

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/>

聯絡銷售人員 支援 ▼ 中文(繁體) ▼ 我的帳戶 ▼

建立 AWS 帳戶

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

建立 AWS 帳戶

電子郵件地址

密碼

確認密碼

AWS 帳戶名稱 ⓘ

繼續

[登入現有 AWS 帳戶](#)

© 2020 Amazon Web Services, Inc. 或其附屬公司。
保留所有權利。

[隱私權政策](#) | [使用條款](#)

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**」

聯絡資訊

所有欄位都必須填寫。

請選擇帳戶類型並透過填寫下列欄位，提供您的詳細聯絡資訊。

帳戶類型 ⓘ

☒ 專業級 ☐ 個人

全名

gamesoft.jackylin

公司名稱

電話號碼

國家/地區

美國 ▾

地址

請填入 鄉鎮里、街路、巷弄

門牌號碼、樓層等資訊

縣市

省或地區

郵遞區號

☐ 勾選此欄表示您已閱讀並同意

[AWS 客戶協議條款](#)

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

付款資訊

我們會使用您的付款資訊來驗證您的身分，且僅用於超過 [AWS 免費方案限制](#) 的使用量。低於 AWS 免費方案限制時，我們不會向您收取費用。如需詳細資訊，請參閱[常見問題集](#)。



當您提交付款資訊時，我們將會向您的信用卡收取 1 USD/EUR 作為驗證費用，以確保您的卡片有效。該金額在信用卡對帳單中會顯示為待定達 3 至 5 天，直到驗證完成，屆時此收費將會移除。系統可能會將您重新導向至銀行網站以授權驗證收費。

信用卡/金融卡號

截止日期

持卡人姓名

帳單地址

☒ 使用我的聯絡地址

**No.25, Wenping Rd., Anping Dist.
taipei 70846
TW**

☐ 使用新地址

驗證與加入

AWS Root Account

電話設定

- 電話以行動電話為佳

電話驗證

AWS 會使用自動系統立即打給您。聽到提示時，請用電話鍵盤輸入 AWS 網站上的 4 位數號碼。

提供電話號碼

請在下方輸入您的資訊，然後按一下「立刻打電話給我」按鈕。

國家/地區代碼

臺灣 (+886)

電話號碼 分機

安全性檢查

ba66fe

立刻打電話給我

© 2018 Amazon Web Services, Inc. 或其附屬公司。保留所有權利。
[隱私權政策](#) | [使用條款](#) | [登出](#)

AWS Root Account

電話驗證

- 在手機輸入畫面顯示的驗證碼

正在進行通話...

請接聽 AWS 的來電，聽到提示時，請用電話鍵盤輸入 4 位數號碼。

8 5 7 7

AWS Root Account

支援計劃

- 選擇「Free」(免費)
- Support Ticket 回應比較慢

選取支援計劃

AWS 提供一系列精選支援方案，滿足您的各種需求。依據您的 AWS 用量，選出最適合的支援方案。 [進一步了解](#)



基本方案

免費

- 隨附於所有帳戶
- 全年無休，自助式參與論壇及存取資源
- 最佳實務檢查，協助提升安全性與效能
- 存取健康狀態和通知



開發人員計劃

29 USD/月起

- 用於早期採用、測試與開發
- 營業時間可經由電子郵件聯絡 **AWS Support**
- 1 名主要聯絡人可以拓展的案例數量無限制
- 非生產系統的 12 小時回應時間



商業計劃

100 USD/月起

- 用於生產工作負載和商業關鍵依存項目
- 可經由線上聊天、電話和電子郵件，全年無休聯絡 **AWS Support**
- 無限聯絡人可以拓展的案例數量無限制
- 生產系統的 1 小時回應時間

需要企業級支援？

聯絡您的客戶經理，以獲得更多在 AWS 上執行業務和關鍵任務工作負載的資訊 (15000 USD/月起算)。 [進一步了解](#)

