

负载均衡

后端云服务器

产品文档



腾讯云

【 版权声明 】

©2013–2020 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 商标声明 】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100。

文档目录

后端云服务器

后端云服务器概述

管理后端云服务器

绑定弹性网卡

跨地域绑定2.0（新版）

跨地域绑定1.0（旧版）

混合云部署

后端云服务器的安全组配置

后端云服务器

后端云服务器概述

最近更新时间：2020-02-11 17:19:53

什么是后端云服务器

后端云服务器是创建负载均衡实例后，绑定在负载均衡上处理相应转发请求的 [CVM 实例](#)。在配置 [负载均衡监听器](#) 时，需绑定 CVM 实例作为后端服务器，CLB 通过不同的 [轮询方式](#)，将请求转发到后端云服务器上，并由 CVM 来做处理，保证应用平稳可靠的运行。您可在负载均衡实例所在的地域内的单个或多个可用区中，绑定 CVM 实例，以增加应用程序的健壮性，屏蔽单点故障。

注意事项

在添加后端服务器时，我们建议您：

- 在要添加到负载均衡上的所有 CVM 实例上，安装 Web 服务器（如 Apache 或 IIS），并保持运行应用程序的一致性。
- 建议您开启 [会话保持](#) 功能，使负载均衡维持一个较长时间的 TCP 连接并使多个请求重用它，可减少 Web 服务器上的负载并提高负载均衡的吞吐量。
- 确保后端实例的安全组具有针对负载均衡监听器端口和健康检查端口的入站规则，详情请参见 [后端服务器的访问控制](#)。

管理后端云服务器

最近更新时间：2020-09-08 11:07:07

负载均衡将请求路由至运行正常的后端云服务器实例，首次使用负载均衡或根据业务需求，需要增加或删除后端服务器数量时，可按照本文指引进行操作。

前提条件

需已创建负载均衡实例并配置监听器，详情请参见 [负载均衡快速入门](#)。

操作步骤

添加负载均衡后端云服务器

说明：

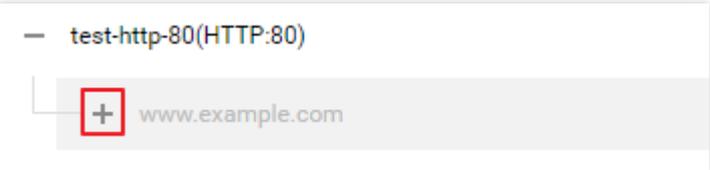
- 如果负载均衡实例与某个弹性伸缩组关联，则该组中的云服务器会自动添加至负载均衡后端云服务器。若从弹性伸缩组移除某云服务器实例，则该云服务器实例会自动从负载均衡后端云服务器中删除。
- 如需使用 API 添加负载均衡后端服务器，请参见 [绑定后端服务器到负载均衡](#) 接口说明。

1. 登录 [负载均衡控制台](#)。
2. 在“实例管理”页面的“负载均衡”页签中，单击目标负载均衡实例右侧操作列的【配置监听器】。
3. 在配置监听器模块中，选择需要绑定后端云服务器的监听器。
 - HTTP/HTTPS 监听器
 - a. 在 HTTP/HTTPS 监听器区域，单击目标监听器左侧的+。



+ test-http-80(HTTP:80)

- b. 在展开的域名左侧单击+。



- test-http-80(HTTP:80)
+ www.example.com

c. 选中展开的 URL 路径，单击【绑定】。



o TCP/UDP/TCP SSL 监听器

在 TCP/UDP/TCP SSL 监听器模块的左侧列表中，选中需要绑定后端云服务器的监听器，单击【绑定】。



4. 为负载均衡实例绑定后端服务。

- o **方式1:** 在“绑定后端服务”弹出框中，单击【云服务器】，选择需要关联的云服务器（可多选），并填写相关云服务器需要被转发的端口与权重，详情请参见 [服务器常用端口](#)，单击【确定】。

② 说明:

- 在“绑定后端服务”弹出框中仅展示同地域、相同网络环境、未被隔离、未过期、带宽（峰值）不为0的可选云服务器。
- 绑定多个后端服务器时，CLB 将按 Hash 算法转发流量，起到均衡负载的作用。
- 权重越大转发的请求越多，默认为10，可配置范围为0 - 100。当权重设置为0，该服务器不会再接受新请求。如开启会话保持，可能会造成后端服务器的请求不均匀，详情请参见 [均衡算法选择与权重配置实例](#)。

绑定后端服务

请选择实例

云服务器 弹性网卡 请输入默认端口

IP地址 按照IP地址搜索, 关键字

ID/实例名

10 条/页 1 / 2页

支持按住 shift 键进行多选

已选择 (2)

ID/实例名	端口	权重	
	80	10	添加端口 删除
	85	11	添加端口 删除

确认 取消

- 方式2: 如需批量绑定服务器且预设端口值一致时, 可在“绑定后端服务”弹出框中, 单击【云服务器】, 并输入默认端口值 (端口选择请参见 [服务器常用端口](#))、再勾选相关服务器并设定权重值, 单击【确定】。

绑定后端服务

请选择实例

云服务器 弹性网卡 80

IP地址 按照IP地址搜索, 关键字

ID/实例名

10 条/页 1 / 2页

支持按住 shift 键进行多选

已选择 (2)

ID/实例名	端口	权重	
	80	10	添加端口 删除
	80	11	添加端口 删除

确认 取消

修改负载均衡后端服务器权重

后端服务器权重决定了云服务器被转发的请求相对数量，在绑定后端云服务器时，需要预设权重信息，接下来将以“HTTP/HTTPS 监听器”为例（TCP/UDP/TCP SSL 监听器的修改方式相同），为您介绍如何修改负载均衡后端服务器权重。

② 说明：

- 如需使用 API 修改负载均衡后端服务器权重，请参见 [修改负载均衡器后端服务器权重](#) 接口说明。
- 有关负载均衡后端服务器权重的更多信息，请参见 [负载均衡轮询方式](#)。

1. 登录 [负载均衡控制台](#)。
2. 在“实例管理”页面的“负载均衡”页签中，单击目标负载均衡实例右侧操作列的【配置监听器】。
3. 在 HTTP/HTTPS 监听器模块左侧列表中，展开实例与监听器规则，选中 URL 路径。



