【AWS】Day 3：AWS 中的帳號與資源管理架構

上一篇我們介紹了 AWS 的基本概念，包括什麼是 Region、Availability Zone，以及怎麼操作 AWS 的幾種方式。

那這篇文章，我們要來聊聊一個很多人初學 AWS 時會感到困惑的問題：**AWS 裡面的資源，到底是怎麼被組織與管理的？**

為什麼要有架構？

當你只是個人開一個帳號、開幾台機器、弄幾個服務，帳號的資源大致上不會太複雜，console 點一點都還可以處理。

但當你是企業使用者、跨部門團隊、有多個環境（dev / uat / prod）、多個專案、甚至上百個服務時，就會遇到一堆問題：

- 權限怎麼分？
- 帳單怎麼分？
- 誰能看？誰能用？
- 怎麼防止誤刪 / 誤操作？

這時候就會用到 AWS 提供的資源管理架構囉～

AWS 的三層資源管理架構

在 GCP 中，我們常會提到 **Project** 的概念。但在 AWS 裡面，這樣的概念其實是被拆成以下幾層來實現的：

1. Account（AWS 帳號）

AWS 帳號是最基本的管理單位。每個帳號就是一個獨立的資源空間，擁有自己的：

- IAM 設定（權限、角色）
- 資源與服務（EC2、S3、RDS 等等）
- 帳單與計費紀錄

可以想像成一個帳號就是一間房間，裡面什麼資源你都自己負責。

 很多企業會用多帳號來隔離環境，例如：

- 一個帳號放開發環境（dev）
- 一個帳號放測試環境（uat）
- 一個帳號放生產環境（prod）

這樣的好處是資源更隔離、權限更清楚、帳單也更容易拆分。

---

2. AWS Organizations（組織）

AWS Organizations 是一個多帳號的管理工具，讓你可以統一控管多個 AWS 帳號，並集中管理費用與權限。

使用 Organizations 後，可以做到：

- 建立帳號之間的層級架構（像是 OU = 組織單位）
- 統一帳單（Consolidated Billing）
- 實作 SCP（Service Control Policies）來限制某些帳號能用的服務

 這就像是你開了一間公司，然後底下開了一堆子公司，每個子公司有自己的帳號，但你這個總部可以看所有分公司的帳單，也能下政策規定大家不能亂搞。

---

3. Resource Tag（資源標籤）

這個就是 AWS 用來補足「Project」概念的做法。

因為 AWS 沒有像 GCP 的 Project 架構，所以會建議大家在建立資源時，**養成加上標籤（Tag）的習慣**！

常見的標籤包含：

- `Project`: live-api、momo-shop、data-pipeline
- `Env`: dev、uat、prod
- `Owner`: treeman、team-data、ops-team
- `CostCenter`: 90123、IT-Backend、Marketing

透過 Tag：

- 可以更清楚知道這台機器是做什麼的
- 可以用在 **成本分析**（Cost Explorer）
- 可以配合 IAM 權限做限制（例如只能操作特定 Project 的資源）
- 還能透過工具（如 Config、Budgets）追蹤管理

小結

這篇文章我們介紹了 AWS 的資源管理架構，總結如下：

概念名稱	對應用途
Account	資源與權限的邊界、計費單位
Organizations	多帳號統一管理架構
Tag	資源標記，模擬 Project 分類

其實 AWS 的架構雖然比 GCP 稍微複雜一點，但也因為彈性大，更能符合企業或大型專案的需求。

那麼下一篇文章，我們就正式進入 **AWS 的運算服務介紹** 啦！包括 EC2、Lambda、ECS、EKS、App Runner……每一種服務適合什麼情境、優缺點是什麼，我們下一篇文章再慢慢拆解！

我們 Day 4 再見啦

修訂版本 #1
★由 treeman 建立於 25 || 2025 18:23:49
由 treeman 更新於 25 || 2025 18:27:44