

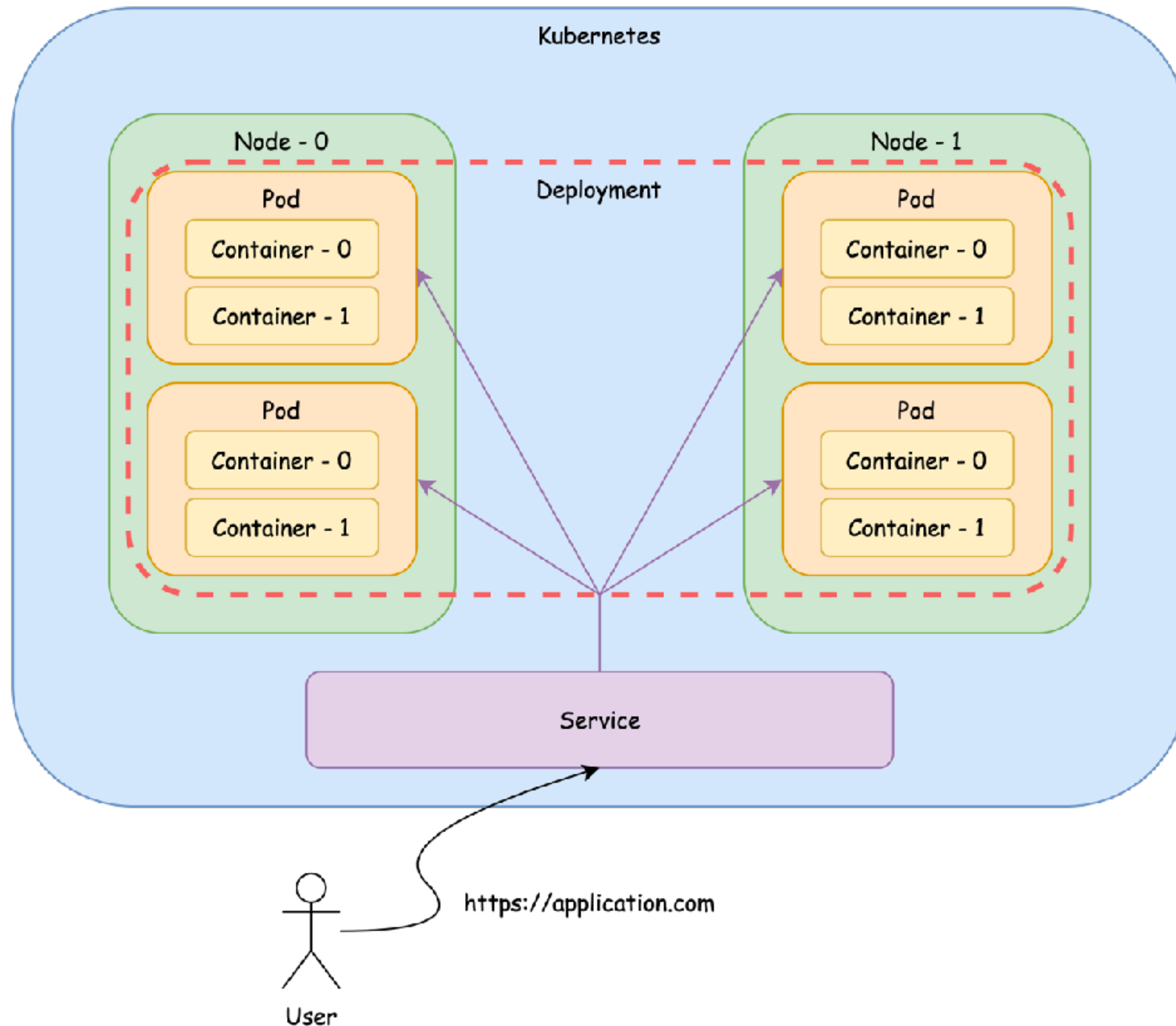
GKE Use Case 02

投資程式設計科 DevOps 組

Outline

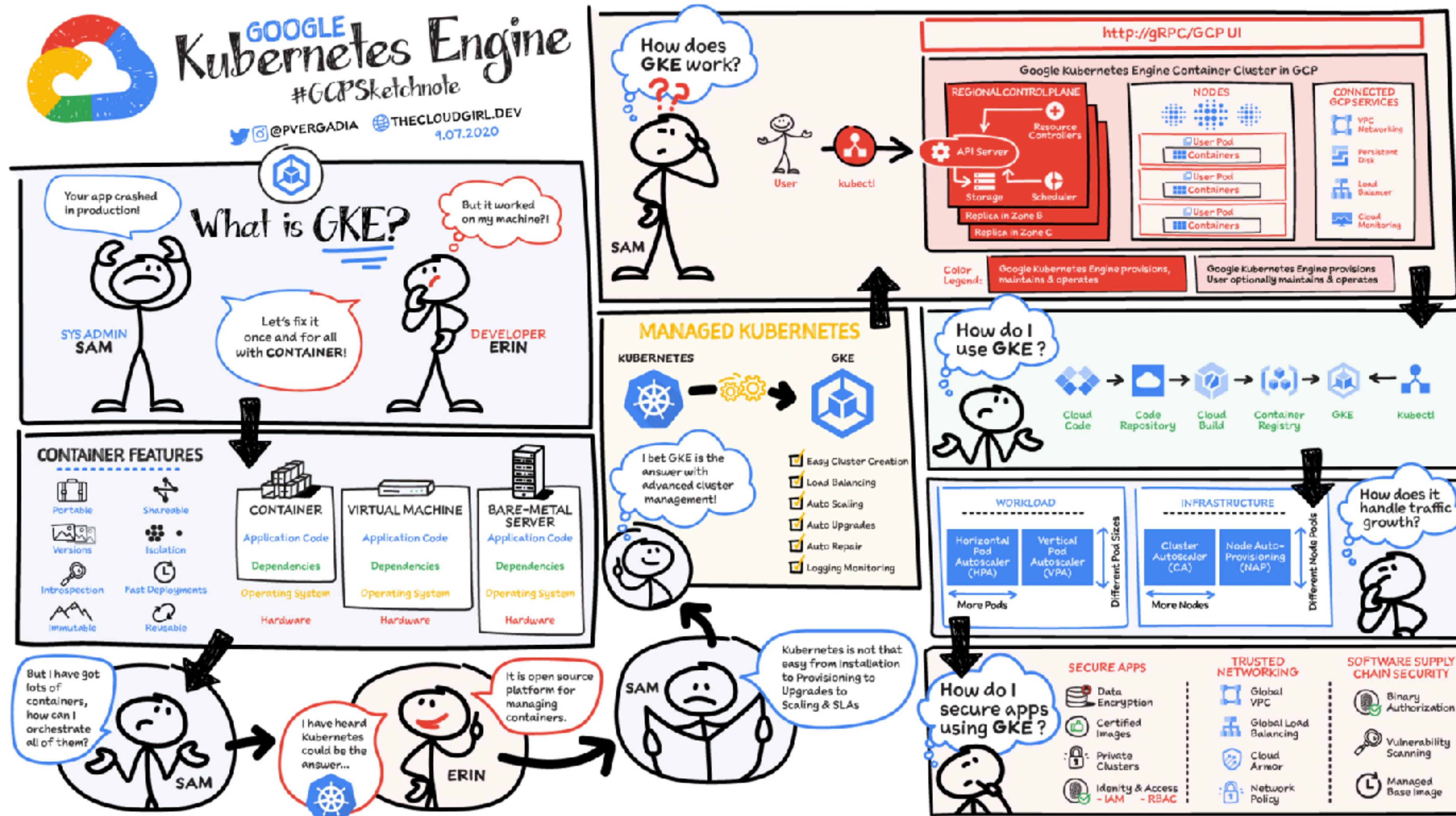
- Kubernetes Recap
- Google Kubernetes Engine (GKE)
- Lab: Set Up and Configure a Cloud Environment in Google Cloud
 - Task 1 and Task 2: VPC
 - Task 3: Bastion Host
 - Task 4: Cloud SQL
 - Task 5: Create Kubernetes Cluster
 - Task 6: Prepare Kubernetes Cluster
 - Task 7: Wordpress
 - Lab - Task 8 and Task 9: Monitoring and IAM
- Recap

Kubernetes Recap




- Kubernetes (K8s)：容器管理平台
- Container：執行程式的獨立環境
 - Image：Container 的模版
- Pod：一個 Pod 可以容納多個 Container
- Node：實際運行 Container 的機器
- Deployment：定義 Pod 的內容
- Service：接收 Request 並轉發至 Pod 上






Google Kubernetes Engine (GKE)



