

Secure by Default

用Serverless實作 零信任的Port Knocking

林家瑋 (Ray Lin)
2025/04



- 全球首批 GCR首位 AWS Security Hero
- iFUS System Consultants Ltd. – 資安長(CISO)
- DataBrushing.ai (QSP) – 數位長(CDO)
- 長宏專案(PM-ABC) – PMI授權培訓講師 (PMP/PMI-ACP)
- 全智網科技(AI Network) – ISC2授權講師 / AWS授權講師
- 巨匠電腦 – 資安課程合作講師
- ISC2 Taipei Chapter – 理事 / 媒體公關委員會 主委 | PMI Taiwan獎項辦公室(PTGA) – 執行長
- DevSecOps Taiwan – 社長
- 登豐數位、鑑智實相、捷虹資訊、德慎精算、睿峯管顧 – 顧問 / 講師
- 曾服務於美商、日商、台商、新創、上市櫃、跨國集團等不同型態的公司
- 擔任過CEO、COO、CISO、CDO、產品主管、IT主管、業務主管、資深SI工程師與資深PG
- 曾獲台灣發明家創意獎、PMI-TW優良志工獎與績優執行理監事、翻譯出版7本知名敏捷書籍，並取得超過40張國際證照

現在的網路使用情境越趨複雜



零信任(Zero Trust)

- 零信任是一種資安策略，2010年由Forrester Research的John Kindervag 提出
- 基本理念：永不信任，始終驗證 (Never Trust, Always Verify)
- 例如：ATM提款、多門大樓



我國政府機關導入零信任

- 2020年美國國家標準技術研究院(NIST)正式頒布標準文件SP800-207：零信任架構(Zero Trust Architecture, ZTA)
- 我國數位發展部資通安全署推動政府機關導入零信任網路
 - **身分鑑別**：以生物識別鑑別器進行無密碼雙因子身分鑑別
 - **設備鑑別**：基於信任平台模組(TPM)之設備鑑別，並進行設備健康管理
 - **信任推斷**：依設備健康狀態、資安威脅情資及使用者情境等資訊，動態支援存取決策



屬性為基礎存取控制(ABAC)_限制IP

此Policy會拒絕來自203.0.113.0/24 IP範圍以外對任何資源執行任何操作

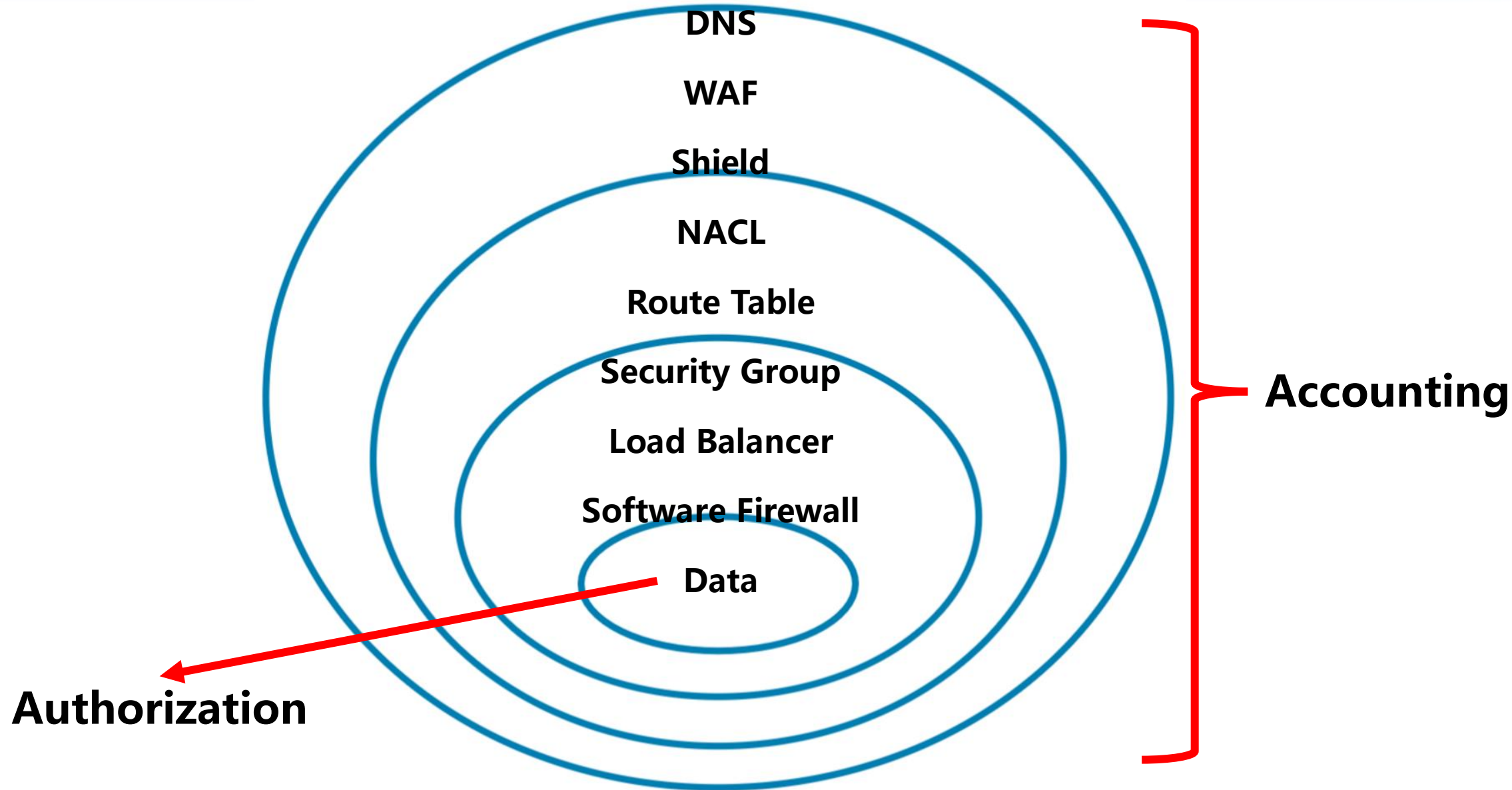
```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NotIpAddress": {"aws:SourceIp": "203.0.113.0/24"}
    }
  }
}
```

