

# 阿里云 专有云企业版 负载均衡

产品简介

产品版本：V3.12.0

文档版本：20200622

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

# 目录

---

法律声明.....	I
通用约定.....	I
1 什么是负载均衡.....	1
2 产品高可用.....	3
3 产品架构.....	6
4 功能特性.....	10
5 应用场景.....	12
6 使用限制.....	15
7 基本概念.....	16

# 1 什么是负载均衡

负载均衡（Server Load Balancer）是将访问流量根据转发策略分发到后端多台云服务器（ECS实例）的流量分发控制服务。负载均衡扩展了应用的服务能力，增强了应用的可用性。

## 概述

负载均衡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和高可用的后端服务池，并根据转发规则，将来自客户端的请求分发给后端服务器池中的ECS实例。

负载均衡默认检查云服务器池中的ECS实例的健康状态，自动隔离异常状态的ECS实例，消除了单台ECS实例的单点故障，提高了应用的整体服务能力。

## 组成部分

负载均衡由以下三个部分组成：

- 负载均衡实例（Server Load Balancer instances）

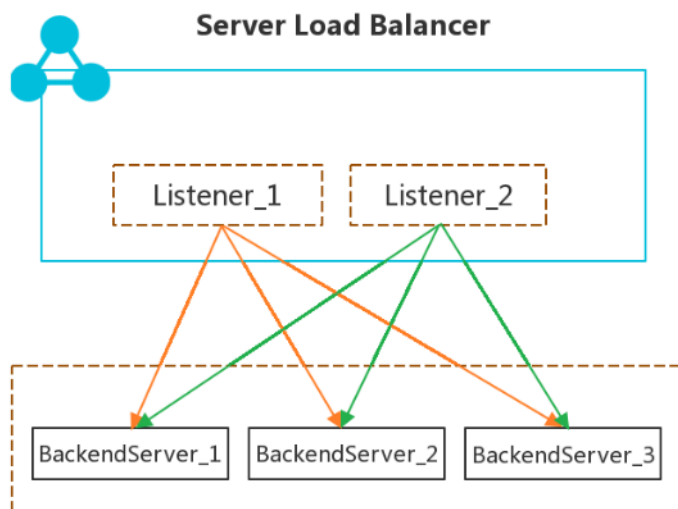
一个负载均衡实例是一个运行的负载均衡服务，用来接收流量并将其分配给后端服务器。要使用负载均衡服务，您必须创建一个负载均衡实例，并至少添加一个监听和两台ECS实例。

- 监听（Listeners）

监听用来检查客户端请求并将请求转发给后端服务器。监听也会对后端服务器进行健康检查。

- 后端服务器（Backend Servers）

一组接收前端请求的ECS实例。您可以单独添加ECS实例到后端服务器池，也可以通过虚拟服务器组或主备服务器组来批量添加和管理。



## 产品优势

- 高可用

采用全冗余设计，无单点，支持同城容灾。搭配DNS可实现跨地域容灾，可用性高达99.95%。

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。

- 可扩展

您可以根据业务的需要，随时增加或减少后端服务器的数量，扩展应用的服务能力。

- 低成本

与传统硬件负载均衡系统高投入相比，成本可下降60%。

- 安全

结合云盾，可提供5Gbps的防DDoS攻击能力。

- 高并发

集群支持亿级并发连接，单实例提供千万级并发能力。

## 2 产品高可用

负载均衡高可用是从系统设计、产品配置等多个方面提供了可用性保障。此外，您可以根据业务需求，配合使用云解析DNS等产品实现跨地域容灾。多可用区高可用指标设计为99.99%，单可用区设计为99.90%。

### SLB系统的高可用

负载均衡实例采用集群部署，可实现会话同步，以消除服务器单点故障，提升冗余，保证服务的稳定性。其中四层负载均衡通过LVS（Linux Virtual Server）+ keepalived的方式实现，七层负载均衡通过Tengine（淘宝网发起的Web服务器项目，在Nginx的基础上，针对有大访问量的网站需求进行了优化）实现。

来自公网的请求通过等价多路径路由（ECMP）到达LVS集群，LVS集群内的每台LVS通过组播报文将会话同步到该集群内的其它LVS机器上，从而实现LVS集群内各台机器间的会话同步。同时，LVS集群会对Tengine集群进行健康检查，将异常机器从Tengine集群移除，保证七层负载均衡的可用性。

最佳实践：

会话同步可以保证长连接不受集群内服务器故障的影响，但是对于短连接或连接未触发会话同步规则时（未完成三次握手），集群内的服务器故障仍可能会影响用户请求。为了防止集群中某台机器故障导致的会话中断，您可以在业务逻辑中加入重试机制，降低对用户访问造成的影响。