© 2018 Amazon Web Services, Inc. 或其附屬公司。保留所有權利。

[隱私權政策](#) | [使用條款](#) | [登出](#)

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

歡迎使用 Amazon Web Services

感謝您建立 Amazon Web Services 帳戶。我們正在啟用您的帳戶，應該只需要幾分鐘的時間。當這個程序完成時，您會收到一封電子郵件。

[登入主控台](#)
[聯絡銷售人員](#)

個人化您的體驗

請填寫以下資訊，以接收符合您的角色和興趣的建議。

我的角色是：[選取角色](#)

我有興趣了解：[選取領域](#)

[提交](#)

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



Sign in ⓘ

Email address of your AWS account

Or to sign in as an IAM user, enter your
[account ID](#) or [account alias](#) instead.

Next

— New to AWS? —

Create a new AWS account

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」](#)

您的安全登入資料

使用此頁面來管理 AWS 帳戶的登入資料。若要管理 AWS Identity and Access Management (IAM) 使用者的登入資料，請使用 [IAM 主控台](#)。

若要進一步了解 AWS 登入資料的類型及其使用方式，請參閱 AWS 一般參考中的 [AWS 安全登入資料](#)。

▲ 密碼

▼ 多重驗證 (MFA)

使用 MFA 提高 AWS 環境的安全性。登入 MFA 保護的帳戶需要使用者名稱和密碼，以及來自 MFA 裝置的身份驗證代碼。

啟動 MFA

▲ 存取金鑰 (存取金鑰 ID 和私密存取金鑰)

▲ CloudFront 金鑰對

▲ X.509 憑證

▲ 帳戶識別符

設定MFA

Virtual MFA (Apps)

- 選擇「A Virtual MFA device」



The screenshot shows a modal dialog titled "管理 MFA 裝置" (Manage MFA Devices) with a close button (X) in the top right corner. The dialog contains the following text and options:

選擇要指派的 MFA 裝置類型：

- ☒ **虛擬 MFA 裝置**
在行動裝置或電腦上安裝的 Authenticator 應用程式
- ☐ **U2F 安全金鑰**
YubiKey 或其他任何相容的 U2F 裝置
- ☐ **其他硬體 MFA 裝置**
Gemalto 符記

如需所支援 MFA 裝置的相關詳細資訊，請參閱 [AWS 多重因素認證](#)

At the bottom right, there are two buttons: "取消" (Cancel) and "繼續" (Continue).

設定MFA

可以利用手機裝 Google Authenticator
掃描條碼去新增

設定虛擬 MFA 裝置

1. 在您的行動裝置或電腦上安裝相容的應用程式
請參閱 [相容應用程式的清單](#)

2. 使用您的虛擬 MFA 應用程式和裝置的相機來掃描 QR 碼



或者，您也可以輸入私密金鑰。 [顯示私密金鑰](#)

