基于 Certificate Manager 管理网域证书 -- DNS authentication

Created	@February 23, 2023 1:39 PM
Tags	Certificate GCLB
Author	

一、关于Google Cloud 证书管理器（Certificate Manger)

用来签发和管理 SSL 证书，并配合 HTTPS 负载均衡器来实现传输层安全

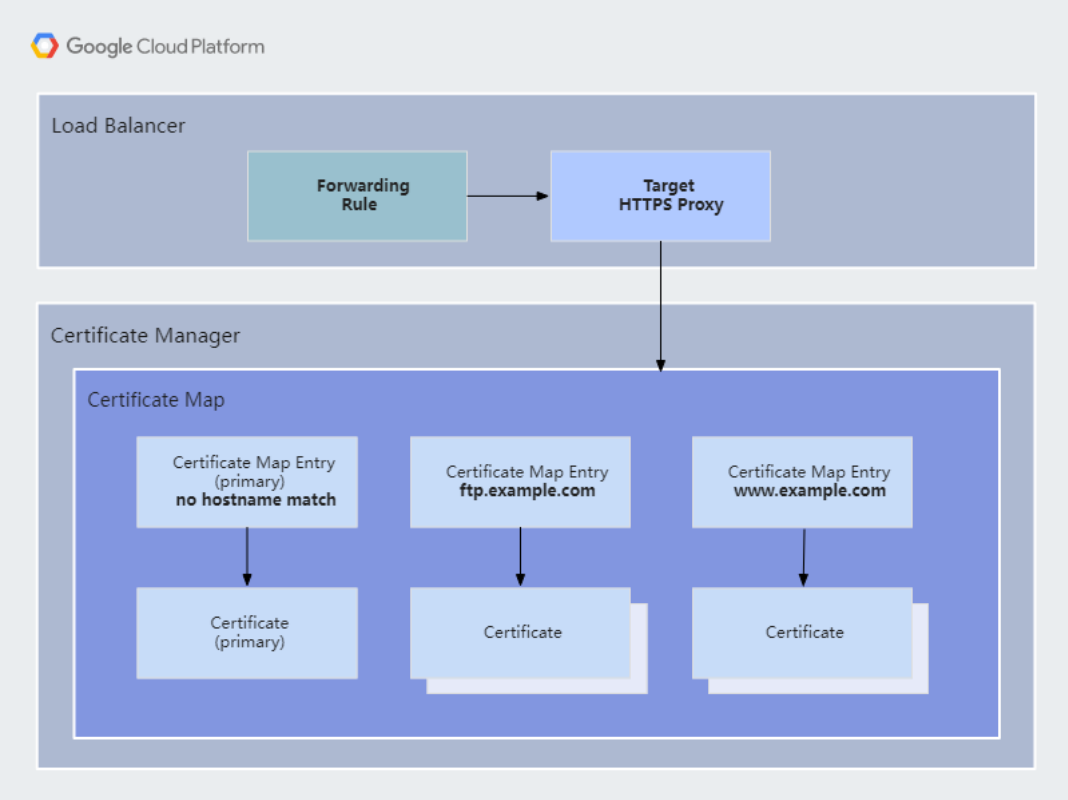
对比于现有负载均衡器授权的使用方式，使用证书管理器有以下优势：

- 支持 Google 管理签发的证书自动颁发和续订
- **支持泛域名证书签发**
- 支持基于 **DNS 的域名验证认证**
- 基于主机名 hostname 控制证书的分配和选择。
- 解除了单一负载均衡器15个证书的限制，Certificate Manager 支持每个负载均衡器多达一百万个证书。

二、Certificate Manager 实现方式：

Certificate Manager 使用灵活的映射机制，使您可以精细控制可以分配哪些证书以及如何为环境中的每个主机名提供这些证书使用。主要包含Certificate Map【证书映射】、证书、证书映射实体、域名所有权认证。

- **DNS 授权**：每个 DNS 授权存储有关设置的 DNS 记录的信息，其中包含单个域及其通配符，例如 mesh.com和 *.mesh.com。
- **证书[Certificates]**: 指定hostname 或域通配符颁发的单个 X.509 传输层安全性 (TLS) (SSL) 证书。
- **证书映射**：引用一个或多个将指定证书分配给特定主机名的证书映射条目，可以一个证书映射关联到不同的负载均衡上使用。
- **证书实体**：指定主机名提供的证书列表。

