

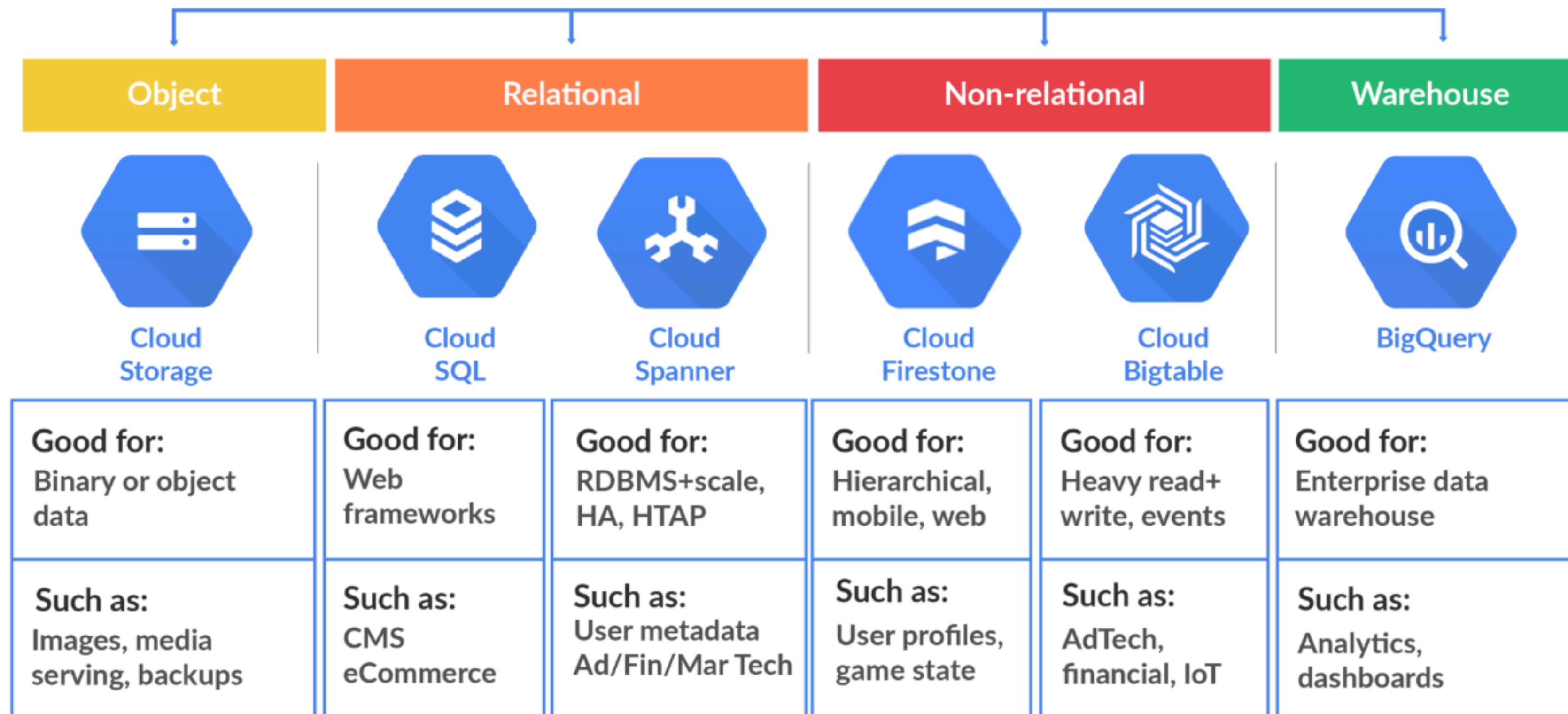
# Cloud SQL

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



