组，IPv4实例只能绑定IPv4访问控制策略组。详情参见访问控制策略组。
开启监听带宽限速	选择是否配置监听带宽。 对于按带宽计费的负载均衡实例，您可以针对不同监听设定不同的带宽峰值来限定监听的流量。实例下所有监听的带宽峰值总和不能超过该实例的带宽。 默认不开启，各监听共享实例的总带宽。 说明: 使用流量计费方式的实例默认不限制带宽峰值。
连接超时时间	指定TCP连接的超时时间，范围10-900秒。
监听名称	设置监听的名称，用户自定义。
获取真实IP	针对四层监听，后端服务器可直接获得来访者的真实IP，无需采用其它手段获取。

监听配置	说明
创建完毕自动启动监听	是否在监听配置完成后启动负载均衡监听，默认开启。

2. 单击下一步。



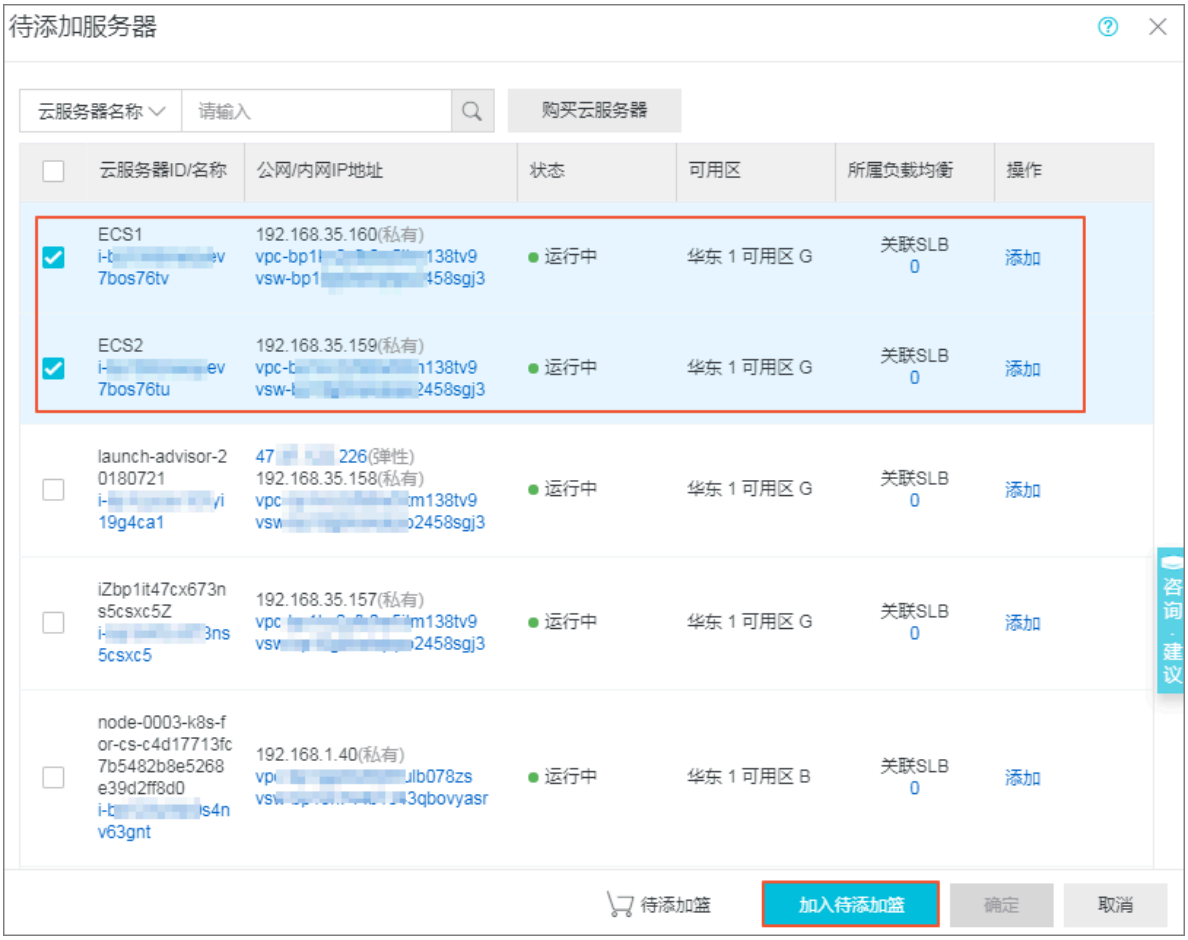
步骤三 添加后端服务器

添加处理前端请求的后端服务器。您可以使用实例配置的默认服务器组，也可以为监听配置一个虚拟服务器组或主备服务组。详情参见后端服务器概述。

本操作中，以默认后端服务器组为例：

1. 选择默认服务器组，单击添加。

2. 选择要添加的ECS实例，然后单击加入待添加篮。单击确定。



3. 配置添加的后端服务器的端口和权重。

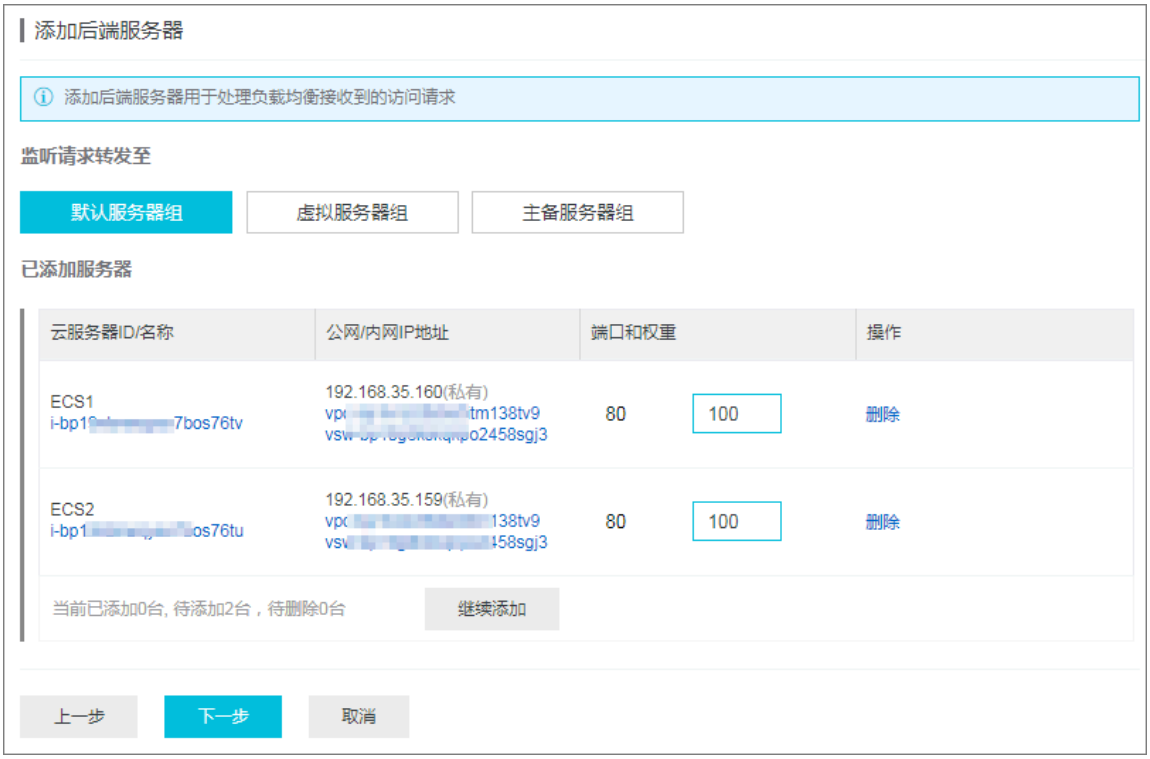
- 端口

  后端服务器（ECS实例）开放用来接收请求的端口，端口范围为1-65535。同一个负载均衡实例内，后端服务器端口可以相同。

- 权重

  后端服务器（ECS实例）的权重。权重越高的ECS实例将被分配到更多的访问请求。

> **说明:**
> 权重设置为0，该服务器不会再接受新请求。



4. 单击下一步。

步骤四 配置健康检查

负载均衡通过健康检查来判断后端服务器（ECS实例）的业务可用性。健康检查机制提高了前端业务整体可用性，避免了后端ECS异常对总体服务的影响。单击修改更改健康检查配置，详情参见配置健康检查。

步骤五 提交配置

完成以下操作，确认监听配置：

1. 在配置审核页面，检查监听配置，您可以单击修改更改配置。
2. 确认无误后，单击提交。

3. 在配置审核页面，配置成功后，单击确定。

配置成功后，您可以在监听页面查看已创建的监听。

相关操作

- 配置健康检查
- 管理默认服务器组
- 管理虚拟服务器组
- 管理主备服务器组
- 设置访问控制

2.3 添加UDP监听

UDP协议多用于关注实时性而相对不注重可靠性的场景，如视频聊天、金融实时行情推送等。您可以添加一个UDP监听转发来自UDP协议的请求。

UDP监听限制

在添加UDP监听前，注意如下限制：

- 每个监听最大连接数限制：100,000。
- 暂不支持分片包。
- 经典网络负载均衡实例的UDP监听暂不支持查看源地址。
- 在以下两种情况下，UDP协议监听配置需要五分钟才能生效：
  - 移除后端服务器。
  - 健康检查检测到异常后，将后端服务器的权重设置为0。

- 由于IPv6的IP头部较IPv4更长，当您在SLB IPv6实例上使用UDP监听时，需要确保后端服务器（通常是ECS云服务器）与SLB通信的网卡的MTU不大于1480（有些应用程序需要根据此MTU值同步修改其配置文件），否则数据包可能会因过大被丢弃。

  如果使用TCP/HTTP/HTTPS监听，TCP协议支持MSS自动协商，因此不需要额外配置。

前提条件

创建负载均衡实例。

步骤一 打开监听配置向导

完成以下操作，打开监听配置向导：

1. 登录负载均衡管理控制台。
2. 在左侧导航栏，选择实例 > 实例管理。
3. 选择实例的地域。
4. 选择以下一种方法，打开监听配置向导：
   - 在实例管理页面，找到目标实例，然后单击添加配置向导。

   - 在实例管理页面，单击目标实例ID。在监听页面，单击添加监听。

步骤二 配置协议监听

完成以下操作， 配置协议监听：

1. 在协议&监听页面，根据以下信息配置UDP监听。

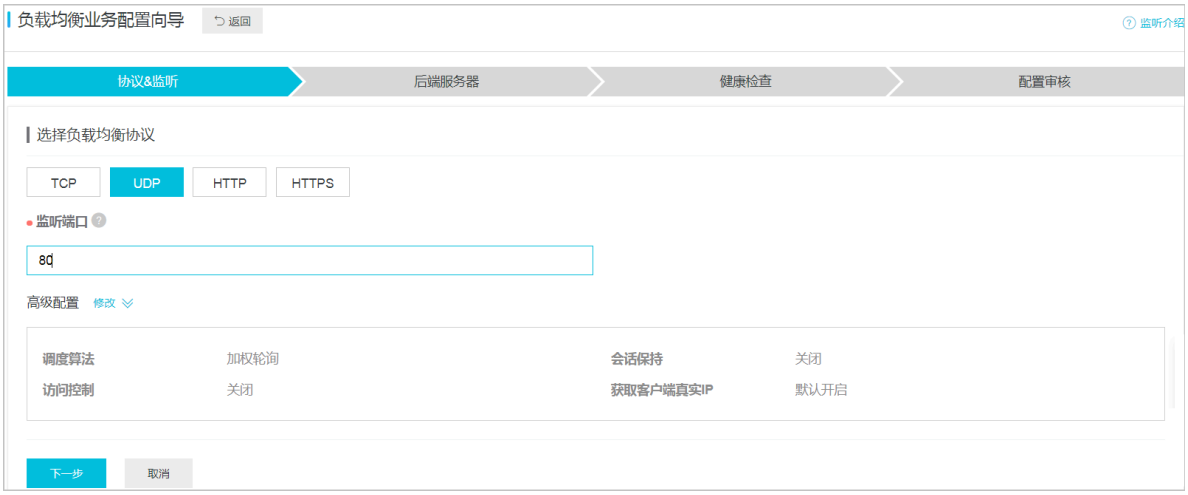
监听配置	说明
监听协议	选择监听的协议类型。 本操作，选择UDP。

监听配置	说明
监听端口	用来接收请求并向后端服务器进行请求转发的监听端口。 端口范围为1-65535。 **说明:** 在同一个负载均衡实例内，监听端口不可重复。
高级配置	

监听配置	说明
调度算法	负载均衡支持轮询、加权轮询（WRR）、加权最小连接数（WLC）三种调度算法。 · 加权轮询：权重值越高的后端服务器，被轮询到的次数（概率）也越高。 · 轮询：按照访问顺序依次将外部请求依序分发到后端服务器。 · 加权最小连接数：除了根据每台后端服务器设定的权重值来进行轮询，同时还考虑后端服务器的实际负载（即连接数）。当权重值相同时，当前连接数越小的后端服务器被轮询到的次数（概率）也越高。 · 一致性哈希（CH）： - 源IP：基于源IP地址的一致性hash，相同的源地址会调度到相同的后端服务器。 - 四元组：基于四元组的一致性hash（源IP+目的IP+源端口+目的端口），相同的流会调度到相同的后端服务器。 - QUIC ID：基于QUIC Connection ID一致性hash，相同的QUIC Connection ID会调度到相同的后端服务器。 ： QUIC协议正在快速演进，该算法基于*draft-ietf-quic-transport-10*实现，无法保证所有QUIC版本的兼容性，建议充分测试后再用于生产环境。 **说明:** 一致性哈希（CH）算法目前仅支持以下地域： - 日本（东京） - 澳大利亚（悉尼） - 马来西亚（吉隆坡） - 印度尼西亚（雅加达） - 德国（法兰克福） - 美国（硅谷） - 美国（弗吉利亚） - 阿联酋（迪拜） - 华北5（呼和浩特）

监听配置	说明
启用访问控制	选择是否启用访问控制。
访问控制方式	开启访问控制后，选择一种访问控制方式： · 白名单：仅转发来自所选访问控制策略组中设置的IP地址或地址段的请求，白名单适用于应用只允许特定IP访问的场景。 设置白名单存在一定业务风险。一旦设置白名单，就只有白名单中的IP可以访问负载均衡监听。如果开启了白名单访问，但访问策略组中没有添加任何IP，则负载均衡监听会转发全部请求。 · 黑名单：来自所选访问控制策略组中设置的IP地址或地址段的所有请求都不会转发，黑名单适用于应用只限制某些特定IP访问的场景。 如果开启了黑名单访问，但访问策略组中没有添加任何IP，则负载均衡监听会转发全部请求。
选择访问控制策略组	选择访问控制策略组，作为该监听的白名单或黑名单。 说明: IPv6实例只能绑定IPv6访问控制策略组，IPv4实例只能绑定IPv4访问控制策略组。详情参见访问控制策略组。
开启带宽峰值	选择是否配置监听带宽。 对于按带宽计费的负载均衡实例，您可以针对不同监听设定不同的带宽峰值来限定监听的流量。实例下所有监听的带宽峰值总和不能超过该实例的带宽。 默认不开启，各监听共享实例的总带宽。 说明: 使用流量计费方式的实例默认不限制带宽峰值。
获取真实IP	UDP协议监听的后端服务器可直接获取客户端的真实IP。 说明: 经典网络实例的UDP协议暂不支持查看源地址。
创建完毕自动启动监听	是否在监听配置完成后启动负载均衡监听，默认开启。

2. 单击下一步。



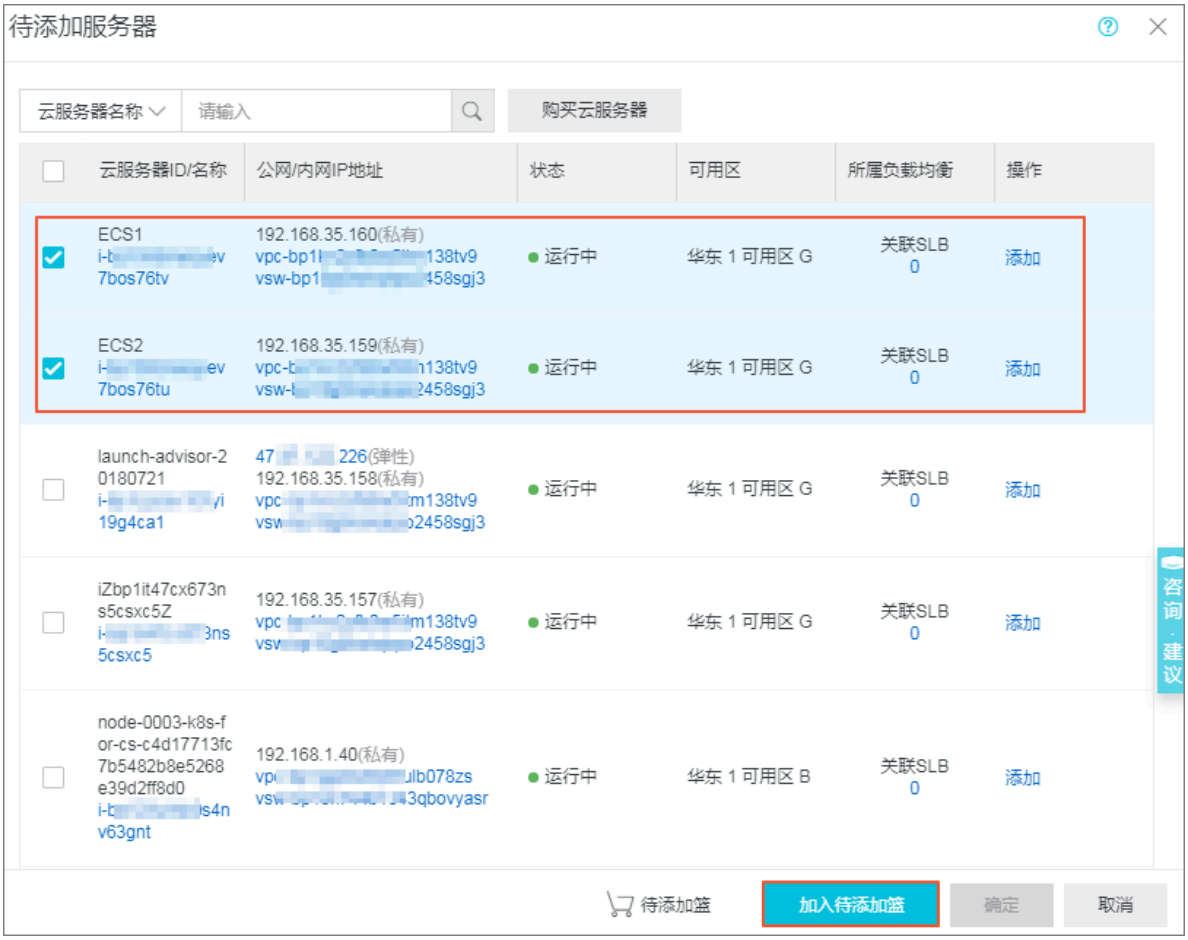
步骤三 添加后端服务器

添加处理前端请求的后端服务器。您可以使用实例配置的默认服务器组，也可以为监听配置一个虚拟服务器组或主备服务组。详情参见后端服务器概述。

本操作中，以默认后端服务器组为例：

1. 选择默认服务器组，单击添加。

2. 选择要添加的ECS实例，然后单击加入待添加篮。单击确定。



3. 配置添加的后端服务器的端口和权重。

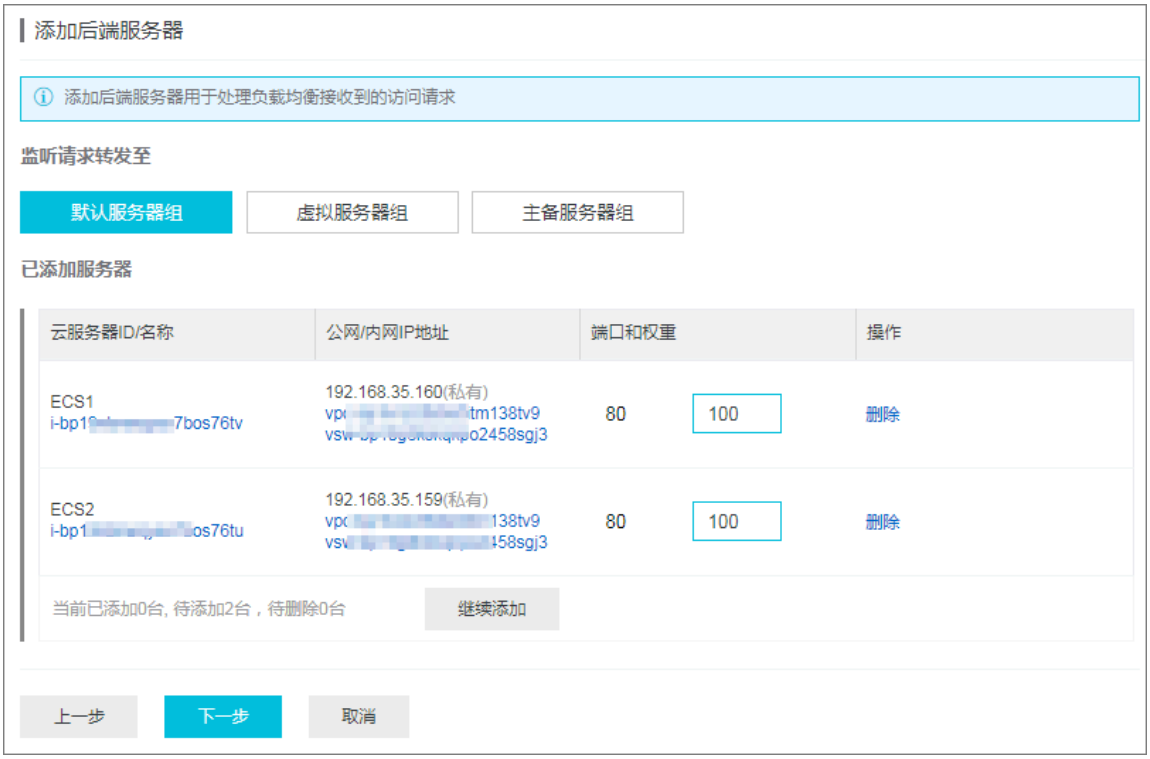
   - 端口

     后端服务器（ECS实例）开放用来接收请求的端口，端口范围为1-65535。同一个负载均衡实例内，后端服务器端口可以相同。

   - 权重

     后端服务器（ECS实例）的权重。权重越高的ECS实例将被分配到更多的访问请求。

     > **说明:**
     > 权重设置为0，该服务器不会再接受新请求。



4. 单击下一步。

步骤四 配置健康检查

负载均衡通过健康检查来判断后端服务器（ECS实例）的业务可用性。健康检查机制提高了前端业务整体可用性，避免了后端ECS异常对总体服务的影响。单击修改更改健康检查配置，详情参见配置健康检查。

步骤五 提交配置

完成以下操作，确认监听配置：

1. 在配置审核页面，检查监听配置，您可以单击修改更改配置。
2. 确认无误后，单击提交。

3. 在配置审核页面，配置成功后，单击确定。

配置成功后，您可以在监听页面查看已创建的监听。

相关操作

- 配置健康检查
- 管理默认服务器组
- 管理虚拟服务器组
- 管理主备服务器组
- 设置访问控制

2.4 添加HTTP监听

HTTP协议适用于需要对数据内容进行识别的应用，如Web应用、小的手机游戏等。您可以添加一个HTTP监听转发来自HTTP协议的请求。

前提条件

创建负载均衡实例。

步骤一 打开监听配置向导

完成以下操作，打开监听配置向导：

1. 登录负载均衡管理控制台。
2. 在左侧导航栏，选择实例 > 实例管理。
3. 选择实例的地域。
4. 选择以下一种方法，打开监听配置向导：

- 在实例管理页面，找到目标实例，然后单击添加配置向导。

- 在实例管理页面，单击目标实例ID。在监听页面，单击添加监听。

步骤二 配置协议监听

完成以下操作， 配置协议监听：

1. 在协议&监听页面，根据以下信息配置HTTP监听。

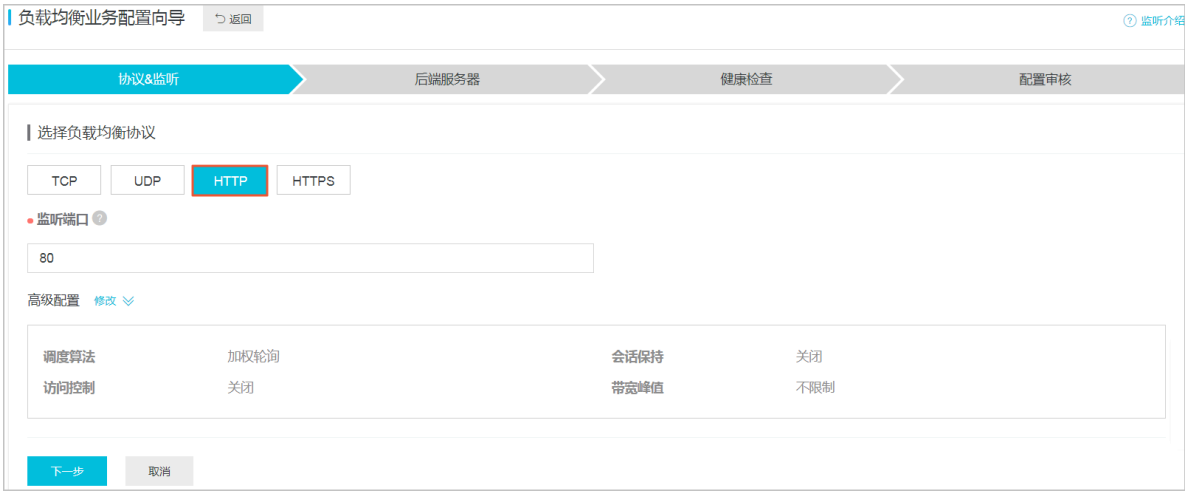
监听配置	说明
监听协议	选择监听的协议类型。 本操作，选择HTTP。
监听端口	用来接收请求并向后端服务器进行请求转发的监听端口。 端口范围为1-65535。 **说明:** 在同一个负载均衡实例内，监听端口不可重复。
高级配置	
调度算法	负载均衡支持轮询、加权轮询（WRR）、加权最小连接数（WLC）三种调度算法。 · 加权轮询：权重值越高的后端服务器，被轮询到的次数（概率）也越高。 · 轮询：按照访问顺序依次将外部请求依序分发到后端服务器。 · 加权最小连接数：除了根据每台后端服务器设定的权重值来进行轮询，同时还考虑后端服务器的实际负载（即连接数）。当权重值相同时，当前连接数越小的后端服务器被轮询到的次数（概率）也越高。

监听配置	说明
监听转发	选择是否将HTTP监听的流量转发到HTTPS监听。  说明: 如果开启监听转发，确保您已经创建了HTTPS监听。
会话保持	选择是否开启会话保持。 开启会话保持功能后，负载均衡会把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。 HTTP协议会话保持基于Cookie。负载均衡提供了两种Cookie处理方式： · 植入Cookie：您只需要指定Cookie的过期时间。 客户端第一次访问时，负载均衡会在返回请求中植入Cookie（即在HTTP/HTTPS响应报文中插入SERVERID），下次客户端携带此Cookie访问，负载均衡服务会将请求定向转发给之前记录到的后端服务器上。 · 重写Cookie：可以根据需要指定HTTPS/HTTP响应中插入的Cookie。您需要在后端服务器上维护该Cookie的过期时间和生存时间。 负载均衡服务发现用户自定义了Cookie，将会对原来的Cookie进行重写，下次客户端携带新的Cookie访问，负载均衡服务会将请求定向转发给之前记录到的后端服务器。 详情参考会话保持规则配置。
启用访问控制	选择是否启用访问控制。

监听配置	说明
访问控制方式	开启访问控制后，选择一种访问控制方式： · 白名单：仅转发来自所选访问控制策略组中设置的IP地址或地址段的请求，白名单适用于应用只允许特定IP访问的场景。 设置白名单存在一定业务风险。一旦设置白名单，就只有白名单中的IP可以访问负载均衡监听。如果开启了白名单访问，但访问策略组中没有添加任何IP，则负载均衡监听会转发全部请求。 · 黑名单：来自所选访问控制策略组中设置的IP地址或地址段的所有请求都不会转发，黑名单适用于应用只限制某些特定IP访问的场景。 如果开启了黑名单访问，但访问策略组中没有添加任何IP，则负载均衡监听会转发全部请求。
选择访问控制策略组	选择访问控制策略组，作为该监听的白名单或黑名单。 说明: IPv6实例只能绑定IPv6访问控制策略组，IPv4实例只能绑定IPv4访问控制策略组。详情参见访问控制策略组。
开启带宽峰值	选择是否配置监听带宽。 对于按带宽计费的负载均衡实例，您可以针对不同监听设定不同的带宽峰值来限定监听的流量。实例下所有监听的带宽峰值总和不能超过该实例的带宽。 默认不开启，各监听共享实例的总带宽。 说明: 使用流量计费方式的实例默认不限制带宽峰值。
连接空闲超时时间	指定连接空闲超时时间，取值范围为1-60秒。 在超时时间内一直没有访问请求，负载均衡会暂时中断当前连接，直到一下次请求来临时重新建立新的连接。 该功能已经在全部地域开放。
请求超时时间	指定请求超时时间，取值范围为1-180秒。 在超时时间内后端服务器一直没有响应，负载均衡将放弃等待，给客户端返回HTTP 504错误码。 该功能已经在全部地域开放。

