

# Cloud CDN

## 背景

Cloud CDN 使用 Google 的全球分布式边缘点来缓存与用户接近的 HTTP ( S ) 负载平衡内容。在 Google 网络边缘缓存内容可以更快地向用户提供内容传输，同时降低服务成本。这篇文章将介绍如何利用 GCE(Google Compute Engine) 建立一个 Anycast 网络，想要实现这个功能，就需要使用 Cross-Region Load Balancing ( 跨地区的负载均衡 )，此功能就相当于一个 HTTP(S) 的反向代理，所以只能针对 HTTP/HTTPS 请求进行负载均衡。

## 概述

GCP 上所实现的这个功能是基于第七层的网络代理，所以其拓扑图是这样的：

用户 —> 边缘服务器 —> 实例

用户到边缘服务器之间的连接：使用 HTTP 或 HTTPS；如果是 HTTPS 连接，那么 TLS 加密过程是在边缘服务器上实现。

边缘服务器到实例的连接：使用 HTTP 或 HTTPS 连接，之前的网络是走的 Google 的专线。不论配置了几个位置的实例，边缘服务器都是使用 Google 全部的边缘服务器。启用这个功能后，就会得到另一个 Anycast 的 IP 地址，这是个独享的 IP 地址。

## 配置

大致步骤：

建议实例->建立实例组->建立健康检查->建立负载均衡器->启动CDN

## 建立实例

打开 Google Compute，创建实例：



Compute Engine

虚拟机实例

[创建实例](#)
[导入虚拟机](#)
[刷新](#)
[启动](#)
[停止](#)
[重置](#)
[删除](#)

虚拟机实例

实例组

实例模板

单租户节点

机器映像

磁盘

快照

过滤虚拟机实例

列

<input type="checkbox"/>	姓名 ^	地区	建议	使用者	内部 IP	外部 IP	连接
<input type="checkbox"/>	instance-1	asia-northeast1-a		instance-group-1	10.146.0.4 (nic0)	34.84.151.192 ↗	SSH ▾ ⋮
<input type="checkbox"/>	instance-2	asia-northeast2-c		instance-group-2	10.174.0.2 (nic0)	34.97.104.40 ↗	SSH ▾ ⋮

根据自己需求选择机器类型、启动磁盘等等配置，区域的话建议选择与网站源站所在机房靠近的，不然可能达不到加速的目的。

创建成功后即可通过 SSH 登录实例 VM，如果登录不上，可能需要先在防火墙开放下端口：



VPC 网络

防火墙规则

[创建防火墙规则](#)
[刷新](#)
[删除](#)

VPC 网络

外部 IP 地址

防火墙规则

路由

VPC 网络对等互连

共享 VPC

无服务器 VPC 访问

数据包镜像

防火墙规则用于控制实例的传入和传出流量。默认情况下，系统会阻止从您的网络之外传入的流量。[了解详情](#)

注意：点击[此处](#)可管理 App Engine 防火墙。

过滤表

<input type="checkbox"/>	名称	类型	目标	过滤条件	协议/端口	操作	优先级	网络 ↑
<input type="checkbox"/>	allow-all	入站	应用到所有实例	IP 地址范围: 0.0.0.0/0	all	允许	1000	default
<input type="checkbox"/>	default-allow-http	入站	http-server	IP 地址范围: 0.0.0.0/0	tcp:80	允许	1000	default
<input type="checkbox"/>	default-allow-https	入站	https-server	IP 地址范围: 0.0.0.0/0	tcp:443	允许	1000	default
<input type="checkbox"/>	default-allow-icmp	入站	应用到所有实例	IP 地址范围: 0.0.0.0/0	icmp	允许	65534	default
<input type="checkbox"/>	default-allow-internal	入站	应用到所有实例	IP 地址范围: 10.128.0.0/9	tcp:0-65535 udp:0-65535 icmp	允许	65534	default
<input type="checkbox"/>	default-allow-rdp	入站	应用到所有实例	IP 地址范围: 0.0.0.0/0	tcp:3389	允许	65534	default
<input type="checkbox"/>	default-allow-ssh	入站	应用到所有实例	IP 地址范围: 0.0.0.0/0	tcp:22	允许	65534	default

主要注意流量方向、执行的操作、目标、来源 IP、协议和端口的配置：

VPC 网络

VPC 网络

外部 IP 地址

防火墙规则

路由

VPC 网络对等互连

共享 VPC

无服务器 VPC 访问

数据包镜像

← 创建防火墙规则

网络 \*  
default

优先级 \*  
1000  
优先级可以从 0 到 65535[检查其他防火墙规则的优先级](#)

