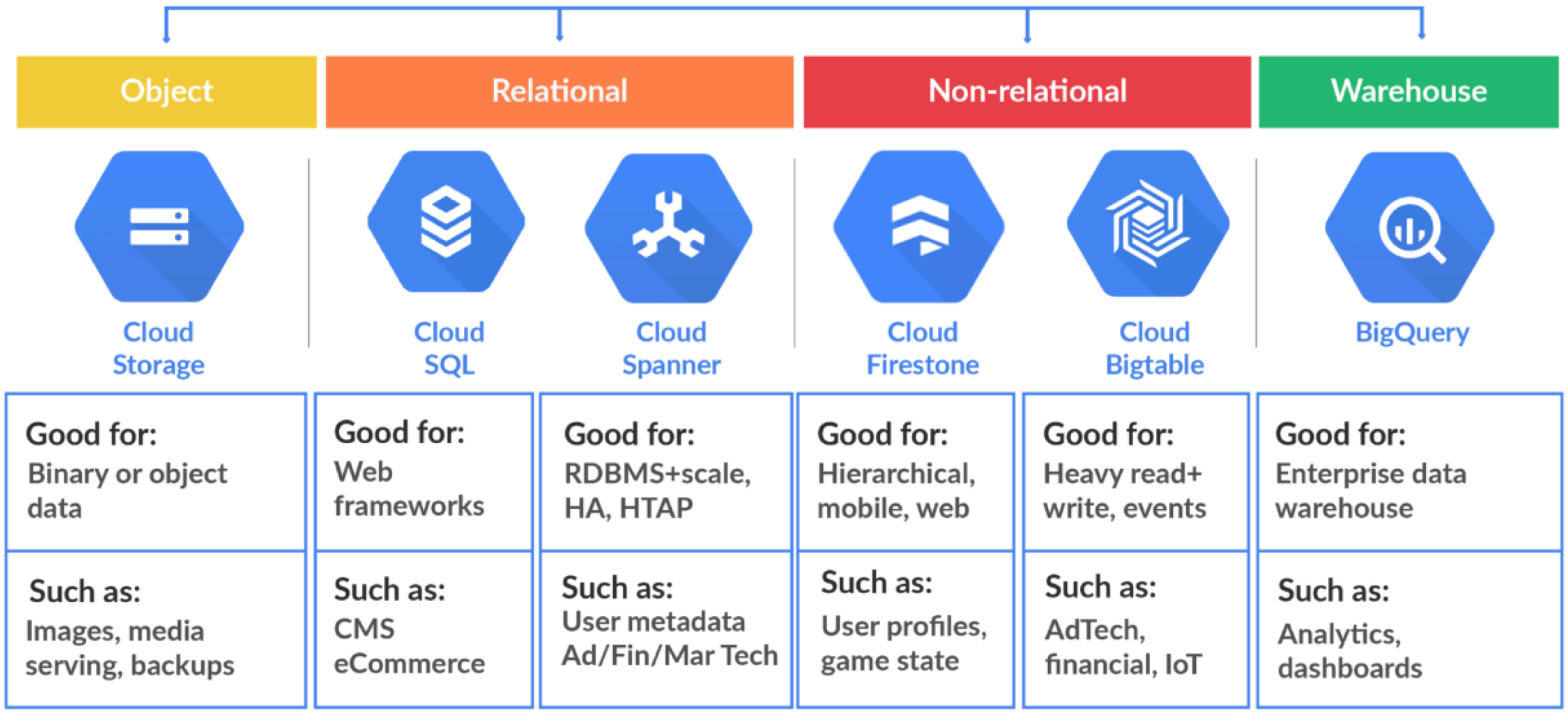
Cloud SQL

投資程式設計科 DevOps 組

Outline

- Storage and Databases on GCP
  - Storage
  - Databases
- Cloud SQL Introduction
- Lab: Cloud SQL for PostgreSQL: Qwik Start
  - Connect Cloud SQL from VM
- Cloud SQL Auth Proxy
- Cloud SQL with private IP only

