AWS Certified Solutions Architect

課程0 前置作業

Jacky

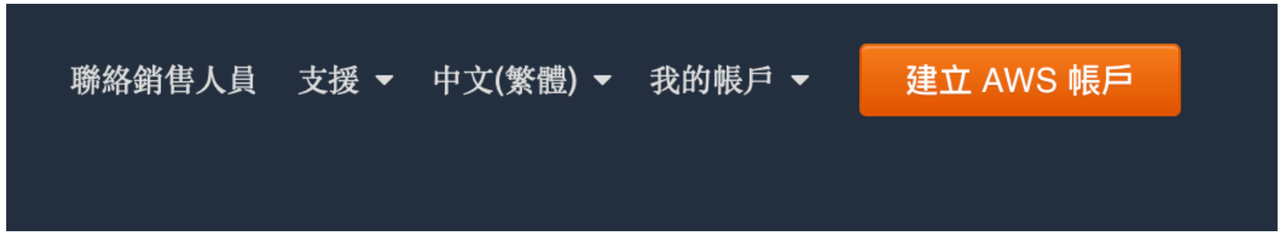
大綱

- 建立 AWS Root Account
- 設定MFA
- 設定 Billing Alarm
- 一年免費方案

AWS Root Account

開始註冊

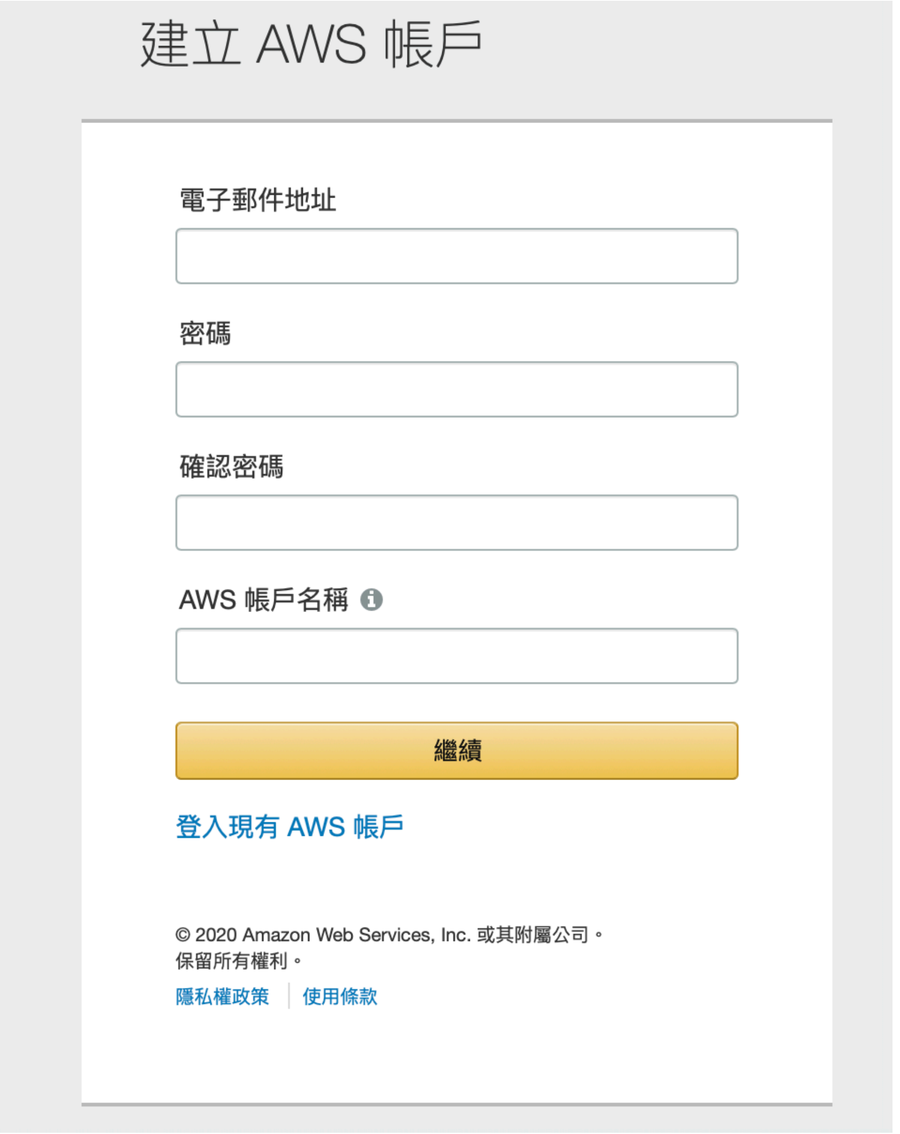
- http://aws.amazon.com/



AWS Root Account

帳號(Email)及密碼