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



# Storage

#GCPSketchnote

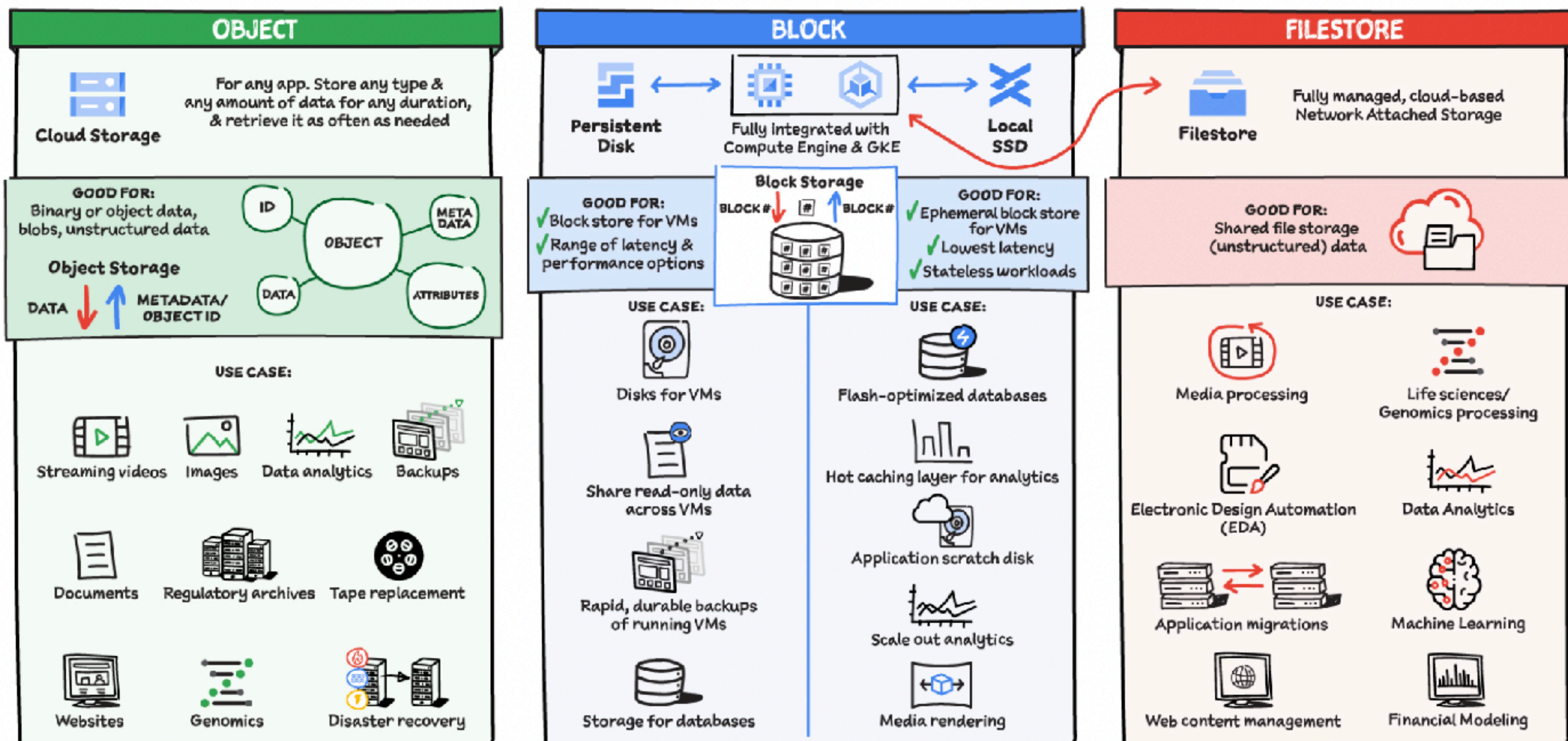