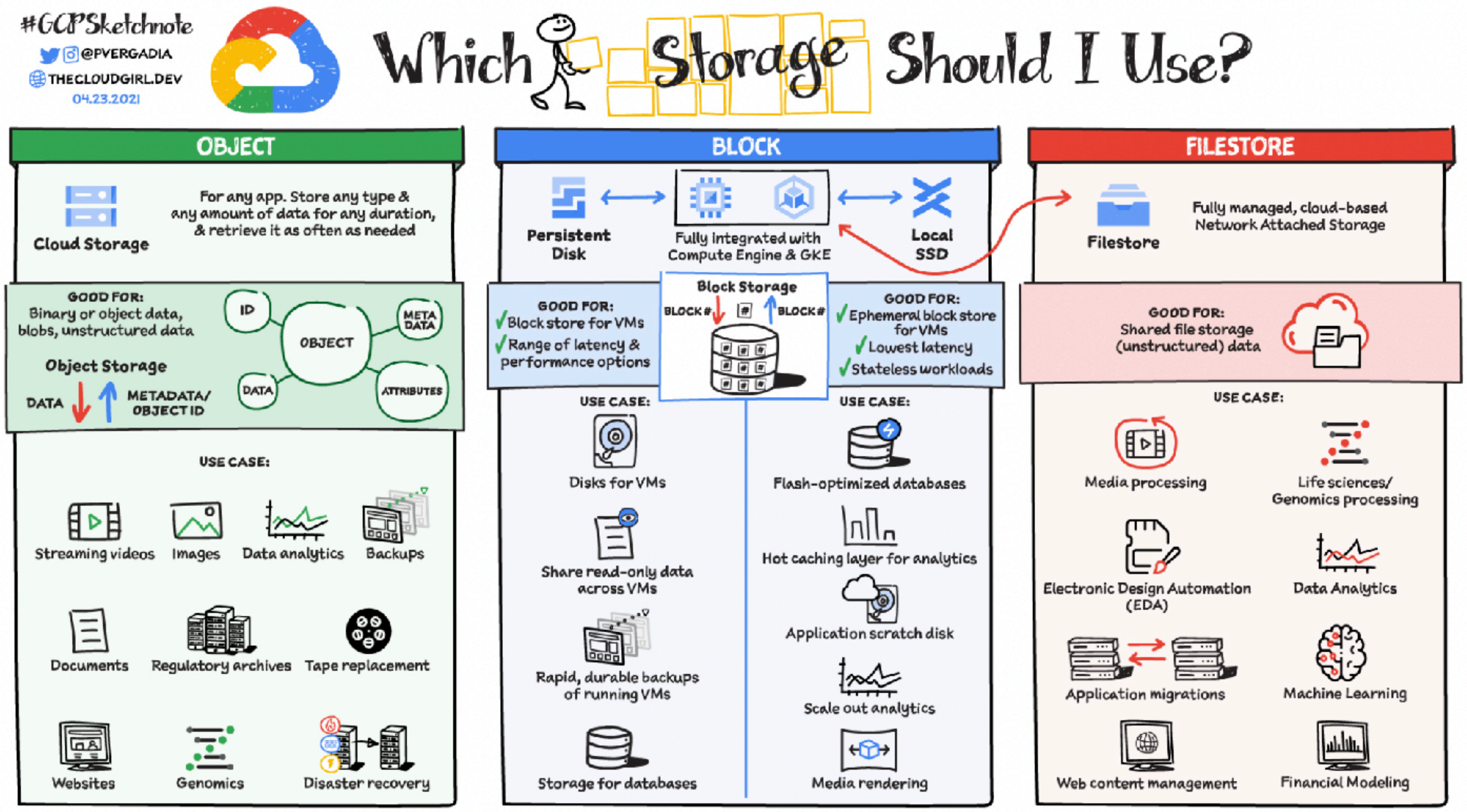
Storage and Databases on GCP



Object	Relational		Non-relational		Warehouse
Cloud Storage	Cloud SQL	Cloud Spanner	Cloud Firestone	Cloud Bigtable	BigQuery
Good for: Binary or object data	**Good for:** Web frameworks	**Good for:** RDBMS+scale, HA, HTAP	**Good for:** Hierarchical, mobile, web	**Good for:** Heavy read+ write, events	**Good for:** Enterprise data warehouse
Such as: Images, media serving, backups	**Such as:** CMS eCommerce	**Such as:** User metadata Ad/Fin/Mar Tech	**Such as:** User profiles, game state	**Such as:** AdTech, financial, IoT	**Such as:** Analytics, dashboards

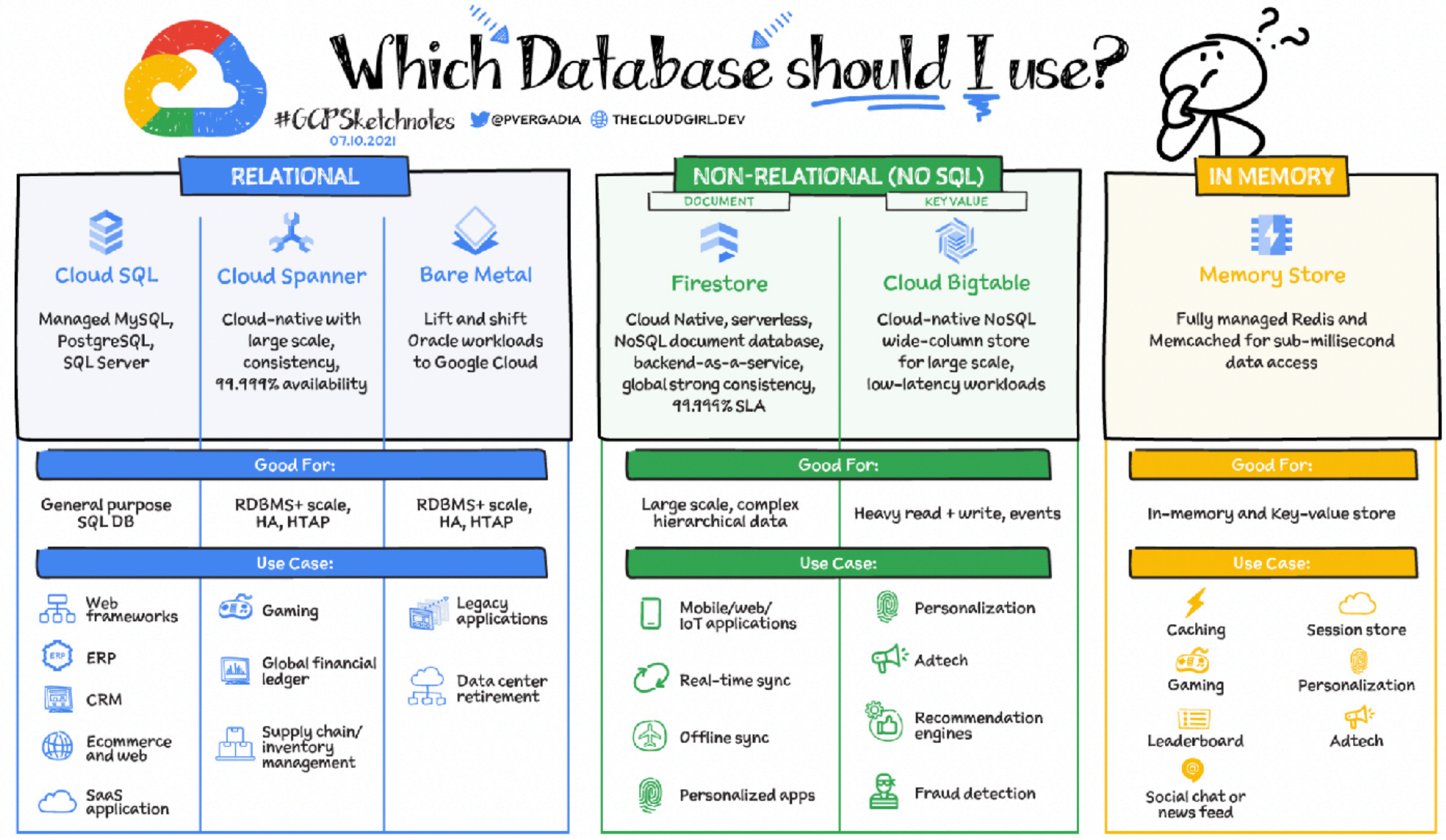
Source: https://www.diarioviral.net/google-cloud-hosting-cost/

Storage



Source: https://thecloudgirl.dev/StorageOptions.html

Databases



Which Database should I use?