监听配置	说明
Gzip数据压缩	开启该配置对特定文件类型进行压缩。 目前Gzip支持压缩的类型包括：text/xml、text/plain、text/css、application/javascript、application/x-javascript application/rss+xml、application/atom+xml、application/xml。
附加HTTP头字段	选择您要添加的自定义HTTP header字段： · 添加X-Forwarded-For字段获取客户端的IP地址。 · 添加X-Forwarded-Proto字段获取实例的监听协议。 · 添加SLB-IP字段获取负载均衡实例的公网IP。 · 添加SLB-ID字段获取负载均衡实例的ID。
获取真实IP	HTTP监听通过 X-Forwarded-For获取客户端真实IP。
创建完毕自动启动监听	是否在监听配置完成后启动负载均衡监听，默认开启。

2. 单击下一步。



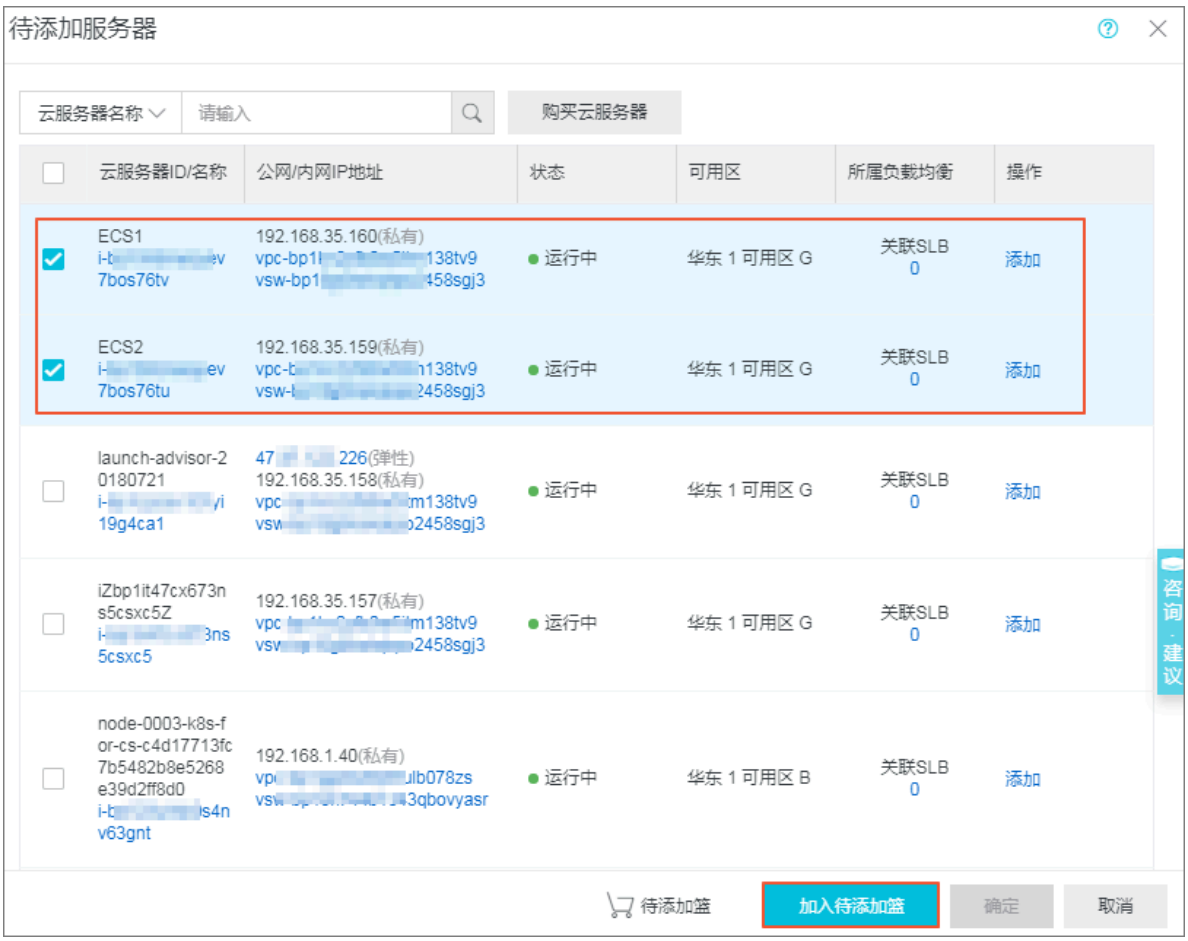
步骤三 添加后端服务器

添加处理前端请求的后端服务器。您可以使用实例配置的默认服务器组，也可以为监听配置一个虚拟服务器组或主备服务组。详情参见后端服务器概述。

本操作中，以默认后端服务器组为例：

1. 选择默认服务器组，单击添加。

2. 选择要添加的ECS实例，然后单击加入待添加篮。单击确定。



3. 配置添加的后端服务器的端口和权重。

- 端口

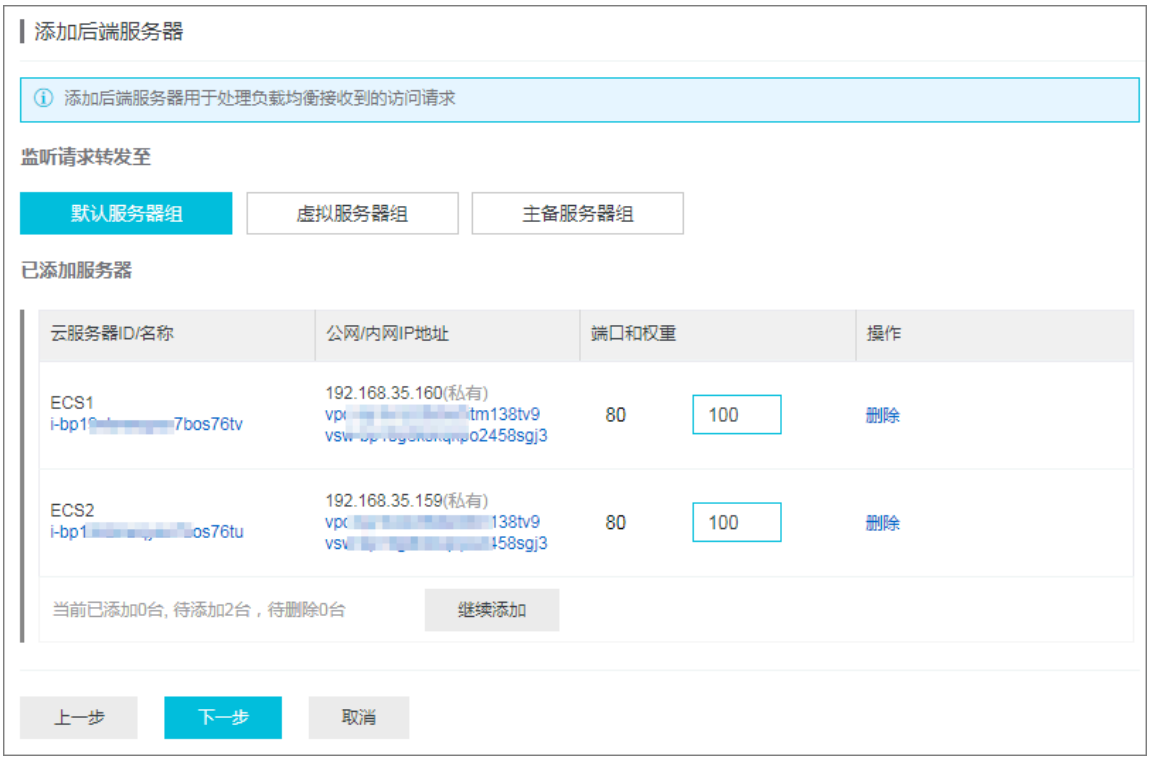
  后端服务器（ECS实例）开放用来接收请求的端口，端口范围为1-65535。同一个负载均衡实例内，后端服务器端口可以相同。

- 权重

  后端服务器（ECS实例）的权重。权重越高的ECS实例将被分配到更多的访问请求。

说明:

权重设置为0，该服务器不会再接受新请求。



4. 单击下一步。

步骤四 配置健康检查

负载均衡通过健康检查来判断后端服务器（ECS实例）的业务可用性。健康检查机制提高了前端业务整体可用性，避免了后端ECS异常对总体服务的影响。单击修改更改健康检查配置，详情参见配置健康检查。

步骤五 提交配置

完成以下操作，确认监听配置：

1. 在配置审核页面，检查监听配置，您可以单击修改更改配置。
2. 确认无误后，单击提交。
3. 在配置审核页面，配置成功后，单击确定。

配置成功后，您可以在监听页面查看已创建的监听。

相关操作

- 配置健康检查
- 管理默认服务器组
- 管理虚拟服务器组
- 管理主备服务器组
- 设置访问控制
- 基于域名/URL路径进行转发
- 管理扩展域名

2.5 添加HTTPS监听

HTTP协议适用于需要加密传输的应用。您可以添加一个HTTPS监听转发来自HTTPS协议的请求。

前提条件

创建负载均衡实例。

步骤一 打开监听配置向导

完成以下操作，打开监听配置向导：

1. 登录负载均衡管理控制台。
2. 在左侧导航栏，选择实例 > 实例管理。
3. 选择实例的地域。
4. 选择以下一种方法，打开监听配置向导：
   - 在实例管理页面，找到目标实例，然后单击添加配置向导。

   - 在实例管理页面，单击目标实例ID。在监听页面，单击添加监听。

步骤二 配置协议监听

完成以下操作， 配置协议监听：

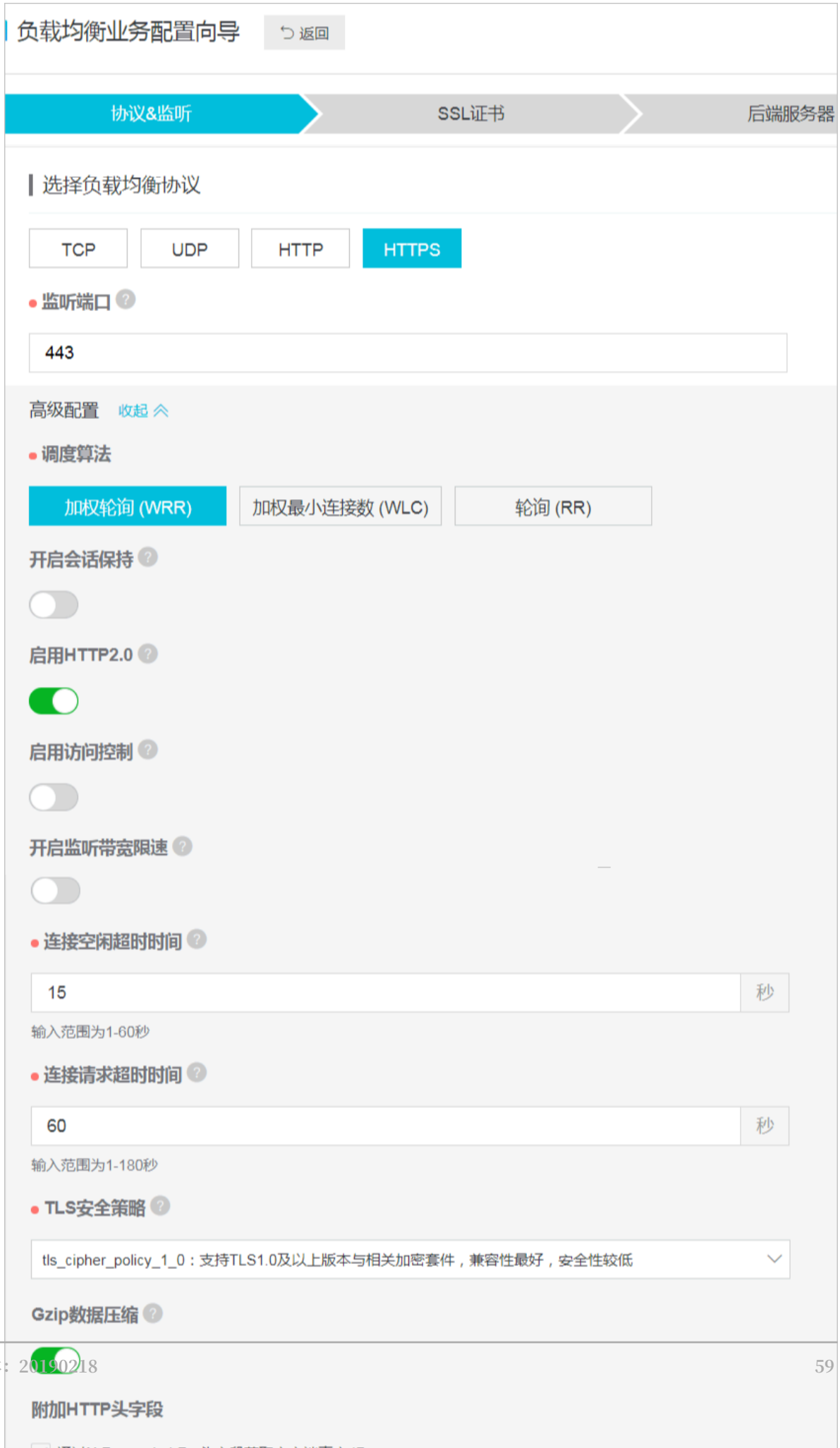
1. 在协议&监听页面，根据以下信息配置HTTPS监听。

监听配置	说明
监听协议	选择监听的协议类型。 本操作，选择HTTPS。
监听端口	用来接收请求并向后端服务器进行请求转发的监听端口。 端口范围为1-65535。 说明: 在同一个负载均衡实例内，监听端口不可重复。
高级配置	

监听配置	说明
调度算法	负载均衡支持轮询、加权轮询（WRR）、加权最小连接数（WLC）三种调度算法。 · 加权轮询：权重值越高的后端服务器，被轮询到的次数（概率）也越高。 · 轮询：按照访问顺序依次将外部请求依序分发到后端服务器。 · 加权最小连接数：除了根据每台后端服务器设定的权重值来进行轮询，同时还考虑后端服务器的实际负载（即连接数）。当权重值相同时，当前连接数越小的后端服务器被轮询到的次数（概率）也越高。
开启会话保持	选择是否开启会话保持。 开启会话保持功能后，负载均衡会把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。 HTTP协议会话保持基于Cookie。负载均衡提供了两种Cookie处理方式： · 植入Cookie：您只需要指定Cookie的过期时间。 客户端第一次访问时，负载均衡会在返回请求中植入Cookie（即在HTTP/HTTPS响应报文中插入SERVERID），下次客户端携带此Cookie访问，负载均衡服务会将请求定向转发给之前记录到的后端服务器上。 · 重写Cookie：可以根据需要指定HTTPS/HTTP响应中插入的Cookie。您需要在后端服务器上维护该Cookie的过期时间和生存时间。 负载均衡服务发现用户自定义了Cookie，将会对原来的Cookie进行重写，下次客户端携带新的Cookie访问，负载均衡服务会将请求定向转发给之前记录到的后端服务器。 详情参考会话保持规则配置。
启用HTTP2.0	选择是否启HTTP 2.0协议。
启用访问控制	选择是否启用访问控制。

监听配置	说明
访问控制方式	开启访问控制后，选择一种访问控制方式： · 白名单：仅转发来自所选访问控制策略组中设置的IP地址或地址段的请求，白名单适用于应用只允许特定IP访问的场景。 设置白名单存在一定业务风险。一旦设置白名单，就只有白名单中的IP可以访问负载均衡监听。如果开启了白名单访问，但访问策略组中没有添加任何IP，则负载均衡监听会转发全部请求。 · 黑名单：来自所选访问控制策略组中设置的IP地址或地址段的所有请求都不会转发，黑名单适用于应用只限制某些特定IP访问的场景。 如果开启了黑名单访问，但访问策略组中没有添加任何IP，则负载均衡监听会转发全部请求。
选择访问控制策略组	选择访问控制策略组，作为该监听的白名单或黑名单。 说明: IPv6实例只能绑定IPv6访问控制策略组，IPv4实例只能绑定IPv4访问控制策略组。详情参见访问控制策略组。
开启监听带宽限速	选择是否配置监听带宽。 对于按带宽计费的负载均衡实例，您可以针对不同监听设定不同的带宽峰值来限定监听的流量。实例下所有监听的带宽峰值总和不能超过该实例的带宽。 默认不开启，各监听共享实例的总带宽。 说明: 使用流量计费方式的实例默认不限制带宽峰值。
连接空闲超时时间	指定连接空闲超时时间，取值范围为1-60秒。 在超时时间内一直没有访问请求，负载均衡会暂时中断当前连接，直到一下次请求来临时重新建立新的连接。 该功能已经在全部地域开放。
连接请求超时时间	指定请求超时时间，取值范围为1-180秒。 在超时时间内后端服务器一直没有响应，负载均衡将放弃等待，给客户端返回HTTP 504错误码。 该功能已经在全部地域开放。
TLS安全策略	仅性能保障型实例支持选择使用的TLS安全策略。 TLS安全策略包含HTTPS可选的TLS协议版本和配套的加密算法套件，具体说明请参见管理*TLS*安全策略。

监听配置	说明
Gzip数据压缩	开启该配置对特定文件类型进行压缩。 目前Gzip支持压缩的类型包括：text/xml、text/plain、text/css、application/javascript、application/x-javascript application/rss+xml、application/atom+xml、application/xml。
附加HTTP头字段	选择您要添加的自定义HTTP header字段： · 添加X-Forwarded-For字段获取客户端的IP地址。 · 添加X-Forwarded-Proto字段获取实例的监听协议。 · 添加SLB-IP字段获取负载均衡实例的公网IP。 · 添加SLB-ID字段获取负载均衡实例的ID。
获取真实IP	HTTP监听通过 X-Forwarded-For获取客户端真实IP。
创建完毕自动启动监听	是否在监听配置完成后启动负载均衡监听，默认开启。


负载均衡业务配置向导
返回
协议&监听
SSL证书
后端服务器
选择负载均衡协议
TCP
UDP
HTTP
HTTPS
监听端口
443
高级配置
收起
调度算法
加权轮询 (WRR)
加权最小连接数 (WLC)
轮询 (RR)
开启会话保持
启用HTTP2.0
启用访问控制
开启监听带宽限速
连接空闲超时时间
15
秒
输入范围为1-60秒
连接请求超时时间
60
秒
输入范围为1-180秒
TLS安全策略
tls_cipher_policy_1_0：支持TLS1.0及以上版本与相关加密套件，兼容性最好，安全性较低
Gzip数据压缩
附加HTTP头字段

2. 单击下一步。

步骤三 配置SSL证书

添加HTTPS监听，您需要上传服务器证书或CA证书，如下表所示。

证书	说明	单向认证是否需要	双向认证是否需要
服务器证书	用来证明服务器的身份。 用户浏览器用来检查服务器发送的证书是否是由自己信赖的中心签发的。	是 服务器证书需要上传到负载均衡的证书管理系统。	是 服务器证书需要上传到负载均衡的证书管理系统。
客户端证书	用来证明客户端的身份。 用于证明客户端用户的身份，使得客户端用户在与服务器端通信时可以证明其真实身份。您可以用自签名的CA证书为客户端证书签名。	否	是 需要客户端进行安装。
CA 证书	服务器用CA证书验证客户端证书的签名。如果没有通过验证，拒绝连接。	否	是 服务器证书需要上传到负载均衡的证书管理系统。

在上传证书前，请注意：

- 上传的证书格式必须是PEM。详情参见证书要求。
- 证书上传到负载均衡后，负载均衡即可管理证书，不需要在后端ECS上绑定证书。
- 因为证书的上传、加载和验证都需要一些时间，所以使用HTTPS协议的实例生效也需要一些时间。一般一分钟后就会生效，最长不会超过三分钟。
- HTTPS监听使用的ECDHE算法簇支持前向保密技术，不支持将DHE算法簇所需要的安全增强参数文件上传，即PEM证书文件中含`BEGIN DH PARAMETERS`字段的字串上传。更多详细信息，参考证书要求。

- 目前负载均衡HTTPS监听不支持SNI（Server Name Indication），您可以改用TCP监听在后端ECS上实现SNI功能。
- HTTPS监听的会话ticket保持时间设置为300秒。
- HTTPS监听实际产生的流量会比账单流量更多一些，因为会使用一些流量用于协议握手。
- 在新建连接数很高的情况下，会占用较大的流量。

完成以下操作，配置SSL证书：

1. 选择已上传的服务器证书，或单击新建服务器证书上传一个服务器证书。

   详情参见创建证书。

2. 如果您要开启HTTPS双向认证，单击修改，开启双向认证。

3. 选择一个已上传的CA证书，或单击新建CA证书上传一个CA证书。

   您可以使用自签名的CA证书，详情参见生成CA证书。

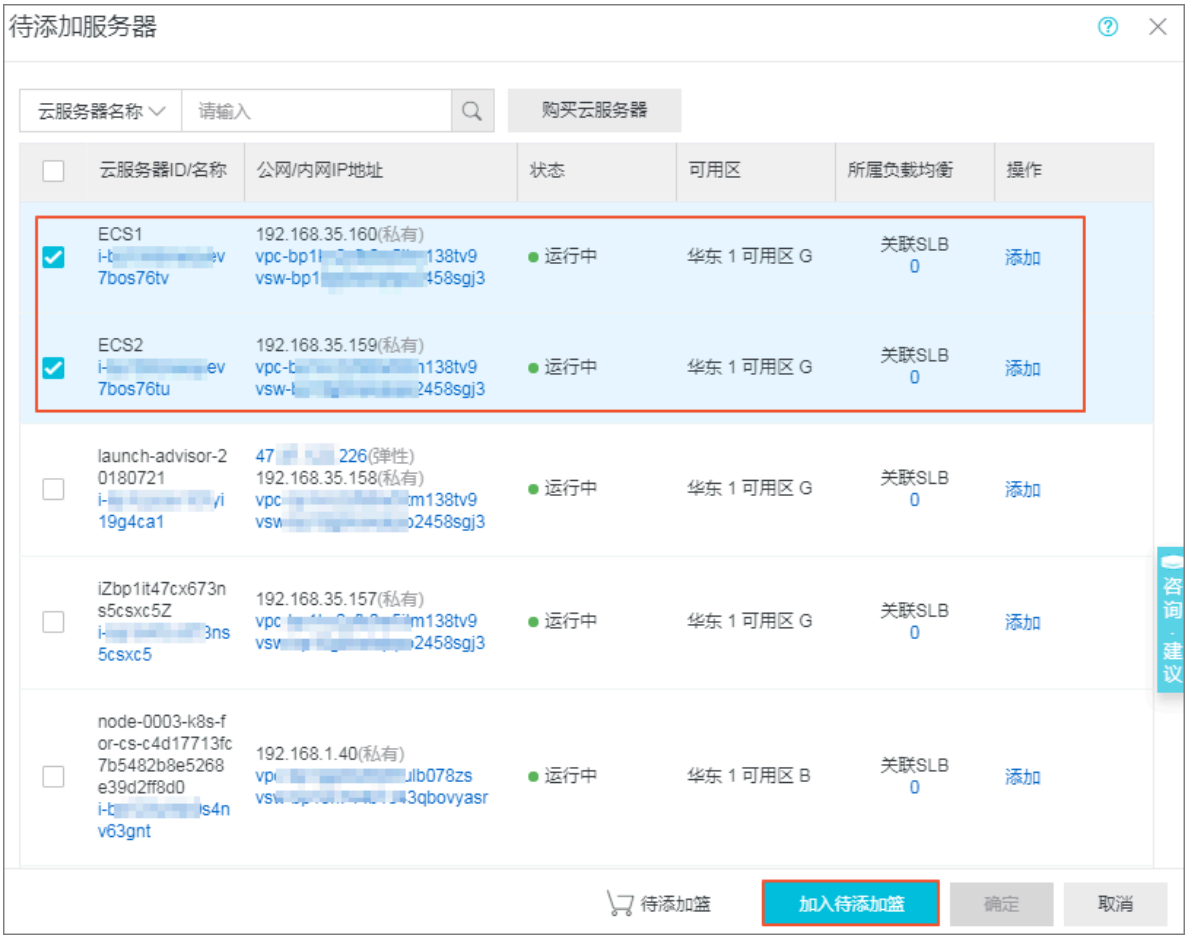
步骤四 添加后端服务器

添加处理前端请求的后端服务器。您可以使用实例配置的默认服务器组，也可以为监听配置一个虚拟服务器组或主备服务组。详情参见后端服务器概述。

本操作中，以默认后端服务器组为例：

1. 选择默认服务器组，单击添加。

2. 选择要添加的ECS实例，然后单击加入待添加篮。单击确定。



3. 配置添加的后端服务器的端口和权重。

- 端口

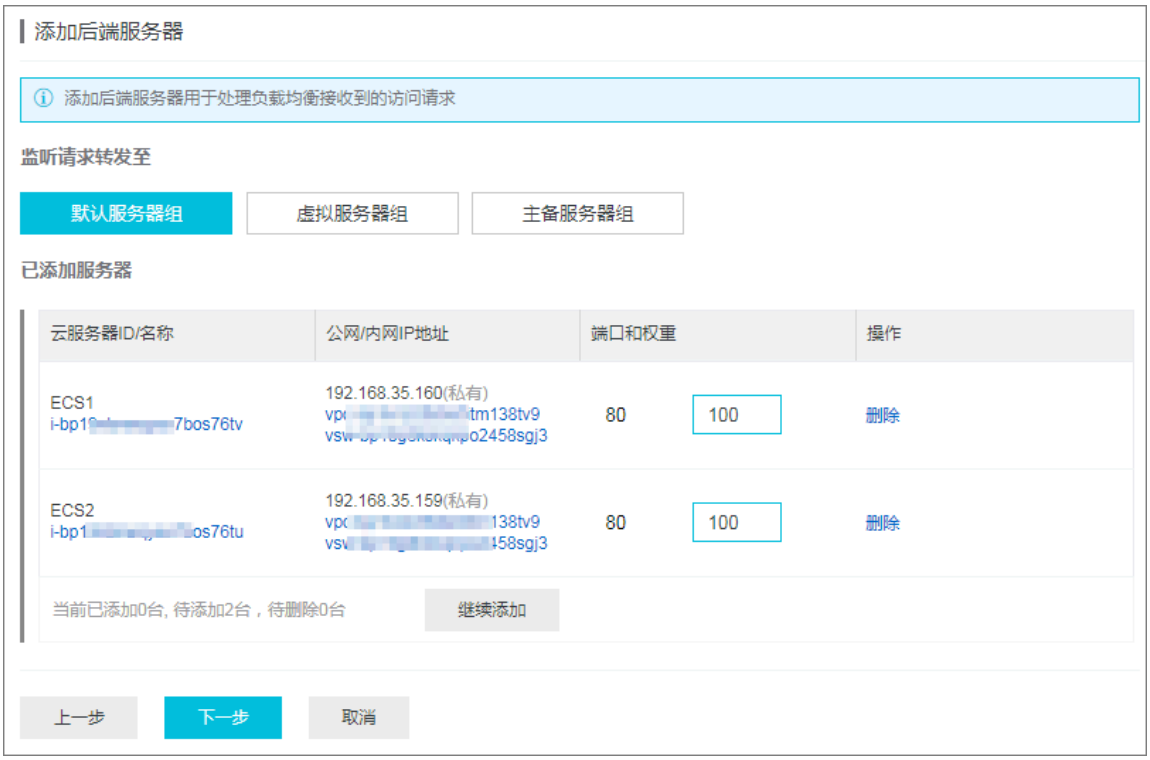
  后端服务器（ECS实例）开放用来接收请求的端口，端口范围为1-65535。同一个负载均衡实例内，后端服务器端口可以相同。

- 权重

  后端服务器（ECS实例）的权重。权重越高的ECS实例将被分配到更多的访问请求。

说明:

权重设置为0，该服务器不会再接受新请求。



4. 单击下一步。

步骤五 配置健康检查

负载均衡通过健康检查来判断后端服务器（ECS实例）的业务可用性。健康检查机制提高了前端业务整体可用性，避免了后端ECS异常对总体服务的影响。单击修改更改健康检查配置，详情参见配置健康检查。

步骤六 提交配置

完成以下操作，确认监听配置：

1. 在审核提交页面，检查监听配置，您可以单击修改更改配置。确认无误后，单击提交。
2. 在配置审核页面，在配置成功后，单击确定。

配置成功后，您可以在监听页面查看已创建的监听。

相关操作

- 配置健康检查
- 管理默认服务器组
- 管理虚拟服务器组
- 管理主备服务器组
- 生成CA证书
- 创建证书
- 设置访问控制
- 基于域名/URL路径进行转发
- 管理扩展域名

2.6 管理TLS安全策略

性能保障型负载均衡实例在创建和配置HTTPS监听时，支持选择使用的TLS安全策略。

您可以在添加或者配置HTTPS监听，配置协议&监听的高级配置时，选择TLS安全策略，详细操作参见添加HTTPS监听。


负载均衡业务配置向导
返回
协议&监听
SSL证书
后端服务器
选择负载均衡协议
TCP
UDP
HTTP
HTTPS
监听端口
443
高级配置
收起
调度算法
加权轮询 (WRR)
加权最小连接数 (WLC)
轮询 (RR)
开启会话保持
启用HTTP2.0
启用访问控制
开启监听带宽限速
连接空闲超时时间
15
秒
输入范围为1-60秒
连接请求超时时间
60
秒
输入范围为1-180秒
TLS安全策略
tls_cipher_policy_1_0：支持TLS1.0及以上版本与相关加密套件，兼容性最好，安全性较低
Gzip数据压缩

