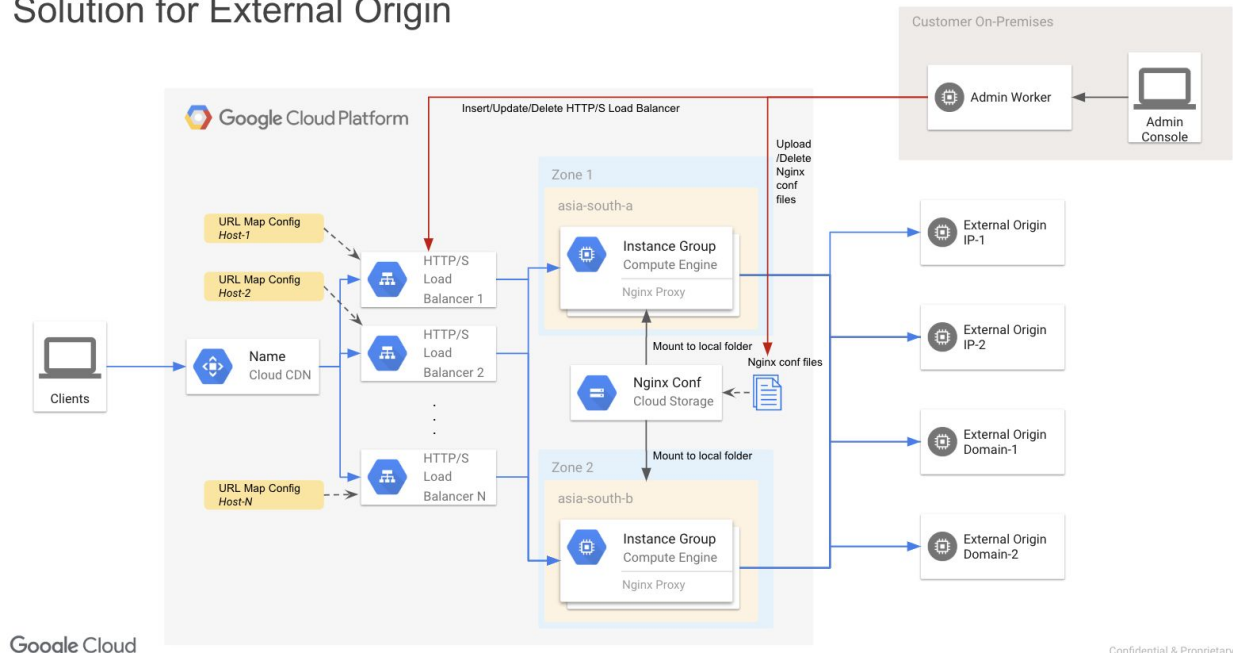


使用Nginx实例组实现CDN外部源站

本文指导如何在谷歌云上创建一个Nginx反向代理实例组，用来实现谷歌云CDN回源到外部源站。本文的配置主要基于下面架构。

Solution for External Origin



本文档介绍的配置主要分为以下几个部分。

[创建配置文件存储桶](#)

[创建模板虚拟机实例](#)

[创建自定义镜像](#)

[创建实例模板](#)

[创建托管实例组](#)

[创建负载均衡和CDN](#)

[修改和更新代理配置](#)

创建配置文件存储桶

首先创建一个Cloud Storage的存储桶，用来存放代理服务器配置文件。

[←](#) Create a bucket

Name [?](#)

Must be unique across Cloud Storage. If you're [serving website content](#), enter the website domain as the name.

Default storage class

Objects added to this bucket are assigned the selected storage class by default. An object's storage class and bucket location affect its geo-redundancy, availability, and costs. You can set storage classes for individual objects in gsutil. [Learn more](#)

[i](#) Nearline and Coldline data in multi-regional locations is now stored geo-redundantly. New locations nam4 and eur4 (available in beta) enable co-location of compute and storage for high performance with geo-redundancy. [Learn more](#)

[Dismiss](#)

- ☐ Multi-Regional
- ☒ Regional
- ☐ Nearline
- ☐ Coldline

Location

[Compare storage classes](#)

Storage cost

\$0.02 per GB-month

Retrieval cost

Free

Class A operations [?](#)

\$0.005 per 1,000 ops

Class B operations [?](#)

\$0.0004 per 1,000 ops

Access control model

Choose how you'll control access to this bucket's objects. [Learn more](#)

- ☒ **Set permissions uniformly at bucket-level (Bucket Policy Only)**
Enforces the bucket's IAM policy without object ACLs. May help prevent unintended access. If selected, this option becomes permanent after 90 days.
- ☐ **Set object-level and bucket-level permissions**
Enforces the IAM policy and object ACLs for more granular control of object access.