屬性為基礎存取控制(ABAC)_限制時間

此Policy會拒絕在2025/11/11 13:00~14:00 UTC一小時之間對任何資源執行任何操作

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "DateGreaterThan": {"aws:CurrentTime": "2025-11-11T13:00:00Z"},
      "DateLessThan": {"aws:CurrentTime": "2025-11-11T14:00:00Z"}
    }
  }
}
```

每道關卡都要Authentication



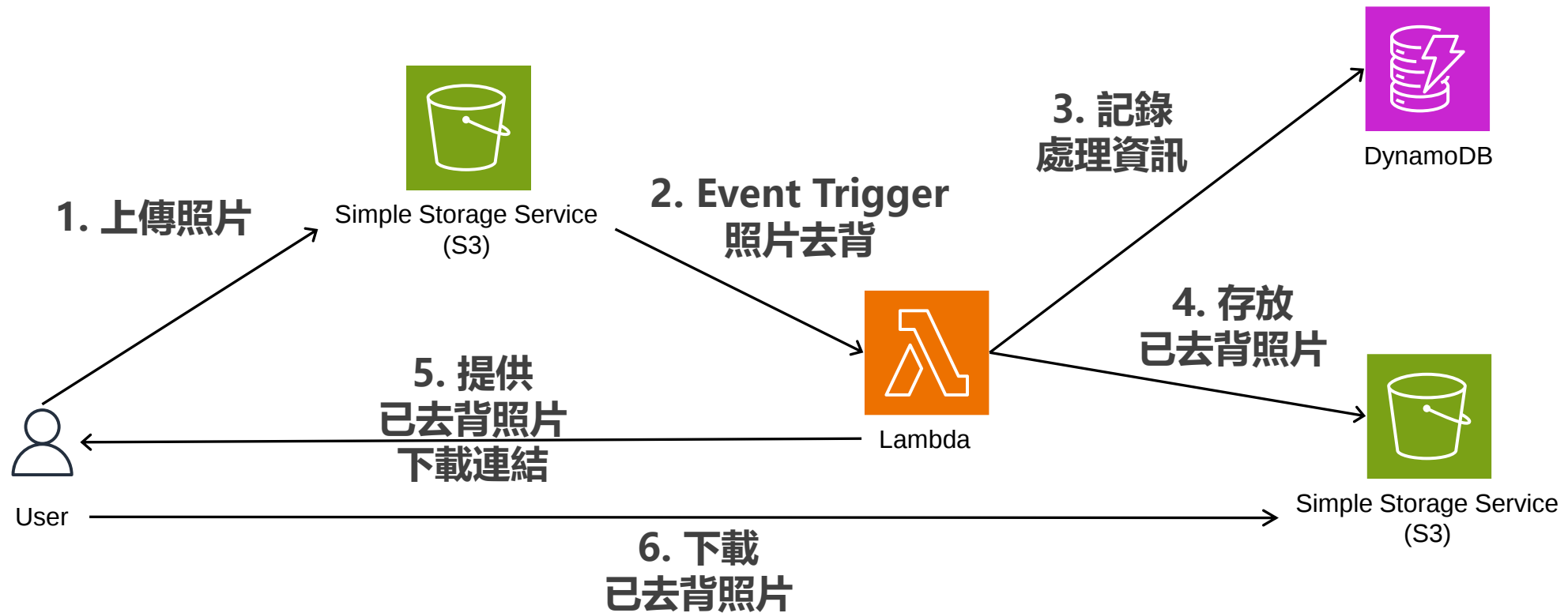
Secure by Default & Port Knocking

- **Secure by Default**: 系統設定應預設為安全狀態，例如：預設開啟MFA
