负载均衡

产品简介

阿里云
aliyun.com

产品简介

产品概述

产品概述

负载均衡（Server Load Balancer）是对多台云服务器进行流量分发的负载均衡服务。负载均衡可以通过流量分发扩展应用系统对外的服务能力，通过消除单点故障提升应用系统的可用性。

负载均衡服务通过设置虚拟服务地址（IP），将位于同一地域（Region）的多台云服务器（Elastic Compute Service，简称ECS）资源虚拟成一个高性能、高可用的应用服务池；根据应用指定的方式，将来自客户端的网络请求分发到云服务器池中。

- 负载均衡服务会检查云服务器池中ECS的健康状态，自动隔离异常状态的ECS，从而解决了单台ECS的单点问题，同时提高了应用的整体服务能力。在标准的负载均衡功能之外，负载均衡服务还具备TCP与HTTP抗DDoS攻击的特性，增强了应用服务器的防护能力。
- 负载均衡服务是ECS面向多机方案的一个配套服务，需要同ECS结合使用。

访问官网

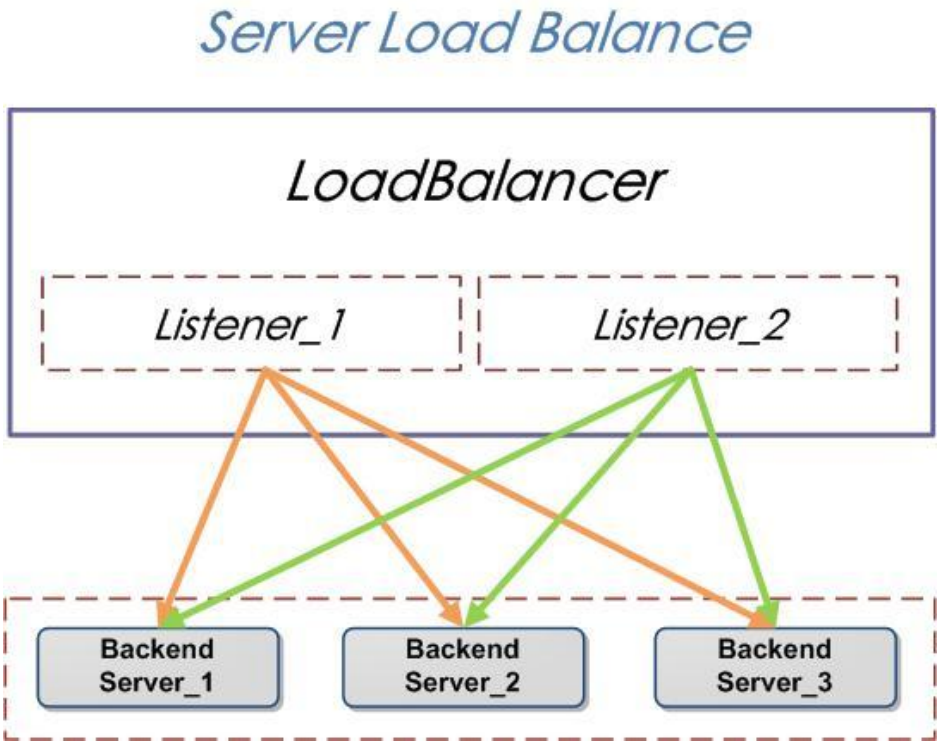
核心概念

负载均衡服务主要有三个核心概念：

- LoadBalancer代表一个负载均衡实例。
- Listener代表用户定制的负载均衡策略和转发规则。
- BackendServer是后端的一组ECS。

来自外部的访问请求，通过负载均衡实例并根据相关的策略和转发规则分发到后端ECS进行处理。

负载均衡核心概念如图示



使用限制

- 负载均衡不支持跨地域（Region）部署，也就是说一个负载均衡实例后端的ECS必须是属于同一地域（Region）的ECS实例。
- 在4层（TCP协议）服务中，当前不支持添加进后端云服务器池的ECS既作为Real Server，又作为客户端向所在的负载均衡实例发送请求。因为，返回的数据包只在云服务器内部转发，不经过负载均衡，所以通过配置在负载均衡内的ECS去访问的VIP是不通的。
- 负载均衡服务不限制通过ECS ping 负载均衡实例的公网IP。但是针对华北1(青岛)节点、华北2(北京)节点和华东1(杭州)节点中一部分新购ECS无法通过ECS ping 负载均衡实例的私网IP。这一限制并不影响负载均衡实例与ECS之间的通信。
- 金融云的客户为了满足其安全合规的需求，目前其公网类型的负载均衡实例端口只能对外开放这些端口：80，443，2800-3300，5000-10000，13000-14000。