4. 在 HTTP/HTTPS 监听器模块右侧服务器列表中，修改相关服务器权重。

② 说明：

权重越大转发的请求越多，默认为10，可配置范围为0 - 100。当权重设置为0，该服务器不会再接受新请求。如开启会话保持，可能会造成后端服务器的请求不均匀，详情请见 [均衡算法选择与权重配置实例](#)。

◦ 方式1：单独修改某台服务器权重。

- a. 找到需要修改权重的服务器，并将鼠标悬浮于对应权重上方，单击  编辑按钮。



- b. 在“修改权重”弹窗中，输入修改后的权重值，单击【提交】。

◦ 方式2：批量修改某些服务器权重。

🔍 说明：

如需使用 API 修改负载均衡后端服务器端口，请参见 [修改监听器绑定的后端机器的端口](#) 接口说明。

1. 登录 [负载均衡控制台](#)。
2. 在“实例管理”页面的“负载均衡”页签中，单击目标负载均衡实例右侧操作列的【配置监听器】。
3. 在 HTTP/HTTPS 监听器模块左侧列表中，展开实例与监听器规则，选中 URL 路径。



4. 在 HTTP/HTTPS 监听器模块右侧服务器列表中，修改相关服务器端口，端口选择请参见 [服务器常用端口](#)。
 - 方式1：单独修改某台服务器端口。

a. 找到需要修改端口的服务器，并将鼠标悬浮于对应端口上方，单击  编辑按钮。

<input type="checkbox"/>	CVM ID/名称	端口健康状态 ⓘ	IP地址	端口	权重	操作
<input type="checkbox"/>		异常		85 	10 	解绑
<input type="checkbox"/>		健康		80	11	解绑

b. 在“修改端口”弹窗中，输入修改后的端口值，单击【提交】。

方式2: 批量修改某些服务器端口。

 说明：
批量修改端口后的服务器端口相同。

a. 单击服务器前方复选框，选中多台服务器，在列表上方，单击【修改端口】。

<input checked="" type="checkbox"/>	CVM ID/名称	端口健康状态 ⓘ	IP地址	端口	权重	操作
<input checked="" type="checkbox"/>		异常		85	10	解绑
<input checked="" type="checkbox"/>		健康		80	11	解绑

b. 在“修改端口”弹窗中，输入修改后的端口值，单击【提交】。

解绑负载均衡后端服务器

负载均衡控制台支持解绑已绑定的后端服务器，接下来将以“HTTP/HTTPS 监听器”为例（TCP/UDP/TCP SSL 监听器的解绑方式相同），为您介绍如何解绑已绑定的负载均衡后端服务器。

-  说明：
- 解绑后端服务器会解除负载均衡实例与云服务器实例的关联关系，且负载均衡会立即停止对其的请求转发。
 - 解绑后端服务器不会对云服务器的生命周期产生任何影响，您也可以再次将它添加至后端服务器集群中。

- 如需使用 API 解绑负载均衡后端服务器，请参见 [从负载均衡监听器上解绑后端服务](#) 接口说明。

- 登录 [负载均衡控制台](#)。
- 在“实例管理”页面的“负载均衡”页签中，单击目标负载均衡实例右侧操作列的【配置监听器】。
- 在 HTTP/HTTPS 监听器模块左侧列表中，展开实例与监听器规则，选中 URL 路径。



- 在 HTTP/HTTPS 监听器模块右侧服务器列表中，解绑已绑定的后端服务器。
 - 方式1：单独解绑某台服务器。**
 - 找到需要解绑的服务器，在右侧操作栏，单击【解绑】。



- 在“解绑”弹窗中，确认解绑的服务，单击【提交】。

- 方式2：批量解绑某些服务器。**

- 单击服务器前方复选框，选中多台服务器，在列表上方，单击【解绑】。



- 在“解绑”弹窗中，确认解绑的服务，单击【提交】。

绑定弹性网卡

最近更新时间：2020-03-12 10:33:28

弹性网卡简介

弹性网卡 (Elastic Network Interface, ENI) 是一种可以绑定私有网络内 CVM 实例上的虚拟网卡。弹性网卡可以自由地在相同私有网络、可用区下的 CVM 间自由迁移，通过弹性网卡可以实现高可用集群搭建、低成本故障转移和精细化的网络管理。

CLB 的后端服务支持 CVM 和 ENI，即 CLB 支持绑定 CVM 和 ENI。CLB 与后端服务之间使用内网通信，当 CLB 绑定多台 CVM 和 ENI 时，访问流量会被转发到 CVM 的内网 IP 和 ENI 的内网 IP 上。

前提条件

ENI 必须先绑定在某台云服务器上，CLB 才能绑定该 ENI。CLB 只做负载均衡转发流量，并不实际处理业务逻辑，因此需要计算资源 CVM 实例来处理用户请求。请前往 [弹性网卡控制台](#)，将所需的弹性网卡与云服务器做绑定。

弹性网卡 华南地区 (广州) 全部私有网络 弹性网卡帮助文档

ID/名称	网卡属性	所属网络	所属子网	绑定云服务器	内网IP	IPv6 地址	创建时间	操作
	辅助网卡			-	2	0	2019-08-19 0...	绑定云服务器 编辑标签 删除
	辅助网卡			-	2	0	2019-10-30 11...	绑定云服务器 编辑标签 删除