TLS安全策略包含HTTPS可选的TLS协议版本和配套的加密算法套件。

TLS安全策略

安全策略	特点	支持TLS版本	支持加密算法套件
tls_cipher_policy_1_0	兼容性最好，安全性较低	TLSv1.0、TLSv1.1和TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256、ECDHE-RSA-AES256-GCM-SHA384、ECDHE-RSA-AES128-SHA256、ECDHE-RSA-AES256-SHA384、AES128-GCM-SHA256、AES256-GCM-SHA384、AES128-SHA256、AES256-SHA256、ECDHE-RSA-AES128-SHA、ECDHE-RSA-AES256-SHA、AES128-SHA、AES256-SHA和DES-CBC3-SHA
tls_cipher_policy_1_1	兼容性较好，安全性较好	TLSv1.1和TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256、ECDHE-RSA-AES256-GCM-SHA384、ECDHE-RSA-AES128-SHA256、ECDHE-RSA-AES256-SHA384、AES128-GCM-SHA256、AES256-GCM-SHA384、AES128-SHA256、AES256-SHA256、ECDHE-RSA-AES128-SHA、ECDHE-RSA-AES256-SHA、AES128-SHA、AES256-SHA和DES-CBC3-SHA
tls_cipher_policy_1_2	兼容性较好，安全性很高	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256、ECDHE-RSA-AES256-GCM-SHA384、ECDHE-RSA-AES128-SHA256、ECDHE-RSA-AES256-SHA384、AES128-GCM-SHA256、AES256-GCM-SHA384、AES128-SHA256、AES256-SHA256、ECDHE-RSA-AES128-SHA、ECDHE-RSA-AES256-SHA、AES128-SHA、AES256-SHA和DES-CBC3-SHA
tls_cipher_policy_1_2_strict	仅支持前向安全的加密套件，安全性极高	TLSv1.2	ECDHE-RSA-AES128-GCM-SHA256、ECDHE-RSA-AES256-GCM-SHA384、ECDHE-RSA-AES128-SHA256、ECDHE-RSA-AES256-SHA384、ECDHE-RSA-AES128-SHA和ECDHE-RSA-AES256-SHA

TLS安全策略差异说明

安全策略		tls_cipher_policy_1_0	tls_cipher_policy_1_1	tls_cipher_policy_1_2	tls_cipher_policy_1_2_strict
TLS		1.2/1.1/1.0	1.2/1.1	1.2	1.2
CIPHER	ECDHE-RSA-AES128-GCM-SHA256	#	#	#	#
	ECDHE-RSA-AES256-GCM-SHA384	#	#	#	#
	ECDHE-RSA-AES128-SHA256	#	#	#	#
	ECDHE-RSA-AES256-SHA384	#	#	#	#
	AES128-GCM-SHA256	#	#	#	
	AES256-GCM-SHA384	#	#	#	
	AES128-SHA256	#	#	#	
	AES256-SHA256	#	#	#	
	ECDHE-RSA-AES128-SHA	#	#	#	#
	ECDHE-RSA-AES256-SHA	#	#	#	#
	AES128-SHA	#	#	#	
	AES256-SHA	#	#	#	
	DES-CBC3-SHA	#	#	#	

2.7 管理扩展域名

性能保障型负载均衡HTTPS监听支持挂载多个证书，将来自不同访问域名的请求转发至不同的后端服务器组。

扩展域名介绍

服务器名称指示（Server Name Indication, SNI）是对SSL / TLS协议的扩展，允许在单个IP地址上承载多个SSL证书。当客户端访问负载均衡时，默认使用访问域名配置的证书解密。如果找不到匹配的证书，则使用监听配置的证书。

> **说明:**
> 仅性能保障型负载均衡支持SNI。

当您有将多个域名绑定到同一个负载均衡服务地址上，然后通过不同的域名区分不同的访问来源并且使用HTTPS加密访问的需求时，可以通过配置扩展域名实现。

扩展域名功能已在各地域发布。

添加扩展域名

1. 登录负载均衡管理控制台。
2. 选择地域，查看该地域的所有负载均衡实例。
3. 单击负载均衡实例的ID。
4. 在左侧导航栏，单击监听。
5. 在监听页面，找到已创建的HTTPS监听，选择更多 > 扩展域名管理。

6. 单击添加扩展域名，配置扩展域名：
   a. 输入域名。域名只能使用字母、数字、连字符（-）、点（.）。

      域名转发策略支持精确匹配和通配符匹配两种模式：

      - 精确域名：www.aliyun.com
      - 通配符域名（泛域名）：*.aliyun.com, *.market.aliyun.com

        当前端请求同时匹配多条域名策略时，策略的匹配优先级为：精确匹配高于小范围通配符匹配，小范围通配符匹配高于大范围通配符匹配，如下表所示。

模式	请求测试URL	配置的域名转发策略		
		www.aliyun.com	*.aliyun.com	*.market.aliyun.com
精确匹配	www.aliyun.com	√	×	×
泛域名匹配	market.aliyun.com	×	√	×
泛域名匹配	info.market.aliyun.com	×	×	√

b. 选择该域名关联的证书。

> **说明:**
> 证书中的域名和您添加的扩展域名必须一致。

c. 单击确定。

7. 在监听页面，找到已创建的HTTPS监听，单击添加转发策略。
8. 在转发策略页面，单击添加转发策略。
9. 配置转发策略，详情参见基于域名/URL路径进行转发。

> **说明:**
> 确保转发策略中配置的域名和您添加的扩展域名一致。

编辑扩展域名

您可以替换已添加的扩展域名使用的证书。

完成以下操作，编辑扩展域名：

1. 登录负载均衡管理控制台。

2. 选择地域，查看该地域的所有负载均衡实例。
3. 单击负载均衡实例的ID。
4. 在左侧导航栏，单击监听。
5. 在监听页面，找到已创建的HTTPS监听，然后单击更多 > 扩展域名管理。
6. 找到目标扩展域名，然后单击编辑。
7. 在修改扩展域名对话框，选择新的证书，然后单击确定。

删除扩展域名

完成以下操作，删除扩展域名：

1. 登录负载均衡管理控制台。
2. 选择地域，查看该地域的所有负载均衡实例。
3. 单击负载均衡实例的ID。
4. 在左侧导航栏，单击监听。
5. 在监听页面，找到已创建的HTTPS监听，然后单击更多 > 扩展域名管理。
6. 找到目标扩展域名，然后单击删除。

7. 在弹出的对话框，单击确定。

2.8 共享实例带宽

负载均衡支持按带宽计费的负载均衡实例下的所有监听共享实例的总带宽。在创建监听时，您可以设置带宽峰值也可以选择不设置。

- 配置：您可以对监听的带宽进行限制，但所有监听带宽峰值的总和不能超过实例的带宽峰值。
- 不限制：不限制带宽的情况下，实例下的监听共享实例带宽。

如何共享带宽?

假如您购买了一个带宽峰值为 10MB 的负载均衡实例，并在该实例下创建了三个监听（监听A、监听B和监听C）。监听A的带宽峰值设置为 4MB，另外两个监听没有设置带宽峰值。三个监听的带宽使用可能出现如下几种情况：

- 如果监听A和监听C一直没有出流量，那么监听B最多也只能跑满剩余的 6MB 带宽（10MB - 4MB)。
- 如果监听C一直没有出流量，而监听B的出流量很大，超过了剩余的 6MB 带宽。此时，监听B已经产生丢包，而监听A只有 4MB 的出流量，没有超过设置的带宽峰值，所以不会产生丢包。
- 如果监听A一直是满速在跑（监听峰值 4MB），而后监听B和监听C也有出流量并且两个监听的流量很大，那么监听B和监听C就会共享（竞争）剩余的 6MB 带宽。此时，监听A的流量不会受监听B和监听C的影响，始终能达到预留的 4MB 峰值；如果监听B和监听C出流量同等大小，两个监听占用的带宽去会趋近于均分。

因此，对监听带宽的限制值是资源预留，这是为了保证核心的业务始终有足够的带宽。非核心的业务可以不设置监听带宽值，它们竞争实例剩余的带宽资源。

2.9 配置监听转发（redirect）

HTTPS是加密数据传输协议，安全性高。负载均衡支持将HTTP访问重定向至HTTPS，方便您进行全站HTTPS部署。负载均衡已经在全部地域开放了HTTP重定向功能。

前提条件

已创建了HTTPS监听，详情参见添加*HTTPS*监听。

背景信息

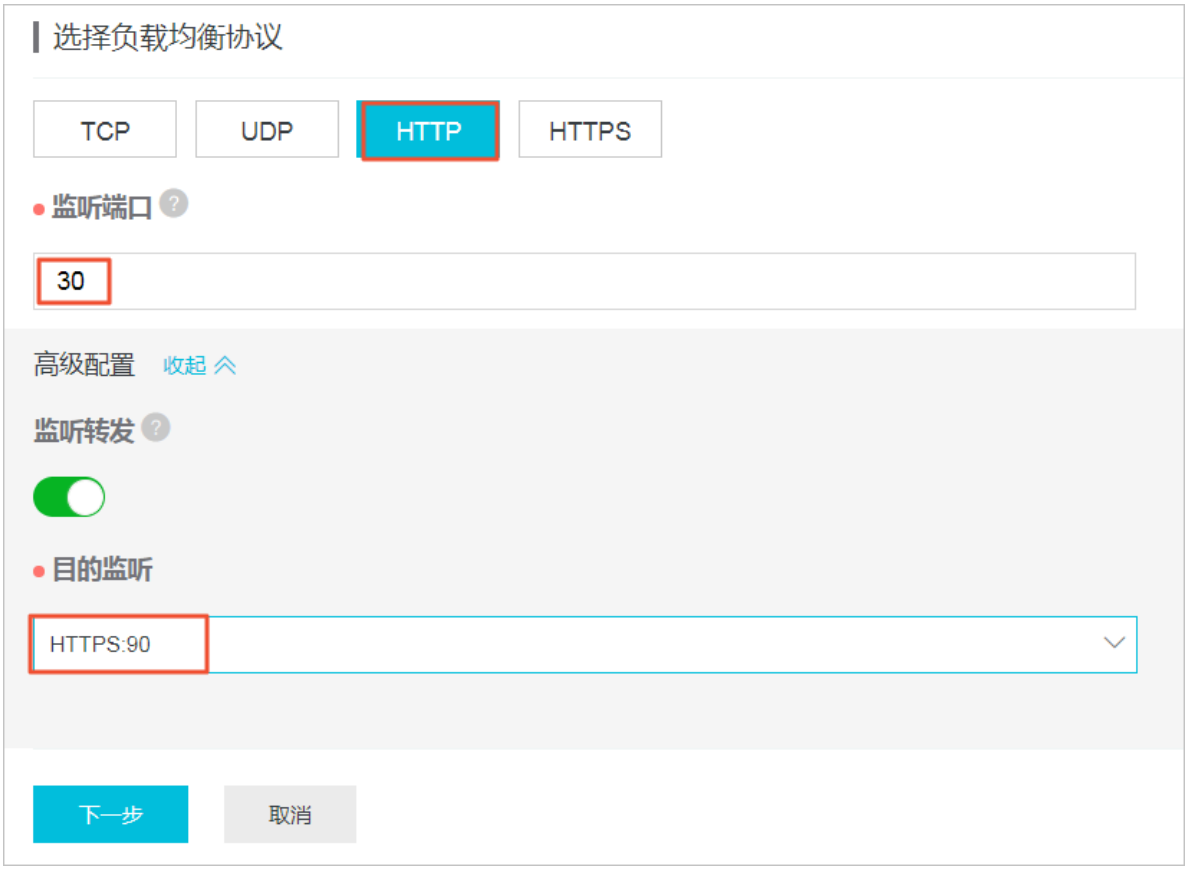
仅负载均衡新版控制台支持监听转发功能。

操作步骤

1. 登录负载均衡管理控制台。

2. 在顶部菜单栏选择负载均衡实例的所属地域。
3. 在实例管理页面，单击目标实例的ID链接。
4. 在监听页签下，单击添加监听。
5. 在添加监听对话框，负载均衡协议选择HTTP，配置监听端口。
6. 在高级配置下，开启监听转发，选择目的监听。

   此处目的监听可以是该实例下任意端口的HTTPS监听。



7. 单击下一步。
8. 确认后，单击提交。

   转发开启后，所有来自HTTP的访问都会转发至HTTPS，并根据HTTPS的监听配置进行转发。

3 健康检查

3.1 健康检查介绍

负载均衡通过健康检查来判断后端服务器（ECS实例）的业务可用性。健康检查机制提高了前端业务整体可用性，避免了后端ECS异常对总体服务的影响。

开启健康检查功能后，当后端某台ECS健康检查出现异常时，负载均衡会自动将新的请求分发到其它健康检查正常的ECS上；而当该ECS恢复正常运行时，负载均衡会将其自动恢复到负载均衡服务中。

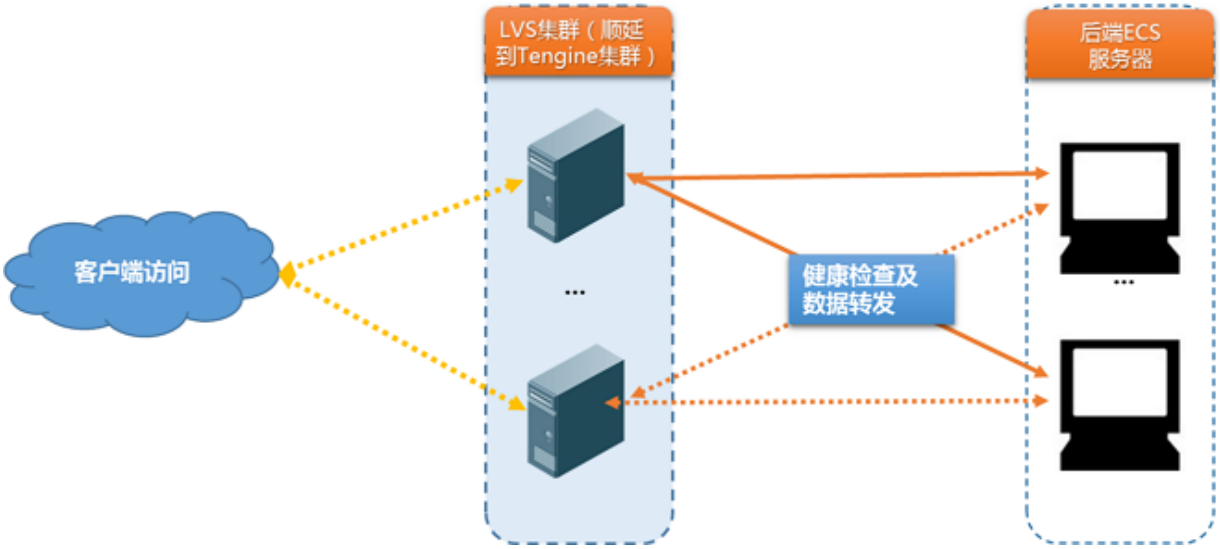
如果您的业务对负载敏感性高，高频率的健康检查探测可能会对正常业务访问造成影响。您可以结合业务情况，通过降低健康检查频率、增大健康检查间隔、七层检查修改为四层检查等方式，来降低对业务的影响。但为了保障业务的持续可用，不建议关闭健康检查。

健康检查过程

负载均衡采用集群部署。LVS集群或Tengine集群内的相关节点服务器同时承载了数据转发和健康检查职责。

LVS集群内不同服务器分别独立、并行地根据负载均衡策略进行数据转发和健康检查操作。如果某一台LVS节点服务器对后端某一台ECS健康检查失败，则该LVS节点服务器将不会再将新的客户端请求分发给相应的异常ECS。LVS集群内所有服务器同步进行该操作。

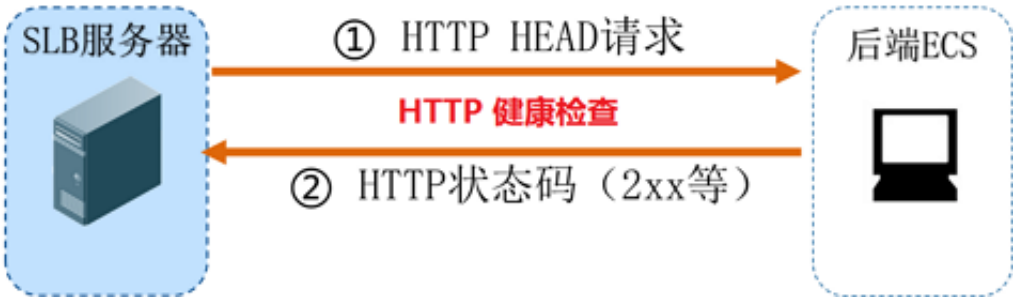
如下图所示，负载均衡健康检查使用的地址段是100.64.0.0/10，后端服务器务必不能屏蔽该地址段。您无需在ECS安全组中额外针对该地址段配置放行策略，但如有配置iptables等安全策略，请务必放行（100.64.0.0/10 是阿里云保留地址，其他用户无法分配到该网段内，不会存在安全风险）。



HTTP/HTTPS监听健康检查机制

针对七层（HTTP或HTTPS协议）监听，健康检查通过HTTP HEAD探测来获取状态信息，如下图所示。

对于HTTPS监听，证书在负载均衡系统中进行管理。负载均衡与后端ECS之间的数据交互（包括健康检查数据和业务交互数据），不再通过HTTPS进行传输，以提高系统性能。

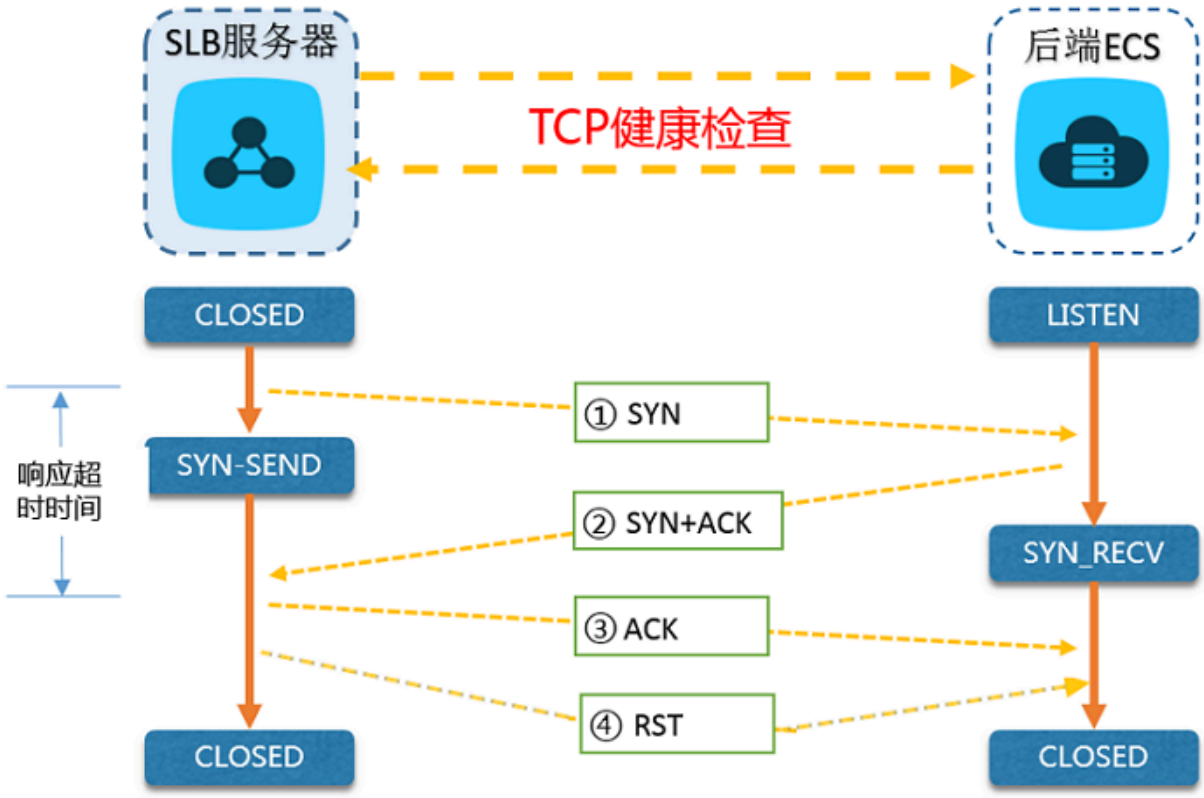


七层监听的检查机制如下：

1. Tengine节点服务器根据监听的健康检查配置，向后端ECS的内网IP+【健康检查端口】+【检查路径】发送HTTP HEAD请求（包含设置的【域名】）。
2. 后端ECS收到请求后，根据相应服务的运行情况，返回HTTP状态码。
3. 如果在【响应超时时间】之内，Tengine节点服务器没有收到后端ECS返回的信息，则认为服务无响应，判定健康检查失败。
4. 如果在【响应超时时间】之内，Tengine节点服务器成功接收到后端ECS返回的信息，则将该返回信息与配置的状态码进行比对。如果匹配则判定健康检查成功，反之则判定健康检查失败。

TCP监听健康检查机制

针对四层TCP监听，为了提高健康检查效率，健康检查通过定制的TCP探测来获取状态信息，如下图所示。



TCP监听的检查机制如下：

1. LVS节点服务器根据监听的健康检查配置，向后端ECS的内网IP+【健康检查端口】发送TCP SYN数据包。
2. 后端ECS收到请求后，如果相应端口正在正常监听，则会返回SYN+ACK数据包。
3. 如果在【响应超时时间】之内，LVS节点服务器没有收到后端ECS返回的数据包，则认为服务无响应，判定健康检查失败；并向后端ECS发送RST数据包中断TCP连接。
4. 如果在【响应超时时间】之内，LVS节点服务器成功收到后端ECS返回的数据包，则认为服务正常运行，判定健康检查成功，而后向后端ECS发送RST数据包中断TCP连接。

说明：

正常的TCP三次握手，LVS节点服务器在收到后端ECS返回的SYN+ACK数据包后，会进一步发送ACK数据包，随后立即发送RST数据包中断TCP连接。

该实现机制可能会导致后端ECS认为相关TCP连接出现异常（非正常退出），并在业务软件如Java连接池等日志中抛出相应的错误信息，如`Connection reset by peer`。

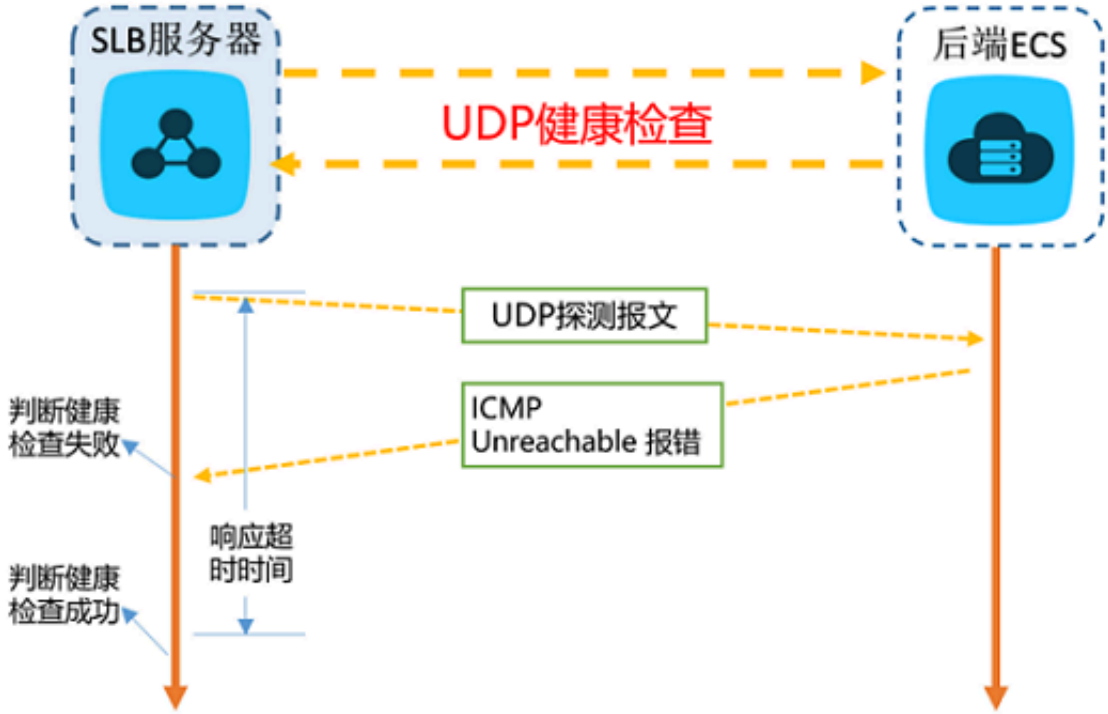
解决方案：

- TCP监听采用HTTP方式进行健康检查。

- 在后端ECS配置了获取客户端真实IP后，忽略来自前述负载均衡服务地址段相关访问导致的连接错误。

UDP监听健康检查

针对四层UDP监听，健康检查通过UDP报文探测来获取状态信息，如下图所示。



UDP监听的检查机制如下：

1. LVS节点服务器根据监听的健康检查配置，向后端ECS的内网IP+【健康检查端口】发送UDP报文。
2. 如果后端ECS相应端口未正常监听，则系统会返回类似返回 `port XX unreachable` 的ICMP报错信息；反之不做任何处理。
3. 如果在【响应超时时间】之内，LVS节点服务器收到了后端ECS返回的上述错误信息，则认为服务异常，判定健康检查失败。
4. 如果在【响应超时时间】之内，LVS节点服务器没有收到后端ECS返回的任何信息，则认为服务正常，判定健康检查成功。

说明：

当前UDP协议服务健康检查可能存在服务真实状态与健康检查不一致的问题：

如果后端ECS是Linux服务器，在大并发场景下，由于Linux的防ICMP攻击保护机制，会限制服务器发送ICMP的速度。此时，即便服务已经出现异常，但由于无法向前端返回`port XX`

unreachable报错信息，会导致负载均衡由于没收到ICMP应答进而判定健康检查成功，最终导致服务真实状态与健康检查不一致。

解决方案：

负载均衡通过发送您指定的字符串到后端服务器，必须得到指定应答后才认为检查成功。但该实现机制需要客户端程序配合应答。

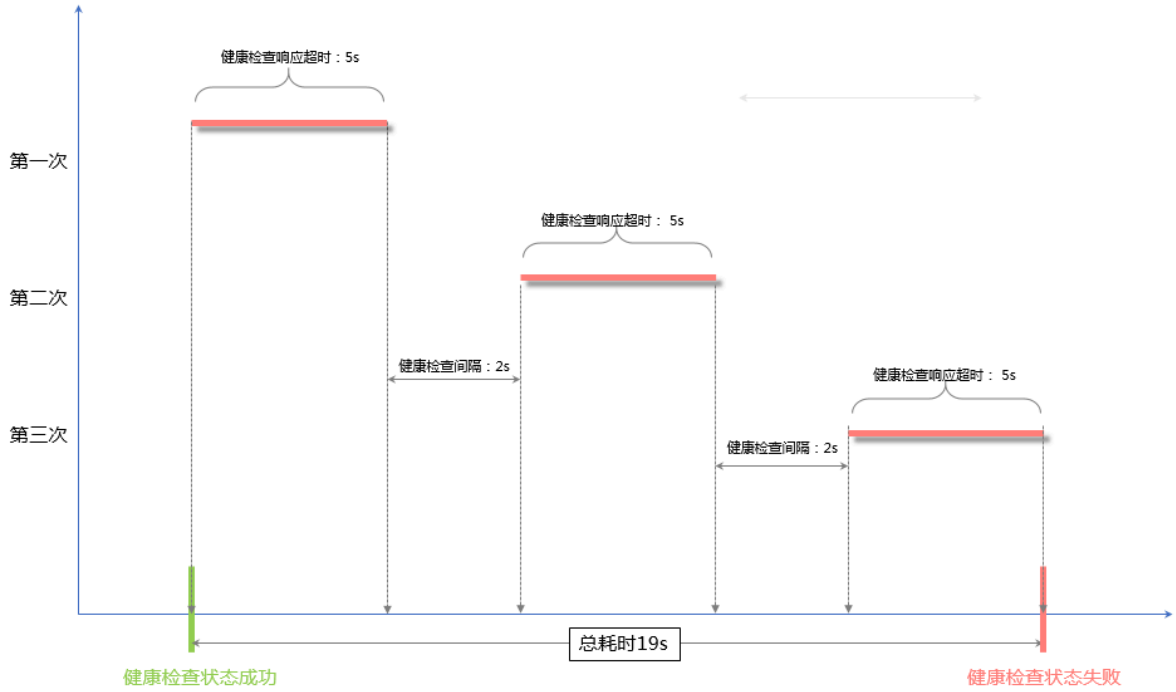
健康检查时间窗

健康检查机制的引入，有效提高了业务服务的可用性。但是，为了避免频繁的健康检查失败引起的切换对系统可用性的冲击，健康检查只有在健康检查时间窗内连续多次检查成功或失败后，才会进行状态切换。健康检查时间窗由以下三个因素决定：

- 健康检查间隔 (每隔多久进行一次健康检查)
- 响应超时时间 (等待服务器返回健康检查的时间)
- 检查阈值 (健康检查连续成功或失败的次数)