### 单SLB实例的高可用

为了向广大用户提供更稳定可靠的负载均衡服务，阿里云负载均衡已在大部分地域部署了多可用区以实现同地域下的跨机房容灾。当主可用区出现故障或不可用时，负载均衡有能力在非常短的时间内（约30秒）切换到备可用区并恢复服务；当主可用区恢复时，负载均衡同样会自动切换到主可用区提供服务。



#### 说明：

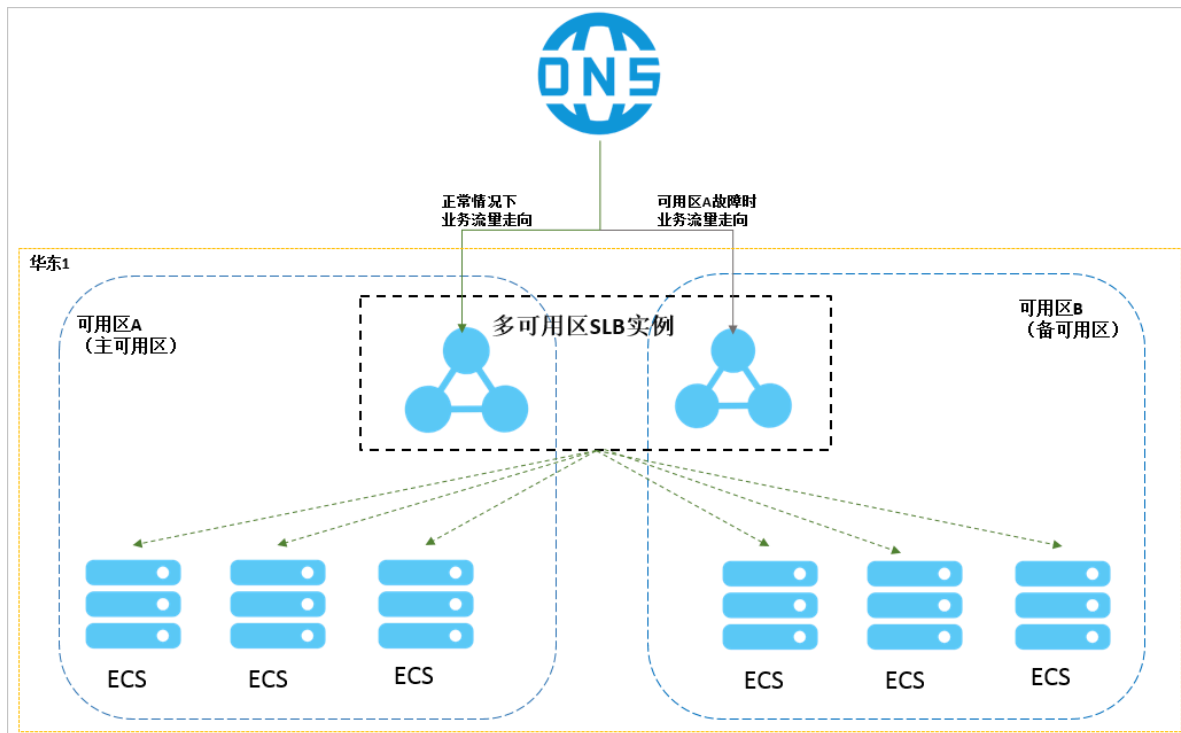
负载均衡的主备可用区是可用区级别的容灾。只有当主可用区整体不可用时，如机房整体断电或者机房出口光缆中断等，负载均衡才会切换到备可用区。而并非某个实例出现故障，就切换到备可用区。

最佳实践：

1. 为了更好的利用负载均衡的主备可用区机制，建议您在支持主备可用区的地域创建负载均衡实例，即在购买负载均衡实例时选择可用区类型为多可用区的地域。

2. 当您选择SLB的主备可用区时，可以根据ECS实例的可用区分布进行选择。大部分ECS实例位于哪个可用区，就将哪个可用区选择为SLB的主可用区，以获取最小的访问延迟。

但是并不建议您将全部ECS实例都部署在一个可用区内，您也需要在SLB的备可用区部署少量ECS实例，以便在极端情况下（主可用区整体不可用时），切换到备可用区后仍旧可以正常处理负载均衡转发的请求。



