

用户指南

为了无法计算的价值 | [] 阿里云

用户指南

负载均衡实例

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。要使用负载均衡服务,您必须创建一个负载均衡实例,然后在 实例中添加监听和后端服务器。详情参考创建负载均衡实例。



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来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对负载均衡的私网具有访问权限的 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。



性能保障型实例

什么是性能保障型实例

性能保障型实例提供了可保障的性能指标(性能SLA)。与之相对的是性能共享型实例,即不保障实例的性能

指标,资源是所有实例共享的。

在阿里云负载均衡推出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绿色图标,可查看具体的性能指标,如下图所示。

| □ 负载均衡ID/名称 | 可用区 | 服务地址(全部) 👻 | 状态 | 网络类型(全部) 🔻 | 端口/健康检查 | 后端服务器 | 实例规格 | 带宽计费方式(全部) 🔻 | 付费方式(全部) ▼ | 操作 |
|--------------------------------------|--------------------------------|---------------|-------|------------|---------|-----------|------------------------|-------------------------------------|--------------------------------|--------|
| □ <mark>Ib-bp1irlw0i</mark> (未设置) | 华东 1 可用区 F(主) 华东 1 可用区 E(备) | 120.55 公网 | ❷ 运行中 | 经典网络 | 未配置(配置) | 未配置(配置) | 性能共享型 | 按固定带宽 | 包年包月 2017-09-08 00:00:00 到期 | 管理 更多、 |
| □ <mark>Ib-wz9nznspn</mark> (未设置) | 华南 1 可用区 A(主) 华南 1 可用区 B(备) | 120.78. 公网 | ❷ 运行中 | 经典网络 | 未配置(配置) | 未配置(配置) ѕ | 生能保障型 lb.s1.small 🕖 | 连接数: 5000 CPS: 3000 QPS: 1000 | 按量付费 2017-08-07 21:48:36 创建 | 管理 更多、 |

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提供了如下六种实例规格。

| 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) | 5000 | 3000 | 1000 | | |
| 规格 2 | 标准型I (slb.s2.small) | 50000 | 5000 | 5000 | | |
| 规格 3 | 标准型II (slb.s2.medium) | 100000 | 10000 | 10000 | | |
| 规格 4 | 高阶型I (slb.s3.small) | 200000 | 20000 | 20000 | | |
| 规格 5 | 高阶型II (slb.s3.medium) | 500000 | 50000 | 30000 | | |
| 规格 6 | 超强型I (slb.s3.large) | 1000000 | 100000 | 50000 | | |

性能保障型实例的变配操作限制

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目前暂时只允许升配,不 允许降配。

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。

另外,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。

注意: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,因此建议在业务低谷期进行此类变配,或通过 GSLB来做实例间的负载均衡后,再进行变配。



性能保障型实例的定价

性能保障型实例根据不同规格收取规格费,如下表所示。阿里云负载均衡提供了一种免费的规格,可满足以前 绝大部分共享型实例用户的需求。

注意: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配置费用和流量费保持不变。更 多详细信息,参考**计费说明**。

| 抑格 | | 最大连 | 每秒新 | 每秒查 | 包年包月 | 按量付 费 | |
|---------|----------------------------------|-------------|----------------|-------------|--------------|---------------|--------------|
| 7901127 | | 接数 | 建建安 数 (CPS) | 问致 (QPS) | 月价(元 /月) | 年价(元 /年) | 小时价 (元/时) |
| 规格 1 | 简约型I (slb.s1.s mall) | 5000 | 3000 | 1000 | 免费 | 免费 | 免费 |
| 规格 2 | 标准型I (slb.s2.s mall) | 50000 | 5000 | 5000 | 190.00 | 1,938.0 0 | 0.32 |
| 规格 3 | 标准型II (slb.s2. mediu m) | 100000 | 10000 | 10000 | 380.00 | 3,876.0 0 | 0.63 |
| 规格 4 | 高阶型I (slb.s3.s mall) | 200000 | 20000 | 20000 | 760.00 | 7,752.0 0 | 1.27 |
| 规格 5 | 高阶型II (slb.s3. mediu m) | 500000 | 50000 | 30000 | 1,143.0 0 | 11,658. 60 | 1.91 |
| 规格 6 | 超强型I (slb.s3.l arge) | 100000 0 | 100000 | 50000 | 1,908.0 0 | 19,461. 60 | 3.18 |

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

登录负载均衡管理控制台。

在**实例管理**页面,单击右上角的**创建负载均衡**。

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。

| | 根据如 | 下信息, | 配置负 | 1载均衡实例。 |
|--|-----|------|-----|---------|
|--|-----|------|-----|---------|

| 配置 | | 说明 |
|------|-------|--|
| | 地域 | 选择负载均衡实例的所属地域。 注意: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。 |
| 基本配置 | 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?。 |
| 网络与实例类型 | 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,参考实例与 网络类型。 - 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。 |
| | 计资力式 | 远挥 ^一 种订货力式。 |
| 购买量 | 购买数量 | 选择购买数量。 |

单击**立即购买**。

在**确认订单**页面,核对配置信息,单击**去开通**完成创建。

管理负载均衡实例

在 实例管理页面,选择负载均衡实例的所属地域,您可以查看该地域的所有负载均衡实例。此外,您还可以:

修改负载均衡实例名称

将光标移至负载均衡ID区域,单击出现的铅笔图标,输入实例名称。

暂停负载均衡实例

勾选负载均衡实例,单击页面下方的停止,或单击更多>停止。

启动暂停的负载均衡实例

勾选已经停止运行的负载均衡实例,单击页面下方的启动,或单击更多>启动。

释放负载均衡实例

勾选负载均衡实例,单击页面下方的**释放设置**,或单击 更多>释放。在释放设置对话框,选择立即释放或在某个特定时刻释放实例。

设置标签

您可以通过标签实例进行分类和统一管理。详情参考管理标签。

变更计费

预付费模式下,您可以变更购买实例的带宽规格,但只支持升级带宽,不支持降低带宽:单击**更多>变更带宽规格**。

后付费模式下,您可以在按使用流量和按公网带宽两种计费方式间切换,单击**更多>变更计** 费方式。

更多详细信息,参考变配流程。

查看负载均衡实例详情

单击负载均衡实例的ID链接或管理,查看负载均衡实例详情。

在详情页面,您可以单击消费明细,查看负载均衡服务的费用明细。

| < | acs-slb-ce043bbfe4 • wEconomia | 金田間報約回主要事項 |
|-------------------|---------------------------------|----------------------------|
| 洋情 | 基本信用 | ^ |
| • 82m38 | 均能均能IID: Ib-bpllefbcdeksgtrAmai | 秋志: ② 遠行中 |
| 5282A.M | 负期均衡系称: acssb.col/43bbfe4 | 地域: 編集1 |
| -excision million | 地址理题: 公開 | 可用区: 傘体1町用区町(主)/傘体1町用区D(番) |
| 主要服务器组 | 网络洪型: 经典网络 | |
| <u>200</u> | 付费值息 | 演奏现任 算法定款 个 |
| | 付跟方式: 接触用高量 | 创题时间: 2017-04-13 13:47:35 |
| | | 自动用估时间: 无 |

单击监听,查看或添加负载均衡监听。详情参考监听介绍。

单击服务器,查看或添加后端服务器。详情参考后端服务器概述。

单击监控,查看监控信息,设置报警机制。详情参考设置报警规则。

后付费实例变配

您可以更改后付费实例的带宽、实例规格和计费方式。

完成以下操作,更改后付费实例的配置:

登录负载均衡管理控制台。

选择目标实例的所属地域。

找到目标实例,然后单击更多>变更配置。

| 关于负载地 阿里云负载 续保持规格 | 的衝收费的; 均衡国内: 8免费,后线 | 说明: 5大区域组 续收费计 | 2面开启性; 划将通过首 | 能保障型实例 (网公告、短(|),目前用户 信、邮件方: | 可以在北京 式进行通知 | ā、杭州、洌 ,关于性能 | 梁圳、上海、青岛5大 保障型实例如何使用i | 地域通过 青 查看诗 | 控制台购买性能 情 | 保障型实例(API智 | 未开放)同时能 | 建续保留共享型实 | 例售卖, | 现计划延长 | 公測期, | , 继 |
|--------------------------------|---------------------------|-----------------------|--------------------------------|--------------------------------|--|-------------------------|---|-----------------------------------|---------------|------------------------------|------------------|------------------------|------------------|----------------------|-------------------------|------|--------|
| (実例管理) (気動均衡名) | 华北 1 美国东音 称 | 华北 2 ß 1 (弗吉 请编 | 华北 3 尼亚) 美 认实例名称 | 华北 5 4 画西部 1 (时 | (株1 年年) (株1) (株2) (株3) (4) (4)<!--</th--><th>₹ 2 华南 东部 1 (油 分隔</th><th>1 香港 () 欧洲 () 酸 () () 酸 () () 酸 () () () () () () () () () () () () () (</th><th>亚太东北 1 (东京) 中部 1 (法兰克福) ●标签</th><th>亚太东</th><th>南 1 (新加坡)</th><th>亚太东南 2 (悉尼)</th><th>亚太东南3(</th><th>(吉隆坡)</th><th>C.6</th><th>lish di</th><th>建负载出</th><th>资 章</th> | ₹ 2 华南 东部 1 (油 分隔 | 1 香港 () 欧洲 () 酸 () () 酸 () () 酸 () () () () () () () () () () () () () (| 亚太东北 1 (东京) 中部 1 (法兰克福) ●标签 | 亚太东 | 南 1 (新加坡) | 亚太东南 2 (悉尼) | 亚太东南3(| (吉隆坡) | C.6 | lish di | 建负载出 | 资 章 |
| □ 负载均衡 | iID/名称 | P | 用区 | 服务地 | 址(全部) ▾ | 状态 | 网络类型 部) ▼ | (全 第口/健康检查 | | 后端服务器 | 标签 | 实例规格 | 带宽计费方式 (全部) ▼ | 付费方 | 元(全部) 🗸 | | 操作 |
| ■ ^{lb-bp1wi} (未设置) | z7h8w | 华 F(: 华 E(: | 东1可用四 主) 东1可用四 街) | <u>×</u> 120 <u>×</u> 阿) | 5(公 | ●运行 中 | 经典网络 | 未配置(配置) | | 未配置(配置) | 未绑定 | 性能保障型 slb.s2.small(| 0 按固定带宽 | 按量的 2017- 19:4 | 摟 11-30 启动 | 管理 | 更多, |
| acs-slb-c | ekef 4e1afcd9e | 华 F(i 华 E(i | 东 1 可用2 主) 东 1 可用2 备) | <u>₹</u> 118 <u>₹</u> 阿) | ,29(公 | ⊘ 运行 中 | 经典网络 | TCP: 80 | 正常 | c4e1afcd9efe c4e1afcd9efe | 2547 2547 未绑定 | 性能共享型 | 按使用流量 | 按量 2017 15:3 | 停止 释放 编辑标签 | | |
| | | 丝 | 东1可用网 | र | | | | | | ca5ce0cca9d | a346 | | | | 变更配置 | | |

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。

说明: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。

| 配 | 置变更 | Ē | |
|--|---------|--------|--|
| | | | |
| | | 实例规格 | 标准型 (slb.s2.small) ★ 法接数: 50000,新能连接数 (CPS): 5000,每秒查询数 (QPS): 5000 性能保障理实例公测期间,免收性能规格费,正式收费后,该规格费用为:¥0.32/小时详情点击>> |
| | | 实例类型 | 公网 实际类型详解 > ⑦ |
| 100 4 4 10 10 10 10 10 10 10 10 10 10 10 10 10 | 网络与实例类型 | 计费方式 | 按使用流量计费 按固定带宽计费 开通后即开始按固定带宽计费,和实例状态及使用流量无关 进行变面操作时,若选择的计费方式与当前计费方式不同,则代表变更计费方式,变更计费方式将在第二天0点生效 进行变面操作时,若选择的计费方式与当前计费方式相同,则代表变更带宽规格,变更带宽规格即时生效 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>> |
| | | 带宽值 | 11 1250Mbps 2500Mbps 5000Mbps 9 Mbps 开通后即开始按固定带宽计费,和实例状态及使用流量无关 |
| | | 服务监听设置 | 每个服务监听都需要设置带宽峰值限制,并且只能为大于0的整数,总和不能大于带宽值。 |

包年包月实例变配

您可以升高或降低包年包月实例的带宽,也可以升高或降低其性能规格。

说明:您需要提交工单开通白名单后,方可使用降配功能。

完成以下操作,更改包年包月实例配置:

登录负载均衡管理控制台。

选择目标实例的所属地域。

找到目标实例,然后单击**更多>降配**或升配。

| (| lb-bp1x9u9oa HTTPS | • | 华东 1 可用区 E(主) 华东 1 可用区 D(晉) | 118. 网) | 34(公 🥑 运行 中 | 经典网络 | TCP : | 80 | 未配置(配置) | Proto netwo | 性能 共享 型 | 按固定带宽 | 包年包月 2017-06-11 (启动 | 管理 更多 |
|---|-----------------------|-----|--------------------------------------|------------|----------------|------|-------|----|---------|----------------|---------------|--------|--------------------------------------|-------|
| | 自动停 | 91E | 释放设置 | 编辑标签 | 共4个实例 | | | | | 共有4条 ,每页5 | 示:[| 10 🔻 🎊 | 停止 编辑标签 | |
| | | | | | | | | | | | | | 升配 | |
| | | | | | | | | | | | | | 障配 | |
| L | | | | | | | | | | | | | 续费 | |

在配置变更区域,选择新的带宽值或规格,完成支付。

| 配 | 置变 | 更 | |
|---|-----|--------|--|
| | | | |
| | | 实例规格 | 简约型 (slb.s1.small) ▼ |
| | 酬 | | 连接数: 5000 , 新建连接数 (CPS): 3000 , 每秒查询数 (QPS): 1000 性能保障型实例公测期间 , 免收性能规格费 , <mark>正式收费后 , 该规格费用为: ¥0.00/月 详情点击>></mark> |
| | 東回来 | 带宽值 | 1Mbps 2Mbps II 5Mbps 3 Mbps 🜩 |
| | 网络气 | | 开通后即开始按固定带宽计费,和实例状态及使用流量无关 |
| | | 服务监听设置 | 服务监听1: TCP:80 带宽峰值限制: ON 3 Mbps |
| | | | 每个服务监听都需要设置带宽峰值限制,并且只能为大于0的整数,总和不能大于带宽值。 |



标签概述

负载均衡提供标签管理功能,方便您通过对负载均衡实例添加标签进行负载均衡服务分类。 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:

目前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

登录负载均衡管理控制台。

在实例管理页面,选择地域,然后勾选需要添加同一标签的实例。

单击**编辑标签**。

| 实例管理 亚太东南1(和 | ftu坡) 欧洲中部 1 (法兰) | 电描》 \$4:北 1 美国东 | 部 1 (弗吉尼3 | ② 傘北 2 歩东 2 亚太 | 东北1(东唐) 华南1 | 香港 | 亚太东南 2 (悉尼) (美国西部 1 (| (建谷) 中东3 | 5郎1(迪拜) | 舉北3 郑东1 | ○ 刑新 | energy and the second s |
|------------------------------------|--------------------------------|-----------------|-----------|---------------------------------|------------------------|--------------|-----------------------|----------|---------|--------------|--------------------------------|--|
| 为航均街D • 词 | 1输入实例ID进行模糊查询。多 | 个统分隔 200 | • • • • | <u>K</u> | | | | | | | | <u>×</u> • |
| □ 负载均衡四/名称 | 可用区 | 服务地址(全部) マ | 状态 | 同塔英型(全部) - | 第日/健康检 | 查 | 后前服务器 | 标签 | 实例现格 | 带宽计费方式(全部) - | 付卖方式(全部) ▼ | 操作 |
| B-bp1mt9k1 acs-slb-cd77515676 | 华东 1 可用区 E(主) 华东 1 可用区 D(倍) | 101.37. 公网 | ● 运行中 | 经典网络 | TCP : 80 | 正常 | cd7751567697e4b | 未做定 | 性能共享型 | 按使用流量 | 按量付费 2017-06-05 13:52:07 创建 | 管理 更多~ |
| lb-bp1govd4b acs-slb-c4765cdf53 | 华东 1 可用区 E(主) 华东 1 可用区 D(倍) | 101.37. 公网 | ● 运行中 | 经典网络 | TCP: 80 | ĿЖ | c4765cdf537a945 | 未御定 | 性能共享型 | 按視用流量 | 按量付器 2017-06-05 11:48:53 创建 | 管理 更多+ |
| DneWayHTTPS | 华东 1 可用区 E(主) 华东 1 可用区 F(告) | 101.37. 公网 | ● 运行中 | 经典网络 | HTTPS : 443 | 3 E X | ubuntu2 ubuntu1 | 未御定 | 性能共享型 | 按使用流量 | 按量付購 2017-05-27 09:32:58 创建 | 管理 更多+ |
| HTTPS | 緣东 1 可用区 E(主) 綠东 1 可用区 D(告) | 118.178. 公网 | ● 遺行中 | 经典网络 | HTTPS : 443 | 3 E # | ubuntu2 ubuntu1 | 未御定 | 住能共享型 | 按固定考虑 | 包年包月 2017-06-11 00:00:00 到期 | 管理 更多w |
| Ib-bp1ub210u Intranet_VPC | 华东 1 可用区 E(主) 华东 1 可用区 D(册) | 10.0. 私用 | ● 运行中 | 专有网络 vpc-bp10d617s0m3onih7in | HTTP: 90 kf TCP: 80 | | 未配置(配置) | 未绑定 | 性能共享型 | 按使用流量 | 按量付器 2017-04-12 17:28:55 创建 | 管理 更多・ |
| Ib-bp113ltfv Intranet_classic | 华东 1 可用区 E(主) 华东 1 可用区 D(質) | 100.114.1 新期 | ● 运行中 | 经典网络 | HTTP: 80 | | 负载均衡测试1 负载均衡实例2 | 未供定 | 性能共享型 | 按使用流量 | 按量付费 2017-04-12 17:27:09 创建 | 管理 更多・ |
| 0 en #it | FEX:28 (#4853 | 共6个实例 | | | | | | | | | | |

在编辑标签窗口,单击新建标签,然后输入新建标签的标签键和值,单击确定。

标签搜索实例

登录负载均衡管理控制台。

在实例管理页面,选择地域,查看该地域的所有实例。

单击标签,然后选择要搜索的实例绑定的标签键和标签值。

符合您选择条件的实例会显示在实例列表。

| 实例管理 亚大东南 1 (新tok | 支) 欧洲中部1(法兰克福) | 华北1 美国东部 | 1 (売吉尼亞) 4 | 416.2 华东 | 2 亚太东北 1 (东京) | \$3第1 個 | (港 亞太东南 2 (悉尼) | 創創西部1(社谷) | 中东东部1(油料) | \$48比3 \$ \$ 9开1 | C Rist | 的建立成均衡 |
|----------------------------------|------------------------------|--------------|-----------------|--------------|---------------|---------|----------------|-------------------|---------------|-------------------------|--------------------------------|------------|
| (気能均衡D * 消症) | 、实例即进行植物查询,多个校, | .分隔 技法 | % सम्म । | Protocol:TCP | 0 | | | | | | | <u>×</u> • |
| ◎ 负载均衡D/名称 | 可用区 | 服务地址(全部) - | 标签键 | | 标签值 | -m | 后纳服务器 | 标签 | 实例现格 | 带您计最方式(全部) 👻 | 付職方式(全部) - | 操作 |
| Ib-bp1mt9k1 acs-sb-cd77515676 | 华东1 可用区 E(主) 徐东1 可用区 D(音) | 101.37 公网 | Protocol | ~) | нттря (тор | ER | cd77515676 | 97e4b Prot neb | 0 性能共享型 vo | 按使用流量 | 按量付票 2017-06-05 13:52:07 创建 | 繁理 更多・ |
| B-bp1govd4b acs-sb-c4765cdf53 | 幼东1可用区E(主) 幼东1可用区D(由) | 101.37 公网 | ◎ 還行中 | 经典网络 | TOP : 1 | 90 E% | c4765cdf537 | a945 Prot | o 性能共享型 vo | 按使用流量 | 按量付票 2017-06-05 11:48:53 创建 | 智理 更多・ |

单击标签旁边已选的标签键的删除图标,清除标签过滤条件。

移除实例标签

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。

登录负载均衡管理控制台。

在实例管理页面,选择地域,查看该地域的所有实例。

选择要删除标签的实例,单击更多 > 编辑标签。

在编辑标签窗口,单击要移除的标签的删除图标,然后单击确定。

注意: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。

| 编辑标签 | < |
|--|---|
| Protocol:TCP 🚳 network:classic 🛇 | |
| 注:每个资源最多可绑定10个标签,单次操作绑定/解绑标签的数量分别不能超过5个 绑定: 已有标签 新建标签 | |
| 确定取消 | |

后端服务器

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。

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。

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。默认后端服务器是在实例维度上维护的,即负载均衡实例下的所有监听都只能够将流量转发到相同服务器的相同端口上。

您也可以通过服务器组的方式添加ECS。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的不同 监听就可以将请求转发给不同的服务器组内不同端口的ECS。

注意:如果您在配置监听时,选择使用服务器组,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后端服务器池中的ECS。

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,流量将直接走主机;当主机宕机时,流量将走到备机。此时,可以使用主备服务器组,避免服务中断。

由于备机不会做健康检查,所以只要主机健康检查失败,系统会直接将流量切到备机。当主机健康检查成功恢 复服务后,流量会自动切到主机。

主备服务器组是在监听维度上维护的,并且只支持四层监听,详情参考创建主备服务器组。

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。详情参考创建虚拟服务器组。

注意事项

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。负载均衡监听的前端端口对应后端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 ,您可以根据后端ECS实例的对外服务能力和情况来区别设定。

注意:如果您同时开启了会话保持功能,那么有可能会造成对后端应用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,建议您可以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:

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。

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。(如设置会话保持,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。)

添加后端服务器

前提条件

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。如果您以前未使用过ECS,参考快速入门(Linux)和快速入门(Windows)创建ECS实例。

操作步骤

登录负载均衡管理控制台。

在实例管理页面,选择目标实例的所属地域。

单击目标实例的ID链接,进入负载均衡实例的详情页面。

在左侧导航栏,单击**服务器 > 后端服务器**。

在**负载均衡服务器池**页面,单击**未添加的服务器**页签。

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批量添加。

注意: ECS实例的网络类型要和该负载均衡实例的类型匹配。详情查看负载均衡实例类型。

- 经典网络的公网负载均衡实例,可添加经典网络类型的ECS或者同属于同一VPC的ECS;
- 专有网络的私网负载均衡实例, 仅能添加和负载均衡实例相同VPC内的ECS;
- 经典网络的私网负载均衡实例, 仅能添加经典网络类型的ECS。

在添加后端服务器对话框,指定添加的ECS实例的权重,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。您可以根据后端ECS实例的对外服务能力和情况来 区别设定。

注意:权重设置为0,该服务器不会再接受新请求。

添加后的实例会显示在已添加的服务器页签下,您可以移除或者修改添加的ECS实例的权重。

| A acs-slb-cb9e3635c9 : このののからおう の の の の の の の の の の の の の の の の の の の | | | | | | 的位主意事项 | |
|--|---------------|----------------------------|----------|-----------------------|--------|--------|------|
| 免難功率指示器法 所在始結: 34 伝 1 (秋川) 明期版: 3 伝 (1 可用区 8 (土) /4 伝 1 可用区 0 (魚) ● | | | | | | | |
| 已录此的编装器 未添加的编装器 | | | | | | | |
| 王編8月85日 • 周白)王振为指式市地行振动的 (現在) | | | | | | | |
| 0 云服务器(0/名称 | 可用区 | 公司/内司印始址 | 秋志(全部) = | 网络类型(全部) ~ | 健康检查状态 | 67.BL | 盛作 |
| D i-bp1;8 cb9e36 | cn-hangzhou-e | 116.6 4 (3世生) 192-1 私知) | Si5+ | 参询网络 (vpc-bp1k/fp | 正常 | 100 | 1539 |
| i-bp1ix cb9e36 | cn-hangzhou-e | 116.6 (3时生) 192.1 (私物) | S 267中 | 參有詞論 (vpc-bp1k/fp) | шж. | 100 🖌 | 818 |

创建主备服务器组

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,可选择使用主备服务器组。当主机正常工作时,流量将直接走主机;当主机不可用时,流量将走到备机,避免服务中断。

主备服务器组和虚拟服务器组都是在监听维度上维护的,即实例下的不同监听可将流量转发到不同的服务器组。但是一个虚拟服务器组可以添加多个ECS实例,而一个主备服务器组只允许添加两个ECS实例,其中一个作为主机,另外一个作为备机。

注意:主备服务器组只支持四层监听(TCP和UDP协议)。

前提条件

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。如果您以前未使用过ECS,参考快速入门(Linux)和快速入门(Windows)创建ECS实例。

操作步骤

登录负载均衡管理控制台。

在实例管理页面,选择目标实例的所属地域。

单击目标实例的ID链接,进入负载均衡实例的详情页面。

在左侧导航栏,单击**服务器 > 主备服务器组**。

在主备服务器组页面,单击创建主备服务器组。

在创建主备服务器组对话框,完成如下操作:

在分组名称文本框中,输入主备服务器组名称。

选择目标ECS实例的网络类型。

注意: ECS实例的网络类型要和该负载均衡实例的类型匹配。详情查看负载均衡实例类型

- i. 经典网络的公网负载均衡实例,可添加经典网络类型的ECS或者同属于同一 VPC的ECS;
- ii. 专有网络的私网负载均衡实例,仅能添加和负载均衡实例相同VPC内的ECS;
- iii. 经典网络的私网负载均衡实例,仅能添加经典网络类型的ECS。

在可选服务器列表中,单击目标ECS实例。

在**已选服务器列表**中,输入ECS实例的端口和权重,并选择作为主机使用的ECS实例,单击确定。

创建虚拟服务器组

概述

虚拟服务器组(VServer group)是一组 ECS 实例。虚拟服务器组允许您在监听维度上个性化定义服务器组 ,即实例下的不同监听可使用不同的后端服务器组,可满足域名和 URL 转发个性化需求。

如果您没有创建虚拟服务器组,负载均衡实例会将请求按照您设置的权重和监听规则转发给所有添加的后端服务器(ECS 实例);如果您创建了虚拟服务器组,负载均衡实例会将请求按照您设置的监听规则转发给关联的虚拟服务器组,默认实例维度添加的独立的后端服务器不再接收请求。

注意:如果您在一个负载均衡实例的 HTTP/HTTPS 监听下,添加了后端服务器、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,即将流量转发到实例级别添加的各后端服务器。

使用限制

虚拟服务器组只能添加监听所在地域的后端服务器。

一个后端服务器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。

虚拟服务器组由服务器+端口组成。

前提条件

您已经创建了负载均衡实例。

您创建了 ECS 实例,用来接收转发的请求。如果您以前未使用过阿里云 ECS,参考快速入门(Linux)或快速入门(Windows)创建 ECS 实例。

操作步骤

登录负载均衡管理控制台。

在实例管理页面,选择地域,查看该地域下的所有负载均衡实例。

单击负载均衡实例的 ID 链接,进入负载均衡的详情页面。

在负载均衡实例菜单栏,单击 服务器 > 虚拟服务器组。

在虚拟服务器组页面,单击创建虚拟服务器组。

在 创建虚拟服务器组 对话框,完成如下操作:

在 分组名称 文本框中,输入虚拟服务器组名称。

选择您要添加的 ECS 实例的网络类型。

注意: ECS 实例的网络类型要和负载均衡实例的类型匹配,如果不匹配,添加按钮则会灰掉。详情查看负载均衡实例类型。

- i. 经典网络的公网负载均衡实例,可添加经典网络 ECS 实例或者同一 VPC 实例 ID 的 ECS 实例;
- ii. 专有网络的私网负载均衡实例, 仅能添加同一 VPC 实例 ID 的 ECS 实例;
- iii. 经典网络的私网负载均衡实例, 仅能添加经典网络的 ECS 实例。

在可选服务器列表,单击要添加的实例。

选中添加的实例会显示在右侧的已选服务器列表中。

在 已选服务器列表, 输入每个 ECS 实例的端口和权重, 单击确定。

创建的虚拟服务器组会显示在 虚拟服务器组 页面,您可以删除或者增加虚拟服务器的 ECS 实例数量(单击 编辑)。您也可以将该虚拟服务器组和实例下的监听或者转发策略关联。

| < | 🔒 Intranet_classic 🔹 alicentation de anticación de la constante de la consta | | |
|-------------|--|---|------------------|
| 94 0 | 虚拟服务器组 | | dalkersalar Ami |
| - 総分務 | 含數均衡數以是在中间建度上维护后间接导器的 | 3、到去树下的所有监听都像两条物的类编程分器包,或和服务器包允许用个在监听地算上个性化足又服务器包,即共伤下的不能监听可他带不能的实确服务器包,可用定地实和以和教力性化需求。 | |
| 后间接外籍 | 分组名称 | (S) BID | 摄作 |
| 虚拟服务器组 | 经角间培ECS | np-bp1vf: | 业 看(编辑)出行 |
| 主義報告書編 | | | |
| 212 | | | |

监听

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。

负载均衡监听包括监听配置和健康检查配置。

监听配置

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 |
|------|---|---|
| ТСР | - 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 |
| 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 |
| НТТР | - 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 |

| | - 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 | |
| | 36 1961年成为 | |
| нттрѕ | , 用户可以将证书上 | 雲要加密传输的应田 |
| | 传到负载均衡,解密 | |
| | 操作直接在负载均衡 | |
| | 上完成 | |
| | | |