- Email為 Root Account
- 請用最常用信箱
- 最好是每天會收信的信箱
- 密碼，請設長一點及不要用懶人密碼
- AWS 帳戶名稱:顯示用



AWS Root Account

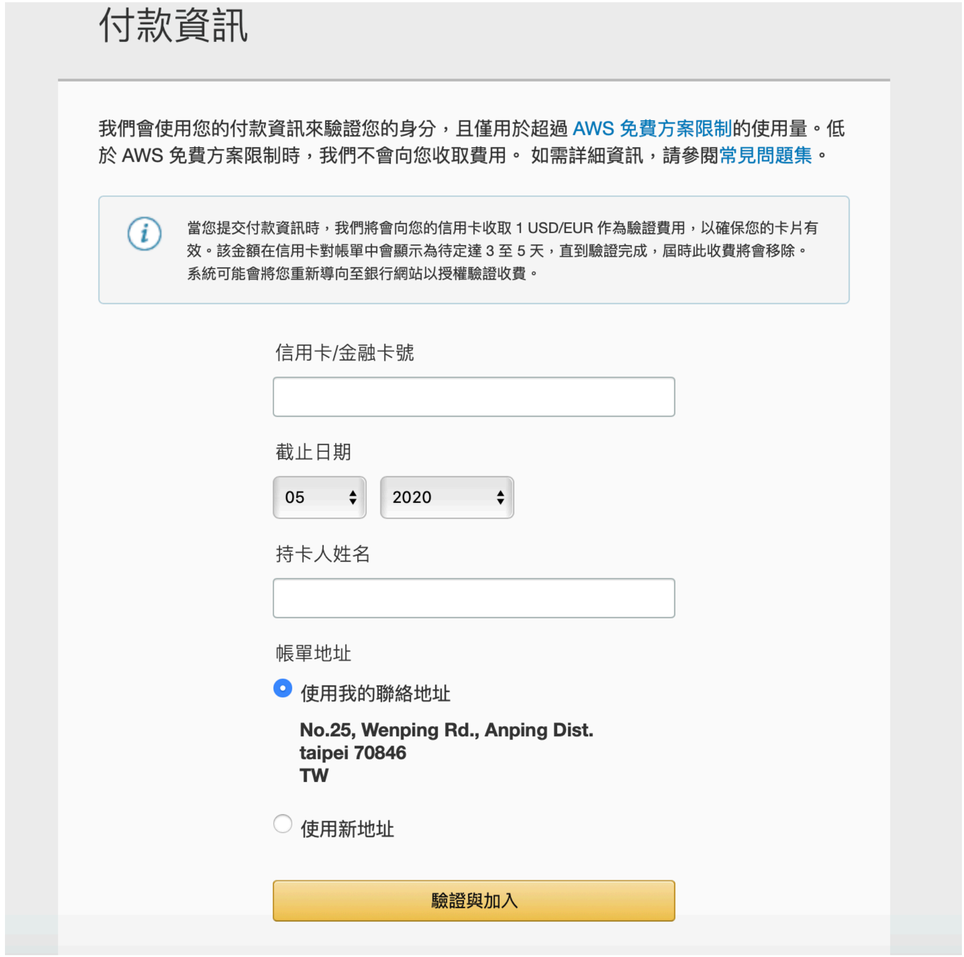
聯絡資訊設定

- 輸入正確的個人資料
- 確保 AWS 忘記密碼時能找回帳號
- 帳戶類型選「個人」

AWS Root Account

付款方式驗證

- 請輸入有效的信用卡號
- 會刷 1~2美元確認，但不會請款



AWS Root Account

電話設定

- 電話以行動電話為佳