- **Port Knocking**: 一種網路安全技術，允許遠端使用者透過向特定Port發送一系列"敲門"請求（按特定順序連接到特定Port）來打開防火牆中原本關閉的Port。這有點像在進入建築物前敲一個特殊的敲門序列

芝麻開門



無伺服器(Serverless)



星爺曾經說過



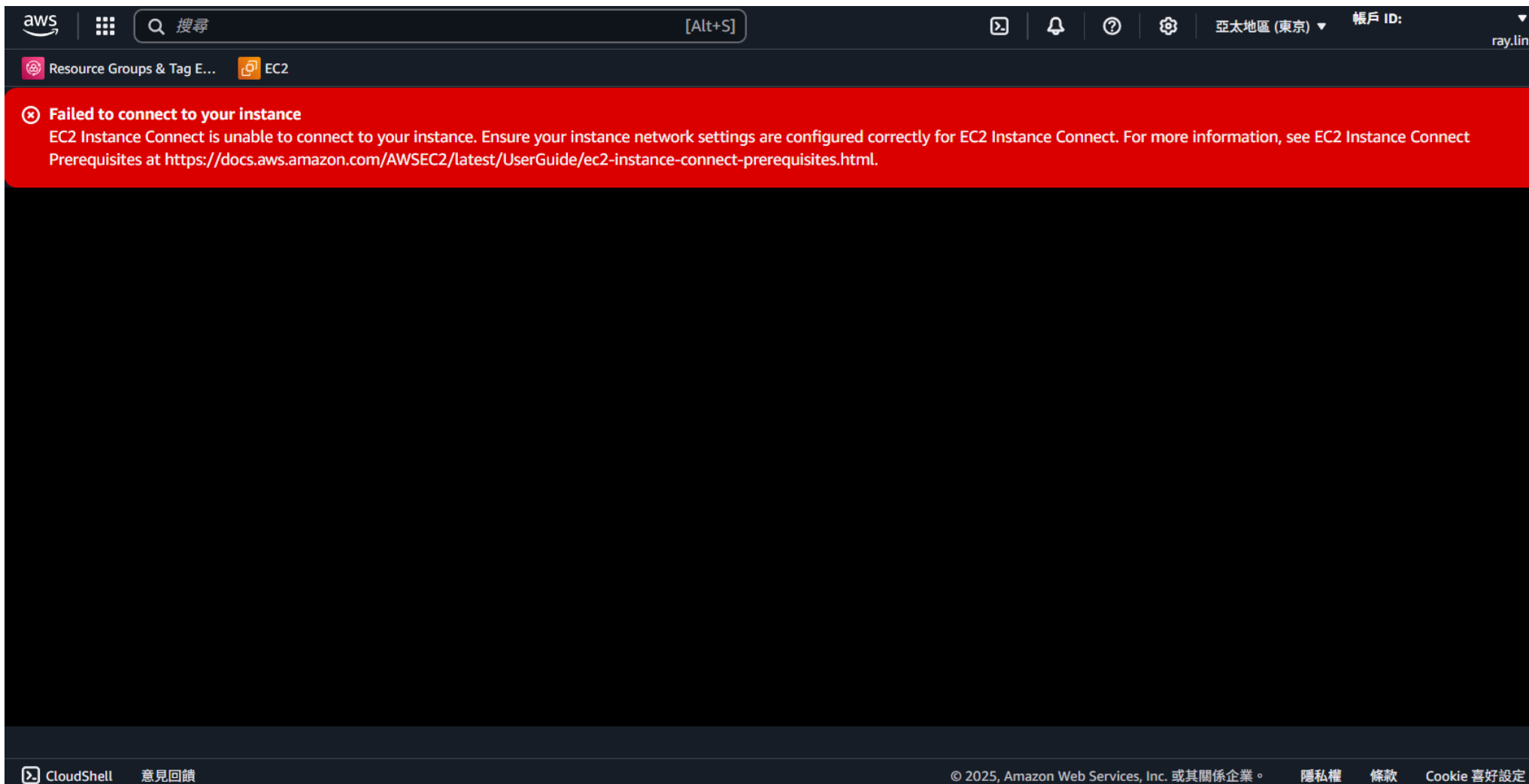
Port Knocking模擬

- 使用AWS S3+ AWS Lambda模擬Port Knocking，當S3收到PortKnocking檔案時，觸發Lambda把Security Group的SSH傳入設定為0.0.0.0/0
- 步驟
 1. 啟動AWS EC2，測試SSH是否正常連線
 2. 調整AWS Security Group，確認SSH無法連線
 3. 建立S3 Bucket
 4. 在Lambda建立Python程式碼並Deploy
 5. 建立Lambda要使用的IAM Policy