使用注意事项

- 在通过负载均衡对外提供服务前，首先要确保已经完成并正确配置了所有负载均衡后端ECS上的应用服务，且能通过ECS的服务地址正确访问该服务。
- 负载均衡不提供ECS间的数据同步服务，如果部署在负载均衡后端ECS上的应用服务是无状态的，那么可以通过独立的ECS或RDS服务来存储数据；如果部署在负载均衡后端ECS上的应用服务是有状态的，那么需要确保这些ECS上的数据是同步的。
- 当负载均衡实例的服务地址（IP）已经解析到正常的域名进行对外服务时，请不要随意删除该负载均衡实例。删除负载均衡实例操作会将该负载均衡实例的服务地址（IP）一同释放掉，从而导致已经对外提供的服务中断。如果创建新的负载均衡实例，系统会重新分配一个服务地址（IP）。

协议支持

当前提供4层（TCP协议和UDP协议）和7层（HTTP和HTTPS协议）的负载均衡服务。

健康检查

可以对后端ECS进行健康检查，自动屏蔽异常状态的ECS，待该ECS恢复正常后自动解除屏蔽。

会话保持

提供会话保持功能，在Session的生命周期内，可以将同一客户端请求转发到同一台后端ECS上。

调度算法

支持加权轮询（WRR），加权最小连接数（WLC）这两种调度算法。WRR的方式将外部请求依序分发到后端ECS上，WLC的方式将外部请求分发到当前连接数最小的后端ECS上，后端ECS权重越高被分发的几率也越大。

域名URL转发

针对七层协议（HTTP协议和HTTPS协议），支持按用户访问的域名和URL来转发流量到不同的虚拟服务器组。

多可用区

可以支持指定可用区创建负载均衡实例，在多可用区部署的地域还支持主备可用区，当主可用区出现故障时，可自动切换到备可用区上提供服务。

访问控制

可以支持白名单控制，可以针对负载均衡监听设置仅仅允许哪些IP访问，适用于用户的应用只允许特定IP访问的场景。

安全防护

提供应用防火墙和CC防护功能，集群内置WAF模块，不用修改CNAME即可进行WAF防护；结合云盾，还可提供5G以下的防DDOS攻击能力。

证书管理

针对HTTPS协议，提供统一的证书管理服务，证书无需上传后端ECS，解密处理在负载均衡上进行，降低后端ECS CPU开销。

带宽控制

支持针对监听来分配其对应服务所能达到的带宽峰值。

实例/网络类型支持

- 可以支持公网或私网类型的负载均衡服务。
- 可以支持经典网络或专有网络类型的负载均衡服务。

监控

提供丰富的监控数据，实时了解负载均衡运行状态。

管理方式

提供控制台、API、SDK多种管理方式。

产品名词解释

术语表

术语	全称	中文	说明
负载均衡	Server Load Balancer	负载均衡服务	阿里云计算提供的一种网络负载均衡服务，可以结合阿里云提供的ECS服务为用户提供基于ECS实例的TCP与HTTP负载均衡服务。
LoadBalancer	Load Balancer	负载均衡服务实例	负载均衡实例可以理解为负载均衡服务的一个运行实例，用户要使用负载均衡服务，就必须先创建一个负载均衡实例，LoadBalancerId是识别用户负载均衡实例的唯一标识。
Listener	Listener	负载均衡服务监听	负载均衡服务监听，包