@PVERGADIA

THECLOUDGIRL.DEV

04.23.2021



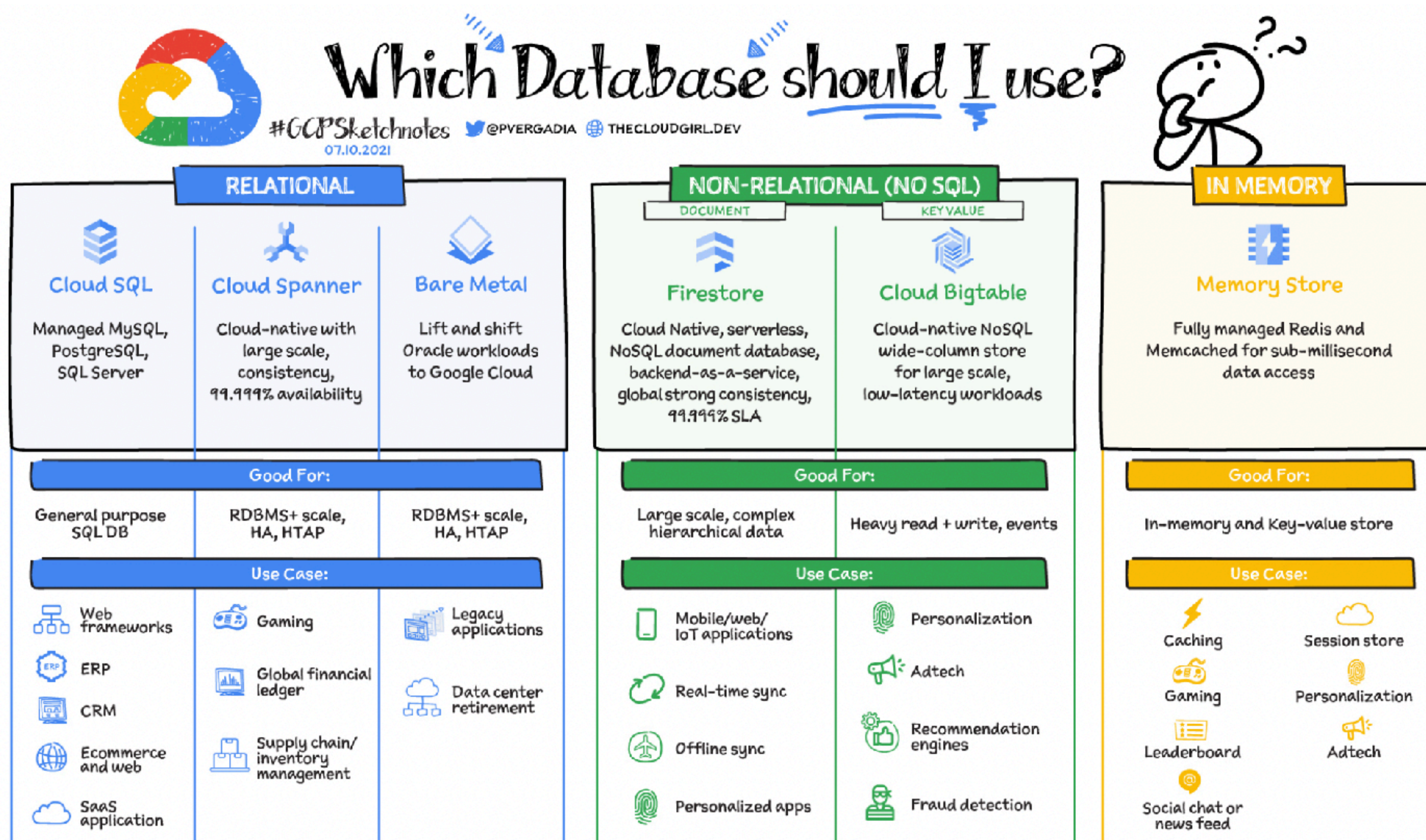
## Which Storage Should I Use?



