INTERNAL ENGINEERING BRIEF · 2026

在 GCP 上自架 Vaultwarden

自架密碼管理器:詳細步驟、架構決策與踩坑紀錄

Google Cloud Platform · Self-Hosted
asia-east1 · vault.example.com

STACK

Cloud Run · Cloud SQL (PG)

GCS · Secret Manager

External HTTPS LB · IAP

Workspace SSO (OIDC)

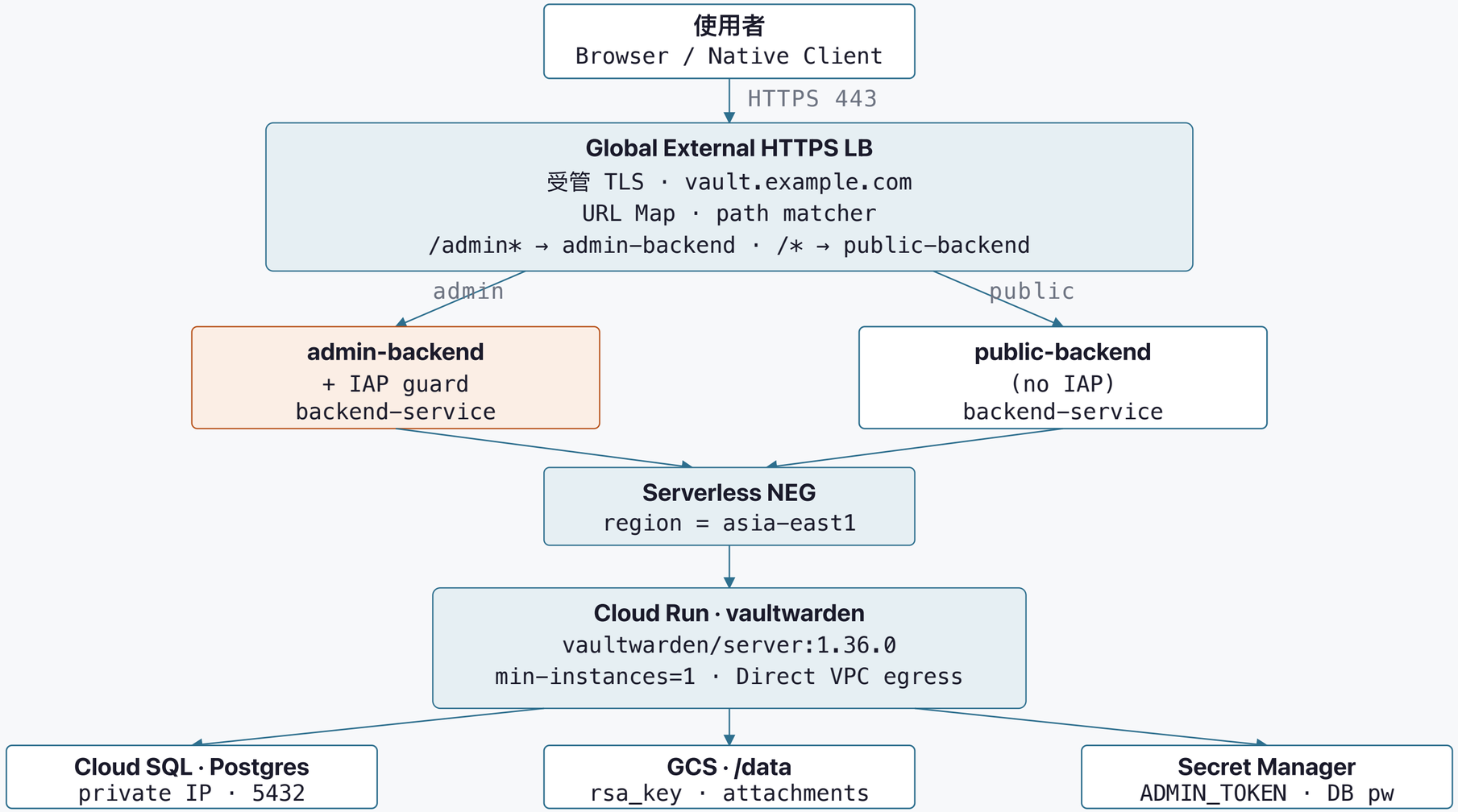
為什麼選 Vaultwarden?