AWS Root Account

電話驗證

- 在手機輸入畫面顯示的驗證碼

AWS Root Account

支援計劃

- 選擇「Free」(免費)
- Support Ticket 回應比較慢

AWS Root Account

設定完成

- 個人化體驗可以不用選，待帳號建立後，會收到一封確認函

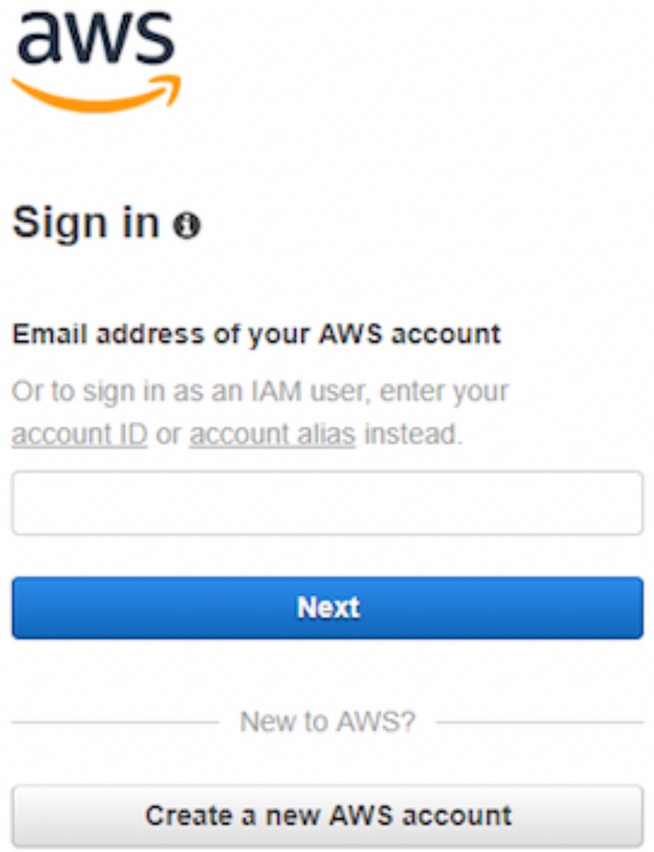
AWS Root Account

登入

- 請登入申請時Email
- 申請時的Email為Root Account

重要提醒!重要提醒!重要提醒!