#GCPSketchnotes @PVERGADIA THECLOUDGIRL.DEV

07.10.2021

RELATIONAL

Cloud SQL

Managed MySQL, PostgreSQL, SQL Server

Cloud Spanner

Cloud-native with large scale, consistency, 99.999% availability

Bare Metal

Lift and shift Oracle workloads to Google Cloud

Good For:

Cloud SQL	Cloud Spanner	Bare Metal
General purpose SQL DB	RDBMS+ scale, HA, HTAP	RDBMS+ scale, HA, HTAP

Use Case:

Cloud SQL	Cloud Spanner	Bare Metal
Web frameworks ERP CRM Ecommerce and web SaaS application	Gaming Global financial ledger Supply chain/ inventory management	Legacy applications Data center retirement

NON-RELATIONAL (NO SQL)

DOCUMENT

Firestore

Cloud Native, serverless, NoSQL document database, backend-as-a-service, global strong consistency, 99.999% SLA

KEY VALUE

Cloud Bigtable

Cloud-native NoSQL wide-column store for large scale, low-latency workloads

Good For:

Firestore	Cloud Bigtable
Large scale, complex hierarchical data	Heavy read + write, events

Use Case:

Firestore	Cloud Bigtable
Mobile/web/ IoT applications Real-time sync Offline sync Personalized apps	Personalization Adtech Recommendation engines Fraud detection

IN MEMORY

Memory Store

Fully managed Redis and Memcached for sub-millisecond data access

Good For:

In-memory and Key-value store

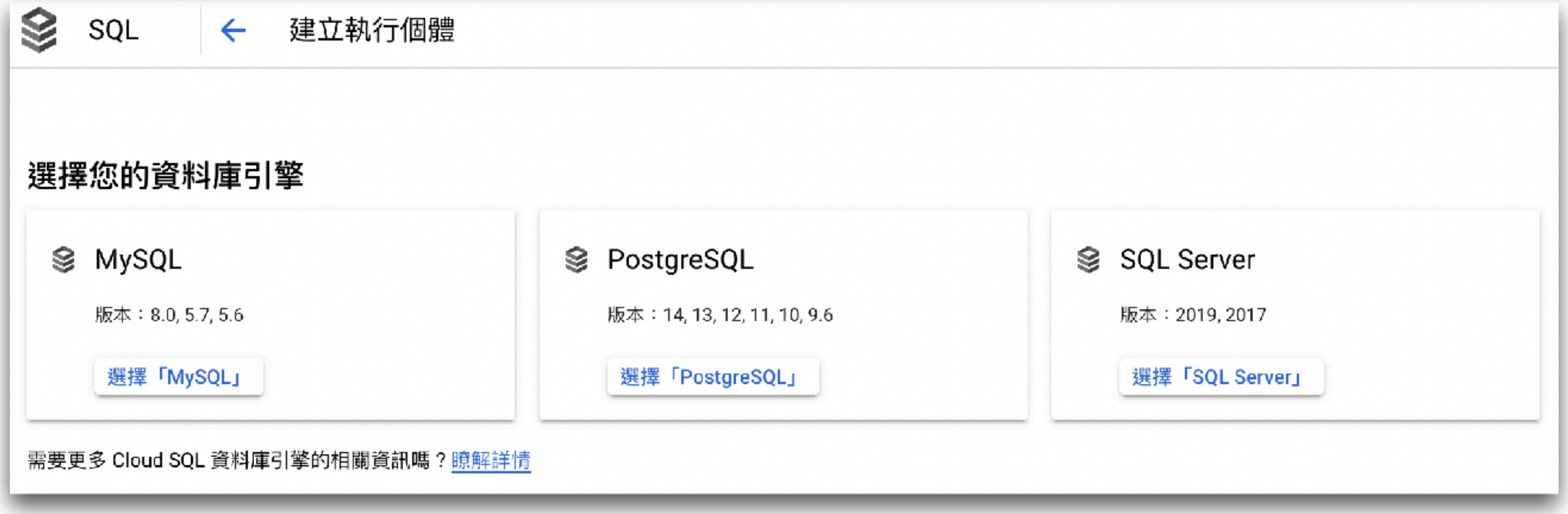
Use Case:

- Caching
- Session store
- Gaming
- Personalization
- Leaderboard
- Adtech
- Social chat or news feed

Source: https://thecloudgirl.dev/dboptions.html

Cloud SQL

- https://cloud.google.com/sql
- Googel 全代管資料庫服務
- 支援 DB：MySQL, PostgreSQL, SQL Server