			括监听端口、负载均衡策略和健康检查配置等，每个监听对应后端的一个应用服务
BackendServer	Backend Server	后端服务器	接受负载均衡分发请求的一组ECS，负载均衡服务将外部的访问请求按照用户设定的规则转发到这一组后端ECS上进行处理。
Address	Address	服务地址	系统分配的服务地址，当前为IP地址。用户可以选择该服务地址是否对外公开，来分别创建公网和私网类型的负载均衡服务。
Certificate	Certificate	证书	用于 HTTPS 协议。用户将证书上传到负载均衡中，在创建https 协议监听的时候绑定证书，提供https服务。
Master Availability Zone	Master Availability Zone	主可用区	负载均衡会在某些地域的多个可用区进行部署，用户可指定主备可用区创建负载均衡实例，该实例将默认工作在主可用区。
Slave Availability Zone	Slave Availability Zone	备可用区	负载均衡会在某些地域的多个可用区进行部署，用户可指定主备可用区创建负载均衡实例，当主可用区发生故障时，该实例可切换到备可用区工作。

配置说明

配置和管理一个负载均衡实例，主要涉及3部分的功能操作，包括：负载均衡实例属性配置、负载均衡服务监听配置和负载均衡后端ECS配置。通过实例属性配置来定义一个负载均衡实例的类型，通过服务监听配置来定义一个负载均衡实例的各项策略和转发规则，通过后端ECS配置来定义一个负载均衡实例后端用来处理用户请求的多个ECS实例。

负载均衡实例属性配置

负载均衡名称

用户可以为其创建的负载均衡实例指定一个易于识别的名称，如果用户不指定，那么系统将以该负载均衡实例的LoadBalancerId作为名称进行展示，LoadBalancerId是识别用户负载均衡实例的唯一标识，无法修改。

负载均衡类型

当前提供公网和私网2种类型的负载均衡供用户选择，用户可根据其业务场景来选择配置对外公开或对内私有的负载均衡服务，系统根据用户的选择分配公网或私网服务地址（IP）。

负载均衡服务地址

根据用户选择的负载均衡类型不同，系统会分配不同的服务地址给用户。针对需要通过域名对外提供服务的应用，需要将域名解析到相应的公网服务地址上生效后即可通过域名访问。

负载均衡服务监听配置

负载均衡协议/端口

- 协议：当前提供4层（TCP协议和UDP协议）和7层（HTTP和HTTPS协议）的负载均衡服务。
- 端口：用户负载均衡实例对外或对内提供服务时用来接收请求并向后端服务器进行请求转发的负载均衡系统前端端口，在同一个负载均衡实例内不可重复。

后端协议/端口

- 协议：当前提供4层（TCP协议和UDP协议）和7层（HTTP和HTTPS协议）的负载均衡服务。
- 端口：用户负载均衡实例后端添加的一组用来处理外部或内部请求的ECS上开放的用来接收请求的后端端口，在同一个负载均衡实例内可重复。针对同一组后端ECS上部署多个应用服务的情况，当前负载均衡最多支持50个监听配置规则。

转发规则

当前负载均衡支持轮询和最小连接数2种模式的转发规则。"轮询模式"会将外部和内部的访问请求依序分发给后端ECS进行处理，而"最小连接数模式"会将外部和内部的访问请求分发给当前连接数最小的一台后端ECS进行处理。

获取来访者真实IP

- 针对7层（HTTP协议）服务，由于采取替换HTTP头文件IP地址的方式来进行请求转发，所以后端云服务器看到的访问IP是负载均衡系统的本地IP而不是实际来访者的真实IP。所以系统支持用户采用X-Forwarded-For的方式获取访问者真实IP，系统默认开启7层（HTTP协议）服务监听的"获取真实访问IP"功能，不可关闭。针对常用的应用服务器的配置指引点击这里查看。

- 针对4层（TCP协议）服务，后端云服务器将直接获得来访者的真实IP，所以无需采用其他手段获取。

会话保持

用户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ECS上进行处理。针对7层（HTTP协议和HTTPS协议）服务，负载均衡系统是基于cookie的会话保持。负载均衡系统提供了两种cookie处理方式：

- cookie植入，表示直接由负载均衡系统来分配和管理对客户端进行的cookie植入操作，用户在进行配置时需要指定会话保持的超时时间。

说明：如果用户配置了"植入 Cookie"方式的会话保持, 并且后端 RS 返回的 HTTP 状态代码为 4xx 时, SLB 不支持植入 Set-Cookie 头部, 可能会导致会话保持失败。后端 RS 返回的 HTTP 代码在以下代码中时, SLB 将植入会话保持所需头部：200、201、204、206、301、302、303、304、307。