- 部門共享機密(API keys、service account、憑證)需要統一管理
- **自管資料**:機密不落第三方 SaaS
- **省授權費**:Vaultwarden 相容 Bitwarden 用戶端,開源免費
- 多因素驗證 + 組織 / Collection 存取控管
- 目標:全員以 `alice@example.com` Google Workspace 帳號 SSO 登入

CLIENT COMPATIBILITY

瀏覽器 Web Vault	✓ 相容
手機 App (iOS/Android)	✓ 相容
瀏覽器擴充功能	✓ 相容
桌面 App	✓ 相容
CLI (bw)	✓ 相容

系統架構總覽


使用者
Browser / Native Client
HTTPS 443
Global External HTTPS LB
受管 TLS · vault.example.com
URL Map · path matcher
/admin* → admin-backend · /* → public-backend
admin
public
admin-backend
+ IAP guard
backend-service
public-backend
(no IAP)
backend-service
Serverless NEG
region = asia-east1
Cloud Run · vaultwarden
vaultwarden/server:1.36.0
min-instances=1 · Direct VPC egress
Cloud SQL · Postgres
private IP · 5432
GCS · /data
rsa_key · attachments
Secret Manager
ADMIN_TOKEN · DB pw

關鍵架構決策

- **專用 GCP project 隔離** — 獨立 project `your-gcp-project`,IAM 不污染母 org
- **Cloud Run(而非 GCE / GKE)** — 無伺服器、自動縮放、原生 HTTPS;`min-instances=1` 避免冷啟動登出
- **Cloud SQL Postgres(非 SQLite)** — 官方建議生產使用 Postgres;自動備份、PITR、HA 可選
- **External HTTPS LB + Serverless NEG** — 受管 TLS;path-level routing(`/admin` vs `/*`)
- **IAP 只守 `/admin`** — 原生用戶端無法過 IAP(詳見 Slide 14)
- **Direct VPC egress(`private-ranges-only`)** — Cloud Run 透過私有 IP 連 Cloud SQL;公網流量直出

前置作業:啟用 GCP API

```
# 在 your-gcp-project 啟用所有需要的 API
gcloud services enable \
  run.googleapis.com \
  sqladmin.googleapis.com \
  iap.googleapis.com \
  secretmanager.googleapis.com \
  compute.googleapis.com \
  dns.googleapis.com \
  artifactregistry.googleapis.com \
  storage.googleapis.com \
  servicenetworking.googleapis.com \
  vpcaccess.googleapis.com \
  --project=your-gcp-project
```

- `servicenetworking` + `vpcaccess` — Cloud SQL private IP & Direct VPC egress 所需
- `iap` — Identity-Aware Proxy
- `artifactregistry` — remote repo 代理 Docker Hub

Service Account 與 Secret Manager

- 建立專用最小權限 Service Account(後續 Slide 9 綁 IAM role)
- `ADMIN_TOKEN` 必須以 **argon2 雜湊**存入 Secret Manager(明文有警告)

雜湊指令(擇一)

```
# 方法 1:用 Vaultwarden 官方 Docker image
docker run --rm vaultwarden/server:1.36.0 \
  /vaultwarden hash --preset owasp

# 方法 2:argon2 CLI
echo -n "your-admin-password" | \
  argon2 "$(openssl rand -base64 32)" \
  -id -t 3 -m 16 -p 4 -l 32 -e
```

存入 Secret Manager

```
# 存 ADMIN_TOKEN(argon2 雜湊後字串)
echo -n '$argon2id$v=19$m=...' | \
  gcloud secrets create vaultwarden-admin-token \
  --data-file=- --project=your-gcp-project

# 存隨機 DB 密碼
openssl rand -base64 32 | \
  gcloud secrets create vaultwarden-db-password \
  --data-file=- --project=your-gcp-project
```

Cloud SQL(Postgres,私有 IP)