健康检查时间窗的计算方法如下：

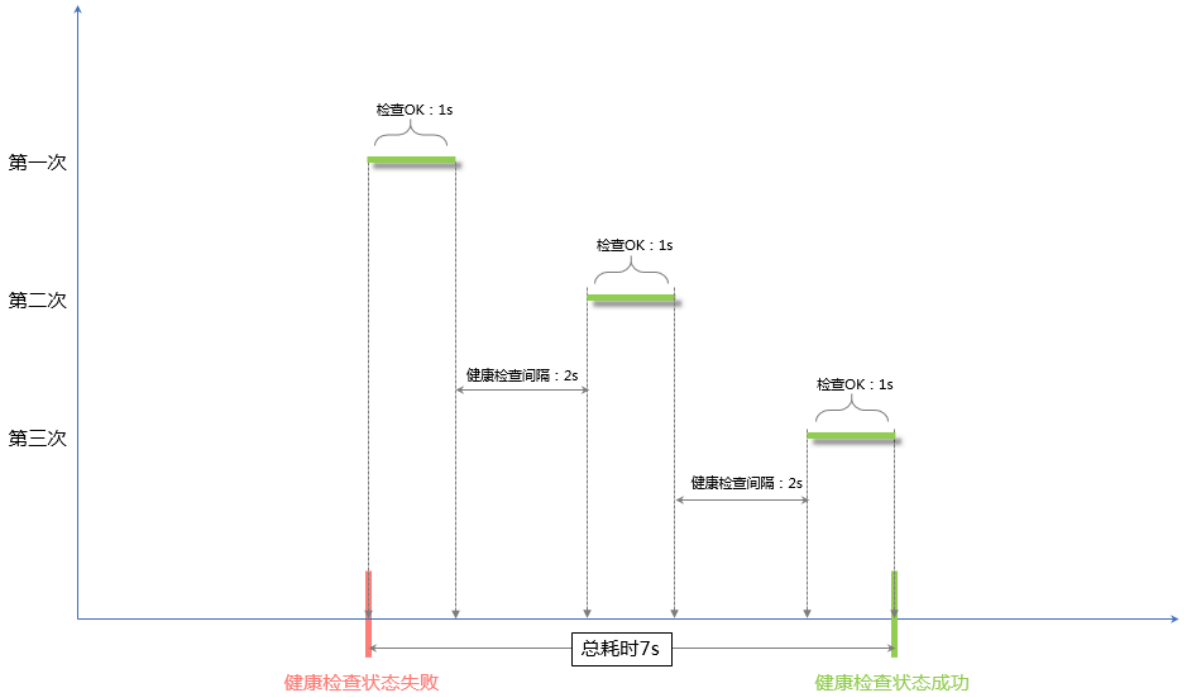
- 健康检查失败时间窗=响应超时时间×不健康阈值+检查间隔×(不健康阈值-1)



- 健康检查成功时间窗= (健康检查成功响应时间x健康阈值)+检查间隔x(健康阈值-1)

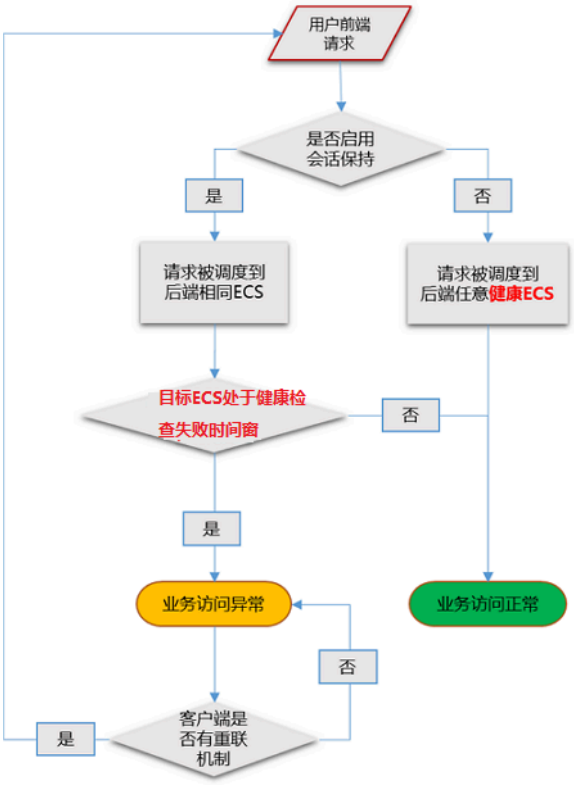
说明：

健康检查成功响应时间是一次健康检查请求从发出到响应的时间。当采用TCP方式健康检查时，由于仅探测端口是否存活，因此该时间非常短，几乎可以忽略不计。当采用HTTP方式健康检查时，该时间取决于应用服务器的性能和负载，但通常都在秒级以内。



健康检查状态对请求转发的影响如下：

- 如果目标ECS的健康检查失败，新的请求不会再分发到相应ECS上，所以对前端访问没有影响。
- 如果目标ECS的健康检查成功，新的请求会分发到该ECS上，前端访问正常。
- 如果目标ECS存在异常，正处于健康检查失败时间窗，而健康检查还未达到检查失败判定次数（默认为三次），则相应请求还是会被分发到该ECS，进而导致前端访问请求失败。



3.2 配置健康检查

您可以在添加监听时配置健康检查。通常，使用默认的健康检查配置即可。

配置健康检查

您可以通过控制台或API配置监听的健康检查。更多详细信息，参见健康检查介绍和健康检查常见问题。

完成以下操作，配置健康检查：

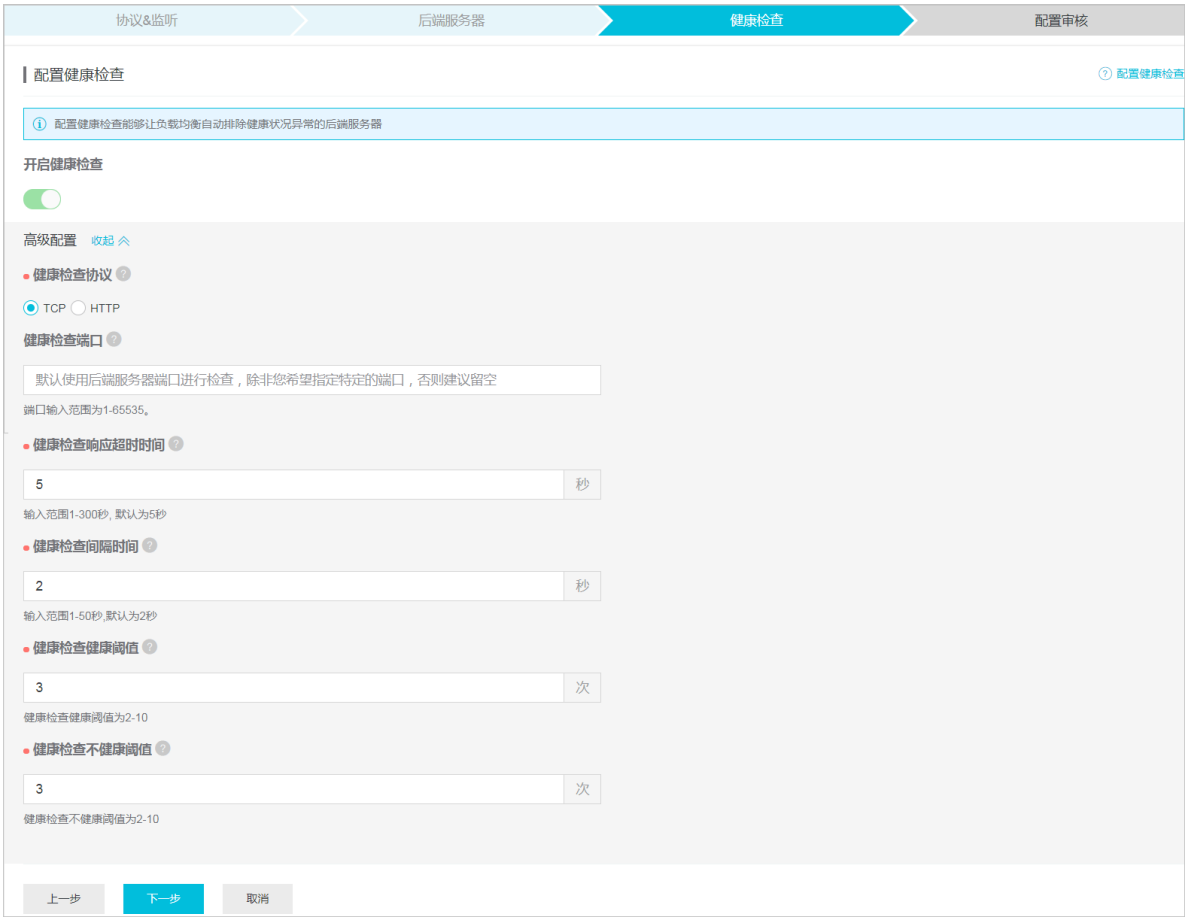
1. 登录负载均衡管理控制台。
2. 选择地域，查看该地域的所有负载均衡实例。
3. 单击负载均衡实例的ID。
4. 在实例详情页面，单击监听。
5. 单击添加监听或目标监听的配置选项。
6. 在健康检查页面，配置健康检查。

   在配置健康检查时，建议您使用默认值。

表 3-1: 健康检查配置说明

健康检查配置	说明
健康检查协议	监听为TCP协议时，健康检查方式可选TCP或HTTP模式。 · TCP模式的健康检查是基于网络层探测。 · HTTP模式的健康检查是通过发送head请求。
域名和检查路径（仅限HTTP方式的健康检查）	HTTP健康检查默认由负载均衡系统通过后端ECS内网IP地址向该服务器应用配置的缺省首页发起http head请求。 如果您用来进行健康检查的页面并不是应用服务器的缺省首页，需要指定具体的检查路径。 因为有些应用服务器会对请求中的host字段做校验，即要求请求头中必须存在host字段。如果在健康检查中配置了域名，则SLB会将域名配置到host字段中去，反之，如果没有配置域名，SLB则不会在请求中附带host字段，因此健康检查请求就会被服务器拒绝，可能导致健康检查失败。综上原因，如果您的应用服务器需要校验请求的host字段校，那么则需要配置相关的域名，确保健康检查正常工作。
正常状态码（仅限HTTP方式的健康检查）	选择健康检查正常的HTTP状态码。 默认值为http_2xx和http_3xx。
健康检查端口	健康检查服务访问后端时的探测端口。 默认值为配置监听时指定的后端端口。 说明: 如果该监听配置了虚拟服务器组或主备服务器组，且组内的ECS实例的端口都不相同，此时不需要配置检查端口。负载均衡系统会使用各自ECS的后端端口进行健康检查。
健康检查响应超时时间	接收来自运行状况检查的响应需要等待的时间。如果后端ECS在指定的时间内没有正确响应，则判定为健康检查失败。 范围是1-300秒，UDP监听的默认值为10秒，HTTP/HTTPS/TCP监听的默认值为5秒。
健康检查间隔时间	进行健康检查的时间间隔。 LVS集群内所有节点，都会独立、并行地遵循该属性对后端ECS进行健康检查。由于各LVS节点的检查时间并不同步，所以，如果从后端某一ECS上进行单独统计，会发现来自负载均衡的健康检查请求在时间上并不会遵循上述时间间隔。 范围是1-50秒，UDP监听的默认值为5秒，HTTP/HTTPS/TCP监听的默认值为2秒。
健康检查不健康阈值	同一LVS节点服务器针对同一ECS服务器，从成功到失败的连续健康检查失败次数。 可选值2-10，默认为3次。

健康检查配置	说明
健康检查健康阈值	同一LVS节点服务器针对同一ECS服务器，从失败到成功的连续健康检查成功次数。 可选值 2-10，默认为3次。
健康检查请求和健康检查返回结果	为UDP监听配置健康检查时，您可以在健康检查请求中输入请求的内容（比如youraccountID），在健康检查返回结果中输入预期的返回结果（比如slb123）。 同时在后端服务器的应用逻辑中加入相应的健康检查应答逻辑，如收到youraccountID的请求时，回应slb123。 此时，当负载均衡收到后端服务器发来的正确响应时，则认为健康检查成功，否则认为健康检查失败。此方式能最大程度确保健康检查的可靠性。



健康检查响应超时和健康检查间隔示例

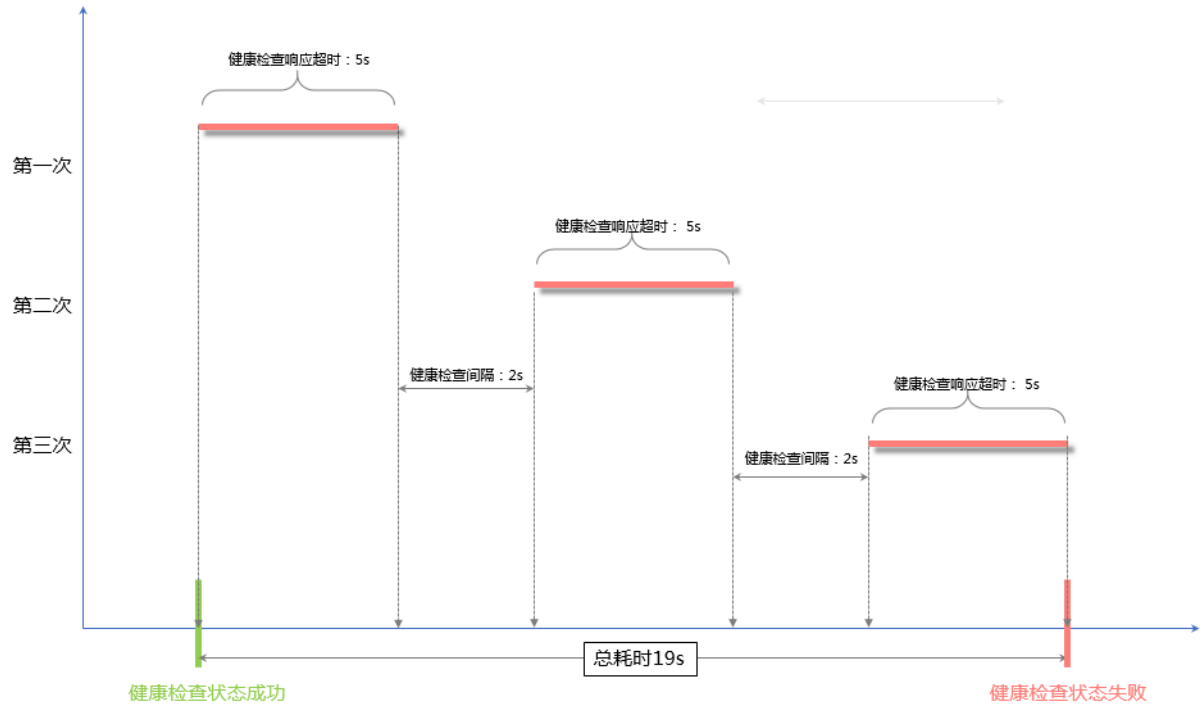
以如下健康检查配置为例：

- 响应超时时间：5秒
- 健康检查间隔：2秒
- 健康阈值：3次

· 不健康阈值：3次

健康检查失败时间窗=响应超时时间×不健康阈值+检查间隔×(不健康阈值-1)，即5×3+2×（3-1）=19s。

从健康状态到不健康状态的检查过程如下图所示：

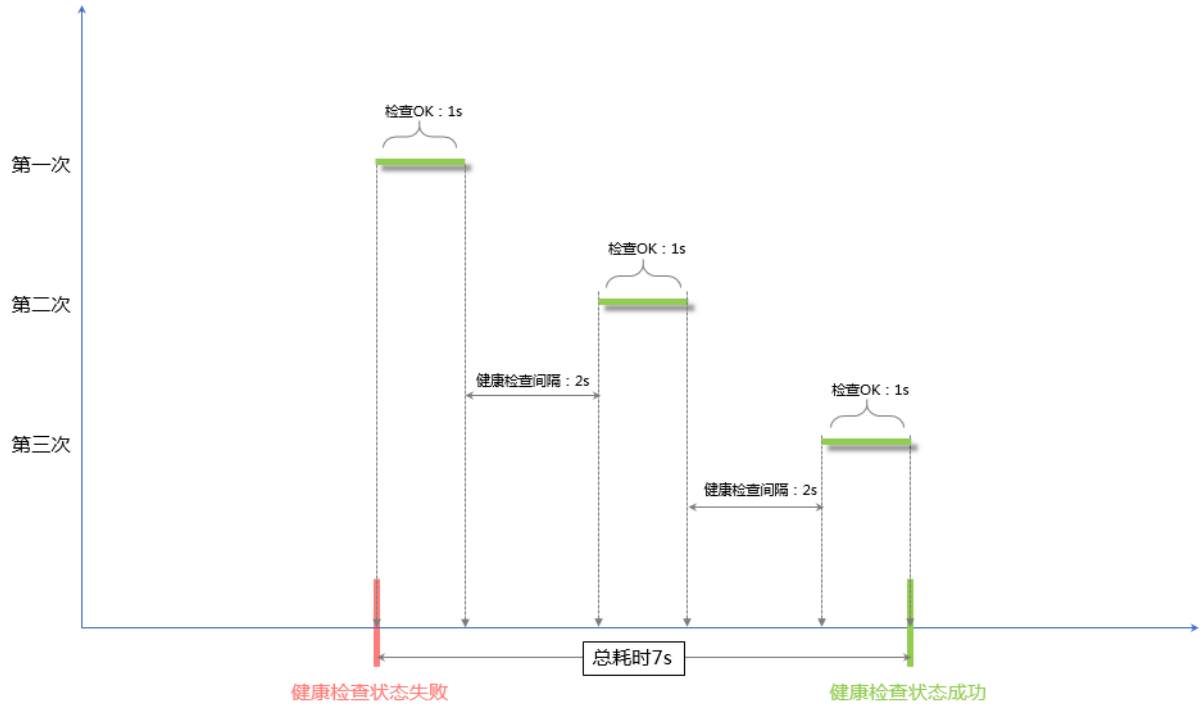


健康检查成功时间窗= (健康检查成功响应时间×健康阈值)+检查间隔×(健康阈值-1)，即（1×3）+2×（3-1）=7s。

说明:

健康检查成功响应时间是一次健康检查请求从发出到响应的时间。当采用TCP方式健康检查时，由于仅探测端口是否存活，因此该时间非常短，几乎可以忽略不计。当采用HTTP方式健康检查时，该时间取决于应用服务器的性能和负载，但通常都在秒级以内。

从不健康状态到健康的状态检查过程如下图所示（假设服务器响应健康检查请求需要耗时1s）：



HTTP健康检查中域名的设置

当使用HTTP方式进行健康检查时，可以设置健康检查的域名，但并非强制选项。因为有些应用服务器会对请求中的host字段做校验，即要求请求头中必须存在host字段。如果在健康检查中配置了域名，则SLB会将域名配置到host字段中去，反之，如果没有配置域名，SLB则不会在请求中附带host字段，因此健康检查请求就会被服务器拒绝，可能导致健康检查失败。综上原因，如果您的应用服务器需要校验请求的host字段，那么则需要配置相关的域名，确保健康检查正常工作。

3.3 关闭健康检查

您可以关闭健康检查功能，但关闭健康检查后，当后端某个ECS健康检查出现异常时，负载均衡还是会把请求转发到该异常的ECS上，造成部分业务不可访问。所以建议一般情况下不要关闭健康检查。

背景信息

> 说明:
> 只有HTTP和HTTPS监听支持关闭健康检查。UDP和TCP监听无法关闭健康检查。

操作步骤

1. 登录负载均衡管理控制台。
2. 在实例管理页面，单击负载均衡实例的ID。
3. 在监听页签下，单击监听操作列的配置。

4. 在配置监听对话框，单击下一步至健康检查页签。

5. 关闭健康检查开关，单击下一步，单击提交，然后单击确定。

4 后端服务器

4.1 后端服务器概述

在使用负载均衡服务前，您需要添加ECS实例作为负载均衡实例的后端服务器，用来接收负载均衡监听转发的请求。

负载均衡服务通过设置虚拟服务地址，将添加的同一地域的多台ECS实例虚拟成一个高性能、高可用的应用服务池。您也可以通过虚拟服务器组管理后端服务器。不同的监听可以关联不同的服务器组，这样一个负载均衡实例可以将请求根据不同监听转发给不同的服务器组内不同端口的后端服务器。

说明:

如果您在配置监听时，选择使用虚拟服务器组，那么该监听会将请求转发到关联的服务器组中的ECS，而不会再将请求转发给默认服务器组中的ECS实例。

您可以在任意时刻增加或减少负载均衡实例的后端ECS数量，还可以在不同ECS实例之间进行切换。但是为了保证您对外服务的稳定性，确保在执行上述操作时，开启了负载均衡的健康检查功能并同时保证负载均衡实例中至少有一台正常运行的ECS。

添加后端服务器时，注意：

- 负载均衡不支持跨地域部署，确保ECS实例的所属地域和负载均衡实例的所属地域相同。
- 负载均衡本身不会限制后端ECS实例使用哪种操作系统，只要您的两台ECS实例中的应用服务部署是相同的且保证数据的一致性即可。建议您选择相同操作系统的ECS实例作为后端服务器，以便日后管理和维护。
- 一个负载均衡实例最多支持添加50个监听，每个监听对应后端ECS实例上的一个应用。负载均衡的监听端口对应后端ECS实例上的应用服务端口。
- 您可以指定后端服务器池内各ECS实例的转发权重。权重越高的ECS实例将被分配到更多的访问请求。
- 如果您同时开启了会话保持功能，那么有可能会造成后端服务器的访问并不是完全相同的。如果出现了访问不均衡的情况，建议您暂时关闭会话保持功能，观察一下是否依然存在这种情况。

  当负载均衡服务分发请求不均匀时，可以参考以下方法检查处理：

  1. 统计一个时间段内，后端ECS实例的Web服务访问日志记录数据量。

2. 按照负载均衡的配置，对比多台ECS实例日志的数量是否有相差。（开启会话保持后，需要剥离相同IP的访问日志。如果负载均衡配置了权重，要根据权重比例计算日志中访问比例是否正常。）

· ECS进行热迁移时，可能导致SLB长连接断开。重新连接后即可恢复，请做好应用的重连工作。

默认服务器组

用来接收前端请求的ECS实例。如果监听没有设置虚拟服务器组或主备服务器组，默认将请求转发至默认服务器组中的ECS。

参见管理默认服务器组创建一个默认服务器组。

主备服务器组

一个主备服务器组只包括两台ECS实例，一台作为主服务器，一台作为备服务器。由于备服务器不会做健康检查，所以只要主服务器健康检查失败，系统会直接将流量切到备机。当主服务器健康检查成功恢复服务后，流量会自动切到主服务器。

参见管理主备服务器组创建一个主备服务器组。

说明:

只有TCP和UDP监听支持添加主备服务器组。

虚拟服务器组

当您需要将不同的请求转发到不同的后端服务器上时，或需要通过域名和URL进行请求转发时，可以选择使用虚拟服务器组。

参见管理虚拟服务器组创建一个虚拟服务器组。

4.2 管理默认服务器组

在使用负载均衡服务前，必须至少添加一台默认服务器接收负载均衡转发的客户端请求。

添加默认服务器

在向默认服务器组中添加ECS实例前，确保：

· 您已创建负载均衡实例。

· 您已创建了ECS实例并部署了相关应用，用来接收转发的请求。

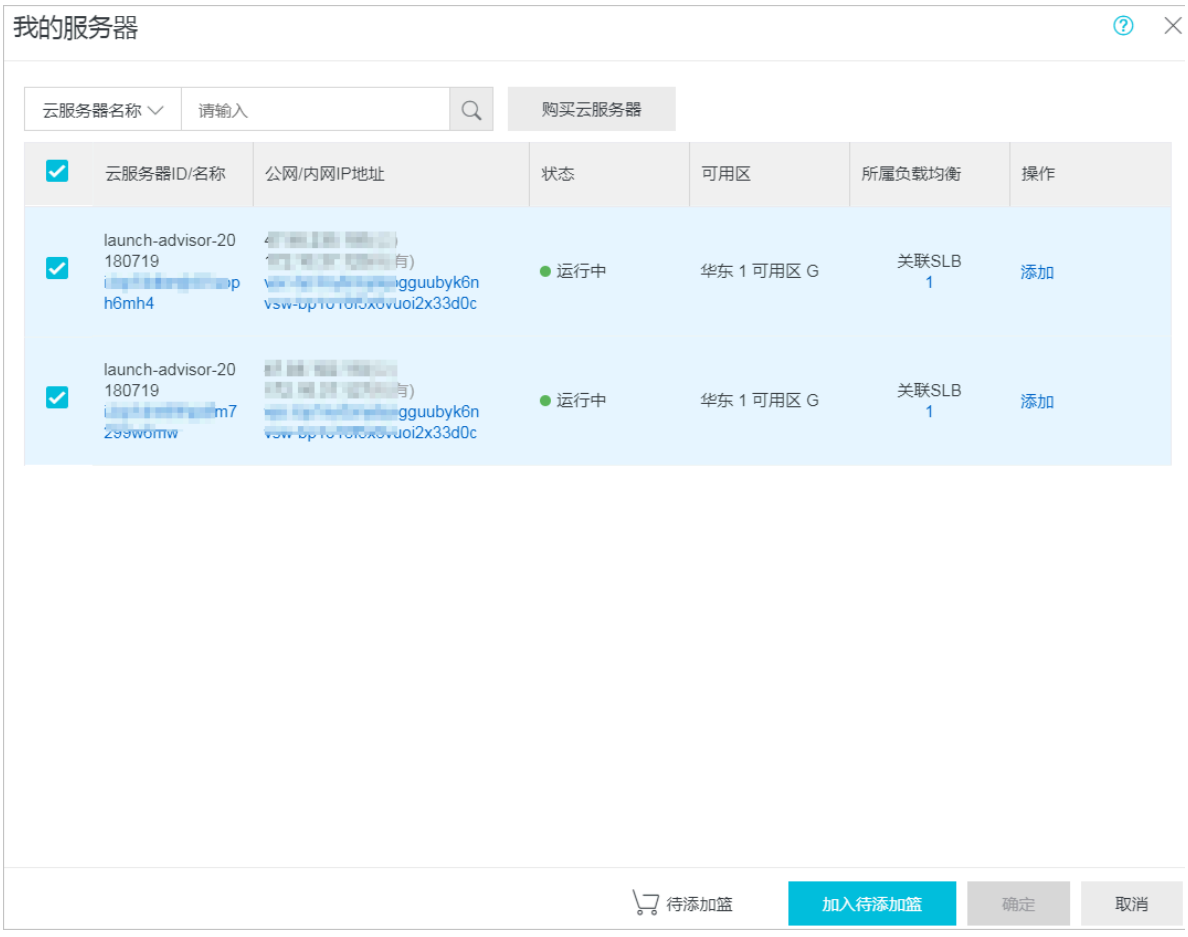
完成以下操作添加ECS实例：

1. 登录负载均衡管理控制台。

2. 在实例管理页面，选择目标实例的所属地域。

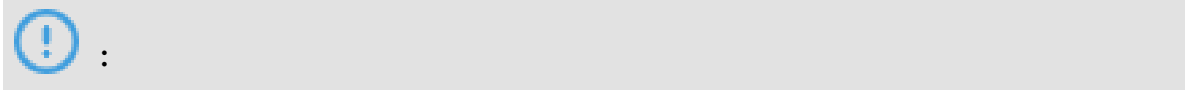
3. 单击目标实例的ID。
4. 单击默认服务器组页签。
5. 单击添加。

6. 在我的服务器页面，单击目标ECS实例对应的添加，或者勾选多个目标ECS实例，然后单击页面下方的加入待添加篮。



7. 单击确定。
8. 在待添加服务器对话框，指定添加的ECS实例的后端服务权重，然后单击确定。

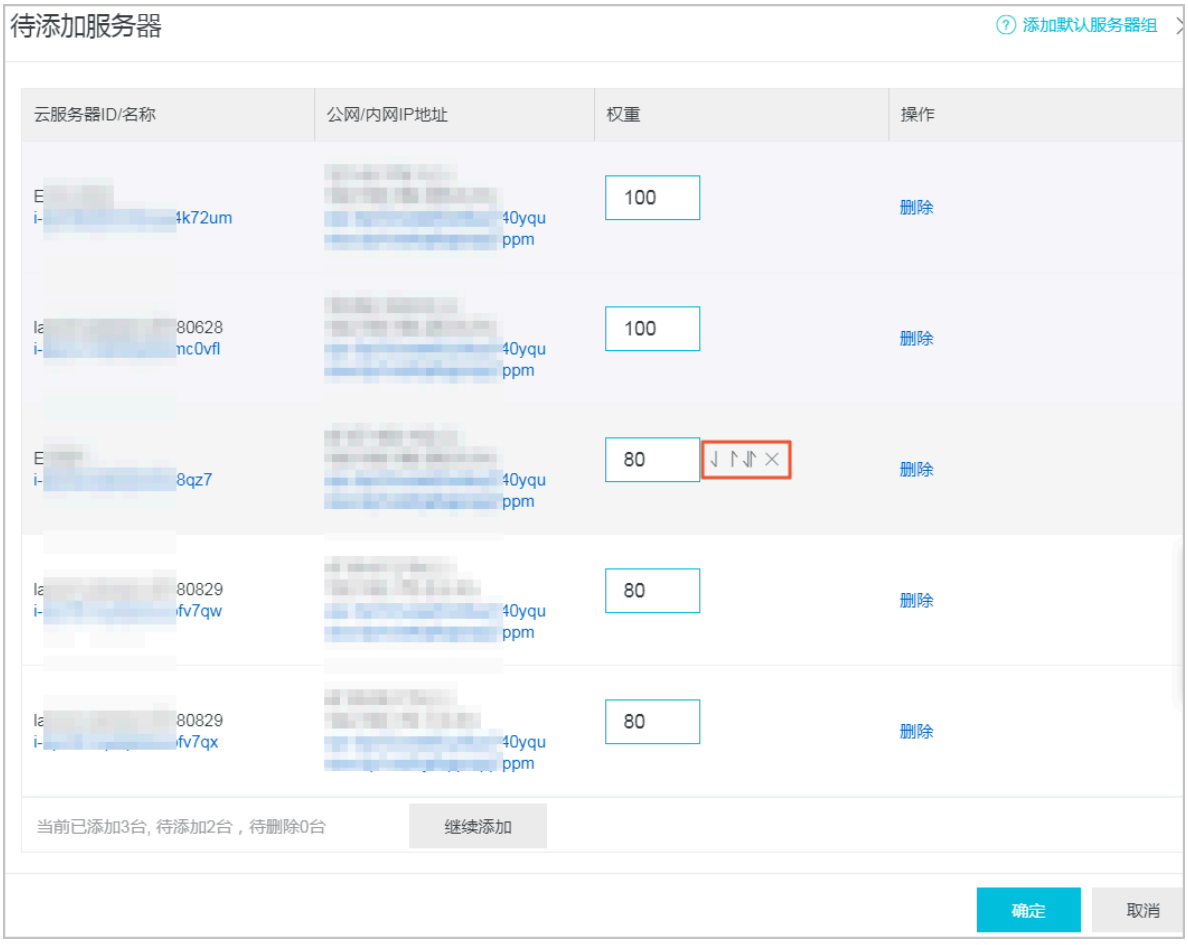
   权重：权重越高的ECS实例将被分配到更多的访问请求。


：

权重设置为0，该服务器不会再接受新请求。

支持批量服务器的权重。

- **单击  ：向下复制，如果修改当前服务器的权重，该服务器以下所有服务器的权重同步改变。**
- **单击  ：向上复制，如果修改当前服务器的权重，该服务器以上所有服务器的权重同步改变。**
- **单击  ：全部复制，如果修改当前服务器的权重，该默认服务器组中所有服务器的权重同步改变。**
- **单击  ：全部清除，如果清除当前服务器的权重，该默认服务器组中所有服务器的权重同步清除。**



