巧禾展示與測試伺服器操作準則

版本: V1.2

2025/06/24

版本紀錄

版本	編輯日期	描述	作者
V1.0	2025/06/20	初版。	林晉頡
V1.1	2025/06/23	新增 Docker Volume 使用建議。	林晉頡
V1.2	2025/06/24	新增 MariaDB 與 Nginx Proxy 的子網路使用準則。	林晉頡

零、前言

為確保展示與測試的專案執行環境不會相互影響或衝突。請詳閱下述各項準則並確實遵守，如有疑義或未盡說明之處請隨時提出討論。名詞解釋請見附件一。

一、主機環境說明

- OS：Ubuntu 24.04.2
- CPU 核心數：4
- RAM：8GB
- 儲存空間：150 GB
- 時區：Asia/Taipei (UTC+8)

二、帳號權限準則

- 帳號不得多人共用。
- 需要 root 權限時，請用 sudo 指令進行提權。

三、伺服器登入方式準則

- 為維護伺服器資安，僅可透過 SSH 金鑰登入，SSH 監聽 port 為 25565。
- 限制 root 帳號不可以透過 SSH 遠端登入。

四、防火牆準則

- 不可關閉 UFW 防火牆。
- 資料庫類型的服務使用的 port 必須限制為僅可透過公司固定 IP「106.104.165.127」訪問。
- Docker 容器如需對外連線，必須使用「ufw-docker」指令設定允許容器通過防火牆。

五、命名準則

- 「展示專案」以「demo-」開頭命名「專案目錄」與「專案」。
- 「測試專案」以「test-」開頭命名「專案目錄」與「專案」。

六、專案執行環境準則

- 不可於本伺服器執行正式上線的 production 環境。
- 必須使用 Docker 打包執行環境，本伺服器僅可使用 Docker 執行專案程式。包括但不限於 Apache、Nginx、MariaDB、phpMyAdmin 等環境。
- 必須透過 Nginx 進行連線的反向代理。

七、Docker 執行方式準則

- 必須在/opt 目錄中設定各「專案」專用的目錄，非必要不得共用目錄。
- 目錄名稱應遵守命名準則，並使用小寫英文單詞命名，單詞之間以減號分隔。
- 必須使用 docker-compose.yml 組成「專案」的形式啟動。
- 如需將 Docker Container 內的檔案掛載出來到宿主機中，僅可映射到該服務所屬專案的目錄中。

八、docker-compose.yml 設定準則

- 不需要於 docker-compose.yml 檔案中設定 version 標籤。
- 各容器如需於宿主機重啟後自動啟動，應將 restart 設定為 always。
- 同一專案中的容器，如需互相呼叫必須使用「服務名稱」來代替 IP。
- 各 docker container 必須使用 container_name 設定「容器名稱」。
- 「服務名稱」與「容器名稱」皆應遵守命名準則，並使用小寫英文單詞命名，單詞之間以減號分隔。
- 優先使用 Docker Volume 作為檔案的長期儲存體。
- 除 Apache 與 Nginx 服務外，其餘服務不可佔用素主機 1024 以下(含)的 port。

九、資料庫使用準則

- 除非專案有特殊的資料庫類型或版本需求，否則皆應使用共用的 MariaDB 或 Redis。
- 資料庫帳號不得共用，每個專案應該有專屬的資料庫連線帳號密碼。
- 每個專案的專屬帳號，只能看到該專案使用的資料庫。
- 要使用共用的 MariaDB 需將 Docker 容器掛入「mariadb_network」Docker 子網段。

十、GitLab 自動部署

- 僅可透過專用帳號「gitlab」登入與操作。
- 已透過「gitlab」帳號啟動的 Docker 容器，如需重啟、人工調整設定，必須使用指令 su 切換至 gitlab 帳號操作。

十一、 Nginx 反向代理準則

- 請使用 Nginx Proxy Manager 進行反向代理設定。
- Nginx Proxy Manager 僅可從公司固定 IP 連線，連線位置：http://172.105.194.150:81/
- Nginx Proxy Manager 賬號不得共用。
- 要使用反向代理需將 Docker 容器掛入「nginx_proxy_network」Docker 子網段。

十二、 SSL/TLS 憑證

- 若為公司的 kahap.com 網域，一律統一使用公司購買之 SSL/TLS 憑證。
  公司的憑證檔案一律放置於/etc/ssl 目錄中。
  憑證檔完整路徑：/etc/ssl/certs/kahap.com.cert
  憑證金鑰檔完整路徑：/etc/ssl/private/kahap.com.key
- 若為客戶提供的網域，可以使用客戶提供的憑證或使用免費的 Let's Encrypt 憑證。
  客戶提供的憑證一律放置於所屬專案資料夾的 ssl 目錄中，並以客戶網域命名，檔名中不加年月日。

A. 展示專案

系指已結案的專案，用於作爲公司作品集展示給潛在客戶看。

B. 測試專案

系指開發中的專案，用於提供當前合作的客戶測試使用。

C. 宿主機

系指 Ubuntu 主機本身。

D. 專案

系指由一個 docker-compose.yml 檔案所定義的一組資源與設定。

E. 服務名稱

系指 docker-compose.yml 檔案中，services 層級下一層的字串標籤。

如下所示的第 2 行與第 5 行，即為「服務名稱」。

```
1. services:
2.   app:
3.     image: xxx
4.     container_name: test-app
5.   db:
6.     image: mysql
7.     container_name: test-db
```

F. 容器名稱

系指 docker-compose.yml 檔案中的 container_name 所設定的名稱。

G. GitLab 自動部署

系指透過 GitLab 流水線自動執行的程式部署。