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

Lab

 Set Up and Configure a Cloud Environment in Google Cloud: Challenge Lab




Start Lab01:00:00

Set Up and Configure a Cloud Environment in Google Cloud: Challenge Lab

1 hour7 Credits★★★★☆

GSP321

 Google Cloud Self-Paced Labs

GSP321

—/100

Overview

Challenge scenario

Task 1. Create development VPC manually

Task 2. Create production VPC manually

Task 3. Create bastion host

Task 4. Create and configure Cloud SQL instance

Task 5. Create Kubernetes cluster

Task 6. Prepare the Kubernetes cluster

Task 7. Create a WordPress deployment

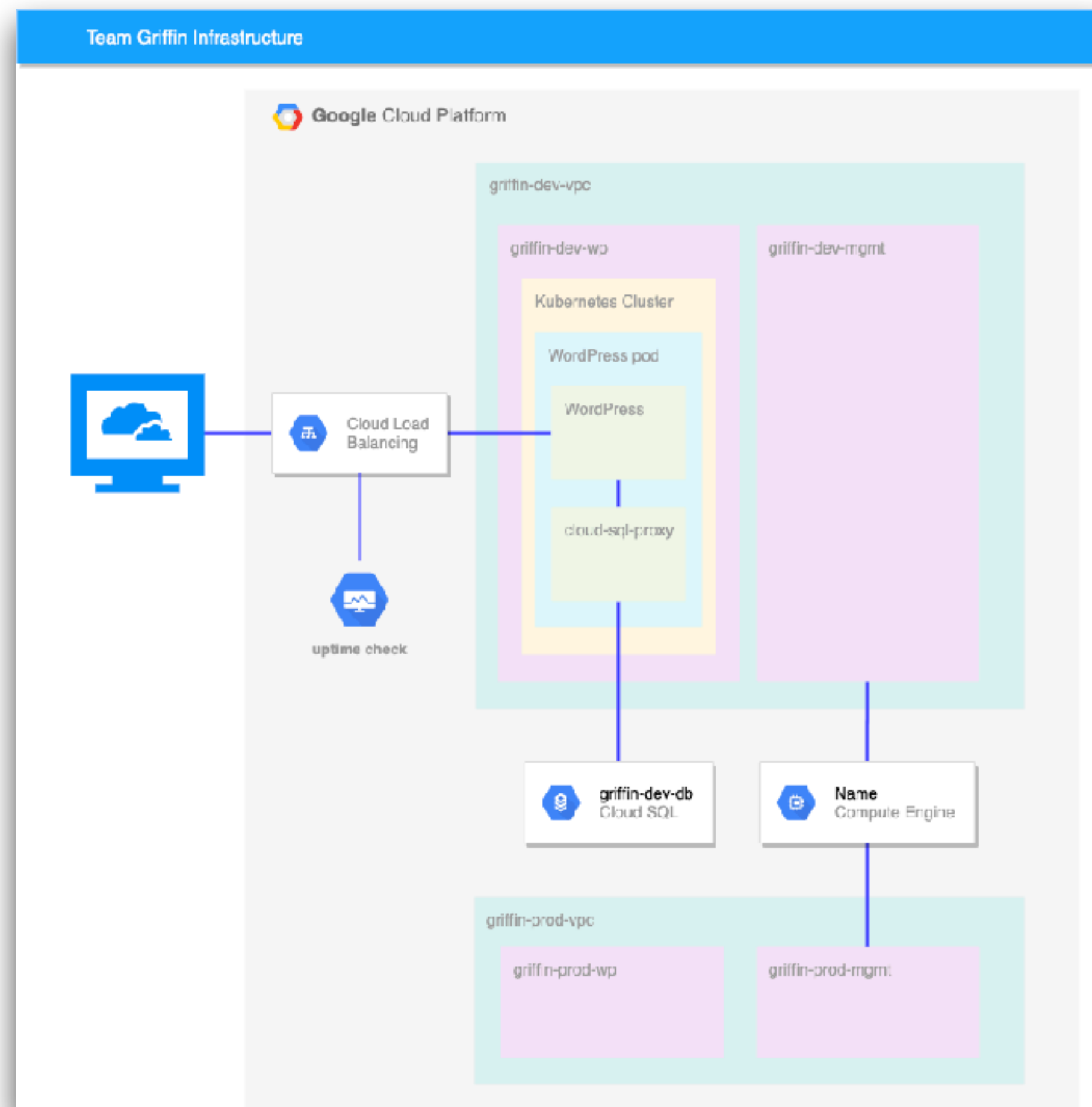
Task 8. Enable monitoring

Task 9. Provide access for an additional engineer

Congratulations!