- cookie重写，表示负载均衡系统会根据用户自定义cookie名称来分配和管理对客户端进行的cookie植入操作，便于用户识别和区分自定义的cookie名称，从而有选择的针对后端应用服务器上的不同应用设定会话保持规则，用户在进行配置时需要指定相应的cookie名称。针对多个域名配置不同会话保持规则的实现方法点击这里查看。

针对4层（TCP协议和UDP协议）服务，负载均衡系统是基于IP地址的会话保持。负载均衡会将来自同一IP地址的访问请求转发到同一台后端云服务器进行处理。

健康检查

- 用户开启健康检查功能后，当后端某个ECS健康检查出现问题时会将请求转发到其他健康检查正常的ECS上，而当该ECS恢复正常运行时，负载均衡会将其自动恢复到对外或对内的服务中。
- 针对7层（HTTP协议和HTTPS协议）服务，负载均衡系统的健康检查机制为：默认由负载均衡系统通过后端ECS内网IP地址来向该服务器应用服务器配置的缺省首页发起http head请求（缺省通过在服务监听配置中指定的后端ECS端口进行访问），返回200 OK后将视为后端ECS运行正常，否则视为后端ECS运行异常。如果用户用来进行健康检查的页面并不是应用服务器的缺省首页，那么需要用户指定相应的URI。如果用户对http head请求限定了host字段的参数，那么需要用户指定相应的URL。用户也可以通过设定健康检查的频率、健康阈值和不健康阈值来更好的控制健康检查功能。
- 针对4层（TCP协议和UDP协议）服务，负载均衡系统的健康检查机制为：默认由负载均衡系统通过在服务监听配置中指定的后端ECS端口发起访问请求，如果端口访问正常则视为后端ECS运行正常，否则视为后端ECS运行异常。
- 针对可能引起健康检查异常的排查思路点击这里查看。

关于TCP/HTTP/HTTPS健康检查的参数配置，提供如下参考建议：

响应超时时间：5秒
健康检查间隔：2秒
不健康阈值：3
健康阈值：3

在此配置下有利于用户服务及应用状态的尽快收敛：
ECS健康检查失败响应时间（网络有问题）：(2+5)×3=21秒

如果用户有更高要求，可以适当地降低响应超时时间值，但必须先保证自己服务在正常状态下的处理时间小于这个值。
ECS健康检查成功响应时间：2×3=6秒

关于UDP健康检查的参数配置，提供如下参考建议：

响应超时时间：10秒
健康检查间隔：5秒
不健康阈值：6
健康阈值：6

在此配置下有利于用户服务及应用状态的尽快收敛：
ECS健康检查失败响应时间（网络有问题）：(5+10)×6=90秒
如果用户有更高要求，可以适当地降低响应超时时间值，但必须先保证自己服务在正常状态下的处理时间小于这个值。
ECS健康检查成功响应时间：5×6=30秒

带宽峰值

用户可以针对监听设定不同的带宽峰值来限定后端ECS上的不同应用所能对外提供的服务能力。

带宽峰值的设定规则：

- 一个负载均衡实例最多对应50个监听，每个监听可独立设定限定规则；
- 单个监听可限定5-1000Mbps范围的带宽峰值；
- 当单个监听上限无法满足用户业务需求时，可以选择不限带宽峰值。

负载均衡后端ECS配置

对于添加到负载均衡实例后端的ECS，原则上不需要进行特别的配置。如果针对关联到负载均衡 4层（TCP协议和UDP协议）服务的Linux系统的ECS，如果发现无法正常访问，需要确保系统配置文件/etc/sysctl.conf的以下三项为0：

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

如果部署在同一内网网段下的ECS之间有通信需求，且发现有无法通信的情况存在，那么需要检查如下参数的配置是否正确：

```
net.ipv4.conf.default.arp_announce =2
net.ipv4.conf.all.arp_announce =2
```