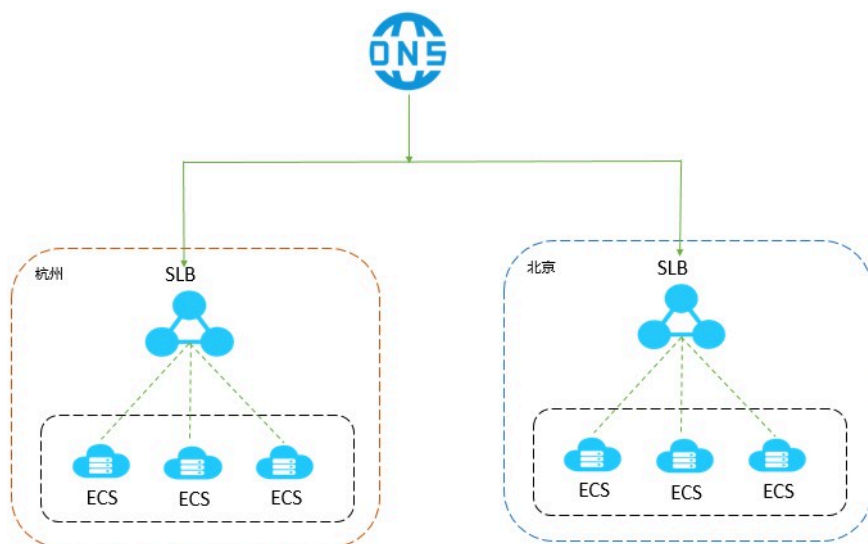
### 多SLB实例的高可用

如果您对可用性的要求特别高，负载均衡实例自身的可用性保障机制可能无法满足您的需求。例如当网络攻击或配置错误等情况导致负载均衡实例不可用时，由于未出现可用区级故障，不会触发负载均衡实例的可用区切换。此时，您可以创建多个SLB实例，通过云解析DNS对访问进行调度，或通过全球负载均衡解决方案实现跨地域容灾备份。

最佳实践：

您可以在一个地域内的多个可用区或多个地域内部署负载均衡实例和后端ECS实例，然后使用云解析DNS对访问进行调度。





### 后端ECS实例的高可用

负载均衡通过健康检查来判断后端ECS实例的可用性。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，当后端某个ECS实例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他健康检查正常的ECS实例上，而当该ECS实例恢复正常运行时，负载均衡会将其自动恢复到负载均衡服务中。关于健康检查的详细机制，请参见用户指南中的健康检查概述。

最佳实践：

为了使健康检查功能正常运作，您需要开启并正确配置健康检查。具体的操作流程请参见用户指南中的配置健康检查。

## 3 产品架构

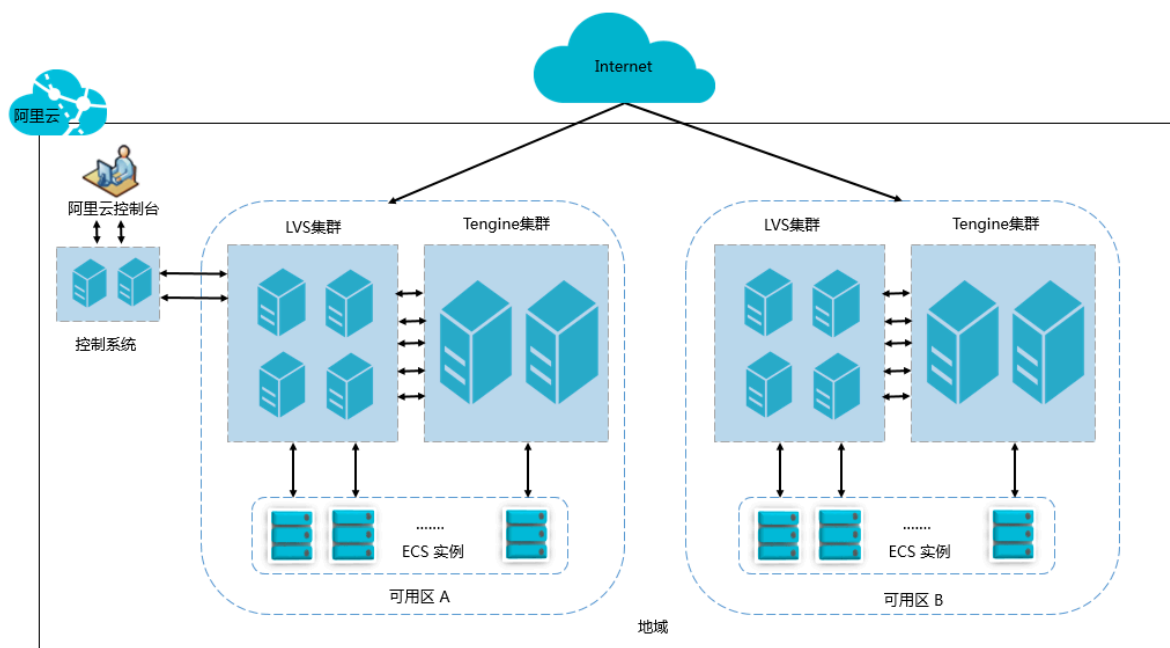
负载均衡基础架构是采用集群部署，提供四层（TCP协议和UDP协议）和七层（HTTP和HTTPS协议）的负载均衡，可实现会话同步，以消除服务器单点故障，提升冗余，保证服务的稳定性。