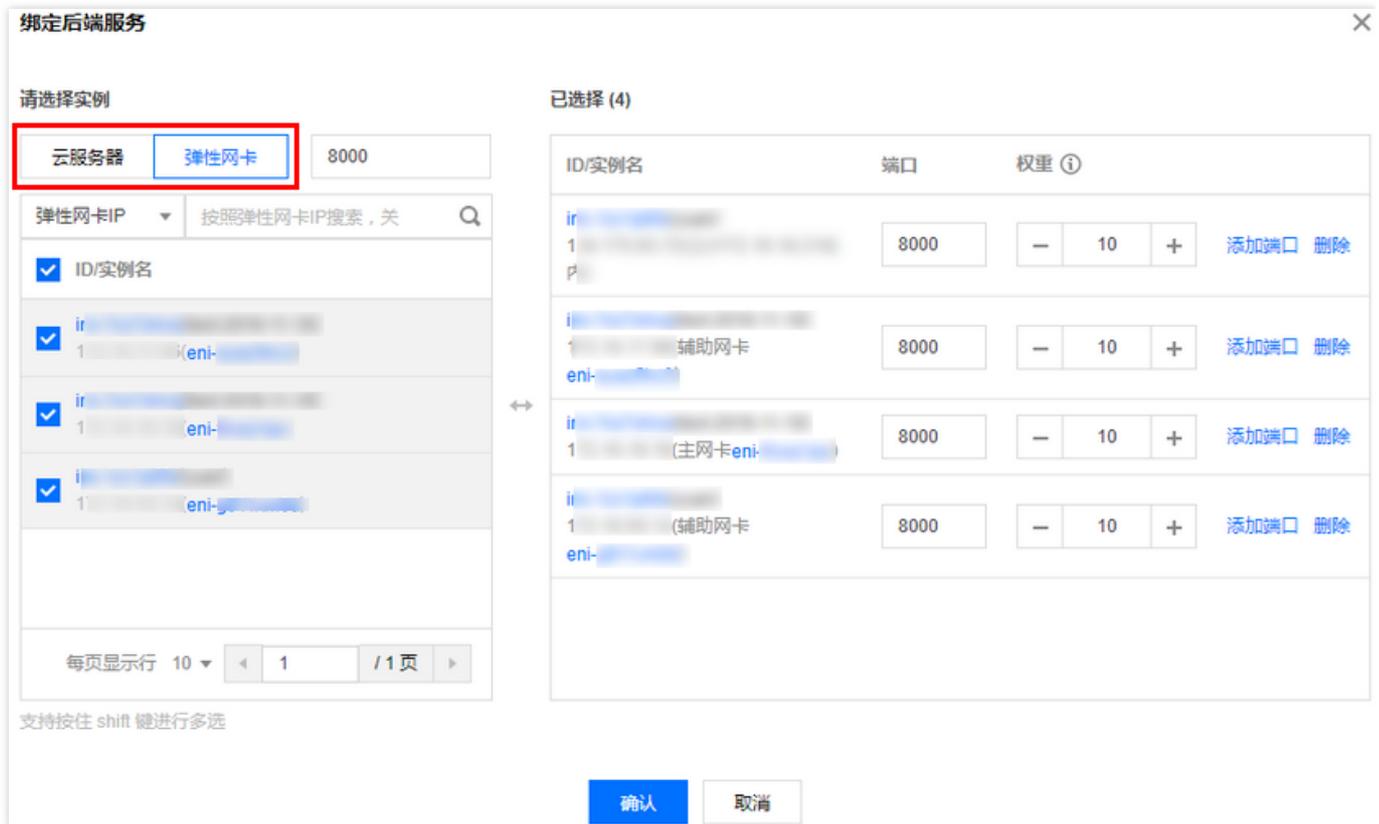
操作步骤

1. 您需要先配置负载均衡监听器，详情请参见 [负载均衡监听器概述](#)。
2. 单击已创建完毕的监听器左侧的【+】展开域名和 URL 路径，选中具体的 URL 路径，在监听器右侧查看已绑定的后端服务。



3. 单击【绑定】，即可在弹出框中选择需绑定的后端服务器，并配置服务端口和权重，绑定后端服务时，可选“云服务器”或“弹性网卡”：

- 云服务器：可绑定与 CLB 同私有网络下所有云服务器主网卡的主内网 IP。
- 弹性网卡：可绑定与 CLB 同私有网络下除云服务器主网卡的主内网 IP 之外的所有弹性网卡 IP，如主网卡的辅助内网 IP 和辅助网卡的内网 IP。弹性网卡 IP 种类详情请参见 [弹性网卡-相关概念](#)。



4. 绑定完毕的配置详情如下。

HTTP/HTTPS监听器

新建

- test(HTTP.80)
 - www.example.com
 - /index
 - /image

转发规则详情 展开

已绑定后端服务

绑定 修改端口 修改权重 解绑

<input type="checkbox"/>	CVM ID/名称	端口状态	IP地址	端口	权重	操作
<input type="checkbox"/>	ins- szf	异常	118. 172	8000	10	解绑
<input type="checkbox"/>	ins- szf	异常	172. eni-	8000	10	解绑
<input type="checkbox"/>	ins- szf	异常	172. eni-	8000	10	解绑
<input type="checkbox"/>	ins- szf	异常	172. eni-	8000	10	解绑