说明:负载均衡已在欧洲中部(法兰克福)与亚太东南3(吉隆坡)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。

健康检查配置

负载均衡对后端服务器提供健康检查,提高服务的可用性。详情参见健康检查原理和健康检查配置。

| 添加监听 | | \times |
|----------------|---|----------|
| 1.基本配置 | 2.健康检查配置 3.配置成功 | |
| 健康检查方式: 🛛 | ⊛ тср ⊙ нттр | |
| 检查端口: | 端口输入范围为1-65535。 默认使用后端服务器的端口进行健康检查 | |
| ▼ 收起高级配置 | | |
| 响应超时时间:* | 5 秒 | |
| 健康检查间隔:★ | 每次健康检查响应的最大超时时间; 输入范围1-300秒,默认为5秒 2 进行健康检查的时间间隔; 输入范围1-50秒,默认为2秒 | |
| 不健康阈值:+ | | |
| 健康阈值: * | 2 3 - 5 0 / 0 9 10 表示云服务器从成功到失败的连续健康检查失败次数。 2 3 4 5 6 7 8 9 10 2 3 4 5 6 7 8 9 10 | |
| | 农小石版另新州大坝到队初的进续进展位亘队初八级。 | |
| | 上一步 确认 | 取消 |



配置四层监听

四层监听概述

阿里云提供四层(TCP协议和UDP协议)的负载均衡服务。四层监听将请求直接转发到后端ECS实例,而且不修改请求标头。

TCP协议

TCP是面向连接的协议,在正式收发数据前,必须和对方建立可靠的连接。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、远程登录和无特殊要求的Web应用。

UDP协议

UDP是面向非连接的协议,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,可靠性相对低但数据传输快。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。

UDP协议监听有如下限制:

- 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。

四层监听配置

| 监听配置 | 说明 |
|-----------|--|
| | 用来接收请求并向后端服务器进行请求转发的前端 协议和端口。 |
| 前端协议 [端口] | 配置四层监听 , 协议选择TCP或UDP , 端口为1- 65535。 |
| | 注意 :在同一个负载均衡实例内,前端端口不可 重复。 |

| 后端协议 [端口] | 后端服务器(ECS实例)开放用来接收请求的后端端口。 后端的协议类型和前端相同,端口为1-65535。 注意:在同一个负载均衡实例内,后端端口可重复。 |
|-----------|--|
| 带宽峰值 | 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 。 当不限制监听带宽时,各监听共享实例的总带宽。 更多详细信息,参考共享实例带宽。 |
| 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。 - 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。 - 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。 |
| 使用服务器组 | 选择是否使用服务器组。使用服务器组,可以在监 听维度上个性化定义服务器组,即实例下的不同监 听可使用不同的服务器组。 注意:使用服务器组后,该监听会将流量转发到选 择的服务器组,实例维度的后端服务器不再生效。 如果不开启服务器组,监听会将流量转发到后端服 务器池内添加的服务器上。详情参考添加后端服务 器。 |
| 服务器组类型 | 如果选择使用服务器组,选择您要使用的服务器组 类型: - 虚拟服务器组:一个虚拟服务器组 (VServer group)由多个后端服务器组 成,且后端服务器的端口可以不同。您可 以为不同的监听配置不同的虚拟服务器组 ,这样就可以将请求转发至不同的后端服 务器。详情参考创建虚拟服务器组。 - 主备服务器组:一个主备服务器组由两台 后端服务器组成,即一台主服务器,一台 备服务器。当您有传统的主备需求时,可 以使用主备服务器组。当主机工作正常时 |

| | ,将流量转发至主服务器;当主机宕机时 ,会将流量转发至备服务器,避免服务中 断。详情参考创建主备服务器组。 |
|------------|--|
| 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。 |
| 高级配置 | |
| 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。 注意:经典网络的负载均衡实例的UDP监听暂不支持查看源地址。 |
| 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。 针对TCP监听,负载均衡是基于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。 注意 :UDP监听不支持会话保持。 |
| 连接超时时间 | 指定TCP连接的超时时间。可选值为10-900秒。 注意:此配置只适用于TCP监听。 |



配置七层监听

七层监听概述

阿里云提供七层(HTTP协议和HTTPS协议)的负载均衡服务,负载均衡七层监听原理上是反向代理的一种实现 。客户端HTTP请求到达负载均衡监听后,负载均衡服务器会通过与后端服务器建立TCP连接,即再次通过新 TCP连接HTTP协议访问后端服务器,而不是直接转发报文到后端服务器。

HTTP协议

HTTP是应用层协议,主要解决如何包装数据。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。

HTTPS协议

HTTPS是以安全为目标的HTTP通道,即HTTP下加入SSL层来保证数据安全。负载均衡支持HTTPS单向和双向认证。提供证书管理功能,无需在后端服务器上进行证书配置,详情查看配置HTTPS监听。

七层监听配置

| 监听配置 | 说明 |
|-----------|--|
| 前端协议 [端口] | 用来接收请求并向后端服务器进行请求转发的前端协议和端口。 配置七层监听,协议选择HTTP或HTTPS,端口为1- 65535。 注意:在同一个负载均衡实例内前端端口不可重复。 |
| 后端协议 [端口] | 后端服务器(ECS实例)开放用来接收请求的后端端口。 后端的协议类型为HTTP,端口为1-65535。 注意:在同一个负载均衡实例内后端端口可重复。 |
| 带宽峰值 | 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。 当不限制监听带宽时,各监听共享实例的总带宽。更多详细 信息,参考共享实例带宽。 |
| 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。 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。 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。 |
| 使用服务器组 | 开启配置后,可以在监听维度上个性化定义服务器组,即实 |

| | 例下的不同监听可使用不同的后端服务器组。 |
|------------|--|
| | 一个虚拟服务器组(VServer group)由多个后端服务器组成,且后端服务器的端口可以不同。您可以为不同的监听配置不同的虚拟服务器组,这样就可以将请求转发至不同的后端服务器。详情参考创建虚拟服务器组。 |
| | 注意 :使用服务器组后,该监听会将流量转发到选择的服务 器组,实例维度的后端服务器不再生效。如果不开启服务器 组,监听会将流量转发到后端服务器池内添加的服务器上。 详情参考添加后端服务器。 |
| | 开启该配置后支持在服务端和客户端进行HTTPS双向认证 ,您需要上传服务器证书和CA证书。 |
| 双向认证 | 不开启,单向认证只需上传服务器证书。 |
| | 注意 :该选项只适用于HTTPS监听。 |
| | 用于用户浏览器检查服务器发送的证书是否是由自己信赖的中心签发的。 |
| 服务器证书 | 服务器证书可以到阿里云云盾证书服务购买 , 也可以到其它 服务商购买。服务器证书需要上传到负载均衡的证书管理系 统。详情参考上 传证书 。 |
| | 注意 :该选项只适用于HTTPS监听。 |
| CA证书 | 服务器用CA证书验证收到的客户端证书。如果没有通过验 证,拒绝连接。开启双向认证功能后,CA证书和服务器证 书都需要上传到负载均衡的证书管理系统。详情参考生成证 书。 |
| | 注意 :该选项只适用于HTTPS监听。 |
| 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。 |
| 高级配置 | |
| 获取真实IP | 针对七层服务,负载均衡通过HTTP Header: X- Forwarded-For获取来访者真实IP。详情参考获取来访者真 实IP。 |
| | 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。 |
| | 针对七层(HTTP协议和HTTPS协议)监听,负载均衡使用 Cookie进行会话保持。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。 |
| 会话保持 | 客户端第一次访问时,负载均衡会在返回请求中 |
| | 個人COOKIE(即任HITP/HITPS响应报文中插入 SERV/ERID) 下次安白逆進共地Cookia注词 |
| | ,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。 查看会话保持常见问题了解更多信息。 |
|-----------|--|
| 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: - X-Forwarded-For:添加该字段获取客户端的IP地 址。 - X-Forwarded-Proto:添加该字段获取客户端与监 听连接时所用的协议(HTTP或HTTPS)。 - SLB-IP:添加该字段获取负载均衡实例的公网IP。 - SLB-ID:添加该字段获取负载均衡实例的ID。 |

HTTPS监听

为了满足数据传输的安全需求,负载均衡提供了HTTPS监听,支持单向和双向认证。

在使用HTTPS监听时,注意:

在使用HTTPS监听前,您需要将需要的证书上传到负载均衡系统。详情查看上传证书。

| 证书 | 说明 | 单向认证是否需要 | 双向认证是否需 |
|-------|---|-------------------------------------|-------------------------------------|
| 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。 | 否 | 是 需要客户端进行安 |

| | 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。 | | 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。 |

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。

配置HTTPS单向认证

本指南提供配置HTTPS监听(单向认证)的完整教程。完成以下三个任务完成配置:

- 1. 上传服务器证书
- 2. 配置负载均衡实例
- 3. 测试负载均衡服务

上传服务器证书

在配置HTTPS监听(单向认证)前,您需要购买服务器证书,并将服务器证书上传到负载均衡的证书管理系统。上传后,无需在后端ECS上进行其它证书配置。

登录负载均衡管理控制台。

在左侧导航栏,单击证书管理,然后单击创建证书。

按照以下信息,配置证书:

证书Region: 选择**华东 1**。

注意:证书的地域和负载均衡实例的地域要相同。

证书类型:选择**服务器证书**。

证书内容和私钥:复制服务器证书的内容和私钥。单击**导入样例**查看合法的证书格式。上 传的证书必须是PEM格式,详情查看证书格式要求。



单击确定完成上传。

配置负载均衡实例

登录负载均衡管理控制台。

在实例管理页面,单击创建负载均衡。

配置负载均衡实例,单击立即购买完成支付。

注意:网络类型选择:公网,地域选择华东1。详细配置信息参考创建负载均衡实例。

创建成功后,返回实例管理页面,单击华东1地域,然后单击已创建的负载均衡实例ID链接。

在详情左侧导航栏,单击监听,然后单击添加监听。

在添加监听窗口,完成如下配置。

| 」」 </th <th>2 80</th> | 2 80 |
|---|--|
| | 00. |
| 调度算法:轮询。 | |
| | |
| 服务器证书:选择已上位 | 专的服务器证书。 |
| 添加监听 | |
| 1.基本配置 | 2.健康检查配置 3.配置成功 |
| 前端协议[端口]: \star | HTTP! ▼ : 443 端口輸入范围为1-65535。 四层监听请选择TCP、UDP;七层监听请选择HTTP、HTTPS; 查看详 情 |
| 后端协议 [端口]:* | HTTP : 80 端口输入范围为1-65535。负载均衡协议为HTTPS时,后端协议为HTTP |
| 带宽峰值: | 不限制 配置 使用流量计费方式的实例默认不限制带宽峰值;峰值输入范围1-5000 |
| 调度算法: | 轮询 ▼ |
| 使用虚拟服务器组: | 0 |
| 双向认证: | ○ 关闭 |
| 服务器证书:★ | serverCer1/1309208528360047_159489034ed ▼ 新建证书 |
| 创建完毕自动启动 监听: | ● 已开启 |
| | |

在左侧导航栏,单击**服务器 > 后端服务器**,然后单击**添加后端服务器**,添加ECS服务器。

取消

测试负载均衡服务

负载均衡实例配置完成后,在**实例管理**页面,查看健康检查状态。当状态为**正常**时,表示后端服务器可以正常接收处理负载均衡监听转发的请求。



在浏览器中,输入负载均衡的公网服务地址。刷新浏览器,您可以观察到请求在两台ECS服务器之间 转换。

因为使用了自建的服务器证书,所以下图示例中会有不信任提示。

| | ♀ ▼ 😢 证 | . 🖒 <i>ể</i> 101.37. | × |
|------------------------------|---------|----------------------|---|
| Hello World ! This is ECS01. | | | |
| | | | |
| | | | |
| ← → @ https://101 | ♀ ▼ 😢 证 | . 🖒 🙋 101.37. | × |
| Hello World ! This is ECS02. | | | |
| | | | |
| | | | |

配置HTTPS双向认证

本指南将引导您配置HTTPS双向认证的负载均衡服务。本指南中使用自签名的CA证书为客户端证书签名。

完成以下操作配置HTTPS监听(双向认证):

- 1. 准备服务器证书
- 2. 使用OpenSSL生成CA证书
- 3. 生成客户端证书
- 4. 上传服务器证书和CA证书
- 5. 安装客户端证书
- 6. 配置负载均衡实例
- 7. 测试负载均衡服务

步骤一: 准备服务器证书

服务器证书用于用户浏览器检查服务器发送的证书是否是由自己信赖的中心签发的,服务器证书可以到阿里云 云盾证书服务购买,也可以到其他服务商处购买。

步骤二: 使用OpenSSL生成CA证书

运行以下命令在/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(证书备份目录)。
- 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。

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

运行以下命令牛成私钥kev文件。

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

运行结果如下图所示。

```
coot@iZbp1hfvivcqx1jbwap31iZ:~/ca/conf# cd /root/ca
coot@iZbp1hfvivcqx1jbwap31iZ:~/ca# sudo openss1 genrsa -out private/ca.key
Generating RSA private key, 2048 bit long modulus
....+++
.+++
e is 65537 (0x10001)
```

运行以下命令并按命令后的示例提供需要输入的信息,然后回车,生成证书请求csr文件。

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

注意:Common Name请输入您的负载均衡服务的域名。



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

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

运行以下命令创建CA键库。

\$ sudo touch index.txt
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

步骤三: 生成客户端证书

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

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

注意: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。

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,提供对应的信息。

注意:**A challenge password**是客户端证书口令(请注意将它和client.key的口令区分开,本教 程设置密码为test),可以与服务器端证书或者根证书口令一致。