 6. 將IAM Policy新增到Lambda的角色
 7. 新增s3:ObjectCreated:Put事件觸發
 8. 在S3上傳一個PortKnocking檔案，等30-60秒左右，測試SSH已可正常連線
 9. 在S3刪除PortKnocking檔案，等30-60秒左右，確認SSH無法連線

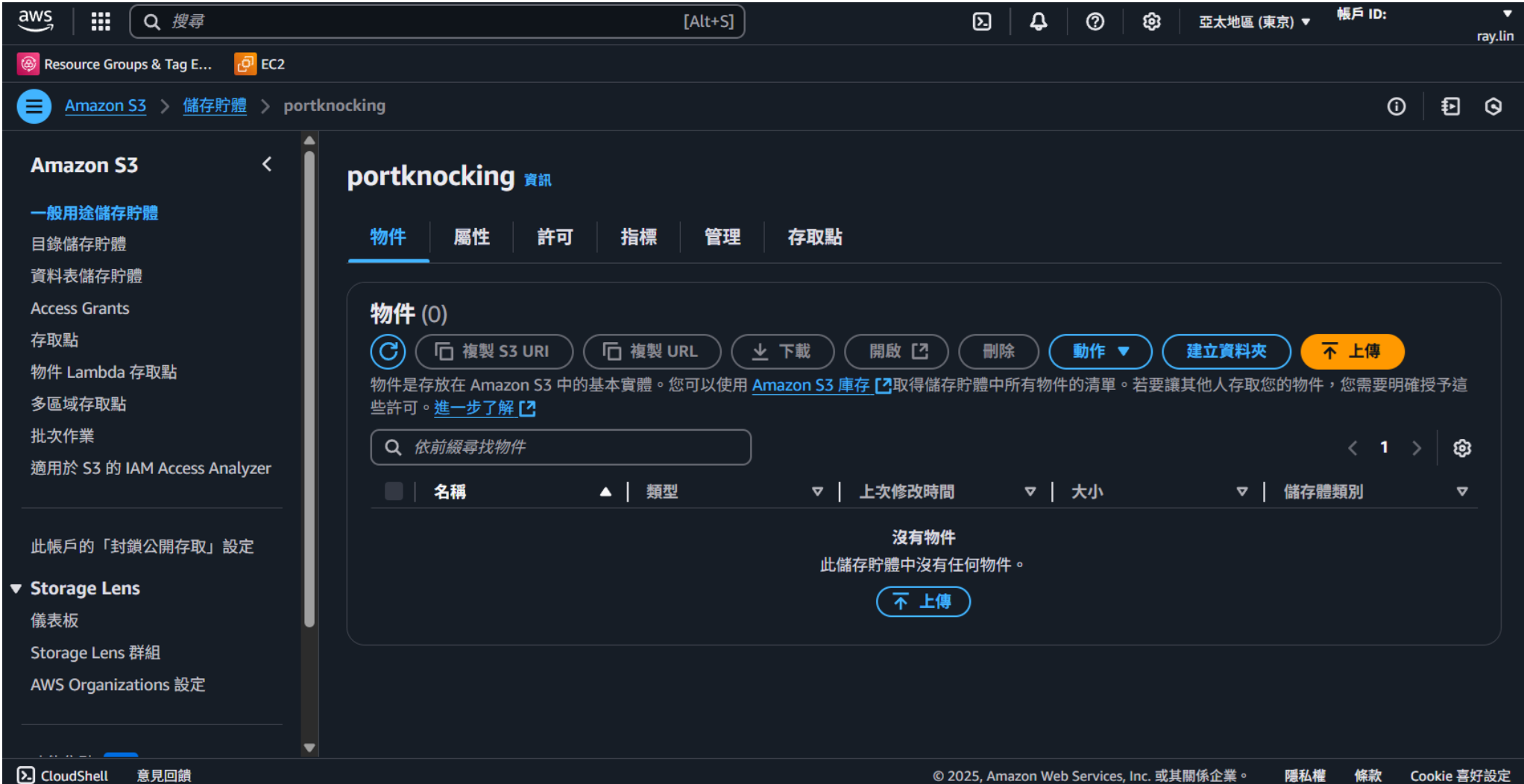
啟動AWS EC2，測試SSH是否正常連線

The image shows a screenshot of an AWS CloudShell terminal window. At the top, there's a navigation bar with the AWS logo, a search bar, and various icons. Below the navigation bar, there's a header for 'Resource