選擇您的資料庫引擎

MySQL

版本：8.0, 5.7, 5.6

PostgreSQL

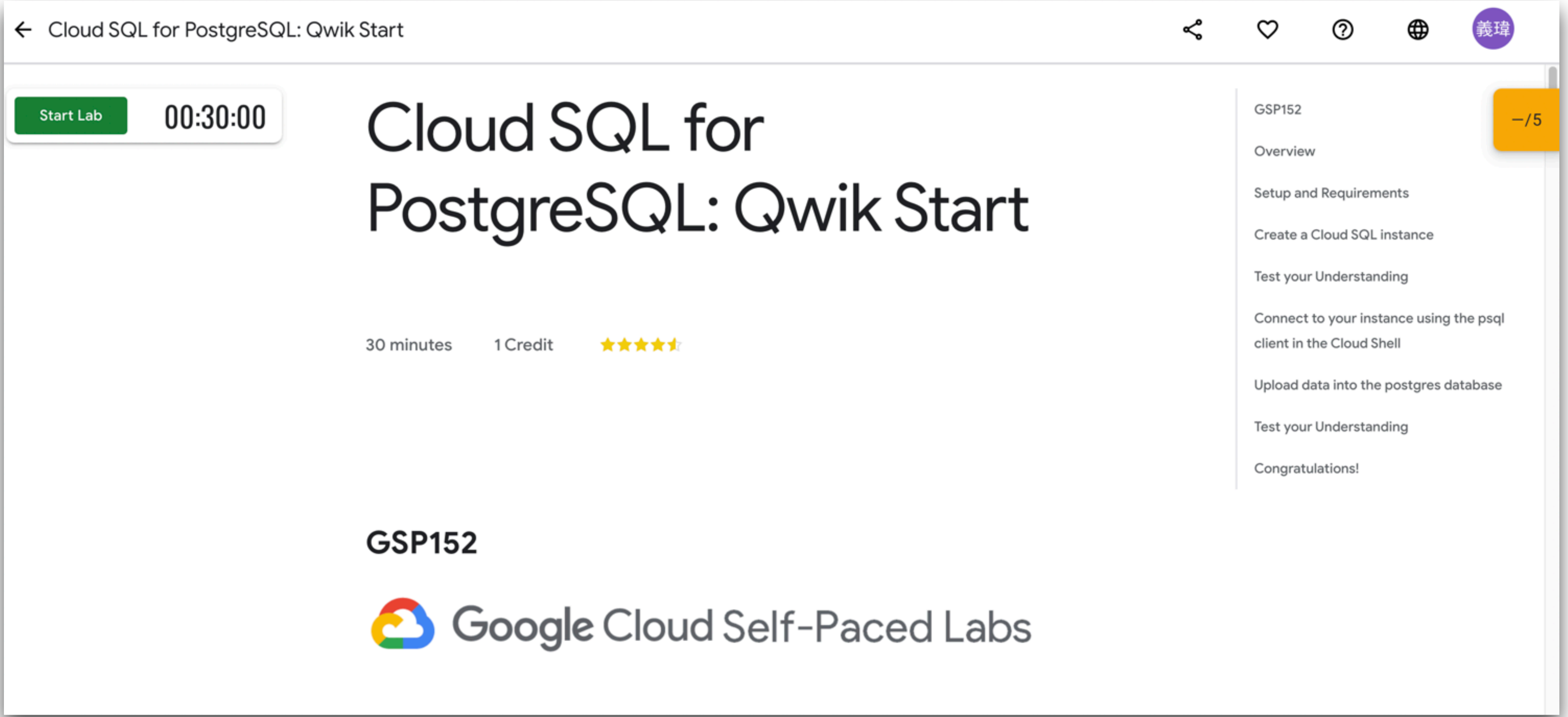
版本：14, 13, 12, 11, 10, 9.6

SQL Server

版本：2019, 2017

需要更多 Cloud SQL 資料庫引擎的相關資訊嗎？瞭解詳情

Lab: Cloud SQL for PostgreSQL: Qwik Start



Cloud SQL for PostgreSQL: Qwik Start

30 minutes 1 Credit ★★★★★

GSP152

Overview

Setup and Requirements

Create a Cloud SQL instance

Test your Understanding

Connect to your instance using the psql client in the Cloud Shell

Upload data into the postgres database

Test your Understanding

Congratulations!

GSP152

Google Cloud Self-Paced Labs

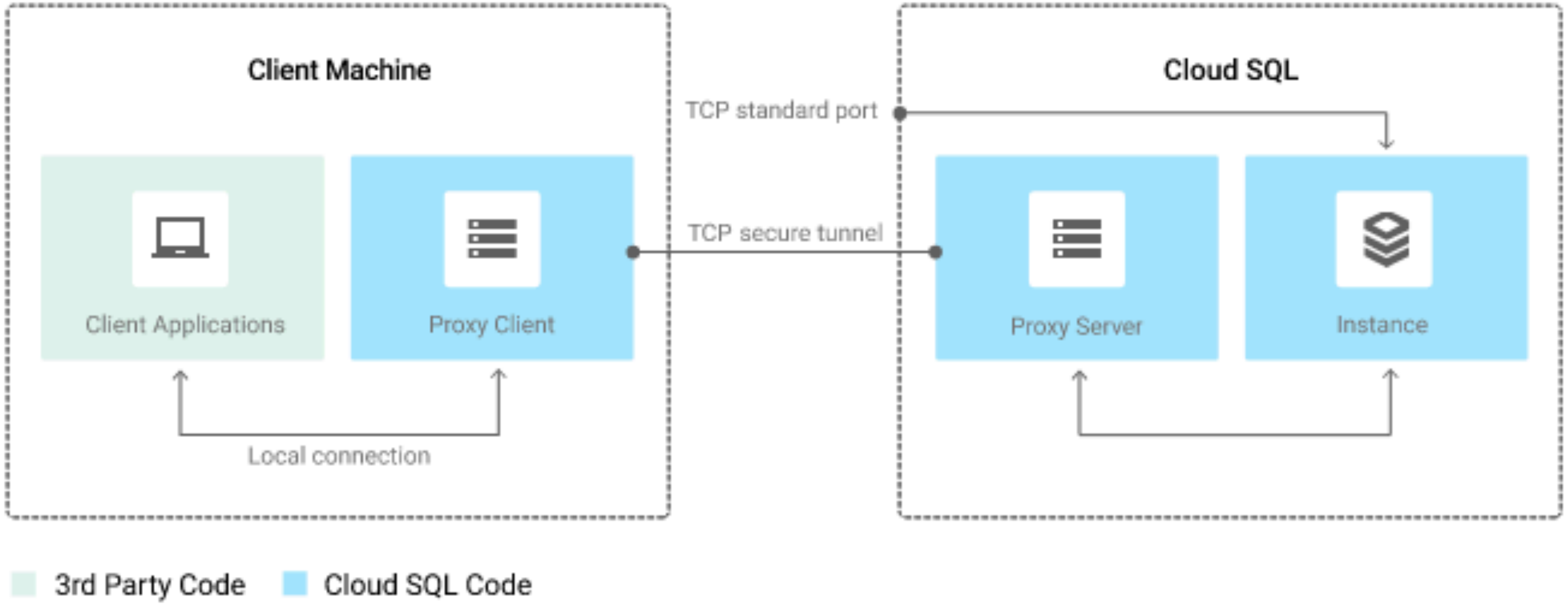
https://www.cloudskillsboost.google/focuses/937?parent=catalog