运行以下命令使用步骤二中的CA Key为刚才的客户端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。



运行以下命令将证书转换为大多数浏览器都能识别的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



运行以下命令查看生成的客户端证书。



步骤四: 上传服务器证书和CA证书

登录负载均衡管理控制台。

在**实例管理**页面,单击**创建负载均衡**。

配置负载均衡实例,单击**立即购买**完成支付。

注意:网络类型选择:公网,地域选择华东1。详细配置信息参考创建负载均衡实例。

创建成功后,在**实例管理**页面,将鼠标移至实例名称区域,单击出现的铅笔图标,修改负载均衡实例 名称。

在负载均衡左侧导航栏,单击证书管理,然后单击创建证书,上传服务器证书。

在创建证书页面,完成如下配置后,单击确定。

证书地域:本教程中**选择华东1**。

注意:证书的地域和负载均衡实例的地域要相同。

证书类型:选择**服务器证书**。

证书内容和私钥:复制您的服务器证书内容和私钥。

在复制内容前,您可以单击**导入样式**,查看正确的证书和私钥格式。更多详细信息查 看**证书要求**。



在负载均衡左侧导航栏,单击**证书管理**,然后单击创建证书,上传CA证书。

在创建证书页面,完成如下配置后,单击确定。

证书地域:本教程中**选择华东1**。

注意:证书的地域和负载均衡实例的地域要相同。

证书类型:选择**CA证书**。

证书内容:复制您的CA证书内容。

在复制内容前,您可以单击**导入样式**,查看正确的CA证书格式。更多详细信息查看证书要求。

| 创建证书 * 返回证书列表 | |
|-----------------|---|
| 证书名称: | CA1 |
| x)THeolog | 长度限制力1-80个字符,只分许包含字母、数字、□、「、□」 □ 四十七方,(石(小(本))) □ 4/4 (● 単同に切) □ 4/4 (■ 4/4 (■ 4/4) □ 4/4 (■ 4/4) □ 4/4 (■ 4/4 (■ 4/4) □ 4/4 (■ 4/4 (■ 4/4) □ 4/4 (■ 4/4 (■ 4/4 (■ 4/4 (■ 4/4) □ 4/4 (■ 4/4 (■ 4/4 (■ 4/4 (■ |
| "IE-bregion : | - エススパート、INTURNAL - MARLEL - MAR |
| *证书类型: | |
| 2. 五式山峦。 | 证书编辑器里面的格式仪验功能只起影腾醒的功能,格式仪验递过不能代表证书格式一定能被识别 |
| €, br3₩ - | 2 |
| | 127 U(ARC98270gKrcSinebu74m221H275H0o5KWr210m54g5KuF76h275690hH075m 18. 20Km12H2M6707HKr487a/STAM5FY164Tent/JNMSKH38U26TsABHMKAS61BBPv (pem時時) 員入社例 |
| | ahu Role |

步骤五:安装客户端证书

将生成的客户端证书安装到客户端。本教程以Windows客户端,IE浏览器为例。

打开Git Bash命令行窗口,运行以下命令导出步骤三中生成的客户端证书。

scp root@IPaddress:/root/ca/users/client.p12 ./

注意: IPaddress是生成客户端证书的服务器的IP地址。

在IE浏览器中导入下载的客户端证书。

打开IE浏览器,单击设置 > Internet选项。

单击**内容**页签,然后单击**证书**,导入下载的客户端证书。在导入证书时需要输入在步骤三时生成PKCS12文件的密码。

| 证书 | | | | | | × |
|--------------|-------------|--------------------|--------------|---------------|-------|----------|
| 预期目的(| (N): | 〈所有〉 | | | | • |
| 个人 | 其他人 | 中级证书颁发机构 | 受信任的根证 | E书颁发机构 | 受信任的发 | 布者 未受信 🚺 |
| 颁发给 | \$ | 颁发者 | 截止 | 友好名称 | | |
| | an Santa | And and the second | 2022 2019 | 133952 〈无〉 | | |
| myd | omain | mydomain | 2018 | 〈无〉 | | |
| | | | | | | |
| □导入(I) | ··· Ę | ≩出(E) ── 册 |]除(R) | | | 高级(A) |
| 证书的预 | 前期目的 | | | | | |
| 〈所有〉 | | | | | | 查看(\\) |
| 了解 <u>证书</u> | 的详细信。 | 息 | | | | 关闭(C) |

步骤六: 配置HTTPS双向认证监听

登录负载均衡管理控制台。

在实例管理页面,单击华东1地域,然后单击已创建的负载均衡实例ID链接。

在**详情**左侧导航栏,单击**监听**,然后单击**添加监听**。

在添加监听窗口,完成如下配置。

前端协议 [端口]:HTTPS 443。

后端协议 [端口]:HTTP 80。

带宽峰值: 输入带宽峰值。

调度算法:轮询。

双向认证:开启。

服务器证书:选择已上传的服务器证书。

CA证书:选择已上传的CA证书。

| 单击下一步, 领 | 然后单击确认完成配置。 |
|----------|-------------|
|----------|-------------|

| 2.健康检查配置 3.配置成功 HTTPS ▼ : 443 端口输入范围为1-65535。 四层监听请选择TCP、UDP;七层监听请选择HTTP、HTTPS;查看详情 |
|---|
| HTTPS ▼ : 443 端口输入范围为1-65535。 四层监听请选择TCP、UDP;七层监听请选择HTTP、HTTPS; 查看详情 |
| |
| HTTP : 80 端口输入范围为1-65535。负载均衡协议为HTTPS时,后端协议为HTTP |
| 5 M 可用: 5M (已用0M,共5M) 固定带宽计费方式的实例,不同监听分配的带宽峰值总和不能超出在创建负载 均衡实例时设定的带宽总值 |
| 轮询 ▼ |
| 0 |
| |
| server1/1231579085529123 ▼ 新建证书 |
| CA1/1231579085529123_ ▼ 新建证书 |
| 日本 日 |
| |
| |

在**详情**左侧导航栏,单击**服务器 > 后端服务器**,然后单击**添加后端服务器**,添加ECS服务器。

步骤七: 测试HTTPS双向认证

在**实例管理**页面,查看健康检查状态。当状态为**正常**时,表示后端服务器可以正常接收处理负载均衡 监听转发的请求。

| 宮例管理 亚太东南1(新加 | 峻) 欧洲中部1(法兰克福) | 绿北1 美国 东部1 | (弗吉尼亚) 华 | 出2 华东2 | 聖太东北 1 (东南) | \$4周1 | 8R : | 亚太东南 2 (悉尼) | 創田西部1(社谷) | 中东东部1(遗拜) | 华纪3 华东1 | 0 | Right | 93204096 |
|----------------------------------|-----------------------------------|-------------------|----------|--------|-------------|-------|----------|-------------|--------------------|-----------|--------------|--------------------------------|-------|------------|
| 负载均衡D v 请编 | 入实例ID进行模糊查说:多个按 | .9稿 抱床 | ●标签 | | | | | | | | | | | <u>×</u> • |
| □ 负载均衡四/名称 | 可用区 | 服务地址(全部) マ | 状态 | 网络类型(全 | 部) * | 3 | A口/健康 | 检查 | 后端服务器 | 实例规格 | 带宽计费方式(全部) 👻 | 付费方式(全部) 👻 | | 操作 |
| B-bp17vpctt acs-sb-caa21d1eab | cn-hangzhou-e(主) 华在1可用区 F(音) | 101.37 公网 | ● 运行中 | 经典网络 | | т | CP : 8 | 0 | 未乾豐(乾雪) | 性能共享型 | 按使用流量 | 按量付费 2017-05-27 09:32:58 创建 | | 管理 更多・ |
| HTTPS | cn-hangzhou-e(主) 终东 1 可用区 D(音) | 118.178 | ● 运行中 | 经典网络 | | H | ITTPS :4 | 43 正常 | ubuntu2 ubuntu1 | 性能共享型 | 技图注带宽 | 包年包月 2017-06-11 00:00:00 到期 | | 管理 更多・ |

在浏览器中,输入负载均衡的公网服务地址,当提示是否信任客户端证书时,选择信任。

| Windows 安全 | |
|--|---|
| <mark>确认证书</mark> 通过单击"确定"确认此证书。如果这不是正确的证书,则单击"取消" 。 | |
| mydomain 颁发者: mydomain 有效期: 2017/6/4 至 2018/6/4 单击此处查看证书属性 | |
| 确定取消 |] |

刷新浏览器,您可以观察到请求在两台ECS服务器之间转换。

因为使用了自建的服务器证书,所以下图示例中会有不信任提示。

| ← → € https://118 | p ▾ 😫 证 | 0 2 118.178 | × |
|------------------------------|---------|-------------|---|
| Hello World ! This is ECS01. | | | |
| | | | |
| | | | |
| | | | |
| | ♀ ▼ 😣 诓 | 0 🥭 118.178 | × |
| Hello World ! This is ECS02. | | | |
| | | | |
| | | | |

添加域名或URL转发规则

域名或URL转发规则

七层负载均衡服务支持配置域名或者URL转发策略,将来自不同域名或者URL的请求转发给不同的ECS处理。您可以在一个监听下添加多条转发策略,每条转发策略关联不同的虚拟服务器组(一个虚拟服务器组由一组 ECS实例组成)。比如您可以将所有读请求转发到一组后端服务器上而将写请求转发到另一组后端服务器上,这样可以更灵活地适配业务需求,合理分配资源。

如下图所示,在配置了转发策略后,负载均衡系统将按照以下规则转发前端请求:

如果能匹配到相应监听关联的转发策略,则按转发策略,将请求转发到对应的虚拟服务器组。

如果未匹配,而对应监听启用并配置了虚拟服务器组,则将请求转发到对应的虚拟服务器组。

如果均未匹配,则转发到负载均衡实例后端服务器池中的ECS。



您不需要在转发规则上单独配置健康检查,下表对比描述了三个维度的健康检查机制。

| 维度 | 健康检查配置 | 健康检查目标服务器 |
|--------|----------------|----------------|
| 后端服务器 | 使用配置监听时的健康检查配置 | 所有后端ECS |
| 虚拟服务器组 | 使用配置监听时的健康检查配置 | 相应虚拟服务器组包含的服务器 |
| 转发策略 | 使用配置监听时的健康检查配置 | 相应虚拟服务器组包含的服务器 |

注意:由于虚拟服务器组中可以对ECS配置不同的端口,因此在配置健康检查时不要设置检查端口,否则会导致采用了不一致端口承载服务的服务器健康检查失败。

域名或URL转发规则说明

负载均衡支持分别添加域名或URL转发规则,也支持添加域名+URL组合的转发规则。

域名转发规则配置

单独配置域名转发规则时,URL配置项留空(不用输入/)。域名只能使用字母、数字、连字符(-)、点(.)。

| 添加转发策略 | | | | \times |
|---|--|------------------------------|-------------------|----------|
| | | | | |
| 规则名称 | 域名 | URL | 虚拟服务器组 | 操作 |
| rule1 | www.aliyun.com | | TOM 🔻 | 删除 |
| | 添 | 加转发策略 + | | |
| * 域名规范: 只能使用字母、数字 - 标准域名:www.te - 泛解析域名:*.test | 、'-'、`-',只支持以下两 st.com; com , *一定在第一个雪 | 种形式的domain形式 字符,并且是*.的格式, | *不能在最后。 | |
| * URL规范 : 长度限制为2-80个字 为/,但必须以/开头。 | 符,只能使用字母、数: | 字、`-'、`/'、`-'、`%'、`?' | 、`#′、`&′这些字符; UR/ | L不能只 |
| * 域名与URL请至少城 | 直写一项。 | | | |
| | | | 确认 | 取消 |

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规则时,规则的匹配优先级为:精确匹配 > 小范围通配符匹配 > 大范围通配符匹配,如下表所示。

| 模式 | 请求测试 URL | 域名规则与匹配情况 | | | | | |
|-------|-----------------------|--------------------|--------------|-------------------------|--|--|--|
| | | www.aliyun. com | *.aliyun.com | *.market.ali yun.com | | | |
| 精确匹配 | www.aliyun. com | \checkmark | | | | | |
| 泛域名匹配 | market.aliyu n.com | | \checkmark | | | | |
| 泛域名匹配 | info.market. | | | \checkmark | | | |

| aliyun.com | | |
|------------|--|--|

URL转发规则配置

单独配置URL转发规则时,域名配置项留空。参考以下原则添加URL:

URL只能包含字母、数字和以下特殊字符:

-./%?#&.

URL必须以斜杆(/)开头。

注意:如果您在URL中只输入了一个斜杆(/),则URL转发规则失效。

URL转发支持字符串匹配,按照顺序匹配原则。比如/admin、/bbs、/test。

| 添加转发策略 | | | | × |
|--|--|-----------------------------------|--------------------|--------|
| | | | | |
| 规则名称 | 域名 | URL | 虚拟服务器组 | 操作 |
| rule2 | | /tom | том | 删除 |
| | | 添加转发策略 + | | |
| * 域名规范: 只能使用字母、数 - 标准域名:www - 泛解析域名:*.t | 字、`-'、`-',只支 .test.com; est.com,*一定在 | 持以下两种形式的domain册 王第一个字符,并且是*.的棺 | (式); *不能在最后。 | |
| * URL规范: 长度限制为2-80个 为/,但必须以/开头 | 字符,只能使用: :。 | 字母、数字、`-'、`/'、`'、`% | /、`?'、`#'、`&'这些字符; | URL不能只 |
| * 域名与URL请至 | 少填写一项。 | | | |
| | | | 确认 | 取消 |

域名+URL转发规则配置

当需要根据相同域名下不同的URL路径进行流量转发时,建议您配置一个默认转发策略(URL留空),以免未匹配到的其它URL访问出错。参见如何实现相同域名不同路径的流量转发。

比如有两个域名分别是www.aaa.com和www.bbb.com,要求访问www.aaa.com/index.html时,将 请求转发给ServerGroup1处理,其它来自xxx.html的请求转发给ServerGroup2处理。您需要配置如 下转发策略,否则匹配到www.aaa.com的域名但没有相关策略匹配会返回404的响应码。

| ž | 添加转发策略 | | | | \times | | | | | |
|---|----------|-------------|-------------|----------------|----------|--|--|--|--|--|
| | | | | | | | | | | |
| | 规则名称 | 域名 | URL | 虚拟服务器组 | 操作 | | | | | |
| | rule1 | www.aaa.com | /index.html | ServerGroup1 🔻 | 删除 | | | | | |
| | rule2 | www.aaa.com | | ServerGroup2 🔻 | 删除 | | | | | |
| | 添加转发策略 + | | | | | | | | | |

配置域名URL转发策略

前提条件

您已经创建了七层 (HTTP/HTTPS) 监听, 详情参考配置监听。

您已经创建了接收请求的虚拟服务器组。详情参考创建虚拟服务器组。

操作步骤

登录负载均衡管理控制台。

在实例管理页面,选择地域,查看该地域的所有负载均衡实例。

单击负载均衡实例的ID链接。

在详情页面的左侧导航栏,单击监听。

单击目标七层监听的操作列内的更多 > 添加转发策略。

在**转发策略**页面,单击**添加转发策略**。

在添加转发策略对话框,配置转发规则,然后单击确认。

单击添加转发策略+添加另一条转发策略,单击确认完成配置。

健康检查

健康检查配置

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。关于健康检查的原理参考负载均衡健康检查原理。其它健康检查问题,参考健康检查常见问题。