跨地域绑定2.0（新版）

最近更新时间：2020-09-29 12:14:00

负载均衡（CLB）支持通过云联网，跨地域绑定云服务器，允许客户选取多个后端云服务器的地域，跨 VPC、跨地域绑定后端云服务器。

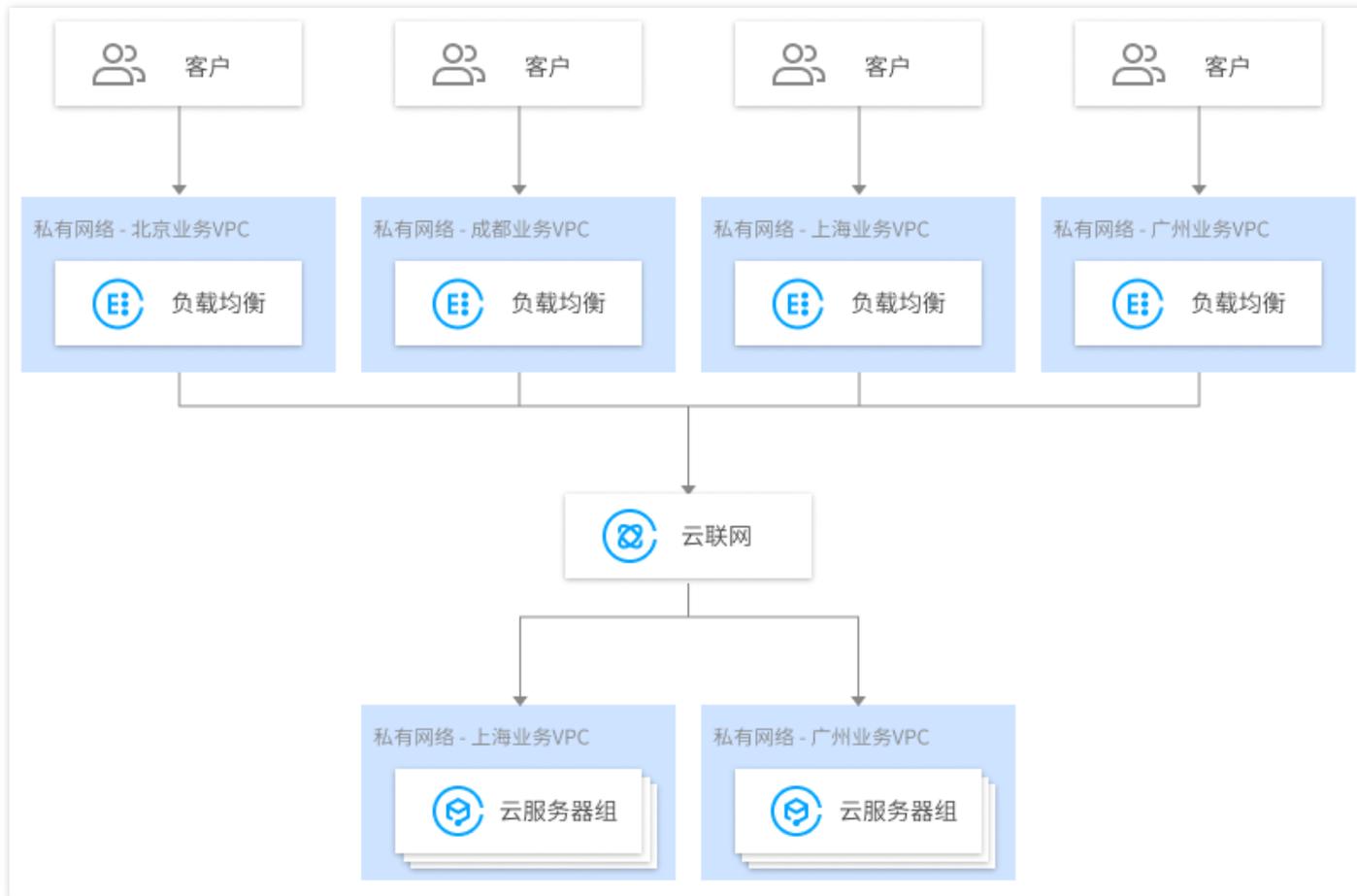
目前该功能处于内测阶段，如果您需要体验该功能，境内跨地域绑定请通过 [内测申请](#)，境外跨地域绑定请进行 [商务申请](#)。

说明：

- 跨地域互联绑定云服务器暂不支持传统型负载均衡。
- 该功能仅标准账户类型支持。若您无法确定账户类型，请参见 [账户类型区分](#)。

应用场景

1. 满足 P2P 等游戏业务中，多地同服的场景。客户后端服务集群在广州，客户希望在上海、北京等多地创建 CLB，绑定相同的广州后端服务集群。起到游戏加速、流量收敛的作用，有效保证数据传输质量，降低时延。
2. 满足金融业务支付、订单付款等场景，有效保证关键业务的数据传输质量，保证数据一致性。



与旧版跨地域绑定的区别

对比项	跨地域绑定2.0（新版）	跨地域绑定1.0（旧版）
是否支持同时绑定多地域内服务	支持： <ul style="list-style-type: none"> 新版跨地域绑定 CLB 支持同时绑定多个地域的 CVM。 例如北京的 CLB 可以同时绑定北京和上海的 CVM。 	不支持： <ul style="list-style-type: none"> 旧版跨地域绑定 CLB 仅能绑定一个地域的 CVM。 例如北京的 CLB 可以绑定上海的 CVM，但北京的 CLB 不能同时绑定北京和上海的 CVM。
是否支持跨域后改回不跨域	支持： <ul style="list-style-type: none"> 新版跨地域绑定支持修改回原来的同地域绑定。 	不支持： <ul style="list-style-type: none"> 旧版跨地域绑定修改后端实例地域属性后，如该地域和 CLB 地域不同，将无法修改回原来的同地域绑定。
支持 CLB 类型	支持公网 CLB 和内网CLB。	支持公网 CLB。
CVM 释放时 CLB 是否自动解绑	同地域绑定时自动解绑： <ul style="list-style-type: none"> CLB 绑定同地域的 CVM，若该 CVM 被释放，则 CLB 会自动与该 CVM 解绑。 跨地域绑定时自动解绑： <ul style="list-style-type: none"> CLB 跨地域绑定 CVM，若该 CVM 被释放，则 CLB 不会自动解除与该 CVM 的绑定关系，需手动解绑。 	同地域绑定时自动解绑： <ul style="list-style-type: none"> CLB 绑定同地域的 CVM，若该 CVM 被释放，则 CLB 会自动与该 CVM 解绑。 跨地域绑定时自动解绑： <ul style="list-style-type: none"> CLB 跨地域绑定 CVM，若该 CVM 被释放，则 CLB 会自动与该 CVM 解绑。
价格是否优惠	通过 云联网计费 ，会进行精细化成本核算，价格更低。	日95计费 。

前提条件

1. 已提交内测申请，境内跨地域绑定请通过[内测申请](#)，境外跨地域绑定请进行[商务申请](#)。
2. 已创建负载均衡实例，详情请参见[创建负载均衡实例](#)。
3. 已创建云联网实例，详情请参见[新建云联网实例](#)。
4. 将需要绑定的目标 VPC 关联至已创建的云联网实例，详情请参见[关联网络实例](#)。

操作步骤

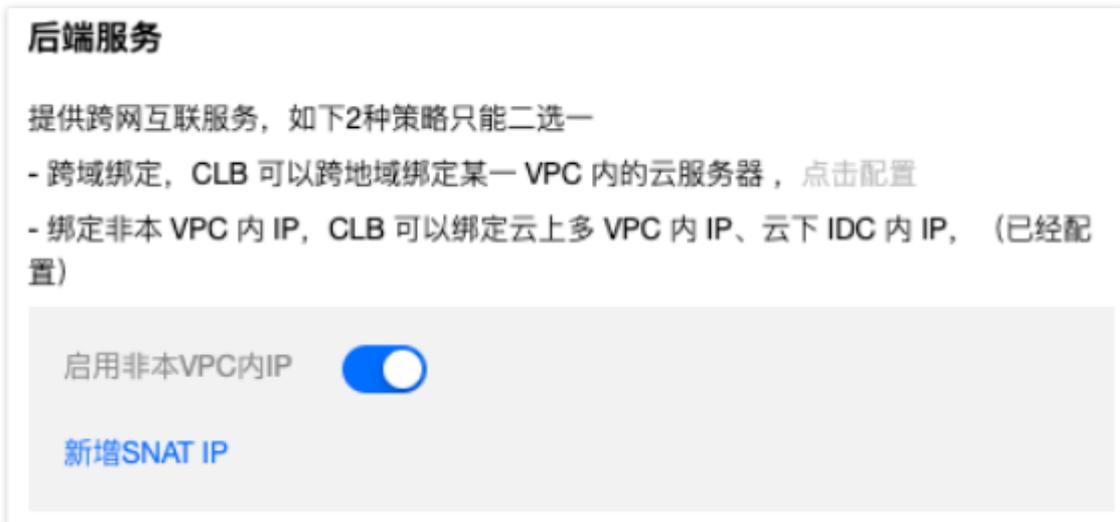
1. 登录 [负载均衡控制台](#)。
2. 在实例详情页面找到目标负载均衡实例，单击实例 ID。
3. 在“基本信息”页面的“后端服务”区域，单击【[点击配置](#)】绑定非本 VPC 的内网 IP。