9. **单击确定。**

编辑后端服务器的权重

完成以下操作，修改后端服务器的权重：

1. 登录负载均衡管理控制台。
2. 在实例管理页面，选择目标实例的所属地域。
3. 单击目标实例的ID。
4. 单击默认服务器组页签。
5. 将鼠标移至目标后端服务器的权重区域，然后单击出现的铅笔图标。

6. 修改权重，然后单击确定。

   权重越高的ECS实例将被分配到更多的访问请求。

   ：

   权重设置为0，该服务器不会再接受新请求。

移除后端服务器

完成以下操作，移除后端服务器：

1. 登录负载均衡管理控制台。
2. 在实例管理页面，选择目标实例的所属地域。
3. 单击目标实例的ID。
4. 单击默认服务器组页签。
5. 单击操作列的移除，移除后端服务器。

4.3 管理虚拟服务器组

虚拟服务器组 （VServer group）是一组 ECS 实例。将虚拟服务器组和一个监听关联后，监听只会将流量转发给关联的虚拟服务器组的后端服务器，不会再将流量转发给其他后端服务器。

如果您同时为一个七层监听添加了默认后端服务器、虚拟服务器组和转发规则，请求转发的顺序如下：

- 判断请求其是否能够匹配上某条转发规则，如果匹配，则将流量转发到该规则的虚拟服务器组。
- 若不匹配并且在该监听上设置了虚拟服务器组，那么将流量转发到监听关联的虚拟服务器组。

- 若您没有在该监听上设置虚拟服务器组，即将流量转发给默认服务器组中的ECS实例。

创建虚拟服务器组

在创建虚拟服务器组前，确保：

- 您已创建负载均衡实例。
- 您已创建了ECS实例并部署了相关应用，用来接收转发的请求。

在创建虚拟服务器组时，请注意：

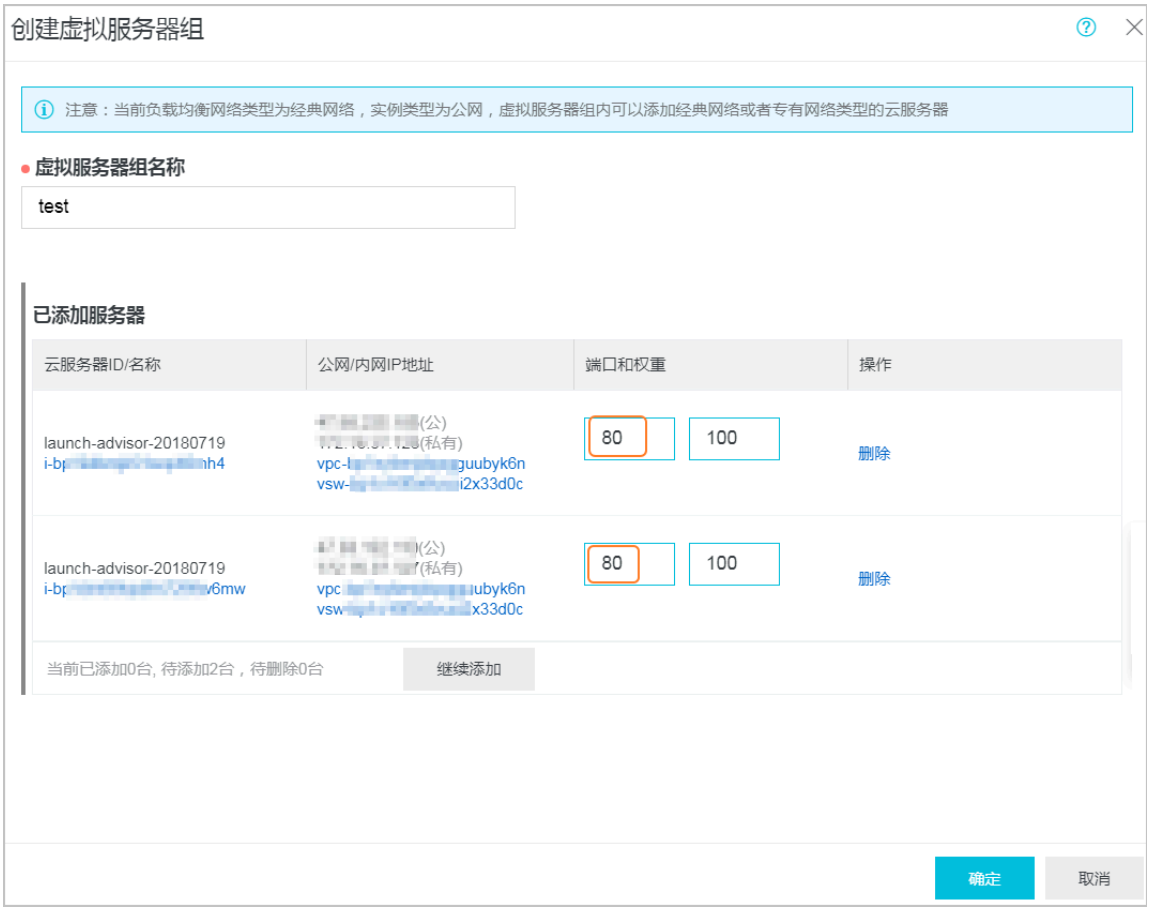
- 虚拟服务器组中添加的ECS实例的地域必须和负载均衡实例相同。
- 一个ECS实例可以属于多个虚拟服务器组。
- 一个虚拟服务器组可绑定在一个实例的多个监听上。
- 虚拟服务器组由ECS实例和应用端口组成。

完成以下操作添加ECS实例：

1. 登录负载均衡管理控制台。
2. 在实例管理页面，选择目标实例的所属地域。
3. 单击目标实例的ID。
4. 单击虚拟服务器组页签。
5. 在 虚拟服务器组页面，单击 创建虚拟服务器组。
6. 在 创建虚拟服务器组 页面，完成如下操作：
   a. 在 虚拟服务器组名称 文本框中，输入虚拟服务器组名称。
   b. 单击添加，在我的服务器列表选择要添加的服务器。
   c. 单击加入待添加篮，然后单击确定。
   d. 在已添加服务器页签下，输入每个ECS实例的端口和权重，单击 确定。
      - 端口：ECS实例开放用来接收请求的后端端口。

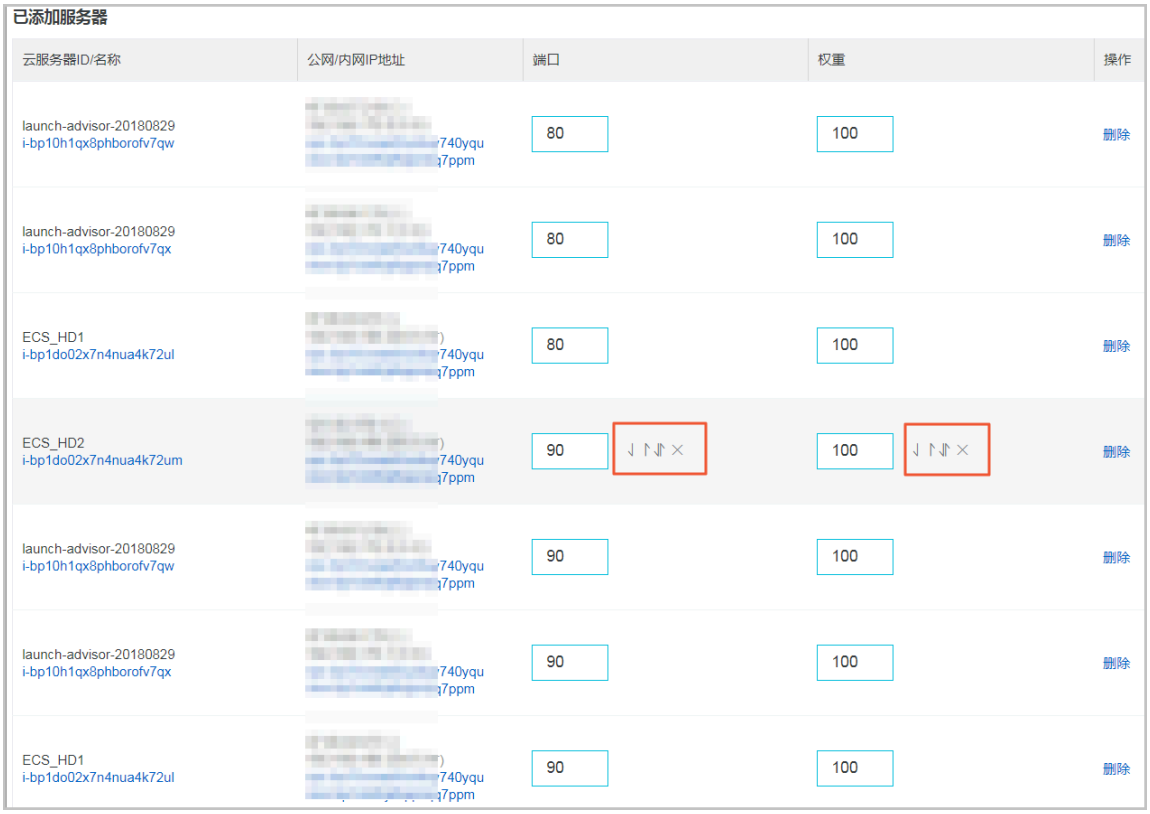
        在同一个负载均衡实例内，后端端口可重复。
      - 权重：权重越高的ECS实例将被分配到更多的访问请求。

        ：
        权重设置为0，该服务器不会再接受新请求。



支持批量修改已添加服务器的端口号和权重。

- 单击  ：向下复制，如果修改当前服务器的端口号或权重，该服务器以下所有服务器的端口号或权重同步改变。
- 单击  ：向上复制，如果修改当前服务器的端口号或权重，该服务器以上所有服务器的端口号或权重同步改变。
- 单击  ：全部复制，如果修改当前服务器的端口号或权重，该虚拟服务器组中所有服务器的端口号或权重同步改变。
- 单击  ：全部清除，如果清除当前服务器的端口号或权重，该虚拟服务器组中所有服务器的端口号或权重同步清除。



编辑虚拟服务器组

完成以下操作，修改虚拟服务器组中的ECS实例配置：

1. 登录负载均衡管理控制台。
2. 在实例管理页面，选择目标实例的所属地域。
3. 单击目标实例的ID。
4. 单击虚拟服务器组页签。
5. 单击目标虚拟服务器组对应的编辑选项。

6. 修改ECS实例的端口和权重，或单击删除将ECS实例从虚拟服务器组中移除，然后单击确定。

删除虚拟服务器组

完成以下操作，删除虚拟服务器组：

1. 登录负载均衡管理控制台。
2. 在实例管理页面，选择目标实例的所属地域。
3. 单击目标实例的ID。
4. 单击虚拟服务器组页签。
5. 单击目标虚拟服务器组对应的删除选项。

6. 在弹出的对话框中，单击确定。

4.4 管理主备服务器组

当您有传统的主备需求时，即后端服务器中有一台主机和一台备机。当主机工作正常时，流量将直接转发至主机；当主机宕机时，流量将切换至备机。此时，使用主备服务器组可避免服务中断。

一个主备服务器组只包括两台ECS实例，一台作为主服务器，一台作为备服务器。由于备服务器不会做健康检查，所以只要主服务器健康检查失败，系统会直接将流量切到备机。当主服务器健康检查成功恢复服务后，流量会自动切到主服务器。

：
主备服务器组只支持四层监听（TCP和UDP协议）。

创建主备服务器组

在创建主备服务器组前，确保：

- 您已创建负载均衡实例。
- 您已创建了ECS实例并部署了相关应用，用来接收转发的请求。

完成以下操作添加ECS实例：

1. 登录负载均衡管理控制台。
2. 在实例管理页面，选择目标实例的所属地域。
3. 单击目标实例的ID。
4. 单击主备服务器组页签。

5. 在 主备服务器组页面，单击 创建主备服务器组。
6. 在 创建主备服务器组 页面，完成如下操作：
   a. 在 主备服务器组名称 文本框中，输入主备服务器组名称。
   b. 单击添加，在我的服务器列表选择要添加的服务器。

      主备服务器组只能添加两台ECS实例。
   c. 单击加入待添加篮，然后单击确定。
   d. 在已添加服务器页签下，完成以下配置，然后单击 确定。
      - 端口：ECS实例开放用来接收请求的后端端口。

        在同一个负载均衡实例内，后端端口可重复。
      - 主机：选择将一台服务器作为主服务器。

删除主备服务器组

完成以下操作，删除主备服务器组：

1. 登录负载均衡管理控制台。
2. 在实例管理页面，选择目标实例的所属地域。
3. 单击目标实例的ID。

4. 单击主备服务器组页签。
5. 单击目标主备服务器组对应的删除选项。

6. 在弹出的对话框中，单击确定。

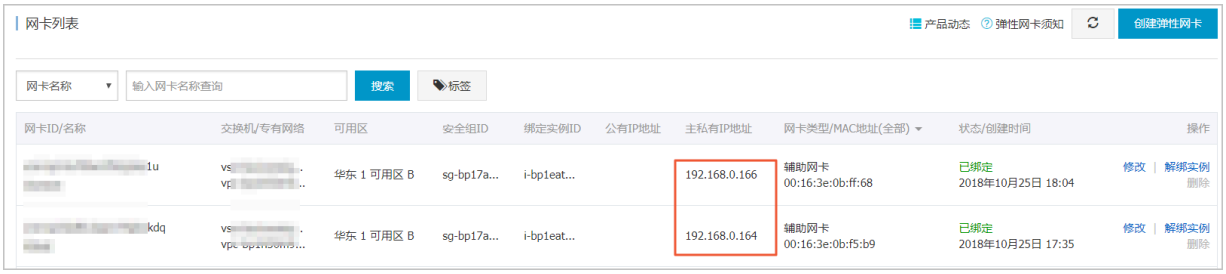
4.5 后端服务器支持添加ECS弹性网卡ENI

弹性网卡（ENI）是一种可以附加到专有网络VPC类型ECS实例上的虚拟网卡，通过弹性网卡，您可以实现高可用集群搭建、低成本故障转移和精细化的网络管理。性能保障型实例负载均衡实例后端服务器支持挂载ECS弹性网卡ENI。

前提条件

负载均衡实例添加后端服务器组时，如果ECS实例绑定多个弹性网卡，支持挂载弹性网卡ENI。

将弹性网卡绑定到ECS实例的方法请参见将弹性网卡附加到实例。

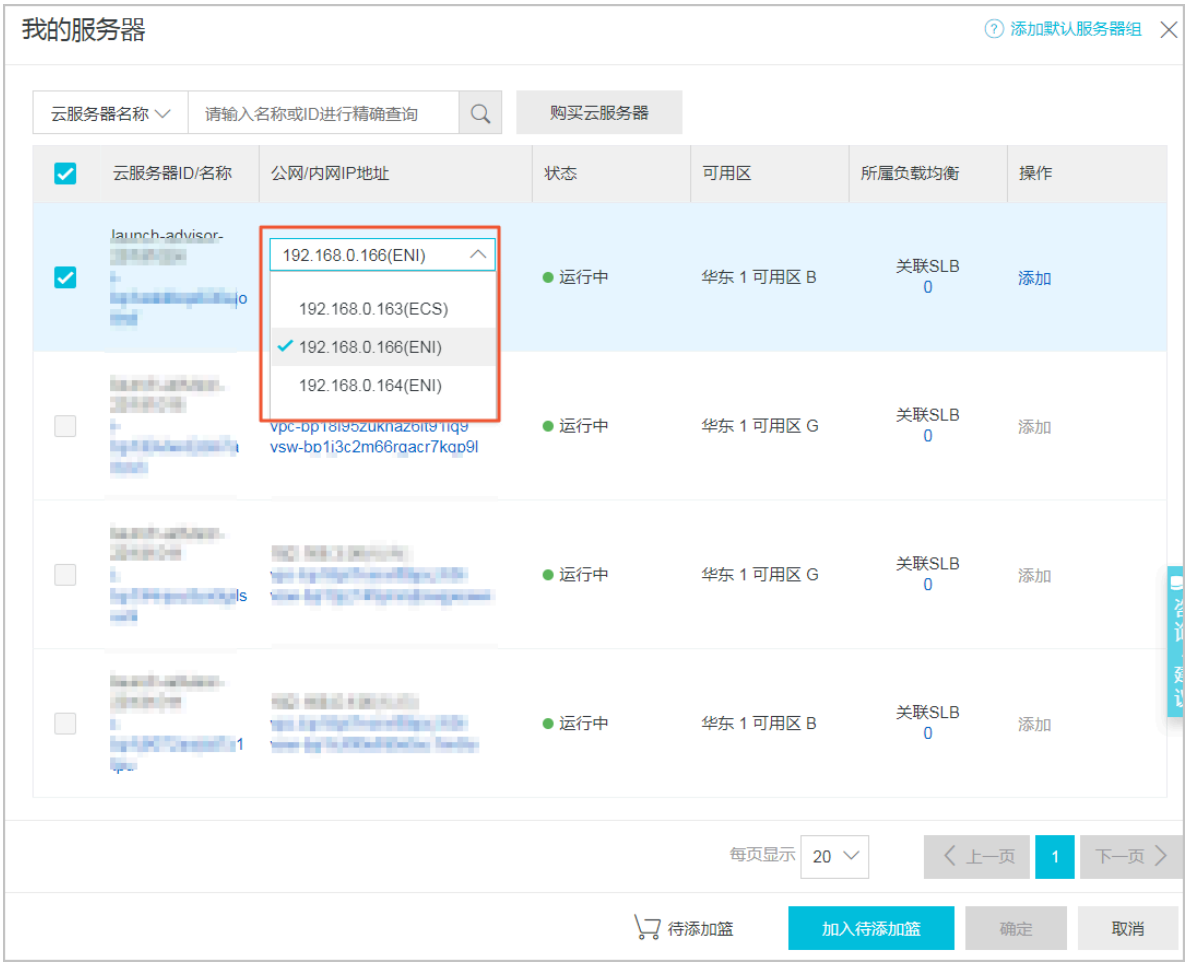


说明:

仅性能保障型实例后端服务器支持添加弹性网卡ENI。

操作步骤

1. 登录负载均衡管理控制台。
2. 在左侧导航栏，单击实例管理，在实例管理页面，单击需要添加后端服务器组的实例ID。
3. 选择后端服务器组类型，默认服务器组、虚拟服务器组和主备服务器组均支持挂载弹性网卡ENI，单击添加。
4. 在我的服务器页面，选择后端服务器，可以选择弹性网卡ENI。



5. 单击加入待添加篮。
6. 单击确定。

返回实例管理页面，可以看到挂载了弹性网卡的后端服务器组如下：

其中，

-  ：表示ECS实例。
-  ：表示弹性网卡ENI。

5 证书管理

5.1 证书要求

负载均衡只支持PEM格式的证书。在上传证书前，确保您的证书、证书链和私钥符合格式要求。

Root CA机构颁发的证书

如果是通过Root CA机构颁发的证书，您拿到的证书是唯一的一份，不需要额外的证书，配置的站点即可被浏览器等访问设备认为可信。

证书格式必须符合如下要求：

- 以`-----BEGIN CERTIFICATE-----`，`-----END CERTIFICATE-----`开头和结尾；请将这些内容一并上传。
- 每行64个字符，最后一行长度可以不足64个字符。
- 证书内容不能包含空格。

下图为PEM格式的证书示例。

中级机构颁发的证书

如果是通过中级CA机构颁发的证书，您拿到的证书文件包含多份证书，需要将服务器证书与中级证书合并在一起上传。

证书链格式必须符合如下要求：

- 服务器证书放第一位，中级证书放第二位，中间不能有空行。
- 证书内容不能包含空格。
- 证书之间不能有空行，并且每行64字节。详情参见*RFC1421*。
- 符合证书的格式要求。一般情况下，中级机构在颁发证书时会有对应说明，证书要符合证书机构的格式要求。

中级机构颁发的证书链示例。

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

RSA私钥格式要求

在上传服务器证书时，您也需要上传证书的私钥。

RSA私钥格式必须符合如下要求：

- 以`-----BEGIN RSA PRIVATE KEY-----`，`-----END RSA PRIVATE KEY-----`开头和结尾，请将这些内容一并上传。
- 字串之间不能有空行，每行64字符，最后一行长度可以不足64字符。详情参见*RFC1421*。

如果您的私钥是加密的，比如私钥的开头和结尾是`-----BEGIN PRIVATE KEY-----`，`-----END PRIVATE KEY-----`或`-----BEGIN ENCRYPTED PRIVATE KEY-----`，`-----END ENCRYPTED PRIVATE KEY-----`，或者私钥中包含`Proc-Type: 4,ENCRYPTED`，需要先运行以下命令进行转换：

```
openssl rsa -in old_server_key.pem -out new_server_key.pem
```

下图为RSA私钥示例。

5.2 创建证书

配置HTTPS监听，您可以直接使用SSL证书服务中的证书或者将所需的第三方签发的服务器证书和CA证书上传到负载均衡。上传后，无需在后端服务器再配置证书。

负载均衡支持两种来源的证书：

- 在阿里云SSL证书服务中签发或托管的证书：从阿里云SSL证书服务选择，可实现证书到期提醒和一键续期。

  暂未支持客户端CA证书。
- 第三方签发的证书：上传第三方签发证书，您需要持有证书的公钥/私钥文件。

  支持HTTPS服务器证书及客户端CA证书。

在创建证书前，注意：

- 如果一个证书要在多个地域使用，那么创建证书时就需要选择多个地域。
- 每个账号最多可以创建100个证书。

从SSL证书服务选择

阿里云提供的证书签发服务是指在云上签发各品牌数字证书，实现网站HTTPS化，使网站具备可信、防劫持、防篡改和防监听等特点，并对证书进行统一生命周期管理，简化证书部署，详情参见SSL证书服务详情。

如果您需要使用SSL证书服务中的证书，您需要登录SSL证书控制台，购买证书或者上传第三方证书到SSL证书服务。

完成以下操作，您可以从SSL证书服务中选取证书。

1. 登录负载均衡管理控制台。
2. 在左侧导航栏，单击证书管理。
3. 单击创建证书，在创建证书页面，选择从SSL证书服务选择。

4. 单击下一步，在从SSL证书服务选择页面，设置证书部署地域并从证书列表中选择使用的SSL证书。

   证书不支持跨地域使用，如果该证书需要在多个地域使用，选择所有需要的地域。
5. 单击确定。

上传第三方签发证书

上传第三方签发证书前，您必须：

- 已经购买了服务器证书。
- 已经生成了CA证书和客户端证书。详情参见生成证书。

完成以下操作，您可以将第三方签发证书上传到负载均衡。

1. 登录负载均衡管理控制台。

2. 在左侧导航栏，单击证书管理。
3. 单击创建证书。
4. 在创建证书页面，选择上传第三方签发证书。

5. 单击下一步，在上传第三方签发证书页面，上传证书内容。

配置	说明
证书名称	输入证书名称。 名称在1-80个字符之间，只能包含字母、数字和以下特殊符号： _/.-
证书部署地域	选择证书的地域。 证书不支持跨地域使用，如果该证书需要在多个地域使用，选择所有需要的地域。
证书类型	选择要上传的证书类型： · 服务器证书：配置HTTPS单向认证，只需要上传服务器证书和私钥。 · CA证书：配置HTTPS双向认证，除了上传服务器证书外，还需要上传CA证书。
证书内容	复制服务器或者CA证书内容。 单击导入样式查看正确的证书样式。详情参见证书要求。
私钥	复制服务器证书的私钥内容。 单击导入样式查看正确的证书样式。详情参见证书要求。 ： 只有上传服务器证书时，才需要上传私钥。

6. 单击确定。

5.3 生成CA证书

在配置HTTPS监听时，您可以使用自签名的CA证书，并且使用该CA证书为客户端证书签名。

使用Open SSL生成CA证书

1. 执行如下命令，在*/root*目录下新建一个*ca*文件夹，并在*ca*文件夹下创建四个子文件夹。

```
$ sudo mkdir ca
$ cd ca
$ sudo mkdir newcerts private conf server
```

   - *newcerts*目录将用于存放CA签署过的数字证书。
   - *private*目录用于存放CA的私钥。
   - *conf*目录用于存放一些简化参数用的配置文件。
   - *server*目录存放服务器证书文件。

2. 在*conf*目录下新建一个包含如下信息的*openssl.conf*文件。

```
[ ca ]
default_ca = foo
[ foo ]
dir = /root/ca
database = /root/ca/index.txt
new_certs_dir = /root/ca/newcerts
certificate = /root/ca/private/ca.crt
serial = /root/ca/serial
private_key = /root/ca/private/ca.key
RANDFILE = /root/ca/private/.rand
default_days = 365
default_crl_days= 30
default_md = md5
unique_subject = no
policy = policy_any
[ policy_any ]
countryName = match
stateOrProvinceName = match
organizationName = match
organizationalUnitName = match
localityName = optional
commonName      = supplied
emailAddress    = optional
```

3. 执行如下命令，生成私钥key文件。

```
$ cd /root/ca
 $ sudo openssl genrsa -out private/ca.key
```

   运行结果如下图所示。

```
root@iZbp1hfvivcqx1jbwap31iZ:~/ca/conf# cd /root/ca
root@iZbp1hfvivcqx1jbwap31iZ:~/ca# sudo openssl genrsa -out private/ca.key
Generating RSA private key, 2048 bit long modulus
.....................................................................
.....+++
..+++
e is 65537 (0x10001)
```

4. 运执行如下命令，按照提示输入所需信息，然后按下回车键生成证书请求*csr*文件。

```
$ sudo openssl req -new -key private/ca.key -out private/ca.csr
```

说明:

Common Name需要输入负载均衡的域名。

```
root@iZbp1hfvivcqx1jbwap31iZ:~/ca# sudo openssl req -new -key private/ca.key -ou
t private/ca.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:ZheJiang
Locality Name (eg, city) []:HangZhou
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Alibaba
Organizational Unit Name (eg, section) []:Test
Common Name (e.g. server FQDN or YOUR name) []:mydomain
Email Address []:a@alibaba.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@iZbp1hfvivcqx1jbwap31iZ:~/ca#
```

5. 运行以下命令生成凭证*crt*文件。

```
$ sudo openssl x509 -req -days 365 -in private/ca.csr -signkey
private/ca.key -out private/ca.crt
```

6. 运行以下命令为CA的key设置起始序列号，可以是任意四个字符。

```
$ sudo echo FACE > serial
```

7. 运行以下命令创建CA键库。

```
$ sudo touch index.txt
```

8. 运行以下命令为移除客户端证书创建一个证书撤销列表。

```
$ sudo openssl ca -gencrl -out /root/ca/private/ca.crl -crldays 7 -
config "/root/ca/conf/openssl.conf"
```

输出为：

```
Using configuration from /root/ca/conf/openssl.conf
```

为客户端证书签名

1. 运行以下命令在*ca*目录内创建一个存放客户端key的目录*users*。

```
$ sudo mkdir users
```

2. 运行以下命令为客户端创建一个key。

```
$ sudo openssl genrsa -des3 -out /root/ca/users/client.key 1024
```

说明：

创建key时要求输入pass phrase，这个是当前key的口令，以防止本密钥泄漏后被人盗用。两次输入同一个密码。

3. 运行以下命令为客户端key创建一个证书签名请求*csr*文件。

```
$ sudo openssl req -new -key /root/ca/users/client.key -out /root/ca
/users/client.csr
```

输入该命令后，根据提示输入上一步输入的pass phrase，然后根据提示输入对应的信息。

说明：

A challenge password是客户端证书口令。注意将它和client.key的口令进行区分。

4. 运行以下命令使用CA证书的key为客户端key签名。

```
$ sudo openssl ca -in /root/ca/users/client.csr -cert /root/ca/
private/ca.crt -keyfile /root/ca/private/ca.key -out /root/ca/users/
client.crt -config "/root/ca/conf/openssl.conf"
```

当出现确认是否签名的提示时，两次都输入y。

```
root@iZbp1hfvivcqx1jbwap31iZ:~/ca# sudo openssl ca -in /root/ca/users/client.csr
 -cert /root/ca/private/ca.crt -keyfile /root/ca/private/ca.key -out /root/ca/us
ers/client.crt -config "/root/ca/conf/openssl.conf"
Using configuration from /root/ca/conf/openssl.conf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :ASN.1 12:'ZheJiang'
localityName          :ASN.1 12:'HangZhou'
organizationName      :ASN.1 12:'Alibaba'
organizationalUnitName:ASN.1 12:'Test'
commonName            :ASN.1 12:'mydomain'
emailAddress          :IA5STRING:'a@alibaba.com'
Certificate is to be certified until Jun  4 15:28:55 2018 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
root@iZbp1hfvivcqx1jbwap31iZ:~/ca#
```