Groups & Tag E...' and 'EC2'. The main area of the terminal displays the Amazon Linux 2023 logo, which consists of a stylized 'A' made of hash symbols and the text 'Amazon Linux 2023'. Below the logo, the URL 'https://aws.amazon.com/linux/amazon-linux-2023' is shown. The terminal prompt is '[ec2-user@ip-172-31-163-43 ~]\$'.

調整AWS SG，確認SSH無法連線

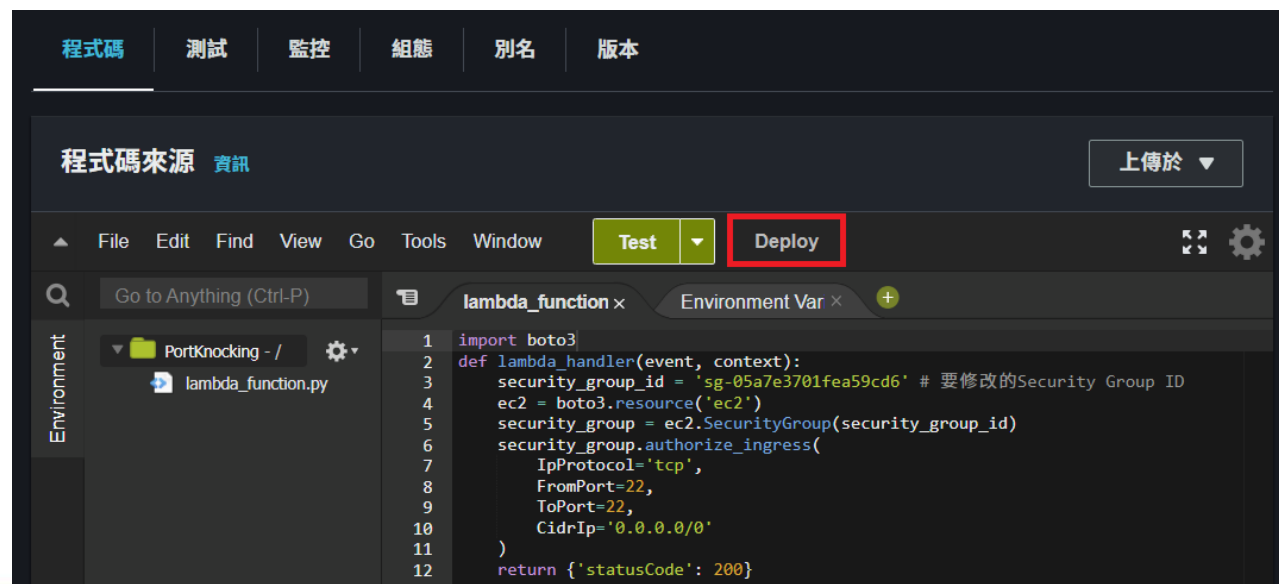


建立AWS S3 Bucket



在Lambda建立Python程式碼並Deploy