4. 在弹出的“打开启用非本 VPC 内 IP”对话框中，单击【[提交](#)】。

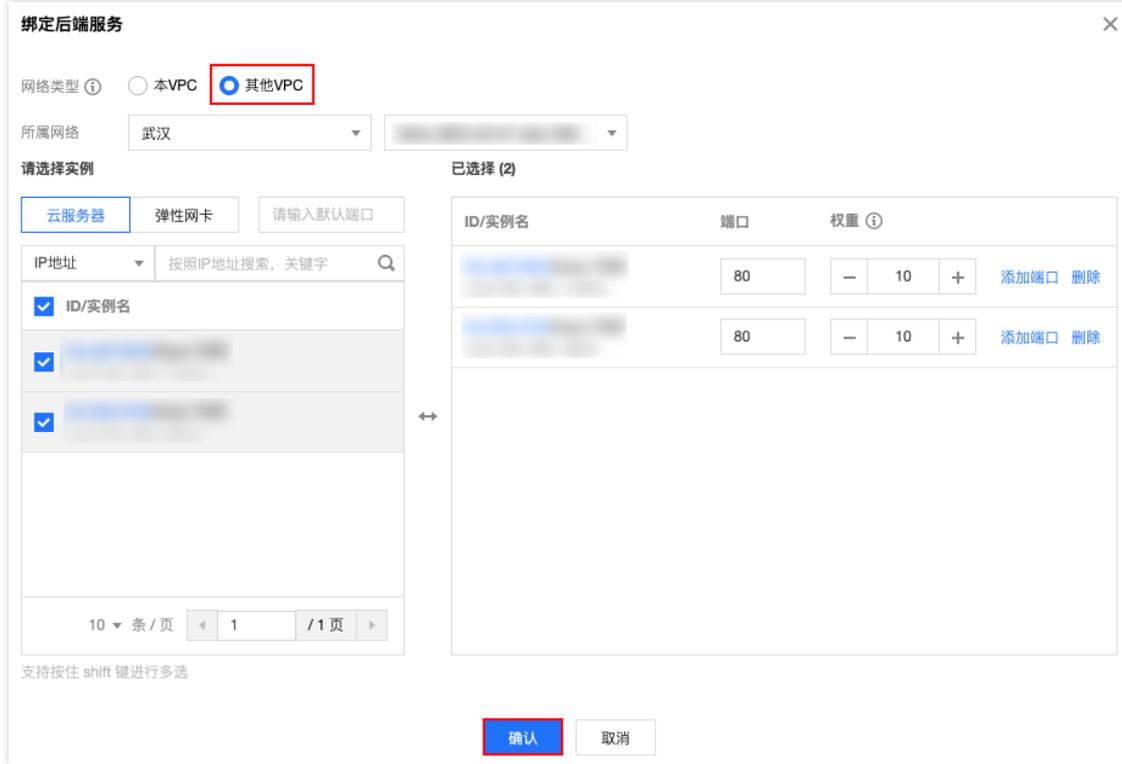


5. 在“基本信息”页面的“后端服务”区域查看到“启用非本 VPC 内 IP”开关已开启，表示可以绑定云上 IP。



6. 在实例详情页面，单击“监听器管理”页签，在配置监听器模块中，为负载均衡实例绑定后端服务，详情请参见 [添加负载均衡后端云服务器](#)。

7. 在弹出的“绑定后端服务”对话框中，选择“其他 VPC”，单击【云服务器】，选择需要关联的云服务器（可多选），并填写相关云服务器需要被转发的端口与权重，详情请参见 [服务器常用端口](#)，单击【确认】。



8. 返回“已绑定后端服务”区域可以查看已绑定的其他地域的 CVM。



跨地域绑定1.0（旧版）

最近更新时间：2020-09-15 16:35:43

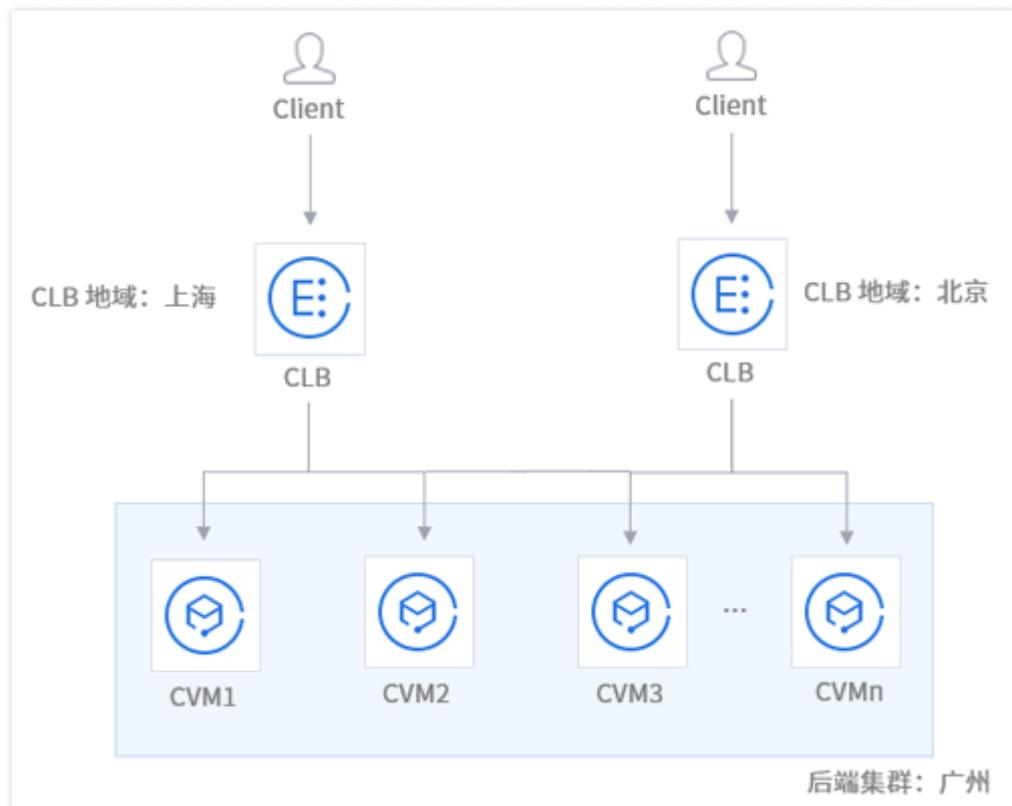
当前，公网负载均衡已支持跨地域绑定云服务器，允许客户选取其他某个地域的云服务器，跨 VPC、跨地域绑定后端云服务器。如果您需要体验该功能，境内跨地域绑定请通过 [工单申请](#)，境外跨地域绑定请进行 [商务申请](#)。