- 請不要用 Root Account 開機器，及設定Access Key
- 原則上:Root Account 只用來管理帳單，及開第一個Admin帳號



設定MFA

選擇 Security Credentials

- 登入後，選「My Security Credentials」

「我的安全登入資料」

設定MFA

MFA設置

- 按「Active MFA」

設定MFA

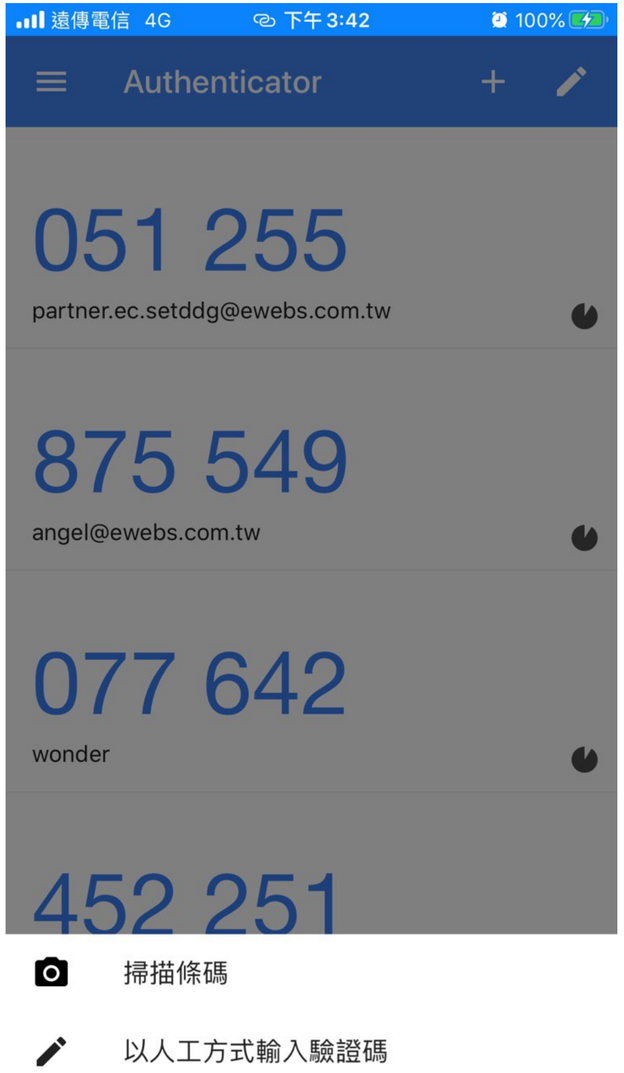
Virtual MFA (Apps)

- 選擇「A Virtual MFA device」

設定MFA

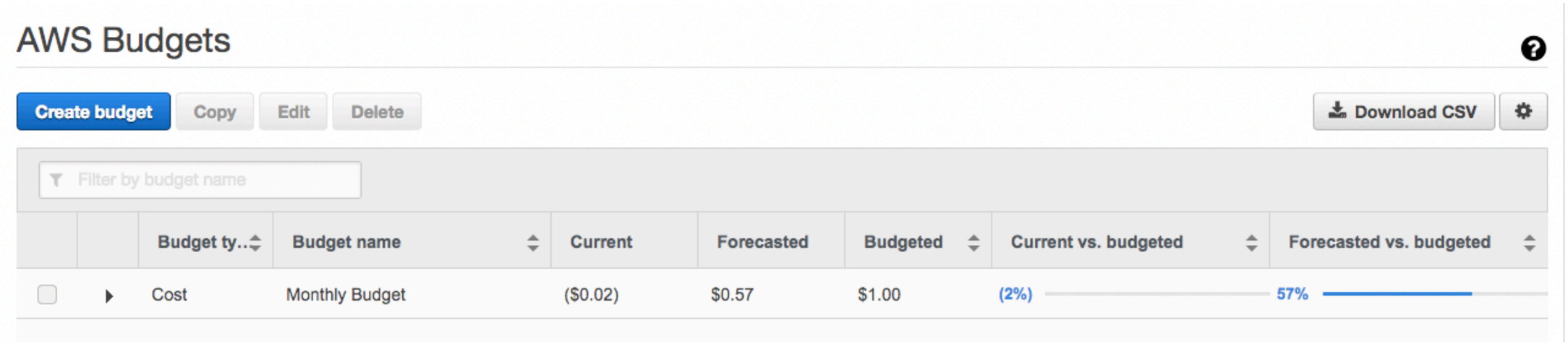
可以利用手機裝 Google Authenticator

掃描條碼去新增



設定 Billing Alarm

- 請依官方教學設定
  https://aws.amazon.com/tw/aws-cost-management/aws-budgets/
- 已設定 credit的部份，在超過 credit 時才會觸發 alarm



一年免費方案

Free Tier

https://aws.amazon.com/tw/free/

- EC2 - T2.micro，每個月 750 小時
- S3-5GB,2,000Put/20,000Get
- RDS - db.t2.micro，每個月750小時
- Lambda - 1百萬次請求