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



# Databases

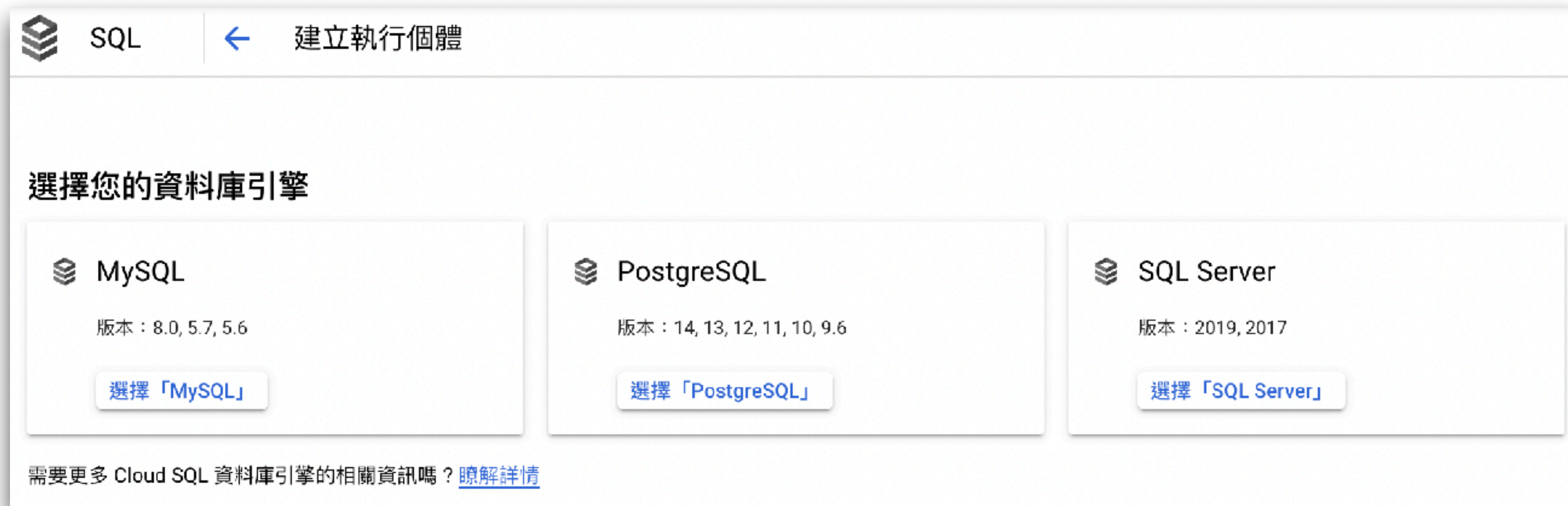


Source: <https://thecloudgirl.dev/dboptions.html>



# Cloud SQL

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



# Lab: Cloud SQL for PostgreSQL: Qwik Start

The screenshot shows the Google Cloud Self-Paced Labs interface for the lab 'Cloud SQL for PostgreSQL: Qwik Start'. The lab is identified by the code 'GSP152'. It has a duration of 30 minutes, is worth 1 credit, and has a 4.5-star rating. A 'Start Lab' button and a timer showing '00:30:00' are in the top left. The main title 'Cloud SQL for PostgreSQL: Qwik Start' is prominently displayed. On the right, a table of contents lists the lab's steps: 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, and Congratulations!. A progress indicator shows '-/5'.


← Cloud SQL for PostgreSQL: Qwik Start

Start Lab 00:30:00

## Cloud SQL for PostgreSQL: Qwik Start

30 minutes 1 Credit ★★★★★

GSP152

 Google Cloud Self-Paced Labs

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!