说明：

跨地域绑定云服务器暂不支持内网负载均衡和传统型负载均衡。

应用场景

1. 满足 P2P 等游戏业务中，多地同服的场景。客户后端服务集群在广州，客户希望在上海、北京等多地创建 CLB，绑定相同的广州后端服务集群。起到游戏加速、流量收敛的作用，有效保证数据传输质量，降低时延。
2. 满足金融业务支付、订单付款等场景，有效保证关键业务的数据传输质量，保证数据一致性。



操作步骤

1. 登录 [负载均衡控制台](#)。
2. 在实例详情页面找到目标负载均衡实例，单击实例 ID。
3. 在“基本信息”页面的“后端服务”区域，单击【编辑】修改后端云服务器的地域及网络属性。

 说明：

- 当前负载均衡仅能绑定一个地域的云服务器，例如，北京的 CLB 可以绑定上海的 CVM，但是北京的 CLB 不能同时绑定北京和上海的 CVM。
- 当您修改后端实例服务属性后，如该地域和 CLB 地域不同，将无法修改回原来的同地域绑定。
- 当前暂不允许同地域跨 VPC 绑定负载均衡和云服务器。
- 支持跨基础网络和 VPC 的场景。
- 跨域绑定产生的带宽费用将按天结算，使用带宽峰值阶梯计费，详情请参见 [跨地域绑定计费说明](#)。

修改后端服务配置

温馨提示：当您修改后端实例地域属性时，如该地域和CLB地域不同，将无法修改回同地域绑定。后续需求请提工单申请。

LB地域

LB所属网络

后端服务地域

后端服务网络

费用 [计费详情](#)

计费说明

跨地域绑定的功能通过跨域对等连接的原理实现，计费详情请参见 [计费说明](#)。

混合云部署

最近更新时间：2020-11-11 14:48:03

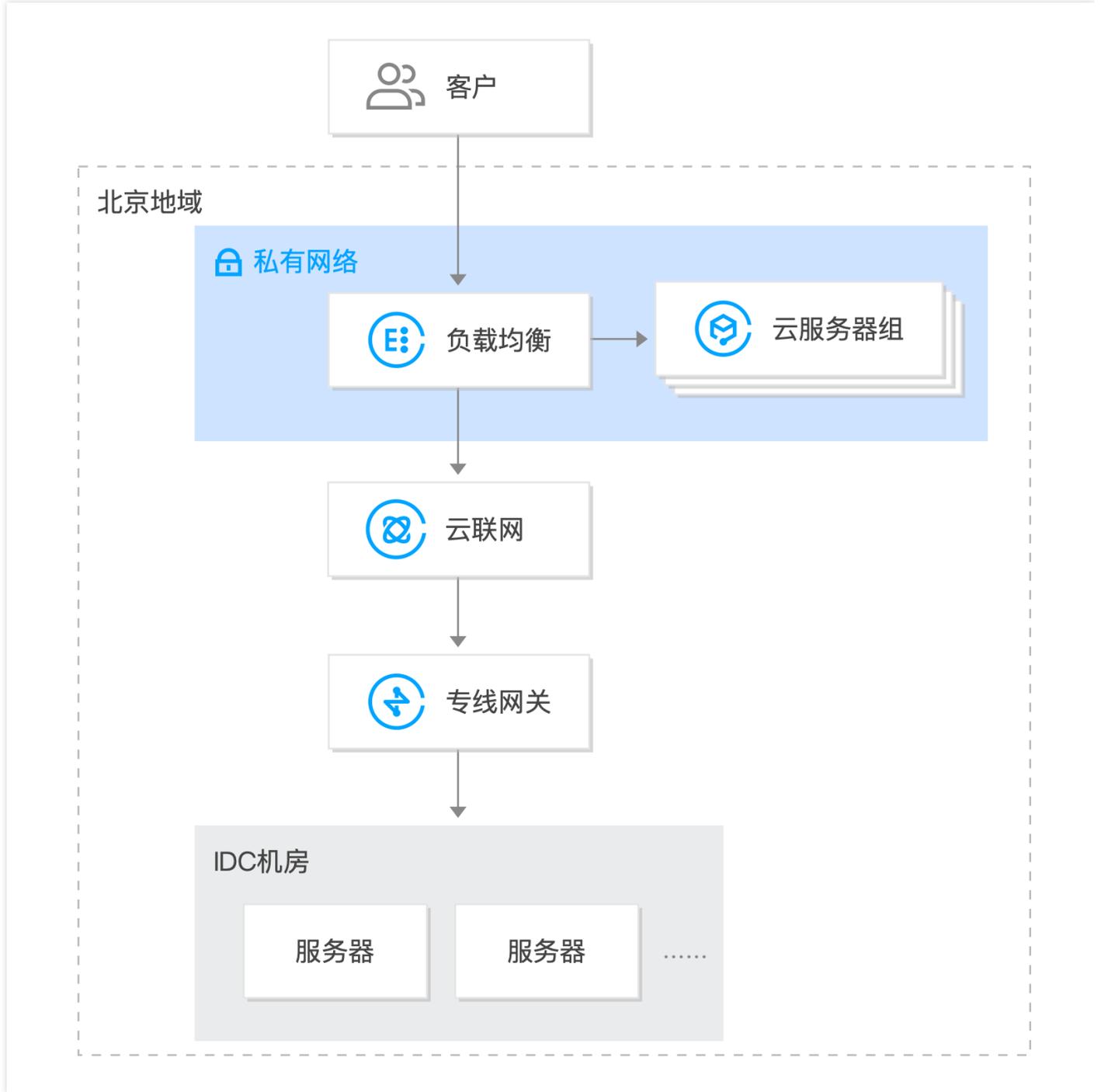
在混合云部署的场景中，可以使用负载均衡直接绑定云下本地数据中心（IDC）内 IP，实现跨 VPC 与 IDC 之间的后端云服务器的绑定。