[⌵ Show advanced settings](#)

[Create](#)[Cancel](#)

在本地创建一个名为的配置文件，并上传到存储桶。配置文件的内容如下。注意将回源域名改为实际使用的域名。

```
server {
    listen      80;
    server_name ~^(.+)$;
    gzip on;
    gzip_proxied any;

    location / {
        access_log /var/log/nginx/upstream.log;
        add_header Cache-Control "public, max-age=604800";
        proxy_http_version 1.1;
        proxy_pass https://xxx.s3.amazonaws.com/;
    }
}
```

创建模板虚拟机实例

创建一个GCE VM实例，用来制作实例组的模板。

Name ?**Region** ?**Zone** ?**Machine type**

Customize to select cores, memory and GPUs.

3.75 GB memory

[Customize](#)**Container** ?☐ Deploy a container image to this VM instance. [Learn more](#)**Boot disk** ?

New 100 GB standard persistent disk

Image

Google Drawfork Ubuntu 16.04 LTS

[Change](#)**Identity and API access** ?**Service account** ?**Access scopes** ?

- ☒ Allow default access
- ☐ Allow full access to all Cloud APIs
- ☐ Set access for each API

Firewall ?

Add tags and firewall rules to allow specific network traffic from the Internet

- ☒ Allow HTTP traffic
- ☒ Allow HTTPS traffic

[Management, security, disks, networking, sole tenancy](#)

The following options have been customized:

Network tags

You will be billed for this instance. [Compute Engine pricing](#) [↗](#)[Create](#)[Cancel](#)Equivalent [REST](#) or [command line](#)

在实例创建完毕后，点击“SSH”按钮登录到虚拟机命令行。

<input type="checkbox"/>	Name ^	Zone	Recommendation	In use by	Internal IP	External IP	Connect
<input checked="" type="checkbox"/>	cdn-proxy	asia-southeast1-b			10.148.0.2 (nic0)	35.198.234.55 ↗	SSH ▾

运行以下命令，安装gcsfuse。

```
export GCSFUSE_REPO=gcsfuse-`lsb_release -c -s`

echo "deb http://packages.cloud.google.com/apt $GCSFUSE_REPO main" | sudo
tee /etc/apt/sources.list.d/gcsfuse.list

curl https://packages.cloud.google.com/apt/doc/apt-key.gpg | sudo apt-key
add -

sudo apt-get update
sudo apt-get install gcsfuse
```

修改/etc/fuse.conf，将“user_allow_other”前面的注释符去掉。

```
/etc/fuse.conf - Configuration file for Filesystem in Userspace (FUSE)

# Set the maximum number of FUSE mounts allowed to non-root users.
# The default is 1000.
#mount_max = 1000

# Allow non-root users to specify the allow_other or allow_root mount options.
user_allow_other

~
```

运行下面命令，将之前创建的存放配置文件的存储桶挂载到本地目录。

```
mkdir ~/gcs
gcsfuse -o allow_other cdn-proxy-config /home/eugeneyu/gcs
```

运行下面命令，确认可以访问到存储桶上的配置文件。

```
eugeneyu@cdn-proxy:~$ ls gcs/
nginx-proxy-config.conf
eugeneyu@cdn-proxy:~$
```

运行下面命令，将可使用的文件句柄上限提高。

```
sudo su -  
ulimit -n 99999  
echo "fs.file-max=99999" >> /etc/sysctl.conf  
echo "* soft nofile 99999" >> /etc/security/limits.conf  
echo "* hard nofile 99999" >> /etc/security/limits.conf  
exit
```

运行以下命令，安装Nginx服务。

```
sudo apt-get update  
sudo apt-get install -y nginx
```

修改Nginx的主配置文件/etc/nginx/nginx.conf，增加最大连接数，并将反向代理配置文件导入。

```
user www-data;  
worker_processes auto;  
pid /run/nginx.pid;  
worker_rlimit_nofile 10000;  
  
events {  
    worker_connections 5000;  
    # multi_accept on;  
}
```

```
http {  
    ##  
    # Basic Settings  
    ##  
  
    sendfile on;  
    tcp_nopush on;  
    tcp_nodelay on;  
    keepalive_timeout 65;  
    types_hash_max_size 2048;  
    # server_tokens off;  
  
    # server_names_hash_bucket_size 64;  
    # server_name_in_redirect off;  
  
    include /etc/nginx/mime.types;  
    default_type application/octet-stream;  
    include /home/eugenyu/gcs/nginx-proxy-config.conf;  
    ##  
    # SSL Settings  
    ##  
}
```

运行下面命令重启Nginx

```
sudo service nginx restart
```

测试Nginx代理访问源站资源是否成功。请将下面地址中的IP替换成Nginx服务器的公网IP，将文件路径替换成源站测试文件的路径。

```
curl -X GET http://35.198.234.55/do_not_delete/test.txt
```

创建自定义镜像

基于Nginx服务器系统盘创建自定义镜像。

Compute Engine

VM instances

Instance groups

Instance templates

Sole tenant nodes

Disks

Snapshots

Images

TPUs

Committed use discounts

Metadata

Health checks

Zones

Network endpoint groups

Operations

Security scans

Settings

Create an image

Name ?

image-nginx-proxy-v1

Family (Optional) ?