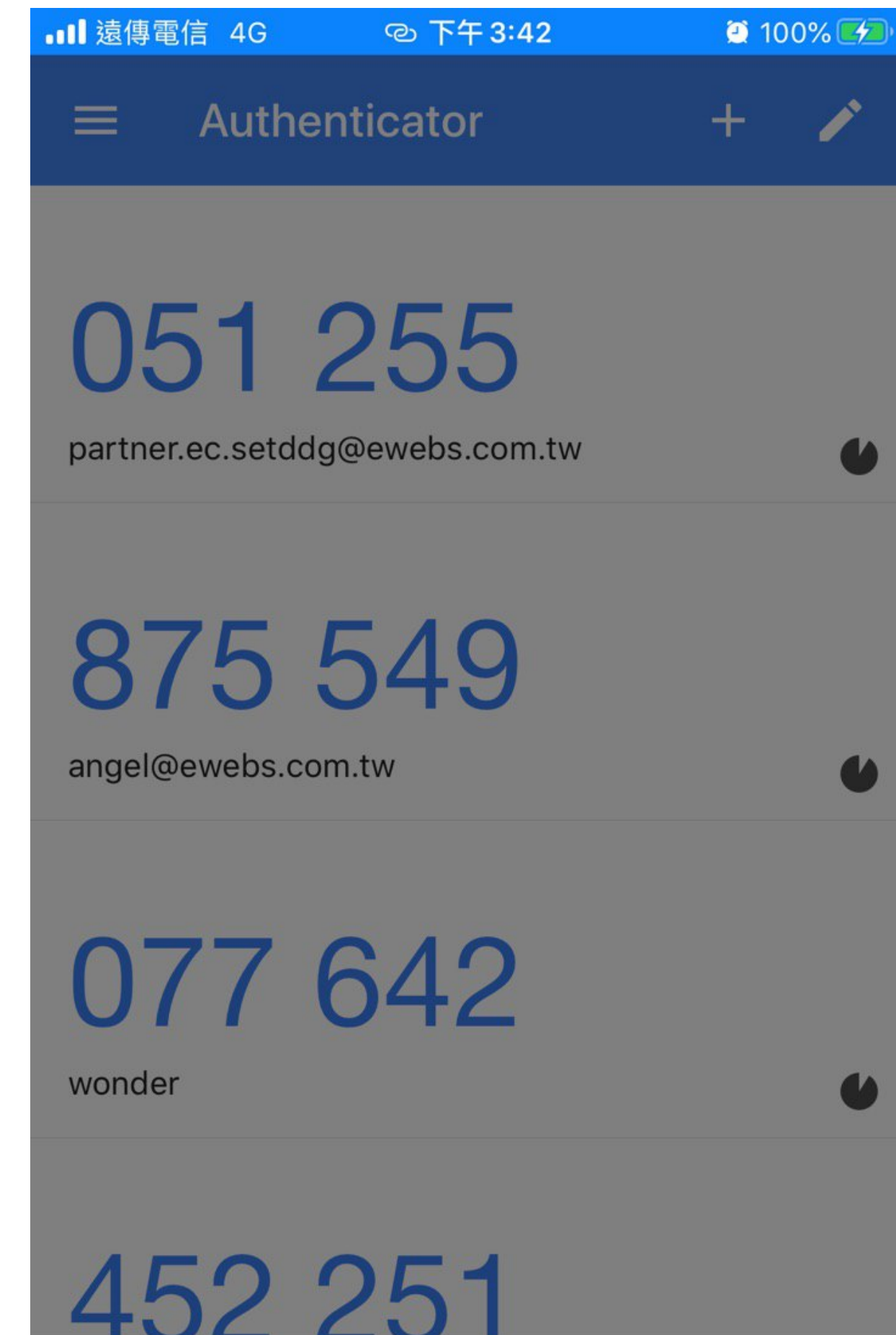
3. 在下方輸入兩組連續的 MFA 代碼

MFA 代碼 1

取消

上一個

指派 MFA



 掃描條碼

 以人工方式輸入驗證碼

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

AWS Budgets									
<div>Create budgetCopyEditDeleteDownload CSV?</div>									
Filter by budget name									
		Budget ty..↕	Budget name↕	Current	Forecasted	Budgeted↕	Current vs. budgeted↕	Forecasted vs. budgeted↕	
<input type="checkbox"/>	▶	Cost	Monthly Budget	(\$0.02)	\$0.57	\$1.00	(2%)	57%	