5. 运行以下命令将证书转换为*PKCS12*文件。

```
$ sudo openssl pkcs12 -export -clcerts -in /root/ca/users/client.crt
 -inkey /root/ca/users/client.key -out /root/ca/users/client.p12
```

按照提示输入客户端client.key的pass phrase。再输入用于导出证书的密码。这个是客户端证书的保护密码，在安装客户端证书时需要输入这个密码。

6. 运行以下命令查看生成的客户端证书。

```
cd users
ls
```

5.4 转换证书格式

负载均衡只支持PEM格式的证书，其它格式的证书需要转换成PEM格式后，才能上传到负载均衡。建议使用Open SSL进行转换。

DER转换为PEM

DER格式通常使用在Java平台中，证书文件后缀一般为*.der*、*.cer*或者*.crt*。

- 运行以下命令进行证书转化：

```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

-

- 运行以下命令进行私钥转化：

```
openssl rsa -inform DER -outform PEM -in privatekey.der -out
privatekey.pem
```

P7B转换为PEM

P7B格式通常使用在Windows Server和Tomcat中。

运行以下命令进行证书转化：

```
openssl pkcs7 -print_certs -in incertificate.p7b -out outcertificate.
cer
```

PFX转换为PEM

PFX格式通常使用在Windows Server中。

- 运行以下命令提取证书：

```
openssl pkcs12 -in certname.pfx -nokeys -out cert.pem
```

- 运行以下命令提取私钥：

```
openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes
```

5.5 替换证书

为避免证书过期对您的服务产生影响，请在证书过期前替换证书。

操作步骤

1. 新建并上传一个新的证书。

   详情参见生成*CA*证书和创建证书。

2. 在HTTPS监听中配置新的证书。

   详情参见添加*HTTPS*监听。

3. 打开证书管理页面，找到目标证书，然后单击删除。

4. 在弹出的对话框中，单击确认。

6 日志管理

6.1 查看操作日志

您可以查看负载均衡实例、HTTP监听和服务器证书资源一个月内的操作日志。

背景信息

负载均衡的操作日志需要在ActionTrail控制台查看。操作审计(ActionTrail)记录您的云账户资源操作，提供操作记录查询，并可以将记录文件保存到您指定的OSS存储空间。

操作步骤

1. 登录负载均衡控制台。
2. 在左侧导航栏，单击日志管理 > 操作日志。
3. 单击去查看操作日志。
4. 在历史事件查询页面，完成以下操作查看操作日志：
   a) 过滤器选择资源类型。
   b) 在资源列表中，选择您要查看的负载均衡资源。
   本操作选择负载均衡实例LoadBalancer。

   c) 选择一种事件类型。
   本操作选择所有类型。
   d) 选择查询时间。
   e) 单击搜索查看所选资源的操作日志。
   您可以展开每条记录，查看详细信息。

6.2 管理健康检查日志

您可以在日志管理页面，查看三天内的健康检查日志。如需要更久的健康检查日志，您需要将健康检查日志存储到OSS中，并可以下载完整的健康检查日志。

存储健康检查日志

您可以通过负载均衡提供的日志管理功能，查看负载均衡实例后端服务器（ECS实例）的健康检查日志。当前，负载均衡只存储三天内的健康检查日志信息，您可以通过开通OSS服务，将所有的健康检查日志存储到创建的bucket中。

您可以随时开启和关闭日志存储功能。开启日志存储后，负载均衡会在所选bucket中创建一个名称为*AliyunSLBHealthCheckLogs*的文件夹用来存储健康检查日志文件。负载均衡的健康检查日志每小时生成一次，系统会自动创建一个以日期为名称的子文件夹用来存储当天的健康检查日志文件，如*20170707*。

当天每小时生成的日志文件以生成的截止时间命名。比如在00:00-01:00生成的健康检查日志，日志文件名为*01.txt*；在01:00-02:00生成的健康检查日志，日志文件名为*02.txt*。

> **说明:**
> **只有检查到后端ECS出现异常时，才会生成健康检查日志。健康检查日志每小时生成一次，若该小时内后端ECS未检测到异常，则无健康检查日志。**

完成以下操作，存储健康检查日志：

1. **创建*Bucket***
2. **授权日志访问**

3. 设置日志存储

步骤一 创建Bucket

1. 打开对象存储OSS产品页面，单击立即开通。
2. 开通OSS服务后，登录OSS管理控制台。
3. 单击新建Bucket。

4. 在新建Bucket对话框，配置Bucket信息，单击确定。

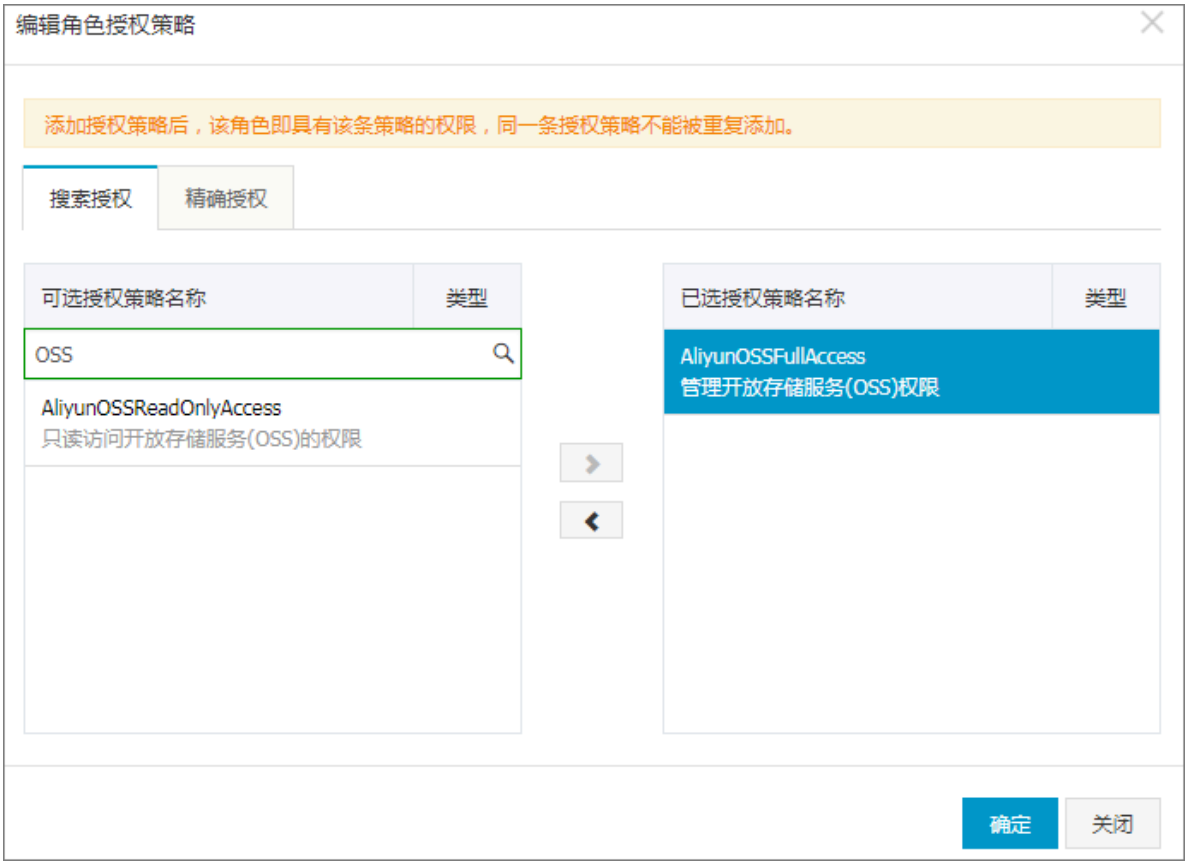
> 说明:
> 确保bucket的地域和负载均衡实例的地域相同。

步骤二 授权日志访问

创建好Bucket后，您还需要对负载均衡的日志角色（SLBLogDefaultRole）授权，允许该角色访问OSS的相关资源。

> :
> 只有首次配置时，才需要进行授权。

1. 在负载均衡管理控制台的左侧导航栏，单击日志管理 > 健康检查日志 。
2. 单击第一步：开通OSS。
3. 开通后，返回健康检查日志页面，然后单击第二步：RAM角色授权区域内的立即前往。
4. 阅读授权内容后，单击同意授权。
5. 登录访问控制管理控制台。
6. 在左侧导航栏，单击角色管理，找到名称为SLBLogDefaultRole的角色，然后单击授权。
7. 在编辑角色授权策略对话框，选择AliyunOSSFullAccess，然后单击确定完成授权。



授权完成后，单击SLBLogDefaultRole，然后单击角色授权策略，查看授权策略。

步骤三 设置日志存储

1. 登录负载均衡控制台。
2. 在左侧导航栏，选择日志管理 > 健康检查日志 。
3. 在健康检查日志页面，单击日志存储页签。
4. 单击目标地域的设置日志存储链接。

5. 在设置日志存储对话框，选择用来存储健康检查日志的Bucket，然后单击确定。
6. 拖动状态栏下的开关，开启日志存储。

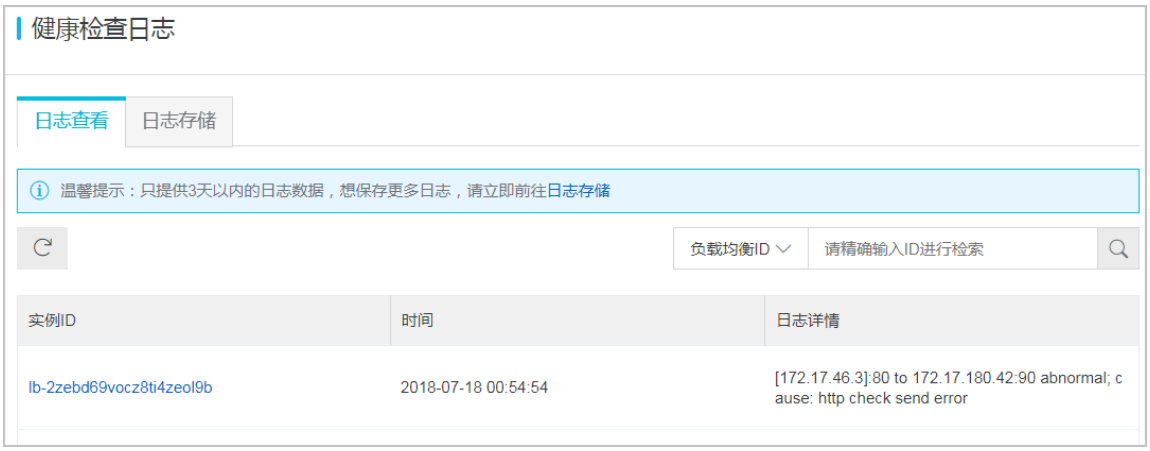
查看健康检查日志

您可以在负载均衡管理控制台，查看三天内的健康检查日志。

1. 登录负载均衡控制台。
2. 在左侧导航栏，选择日志管理 > 健康检查日志。
3. 在健康检查日志页面，单击日志查看页签。

> **说明:**
> 只有检查到后端ECS出现异常时，才会生成健康检查日志。健康检查日志每小时生成一次，若该小时内后端ECS未检测到异常，则无健康检查日志。

- 当健康检查日志的信息为`SLB_instance_IP:port to Added_ECS_instance_IP:port abnormal; cause:XXX`时，代表后端ECS实例健康检查异常，您可以根据提示的异常原因进行排查。
- 当健康检查日志的信息为`SLB_instance_IP:port to Added_ECS_instance_IP:port normal`时，代表后端ECS实例恢复正常。

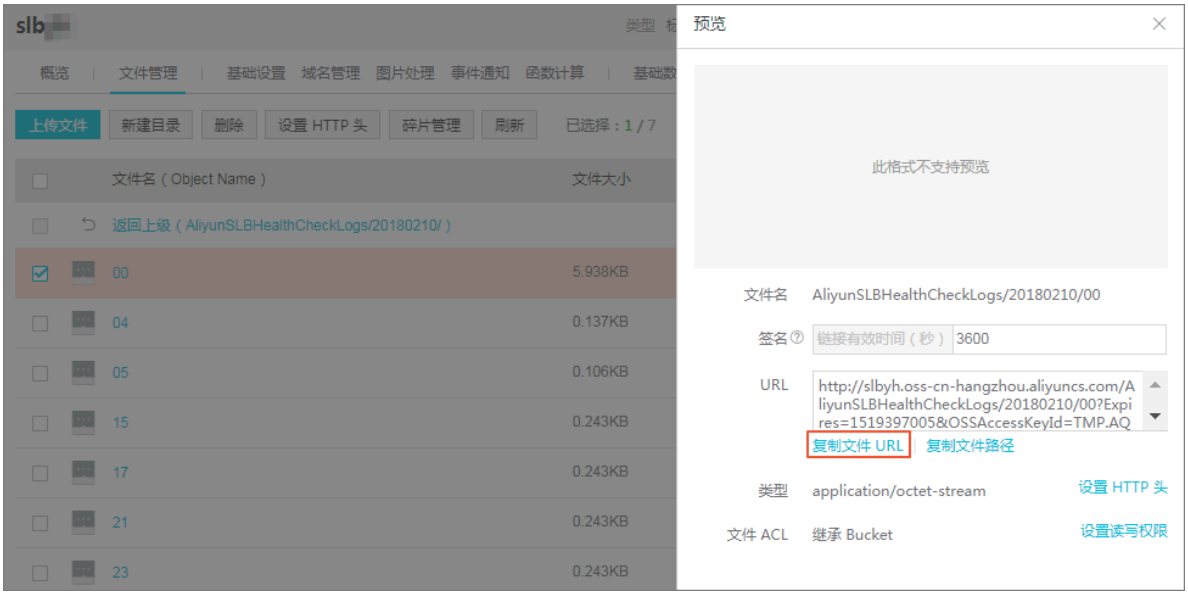


下载健康检查日志

您可以在OSS管理控制台中，下载存储的完整的健康检查日志。

1. 登录OSS管理控制台。
2. 在概览页面，单击目标Bucket，然后单击文件管理。
3. 在文件管理页面，单击健康检查日志文件夹*AliyunSLBHealthCheckLogs/*。

4. 单击您要下载的健康检查日志的文件夹。
5. 单击目标文件的管理，然后单击复制文件 URL。



6. 在浏览器中输入复制的URL，下载日志文件。

6.3 授权子账号使用访问日志

子账号使用负载均衡访问日志功能前，需要主账号对其进行授权。

前提条件

主账号已开通日志访问功能。

1. 以主账号登录RAM控制台。

2. 单击角色管理，查看主账号是否具有负载均衡日志访问角色AliyunLogArchiveRole。

   如果主账号没有该角色权限，请以主账号登录负载均衡控制台，选择日志管理 > 访问日志，单击立即授权，然后在弹出的对话框，单击同意授权，授权SLB访问日志服务。

   说明:
   该操作只有首次配置时需要。

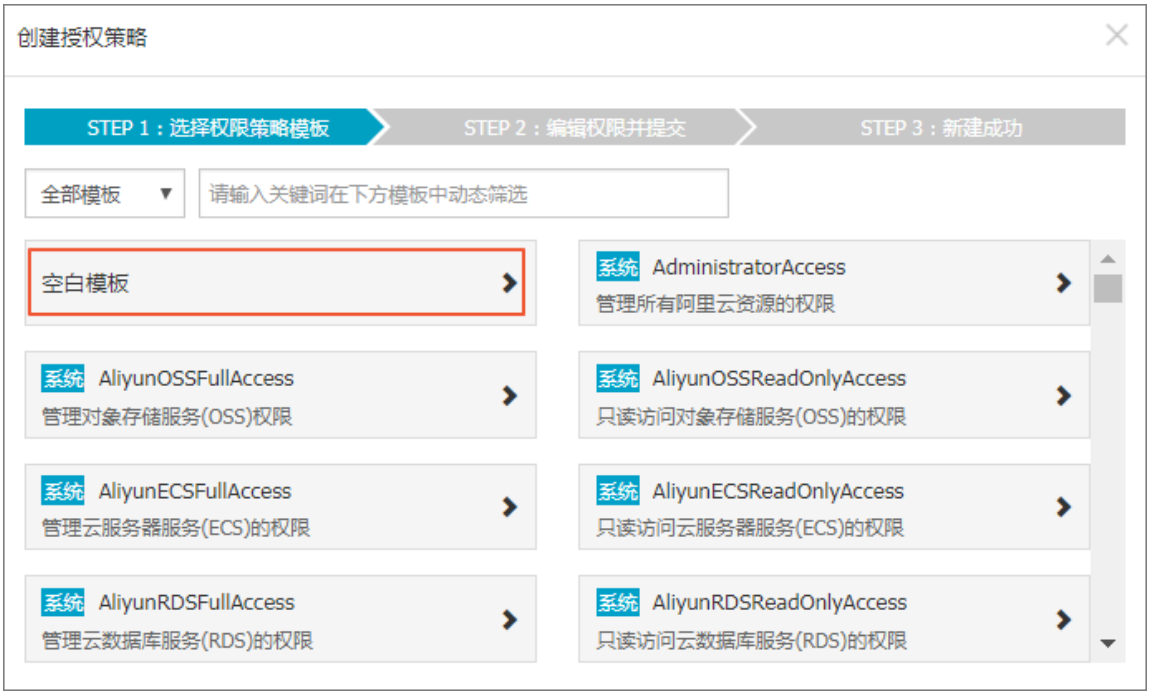
操作步骤

1. 创建授权策略：

   a) 使用主账号登录访问控制RAM控制台。

   b) 在左侧导航栏，单击策略管理，然后单击新建授权策略。

   c) 单击空白模板。



   d) 输入策略名称，如SlbAccessLogPolicySet，然后输入以下策略内容，单击新建授权策略。

```
{
"Statement": [
```

```
 {
   "Action": [
     "slb:Create*",
     "slb:List*"
   ],
   "Effect": "Allow",
   "Resource": "acs:log:*:*:project/*"
 },
 {
   "Action": [
     "log:Create*",
     "log:List*"
   ],
   "Effect": "Allow",
   "Resource": "acs:log:*:*:project/*"
 },
 {
   "Action": [
     "log:Create*",
     "log:List*",
     "log:Get*",
     "log:Update*"
   ],
   "Effect": "Allow",
   "Resource": "acs:log:*:*:project/*/logstore/*"
 },
 {
   "Action": [
     "log:Create*",
     "log:List*",
     "log:Get*",
     "log:Update*"
   ],
   "Effect": "Allow",
   "Resource": "acs:log:*:*:project/*/dashboard/*"
 },
 {
   "Action": "cms:QueryMetric*",
   "Resource": "*",
   "Effect": "Allow"
 },
 {
   "Action": [
     "slb:Describe*",
     "slb:DeleteAccessLogsDownloadAttribute",
     "slb:SetAccessLogsDownloadAttribute",
     "slb:DescribeAccessLogsDownloadAttribute"
   ],
   "Resource": "*",
   "Effect": "Allow"
 },
 {
   "Action": [
     "ram:Get*",
     "ram:ListRoles"
   ],
   "Effect": "Allow",
   "Resource": "*"
 }
],
"Version": "1"
```

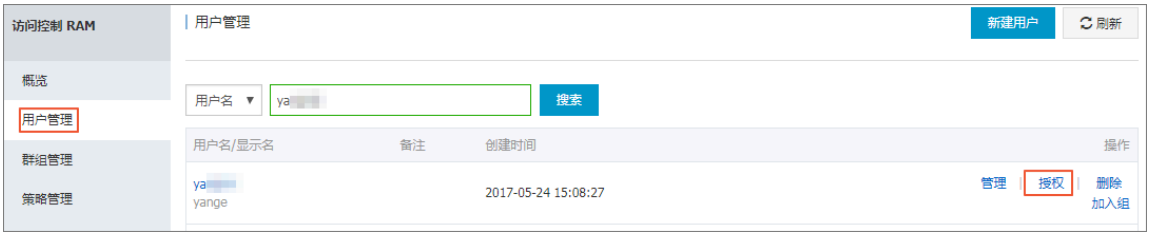
```
}
```

a) 单击关闭。

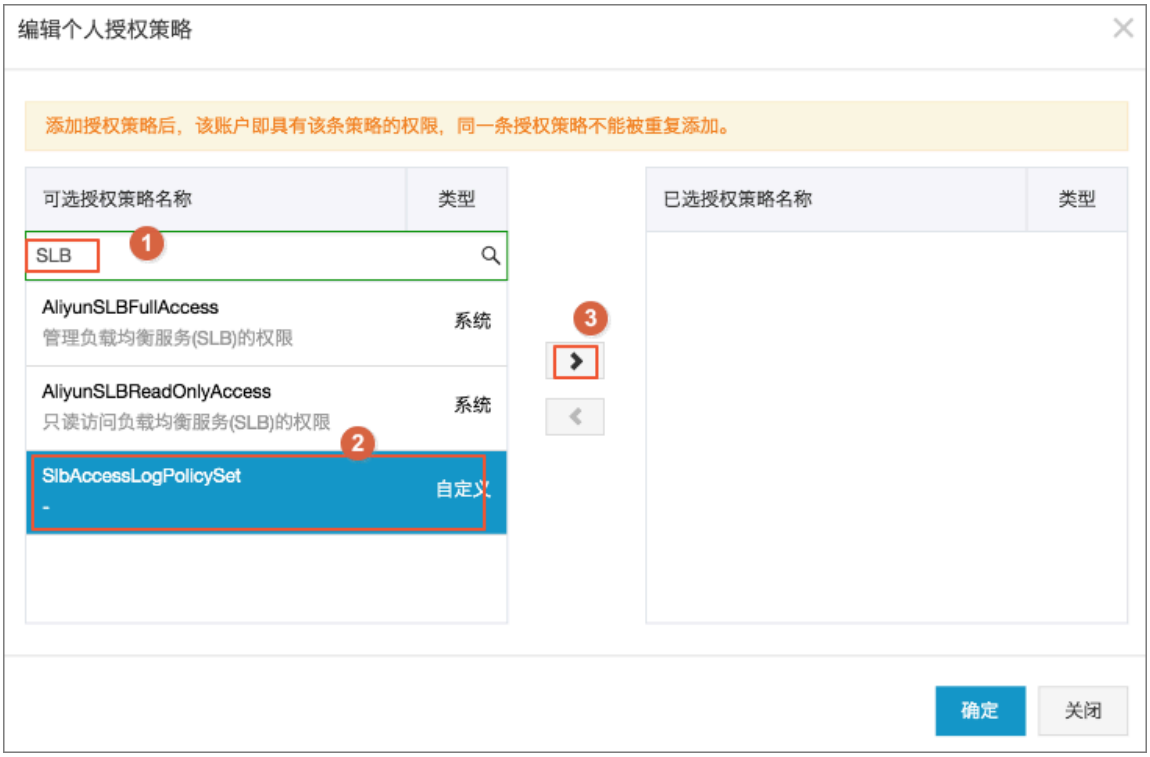
2. 给子账号授权：

a) 在访问控制RAM控制台的左侧导航栏，单击用户管理。

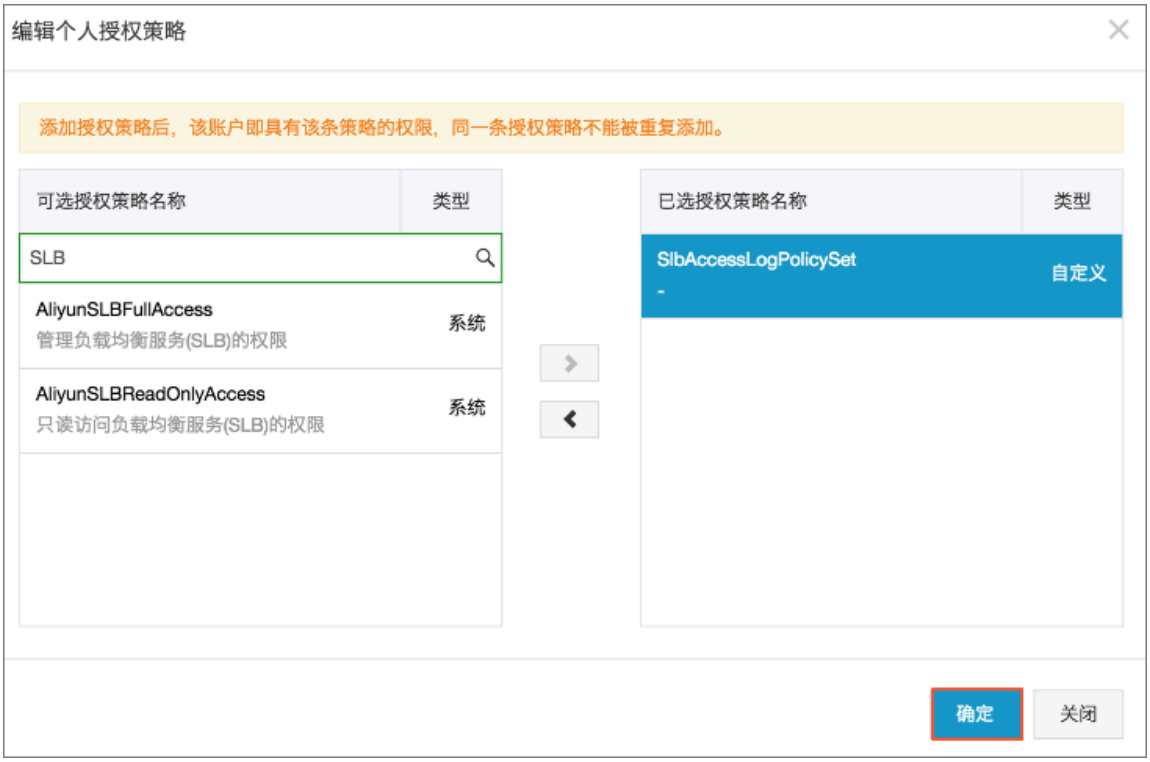
b) 找到目标用户（需要使用访问日志功能的子账号），然后单击授权。



c) 搜索已创建的策略，然后选择该策略授权给目标用户。



d) 单击确定。



e) 返回用户详情页面，查看用户已经拥有了新建的策略，可以使用负载均衡日志访问功能了。

6.4 配置访问日志

结合阿里云日志服务，您可以通过分析负载均衡的访问日志了解客户端用户行为、客户端用户的地域分布，排查问题等。

什么是负载均衡访问日志

负载均衡的访问日志功能收集了所有发送到负载均衡的请求的详细信息，包括请求时间、客户端IP地址、延迟、请求路径和服务器响应等。负载均衡作为公网访问入口，承载着海量的访问请求，您可以通过访问日志分析客户端用户行为、了解客户端用户的地域分布、进行问题排查等。

关于更多负载均衡访问日志的使用案例，访问云栖社区。

在开启负载均衡访问日志后，您可以将访问日志存储在日志服务（SLS）的日志库（Logstore）中，采集分析访问日志。您可以随时删除访问日志的配置。

负载均衡访问日志无需额外付费，您仅需要支付日志服务的费用。

：

- 只有七层负载均衡支持访问日志功能，全部地域都已经开放访问日志功能。
- 确保HTTP header的值不包含| |，否则有可能会造成导出的日志分割错位。

负载均衡访问日志优势

负载均衡访问日志有以下优势：

- 简单

  将开发、运维人员从日志处理的繁琐耗时中解放出来，将更多的精力集中到业务开发和技术探索上去。

- 海量

  负载均衡的访问日志数据规模通常很大，处理访问日志需要考虑性能和成本问题。日志服务可以一秒钟分析一亿条日志，相较于自建开源方案有明显成本优势和性能优势。

- 实时

  DevOps、监控、报警等场景要求日志数据的实时性。传统手段无法满足这一需求，例如将数据ETL到Hive等工具分析耗时很长，其中大量的工作花费在数据集成阶段。负载均衡访问日志结合阿里云日志服务强大的大数据计算能力，秒级分析处理实时产生的日志。

- 弹性

  可按负载均衡实例级别开通或关闭访问日志功能。可任意设置存储周期（1-365天），并且日志Logstore容量可以动态伸缩满足业务增长需求。

配置负载均衡访问日志

在配置访问日志前，确保：

1. 您已经创建了七层负载均衡。
2. 您已经开通了日志服务。

完成以下操作，配置访问日志：

1. 登录负载均衡管理控制台。
2. 在左侧导航栏，选择日志管理 > 访问日志 。
3. 选择实例的所属地域。
4. 单击立即授权，然后在弹出的对话框，单击同意授权授权SLB访问日志服务。

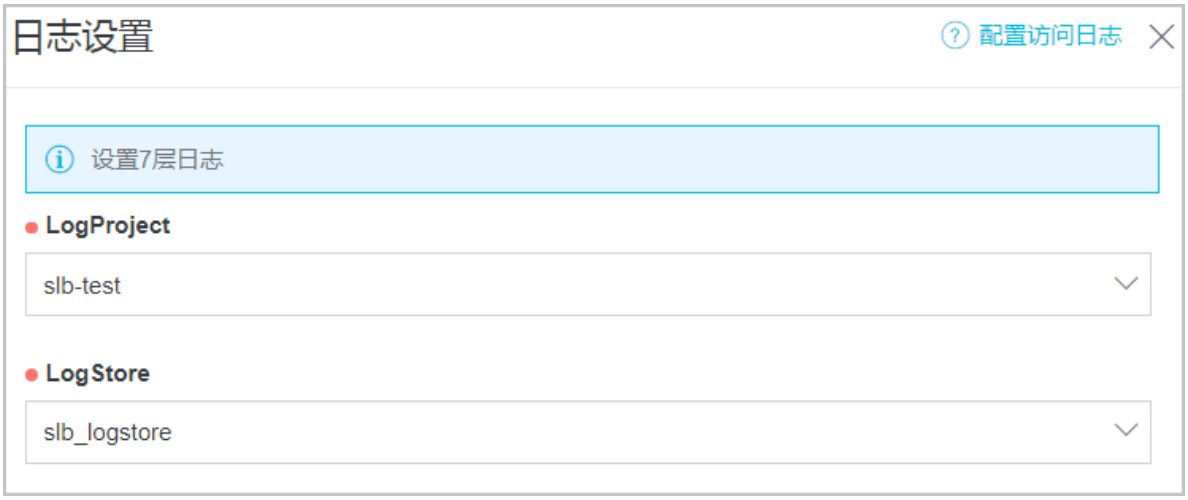
   如果您使用的是子账号，需要主账号进行授权。详情参见授权子账号使用访问日志。

> **说明:**
> 该操作只有首次配置时需要。

5. 在访问日志页面，找到目标SLB实例，然后单击设置。
6. 选择日志服务Project和日志库（LogStore），然后单击确认。

   如果没有可用的LogStore，单击前往SLS创建Store。

> **说明:**
> 确保Project的名称全局唯一，且Project的地域和负载均衡实例的地域相同。



查询、分析访问日志

配置负载均衡访问日志后，您可以在日志服务中查询、检索以下字段的日志信息。

字段	说明
body_bytes_sent	发送给客户端的HTTP Body的字节数
client_ip	请求客户端IP
host	请求报文中的Host header
http_user_agent	SLB收到的请求报文中http_user_agent header的内容
request_length	请求报文的长度，包括startline、HTTP头报文和HTTP body
request_method	请求报文的方法
request_time	SLB收到第一个请求报文的时间到SLB返回应答之间的间隔时间
request_uri	SLB收到的请求报文的URI
slbid	SLB实例ID
status	SLB应答报文的Status

字段	说明
upstream_addr	后端服务器的IP地址和端口
upstream_response_time	从SLB准备向后端发送请求到SLB向客户端发送完应答之间的时间
upstream_status	SLB收到的后端服务器的response status code

查询访问日志

完成以下操作，查询访问日志：

1. 进入日志查询页面。您可以通过负载均衡控制台和日志服务控制台进入日志查询页面。

   - 负载均衡控制台

     在访问日志页面，单击查看日志。

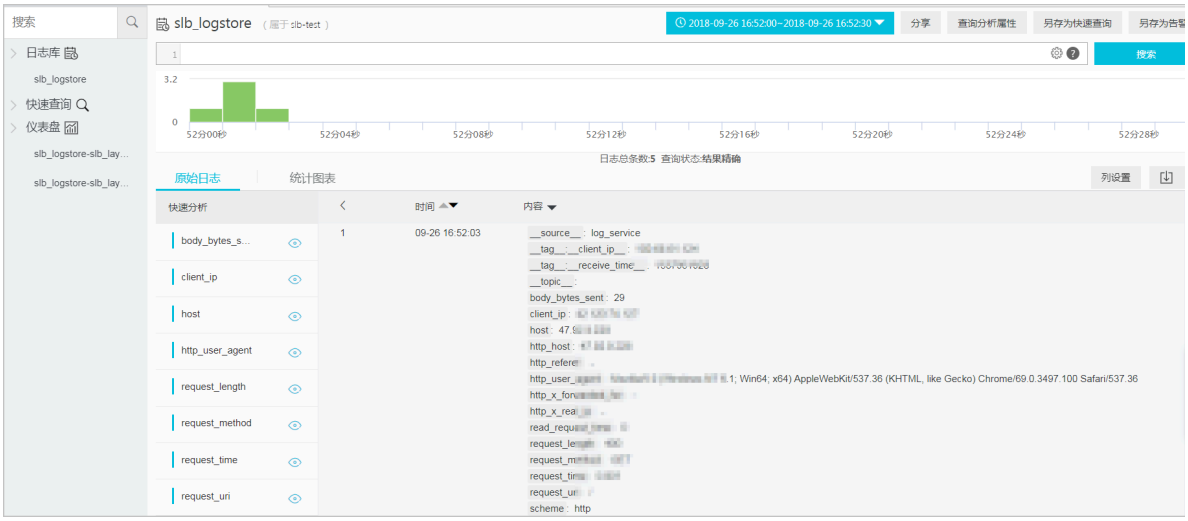
     

   - 日志服务控制台

     在日志库页面，单击SLB日志库的查询选项。

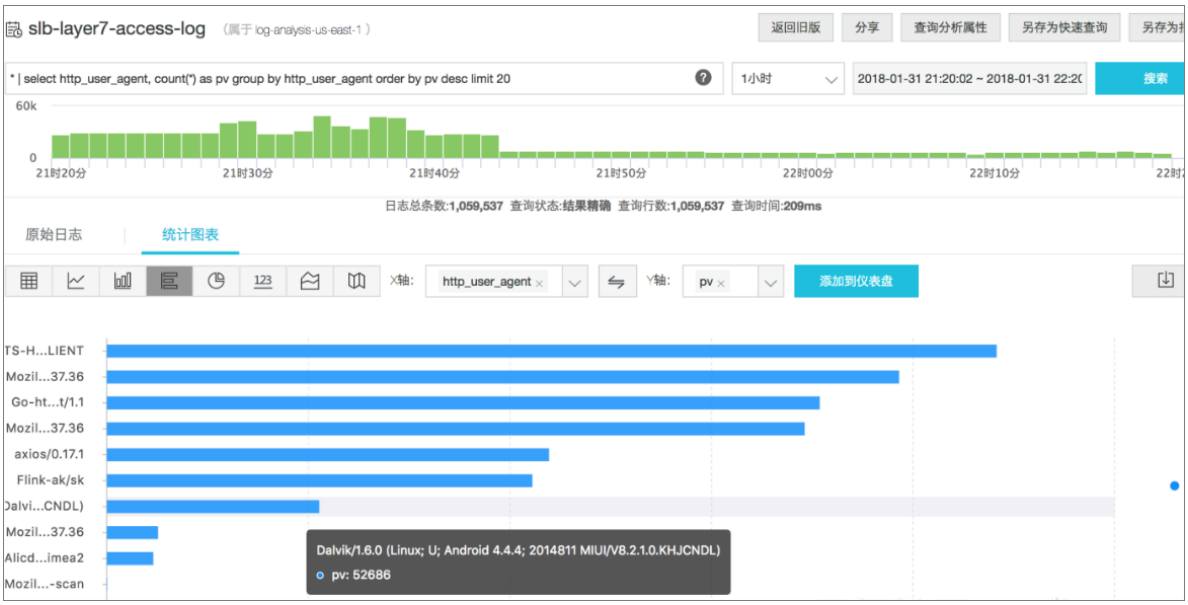
2. 单击目标日志字段，查看对应的日志信息。



3. 输入SQL语句查询特定的访问日志。

   比如输入如下SQL语句查询Top20的客户端，用于分析请求访问来源，辅助商业决策。