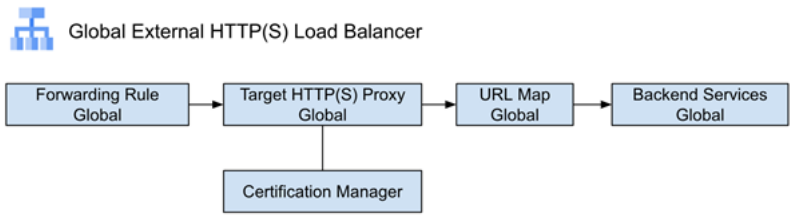


三、场景介绍

1、通常通过load Balancer 授权方式创建证书，往往需要很长时间，这样造成在更新域名或子域名证书时需要较长的停机时间且不支持签发泛域名证书，给实际使用带来了很大的不便利性；使用 Certificate Manager 可以提前创建好证书，然后挂载到相应的 Target HTTPS Proxy 上，大大缩短了停机时间且支持泛域名证书签发。

2、当你的业务需要许多后端服务，同时这些服务需要使用不同的域名来发布时，可以通过使用 Certificate Manager 来动态自动更新证书。

四、使用案例展示



在本实验中，我们将Cloud Storage 作为后端服务，并通过 HTTPS 负载均衡器对外发布。在 URL Map 中，通过证书管理器 Certificate Manager创建SSL 证书，并绑定到 Target HTTPS Proxy 上，最终通过统一的一个 IP 地址对外发布。

1、创建和配置Cert Manager

```
1.1 创建 Certificate Manager DNS Authorizationss
$ gcloud beta certificate-manager dns-authorizations create dns-auth-mesh --domain=mesh.com.cn
Create request issued for: [dns-auth-mesh]
Waiting for operation [projects/yunion-test-286209/locations/global/operations/operation-1661222053860-5e6df6669d41b-91dc6bf0-cf25df1d
...done.
Created dnsAuthorization [dns-auth-mesh].

1.2 查看DNS Authentication Value，通常是CNAME 值：
$ gcloud certificate-manager dns-authorizations list
```

```
NAME: ccm-dns-auth-home
DOMAIN: home.mesh.com.cn
DNS_RECORD: _acme-challenge.home.mesh.com.cn.
RECORD_TYPE: CNAME
DNS_VALUE: a91c93b3-8ac4-4xxxxxdf0804.12.authorize.certificatemanager.goog.


$ gcloud certificate-manager dns-authorizations describe  dns-auth-mesh
createTime: '2022-08-23T02:34:14.047844357Z'
dnsResourceRecord:
  data: 211e25e7-e689-4087-bdde-50afb58f9c85.16.authorize.certificatemanager.goog.
  name: _acme-challenge.mesh.com.cn.
  type: CNAME
domain: mesh.com.cn
name: projects/yunion-test-286209/locations/global/dnsAuthorizations/dns-auth-mesh
updateTime: '2022-08-23T02:34:14.660549270Z'
```