AWS Certified Solutions Architect

課程1 IAM

Jacky

IAM（Identity Access Management）

參考來源：
https://docs.aws.amazon.com/zh_tw/IAM/latest/UserGuide/introduction.html

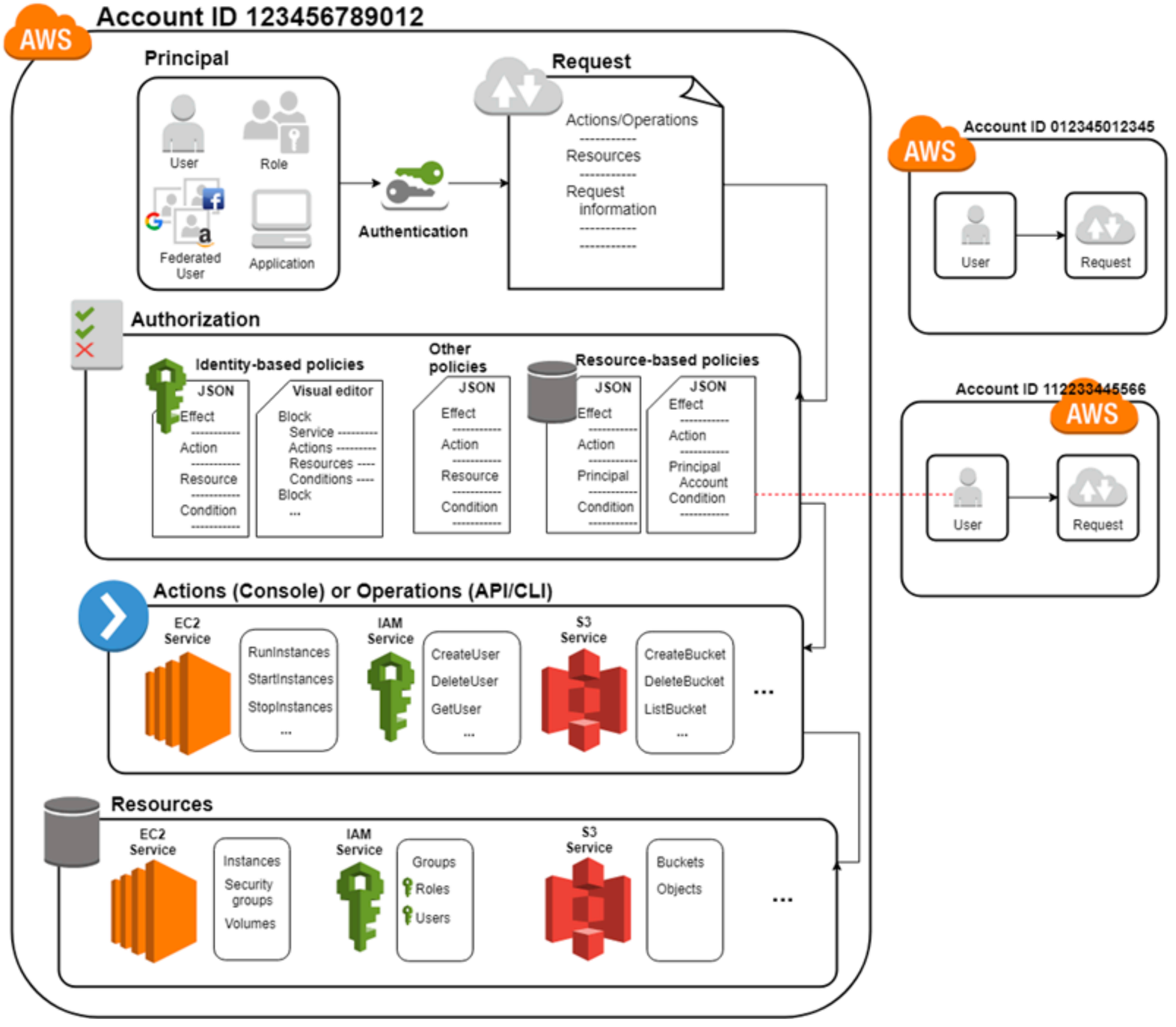
IAM 的功能是什麼？

簡單說就是　**IAM 是提供控制帳戶身分驗證和授權所需的基礎設施**

根據最佳實務，

勿使用 root user 登入資料來進行您的每日工作。

請建立 IAM 實體 (使用者和角色)。您也可以支援聯合身分使用者或程式設計存取，讓應用程式存取您的 AWS 帳戶。


Account ID 123456789012
Principal
User
Role
Federated User
Application
Authentication
Request
Actions/Operations
Resources
Request information
Authorization
Identity-based policies
JSON
Effect
Action
Resource
Condition
Visual editor
Block
Service
Actions
Resources
Conditions
Other policies
Resource-based policies
Principal
Account
Actions (Console) or Operations (API/CLI)
EC2 Service
RunInstances
StartInstances
StopInstances
IAM Service
CreateUser