建立 instance · 資料庫 · 使用者

```
gcloud sql instances create vaultwarden-db \
  --database-version=POSTGRES_16 \
  --edition=ENTERPRISE \
  --tier=db-g1-small \
  --region=asia-east1 \
  --network=projects/your-gcp-project/global/networks/default \
  --no-assign-ip \
  --backup-start-time=18:00 \
  --enable-point-in-time-recovery \
  --project=your-gcp-project

gcloud sql databases create vaultwarden \
  --instance=vaultwarden-db --project=your-gcp-project

gcloud sql users create vaultwarden \
  --instance=vaultwarden-db \
  --password=$(gcloud secrets versions access latest \
    --secret=vaultwarden-db-password --project=your-gcp-project) \
  --project=your-gcp-project
```

⚠ GOTCHA

- Org policy 預設 edition 可能是 `ENTERPRISE_PLUS`;shared-core tier(`db-g1-small`)不相容 ENTERPRISE_PLUS,必須明確指定 `--edition=ENTERPRISE`
- `--no-assign-ip`:不分配公網 IP,只走 private IP

Cloud SQL · vaultwarden-db

Status	● **Runnable**
Edition	ENTERPRISE `required`
Tier	db-g1-small
Public IP	— disabled
Private IP	10.42.0.3

GCS Bucket:持久化 `/data` 目錄

建立 bucket

```
gcloud storage buckets create \
  gs://your-gcp-project-vaultwarden-data \
  --location=asia-east1 \
  --uniform-bucket-level-access \
  --public-access-prevention \
  --project=your-gcp-project
```

- Cloud Run instance 無狀態;`/data` 必須掛載外部 storage
- `--uniform-bucket-level-access`:停用 ACL,統一用 IAM 控管
- `--public-access-prevention`:防止意外公開
- `/data` 包含:資料庫(SQLite 備用)、附件、**`rsa_key`**(關鍵,見 Slide 11)

IAM 角色綁定

```
SA="vaultwarden-sa@your-gcp-project.iam.gserviceaccount.com"
PROJECT="your-gcp-project"
BUCKET="your-gcp-project-vaultwarden-data"

# Secret Manager:讀取 secret
gcloud projects add-iam-policy-binding $PROJECT \
  --member="serviceAccount:$SA" \
  --role="roles/secretmanager.secretAccessor"

# GCS:讀寫 /data bucket
gcloud storage buckets add-iam-policy-binding \
  gs://$BUCKET \
  --member="serviceAccount:$SA" \
  --role="roles/storage.objectAdmin"

# Cloud SQL:連線
gcloud projects add-iam-policy-binding $PROJECT \
  --member="serviceAccount:$SA" \
  --role="roles/cloudsql.client"
```

最小權限 · 三個 role

Role	範圍
secretmanager .secretAccessor	只讀 secret 值
storage .objectAdmin	限定於特定 bucket
cloudsql .client	連線,不含 DDL 管理

Artifact Registry:代理 Docker Hub

- Cloud Run 從 Artifact Registry 拉 image(不直接走 Docker Hub)
- 建立 remote repository 代理 Docker Hub,解決 rate limit 問題

建立 remote repo

```
gcloud artifacts repositories create dockerhub-remote \
  --repository-format=docker \
  --location=asia-east1 \
  --mode=remote-repository \
  --remote-docker-repo=DOCKER_HUB \
  --project=your-gcp-project
```

Image 路徑格式

```
asia-east1-docker.pkg.dev/
  your-gcp-project/
    dockerhub-remote/
      vaultwarden/server:1.36.0
```

部署 Cloud Run 服務

```
gcloud run deploy vaultwarden \
  --image=asia-east1-docker.pkg.dev/your-gcp-project/dockerhub-remote/vaultwarden/server:1.36.0 \
  --region=asia-east1 \
  --service-account=vaultwarden-sa@your-gcp-project.iam.gserviceaccount.com \
  --min-instances=1   --no-cpu-throttling \
  --network=default   --subnet=<serverless-subnet>   --vpc-egress=private-ranges-only \
  --add-volume=name=data,type=cloud-storage,bucket=your-gcp-project-vaultwarden-data \
  --add-volume-mount=volume=data,mount-path=/data \
  --set-secrets=DATABASE_URL=vaultwarden-db-url:latest,ADMIN_TOKEN=vaultwarden-admin-token:latest \
  --set-env-vars=ROCKET_PORT=8080,DATA_FOLDER=/data,DOMAIN=https://vault.example.com,SIGNUPS_ALLOWED=true \
  --allow-unauthenticated   --project=your-gcp-project
```