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。

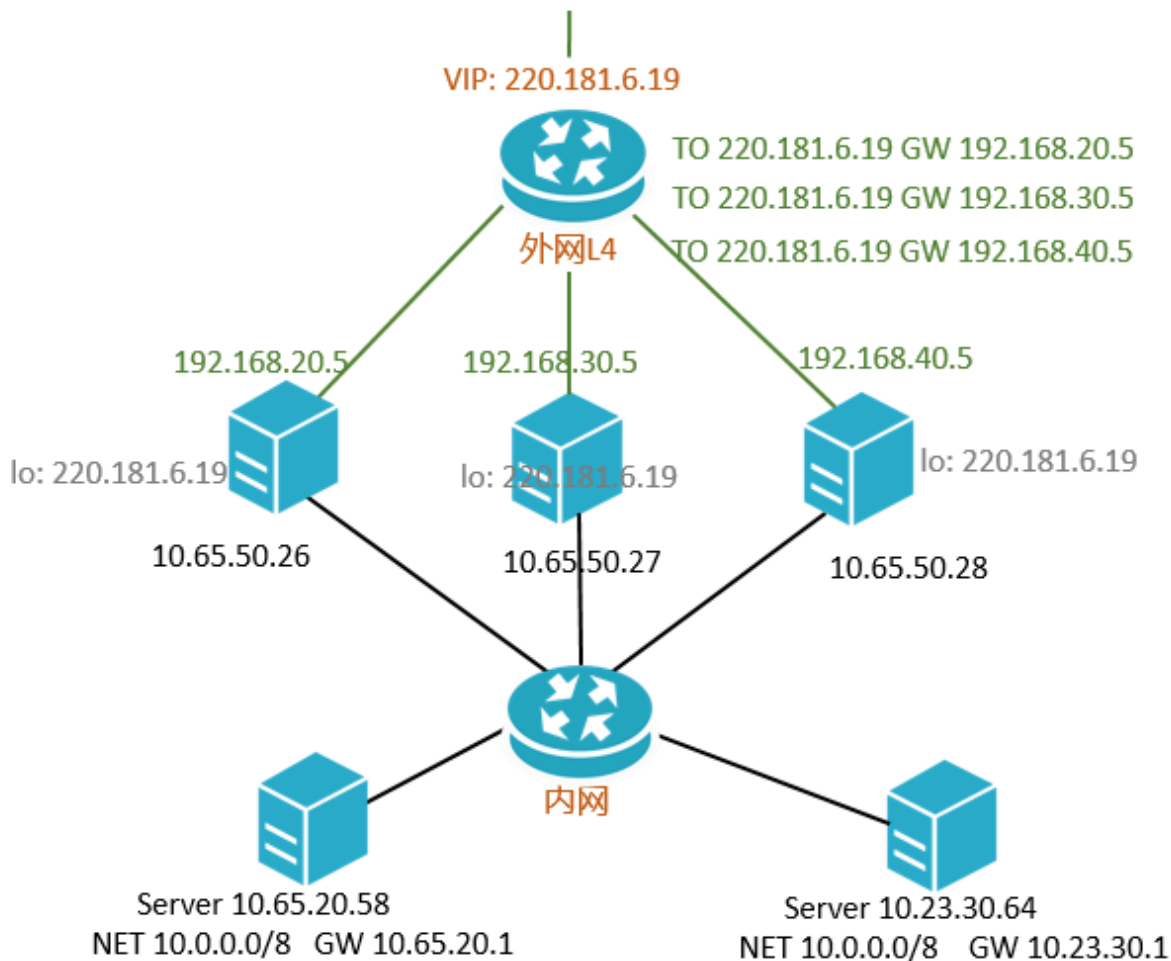
### 基础架构说明

阿里云当前提供四层和七层的负载均衡服务。

- 四层采用开源软件LVS（Linux Virtual Server）+ keepalived的方式实现负载均衡，并根据云计算需求对其进行了个性化定制。
- 七层采用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，针对有大访问量的网站需求，添加了很多高级功能和特性。



如下图所示，各个地域的四层负载均衡实际上是由多台LVS机器部署成一个LVS集群来运行的。采用集群部署模式极大地保证了异常情况下负载均衡服务的可用性、稳定性与可扩展性。