Connect Cloud SQL from VM

- 啟動一台 VM
- 將 VM 的 Public IP 加入 Cloud SQL Instance Connection 的 Authorized networks
- 安裝 PostgreSQL Client
    - sudo apt-get install -y postgresql-client
- 連接 DB
    - psql "sslmode=disable dbname=postgres user=postgres hostaddr=PUBLIC_IP”
- 列出 DB 中的 guestbook Table
    - SELECT * FROM guestbook;
- 列出 DB 中的 User
    - \du

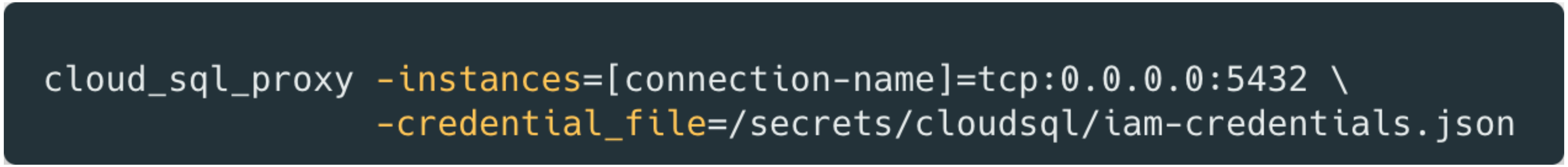
Cloud SQL Auth Proxy (SQL Proxy)

- https://cloud.google.com/sql/docs/mysql/sql-proxy
- https://github.com/GoogleCloudPlatform/cloudsql-proxy
- Cloud SQL 預設將所有連線阻擋，需額外設定白名單 IP 才能連入
- SQL Proxy 以加密方式並透過 IAM 進行認證與 DB Instance 連線



Cloud SQL Auth Proxy (SQL Proxy)

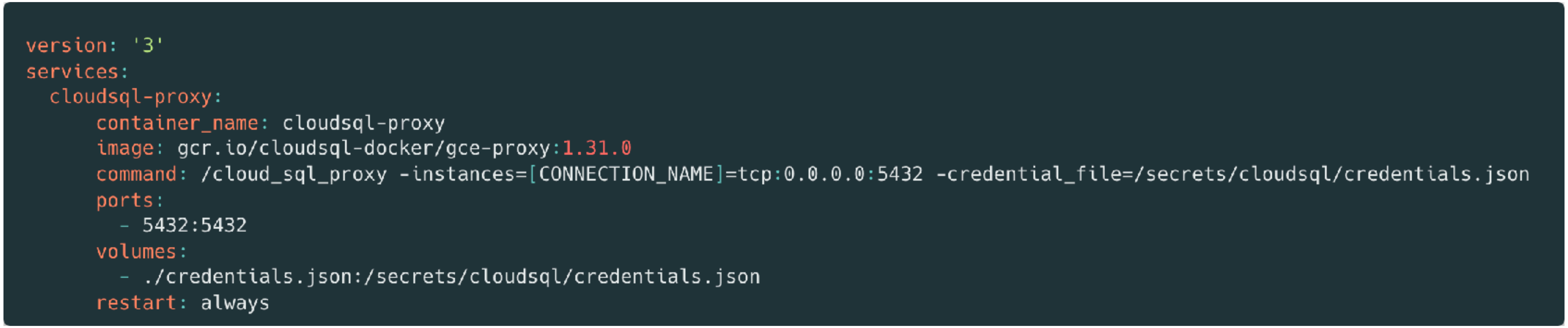
- 使用方式
  - Binary (Linux, macOS, Windows)
- Command
  - TCP socket example



```
cloud_sql_proxy -instances=[connection-name]=tcp:0.0.0.0:5432 \
                -credential_file=/secrets/cloudsql/iam-credentials.json
```

Cloud SQL Auth Proxy (SQL Proxy)

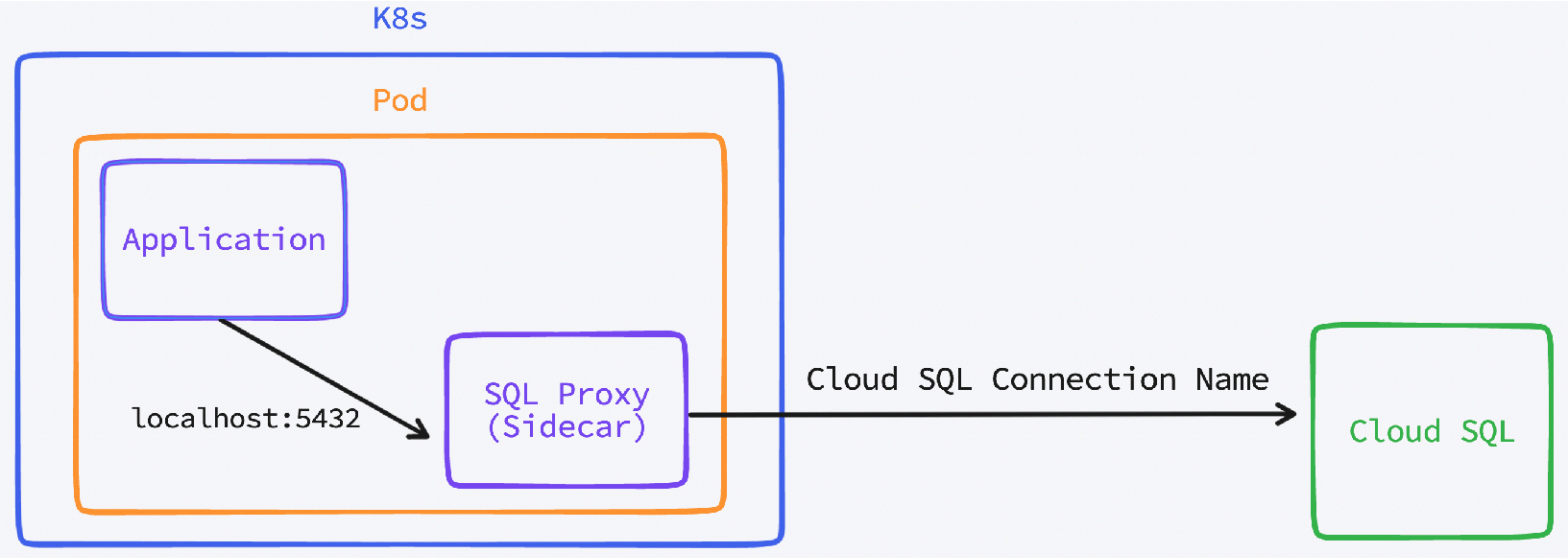
- 使用方式
  - Container (gcr.io/cloudsql-docker/gce-proxy:1.31.0)
- Docker Compose
  - https://github.com/cathaylife-devops/gcp-workshop/2022-06-27-cloud_sql/



```
version: '3'
services:
  cloudsql-proxy:
      container_name: cloudsql-proxy
      image: gcr.io/cloudsql-docker/gce-proxy:1.31.0
      command: /cloud_sql_proxy -instances=[CONNECTION_NAME]=tcp:0.0.0.0:5432 -credential_file=/secrets/cloudsql/credentials.json
      ports:
        - 5432:5432
      volumes:
        - ./credentials.json:/secrets/cloudsql/credentials.json
      restart: always
```