⚠ GOTCHA

- `DATABASE_URL` 格式: `postgresql://vaultwarden:<pw>@<private-ip>:5432/vaultwarden?sslmode=require` (私有 IP + TLS)
- **`rsa_key` 必須持久化於 GCS** — 冷啟動若重建 rsa_key,所有 session token 失效→全員被登出; `/data` 掛 GCS 後自動解決
- `--allow-unauthenticated` :Cloud Run 層保持公開,存取控管交給 LB + IAP(見 Slide 16)

[截圖:Cloud Run service overview — 示意參數標註於 Slide 16 mockup]

External HTTPS Load Balancer 設定

```
# 1. 保留全域靜態 IP
gcloud compute addresses create vaultwarden-ip \
  --global --project=your-gcp-project

# 2. Serverless NEG
gcloud compute network-endpoint-groups create vaultwarden
  --region=asia-east1 \
  --network-endpoint-type=serverless \
  --cloud-run-service=vaultwarden --project=your-gcp-proj

# 3. 兩個 backend service(public + admin)
gcloud compute backend-services create vaultwarden-public
  --global --load-balancing-scheme=EXTERNAL_MANAGED \
  --project=your-gcp-project
gcloud compute backend-services create vaultwarden-admin-
  --global --load-balancing-scheme=EXTERNAL_MANAGED \
  --project=your-gcp-project

# 4. 各自加入 NEG
```

```
# 5. URL map:/admin* → admin,/* → public
gcloud compute url-maps create vaultwarden-urlmap \
  --default-service=vaultwarden-public-backend \
  --project=your-gcp-project
# path matcher 透過 import YAML 或 gcloud 子命令設定

# 6. 受管 SSL 憑證
gcloud compute ssl-certificates create vaultwarden-cert \
  --domains=vault.example.com --global \
  --project=your-gcp-project

# 7. Target HTTPS proxy + Forwarding rule
gcloud compute target-https-proxies create vaultwarden-ht
  --url-map=vaultwarden-urlmap \
  --ssl-certificates=vaultwarden-cert --project=your-gcp-

gcloud compute forwarding-rules create vaultwarden-https-
  --global --target-https-proxy=vaultwarden-https-proxy \
  --address=vaultwarden-ip --ports=443 \
```

DNS · A 記錄 vault.example.com → LB 靜態 IP

受管 SSL 憑證 provision 需 DNS 生效（10–30 分鐘）

Identity-Aware Proxy:保護 `/admin` 路徑

```
# 啟用 IAP on admin-backend
gcloud iap web enable \
  --resource-type=backend-services \
  --service=vaultwarden-admin-backend \
  --project=your-gcp-project

# Provision IAP service agent(關鍵!)
gcloud beta services identity create \
  --service=iap.googleapis.com \
  --project=your-gcp-project

# 授 IAP service agent run.invoker
SUFFIX="@gcp-sa-iap.iam.gserviceaccount.com"
IAP_SA="service-<PROJECT_NUMBER>$SUFFIX"
gcloud run services add-iam-policy-binding vaultwarden \
  --region=asia-east1 \
  --member="serviceAccount:$IAP_SA" \
  --role="roles/run.invoker" --project=your-gcp-project

# 授權管理者存取 /admin
gcloud iap web add-iam-policy-binding \
  --resource-type=backend-services \
  --service=vaultwarden-admin-backend \
  --member="user:admin@example.com" \
```

⚠ GOTCHA · 重要

- 必須先 provision IAP service agent,否則登入 Google 後出現 **"The IAP service account is not provisioned"** 錯誤
- IAP service agent 需要 `roles/run.invoker`,才能代理請求至 Cloud Run

Security · IAP

Resource	vaultwarden-admin-backend
IAP	● **ON** enabled
Service agent	✓ **provisioned**
Principal	user:admin@example.com
public-backend	IAP OFF

[截圖:IAP admin-backend toggle — 示意 mockup]

為什麼 IAP 只能套 `/admin`,不能套全站?