Description (Optional)

Labels ? (Optional)

+ Add label

Encryption

Data is encrypted automatically. Select an encryption key management solution.

☒ Google-managed key

No configuration required

☐ Customer-managed key

Manage via Google Cloud Key Management Service

☐ Customer-supplied key

Manage outside of Google Cloud

Source ?

Disk

Source disk ?

cdn-proxy

☒ Keep instance running (not recommended)

Filesystem integrity can't be guaranteed while the instance is running, which may create a corrupted image

You will be billed for this image. [Compute Engine pricing](#)

CreateCancel

Equivalent [REST](#) or [command line](#)

创建实例模板

镜像创建好后，创建一个Instance Template。修改以下配置。

1. “Machine type”根据需要选择2 vCPUs或者4 vCPUs机型。
2. 修改“Boot disk”配置，选择刚刚创建好的镜像。

Boot disk

Select an image to create a boot disk. The image determines the operating system installed on the instance.

OS images Application images Custom images

Show images from

☒ image-nginx-proxy-v1

Created from on Apr 25, 2019, 4:11:17 PM

3. “Firewall”勾选“Allow HTTP traffic”和“Allow HTTPS traffic”
4. “Networking”中的“Network tags”填写“cdn-proxy”
5. Management中的Startup script中填入以下内容，确保新实例启动时自动挂载配置文件存储桶，并增加文件句柄上限。

Automation

Startup script (Optional)

You can choose to specify a startup script that will run when your instance boots up or restarts. Startup scripts can be used to install software and updates, and to ensure that services are running within the virtual machine. [Learn more](#)

```
#!/bin/bash
sysctl -p
gcsfuse -o allow_other cdn-proxy-config /home/eugeneyu/gcs/
service nginx restart
```

配置好后，点击“Create”按钮创建模板。

创建托管实例组

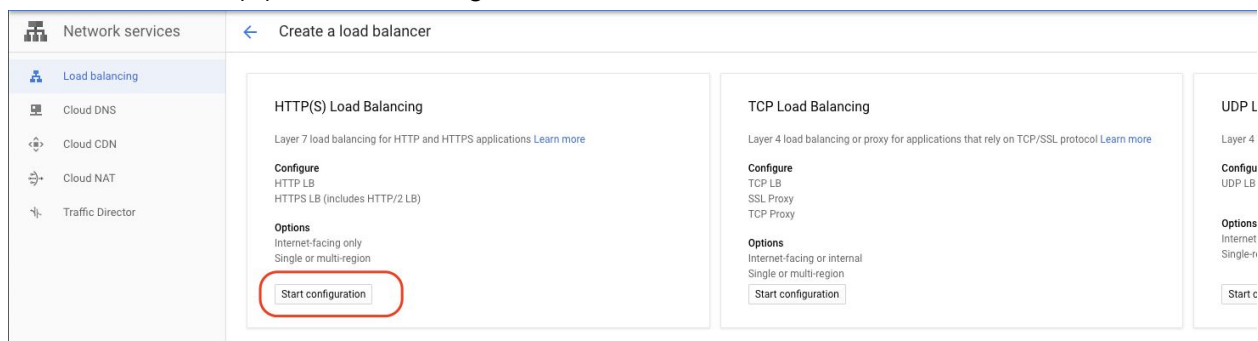
创建实例组。修改以下配置。

1. Location选择Multiple zones
2. Region选择离源站最近的区域，比如新加坡为asia-southeast1
3. Instance template选择上一步创建好的模板
4. Minimum number of instances根据预估用量选择机器数量，比如5000RPS可以选择5台
5. Health check创建一个80端口的健康检查，各项配置采用默认值