-/5

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

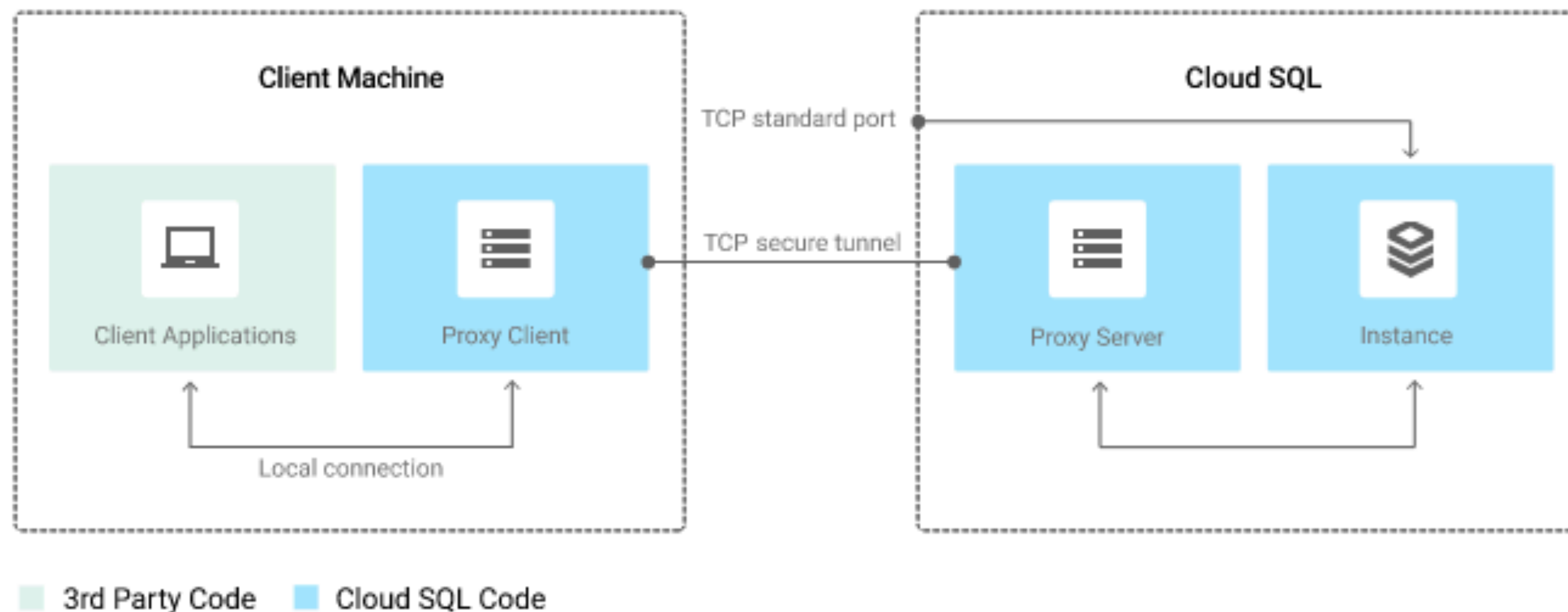
# Connect Cloud SQL from VM

- 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/postgres/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
```



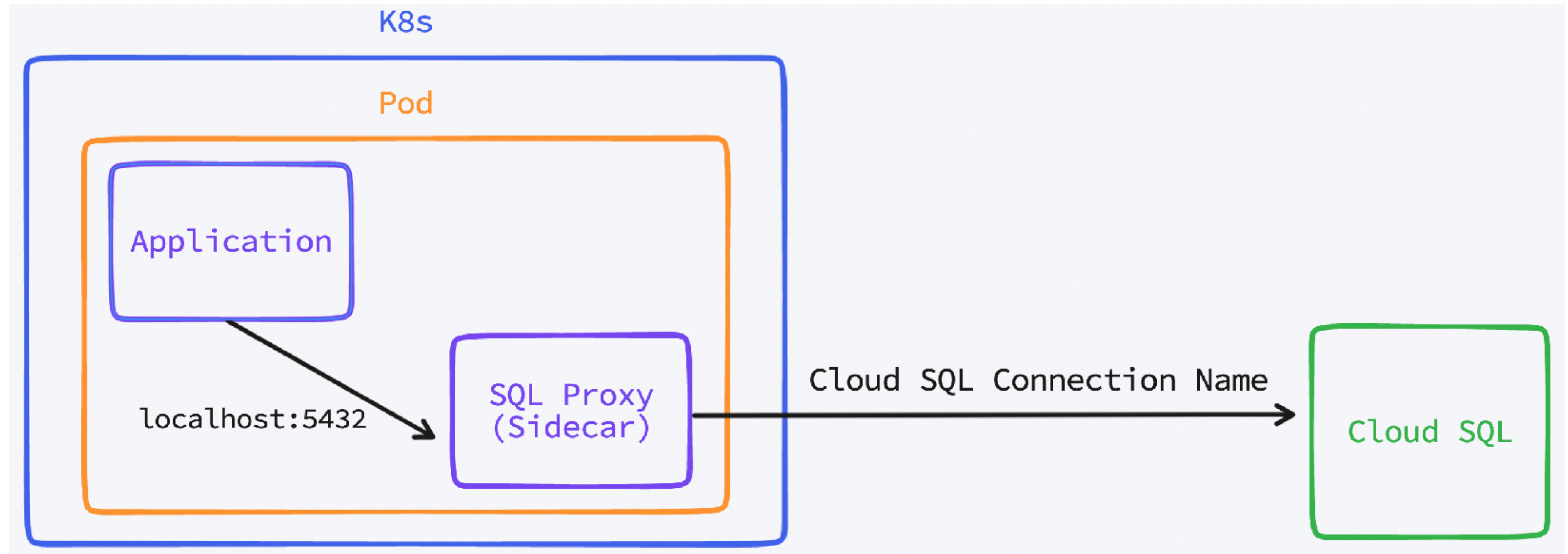
# Cloud SQL Auth Proxy (SQL Proxy)

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

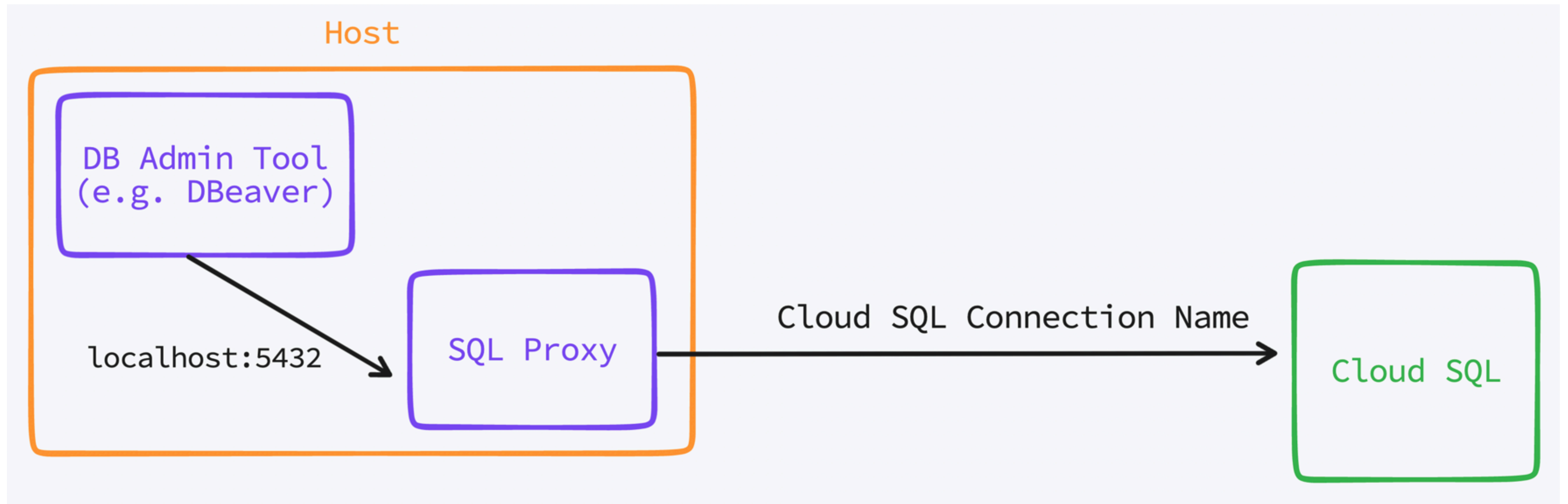
- 使用情境
  - K8s