1.3 在DNS 控制台添加CNAME 记录值，验证域名所有：

具体取决DNS 托管服务，配置方式，以DNSPod 为例：


```
1.4 配置cert manager 签发证书
$ gcloud certificate-manager certificates create home-cert --domains=*.mesh.com.cn --dns-authorizations=dns-auth-mesh
Create request issued for: [home-cert]
Waiting for operation [projects/yunion-test-286209/locations/global/operations/operation-1661223164418-5e6dfa89b999a-9aeac7be-62e567ba
...done.
Created certificate [home-cert].

1.5 查看cert manager 签发证书状态：
$ gcloud beta certificate-manager certificates describe ccm-cert-home-0
createTime: '2022-08-22T14:55:57.056426568Z'
expireTime: '2022-11-20T14:05:15Z'
managed:
  authorizationAttemptInfo:
  - domain: home.mesh.com.cn
    state: AUTHORIZED
............
pemCertificate: |
  -----BEGIN CERTIFICATE-----
  MIIFZTCCBE2gAwIBAgIRAIkQmo3l/+KUEMvo3PgeqZ4wDQYJKoZIhvcNAQELBQAw
  ..........
  ivm63XTzP91kHHIa2Si+cMV6PHsv9UMUTi2EDaYGYc7FGGQS8ohhjJVx4B0BnL95
  XVNPlqPq9ZzreWqVxcOYE6/BDZ6/Qh8qwlYz2S7ZFo4qMSGwgW8ty2w3cHaK1MVZ
  H8IbNKhGJZEuLyk7T0s4YYTk5onCObkwkRsfoUT/juZY/cJqavN3qW4+hgG5rakZ
  BDkanOwYczkqi1LAg6hPVR5We58sAotvaqsSGU2V4dtN0wuRAbSFXvA=
  -----END CERTIFICATE-----
  -----BEGIN CERTIFICATE-----
  MIIFjDCCA3SgAwIBAgINAgCOsgIzNmWLZM3bmzANBgkqhkiG9w0BAQsFADBHMQsw
  ..........
  JDwRjW/656r0KVB02xHRKvm2ZKI03TglLIpmVCK3kBKkKNpBNkFt8rhafcCKOb9J
  x/9tpNFlQTl7B39rJlJWkR17QnZqVptFePFORoZmFzM=
  -----END CERTIFICATE-----
  -----BEGIN CERTIFICATE-----
  MIIFYjCCBEqgAwIBAgIQd70NbNs2+RrqIQ/E8FjTDTANBgkqhkiG9w0BAQsFADBX
  .......
  +qduBmpvvYuR7hZL6Dupszfnw0Skfths18dG9ZKb59UhvmaSGZRVbNQpsg3BZlvi
  d0lIKO2d1xozclOzgjXPYovJJIultzkMu34qQb9Sz/yilrbCgj8=
  -----END CERTIFICATE-----
sanDnsnames:
- home.mesh.com.cn
updateTime: '2022-08-22T14:55:57.360080809Z'

-----
PROVISIONING 状态，说明dns-auth 已经验证过，现在需要等待签发证书，
注：[一般证书签发需要在几分钟到半个小时左右]
$ gcloud certificate-manager certificates describe home-cert
[大概10min 完成了证书签发]
createTime: '2022-08-23T02:52:44.553453560Z'
managed:
  authorizationAttemptInfo:
  - domain: '*.mesh.com.cn'
    state: AUTHORIZING
  dnsAuthorizations:
  - projects/587936279668/locations/global/dnsAuthorizations/dns-auth-mesh
  domains:
  - '*.mesh.com.cn'
```

```
  state: PROVISIONING
name: projects/yunion-test-286209/locations/global/certificates/home-cert
sanDnsnames:
- '*.mesh.com.cn'
updateTime: '2022-08-23T02:52:44.894467832Z'
```

查看已经签发的Certification，有EXPIRE_TIME 说明证书也已经签发完成了：

```
$ gcloud certificate-manager certificates list
NAME: ccm-cert-all
SUBJECT_ALTERNATIVE_NAMES: *.home.mesh.com.cn
DESCRIPTION:
SCOPE:
EXPIRE_TIME: 2022-11-21 00:17:53 +00:00
CREATE_TIME: 2022-08-23 01:08:35 +00:00
UPDATE_TIME: 2022-08-23 01:08:35 +00:00
```

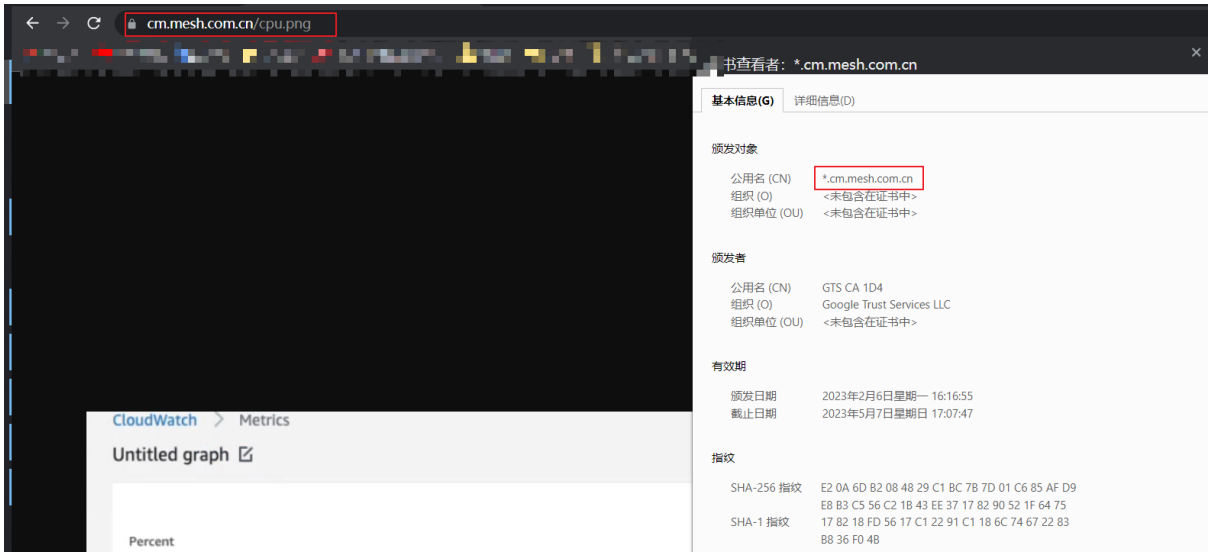
创建用于关联负载均衡器的证书映射Maps:

```
# 通过DNS AUTH 方式创建证书
$ gcloud certificate-manager certificates create cm-mesh-com-cn-crt0 \
  --domains=cm.mesh.com.cn --dns-authorizations=cm-mesh-com-cn-dnsauth
Create request issued for: [cm-mesh-com-cn-crt0]
Waiting for operation [projects/yunion-test-286209/locations/global/operations/operation-1675678072902-5f405344b142b-73fff750-d09957d3
Created certificate [cm-mesh-com-cn-crt0].

## 查看证书：
$ gcloud certificate-manager certificates describe cm-mesh-com-cn-crt0
createTime: '2023-02-06T10:07:53.040703874Z'
expireTime: '2023-05-07T10:07:54Z'
managed:
  authorizationAttemptInfo:
  - domain: cm.mesh.com.cn
    state: AUTHORIZED
  dnsAuthorizations:
  - projects/587936279668/locations/global/dnsAuthorizations/cm-mesh-com-cn-dnsauth
  domains:
  - cm.mesh.com.cn
  state: ACTIVE
name: projects/yunion-test-286209/locations/global/certificates/cm-mesh-com-cn-crt0
pemCertificate: |

### 创建证书映射 Map
gcloud certificate-manager maps create CERTIFICATE_MAP_NAME

## 将证书与Entry 关联添加到Maps 中：
$ gcloud certificate-manager maps entries create cm-mesh-com-cn-entry0
 --map="cm-mesh-com-cn-maps"   --certificates="cm-mesh-com-cn-crt0"
 --hostname="cm.mesh.com.cn"

## 查看Entry 状态：
$ gcloud certificate-manager maps entries create cm-mesh-com-cn-entry0 \
  --map="cm-mesh-com-cn-maps"   --certificates="cm-mesh-com-cn-crt0"   \
  --hostname="cm.mesh.com.cn"
```