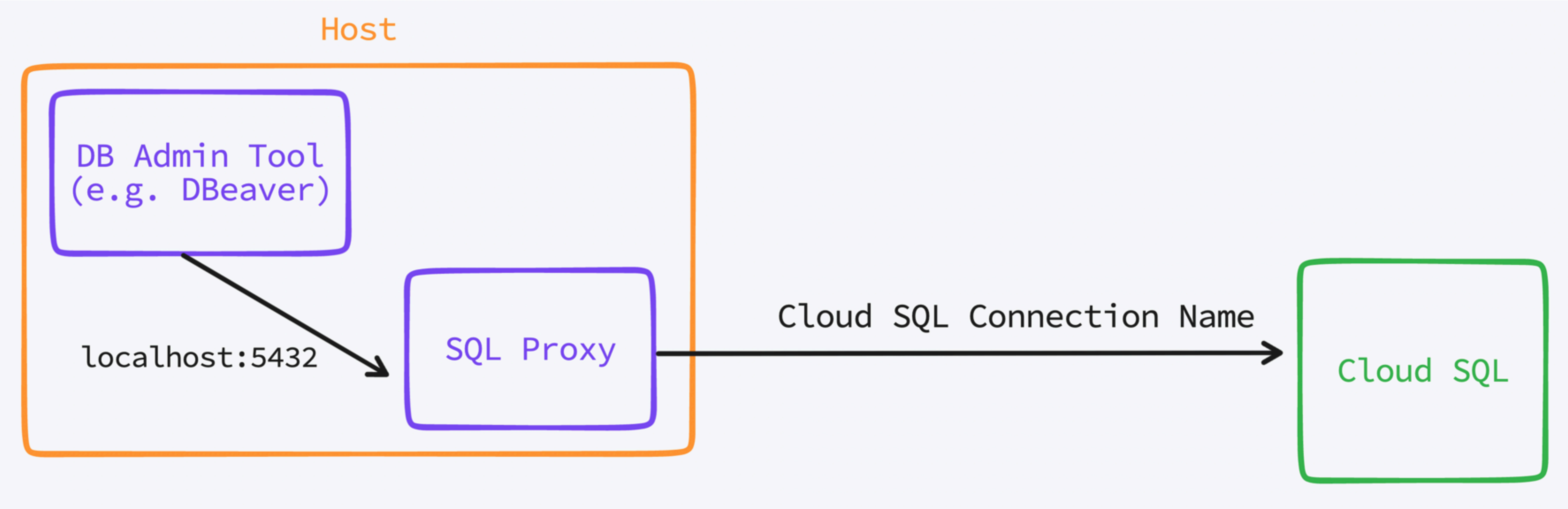
Cloud SQL Auth Proxy (SQL Proxy)

- 使用情境
  - K8s



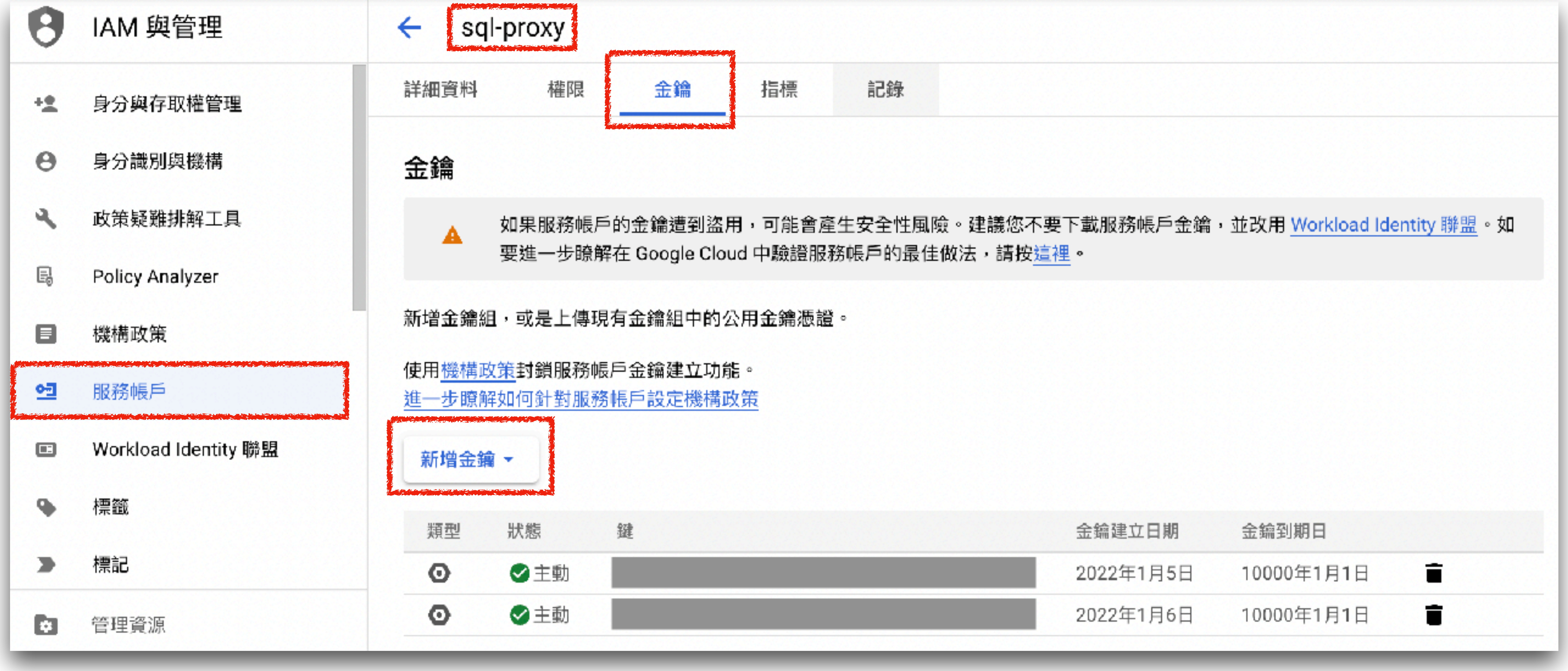
Cloud SQL Auth Proxy (SQL Proxy)