注意:负载均衡监听为TCP协议时,健康检查方式可选TCP或HTTP。

在负载均衡实例的详情页面,单击监听 > 添加监听,在添加监听的第二步可进行健康检查配置。

| 1.基本配置 | 2.健康检查配置 3.配置成功 |
|-----------|---|
| 健康检查方式: 🕢 | ○ TCP O HTTP |
| 域名: | 长度1-80个字符 |
| | 只能使用字母、数字、'-'、',' 默认使用各后端服务器的内网IP为域名 |
| 检查端口: | 端口输入范围为1-65535。 |
| | 默认使用后端服务器的端口进行健康检查 |
| 检查路径: | / |
| | 用于健康检查页面文件的URI,建议对静态页面进行检查。长度限制为1-80个 字符,只能使用字母、数字、'-'、'/、'.'、'%'、'?'、'#'、'&'、'='这些字符。 |
| 正常状态码: | V http_2xx V http_3xx http_4xx http_5xx |
| | 健康检查正常的http状态码 |
| ▼ 收起高级配置 | |
| 响应超时时间: ★ | 5 秒 |
| | 每次健康检查响应的最大超时时间;输入范围1-300秒,默认为5秒 |
| 健康检查间隔: * | 2 秒 |
| | 进行健康检查的时间间隔;输入范围1-50秒,默认为2秒 |
| 不健康阈值: * | 2 3 4 5 6 7 8 9 10 |
| | 表示云服务器从成功到失败的连续健康检查失败次数。 |
| 健康阈值: * | 0 |
| | 2 3 4 5 6 7 8 9 10 表示云服务器从失败到成功的连续健康检查成功次数。 |
| | |

健康检查参数说明

在配置健康检查时,建议您使用默认值。

| 健康检查配置 | 说明 |
|-----------------|--|
| | 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。 |
| 域名和检查路径 | 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。 |
| (仅限HTTP方式的健康检查) | 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 | 选择健康检查正常的HTTP状态码。 |
| (仅限HTTP方式的健康检查) | 默认值为http_2xx和http_3xx。 |
| 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。 注意:如果该监听配置了虚拟服务器组或主备服务 器组,目组内的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。 |
| 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 | 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。 |
| 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x(不健康阈值-1),即5x3+2x(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x健康阈值)+检查间隔x(健康阈值-1),即(1x3)+2x(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字段校,那么则需要配置相关的域名,确保健康检查正常工作。

设置白名单访问控制

特别提醒:访问控制白名单现已经全网开放,无需提工单开通。

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。

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人可以访问。

设置白名单的过程中可能会引起访问负载均衡监听短时中断。

操作步骤

登录负载均衡管理控制台。

选择地域,查看该地域下的负载均衡实例。

单击需要设置访问控制的负载均衡实例的ID链接,打开详情页。

在负载均衡实例菜单栏,单击监听,打开监听配置页面。

在监听页面,单击更多 > 设置访问控制。

| < | 🔥 acs-slb | | | | | | | | | | AT THE OWNER OF COMPANY | 2940 |
|-------------|--------------|--------------|-------|------------|------|-------|------|------|--|-------|-------------------------|-------------|
| 详情 1147 | 1921F | | | | | | | | | 15103 | 295 | 周新 |
| ▼ ※約冊 | ■ mianok/jac | 后期协议/第日 | 状态 | 1420-1920) | 会适保持 | 使康检查 | 带挖蜂植 | 服务器组 | | | | 操作 |
| 后纳服务器 | TCP: 80 | TCP: 9080 正常 | ● 运行中 | 加权轮询 | 关闭 | 8开宫 0 | 不限制 | 无 | | 22 | 洋橋 | <u>88</u> - |
| 唐拟服务器组 | | and a | | | | | | | | 启动 | | |
| | SAL NUL | | | | | | | | | 停止 | | |
| 土地的分钟员 | | | | | | | | | | 始時 | | |
| <u>1112</u> | | | | | | | | | | 「設置の月 | 11210 | |

在访问控制设置对话框,进行如下配置:

单击**是否开启访问控制**开关,打开开关。

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。

单击确认,完成配置。

后续操作

如果您想关闭白名单访问控制,单击更多 > 设置访问控制,然后关闭是否开启访问控制开关。

如果你想修改白名单中的IP地址,单击更多 > 设置访问控制,在白名单设置区域内修改IP地址。

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。

| 添加监 | 听 | | \times |
|-----|-------------------------------|--|----------|
| | 1.基本配置 | 2.健康检查配置 3.配置成功 | |
| | 前端协议 [端口]:★ | TCP ▼ : 端口输入范围为1-65535。 四层监听请选择TCP、UDP;七层监听请选择HTTP、HTTPS; 查看详情 | |
| | 后端协议 [端口] : \star | TCP : | |
| | 带宽峰值:¥ | 不限制 配置 固定带宽计费方式的实例,不同监听分配的带宽峰值总和不能超出在创建负载 均衡实例时设定的带宽总值。不限制则共享实例带宽。 | |
| | 调度算法: | 加权轮询 | |
| | 使用服务器组: 🕜 | □什么是服务器组? | |
| | 创建完毕自动启动监 听: ▼ 展开高级配置 — | | |
| | | 下一步取 | 消 |

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一直没有流量进入,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一直没有流量进入,而监听B的入流量很大,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的入流量,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也有流量进入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入流量同等大小,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。

证书管理

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----------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。

注意: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。

----BEGIN RSA PRIVATE KEY-----

MITEpAIBAAKCAQEAvZiSSSChH67bmT8mFykAxQ1tKCYukwBiWZwkOStFEbTWHy8K tTHSfD1u9TL6qycrHEG7cjYD4DK+kVIHU/Of/pUWj9LLnrE3W34DaVzQdKA00I3A Xw95grqFJMJcLva2khNKA1+tNPSCPJoo9DDrP7wx7cQx7LbMb0dfZ8858KIoluzJ /fD0XXyuWoqaIePZtK9Qnjn957ZEPhjtUpVZuhS3409DDM/tJ3Tl8aaNYWhrPBcO jNcz0Z6XQGf1rZG/Ve520GX6rb5dUYpdcfXzN5WM6xYg8alL7UHDHHPI4AYsatdG z5TMPnmEf8yZPUYudT1xgMVAovJr09Dq+5Dm3QIDAQABAoIBAG168Z/nnFyRHrFi laF6+Wen8ZvNqkm0hAMQwIJh1Vplfl74//8Qyea/EvUtuJHyB6T/2PZQoNVhxe35 cgQ93Tx424WGpCwUshSfxewfbAYGf3ur8W0xq0uU07BAxaKHNcmNG7dGyolUowRu S+yXLrpVzH1YkuH8TT53udd6TeTWi77r8dkGi9KSAZ0pRa19B7t+CHKIzm6ybs/2 06W/zHZ4YAxwkTYlKGHjoieYs111ahlAJvICVgTc3+LzG2pIpM7I+KOnHC5eswvM i5x9h/0T/ujZsyX9P0PaAyE2bay0t080tGexM076Ssv0KVhKFvWjLUnhf6WcqFCD xqhhxkECgYEA+PftNb6eyXl+/Y/U8NM2fg3+rSCms0j9Bg+9+yZzF5GhqgHu0edU ZXIHrJ9u6B1XE1arpijVs/WHmFhYSTm6DbdD7S1tLy0BY4cPTRhziFTKt8AkIXMK 605u0UiWsq0Z8hn1Xl4lox2cW9ZQa/HC9udeyQotP4NsMJWgpBV7tC0CgYEAwvNf 0f+/jUjt0HoyxCh4SIAqk4U0o4+hBCQbWcXv5qCz4mRyTaWzfEG8/AR3Md2rhmZi GnJ5fdfe7uY+JsQfX2Q5JjwTadlBW4ledOSa/uKRaO4UzVgnYp2aJKxtuWffvVbU +kf728ZJRA6azSLvGmA8hu/GL6bgfU3fkSkw03ECgYBpYK7TT7JvvnAErMtJf2yS ICRKbQaB3gPSe/lCgzy1nhtaF0UbNxGeuowLAZR0wrz7X3TZgHEDcYoJ7mK346of QhGLITyoehkbYkAUtq038Y04EKh6S/IzMzB0frXiPKg9s8UKQzkU+GSE7ootli+a R8Xzu835EwxI6BwNN1abpQKBgQC8TialClq1FteXQyGcNdcReLMncUhKIKcP/+xn R3kV106MZCfAdqirAjiQWaPkh9Bxbp2eHCrb81MFAWLRQSlok79b/jVmTZMC3upd EJ/iSWjZKPbw7hCFAeRtPhxyNTJ5idEIu9U8EQid8111giPgn0p3sE0HpDI89qZX aaiMEQKBgQDK2bsnZE9y0ZWhGTeu94vziKmFrSkJMGH8pLaTiliw1iRhRYWJysZ9 BOIDxnrmwiPa9bCtEpK80zq28dq7qxpCs9CavQRcvOBh5Hx0yy23m9hFRzfDeQ7z NTKh193HHF1joNM81LHFyGRfEWWrroW5gfBudR6USRnR/6iQ11xZXw= ----END RSA PRIVATE KEY-----



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

运行以下命令在/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。

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

运行以下命令生成私钥key文件。

\$ cd /root/ca

\$ sudo openssl genrsa -out private/ca.key

运行结果如下图所示。



运行以下命令并按提示输入所需信息,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

注意: Common Name需要输入负载均衡的域名。



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

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

运行以下命令创建CA键库。

\$ sudo touch index.txt

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

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

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

注意: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。

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。

注意: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。

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@iZbp1hfvivcqx1jb -cert /root/ca/priva | wap31iZ:~/ca# sudo openssl ca -in /root/ca/users/client.csr te/ca.crt -keyfile /root/ca/private/ca.key -out /root/ca/us |
|---|--|
| ers/client.crt -confi | g "/root/ca/conf/openssl.conf" |
| Using configuration f | rom /root/ca/conf/openssl.conf |
| Check that the reques | t matches the signature |
| Signature ok | |
| The Subject's Disting | uished Name is as follows |
| countryName | :PRINTABLE: 'CN' |
| stateOrProvinceName | :ASN.1 12:'ZheJiang' |
| localityName | :ASN.1 12:'HangZhou' |
| organizationName | :ASN.1 12:'Alibaba' |
| organizationalUnitNam | e: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 certificat | e requests certified, commit? [y/n]y |
| Write out database wi | th 1 new entries |
| Data Base Updated | |
| root@iZbp1hfvivcqx1jb | wap31iZ:~/ca# |

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。

运行以下命令查看生成的客户端证书。

cd users Is



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。

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



为了支持HTTPS数据传输加密认证,负载均衡提供证书管理功能。您可以将证书存储到负载均衡证书管理系统,而不需要将证书直接部署到后端ECS服务器上,上传到证书管理系统的私钥都会加密存储。一个证书可以应用于一个或多个监听。

- 负载均衡证书是分地域管理的,即一个证书如果要在多个地域使用,那么创建、上传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。



已经购买了服务器证书。

已经生成了CA证书和客户端证书。详情参考生成证书。

操作步骤

登录负载均衡控制台。

在**负载均衡**左侧导航栏,单击**证书管理**。

在证书管理页面,单击创建证书。

在创建证书页面,完成如下配置后,单击确定。

证书名称:输入证书名称。

证书地域: 选择要使用证书的地域。如果您的证书需要在多个地域使用,请把对应地域都选上。

证书类型:

服务器证书:HTTPS单向认证,只需要上传服务器证书和私钥。

CA证书:如果您要配置HTTPS双向认证,除了上传服务器证书外,您还需选择 CA证书进行上传。

证书内容:复制您的服务器或者CA证书内容。您可以单击**导入样式**,查看正确的证书样式。更多详情查看证书要求。

私钥:复制您的服务器证书的私钥。可以单击**导入样式**,查看正确的证书样式。更多详情 查看证书要求。

私钥只有服务器类型的证书才需要。

相关操作

上传证书后,您可以在负载均衡管理控制台的证书管理页面中查看证书、编辑证书名称、删除证书。

单击修改名称,修改证书的名称。

单击删除,删除该证书。

注意:证书如果在HTTPS监听中被引用了,则无法删除该证书。

| 征书管理 | 亚太东南 1 (新加坡) | 歐洲中部 1 (法兰克福) | \$41 I | #甜东部 1 (弗吉尼亚 | \$\$dt 2 | 华东 2 | 显太东北 1 (东京) | 华南 1 | 87B | 亚太东南 2 (悉尼) | 美国西部1(独谷) | 中东东部 1 (油稈) | 举北3 华东1 当前区域已经到4 | 个证书。 仅HTTPS协议 | ○周新 以業要证书,每个用户量多可 | éßit 12.6/8/10 | 征书 0个证书 |
|----------------|--------------|---------------|--------|--------------|----------|------|-------------------|-------|-----|---------------|-----------|-------------|---------------------|---------------|----------------------|--------------------------|-------------------|
| 证书实称 | | (EHID | | | | | 证书期级 | | | | | | 地域 | 征书典型 | | | 操作 |
| Server2 | | 12315790 | | 17044.070 | | | 7a:c1:ed:9e:e1:99 | 6d | - | 1.0 | | | 华东 1 | 服気器正形 | 6 | 888 | 209 |
| CAL | | 12315790 | | | | | 0d:f6:9e:ed:c2:6d | df:0 | | | | | 华东 1 | CAIEH | 9 | 改名称 | 819 |
| server1 | | 12315790 | | | | | 7a:c1:ed:9e:e1:99 | :6d:4 | | an Astronomer | | | 华东 1 | 服局醫证书 | 19 | 888 | 209 |
| test_certifica | ite | 12315790 | | | | | cd:90:1b:7b:49:4 | i:1d: | | | | | 华东 1 | 服务器证书 | 9 | 改名称 | 859 |



应用场景

- 证书过期,需要创建新的证书。

- 负载均衡添加证书报错,可能是私钥内容错误,需要替换为新的满足需求的证书。

操作步骤

新建并上传一个新的证书。

详情参见生成证书和上传证书。

在HTTPS监听中配置新的证书。

详情参见配置HTTPS。

打开证书管理页面,找到目标证书,然后单击删除。

在弹出的对话框中,单击确认。



查看操作日志

负载均衡提供日志管理功能,您可以查看某个实例的操作日志和健康检查日志。

操作日志

负载均衡提供近一个月的操作日志信息。目前只支持控制台查看,不支持通过Open API获取这些日志。

健康检查日志

目前负载均衡只存储三天内的健康检查日志信息。如果您想存储更多的健康检查日志,需要设置日志存储。详情查看管理健康检查日志。

操作步骤

登录负载均衡控制台。

在左侧导航栏,单击日志管理。

在日志管理页面,单击日志查看页签。

类型选择操作日志。

查看所有负载均衡实例的操作日志,比如启动、添加、删除监听,添加后端服务器等操作日志。

您可以通过操作结果(成功或失败)过滤要查看的实例操作日志,也可以通过具体的资源ID快速地找 到指定资源的相关操作日志。资源ID是这次操作的主体对象的ID,例如负载均衡实例ID、证书ID、 虚拟服务器组ID、转发策略ID等。

| 日志管理 | | | | |
|---------------------|----------------|-------------|------|---|
| 日志查看日志存储 | | | | |
| 温馨提示:只提供3天以内的 | 日志数据,想保存更多日志,该 | 青立即前往 日志存储 | | |
| 类型 操作日志 ▼ | | | | |
| 资源ID ▼ | | 搜索 | | |
| 操作时间 | 操作详情 | | 操作结果 | RequestId |
| 2017-07-25 11:27:24 | 实例 lb-bp | 添加后端服务器 成功。 | 成功 | |
| 2017-07-25 11:27:08 | 实例 lb-bp | 移除后端服务器 成功。 | 成功 | COMPANY AND |
| 2017-07-25 11:25:14 | 实例 lb-bp | 添加后端服务器 成功。 | 成功 | |
| 2017-07-25 11:24:54 | 实例 lb-bp | 移除后端服务器 成功。 | 成功 | |
| 2017-07-25 11:24:41 | 实例 lb-bp | 泰加后端服务器 失败。 | 失败 | and broke the set of the |