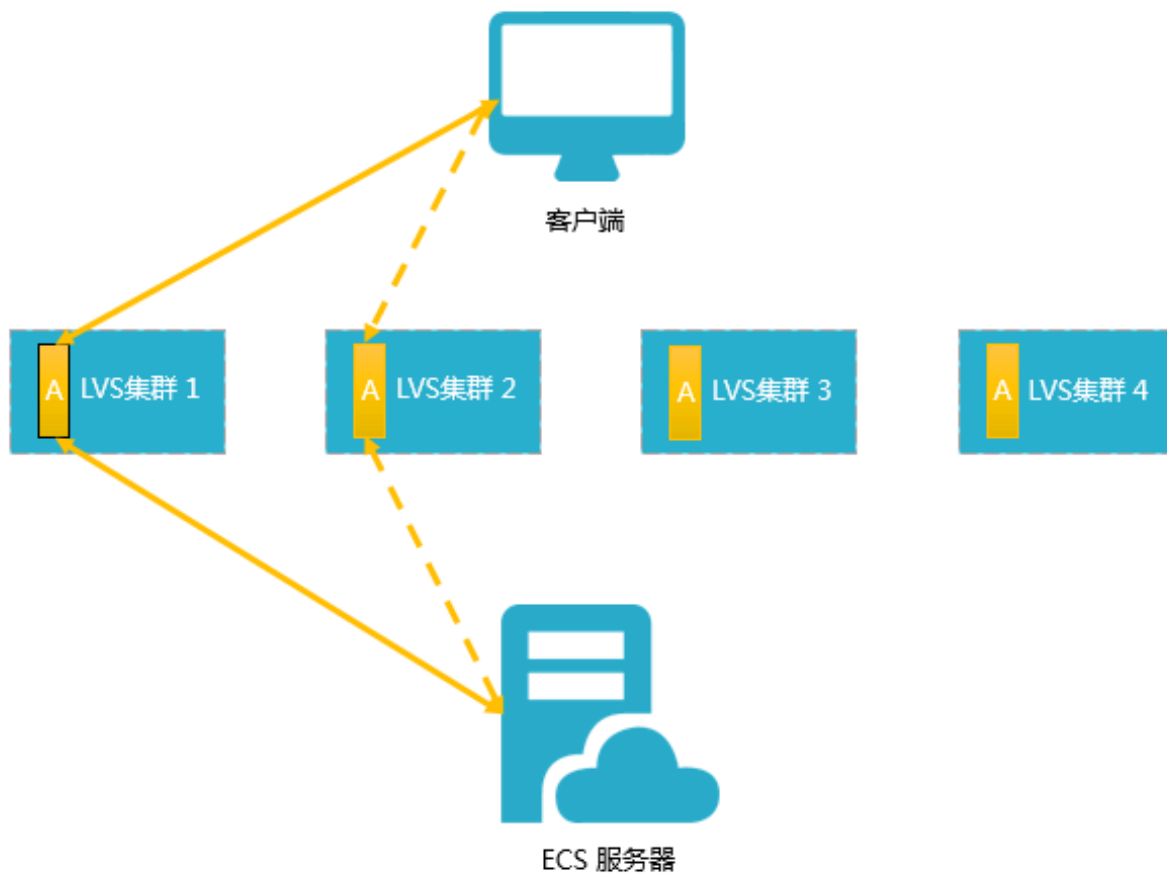


LVS集群内的每台LVS都会进行会话，通过组播报文同步到该集群内的其它LVS机器上，从而实现LVS集群内各台机器间的会话同步。如下图所示，当客户端向服务端传输三个数据包后，在LVS1上建立的会话A开始同步到其它LVS机器上。图中实线表示现有的连接，图中虚线表示当LVS1出现故障或进行维护时，这部分流量会走到一台可以正常运行的机器LVS2上。因而负载均衡集群支持热升级，并且在机器故障和集群维护时最大程度对用户透明，不影响用户业务。



**说明：**

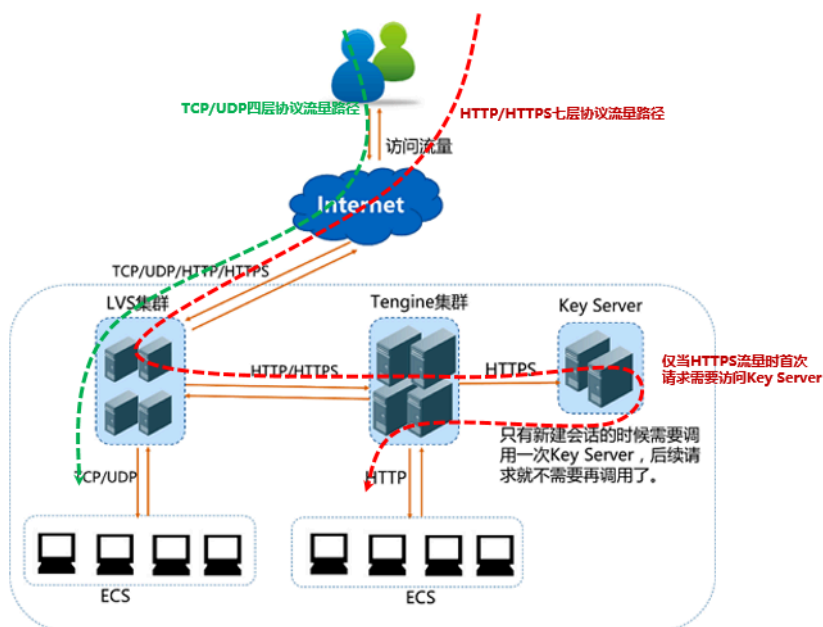
对于连接未建立（三次握手未完成），或者已建立连接但未触发会话同步机制，热升级不保证连接不中断，需要依靠客户端重新发起连接。