DeleteUser
GetUser
S3 Service
CreateBucket
DeleteBucket
ListBucket
Resources
Instances
Security groups
Volumes
Groups
Roles
Users
Buckets
Objects
Account ID 012345012345
Account ID 112233445566

IAM特性

1.集中管理
2.與AD帳號整合達成Single Sign-On (SSO)目的.(如 AWS STS 臨時安全登入)
3.各項AWS資源細部的存取控制
4.透過User/Group/Roles 三種角色搭配來控制存取權限
5.支援多因素認證MFA（Multi-Factor Authentication）
6.必要時可提供users/groups的暫時性存取功能
7.提供使用者自訂密碼輪替規則
8.提供適用於 Payment Card Industry (PCI) Data Security Standard (DSS) 合規的標準化架構。PCI DSS 協助確保企業維持安全的環境，以儲存、處理和傳輸信用卡資訊。

IAM權限管理

- **User**：在 AWS 中建立的實體，代表使用此實體與 AWS 互動的人員或應用程式。AWS 中的使用者包含名稱和登入資料。
- **Group**：需要共用一組相同權限的使用者群組
- **Policies**： AWS 中的一個物件，當其和實體或資源建立關聯時，便可定義其許可，大部分政策以 JSON 文件形式存放
- **Roles**：與Group類似，但是它只能套用在User和AWS資源（例如EC2），而不能套用在Group；一些AWS資源例如EC2或S3可以直接儲存相關的使用者認證，但會有安全疑慮及管理上的麻煩，因此透過Roles可以解決這類的問題。