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
- 查看健康检查日志
- 下载健康检查日志

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ECS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。

注意: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。

配置健康检查日志存储,您需要执行以下操作:

创建Bucket

授权日志访问

设置日志存储

创建Bucket

在设置日志存储前,您需要开通OSS服务并创建用来存储健康检查日志的bucket。

打开对象存储OSS产品页面,单击**立即开通**。

开通OSS服务后,登录OSS管理控制台。

单击新建Bucket。

| 对象存储 | 基础数据 | | | | | | | | | | | |
|---------------|--|--|----------------------------------|--|--|--|--|--|--|--|--|--|
| 概览 | () 总概览及 Bucket 概范基础数据都非实时数据,数据延迟 2-3 个 |) 急痛認及 Bucket 概認基础数据标准实时数据,数据延迟 2-3 个小时。 | | | | | | | | | | |
| 存储空间 十 23 | 存储总量 | 本月流量 流入 流出 CDN回源 | 本月请求次数 PUT GET | | | | | | | | | |
| Q 新建Bucket | 205.88мв | 25.11кв | 2万次 | | | | | | | | | |
| • 101 | High 0.00% T Have 0.00% | 上月便用息流量 0.00Byte | 上月便用思次数 3382次 | | | | | | | | | |
| | | | | | | | | | | | | |
| | 基础起置 | | | | | | | | | | | |
| | 域名管理 2 个Bucket已配置 | 事件通知 配置MNS事件通知(回调)功能,关注Bucket事件 | 跨区域复制 可实现账户内不同地域之间的Bucket同步暂份 | | | | | | | | | |
| | 安全令牌 通过RAM和STS为子账号授予临时的访问权限 | 安全扫描 可提供一键扫描APP漏洞和恶意代码服务 | | | | | | | | | | |
| | | | | | | | | | | | | |

在新建Bucket对话框,配置Bucket信息,单击确定。

注意:确保bucket的地域和负载均衡实例的地域相同。

更多Bucket配置的详细信息,查看创建存储空间。

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。

登录访问控制管理控制台。

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。

| 访问控制 RAM | 角色管理 | | Britatinet: C Riser |
|------------|---------------------------|---------------------|-------------------------|
| 概点 用户管理 | 角色名 ▼ SLBLogDefaulRole 論語 | | |
| \$1(1)钟词 | 角色玄称 | (c)(1)(1)(1) | 現作 |
| 策略管理 | SLBLogDefaultRole | 2017-07-06 19:10:28 | 御理 授权 副除 |
| 角色管理 | | | 共有1条,毎双型示:20条 & < 1 > > |

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。

| 编辑角色授权策略 | | | | × |
|--|-------|--------------------|--|----|
| 添加授权策略后,该角色即具有该条策略 搜索授权 精确授权 | 的权限,同 | 条 授权策略不 | 能被重复添加。 | |
| 可选授权策略名称 | 类型 | | 已选授权策略名称 | 类型 |
| OSS AliyunOSSReadOnlyAccess 只读访问开放存储服务(OSS)的权限 | Q | > < | AliyunOSSFullAccess 管理开放存储服务(OSS)权限 | |
| | | | 确定 | 关闭 |

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

| < | SLBLogDefaultRole | | | 编描授权策略 |
|--------|---------------------|-----------------|----|-------------|
| 角色详情 | | | | |
| 角色授权策略 | 授权策略名称 | 备注 | 理委 | 提作 |
| | AliyunOSSFullAccess | 管理开放存储服务(OSS)权限 | 系统 | 章君权限 解除授权 |

设置日志存储

登录负载均衡控制台。

在左侧导航栏,单击日志管理。

在日志管理页面,单击日志存储页签。

单击目标地域的**设置日志存储**链接。

| 日志管理 | | | |
|-----------|----|------------|--------|
| 日志查看 日志存储 | | | |
| 地域 | 状态 | 训练 | 题作 |
| 44db 1 | | 当前尚未设置日志存储 | 设置日志存植 |
| 44d); 2 | | 当前尚未设置日志存储 | 设置日志存储 |

在设置日志存储对话框,选择用来存储健康检查日志的Bucket,然后单击确认。

单击状态栏下的开关,开启日志存储。

| 日志管理 | | | |
|-----------|----|--------------------|--------|
| 日志宣看 日志存储 | | | |
| 地域 | 状态 | 评估 | 操作 |
| \$845 1 | 0 | 当前尚未设置日志存储 | 设置日志存储 |
| 44네는 2 | | 当前尚未设置日志存储 | 设置日志存储 |
| 华北 3 | 0 | 读地域暂不支持日志存储 | |
| 华东 1 | | 当前尚未设置日志存储 | 设置日志存储 |
| 华东 2 | | 所題Bucket: test0111 | 设置日志存储 |



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。

登录负载均衡控制台。

在左侧导航栏,单击日志管理。

在日志管理页面,单击日志查看页签。

类型选择健康检查日志,然后选择要查看的日志时间。

注意: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。

| 日志管理 | | |
|------------------------------|-------------------------------|--|
| 日志查看日志存储 | | |
| | | |
| 温馨远示:只适供3天以内的日本叙族,您保存更多日本,\$ | 1210时任 日本伊姆 | |
| 类型 健康检查日志 ▼ | | |
| 选择地域 华东 1 ▼ 选择日志时间 201 | 7-07-09 18 ▼ : 51 ▼ 至 2017-03 | -11 18 V : 51 V |
| 负载均衡ID 请精确输入ID进行检索 | 查询 | |
| 实例ID | 时间 | 日志详情 |
| lb-bp | 2017-07-10 15:54:42 | 80 to 9080 normal |
| lb-bp | 2017-07-10 15:54:42 | 80 to 9080 normal |
| lb-bp | 2017-07-10 15:54:42 | 80 to 9080 normal |
| lb-bp | 2017-07-10 15:54:42 | 80 to 9080 normal |
| lb-bp | 2017-07-10 15:54:51 | 80 to :9080 normal |
| lb-bp | 2017-07-10 15:54:51 | 80 to :9080 normal |
| lb-bp | 2017-07-10 15:54:51 | 80 to :9080 normal |
| lb-bp | 2017-07-10 15:54:52 | 80 to :9080 normal |
| lb-bp | 2017-07-10 15:54:52 | 80 to ::::::::::::::::::::::::::::::::::: |
| lb-bp | 2017-07-10 15:54:52 | 80 to :9080 normal |
| lb-bp | 2017-07-10 15:54:53 | 80 to ::9080 normal |
| lb-bp | 2017-07-10 15:54:53 | 80 to :9080 normal |
| b-22/ | 2017-07-10 22:40:41 |):8080 to :51229 abnormal; cause: HTTP code not match. |

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。

登录OSS管理控制台。

在概览页面,单击目标Bucket,然后单击Object管理。

在Object管理页面,单击健康检查日志文件夹AliyunSLBHealthCheckLogs/。

| and a | | 英型:标准存储 | 区域: 幼东 1 | 创建时间: 2017-07-06 19 | 13 删除 |
|-------|---|----------|----------|-------------------------|-------|
| 概范 | Object管理 基础设置 综合管理 图片处理 事件通知 基础数据 热点统计 API统计 Object统计 | | | | |
| 上传 | 新建文件共 副除 设置时行产先 執片管理(0) 期所 | | | 输入Object名前细匹配 | Q接款 |
| | 文件名 | 文件大小 | 存储英型 | 更新时间 | 操作 |
| | AlyunSLBHeathCheckLogs/ | | | | |
| | Cos/tabule | 0.057KB | 标准存储 | 2017-07-25 11:22:4 2 | 섬ૠ |
| | example (pg | 21.327KB | 标准存储 | 2017-07-28 17:14:4 7 | 1872 |

单击您要下载的健康检查日志的文件夹。
| 20 | | | | | | | | | | | |
|----|----|-------------|---------|-------------|------|---------|------|------|------|-------|----------|
| 概览 | | Object管理 | I | 基础设置 | 域名管理 | 图片处理 | 事件通知 | 基础数据 | 热点统计 | API统计 | Object统计 |
| 上传 | | 新建文件夹 | 删除 | 设置H | TTP头 | 碎片管理(0) | 刷新 | | | | |
| | 文件 | 洺 | | | | | | | | | |
| | t | 返回上级 (Aliy | unSLBHe | althCheckLo | gs/) | | | | | | |
| | | 20170725/ | | | | | | | | | |
| | | 20170727/ | | | | | | | | | |
| | | 20170728/ | | | | | | | | | |

单击目标文件的管理,然后单击复制文件 URL。

| ange . | 预览 × |
|--|--|
| 概范 Object管理 基础设置 域合管理 图片处理 事件通知 I 基础数据 | |
| 上传 新建文件夹 副除 设置州口P头 碎片管理(0) 刷新 | 此格式不支持预览 |
| ☑ 文件名 | |
| た 適同上級(AliyunSLBHealthCheckLogs/20170725/) | |
| ✓ 11 | 名称: 11 |
| | 地址: 链接有效时间 3600 秒 |
| | http://slbyh.oss-cn-hangzhoualijumac.com/Allyum SLBHealthCheckLogs/20170725/117Expires=1501 238088205SAccessRaydEntPAQHIbOO-5_8Dn 質制文件 URL 質制文件指任 |
| | 类型: application/octet-stream 设置HTTP头 |
| | Object ACL: 继承Bucket 设置读写权限 |

在浏览器中输入复制的URL,下载日志文件。

您可以使用API、SDK等其它方式下载日志文件,详情参考简单下载。

访问日志

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。

注意:只有七层负载均衡支持访问日志功能,目前开放的地域有:香港、亚太东北1(东京)、亚太东南1(新加坡)、亚太东南2(悉尼)、亚太东南3(吉隆坡)、亚太南部1(孟买)、美国东部1(弗吉尼亚)、美国西部1(硅谷)、中东东部1(迪拜)和欧洲中部1(法兰克福)。

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

前提条件

您已经创建了七层负载均衡。

2. 您已经开通了日志服务。

操作步骤

登录负载均衡管理控制台。

在左侧导航栏,单击日志管理 > 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。

注意: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。

| 负载均衡 | 访问日本 録北1 録北2 録北3 録北5 毎年1 毎年2 録用1 香港 型大东北1(东州) 型大东南1(新加坡) 型大东南2(居田) 型大东南2(居田) 型大东南2(居田) (居田) |
|--------|---|
| 实例管理 | 王文(昭和) * (第二人) 2010年11 (2010年12月11日) 1 (65日) 1 (65日) 1 (5日) 日本(16日) 1 (5日) |
| 证书管理 | 尚未进行角色授权 |
| 标签管理 | 开通后将进行RAM角色搜权确认,搜权后才能保证SLB可以将相关日志写入用户的SLS中。 |
| ▼ 日志管理 | 立即转代 |
| 摄作日志 | |
| 访问日志 | |

在访问日志页面,找到目标SLB实例,然后单击设置。

| 负载均衡 | 访问日志 | 华北 1 | 华北 2 | \$#dt 3 | 华北 5 | 华东 1 | 华东 2 | 华南 1 | 香港 | 亚太东北1(| (东京) | 亚太东南 1 | (新加坡) | | | | | |
|--------------------|----------|-----------|----------|---------|------------|---------------|-------|------|------|--------------------|------|-----------|-------|-------|------------|-----|-----|------|
| abs / 10 / 800 TET | | 亚太东南 | i 2 (悉尼) | 亚太东 | 南3 (吉隆 | 坡) 亚 | 太南部 1 | (孟买) | 美国东部 | 1 (弗吉尼亚) | 美国 | 西部 1 (硅谷) | | | | | | |
| 关闭自理 | | 中东东部 | 31(迪拜) | 欧洲中 | 部 1 (法主 | (売福) | | | | | | | | | | | | |
| | 负载均衡名 | 称 • | 请输入 | 实例名称 | 进行模糊 | 查询.多个 | N按,分隔 | 搜 | R. | | | | | | | | | |
| | ■ 64845 | (新TD/夕称 | | | 服务物制 | (余部) - | | | 5712 | 8米刑(全部)。 | | | 伊杰 | | SIS日主友 | Rž | | 揭作 |
| ▼ 日志管埋 | - Stars | 0010/1019 | | | 2003370241 | .(32.407) * | | | 1.21 | HOMCIEL (SECHIP) * | | | 1000 | | 0100101010 | 10 | | DETP |
| 操作日志 | Web | (3A1) | | | 47. | 82(公 网 | 习) | | 经经 | 电网络 | | | ❷ 运行中 | | | | | 设置 |
| 访问日志 | 批: 批: | 設置 | | | | | | | | | | | 共有1条, | 每页显示: | 10 ▼ 条 | « < | 1 > | » |
| 健康检查日志 | | | | | | | | | | | | | | | | | | |

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**立即创建**。确保Project的名称全局唯一。详情参见日志服务快速入门。

注意:确保Project的地域和负载均衡实例的地域相同。

| 日志设置 | | | | \times |
|------------|---|----------|----|----------|
| | | | | |
| 设置7层日志 | | | | |
| LogProject | | Logstore | | |
| slb | • | slblog | | • |
| | | | | |
| | | | 确认 | 关闭 |

配置数据接入。

您可以在配置完日志库后,单击**数据接入向导**链接根据向导进行配置,也可以单击**确认**,然后在日志服务控制台配置。本操作选择直接通过数据接入向导配置。



单击下一步。

| 1.选择数据类型 | > | 2.数据源设置 | | 3.查询分析 & 可視化 | > | 4.投递 & ETL |
|----------|--------------|-----------------------------------|------------------------------|----------------------------|----------|------------|
| LB 负载均衡 | | | | | | |
| | | | | | | |
| | | | SLB 负载均衡 | | | |
| | 负载均衡 (Server | Load Balancer) 是将访问流量根 均衡扩展了应 | 据转发策略分发到后端多6 7用的服务能力,增强了应 | 合云服务器(ECS实例)的流量的 用的可用件。 | 没控制服务。负载 | |
| | | | ❷ 您已开通负载均衡服务 | | | |
| | | | | | | |
| | | | RAM 授权 | | | |
| | | 建立分发规则之前需要通过 | TRAM给日志服务授权以方 | 更悠的日志库收集日志信息 | | |
| | | 0 | 您已授权日志服务分发日 | 志 | | |
| | | | | | | |
| | | | 建立分发规则 | | | |
| | | | | | | |