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。



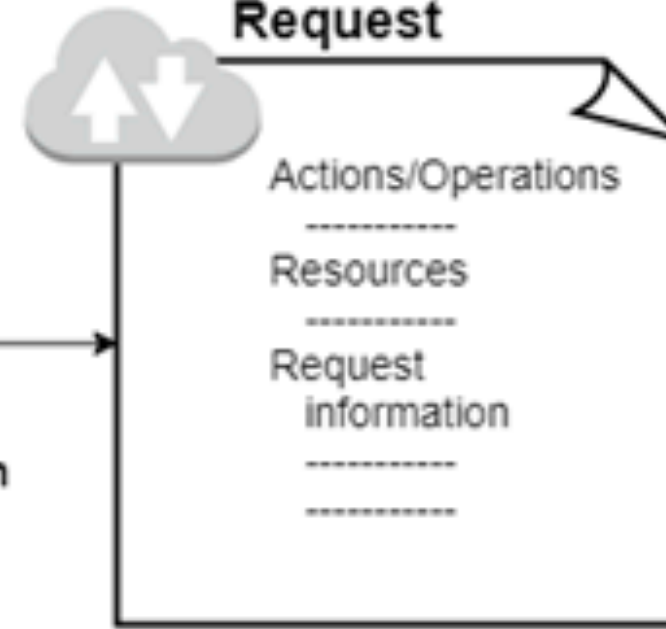
Account ID 123456789012

Principal



Authentication

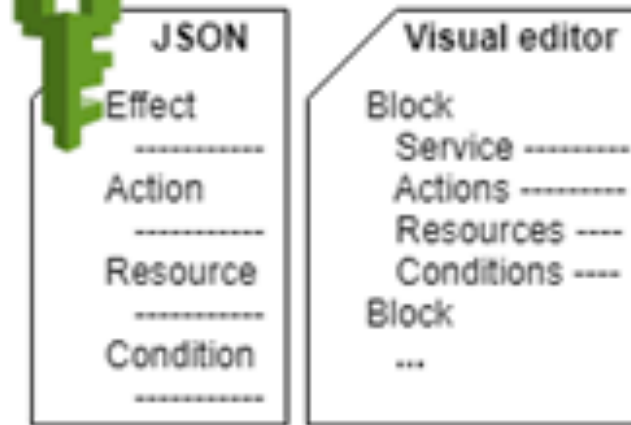
Request



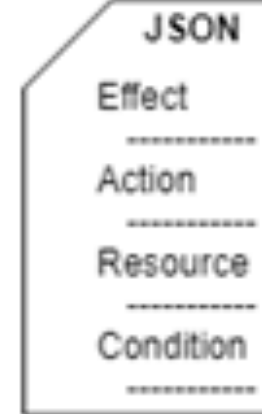
Authorization



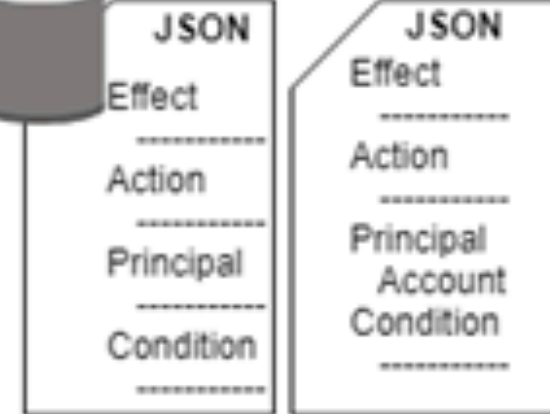
Identity-based policies



Other policies



Resource-based policies



Actions (Console) or Operations (API/CLI)

EC2 Service



RunInstances
StartInstances
StopInstances
...

IAM Service



CreateUser
DeleteUser
GetUser
...

S3 Service



CreateBucket
DeleteBucket
ListBucket
...



Resources

EC2 Service



Instances
Security groups
Volumes

IAM Service



Groups
Roles
Users

S3 Service



Buckets
Objects
...