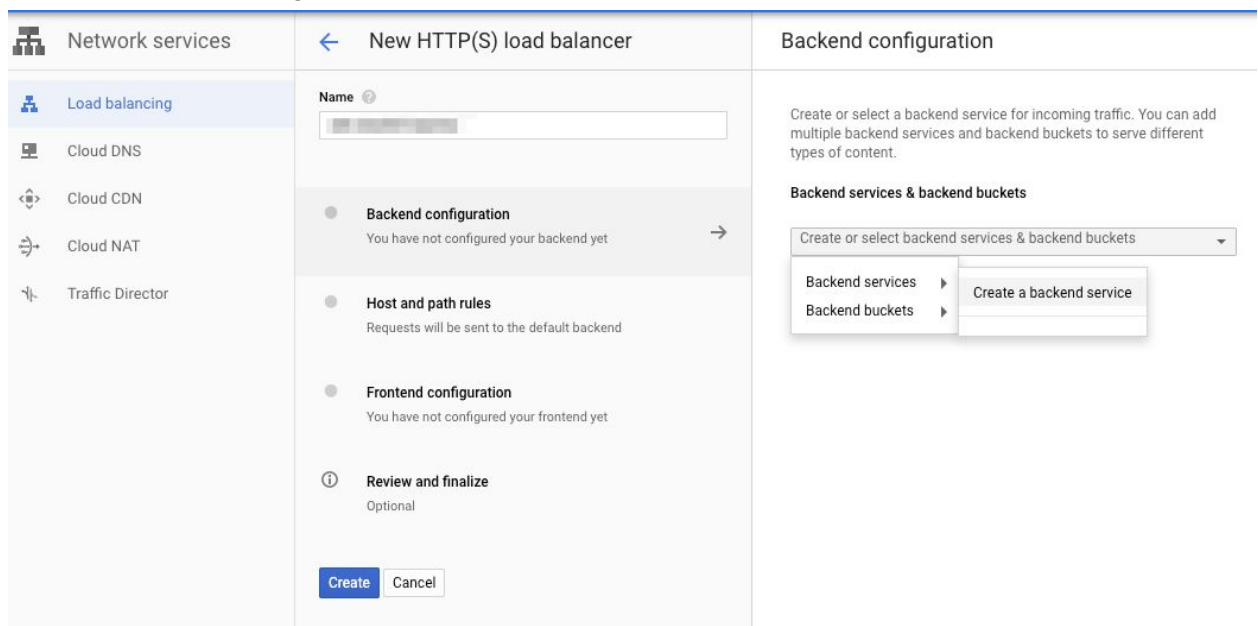
配置好后，点击“Create”按钮创建实例组。

创建负载均衡和CDN

1. 选择HTTP(S) Load Balancing



2. Backend Configuration选择Create a backend service




3. 在新建的Backend service配置中选择之前创建的Instance group，勾选“Enable Cloud CDN”，并选择之前创建的HTTP健康检查。

Create backend service

Name 

backend-nginx-proxy

 Description



Protocol: HTTP Named port: http Timeout: 30 seconds 


Backend type


- ☒ Instance groups
☐ Network endpoint groups


Backends

Regions: asia-southeast1


New backend

Instance group 


mig-cdn-proxy-sg-v1 (asia-southeast1, multi-zone) 

Port numbers 


80


Balancing mode 


☒ Utilization
☐ Rate

Maximum CPU utilization 


80%

Maximum RPS (Optional) 

Max total RPS. Leave blank for unlimited RPS per instance 

Capacity 


100%

 Less


Done

Cancel

 Add backend

Cloud CDN 

☒ Enable Cloud CDN

Health check 

http-healthcheck (TCP) 

port: 80, timeout: 5s, check interval: 10s, unhealthy threshold: 3 attempts

 Advanced configurations (Session affinity, connection draining timeout)

4. 在Frontend configuration中的IP address选择Create IP address，创建一个固定公网地址用于CDN前端访问地址。

配置好后，点击“Create”按钮创建负载均衡和CDN。

负载均衡和CDN大概需要15-20分钟初始化。之后可以访问相关文件进行测试。

修改和更新代理配置

如果源站域名等配置需要修改，可以更新Nginx代理配置，重新上传到配置存储桶覆盖之前文件，并用以下脚本将实例组中所有实例的Nginx运行reload更新配置。

```
#!/bin/bash

# Example: ./nginx_reload.sh mig_nginx

mig_nginx='mig-cdn-proxy-india-v8'
region=asia-south1

if [ "$1" != "" ]; then
    mig_nginx=$1
fi

instance_array=( $(gcloud compute instance-groups list-instances
--region=$region $mig_nginx | cut -d" " -f1) )
total_instances=$(( ${#instance_array[@]} - 1 )
if [ ${#instance_array[@]} -eq 0 ]; then
    echo "Instance Group doesn't exist or is empty!"
    exit
else
    echo "Instance Group has $total_instances instances"
fi

for (( i=1; i<=$(( ${#instance_array[@]} )) - 1; i++ ))
do
    echo -n "Reload Nginx config file on ${instance_array[i]}..."
    gcloud compute ssh ${instance_array[i]} --command="sudo service nginx
reload"
done
```

```
echo -e '\nDone!'
```