日志服务已预设了SLB所需的查询索引,单击下一步。

注意:开启索引后,日志服务会根据索引流量收取费用,详情参见日志服务产品定价。

| 1 | | \rightarrow | | 2.数据源设置 | | > | 3.查询分析&可规化 4.投递& ETL | |
|-------------------|------------|--|--------|--------------------|-------|-----------------------|---|------------------------------------|
| ◇☆歩21 国内: | | | | | | | 预选 | |
| EX850812 | | | | | | B封间)/IP | 内容 | |
| 七小可敏感 false | 分词符 |)[]{}?@&<>/:\n\t | | | | | body_bytes_sent:235_client_ip:35.185.158.47_host:papaorange.org_http_host:papaor ttp_referer:- http_user_agent:Mozilla/S.0 (Macintosh; Intel Mac OS X 10_13_3) AppleWe | ange.org bKit/537.3 |
| 键值索引属性: | | | | | | 18-02-07 11:1 4:34 | (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36 http_x_forwarded_for:- http_ - read_request_time:0 request_length:365 request_method:GET request_time:0, st_uri/ scheme:http server protocol:HTTP/1.1 slb vport:80 slbid:lb-004993av/Smr | _x_real_i 000 requ izmo990 : |
| 1.际数据键名称 | <u>#11</u> | 默认数据键名称 | 大小写敏感 | 分词符 | 开启统计 | log_service | $\label{eq:l_cipher} \begin{split} I_cipher:=ssl_protocol:=status:302 \ tcpinfo_rtt:180000 \ time:2018-02-07T11:14:34+(ream_addr:-upstream_response_time:-upstream_status:-vip_addr:47.252.50.19 \end{split}$ | 08:00 up 7 write_ |
| norty nytes ser • | long | OUUY_Dytes_sent | false | ¥. | | | esponse_time:0 hadv bates centr346 client in:200.126.126.7 heat:47.263.50.107 bits heat:47.263.5 | 0.107.64 |
| rient in • | Text | V clenc.p W boot | false | * ":=000288.cs | | | | .36 (KHT |
| | text | those http://www.sear.acent | false | * , /=ULL/1640CC / | | 18-02-07 09:4 | L, like Gecko) Chrome/57.0.2987.133 Safari/537.36 http_x_forwarded_for:- http_x_rea | il_ip:- n |
| | long | request length | INTOR: | | | 8:07 log service | i:/ scheme:https server_protocol:HTTP/1.1 slb_vport:443 slbid:lb-0xi4t9t9aw/Srrrzm | 1990 ssl |
| equest methor | text | request method | false | T | | | pher:ECDHE-RSA-AES128-GCM-SHA256 ssl_protocol:TLSv1.2 status:502 tcpinfo_rtt:63 2018-02-07T09:48:07+08:00 upstream addr:127.0.0.1:503 upstream response time: | 050 tim 0.000 u |
| request time 🔻 | double | ▼ request_time | | | | | tream_status:502 vip_addr:47.252.50.197 write_response_time:0 | |
| equest uni 🔻 | text | ▼ request uri | false | ▼ ,'";=()[]{}?@&<> | /:\n' | | | |
| thid 🔻 | text | ▼ slbid | false | ▼ ,'";=()[]{)?@&<> | /:\n' | | | |
| tatus 🔻 | lona | ▼ status | | | | | | |
| instream addr 🔻 | text | v upstream_addr | false | Ŧ | | | | |
| instream resni 🔻 | double | • upstream_respons | ie, | | | | | |
| | lona | ▼ upstream_status | | | | | | |

单击**确认**完成数据接入。 slblog 全返回日志库列表 投递 & ETL 开启投递 功能说明:把日志数据投递到大数据计算服务MaxCompute(原ODPS),进一步进行个性化BI分析及数据挖掘 查看帮助 功能说明:把日志数据数据自动归档到OSS,对日志进行长期存储,可以通过自建程序和更多系统(如E-MapReduce)消费OSS数据 查看帮助 功能说明:依托子函数计算题各,日老服务提供完式的全托管数据加工服务,通过配置一个FTL 30b,日老服务将在时获 取数据更新并就发函数执行:增量消费日老服务Logstore的数据,在函数里先成自定义加工任务,用于数据加工的函数可 以是日老服务提供的模板或者用户自定义函数 查看帮助 上一步 确认

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 |
| 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:

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。

| 访(| 问日志 | 亚太东南 | 頁 1 (新加坡 | t) Britter | 中部 1 (法 | 兰克福) | 华北 1 | 美国东部 1 (弗吉尼 | 亚) 亚太南部 1 (加 | 証买) 华北 2 | | | | |
|----|-----------------|--------|------------------|------------|---------|-------|--------|-------------|--------------|-----------------|---------|------|------|----|
| | | 华东 2 | 华南 1 | 亚太东北 | 1 (东京) | 华北 5 | 香港 | 亚太东南 2 (悉尼) | 美国西部1(硅谷) | | | | | |
| | | 中东东音 | 阝1 (迪拜) | 华北 3 | 华东 1 | 亚太东 | 南3 (吉隆 | 坡) | | | | | | |
| 负责 | 胧均衡名利 | × * | 清蝓〉 | 实例名称道 | 进行模糊查 | 间.多个的 | 皮,分隔 | 搜索 | | | | | | |
| | 负载均衡 | 蘄ID/名称 | | 服务 | 地址(全部 |) - | | 网络类型(全部) | - 1 | 迹 | SLS日志存储 | | | 操作 |
| | lb-0xiw: Web | 3x1lj | | 47. | 82(| 公网) | | 经典网络 | • | 运行中 | slb/slb | 查看日志 | 设置(: | 删除 |

日志服务控制台

在日志库页面,单击SLB日志库的查询选项。

| < | ◎ slb 電波回Proje | ct列表 | | | | | 地域:美国东部 | 郎 1 (弗吉尼亚) |
|--|----------------|---------------|------|--------------------------|------|------------------|------------|------------|
| 日志库 | Logstore列表 | | | | | | 查看Endpoint | 创建 |
| ▶ LogHub - 实时采集 | 请输入Logstore名进行 | 模糊查 搜索 | | | | | | |
| LogHub - 实时消费器 Search/Analytics | Logstore名称 | 教涙達入向号 | 吃肉 | 日去采作描述 | | 日志消费模式 | | 19.0= |
| ▶ LoaShipper - 投递 | Lugstore | 20003970999 | xlm. | HIBMORT | 日志消费 | 日志投递 | 查询分析 | 10611- |
| | slblog | 8 | ⊭ | Logtail配置(管理) 诊断 更多 - | 预览 | MaxCompute OSS | 查询 | 修改 删除 |

单击目标日志字段,查看对应的日志信息。

| 誌 slblog (尾于slb) | | | | 返回旧版 | 分享 | 查询分析属性 | 另存为快速查询 |
|------------------|--------|----------------|--|--------|--------|----------------------|----------------|
| 请输入关键字进行搜索 | | | 0 | 15分钟 ~ | 2018-0 | 02-02 22:58:16 ~ 201 | 18-02-02 23:15 |
| 200k 0 58分23秒 | 00分45秒 | | 03分15秒 05分45秒 | 08分15秒 | | 10分 | 45秒 |
| 原始日志 统计图表 | ī, | | 日志总条数:1,722,029 查询状态:结果精确 | | | | |
| 快速分析 | < | 时间 ▲▼ | 内容 ▼ | | | | C |
| body_bytes_s | 1 | 02-02 23:04:14 | source: log_service topic: body_bytes_sent: 612 client ic: 121.42 251 | | | | |
| host | | | host : 4750.197 http_host : 47.25 197 | | | | |
| http_user_agent | | | http_referer: - http_user_agent: PTS-HTTP-CLIENT | | | | |
| request_length | | | http_x_real_ip: - | | | | |
| request_method | | | request_length: 92 request_method: GET | | | | |
| request_time | | | request_time: 0.031 | | | | |

输入SQL语句查询特定的访问日志。

返回旧版 分享 查询分析属性 另存为快速查询 另存为非 slb-layer7-access-log (順子 log-analysis-us-east-1) 1小时 > 2018-01-31 21:20:02 ~ 2018-01-31 22:20 * | select http_user_agent, count(*) as pv group by http_user_agent order by pv desc limit 20 60k 0 21时20分 21时50分 22时10分 21时30分 21时40分 22时00分 228 日志总条数:1,059,537 查询状态:结果精确 查询行数:1,059,537 查询时间:209ms 原始日志 统计图表 [↓] ⊞ 🗠 🔟 🖻 🕒 123 🖓 Üü X%4: http_user_agent × ∨ 与 Y%4: pv × ∨ TS-H...LIENT Mozil...37.36 Go-ht...t/1.1 Mozil...37.36 axios/0.17.1 Flink-ak/sk alvi...CNDL) Mozil...37.36 d 4.4.4; 2014811 MIUI/V8.2.1.0.KHJ0 Alicd...imea2 x; U; A o pv: 52686 Mozil...-scan

比如通过* | select ip_to_province(client_ip) as client_ip_province, count(*) as pv group by client_ip_province order by pv desc limit 50查询Top20的客户端。

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。

在日志服务控制台,单击负载均衡的Project链接。

在左侧导航栏,单击Search/Analytics - 查询分析 > 仪表盘,然后单击查看。

| < | Slb €返回Project涉 表 | 地域:美国东部 1 (弗吉尼亚 |
|----------------------|--------------------------------|--|
| 日志库 | 仪表盘 | 查看Endpoint |
| LogHub - 实时采集 | | |
| LogHub - 实时消费 | 搜索 | |
| Search/Analytics - 奇 | Dashboard名称 | [[[1]]][[1]]][[1]][[1]][[1]][[1]][[1]] |
| | slblog-slb-accesslog-dashboard | 查看 删除 |
| 快速查询 | | |
| 报警配置 | | 共有1条,每页显示:10条 《 < <u>1</u> > » |
| 仪表盘 | | |

您可以通过仪表盘查看TOP客户端、TOP Host、状态码PV等信息。

| accesslog-d | ashboard (届于sib) | | | | 编辑 | 周新 重置时间 分享 全屏 |
|------------------|------------------|---------|---------|---------------|---------------|---------------|
| 最近: 1分钟 15分钟 1小时 | 4小时 1天 1周 | | | | | ○ 自动用限 |
| + Add a filter | | | | | | |
| TOP客户端ip | | | | | | 最近1天 🗸 🦯 |
| 客户端ip | pv | 区域 | 城市 | 运营商 | 返回给客户端流量 (MB) | 发送报文流量 (MB) |
| | 2962787 | 山东省 | 青岛市 | 阿里云 | 1355.22 | 259.95 |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| 状态码分布 | | 最近 | 丘1天 ∨ ↗ | upstream状态码分布 | | 最近1天 > ス |
| | 0.00%0.00% | | | | | |
| | | | | | | |
| | | | • 404 | | | • 200 |
| 50.26% | | | • 503 | 49 74% | | • 500 |
| 50.20% | | 4017470 | • 500 | 40.7476 | | • 404 |

关闭访问日志

登录负载均衡管理控制台。

在左侧导航栏,单击日志管理 > 访问日志。

找到目标负载均衡实例,然后单击删除关闭日志访问功能。

| 负载均衡 | 访问日志 | 华北 3 🔄 | 华北 5 香港 | 亚太东北1(东京 |) 亚太东南 1 (新加坡) | 亚太东南 2 (悉尼 |) | | | |
|--------|-----------------|--------|----------|-------------|----------------|------------|--------------------|--------|-----|----|
| | | 亚太东南3 | (吉隆坡) 🔟 | 2太南部 1 (孟买) | 美国东部 1 (弗吉尼亚) | 美国西部1(硅谷) | 中东东部1(迪拜) | | | |
| 实例管理 | | 欧洲中部 | 1 (法兰克福) | | | | | | | |
| 证书管理 | | | | | | - | | | | |
| 标签管理 | 负载均衡名 | 称 • | 请输入实例 | 名称进行模糊查询.多 | 8个按,分隔 搜索 | | | | | |
| ▼ 日志管理 | □ 负载均 | 僑ID/名称 | 服务地 | 址(全部) 👻 | 网络类型(全部) 👻 | 状态 | SLS日志存储 | | | 攝作 |
| 攝作日志 | Ib-0xiv Web | v3x1lj | 47. | 82(公网) | 经典网络 | ❷ 运行中 | slb/slblog | 查看日志 | 设置 | 删除 |
| 访问日志 | | | | | | | | | | |
| 健康检查日志 | 山北山 | 設置 | | | | 共有19 | ē, 每贝显示: <u>10</u> | r∰ ≪ < | 1 > | >> |

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。

1. 主账号授权日志服务访问SLB

使用主账号登录负载均衡控制台。

在左侧导航栏, 单击日志管理 > 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。



2. 主账号创建授权策略

登录访问控制RAM控制台。

在左侧导航栏,单击策略管理,然后单击新建授权策略。

| 访问控制 RAM | 授权策略管理 | | 新建授权策略 | € 刷新 |
|------------|---------------------|-----------------|--------|------|
| 概览 用户管理 | 系统授权策略 自定义授权策略 | | | |
| 群組管理 | 策略名或备注 ▼ 请输入关键词查询 | 投去 | | |
| 東南日注 | 授权策略名称 | 备注 | 被引用次数 | 操作 |
| 用巴吉理 | AdministratorAccess | 管理所有阿里云资源的权限 | 27 | 查看 |
| ×= | AliyunOSSFullAccess | 管理对象存储服务(OSS)权限 | 4 | 查看 |

单击空白模板。

| 创建授权策略 | × |
|---|---|
| STEP 1: 选择权限策略模板 STEP 2: 编 | 編权限并提交 🛛 🔪 STEP 3 : 新建成功 |
| 全部模板 ▼ 请输入关键词在下方模板中动态筛选 | |
| 空白模板 | S统 AdministratorAccess 管理所有阿里云资源的权限 |
| 系统 AliyunOSSFullAccess管理对象存储服务(OSS)权限 | 系统 AliyunOSSReadOnlyAccess 只读访问对象存储服务(OSS)的权限 |
| 系统 AliyunECSFullAccess 管理云服务器服务(ECS)的权限 | 系統 AliyunECSReadOnlyAccess 只读访问云服务器服务(ECS)的权限 |
| 系統 AliyunRDSFullAccess管理云数据库服务(RDS)的权限 | 系统 AliyunRDSReadOnlyAccess 只读访问云数据库服务(RDS)的权限 |

{ "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" },

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。

| { "Action": ["ram:Get*", "ram:ListRoles"], "Effect": "Allow", "Resource": "*" }], "Version": "1" | | |
|--|----------------------------|---------------|
| 创建授权策略 | | × |
| STEP 1:选择权限策略 | 羹板 STEP 2 : 编辑权限并提交 | STEP 3:新建成功 |
| * 授权策略名称: | SlbAccessLogPolicySet | |
| | 长度为1-128个字符,允许英文字母、数字,或"-" | |
| 备注: | | |
| 策略内容: | <pre>50], 51</pre> | × |
| | 授权策略格式定义 | |
| | | |
| | | 上一步 新建授权策略 取消 |
| | | |