User and Policies

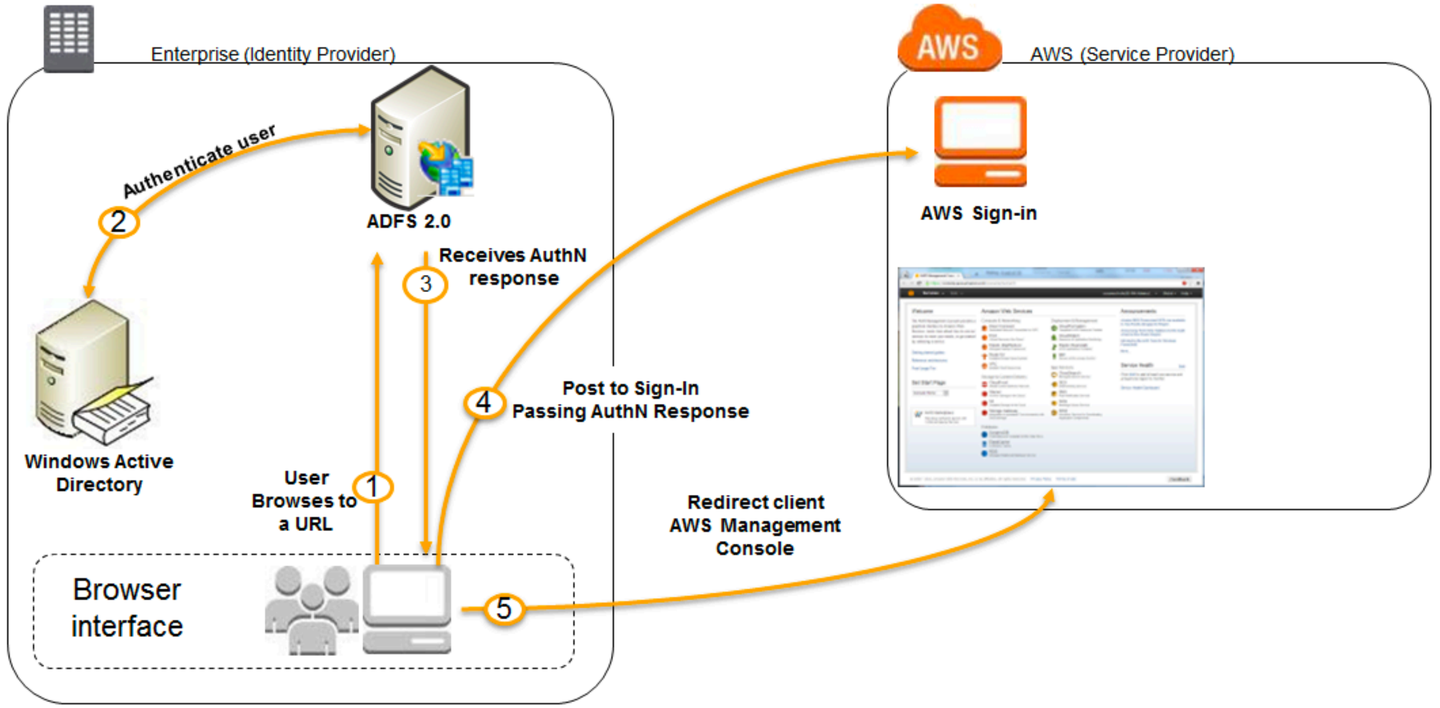
範例顯示 JSON 政策，其允許使用者執行 us-east-2 區域內 123456789012 帳戶之 Books 資料表上的所有 Amazon DynamoDB 動作 (dynamodb:*)。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "dynamodb:*",
    "Resource": "arn:aws:dynamodb:us-east-2:123456789012:table/Books"
  }
}
```

參考來源：

https://docs.aws.amazon.com/zh_tw/IAM/latest/UserGuide/reference_policies_elements.html

整合 AD



參考來源

https://aws.amazon.com/tw/blogs/security/enabling-federation-to-aws-using-windows-active-directory-adfs-and-saml-2-0/

IAM 最佳實務

主題

- 妥善保管 AWS Account Root User 存取金鑰
- 建立個別 IAM 使用者
- 使用群組指派許可給 IAM 使用者
- 授予最低權限
- 開始使用許可搭配 AWS 受管政策
- 使用客戶受管政策而不是內嵌政策
- 使用存取層級來檢閱 IAM 權限
- 為您的使用者設定高強度密碼政策
- 啟用 MFA
- 對於在 Amazon EC2 執行個體上執行的應用程式使用角色
- 使用角以委派許可
- 請勿分享存取金鑰
- 定期輪換登入資料
- 移除不必要的登入資料
- 為擁有額外的安全使用政策條件
- 監控 AWS 帳戶中的活動
- 有關 IAM 最佳實務的影片簡報

參考來源：
https://docs.aws.amazon.com/zh_tw/IAM/latest/UserGuide/reference_policies_elements.html

Lab

動手做

https://console.aws.amazon.com/iam/home#/home

Homework

新增使用者

1 2 3 4 5

成功

您已成功建立如下所示的使用者。您可以檢視和下載使用者安全登入資料。您也可以透過電子郵件向使用者提供 AWS 管理主控台的登入指示。這是可以下載這些登入資料的最後機會。不過，您可以隨時建立新的登入資料。

擁有 AWS 管理主控台存取的使用者能夠登入：https://826982172389.signin.aws.amazon.com/console

下載 .csv

		使用者	存取金鑰 ID	私密存取金鑰
▶	✓	admin	AKIA4BC72Q3SXUD2OMHT	********* 顯示