```
* | select ip_to_province(client_ip) as client_ip_province, count
(*) as pv group by
      client_ip_province order by pv desc limit 50
```



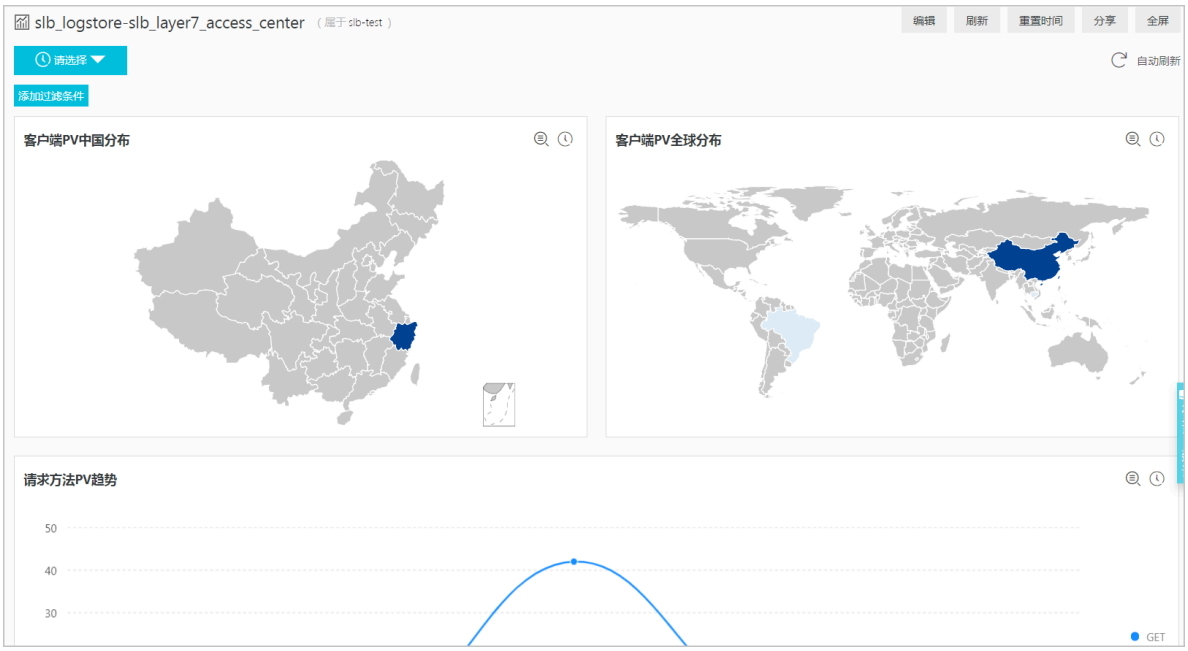
分析访问日志

您可以通过日志服务的仪表盘分析访问日志，仪表盘提供更丰富的数据信息。

完成以下操作，分析访问日志：

1. 在日志服务控制台，单击负载均衡的Project链接。
2. 在左侧导航栏，单击Search/Analytics - 查询分析 > 仪表盘，然后单击访问日志的名称。

您可以通过仪表盘查看TOP客户端、TOP Host、状态码PV等信息。



关闭访问日志

完成以下操作，关闭访问日志：

1. 登录负载均衡管理控制台。
2. 在左侧导航栏，单击日志管理 > 访问日志 。
3. 选择实例的所属地域。
4. 在访问日志页面，找到目标实例，然后单击删除关闭日志访问功能。

5. 在弹出的对话框中，单击确定。

7 访问控制

7.1 配置访问控制策略组

负载均衡提供监听级别的访问控制，您可以针对不同的监听配置不同的访问控制策略（白名单或黑名单）。在配置访问控制前，您需要先配置访问控制策略组。

您可以创建多个访问控制策略组，每个策略组可包含多个IP地址条目或IP地址段条目。访问控制策略组的限制如下：

资源	限制
每个地域单账号可创建的访问控制策略组个数	50
单账号每次可添加的IP地址条目个数	50
每个访问控制策略组可包含的条目个数	300
每个访问控制策略组可绑定监听的个数	50

创建访问控制策略组

完成以下操作，创建访问策略组：

1. 登录负载均衡管理控制台。
2. 选择地域。
3. 在左侧导航栏，选择访问控制页签。
4. 单击创建访问控制策略组，输入名称，然后单击确认。

添加IP条目

完成以下操作，添加IP条目：

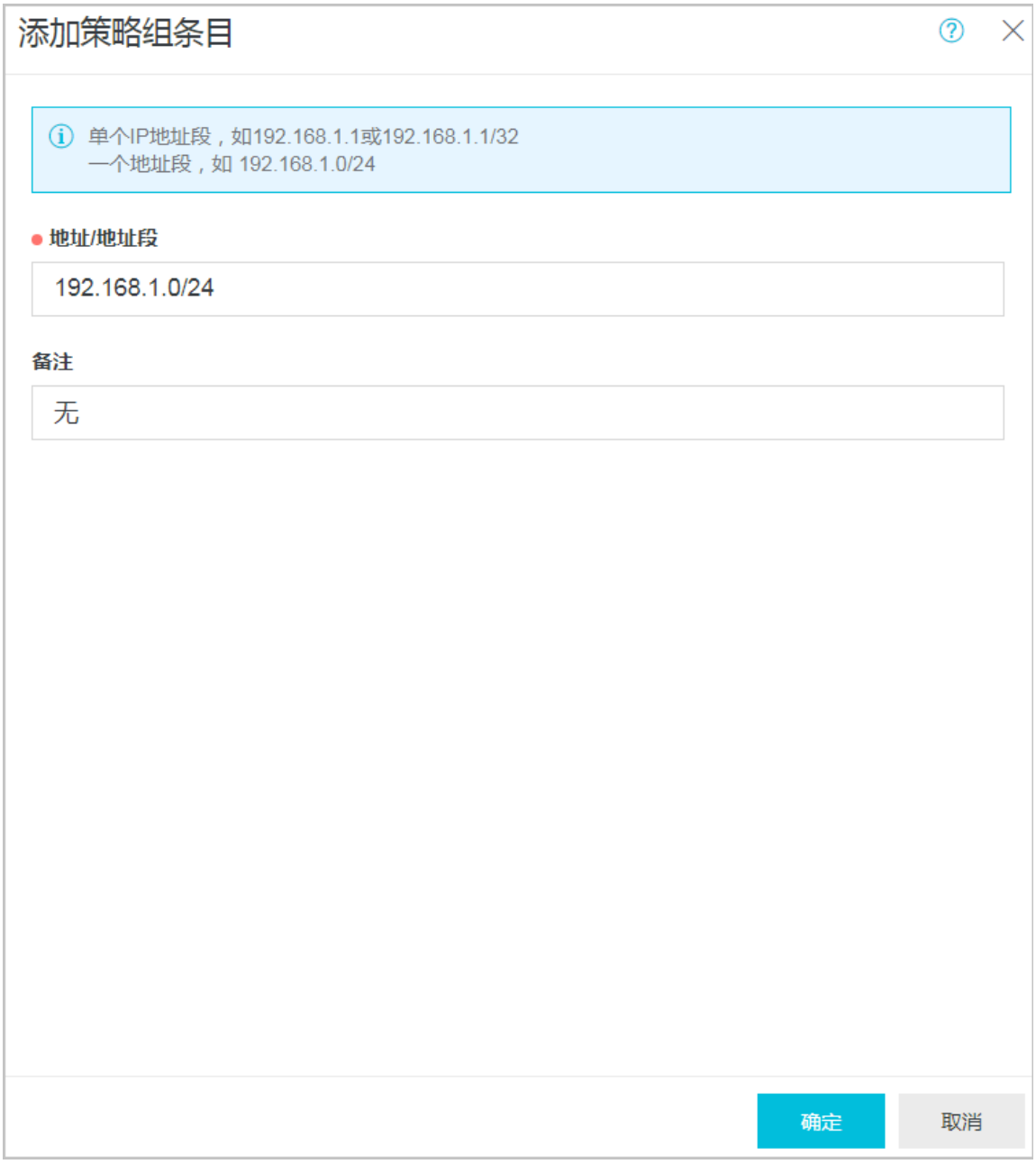
1. 登录负载均衡管理控制台。
2. 选择地域。
3. 在左侧导航栏，单击访问控制。
4. 找到目标访问控制策略组，然后单击管理访问控制策略组。
5. 添加IP条目：
   - 单击批量添加条目，在弹出的对话框中批量添加IP地址或IP地址段，单击确定。

     在添加条目时注意：

     - 每个条目一行，以回车分隔。

- 每个条目中IP地址或IP地址段与备注之间用“|”分隔，如“192.168.1.0/24|备注信息”。

· 单击添加条目，在弹出的对话中输入要添加的IP地址或IP地址段和备注，单击确定。



删除IP条目

完成以下操作，删除IP条目：

1. **登录负载均衡管理控制台。**
2. **选择地域。**
3. **在左侧导航栏，单击访问控制。**
4. **找到目标访问控制策略组，然后单击管理访问控制策略组。**
5. **单击目标IP条目的操作列下的删除，或选择多个IP条目，然后单击删除。**
6. **在弹出对话框中，单击确认。**

7.2 设置访问控制

负载均衡提供监听级别的访问控制。您可以针对不同的监听设置访问白名单或黑名单。

您可以在创建监听时配置访问控制，也可以在监听创建后修改或重新配置访问控制。

本文介绍如何在监听创建后，配置访问控制。

开启访问控制

在开启访问控制前，确保：

- 已经创建访问控制策略，详情参见配置访问控制策略组。
- 已经创建监听。

完成以下操作，开启访问控制：

1. 登录负载均衡管理控制台。
2. 选择实例的所属地域。
3. 单击需要设置访问控制的实例ID。
4. 在实例详情页面，单击监听页签。
5. 找到目标监听，单击更多 > 设置访问控制 。

6. 在访问控制设置页面，开启访问控制，然后选择访问控制方式和访问控制策略组，单击确定。
   - 白名单：仅转发来自所选访问控制策略组中设置的IP地址或地址段的请求，白名单适用于应用只允许特定IP访问的场景。

     设置白名单存在一定业务风险。一旦设置白名单，就只有白名单中的IP可以访问负载均衡监听。如果开启了白名单访问，但访问策略组中没有添加任何IP，则负载均衡监听会转发全部请求。
   - 黑名单：来自所选访问控制策略组中设置的IP地址或地址段的所有请求都不会转发，黑名单适用于应用只限制某些特定IP访问的场景。

如果开启了黑名单访问，但访问策略组中没有添加任何IP，则负载均衡监听会转发全部请求。

关闭访问控制

完成以下操作，关闭访问控制前：

1. 登录负载均衡管理控制台。
2. 选择实例的所属地域。
3. 单击需要设置访问控制的实例ID。
4. 在实例详情页面，单击监听页签。
5. 找到目标监听，单击更多 > 设置访问控制 。
6. 在访问控制设置页面，关闭访问控制，然后单击确定。

7.3 迁移至新版访问控制

如果您之前在监听上配置过访问控制白名单，系统可以自动将白名单中的IP地址或IP地址段自动添加到访问控制策略组并应用到监听上，免去手动迁移的麻烦。

迁移旧版访问控制白名单

完成以下操作，将旧版访问控制白名单切换到新版访问控制：

1. 登录负载均衡管理控制台。
2. 选择目标负载均衡实例的地域，单击目标实例ID。
3. 选择监听页签。
4. 找到目标监听，选择更多 > 设置访问控制 。
5. 单击使用新版访问控制。
6. 输入策略名称，然后单击创建访问控制策略。
7. 单击应用将该策略组作为白名单应用到监听。

> 说明：
> 如果您没有将该策略组应用到监听，则该白名单不生效。

查看迁移的访问控制策略组

完成以下操作，查看迁移的访问控制策略组：

1. 登录负载均衡管理控制台。
2. 选择地域。
3. 在左侧导航栏，单击访问控制。

4. 找到已创建的访问控制策略组，查看绑定的监听，您也可以单击管理访问控制策略组，管理IP条目。

7.4 配置访问控制白名单

白名单是一种访问控制方式，可以为负载均衡监听设置仅允许哪些IP访问，适用于应用只允许特定IP访问的场景。

背景信息

说明:

负载均衡已经在全部地域发布新版访问控制功能，支持设置白名单和黑名单。您可以迁移至新版访问控制，详情参见迁移至新版访问控制。

在设置访问控制白名单前，请注意：

- 设置白名单存在一定业务风险。一旦设置白名单，就只有白名单中的IP可以访问负载均衡监听。
- 如开启访问控制而不设置白名单列表，则这个负载均衡监听就无法访问。

操作步骤

1. 登录负载均衡管理控制台。
2. 选择负载均衡实例的地域。
3. 单击需要设置访问控制的负载均衡实例的ID。
4. 在监听页签下，选择更多 > 设置访问控制。
5. 在访问控制设置对话框，进行如下配置：
   a) 拖动启动访问控制开关，打开开关。
   b) 在白名单设置区域内输入允许访问该监听的IP地址。

      多个IP地址以逗号隔开且不可重复，最多允许输入300个IP地址。支持输入单个IP地址或者IP网段。

   c) 单击确定。

8 监控

8.1 查看监控

结合阿里云云监控服务，您可以查看负载均衡的云监控数据，如连接数、数据包数和流量等。

操作步骤

1. 登录负载均衡管理控制台。
2. 选择负载均衡实例的地域。
3. 单击目标实例的监控图标 。
4. 选择要查看的监控指标，查看监控数据。

负载均衡的监控指标如下表所示。

监控指标	说明
流量	· 流入流量：从外部访问负载均衡所消耗的流量。 · 流出流量：负载均衡访问外部所消耗的流量。
数据包数	· 流入数据包数：负载均衡每秒接到的请求数据包数量。 · 流出数据包数：负载均衡每秒发出的数据包数量。

监控指标	说明
并发连接数	· 活跃连接数：所有ESTABLISHED状态的TCP连接。因为如果您采用的是长连接的情况，一个连接会同时传输多个文件请求。 · 非活跃连接数：表示指除ESTABLISHED状态的其它所有状态的TCP连接数。Windows和Linux服务器都可以使用`netstat -an`命令查看。 · 并发连接数：所有建立的TCP连接数量。
新建连接数	在统计周期内，新建立的从客户端连接到负载均衡的连接请求的平均数。
丢弃流量	· 丢弃入流量：每秒丢失的入流量。 · 丢弃出流量：每秒丢失的出流量。
丢弃数据包数	· 丢弃流入数据包：每秒丢弃的流入数据包的数量。 · 丢弃流出数据包：每秒丢弃的流出数据包的数量。
丢弃连接数	每秒丢弃的连接数。
以下是7层（HTTP/HTTPS）监听特有的监控指标。	
7层协议QPS	每秒可以处理的HTTP/HTTPS请求。
7层协议RT	负载均衡的平均响应时间。
7层协议返回码(2XX)/(3xx)/(4xx)(5xx)(Others)	监听返回的HTTP响应代码的数量。
7层协议UpstreamCode4XX/5XX	后端服务器返回的HTTP响应代码的数量。
7层协议UpstreamRT	后端服务器的平均响应时间。

8.2 设置报警规则

开通云监控服务后，您可以在云监控控制台为负载均衡实例配置监控报警规则。

背景信息

> **说明:**
> 负载均衡的监听或实例被删除，其在云监控设置的报警规则也会相应删除。

操作步骤

1. 登录负载均衡管理控制台。
2. 选择负载均衡实例的地域。

3. 单击实例后的  。

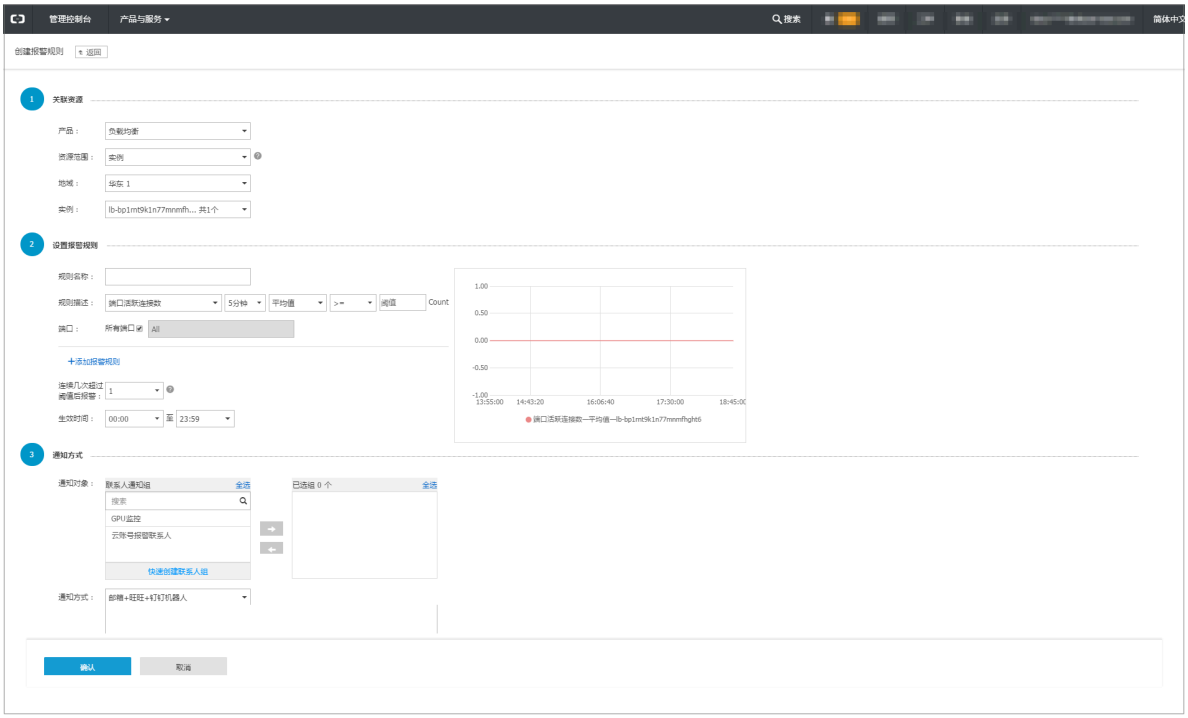
 :

确保该实例已经配置了监听，并开启了健康检查。

4. 单击阈值报警设置，进入云服务监控页面。

5. 单击创建报警规则。

6. 配置报警规则。



9 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

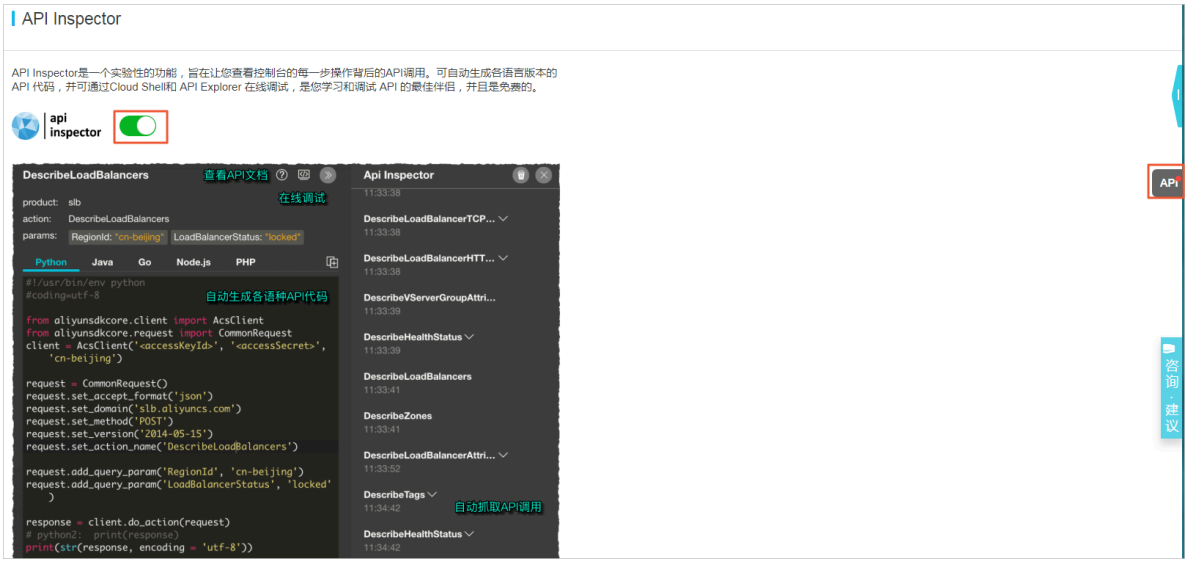
API Inspector与API Explorer、Cloud Shell三位一体，成为阿里云用户学习和调试API的一体化解决方案，具有以下特性：

- 自动录制：想要什么功能的API，在控制台操作相应的功能即可获得相关API调用，详情参见自动录制API调用。
- 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，详情参见一键生成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，所见即所得，详情参见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：

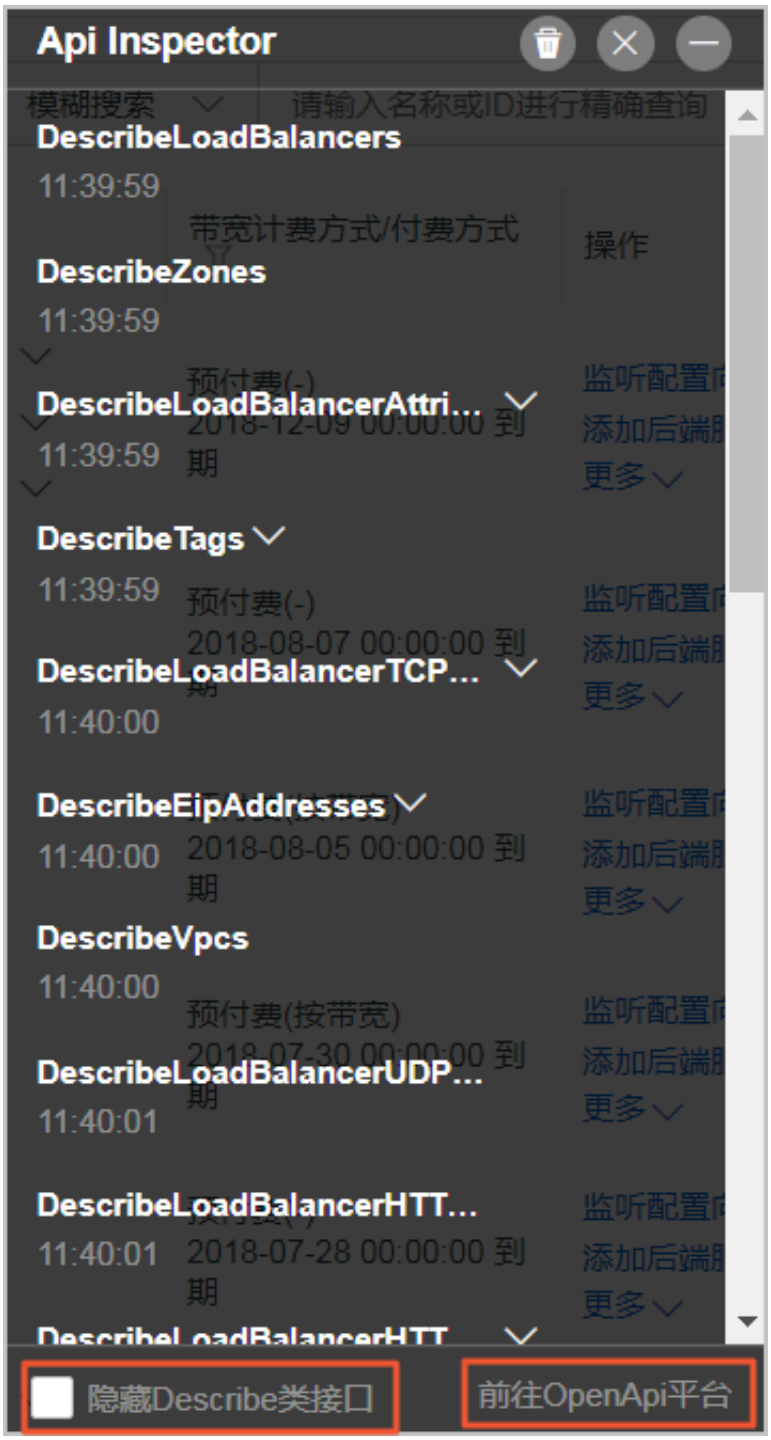
1. 登录负载均衡管理控制台。
2. 在左侧导航栏选择SLB实验室 > API Inspector。
3. 在API Inspector页面，开启API Inspector功能，在页面右侧显示API悬浮挂件。



自动录制API调用

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. 选择实例 > 实例管理。
2. 将某个负载均衡实例的名称修改为SLB1。
3. 单击确定，完成实例名称修改。
4. 单击页面右侧的 API，可以看到上述操作涉及的所有API调用。



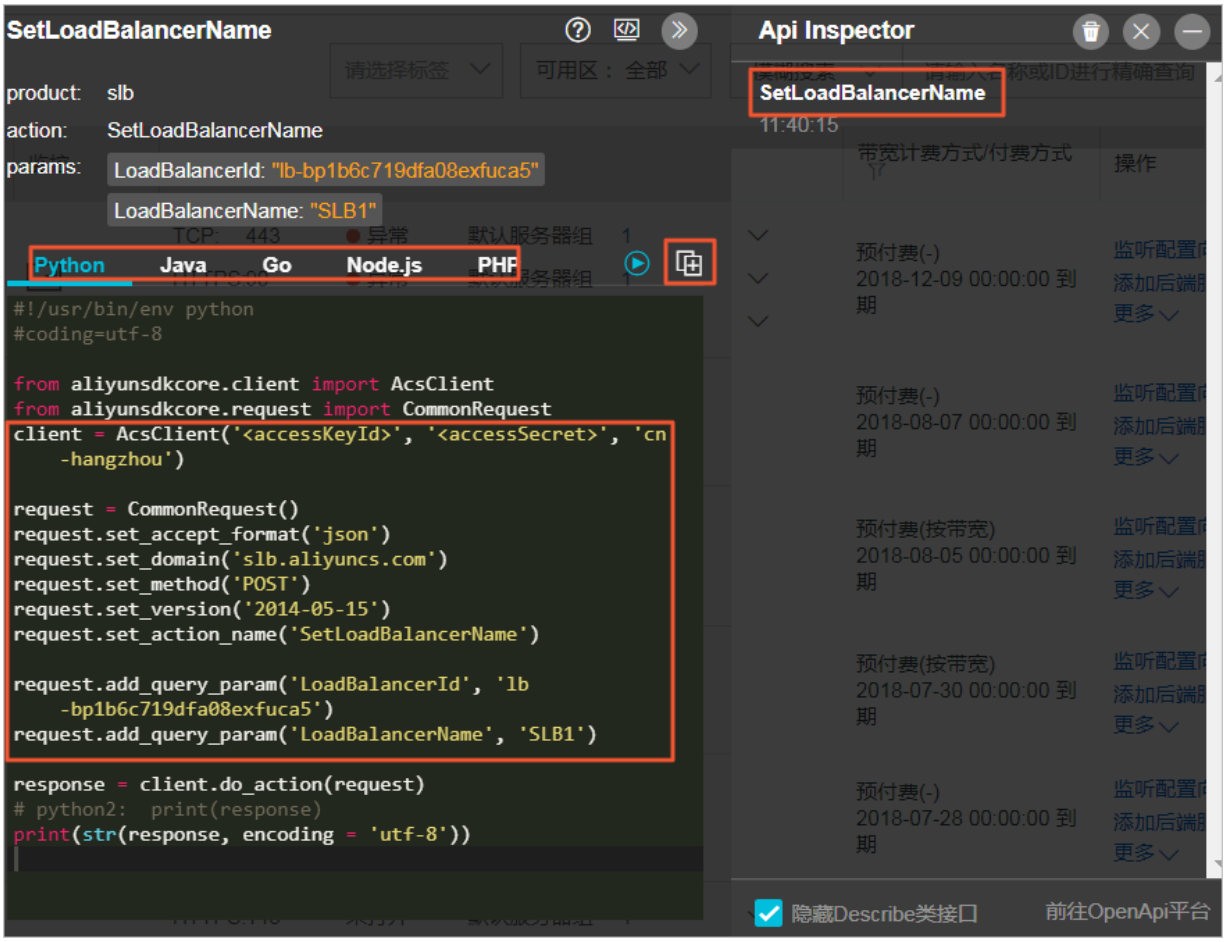
5. 支持勾选隐藏Describe类接口，查看功能核心接口，本示例为`SetLoadBalancerName`。

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和PHP格式的API代码片段参数预填充。

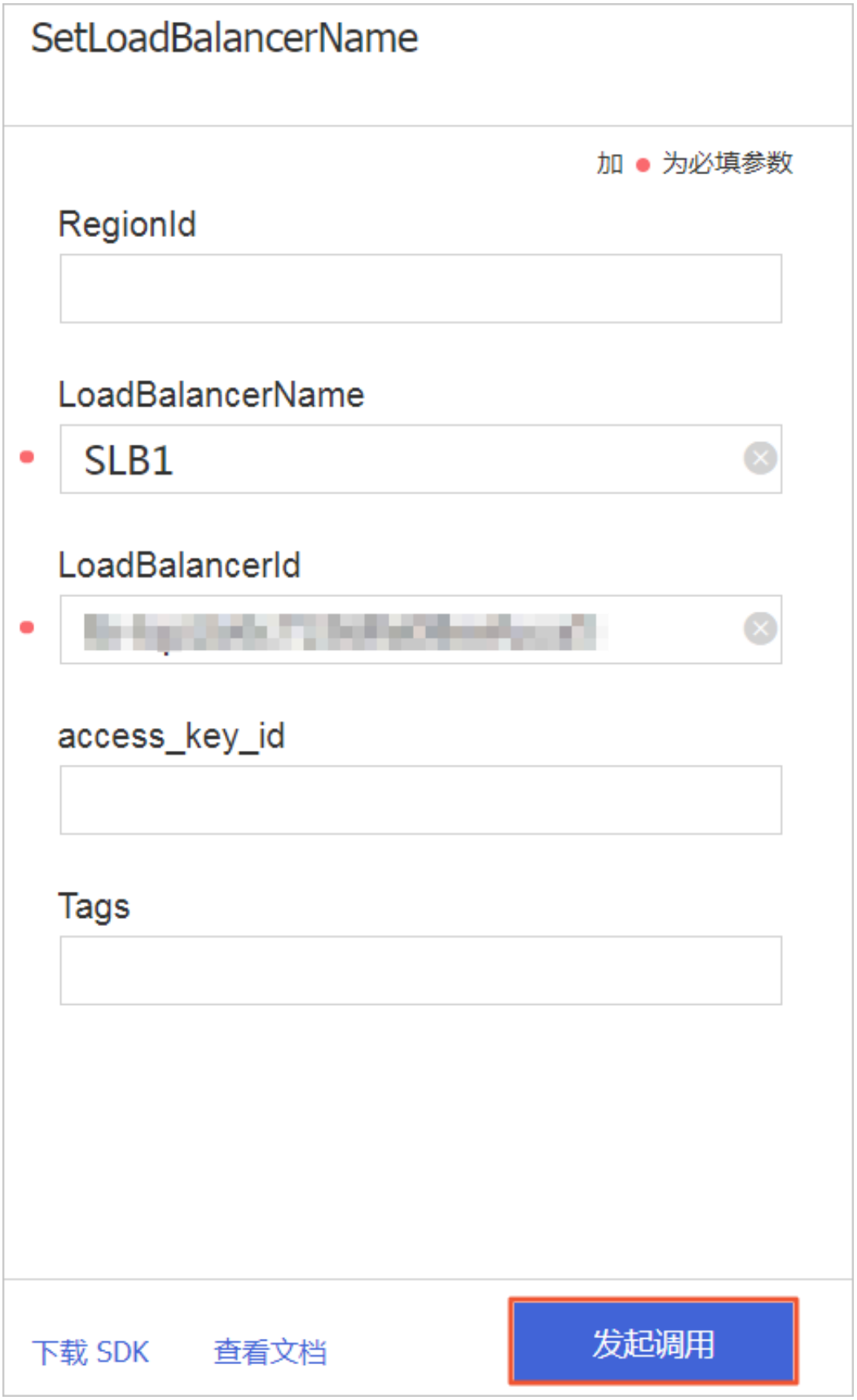
说明:

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平台或者  ，可以直接到*OpenAPI Explorer*控制台调试对应的功能且API参数值已经按照控制台操作自动生成。


SetLoadBalancerName
加 ● 为必填参数
RegionId
LoadBalancerName
SLB1
LoadBalancerId
access_key_id
Tags
下载 SDK
查看文档
发起调用

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：

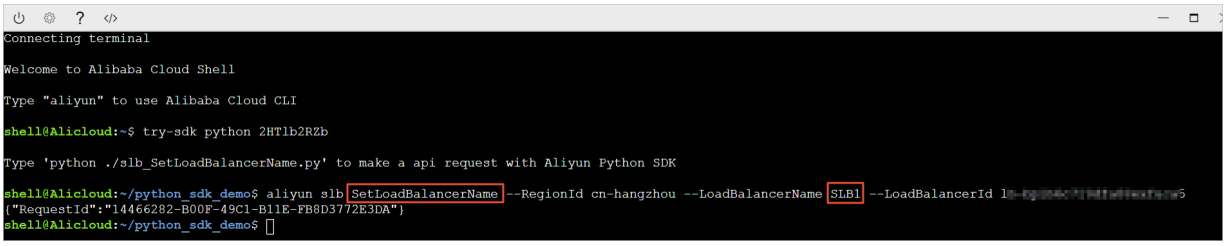
```
aliyun slb actionName --parameter1 value1 --paramter2 value2...
```

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 --LoadBalanc
erName SLB1 --LoadBalancerId lb-bp1b6c719dfa08exfuca5
```