3. 主账号给子账号授权

在访问控制RAM控制台的左侧导航栏,单击用户管理。

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。

| 访问控制 RAM | 用户管理 | | | 新建用户 | ℃刷新 |
|-----------|-------------|----|---------------------|---------|-----------|
| 概览 | 用户名 ▼ ya | | 證案 | | |
| 2963 1011 | 用户名/显示名 | 备注 | 创建时间 | | 攝作 |
| 策略管理 | ya yange | | 2017-05-24 15:08:27 | 管理 授权 | 删除 加入组 |

搜索已创建的策略,然后选择该策略授权给目标用户。

| 编辑个人授权策略 | | | | | × |
|---|---------|---------|----------|----|----|
| 添加授权策略后,该账户即具有该条策略 | 的权限,同一条 | 授权策略不能被 | 重复添加。 | | |
| 可选授权策略名称 | 类型 | | 已选授权策略名称 | | 类型 |
| SLB 1 | ۹ | | | | |
| AliyunSLBFullAccess 管理负载均衡服务(SLB)的权限 | 系统 | 3 | | | |
| AliyunSLBReadOnlyAccess 只读访问负载均衡服务(SLB)的权限 | 系统 | < | | | |
| SlbAccessLogPolicySet - | 自定义 | | | | |
| | | | | | |
| | | | | | |
| | | | | 确定 | 关闭 |

单击**确定**。

| 编辑个人授权策略 | | | | × |
|---|--------|---------|-----------------------|------|
| 添加授权策略后,该账户即具有该条策略的 | 权限,同一务 | 受权策略不能被 | 重复添加。 | |
| 可选授权策略名称 | 类型 | | 已选授权策略名称 | 类型 |
| SLB | ۹ | | SIbAccessLogPolicySet | 自定义 |
| AliyunSLBFullAccess 管理负载均衡服务(SLB)的权限 | 系统 | > | • | |
| AliyunSLBReadOnlyAccess 只读访问负载均衡服务(SLB)的权限 | 系统 | < | | |
| | | | | |
| | | | | |
| | | | | |
| | | | ₹ | 定 关闭 |

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。

| < | | 编辑授权策略 | | |
|--------|-----------------------|--------|-----|---------------|
| 用户详情 | | | | 编辑个人授权策略成功 × |
| 用户授权策略 | 个人授权策略 加入组的授权策略 | | | 用户策略列表刷新 成功 × |
| 用户加入的组 | 授权策略名称 | 备注 | 类型 | 操作 |
| | SibAccessLogPolicySet | | 自定义 | 查看权限 解除授权 |
| | | | | |

监控

监控说明

如果负载均衡开启了健康检查功能,并且后端ECS实例的健康检查状态正常,您就可以在控制台查看负载均衡 服各项监控指标的实时数据和历史数据。



登录负载均衡管理控制台。

单击目标实例的ID链接。

在左侧导航栏,单击**监控**。

选择要查看的监控指标,查看监控数据。



监控指标

| 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 | - 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。 |
|---------------------------------------|--|
| 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 | - 丟弃入流量:每秒丟失的入流量。 - 丟弃出流量:每秒丢失的出流量。 |
| 丟弃数据包 | - 丟弃流入数据包:每秒丟弃的流入数据包 的数量。 - 丟弃流出数据包:每秒丟弃的流出数据包 的数量。 |
| 丢弃连接数 | 每秒丢弃的连接数。 |
| 7层协议QPS | 每秒可以处理的HTTP/HTTPS请求。 注意 :只有7层(HTTP/HTTPS)监听才有该监控 指标。 |
| 7层协议RT | 负载均衡的平均响应时间。 注意 :只有7层(HTTP/HTTPS)监听才有该监控 指标。 |
| 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。 注意 :只有7层(HTTP/HTTPS)监听才有该监控 指标。 |
| 7层协议UpstreamCode4XX/5XX | 后端服务器返回的HTTP响应代码的数量。 注意 :只有7层(HTTP/HTTPS)监听才有该监控 指标。 |
| 7层协议UpstreamRT | 后端服务器的平均响应时间。 |

注意:只有7层(HTTP/HTTPS)监听才有该监控指标。

设置报警规则

开通云监控服务后,您可以在云监控控制台配置监控报警规则。云监控支持"短信"、"邮件"、"旺旺"三种报警方式,暂不支持电话报警。关于云监控的更多详细信息,参考云监控文档。

注意: 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

登录负载均衡控制台。

选择地域,然后单击目标实例的ID链接。

确保该实例已经配置了监听,开启了健康检查。

在详情页面左侧导航栏,单击监控,进入监控页面。

单击阈值报警设置,进入云服务监控页面。

| 220 | 第25年第2 * * * * 近日成为引来 | | | | | HEREICE | 的往此实例控制品 | CRM |
|---------------------------|-----------------------|-------------|----|-------------------------|------|----------------|----------|-----|
| 概范 | | | | | | | | |
| Dashboard | 金拉图表 报警规则 | | | | | | | |
| Desiluteru | 規則名称 状态(全部) * | 日用 血控環(全部)・ | 建度 | 报警规则 | 通知对象 | | | 操作 |
| 应用分编 | | | | | | | | |
| 日志监控 | | | | | | | | |
| 站中管理 | | | | 目前还没有按督规则,您可以应由 这里 活动一个 | | | | |
| 云服务监控 | | | | | | | | |

单击**创建报警规则**。

配置报警规则。

详情参考负载均衡监控配置。

| 管理投制台 产品与服务▼ | ۹.85 |
|--|---|
| 40) <u>* 100</u> | |
| 关款失道 | |
| 产品: | |
| 近岸活動: 二二〇〇 - 〇 | |
| 地域: 华东1 * | |
| 廣例: lb-bp1mt8kin77mmth | |
| 2015年2月1日 2015年2月1日 | |
| | |
| RUE | 1.00 |
| 「現別版法: 調口活動通用数 * 5分钟 * 干均価 * >= * 尚重 Count | 0.50 |
| | 0.00 |
| +添加很要规则 | -0.50 |
| 陽線几次最近 展値供授器: 1 ● | 150 |
| 金38时间: 00:00 · 至 23:59 · | 15,00000 10000100 10000100 1000000 1000000 ● 第二国現活機器 — 平均重一-15-0pLon(5k)L1/77monthybt6 |
| When a start of the start of th | |
| 20075 | |
| | |
| GPU Jacké | |
| 云张母报楹联版人 | |
| 快速保健联系人们 | |
| 0007999 - 0000_0001_0001000 | |
| SERVICE PLANA LA DEPARTO | |
| | |
| and Rea | |
| | |

负载均衡多可用区

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。

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。

注意:

每个地域只有一种属性,不是多可用区就是单可用区。

实例创建后,不能修改主备可用区。

| 地域 | 可用区类型 | 可用区 | | | | |
|-----|-------|------|------|--|--|--|
| 华东1 | | 主可用区 | 备可用区 | | | |
| | 多可用区 | 可用区B | 可用区D | | | |
| | | 可用区D | 可用区E | | | |
| | | | | | | |

| | | 可用区E | 可用区F | | |
|-------|------|------|-----------|--|--|
| | | 可用区F | 可用区E | | |
| | | 主可用区 | 备可用区 | | |
| | | 可用区A | 可用区B | | |
| 华东2 | 多可用区 | 可用区B | 可用区A或可用区D | | |
| | | 可用区C | 可用区B | | |
| | | 可用区D | 可用区B | | |
| | | 主可用区 | 备可用区 | | |
| 化击1 | 夕可田区 | 可用区A | 可用区B | | |
| 平肖⊥ | 多可用区 | 可用区B | 可用区A | | |
| | | 可用区C | 可用区B | | |
| | | 主可用区 | 备可用区 | | |
| 华北1 | 多可用区 | 可用区B | 可用区C | | |
| | | 可用区C | 可用区B | | |
| | | 主可用区 | 备可用区 | | |
| 华北2 | | 可用区A | 可用区B或可用区D | | |
| | 多可用区 | 可用区B | 可用区A或可用区C | | |
| | | 可用区C | 可用区B | | |
| | | 可用区D | 可用区A | | |
| 华北3 | 单可用区 | 可用区A | | | |
| 华北5 | 单可用区 | 可用区A | | | |
| 欧洲中部1 | 单可用区 | 可用区A | | | |
| 中东东部1 | 单可用区 | 可用区A | | | |
| | | 主可用区 | 备可用区 | | |
| 新加坡 | 多可用区 | 可用区A | 可用区B | | |
| | | 可用区B | 可用区A | | |
| 亚太东南2 | 单可用区 | 可用区A | | | |
| 亚太东南3 | 单可用区 | 可用区A | | | |
| 亚太东北1 | 单可用区 | 可用区A | | | |
| | | 主可用区 | 备可用区 | | |
| 香港 | 多可用区 | 可用区B | 可用区C | | |
| | | 可用区C | 可用区B | | |
| 美东1 | 单可用区 | 可用区A | | | |

| 美西1 | | 主可用区 | 备可用区 |
|-----|------|------|------|
| | 多可用区 | 可用区A | 可用区B |
| | | 可用区B | 可用区A |

多可用区与高可用

除了选择具有多可用区的地域实现同城容灾外,也建议用户可以结合自身的应用需要,综合考虑后端服务器部 署来实现更可靠的同地域高可用的方案。

比如,您可以将后端服务器ECS实例分别部署在主备可用区内,如下图所示。



当可用区A未出现故障时,用户访问流量如上图蓝色实线所示;当可用区A发生故障时,用户访问流量的分发将 变成如上图黑色虚线所示,这样就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。

各地域带宽峰值限制

负载均衡各地域的包年包月可售卖最大带宽和按流量实例带宽峰值如下表所示。

注意:所有地域的私网带宽峰值都为5 GB。

| 地域 | 带宽峰值 |
|-------------|-------|
| 华北1(青岛) | 5 GB |
| 华东1(杭州) | 5 GB |
| 华北 2 (北京) | 5 GB |
| 华东 2 (上海) | 5 GB |
| 华南1(深圳) | 5 GB |
| 华北3(张家口) | 5 GB |
| 华北5(呼和浩特) | 5 GB |
| 香港 | 2 GB |
| 美国东部1(弗吉尼亚) | 1 GB |
| 美国西部1(硅谷) | 2 GB |
| 亚太东北1(东京) | 1 GB |
| 亚太东南1(新加坡) | 5 GB |
| 亚太东南2(悉尼) | 1 GB |
| 亚太东南3(吉隆坡) | 5 GB |
| 中东东部1(迪拜) | 500 M |
| 欧洲中部1(法兰克福) | 1 GB |
| 亚太南部 1 (孟买) | 5 GB |

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。

说明: 该功能目前已在青岛、北京、杭州、上海、深圳、香港、新加坡、美东和美西地域上线。

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。

更多信息,查看DDoS基础防护文档。

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:

登录负载均衡管理控制台。

选择地域,查看该地域的所有实例。

将鼠标移至目标实例的云盾图标,查看BPS清洗阈值、PPS清洗阈值和黑洞阈值。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。

| 关于负载均 阿里云负载 知,关于他 | 关于各种教授教授的规则。 图整于各种学校研究的社会社研究社会研究社会研究社会研究社会研究社会研究社会研究社会研究社会研究社会研 | | | | | | | | | | | | | | | | | | | | | | | |
|-------------------------|--|--|--------------|--------------------------------|---|------------------------------|-------|--------|----|----------|--------|----------|-------|-----|----------|--|--|-------------|--------|---------|---------|-------------------------------|---|------------|
| 实例管理 | 缘北 中东3 | 1 年 年 11 年 11 年 11 年 11 年 11 年 11 年 11 | dt 2 (迪拜) | 유지는 3 (2019년 19 | 华北 5 🕺 夢 1 (法兰克 | ¥东1 4 [補] | ¥东 2 | 絊南 1 | 普港 | 亚太东北 1 (| (东京) 亚 | 太东南 1 (新 | i加坡) | 亚太东 | 南 2 (悉尼) |) 型太东南3(| 吉隆坡)(| 美国东部 1 (弗吉尼 | 2) 美国西 | 部1(建谷) | | C # | 新 | 8825464986 |
| 负载均衡名 | 国称 | ٣ | 谢船 | (实例名称) | 进行模糊查 | 词.多个按 | 5分隔 | 83 | • | •标签 | | | | | | | | | | | | | | <u>a</u> 0 |
| □ 负载均衡 | fiD/名称 | | | 可用区 | | 1823 | 务地址(: | 全部) 🗸 | | 状态 | 网络类型(; | 全部) 👻 | 第日/朝 | 建设查 | | 后她服务 | 6 | 标签 | 实例规格 | 带宽计裁方式(| 全部) → (| 対義方式(全部) ▼ | | 操作 |
| acs-slb-c | 2j9yz ca5ce0co | :a9 | , | BPS清洗 PPS清洗 屏洞肉值 详情请见 | 奇儀: 6144 奇信: 15360 : 7.68 Gbpi 云盾DDoSI | Mbps 100 s M3PI2#Iá | 5.31. | 36(公网) | | 9 运行中 | 经共网络 | | TCP : | 80 | 正常 | caSceOcca caSceOcca caSceOcca caSceOcca | 19da346 19da346 19da346 19da346 | 未绑定 | 性能共享型 | 按使用流量 | # 2 | 安量付薨 2017-11-28 10:04:34 创 | 建 | 管理 更多 |

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。

使用主账号登录访问控制RAM管理控制台。

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。

| 访问控制 RAM | 用户管理 | | | 新建用户 | € 刷新 |
|----------|-----------------|-------------------|---------------------|---------|--------------|
| | | | | | |
| 概览 | 田白夕 ▼ 浩協〉田白夕洪行期 | ^{期告询} 搜索 | | | |
| 用户管理 | 107 Jet | 1023LC (H) | | | |
| 群组管理 | 用户名/显示名 | 备注 | 创建时间 | | 攝作 |
| 策略管理 | acs_ram_account | | 2017-12-28 14:54:35 | 管理 授权 | ! 删除 加入组 |

单击用户授权策略,然后单击编辑授权策略。

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**。

| 编辑个人授权策略 | | | | × |
|--------------------------------|-------|---------|--|----|
| 添加授权策略后,该账户即具有该条策略 | 的权限,同 | 一条授权策略不 | 能被重复添加。 | |
| 可选授权策略名称 | 类型 | | 已选授权策略名称 | 类型 |
| AliyunYundunDDosReadOnlyAccess | م | | AliyunYundunDDosReadOnlyAccess 只读访问云盾DDos基础防护(Ant | 系统 |
| | | > | | |
| | | | 确定 | 关闭 |