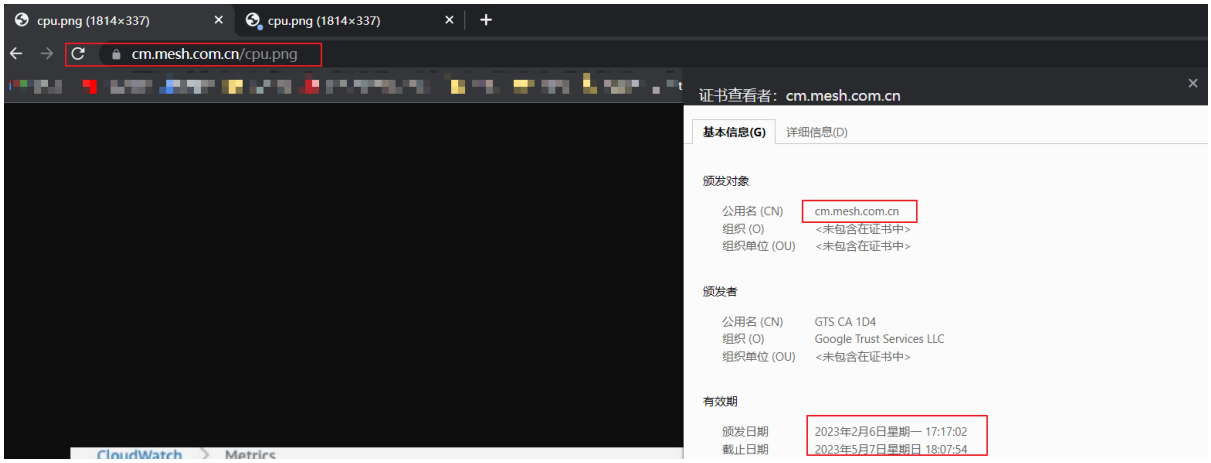
将签发的maps 部署到LB上：

```
## gcloud compute target-https-proxies update gcs-lb-target-proxy-2
--certificate-map="cm-mesh-com-cn-maps"
```

访问验证SSL 证书签发有效性：



签发cm.mesh.com.cn 证书：



Cert Manager 创建的证书：

1、不能在console 中直接查看，只能通过gcloud

2、不能直接在console 中，绑定LB 使用

3、*.domain.com 不包含domain.com 证书 会返回SSL Error

4、在Map 中直接添加Cert Entry 就可以，不需要更新target Proxy

参考：

1、`https://cloud.google.com/certificate-manager/docs/deploy-google-managed-dns-auth#verify_that_the_certificate_is_active`

2、https://cloud.google.com/certificate-manager/docs/deploy-google-managed-dns-auth