并使用sysctl -p更新配置。

后端ECS权重

用户可以指定后端服务器池内各ECS的转发权重，权重越高的ECS将被分配到更多的访问请求，用户可以根据后

端ECS的对外服务能力和情况来区别设定。

产品优势

产品优势点

高可用

采用全冗余设计，无单点，支持同城容灾，搭配DNS可实现跨REGION容灾，可用性高达99.99%。

根据应用负载进行弹性扩容，在流量波动情况下不中断对外服务。

低成本

与传统硬件负载均衡系统高投入相比成本能下降60%，私网类型实例免费使用，无需一次性采购昂贵的负载均衡设备，无需运维投入。

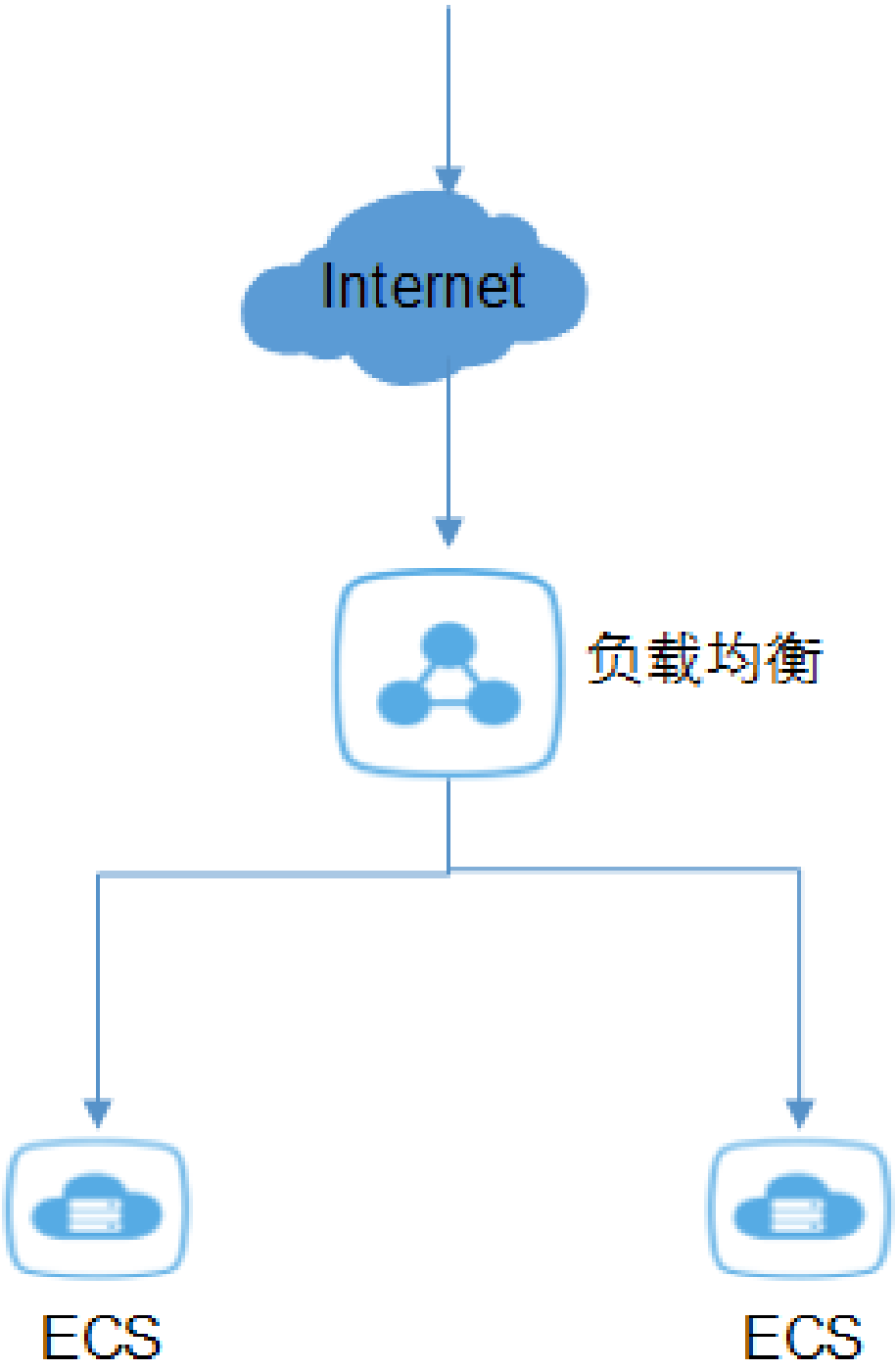
安全

结合云盾提供防DDoS攻击能力，包括：CC、SYN flood等DDoS攻击方式。

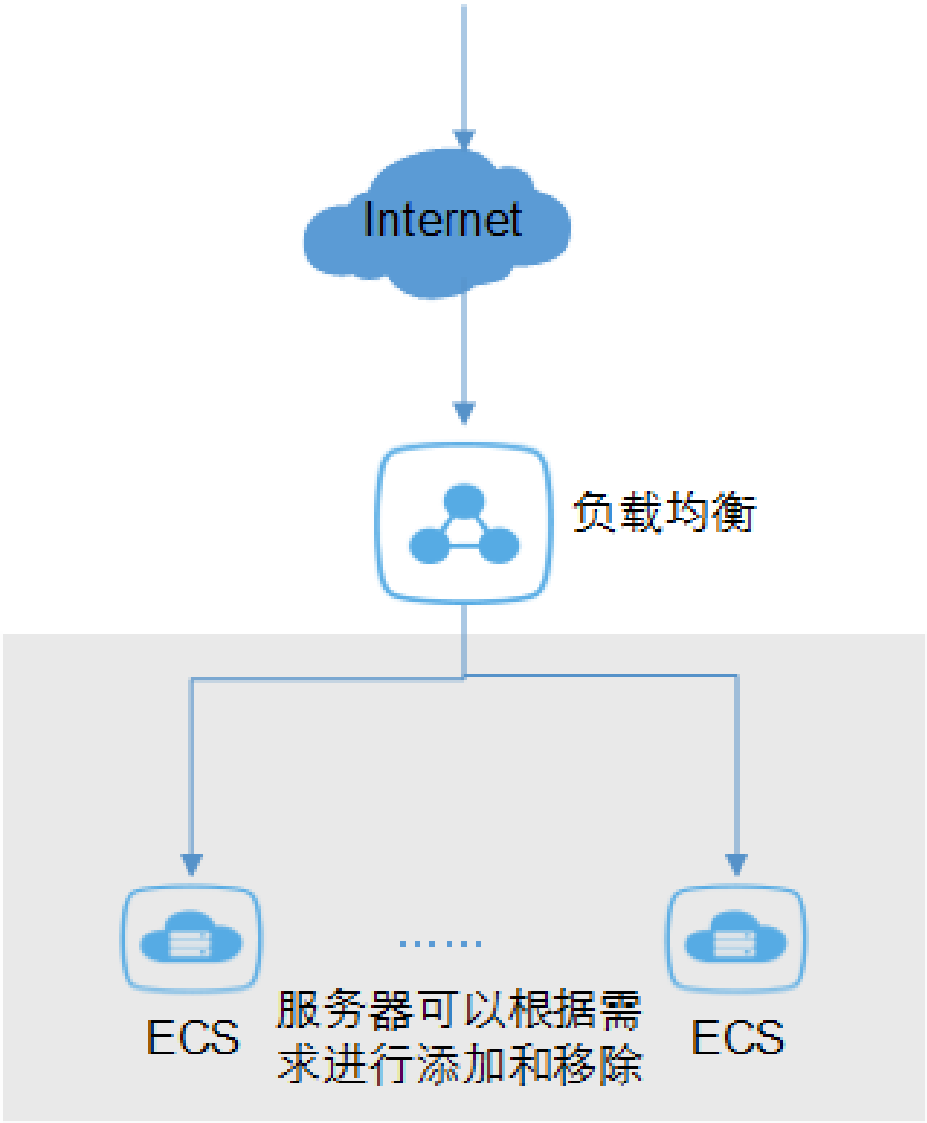
使用场景

负载均衡主要可以应用于以下场景中：

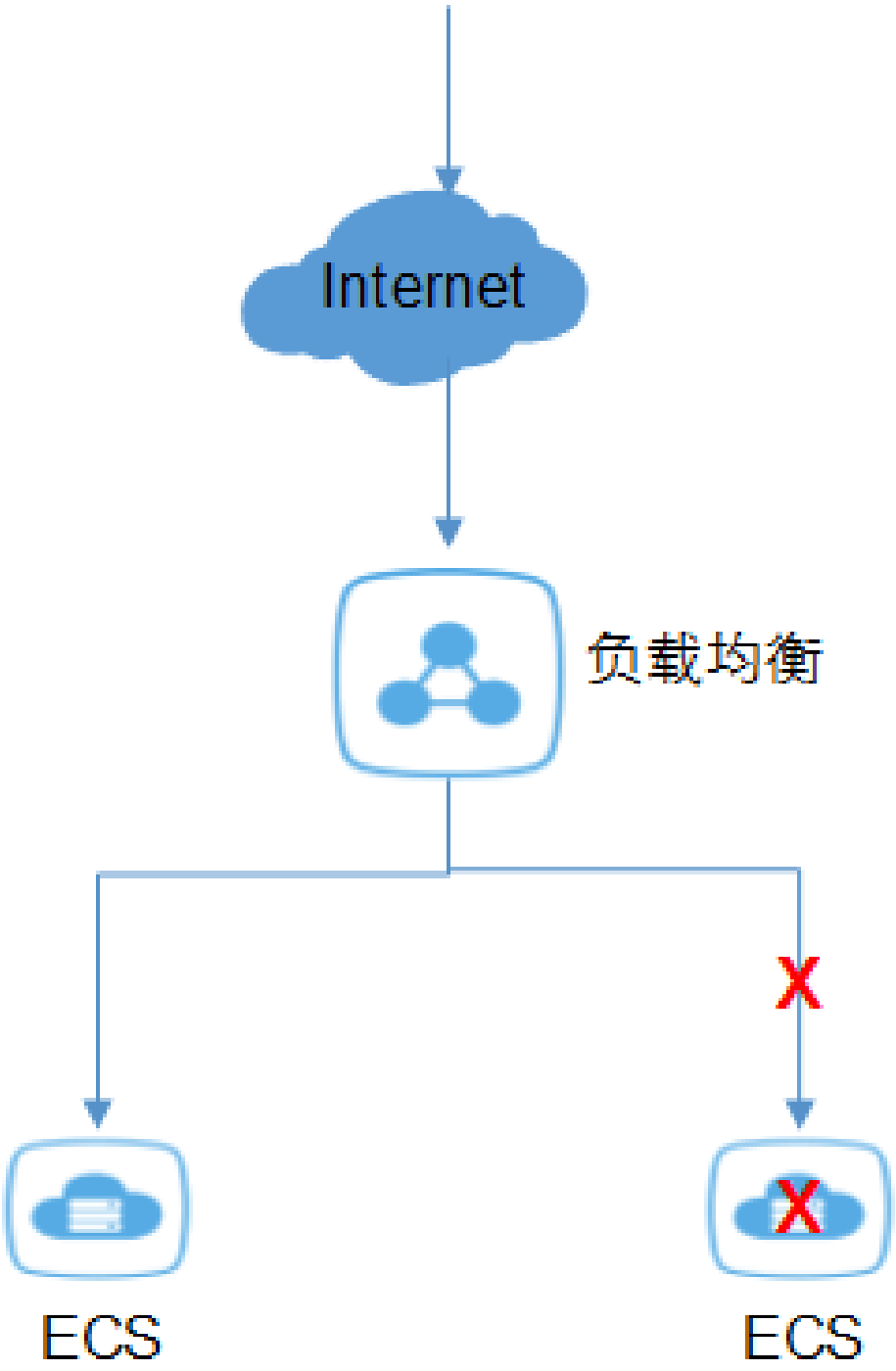
- 灵活的进行流量分发，适用于具有高访问量的业务。