- 使用情境
  - DB Administration tool



Cloud SQL Auth Proxy (SQL Proxy)

- Credential File
  - 於 IAM 建立一組有「Cloud SQL 用戶端」角色的 Service Account
  - 生成一組 Key 供 SQL Proxy 使用



金鑰

如果服務帳戶的金鑰遭到盜用，可能會產生安全性風險。建議您不要下載服務帳戶金鑰，並改用 Workload Identity 聯盟。如要進一步瞭解在 Google Cloud 中驗證服務帳戶的最佳做法，請按這裡。

新增金鑰組，或是上傳現有金鑰組中的公用金鑰憑證。

使用機構政策封鎖服務帳戶金鑰建立功能。
進一步瞭解如何針對服務帳戶設定機構政策

新增金鑰 ▾

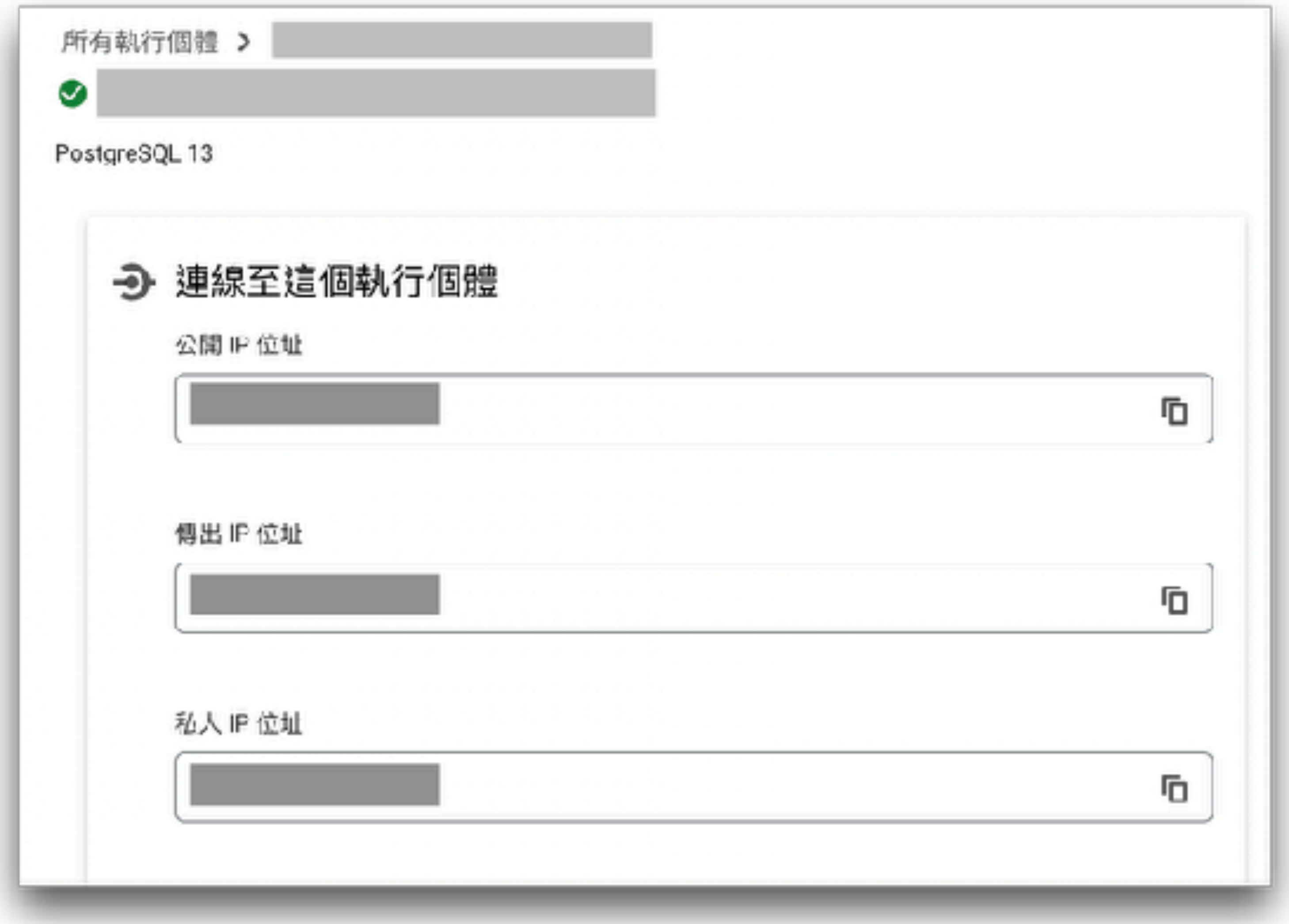
類型	狀態	鍵	金鑰建立日期	金鑰到期日	
⚙	✓主動	[redacted]	2022年1月5日	10000年1月1日	🗑
⚙	✓主動	[redacted]	2022年1月6日	10000年1月1日	🗑

Cloud SQL Auth Proxy (SQL Proxy)