流量方向  
☒ 入站  
☐ 出站

对匹配项执行的操作  
☒ 允许  
☐ 拒绝

目标  
网络中的所有实例

来源过滤条件  
IP 范围

来源 IP 地址范围 \*  
0.0.0.0/0 例如, 0.0.0.0/0、192.168.2.0/24

次要来源过滤条件  
无

协议和端口  
☒ 全部允许  
☐ 指定的协议和端口

停用规则

创建 取消

等效 [REST](#) 或 [命令行](#)

## 创建运行检查

Google Cloud CDN 有个运行状况检查来确定 VM 分流，针对的是有多个 VM 的情况。打开运行状

况检查，创建运行状况检查：

## ← 创建运行状况检查

名称

lb-health-check



说明

范围

☒ 全球

☐ 区域级

协议

HTTP



端口

80



代理协议

无



请求路径

/



▼ 展开

### 运行状况判断标准

定义如何确定运行状况：检查频率、等待响应的时间、成功或失败的尝试达到多少次即可决定

检查间隔

5

秒



超时

5

秒



状况良好判断阈值

2

次连续成功



状况不佳判断阈值

2

次连续失败




您可以免费创建此运行状况检查


## 创建实例组

实例组的作用在 Cloud CDN 种与运行状况检查作用差不多，起到故障转移的作用，通过下一步的

负载均衡实现。

打开实例组，创建实例组：

将虚拟机实例整理到组中，以便集中管理。[实例组](#) 


名称 

名称一旦设置就不能更改

instance-group

说明 (可选)

位置

区域 


asia-northeast1 (东京)

地区 


地区一旦选择就不能更改

asia-northeast1-a

指定端口名称映射 (可选)

网络 

default

子网 


default (10.146.0.0/20)

虚拟机实例

instance-1



无可用实例

您需要为此组中的虚拟机实例付费。[Compute Engine 价格](#) 

创建

取消

等效 [REST](#) 或 [命令行](#)

因为我们先创建了实例，所以这里我们新建非托管式实例组，位置区域选择 VM 实例所在的位置区

域，然后选上 VM 实例点创建。



Compute Engine

虚拟机实例

**实例组**

实例模板

单租户节点

机器映像

磁盘

帮助

实例组

创建实例组

刷新

删除

实例组是虚拟机实例的集合，这些实例使用负载均衡和自动化服务，如自动扩缩和自动修复。[了解详情](#)

过滤资源

列

<input type="checkbox"/> 名称 ^	地区	实例数	模板	创建时间	建议	自动调节	使用者
<input type="checkbox"/>  instance-group-1	asia-northeast1-a	1	—	2020年3月24日 下午10:45:08			lb
<input type="checkbox"/>  instance-group-2	asia-northeast2-c	1	—	2020年3月24日 下午10:45:48			lb

## 负载均衡

Google Cloud CDN 基于负载均衡实现，所以我们需要先创建负载均衡策略。

打开负载均衡，创建 HTTP(S) 的负载均衡器：

网络服务

**负载均衡**

Cloud DNS

Cloud CDN

Cloud NAT

Traffic Director

← 新的 HTTP(S) 负载均衡器

名称 <sup>?</sup>

名称一旦设置就不能更改

使用小写字母，不能有空格

● 后端配置

您尚未配置后端

● 主机和路径规则

您尚未配置主机和路径规则

● 前端配置

您尚未配置前端

① 检查并最终确定

可选

创建

取消

创建 HTTP(S) 负载均衡器

一个 HTTP/HTTPS 负载均衡器包含 3 个部分：

- 后端配置**  
后端服务会将传入的流量引导至实例组。您也可以使用存储分区来处理内容。
- 主机和路径规则**  
主机和路径规则决定着流量被引导的方式。如果您不指定任何规则，系统就会将流量引导至默认后端服务。
- 前端配置**  
您的 IP 地址、协议和端口。这是您的客户端请求将传入的 IP。

负载均衡器需要配置三个部分：后端、主机和路径、前端。

我们——来看看配置。

## 后端配置

后端配置是指要指定 VM 来源，也就是我们创建的反代，通过后端服务来实现。

需要注意的是协议、实例组、端口号，其中协议可以是 HTTP，也可以是 HTTPS。

### 创建后端服务

名称 <sup>?</sup>

名称一旦设置就不能更改

lb-lab

说明

后端类型

实例组

协议、已命名的端口、超时

协议 <sup>?</sup>

HTTP

已命名的端口 <sup>?</sup>

http

超时 <sup>?</sup>

30

秒

后端

区域: asia-northeast1, asia-northeast2

instance-group-1 (地区: asia-northeast1-a, 端口: 80)



instance-group-2 (地区: asia-northeast2-c, 端口: 80)