Account ID 012345012345



User



Request

Account ID 112233445566



User



Request

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

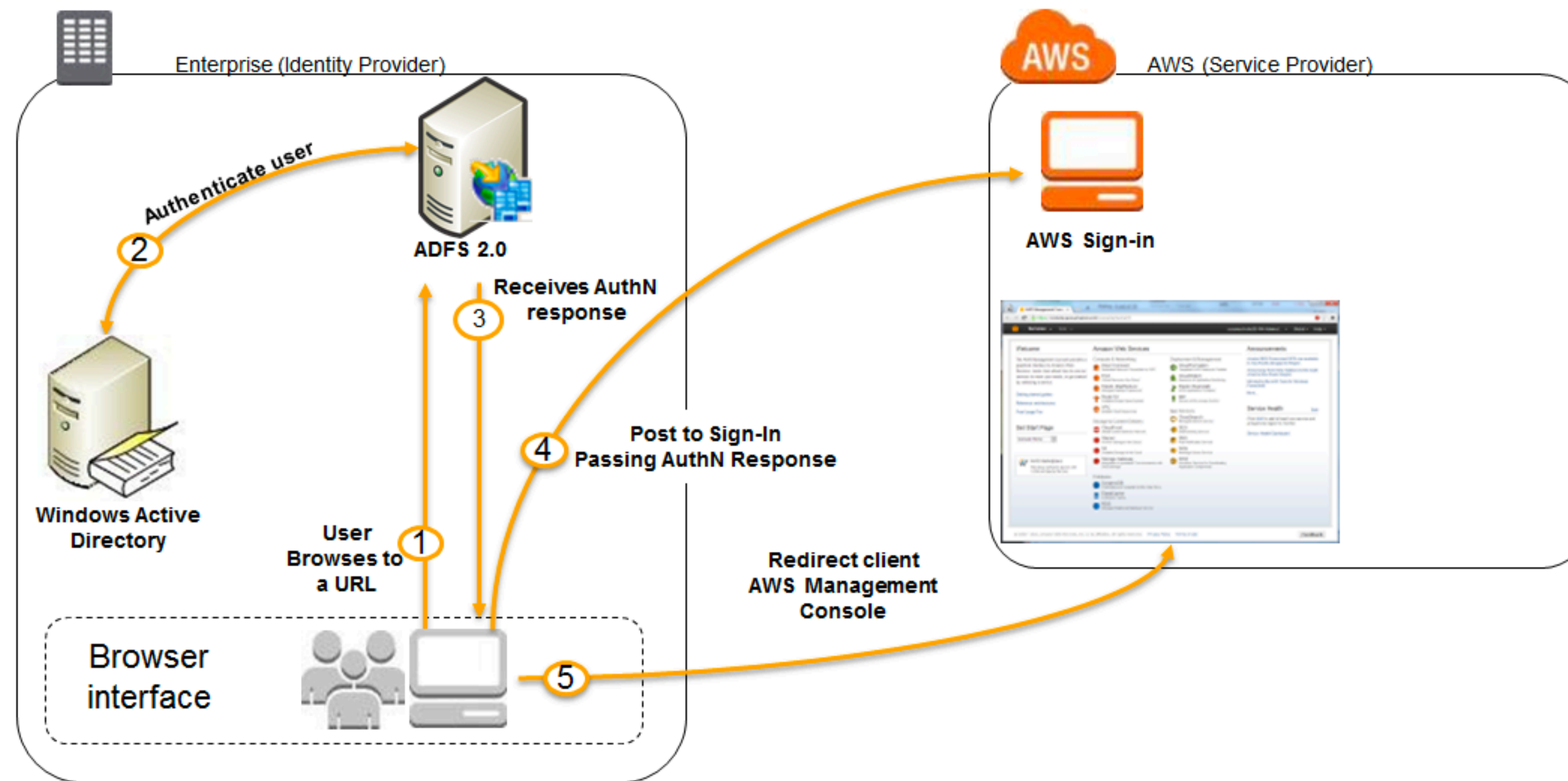
範例顯示 JSON 政策，其允許使用者執行 us-east-2 區域內 123456789012 帳戶之 Books 資料表上的所有 Amazon DynamoDB 動作 (dynamodb:*)。

```
{  
  "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