SQL Proxy Demo

Cloud SQL with private IP only

- Private IP Only
  - 只配發 Private IP 給 Cloud SQL Instance
  - 服務需位於相同 VPC 下，或位於與 Cloud SQL VPC Peering 串連的 VPC 才能連接



所有執行個體 > [redacted]

[redacted]

PostgreSQL 13

連線至這個執行個體

公開 IP 位址

[redacted]

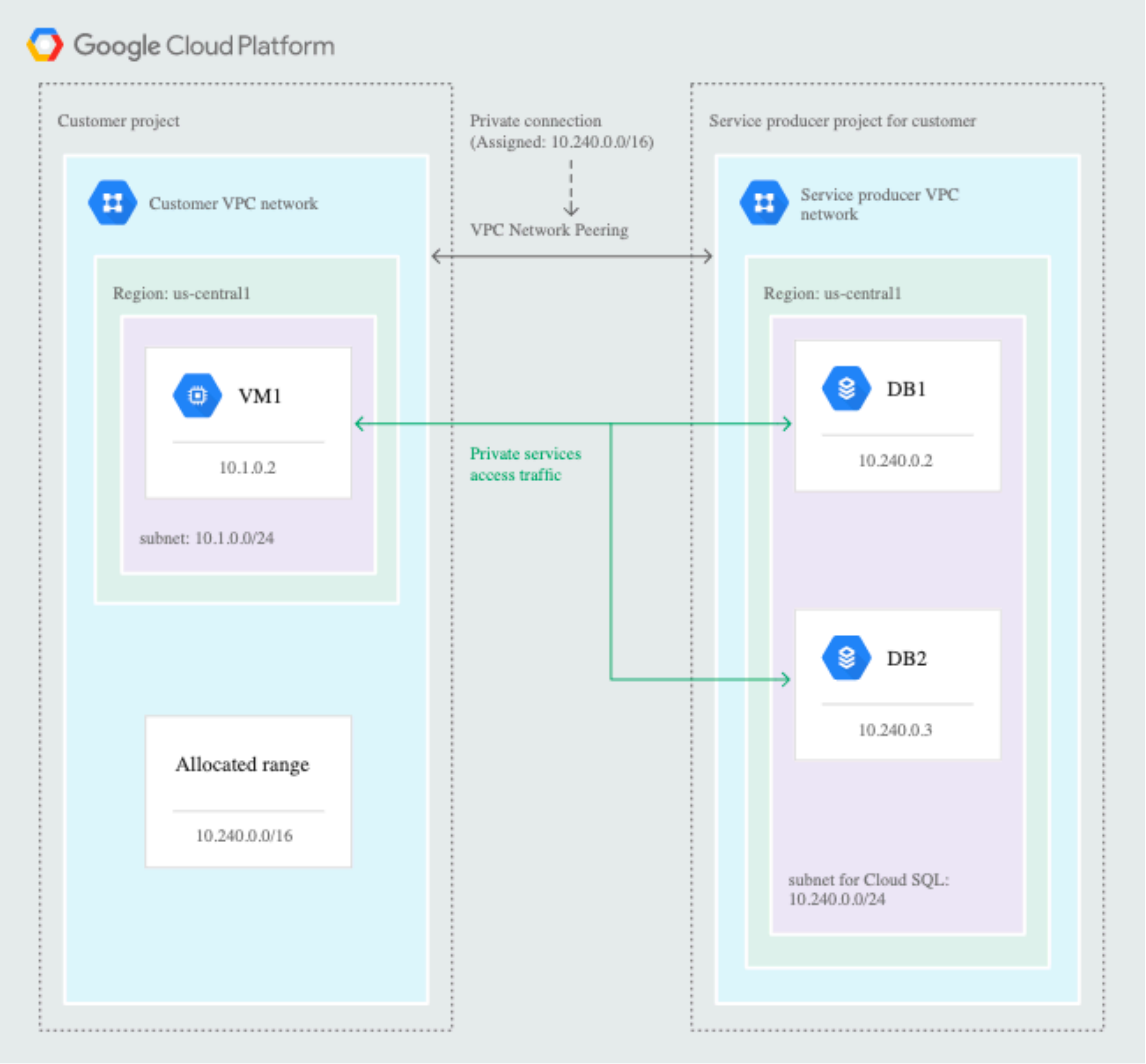
傳出 IP 位址

[redacted]

私人 IP 位址

[redacted]

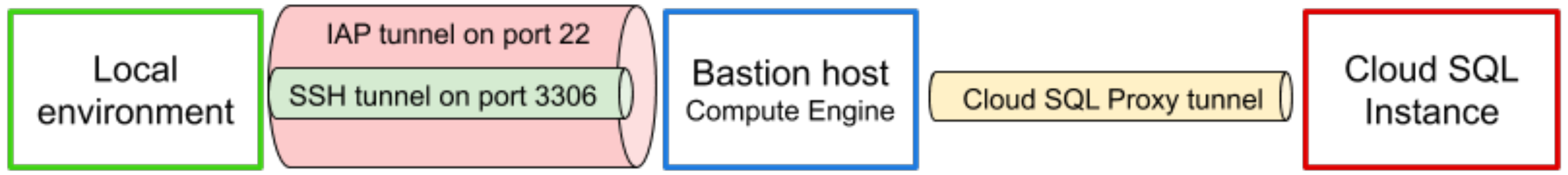
同時配有 Public 與 Private IP 的 Cloud SQL Instance



服務連接範例 Ref: GCP Doc

Cloud SQL with private IP only

- Cloud SQL with private IP only: the Good, the Bad and the Ugly
  - 介紹 Cloud SQL 只有 Private IP 時在以下三個情境下的連線方式
    - Compute Engine connectivity
    - Serverless services connectivity
    - Local environment connectivity
  - 針對禁止使用 Public IP 討論
    - 透過 Firewall Rule 與 Organization Policy 阻擋所有 IP 連入即可
    - Eventually, **allowing a public IP** on Cloud SQL instances **avoids a lot of workaround and strange designs** to deal with, and **without decreasing the security level**.



Local 透過跳板 (Bastion) 連接
Private IP Only Cloud SQL 示意圖