## 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，数据流转如下图所示。

图 3-1: 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。

## 4 功能特性

本章节介绍阿里云负载均衡提供的功能和功能概述，负载均衡支持四层和七层负载均衡，并提供健康检查、会话保持和域名转发等功能，保证后端服务的高可用。

功能	四层负载均衡	七层负载均衡
<p>调度算法</p> <p>负载均衡支持轮询（RR）、加权轮询（WRR）和加权最小连接数（WLC）调度算法。</p>	Y	Y
<p>健康检查</p> <p>负载均衡会检查后端服务器的运行状况。当探测到后端服务器运行状况不佳时，会停止向其发送流量，然后将流量转发给其他正常运行的后端服务器。</p>	Y	Y
<p>会话保持</p> <p>负载均衡提供会话保持功能。在会话的生命周期内，可以将同一客户端的请求转发到同一台后端服务器上。</p>	Y	Y
<p>访问控制</p> <p>负载均衡支持添加白名单，灵活控制客户端访问。</p>	Y	Y
<p>高可用</p> <p>负载均衡可以将流量转发给多个可用区的后端服务器。并且，负载均衡已经在大部分地域支持了多可用区部署，当主可用区出现故障时，负载均衡可自动切换到备可用区上提供服务。</p>	Y	Y
<p>安全防护</p> <p>结合云盾，可提供5Gbps的防DDoS攻击能力。</p>	Y	Y
<p>网络类型支持</p> <p>负载均衡提供公网和私网类型的负载均衡服务。您可以创建一个私网类型的负载均衡实例来均衡专有网络内的流量，或创建一个公网负载均衡实例来均衡来自公网的流量。</p>	Y	Y

功能	四层负载均衡	七层负载均衡
IPv6地址支持 公网负载均衡支持转发来自IPv6客户端的请求。	Y	Y
证书管理 针对HTTPS协议，提供统一的证书管理服务。证书无需上传到后端服务器，解密处理在负载均衡上进行，降低后端服务器的CPU开销。	N	Y
WS/WSS支持 WebSocket是HTML5一种新的协议，在客户端与服务器间提供双向通信渠道，能更好地节省服务器资源和带宽，并达到实时通讯。	N	Y
HTTP/2支持 HTTP/2 (Hypertext Transfer Protocol Version 2) 是超文本传输协议的第二版，向下兼容HTTP1.X协议版本，同时大幅提升性能。	N	Y

## 5 应用场景

---

负载均衡的应用场景为高访问量的业务，提高应用程序的可用性和可靠性。

### 应用于高访问量的业务

如果您的应用访问量很高，您可以通过配置监听规则将流量分发到不同的ECS实例上。此外，您可以使用会话保持功能将同一客户端的请求转发到同一台后端ECS，提高访问效率。

### 扩展应用程序

您可以根据业务发展的需要，随时添加和移除ECS实例来扩展应用系统的服务能力，适用于各种Web服务器和App服务器。

### 消除单点故障

您可以在负载均衡实例下添加多台ECS实例。当其中一部分ECS实例发生故障后，负载均衡会自动屏蔽故障的ECS实例，将请求分发给正常运行的ECS实例，保证应用系统仍能正常工作。