Bitwarden 原生用戶端(手機 App、桌面 App、瀏覽器擴充功能、CLI `bw`) **無法攜帶 Google OAuth 憑證**通過 IAP。

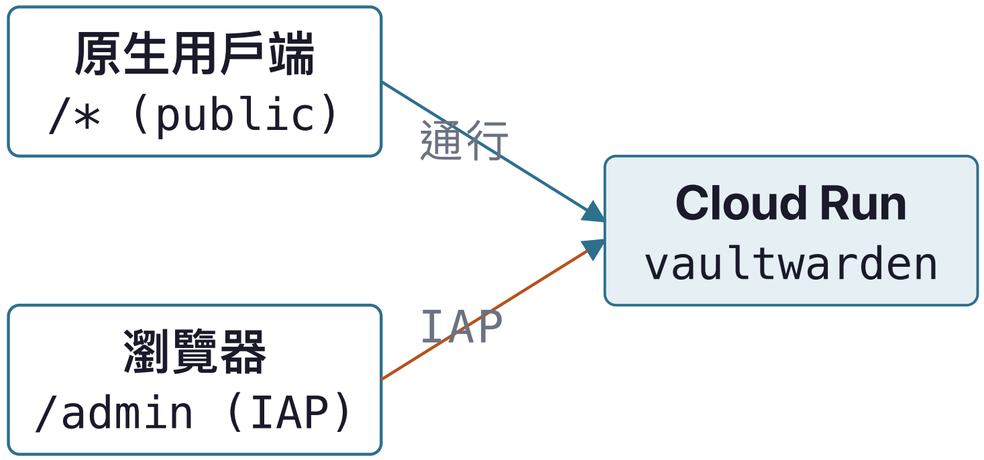
失敗流程 · 原生用戶端

- 原生用戶端 → HTTPS LB → IAP
- IAP 回 302 重導到 Google 登入頁
- 用戶端收到 302 / HTML(非 JSON)
- 解析失敗 → 同步錯誤

用戶端類型	能過 IAP?
瀏覽器 Web Vault	可以
手機 App	不行
桌面 App	不行
瀏覽器擴充功能	不行
CLI (bw)	不行

結論 · 分層存取控管

- IAP 只套 **/admin** backend
- /* 保持公開,Cloud Run `allow-unauthenticated`
- 存取控管交給應用層:SSO + 邀請制
- 封鎖 *.run.app 直連(見 Slide 16)



Google Workspace SSO 整合

前置:建立 OAuth 2.0 Client

- 類型:Web application
- Redirect URI: `https://vault.example.com/identity/connect/oidc-signin`

Cloud Run 環境變數

```
gcloud run services update vaultwarden \
  --region=asia-east1 \
  --set-env-vars=\
SSO_ENABLED=true,\
SSO_AUTHORITY=https://accounts.google.com,\
SSO_CLIENT_ID=<your-oauth-client-id>,\
SSO_AUTHORIZE_EXTRA_PARAMS="access_type=offline&prompt=consent&hd=example.com",\
SSO_ONLY=false,\
SIGNUPS_DOMAINS_WHITELIST=example.com \
  --project=your-gcp-project
```

⚠ GOTCHA

- `SSO_ONLY=false`:保留密碼登入當 **break-glass**(admin 帳號、bot 帳號 `bot@example.com`、CLI 自動化)
- OAuth 同意畫面 **Internal** 最乾淨,但會影響整個 project 其他 OAuth client;若維持 **External**,用 `SIGNUPS_DOMAINS_WHITELIST=example.com` 在應用層鎖網域(官方文件明確記載此白名單套用於 SSO 註冊)
- `hd=example.com`:要求 Google 帳號屬於指定 Workspace 網域
- 即使 SSO 登入,使用者仍需輸入**個人主密碼**解密(E2E 加密,Vaultwarden 無 Key Connector)

收尾強化設定

關閉公開註冊(改邀請制)

```
gcloud run services update vaultwarden \
  --region=asia-east1 \
  --set-env-vars=SIGNUPS_ALLOWED=false \
  --project=your-gcp-project
```

鎖定 ingress(封 run.app 直連)

```
gcloud run services update vaultwarden \
  --region=asia-east1 \
  --ingress=internal-and-cloud-load-balancing \
  --project=your-gcp-project
```