# 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

The screenshot shows the Google Cloud IAM & Admin console. The left sidebar contains the navigation menu with 'IAM 與管理' at the top and '服務帳戶' (Service Accounts) highlighted. The main content area is for the 'sql-proxy' service account, with the '金鑰' (Keys) tab selected. A warning message is displayed, advising against downloading keys and recommending Workload Identity. Below the warning, there is a '新增金鑰' (Add Key) button. At the bottom, a table lists the existing keys.

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)

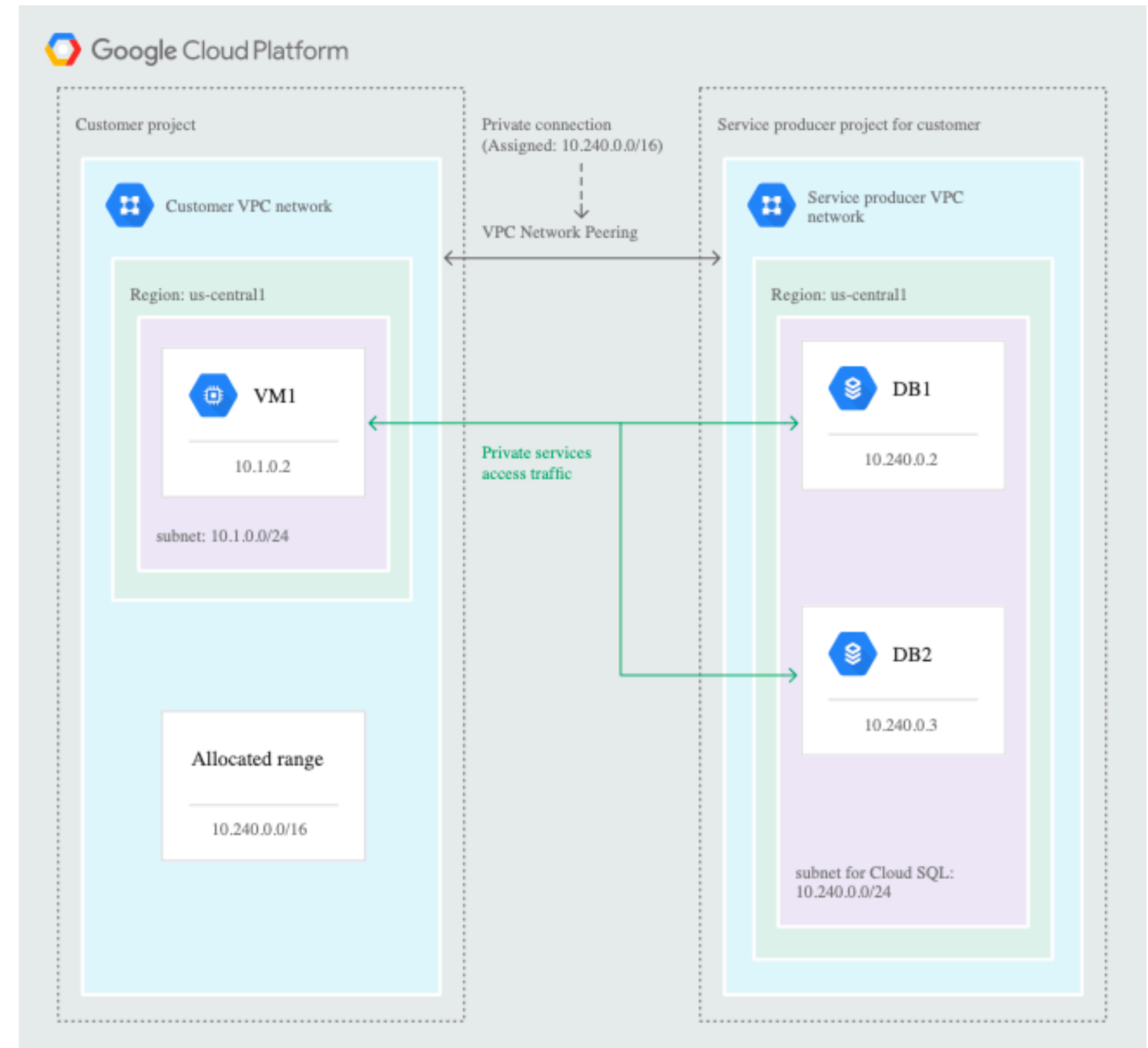
SQL Proxy Demo

# 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



同時配有 Public 與 Private IP 的 Cloud SQL Instance



服務連接範例 Ref: [GCP Doc](#)

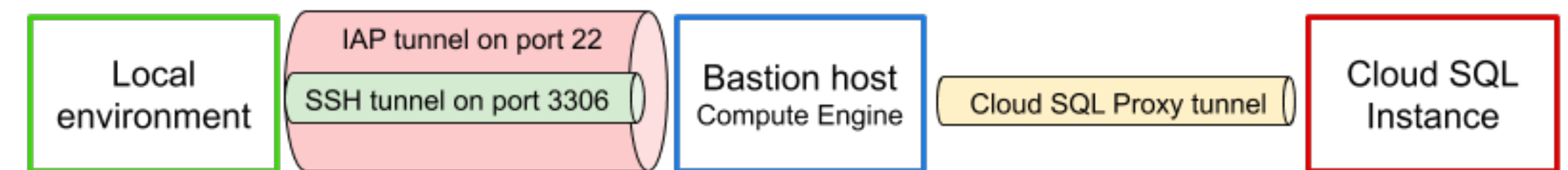


# Cloud SQL with private IP only

- 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



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

- 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**.