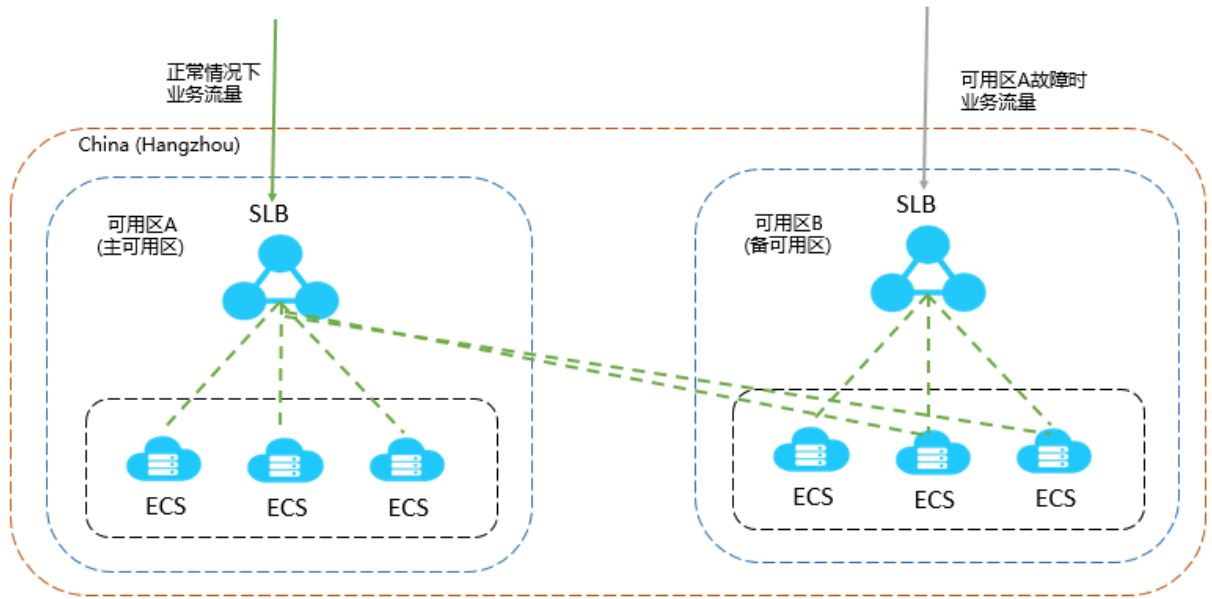
### 同城容灾（多可用区容灾）

为了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部署了多可用区以实现同城容灾。当主可用区出现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（大约30s中断）切换到另外一个备可用区恢复服务能力；当主可用区恢复时，负载均衡同样会自动切换到主可用区提供服务。

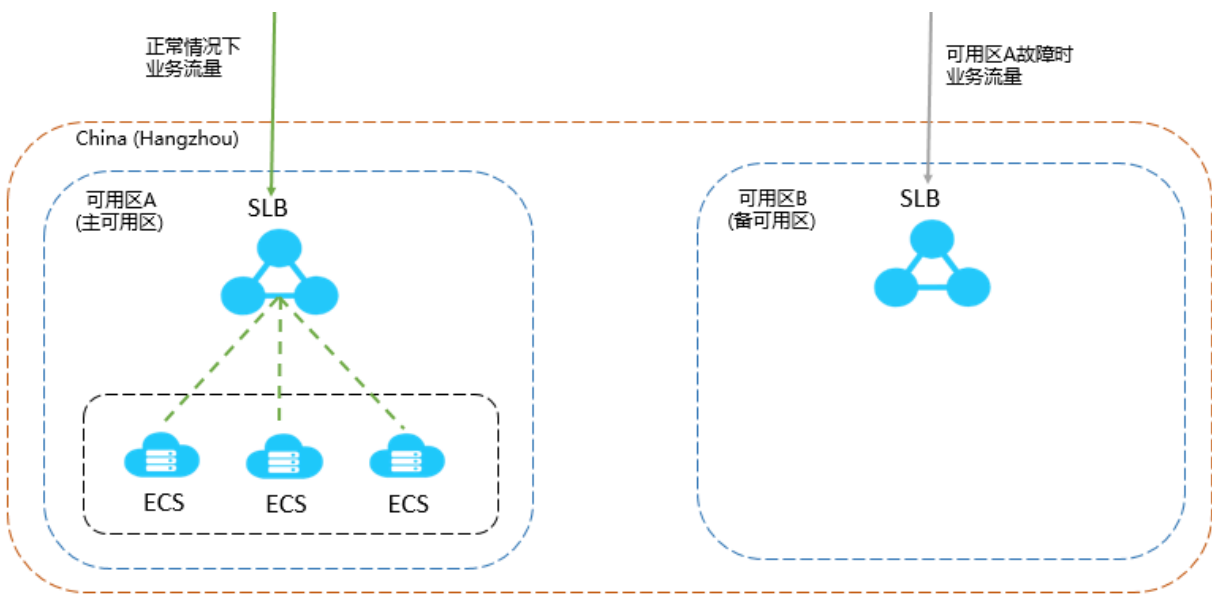
使用负载均衡时，您可以将负载均衡实例部署在支持多可用区的地域以实现同城容灾。此外，建议您结合自身的应用需要，综合考虑后端服务器的部署。如果您的每个可用区均至少添加了一台ECS实例，那么此种部署模式下的负载均衡服务的效率是最高的。

如下图所示，在负载均衡实例下绑定不同可用区的ECS实例。正常情况下，用户访问流量将同时转发至主、备可用区内的ECS实例；当可用区A发生故障时，用户访问流量将只转发至备可用区内的ECS实例。此种部署既可以避免因为单个可用区的故障而导致对外服务的不可用，也可以通过不同产品间可用区的选择来降低延迟。