<https://www.cloudskillsboost.google/focuses/10603?parent=catalog>

Lab - Requirements



- Create a **development VPC** with three subnets manually
- Create a **production VPC** with three subnets manually
- Create a **bastion** that is connected to both VPCs
- Create a development **Cloud SQL** Instance and connect and prepare the WordPress environment
- Create a **Kubernetes cluster** in the development VPC for WordPress
- Prepare the Kubernetes cluster for the WordPress environment
- Create a **WordPress deployment** using the supplied configuration
- Enable **monitoring** of the cluster via stackdriver
- Provide **access** for an additional engineer

Lab - Task 1 and Task 2: VPC

1. 依據 Lab 說明設定 VPC 與 Subnet
2. VPC network
 1. 橫跨所有 Region 的私人網路，在同一個 VPC 裡 VM 都可以透過 Private IP 溝通
 2. 一般 Project 會有一個 default 的 VPC
 3. 每個 Project 最多五個
3. SUBNET
 1. 在單一的 regions 裡，每個 region 裡可以有 multiple subnet
 2. IP 配置 e.g. 192.168.32.0/20
 3. CIDR: 無類別區隔路由，避免傳統切割方式造成 IP 位址的大量浪費
 4. IPv4 / IPv6 CIDR計算器: <https://zh-tw.rakko.tools/tools/27/>

Lab - Task 3: Bastion Host

1. 建立一台跳板機 (Bastion Host)
 1. 只有跳板機可以連入指定的網路，當跳板機關閉時網路等於封閉無法被入侵
 2. 同時連接 griffin-dev-mgmt 跟 griffin-prod-mgmt 兩個 VPC
 3. 建立 SSH 相關的防火牆規則，確保可以 SSH
 1. VM 增加 network tags 供 Firewall Rule 指定
 2. 建立 Firewall Rule 在 griffin-prod-mgmt network 允許 TCP 22

Lab - Task 4: Cloud SQL

1. 建立 MySQL Cloud SQL Instance
2. 連線進入 MySQL 執行 Lab 指定 SQL
 1. 可以在 Cloud Shell 透過 SDK (gcloud) 連結 DB
 2. `gcloud sql connect griffin-dev-db --user=root`
 3. <https://cloud.google.com/sql/docs/mysql/connect-instance-cloud-shell>

Lab - Task 5: Create Kubernetes Cluster

1. 建立 K8s Cluster

1. Name: griffin-dev
2. Subnet: griffin-dev-wp
3. Zone: us-east1-b
4. Nodes: 2
5. Node Machine: n1-standard-4

Lab - Task 6: Prepare Kubernetes Cluster

1. 在 Cluster 取得連線設定指令，設定與 Cluster 的連線
2. 準備 K8s 上的 Wordpress 部屬相關內容，下載 Cloud Storage gs://cloud-training/gsp321/wp-k8s 上的所有檔案
 1. `gsutil cp -r gs://cloud-training/gsp321/wp-k8s .`
3. 更新 wp-k8s 內 wp-env.yaml 的 username 跟 password，更新後 apply wp-env.yaml
 1. `kubectl apply -f wp-env.yaml`
4. 根據 Lab 指令建立一個 Service Account 且生成 json key，並匯入至 K8s Secret 中供後續連接 Cloud SQL 使用

Lab - Task 7: Wordpress

1. 更新 wp-k8s 內的 deployment.yaml
 1. YOUR_SQL_INSTANCE 更改為前面建立的 MySQL 的 Instance connection name
 2. kubectl apply -f wp-deployment.yaml
2. 部屬 Wordpress 的 Service
 1. kubectl apply -f wp-service.yaml

Lab - Task 8 and Task 9: Monitoring and IAM

1. Task 8: Monitoring

1. 在 Monitoring 建立一組 Uptime Check 監控 Wordpress

2. Task 9: IAM

1. 在 IAM 把第二個 User 更改為 Project 的 Editor

Recap

- GKE 是 GCP 提供的**全託管 K8s 服務**，無須自行建立與設定叢集等底層，可以專注於**功能使用與服務發布**
- Cloud Console 的 GKE 頁面可以**檢視與編輯**各種資源
 - Workloads : **Deployment**, Stateful Set, Job
 - Services & Ingress : **Service**, Ingress
 - Secrets & ConfigMaps : Config Map, **Secret**
 - Storage : **Volume**

Recap

- VPC：橫跨所有 Region 的私人網路，在同一個 VPC 裡 VM 都可以透過 Private IP 溝通
- Subnet：IP 配置，可手動、自動，使用 CIDR 切割
- Firewall Rule：通常用 Network Tag 套用規則
- Bastion Host：跳板機，只有跳板機可以連入指定網路，關掉後指定網路即為封閉環境
- Cloud SQL 連線
 - SQL Proxy：利用具有權限的 Service Account 的 Key 與 Connection Name 進行認證與連線
 - gcloud sql connect：如果帳號有權限在 Cloud Shell 也可以利用 Cloud SDK 直接進行連線