+ 添加后端

Cloud CDN <sup>?</sup>

☐ 启用 Cloud CDN

运行状况检查 <sup>?</sup>

lb-health-check (HTTP)

端口: 80, 超时: 5 秒, 检查间隔: 5 秒, 状况不佳判断阈值: 2 次尝试

日志记录 <sup>?</sup>

☒ 启用日志记录

高级配置 (会话粘性、连接排空超时时间、安全策略)

## 主机和路径规则

## 主机和路径规则

主机和路径规则决定着流量被引导的方式。您可以将流量引导至后端服务或存储分区。没有明确匹配主机和路径规则的流量将被引导至在第一行中选择的默认服务。

主机	路径	后端	
任何不匹配的项 (默认)	任何不匹配的项 (默认)	lb-lab	×
<a href="#">+ 添加主机和路径规则</a>			

⌵ 显示配置测试

## 前端配置

前端配置这里就是配置外部要怎么访问我们的后端服务。与后端配置一样，可以配置 HTTP，也可以配置 HTTPS，配置 HTTPS 的话需要添加 SSL 证书，也可以使用谷歌签发的证书，这里配置为 HTTP。IP 地址的话，支持 IPv4，也支持 IPv6，这里可以创建负载均衡器静态 IP：



新建前端 IP 和端口

名称 (可选) ?  
名称一旦设置就不能更改

lb-lab

添加说明

协议 ?  
HTTP

网络服务层级 ?  
☒ 优质 (当前项目级层级, [更改](#)) ?  
☐ 标准 ?

*i* 您的负载均衡器在多个区域拥有后端。标准层级仅支持在一个区域的后端。

IP 版本

IP 地址

IPv4

lb-lab (34.107.203.111)

端口

80

完成

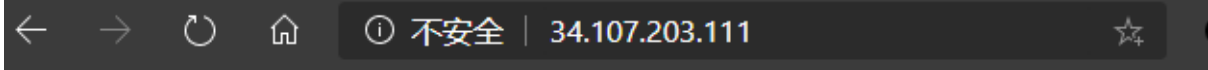
取消

配置好后点创建。

创建后，您会在列表中看到新创建的LB。

<input type="checkbox"/> 名称	<a href="#">协议 ^</a>	区域	后端	
<input type="checkbox"/> lb	HTTP	全局	 1 项后端服务 (2 个实例组, 0 个网络端点组)	

可以测试下LB是否工作。访问LB的前端IP：https://34.107.203.111:80，浏览器显示如下：



## Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to [nginx.org](https://nginx.org).  
Commercial support is available at [nginx.com](https://nginx.com).

*Thank you for using nginx.*

## 创建CDN

在网络服务菜单选择Cloud CDN。

Cloud CDN

网络服务  
CDN

Google Cloud CDN 利用 Google 遍布全球的边缘点，在距您的用户更近的位置缓存 HTTP(S) 内容，以提高内容递交速度并降低服务开销。要开始使用，请点击“添加来源”。[了解详情](#)

[添加来源](#)

点击 添加来源 按钮来选择CDN来源。这里选择“使用现有的Google Cloud Platform资源”

从下拉列表中选择负载均衡器，然后单击添加。

## ← 将来源添加到 Cloud CDN

1 准备 2 配置来源详细信息

### 来源类型

- ☒ 使用现有的 Google Cloud Platform 资源  
Compute Engine、Kubernetes Engine 和/或 Google Cloud Storage
- ☐ 使用自定义来源  
GCP 外部的后端

### 负载均衡器

选择某个负载均衡器作为来源。云端 CDN 会缓存来自来源的响应。

### 后端服务

Cloud CDN 将缓存来自已检查的后端服务的响应

<input checked="" type="checkbox"/>	名称	后端类型	缓存键	已签署的网址	
<input checked="" type="checkbox"/>	lb-lab	实例组 GCE 和 GKE 后端	默认	无	配置

添加

取消

CDN创建成功。

Cloud CDN
+ 添加来源
刷新

 过滤资源 

来源名称 ^	后端	缓存命中率 ?	
 lb	lb-lab (已启用)	无	⋮

至此，Cloud CDN创建成功。您可以更新域名的A记录，将其指向负载均衡器的全局IP。