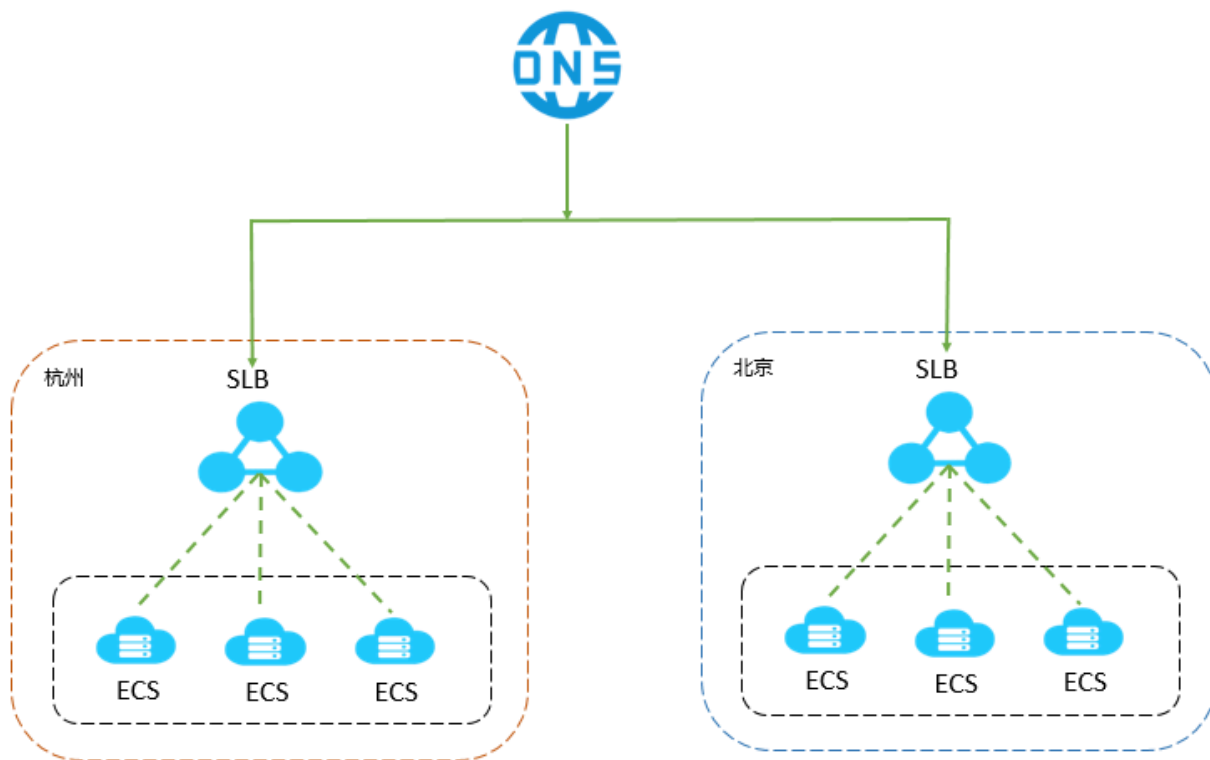


如果您采取如下图所示的部署方案，即在负载均衡实例的主可用区下绑定多台ECS实例，而在备可用区没有任何ECS实例。当主可用区发生故障时会造成业务中断，因为备可用区没有ECS实例来接收请求。这样的部署方式很明显是以牺牲高可用性为代价来获取低延时。



## 跨地域容灾

您可以在不同地域下部署负载均衡实例，并分别挂载相应地域内不同可用区的ECS。上层利用云解析做智能DNS，将域名解析到不同地域的负载均衡实例服务地址下，可实现全局负载均衡。当某个地域出现不可用时，暂停对应解析即可实现所有用户访问不受影响。



## 6 使用限制

---

本章节介绍负载均衡资源使用的配额限制。

资源	默认限制
SLB实例限制	
一个SLB实例可添加的监听数量	500
证书限制	
每个地域可上传的服务器证书数量	1000
每个地域可上传的客户端CA证书数量	1000

## 7 基本概念

本章节介绍阿里云负载均衡服务使用过程中遇到的常用名词的基本概念和简要描述。

名词	说明
负载均衡服务	阿里云计算提供的一种网络负载均衡服务，结合阿里云提供的ECS服务，提供四层和七层负载均衡服务。
负载均衡实例	负载均衡实例是一个运行的负载均衡服务。要使用负载均衡服务，必须先创建一个负载均衡实例。
服务地址	系统为创建的负载均衡实例分配的服务IP地址。根据创建的负载均衡实例的类型，服务地址可能是公网IP也可能是私网IP。您可以将域名解析到公网IP地址提供对外服务。
监听	负载均衡服务监听规定了如何将请求转发给后端服务器。一个负载均衡实例至少添加一个监听。
后端服务器	处理负载均衡分发的前端请求的ECS实例。
默认服务器组	一组处理负载均衡分发的前端请求的ECS实例。 如果监听未配置指定的虚拟服务器组或主备服务器组，则将流量转发给默认服务器组中的后端服务器。
虚拟服务器组	一组处理负载均衡分发的前端请求的ECS实例。 不同的监听可以关联不同的虚拟服务器组，实现监听维度的请求转发。
主备服务器组	一个主备服务器组只包含两台ECS实例，一台作为主服务器，一台作为备服务器。当主服务器健康检查失败，系统会直接将流量切到备服务器。