啟用 org Groups(beta)

```
--set-env-vars=ORG_GROUPS_ENABLED=true
```

⚠ 重要注意事項

- `--ingress=internal-and-cloud-load-balancing` 封鎖 `*.run.app` 直連,流量必須經 LB
- **仍需保留 `--allow-unauthenticated`**:ingress 鎖的是來源,不是認證層;若移除 unauthenticated,Cloud Run 層會要求 Google OIDC token,公開路徑的 Bitwarden 用戶端無法提供→連線失敗

Cloud Run · vaultwarden

Min instances	**1** warm
CPU throttling	**disabled**
VPC egress	private-ranges-only
Volume	/data → GCS bucket
Ingress	internal-and-cloud-LB
Auth	allow-unauthenticated by design

眉角速查表

#	問題	解法
a	Org policy 強制 ENTERPRISE_PLUS,db-g1-small 被拒	明確指定 --edition=ENTERPRISE
b	/admin 登入後出現 "IAP service account is not provisioned"	gcloud beta services identity create --service=iap.googleapis.com + 授 run.invoker
c	IAP 套全站後原生用戶端無法同步	IAP 只套 /admin backend,/* 保持公開
d	重啟 Cloud Run 後全員被登出	rsa_key 必須持久化於 GCS /data(掛 volume 後自動解決)
e	Direct VPC egress 設 private-ranges-only 後外部 OIDC/SMTP 不通	private-ranges-only 只導私網流量走 VPC;公網(Google OIDC discovery、SMTP relay)直出,無需額外設定
f	SMTP 寄信失敗	GCP 永久封鎖 port 25;使用 587(STARTTLS)或 465(TLS)
g	換 SMTP relay 後仍收不到信	Vaultwarden 只支援 SMTP 寄信(不支援 sendmail / API)
h	移除 --allow-unauthenticated 後公開路徑壞掉	保留 allow-unauthenticated;靠 --ingress 控制來源,不靠 Cloud Run 認證層

上線驗證清單

- [ ] GET https://vault.example.com/alive → HTTP 200
- [ ] 瀏覽器開啟 Web Vault → Google SSO 登入成功
- [ ] 手機 App / 瀏覽器擴充功能 → 連線 vault.example.com → 同步成功
- [ ] 瀏覽器開啟 /admin → 302 到 Google 登入 → IAP 驗證通過
- [ ] 直接連 *.run.app → 403 / 無法存取(ingress 封鎖)
- [ ] 重啟 Cloud Run(0 → 1 instance)→ 不需重新登入(rsa_key 持久化)
- [ ] 上傳附件 → 確認落在 GCS bucket
- [ ] Cloud SQL → 自動備份排程已啟用
- [ ] Cloud Monitoring → 無異常 error log

[截圖:Cloud Run service healthy + Cloud SQL 備份已啟用 — 示意以勾選列表代替 console]

月費概估(asia-east1)

元件	規格	概估費用
Cloud SQL	db-g1-small · Postgres 16	~ USD 25–30
Cloud Run	min-instances=1 · 0.5 vCPU	~ USD 5–10
External HTTPS LB	forwarding rule + data	~ USD 10–15
GCS	/data bucket(小量)	< USD 1
Secret Manager	< 10 secrets	< USD 1
合計	**每月**	**~ USD 50–70**

≈ $60 / 月

- 主要成本:Cloud SQL + LB
- 降低成本:若流量低,評估是否需要 `min-instances=1` (移除後有冷啟動風險)
- Cloud SQL tier 可評估 `db-f1-micro` (非生產),但 shared-core 有效能限制

結語

- 完整流程約 **半天**可完成(含踩坑時間)
- 開源自管方案,機密不外流,授權費為零
- 本簡報所有識別資訊為 placeholder,實作時請替換為真實值
- 問題或踩坑歡迎找 `it-support@example.com`

參考資料

Vaultwarden 官方 Wiki
github.com/dani-garcia/vaultwarden/wiki

Vaultwarden SSO(OIDC)設定
github.com/dani-garcia/vaultwarden/wiki/SSO-with-OIDC

GCP IAP for Cloud Run
cloud.google.com/iap/docs/enabling-cloud-run

GCP Serverless NEG
cloud.google.com/load-balancing/docs/negs/serverless-neg-concepts

Cloud Run Direct VPC Egress
cloud.google.com/run/docs/configuring/vpc-direct-vpc

Cloud Run GCS Volume Mount
cloud.google.com/run/docs/configuring/services/cloud-storage-volume-mounts