目前该功能处于内测阶段，如果您需要体验该功能，境内跨地域绑定请通过 [内测申请](#)，境外跨地域绑定请进行 [商务申请](#)。

方案优势

- 快速搭建混合云，无缝连接云上云下，负载均衡可将请求同时转发至云上 VPC 内云服务器和云下 IDC 机房内云服务器。
- 复用腾讯云的高质量公网接入能力。
- 复用腾讯云负载均衡的丰富功能特性，例如四/七层接入、健康检查、会话保持等。

- 内网通过 [云联网](#) 互通，支持精细化选路保障质量，支持多样化阶梯计费降低成本。



限制条件

- 跨网互联绑定云服务器暂不支持传统型负载均衡。
- 该功能仅标准账户类型支持。若您无法确定账户类型，请参见 [账户类型区分](#)。
- 目前仅北京、上海、广州、成都、重庆、香港地域支持该功能。
- TCP 和 TCP SSL 监听器需在 RS 上通过通用 TOA 获取源 IP，详情请参见 [TOA 模块加载方法](#)。
- HTTP 和 HTTPS 监听器需通过 X-Forwarded-For (XFF) 获取源 IP。
- UDP 监听器不支持获取源 IP。

前提条件

1. 已提交内测申请，境内跨地域绑定请通过 [内测申请](#)，境外跨地域绑定请进行 [商务申请](#)。
2. 已创建负载均衡实例，详情请参见 [创建负载均衡实例](#)。
3. 已创建云联网实例，详情请参见 [新建云联网实例](#)。
4. 将与 IDC 关联的专线网关和需要绑定的目标 VPC 关联至已创建的云联网实例，详情请参见 [关联网络实例](#)。

操作步骤

1. 登录 [负载均衡控制台](#)。
2. 在负载均衡“实例管理”页面找到目标负载均衡实例，单击实例 ID。
3. 在“基本信息”页面的“后端服务”区域，单击【[点击配置](#)】绑定非本 VPC 的内网 IP。

The screenshot shows the 'Basic Information' page for a CLB instance. The 'Backend Services' section is highlighted, showing a 'Click Configuration' button. The 'Access Logs' section is also visible, showing that only 7-layer listeners support access logs.

名称	lb-xxxxx_clb
ID	lb-xxxxx
状态	正常
VIP	xxxxx
实例类型	公网
地域	广州
可用区	广州三区
运营商	BGP

访问日志（七层）

仅七层监听器（HTTP/HTTPS）支持配置访问日志（Access Log），四层监听器（TCP/UDP/TCP SSL）不支持

日志服务CLS 未开启

后端服务

提供跨网互联服务，如下2种策略只能二选一

- 跨域绑定，CLB 可以跨地域绑定某一 VPC 内的云服务器，[点击配置](#)
- 绑定非本 VPC 内 IP，CLB 可以绑定云上多 VPC 内 IP、云下 IDC 内 IP，[点击配置](#)

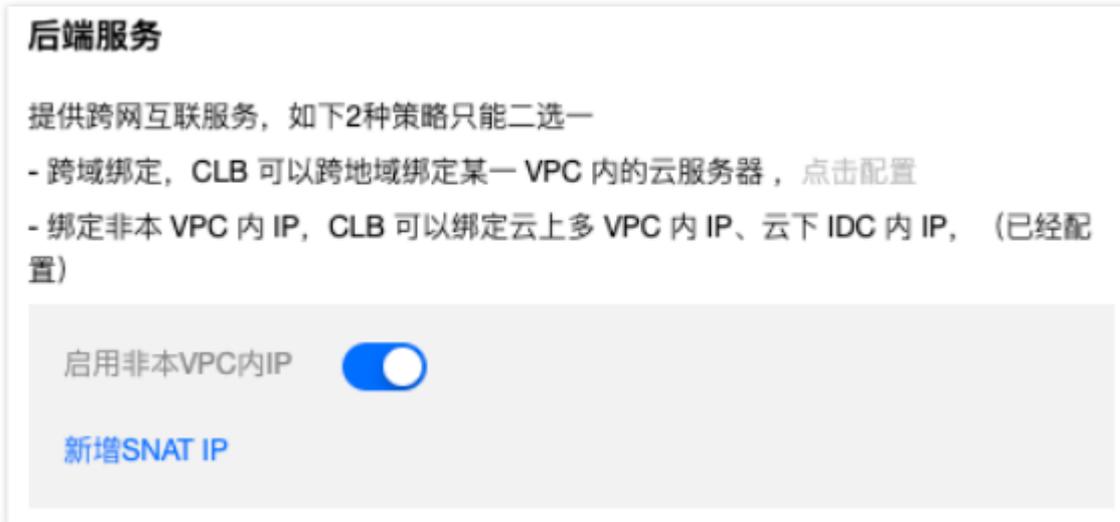
4. 在弹出的“打开启用非本 VPC 内 IP”对话框中，单击【[提交](#)】。

打开启用非本VPC内IP

启用后，CLB 支持绑定非本 VPC 的内网 IP。

[提交](#) [关闭](#)

5. 在“基本信息”页面的“后端服务”区域，单击【新增 SNAT IP】。



6. 在弹出的“新增 SNAT IP”对话框中，选择“子网”，单击【新增】分配 IP，最后单击【保存】。



7. 在实例详情页面，单击“监听器管理”页签，在配置监听器模块中，为负载均衡实例绑定后端服务，详情请参见[添加负载均衡后端云服务器](#)。

8. 在弹出的“绑定后端服务”对话框中，选择“其他内网 IP”，单击【添加内网 IP】，输入需绑定的 IDC 内网 IP 地址，并填写端口与权重，详情请参见[服务器常用端口](#)，最后单击【确认】。