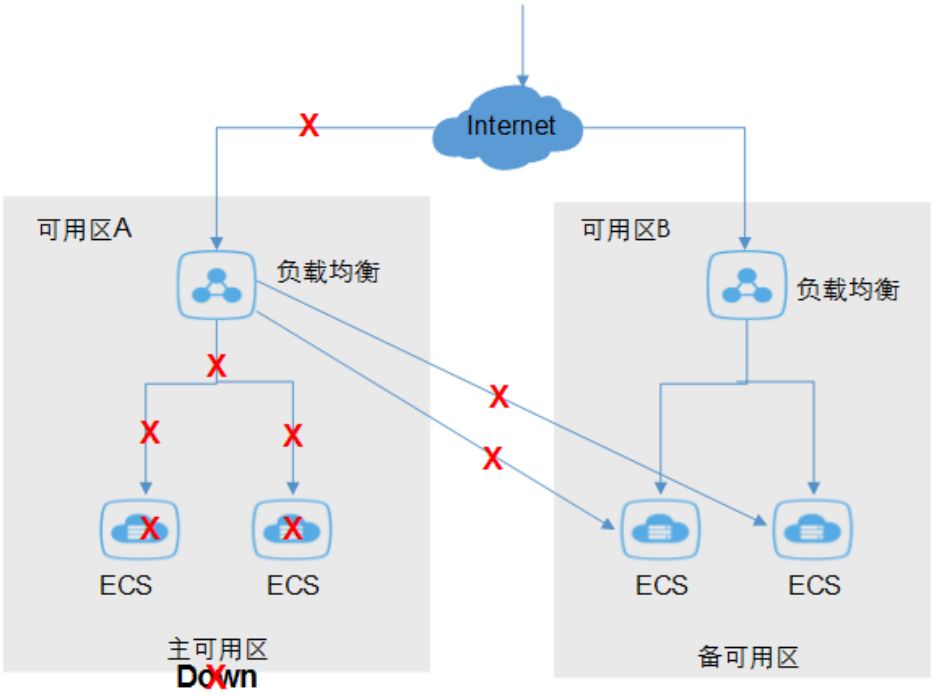
- 横向扩展应用系统的服务能力，适用于各种web server和app server。



- 消除应用系统的单点故障，当其中一部分ECS宕机后，应用系统仍能正常工作。

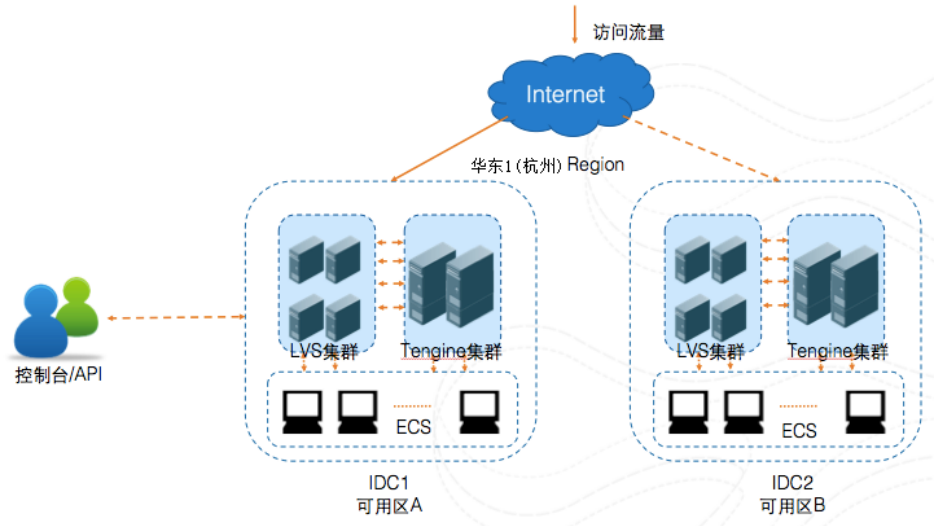


- 提高应用系统容灾能力，多可用区部署，机房宕机后，仍能正常工作。



- 防止应用系统遭受攻击，适用于经常受到WAF和CC困扰的业务。

基础架构



如上图所示，为负载均衡服务的基础架构图，其详细解释如下：

- 当前提供4层和7层上的负载均衡服务。
- 4层采用开源软件LVS + keeplived实现负载均衡。
- 7层采用Tengine实现负载均衡，Tengine是由淘宝网发起的web服务器项目，它在Nginx的基础上，针对大访问量网站的需求，添加了很多高级功能和特性。
- 负载均衡采用集群部署，可实现会话同步，以消除服务器单点，提升冗余，保证服务稳定。
- 在某些region部署两个机房，以实现同城容灾。