返回值为：

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



10 多可用区

在创建负载均衡实例时，您可以选择将负载均衡创建在支持多可用区的地域，提高服务的可用性。

什么是多可用区

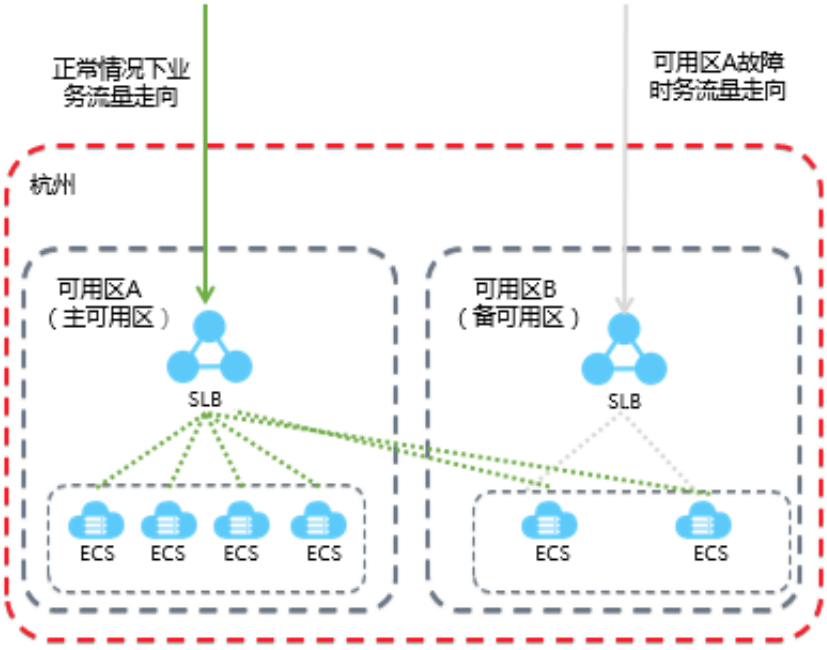
云产品的可用区指的是一套独立的基础设施，不同的可用区之间基础设施（网络，电力和空调等）相互独立，即一个可用区出现基础设施故障不影响另外一个可用区。

为了向广大用户提供更加稳定可靠的负载均衡服务，阿里云负载均衡已在各地域（Region）部署了多可用区以实现同地域下的跨机房容灾。当主可用区的机房故障或不可用时，负载均衡仍然有能力在非常短的时间内（约30秒）切换到另外一个备可用区的机房并恢复服务的能力；当主可用区恢复时，负载均衡同样会自动切换到主可用区的机房提供服务。

关于负载均衡主备可用区，请注意：

- SLB支持跨可用区挂载后端ECS，即只要ECS和SLB实例在同一个地域即可。SLB可以同时将流量分发至不同可用区的ECS上。
- 正常情况下，备可用区的SLB实例处于待机状态。您不可以手动切换SLB实例的主备工作状态，只有当阿里云检测到整个可用区不可用时如如机房整体断电、机房出口光缆中断等，负载均衡才会切换到备可用区。而并非某个实例出现故障，就切换到备可用区。
- SLB和ECS是不同的集群。可用区A的SLB不可用时，ECS并不一定不可用，因此如果仅因为SLB集群故障导致的SLB主备倒换，备可用区的SLB依然可以将流量分发至不同可用区的ECS。但当整个可用区的所有集群断电或光缆中断时，那么可用区的所有服务（包括但不限于SLB、ECS等）就都无法正常工作了。

更多信息，参见负载均衡高可用最佳实践。



主备可用区列表

下表列举了各地域的主备可用区，您也可以通过DescribeZones接口查询可用的主备可用区。

地域	可用区类型	可用区	
华东1（杭州）	多可用区	主可用区	可选备可用区
		可用区B	可用区D 可用区G
		可用区D	可用区E
		可用区E	可用区D 可用区F
		可用区F	可用区E
		可用区G	可用区B 可用区H
		可用区H	可用区G
华东2（上海）	多可用区	主可用区	可选备可用区
		可用区A	可用区B
		可用区B	可用区A 可用区C 可用区D
		可用区C	可用区B

地域	可用区类型	可用区	
		可用区D	可用区B 可用区E
		可用区E	可用区D 可用区F
		可用区F	可用区E
华南1（深圳）	多可用区	主可用区	可选备可用区
		可用区A	可用区B
		可用区B	可用区A 可用区C
		可用区C	可用区B 可用区D
		可用区D	可用区C 可用区E
		可用区E	可用区D
华北1（青岛）	多可用区	主可用区	可选备可用区
		可用区B	可用区C
		可用区C	可用区B
华北2（北京）	多可用区	主可用区	可选备可用区
		可用区A	可用区B 可用区D 可用区E
		可用区B	可用区C
		可用区C	可用区E
		可用区D	可用区A
		可用区E	可用区C 可用区F
		可用区F	可用区E 可用区G
		可用区G	可用区F
华北3（张家口）	多可用区	主可用区	可选备可用区
		可用区A	可用区B
		可用区B	可用区A

地域	可用区类型	可用区	
华北5（呼和浩特）	多可用区	主可用区	可选备可用区
		可用区A	可用区B
		可用区B	可用区A
欧洲中部1（法兰克福）	多可用区	主可用区	可选备可用区
		可用区A	可用区B
		可用区B	可用区A
英国（伦敦）	多可用区	主可用区	可选备可用区
		可用区A	可用区A
		可用区B	可用区B
中东东部1（迪拜）	单可用区	可用区A	
亚太东南1（新加坡）	多可用区	主可用区	可选备可用区
		可用区A	可用区B
		可用区B	可用区A
		可用区C	可用区B
亚太东南2（悉尼）	多可用区	主可用区	可选备可用区
		可用区A	可用区B
		可用区B	可用区A
亚太东南3（吉隆坡）	多可用区	主可用区	可选备可用区
		可用区A	可用区B
		可用区B	可用区A
亚太东南5（雅加达）	单可用区	可用区A	
亚太南部1（孟买）	多可用区	主可用区	可选备可用区
		可用区A	可用区B
		可用区B	可用区A
亚太东北1（东京）	单可用区	可用区A	
香港	多可用区	主可用区	可选备可用区

地域	可用区类型	可用区	
		可用区B	可用区C
		可用区C	可用区B
美东1（弗吉利亚）	多可用区	主可用区	可选备可用区
		可用区A	可用区B
		可用区B	可用区A
美西1（硅谷）	多可用区	主可用区	可选备可用区
		可用区A	可用区B
		可用区B	可用区A

11 结合全局流量管理实现跨地域负载均衡

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。

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。

- 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aliyuntest.club的网站为例（该网站的大多数用户分布在新加坡和国内），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. 参考创建负载均衡实例，分别在北京、深圳、新加坡创建一个公网负载均衡实例。

2. 参考配置负载均衡实例，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。

   a. 登录云解析DNS管理控制台。

   b. 在左侧导航栏，单击全局流量管理。

   c. 在全局流量管理页面，单击创建实例。

   d. 选择套餐版本、购买数量和购买时长。

   e. 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。

   a. 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。

   b. 在左侧导航栏，单击配置管理。

   c. 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，自定义。
   - 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aliyuntest.club。
   - 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。

   d. 单击确认。

3. 配置地址池。

   a. 在地址池配置页签下，单击新增地址池。

   b. 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。

c. 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。

a. 在地址池页签下，单击健康检查后的修改。

b. 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。

a. 在访问策略页签下，单击新增访问策略。

b. 在新增访问策略页面，配置访问策略。

- 不同的访问地应的默认地址池，Failover地址池可以为设置为其他区域的地地池。
- 选择访问地，该区地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。

a. 登录云解析DNS控制台。

b. 单击aliyuntest.club域名操作列的解析设置。

c. 在解析设置页面，单击添加记录。

d. 在添加记录页面，将最终用户访问的aliyuntest.club域名通过CNAME的形式指向全局流量管理实例的别名记录。

e. 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:

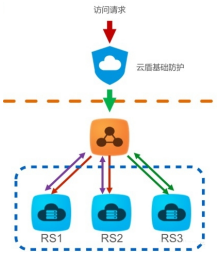
全局流量管理监控到您的IP宕机后需要1-2分钟聚合判断，假设您的监控频率设置是1分钟，那么线路异常切换生效时间在2-3分钟内。

12 DDoS基础防护

负载均衡控制台可以查看公网负载均衡实例的云盾阈值。

DDoS基础防护介绍

阿里云免费为负载均衡服务提供最高5G的DDoS基础防护。如下图所示，所有来自Internet的流量都要先经过云盾再到达负载均衡，云盾会针对常见的攻击进行清洗过滤。云盾DDoS基础防护可以防御SYN Flood、UDP Flood、ACK Flood、ICMP Flood 和DNS Flood等DDoS攻击。



云盾DDoS基础防护根据公网负载均衡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Internet的攻击流量较大或符合某些特定攻击流量模型特征时，云盾将会针攻击流量启动清洗操作，清洗包括攻击报文过滤、流量限速、包限速等。
- 黑洞：当来自Internet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。

阈值的计算遵循如下两个原则：

- 根据SLB实例所购买的带宽来决定阈值的高低，即SLB的出方向带宽，当实例的带宽较高时，各类阈值较高，当实例的带宽较低时，各类阈值相应的会变低。
- 根据用户的安全信誉分来决定黑洞阈值的高低。

> 说明：
> 注意安全信誉分仅影响黑洞阈值，不影响清洗阈值。

完成以下操作，计算阈值：

1. SLB后台根据用户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：
> 如果用户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，目前国内地域带宽上限都是峰值5G，详情参见各地域带宽峰值限制。

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

  清洗PPS阈值 = （SLB带宽值/500）*150000

  带宽值单位为Mbps。
- SLB带宽与黑洞BPS阈值之间的关系
  - 当SLB带宽<1Gbps时，黑洞BPS默认阈值 = 2Gbps
  - 当SLB带宽>1Gbps时，黑洞BPS默认阈值 = MAX(SLB带宽值*1.5,2G)

2. 云盾根据SLB给出的建议值，结合用户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1000M，PPS最小值为30万个。
     - 当SLB传入的参考阈值小于上述最小值时，取上述最小值。
     - 当SLB传入的参考阈值高于上述最小值时，取SLB传入的参考阈值。
   - 云盾根据用户的安全信誉分来决定黑洞阈值的高低。

查看防护阈值

使用子账号登录阿里云控制台后，若无法在控制台上查看防护阈值，需要先对子账号授权。详情参见授予云盾基础防护只读权限。

完成以下操作查看防护阈值：

1. 登录负载均衡管理控制台。
2. 选择地域，查看该地域的所有实例。
3. 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。您可以单击DDoS控制台链接查看更多信息。
   - 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。

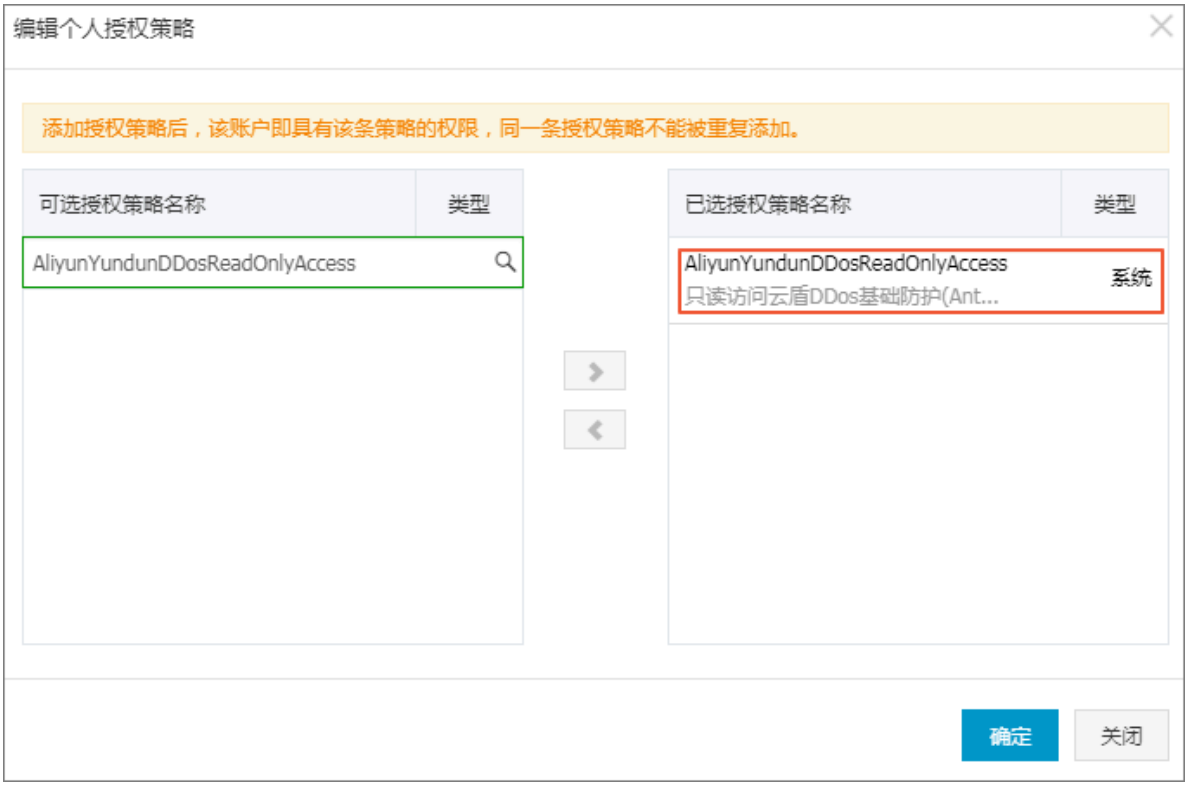
授权云盾基础防护只读权限

完成以下操作授予子账号只读访问云盾DDoS基础防护(Anti-DDoS Basic)的权限：

> **说明:**
> **使用主账号进行授权。**

1. **使用主账号登录访问控制RAM管理控制台。**
2. **在左侧导航栏，单击用户管理，找到目标子账号，然后单击管理。**

3. **单击用户授权策略，然后单击编辑授权策略。**
4. **在弹出的对话框，在可授权策略列表中搜索AliyunYundunDDosReadOnlyAccess，将其加入到已授权策略列表。单击确定。**



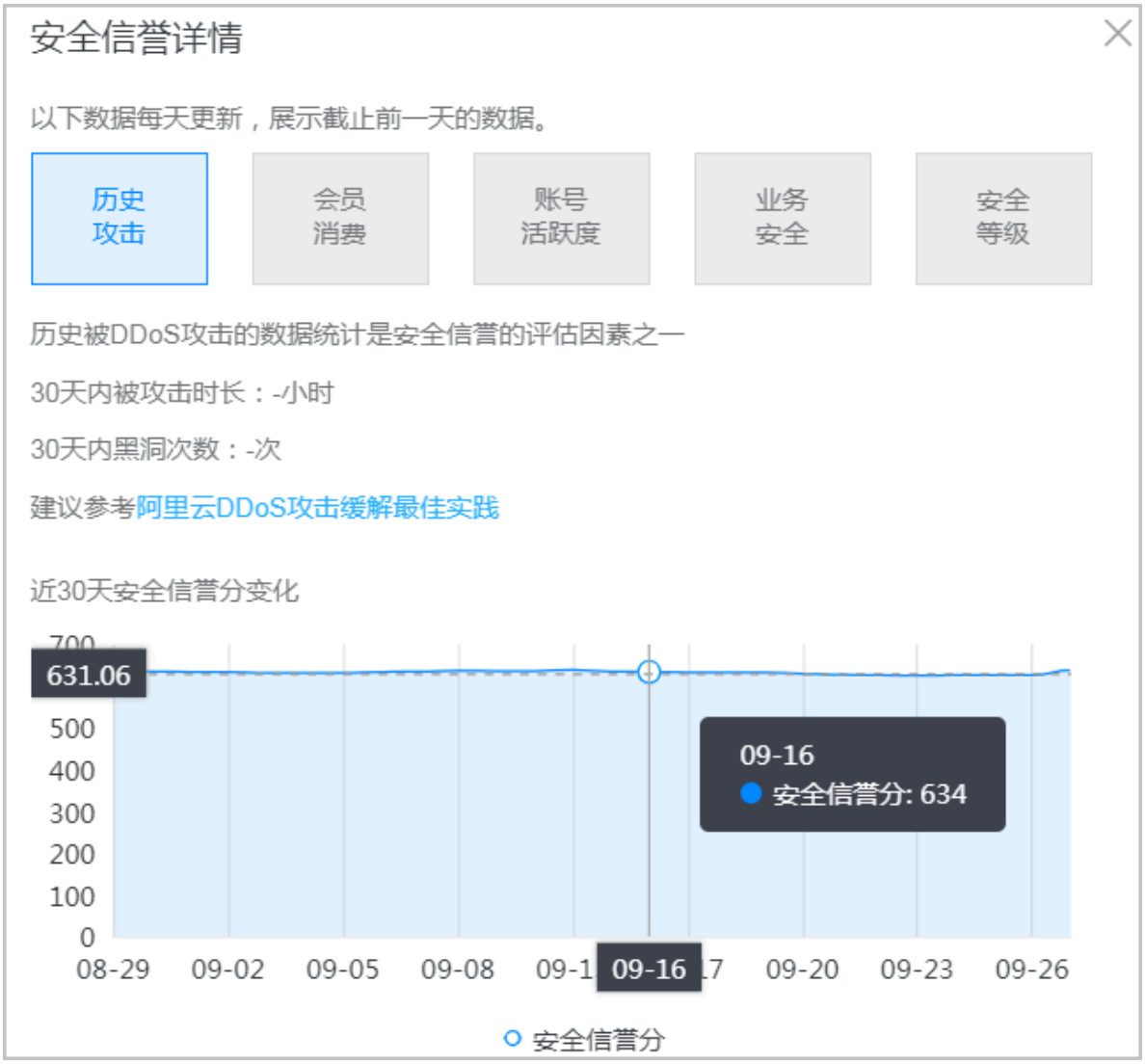
查看安全信誉分

安全信誉分是阿里云对用户的安全信誉做出的评级，结合历史攻击、会员消费、活跃度、安全等级和使用预期等指标综合给出的一个信用评级，用户的安全信誉等级越高，用户则可以拥有更大的免费黑洞阈值，和更短的黑洞时长（被黑洞后多久可以解除黑洞状态）。

完成以下操作，查看安全信誉分：

1. 登录*DDoS基础防护控制台*。
2. 选择基础防护 > 实例。
3. 单击安全信誉链接，查看当前账号的安全信誉分。

> **说明:**
> 安全信誉值是分地域的。


安全信誉详情
以下数据每天更新，展示截止前一天的数据。
历史攻击
会员消费
账号活跃度
业务安全
安全等级
历史被DDoS攻击的数据统计是安全信誉的评估因素之一
30天内被攻击时长：-小时
30天内黑洞次数：-次
建议参考阿里云DDoS攻击缓解最佳实践
近30天安全信誉分变化
700
631.06
500
400
300
200
100
0
09-16
安全信誉分: 634
08-29
09-02
09-05
09-08
09-1
09-16
09-20
09-23
09-26
安全信誉分