绑定后端服务 ×

目标类型 ^① 实例 其他内网IP

默认端口

IP	端口	权重 ^①	
<input type="text"/>	<input type="text" value="80"/>	<input type="button" value="-"/> <input type="text" value="10"/> <input type="button" value="+"/> 添加端口 删除	
<input type="text"/>	<input type="text" value="80"/>	<input type="button" value="-"/> <input type="text" value="10"/> <input type="button" value="+"/> 添加端口 删除	

[添加内网IP](#)

9. 返回“已绑定后端服务”区域可以查看已绑定的 IDC 的内网 IP。

已绑定后端服务

↻

<input type="checkbox"/>	CVM ID/...	网络	端口健康状态 ^①	IP地址	端口	权重	操作
<input type="checkbox"/>		其他网络	健康		80	10	解绑
<input type="checkbox"/>		其他网络	健康		80	10	解绑
<input type="checkbox"/>		本VPC	健康		80	10	解绑

后端云服务器的安全组配置

最近更新时间：2020-01-16 12:02:43

CVM 安全组简介

负载均衡的后端云服务器实例可以通过 [安全组](#) 进行访问控制，起到防火墙的作用。

您可以将一个或多个安全组与后端云服务器关联，并对每个安全组添加一条或多条规则控制不同服务器的流量访问权限。您可以随时修改某个安全组的规则，新规则会自动应用于与该安全组关联的所有实例。有关更多信息，请参阅 [安全组操作指南](#)。在 [私有网络](#) 环境中，您还可以使用 [网络 ACL](#) 进行访问控制。

CVM 安全组配置说明

在 CVM 的安全组上，需放通 Client IP 和服务端口。

若您使用 CLB 转发业务流量到 CVM 上，为保障健康检查功能，在 CVM 的安全组上需做如下配置：

1. 公网负载均衡：您需要在后端 CVM 的安全组上放通 CLB 的 VIP，CLB 使用 VIP 来探测后端 CVM 的健康状态。
2. 内网负载均衡：
 - 对于内网负载均衡（原“应用型内网负载均衡”），如果您的 CLB 属于 VPC 网络，您需要在后端 CVM 的安全组上放通 CLB 的 VIP（用作健康检查）；如果您的 CLB 属于基础网络，无需在后端 CVM 的安全组上配置，默认放通健康检查 IP。
 - 对于传统型内网负载均衡，如果实例创建于2016年12月5日前且网络类型为 VPC 网络，则需要在后端 CVM 的安全组上放通 CLB 的 VIP（用作健康检查）；其他类型的传统型内网 CLB 无需在后端 CVM 的安全组上配置，默认放通健康检查 IP。

CVM 安全组配置示例

如下示例为通过 CLB 访问 CVM 时，CVM 安全组的配置示例。若您在 CLB 上也配置了安全组，请参照 [配置负载均衡安全组](#) 来配置 CLB 上的安全组规则。

• 应用场景 1：

公网负载均衡，监听器配置为 TCP:80 监听器，后端服务端口为8080，希望只允许 Client IP（ClientA IP 和 ClientB IP）访问负载均衡，则后端服务器安全组入站规则配置如下：

```
ClientA IP + 8080 allow
ClientB IP + 8080 allow
CLB VIP + 8080 allow
0.0.0.0/0 + 8080 drop
```

• 应用场景 2:

公网负载均衡，监听器配置为 HTTP:80 监听器，后端服务端口为8080，希望开放所有 Client IP 的正常访问，则后端服务器安全组入站规则配置如下：

```
0.0.0.0/0 + 8080 allow
```

• 应用场景 3:

内网负载均衡（原“应用型内网负载均衡”），网络类型为 VPC 网络，在 CVM 的安全组上需放通 CLB 的 VIP 来做健康检查。为该 CLB 配置 TCP:80 监听器，后端服务端口为8080，希望只允许 Client IP（ClientA IP 和 ClientB IP）访问负载均衡的 VIP，并且希望限制 Client IP 只能访问该 CLB 下绑定的后端主机。

a. 后端服务器安全组入站规则配置如下：

```
ClientA IP + 8080 allow  
ClientB IP + 8080 allow  
CLB VIP + 8080 allow  
0.0.0.0/0 + 8080 drop
```

b. 用作 Client 的服务器安全组出站规则配置如下：

```
CLB VIP + 8080 allow  
0.0.0.0/0 + 8080 drop
```

• 应用场景 4:

传统型内网负载均衡（16年12月5日之后的新购的 VPC 网络 CLB），CVM 安全组仅需放通 Client IP（无需放通 CLB 的 VIP，默认放通健康检查 IP）。为该 CLB 配置 TCP:80 监听器，后端服务端口为8080，希望只允许 Client IP（ClientA IP 和 ClientB IP）访问负载均衡的 VIP，并且希望限制 Client IP 只能访问该 CLB 下绑定的后端主机。

a. 后端服务器安全组入站规则配置如下：

```
ClientA IP + 8080 allow  
ClientB IP + 8080 allow  
0.0.0.0/0 + 8080 drop
```

b. 用作 Client 的服务器安全组出站规则配置如下：

```
CLB VIP + 8080 allow
0.0.0.0/0 + 8080 drop
```

• 应用场景 5: 黑名单

如用户需要给某些 Client IP 设置黑名单，拒绝其访问，可以通过配置云服务关联的安全组实现。安全组的规则需要按照如下步骤进行配置：

- 将需要拒绝访问的 Client IP + 端口添加至安全组中，并在策略栏中选取拒绝该 IP 的访问。
- 设置完毕后，再添加一条安全组规则，默认开放该端口全部 IP 的访问。

配置完成后，安全组规则如下：

```
clientA IP + port drop
clientB IP + port drop
0.0.0.0/0 + port accept
```

⚠ 注意：

- 上述配置步骤有**顺序要求**，顺序相反会导致黑名单配置失效。
- 安全组是有状态的，因此上述配置均为**入站规则**的配置，出站规则无需特殊配置。

CVM 安全组操作指引

使用控制台管理后端服务器安全组

1. 登录 [负载均衡控制台](#)，单击相应的负载均衡实例 ID 进入负载均衡详情页。
2. 在 CLB 绑定的云服务器页面中，单击相应的后端服务器 ID 进入云服务器详情页。
3. 单击【安全组】选项卡，即可绑定/解绑安全组。

使用云 API 管理后端服务器安全组

请参考 [绑定安全组接口](#) 和 [解绑安全组接口](#)。