```
import boto3
def lambda_handler(event, context):
    security_group_id = 'sg-05a7e3701fea59cd6' # 要修改的Security Group ID
    ec2 = boto3.resource('ec2')
    security_group = ec2.SecurityGroup(security_group_id)
    security_group.authorize_ingress(
        IpProtocol='tcp',
        FromPort=22,
        ToPort=22,
        CidrIp='0.0.0.0/0'
    )
    return {'statusCode': 200}
```



新增S3 "PUT"觸發條件

編輯觸發條件

觸發組態



S3

aws

asynchronous

storage

儲存貯體

選擇或輸入當做事件來源的 S3 儲存貯體的 ARN。儲存貯體必須與函數位於相同的區域。



arn:aws:s3:::portknocking



儲存貯體必須位於區域 ap-northeast-1 內

事件類型

選取您要進行觸發 Lambda 函數的事件。您可以選擇性地為事件設定字首或尾碼。然而，針對每一個儲存貯體，個別事件無法擁有多個配置，其中具備與相同的物件金鑰相符的重疊字首或尾碼。

PUT



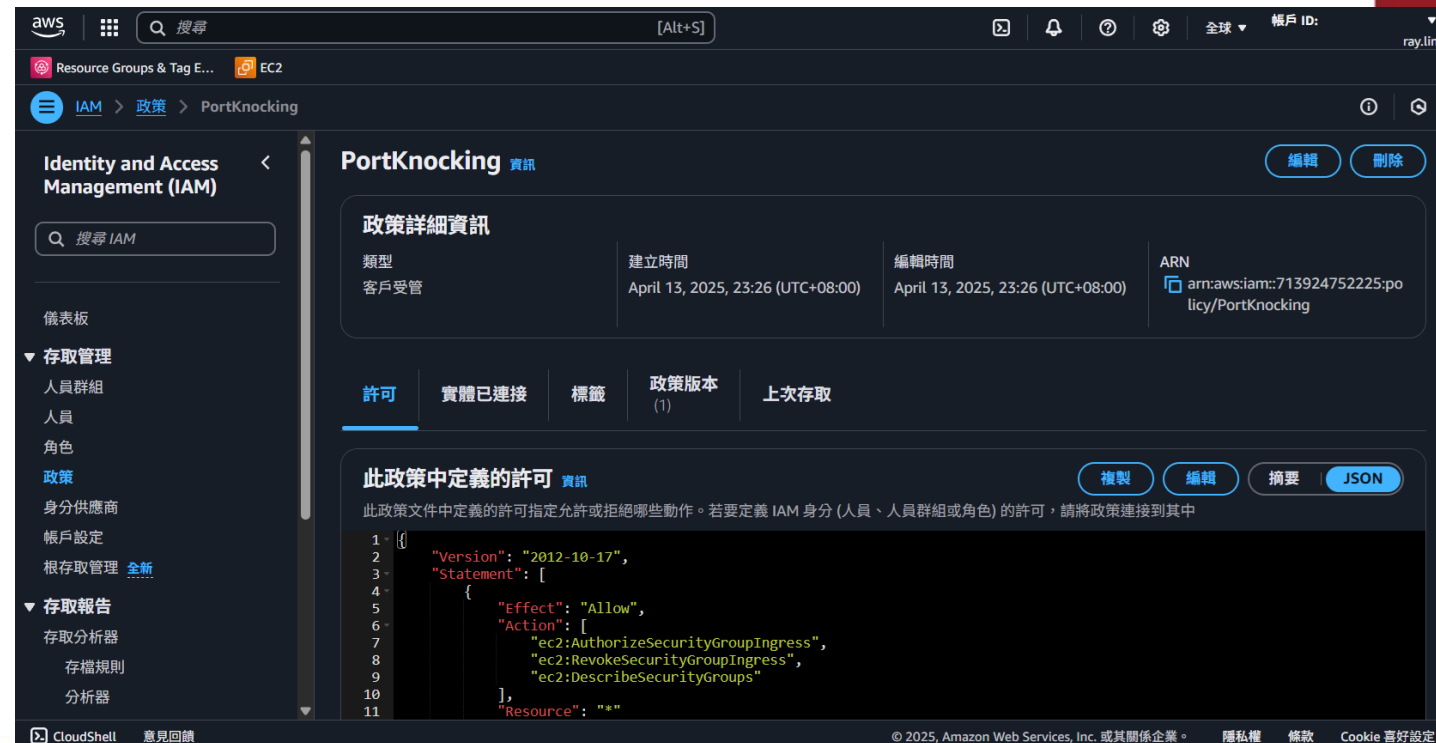
字首 - 選用

輸入一個選用字首來將通知限制為以相符字元為開頭之金鑰的物件。任何 **特殊字元**  均必須為 URL 編碼。

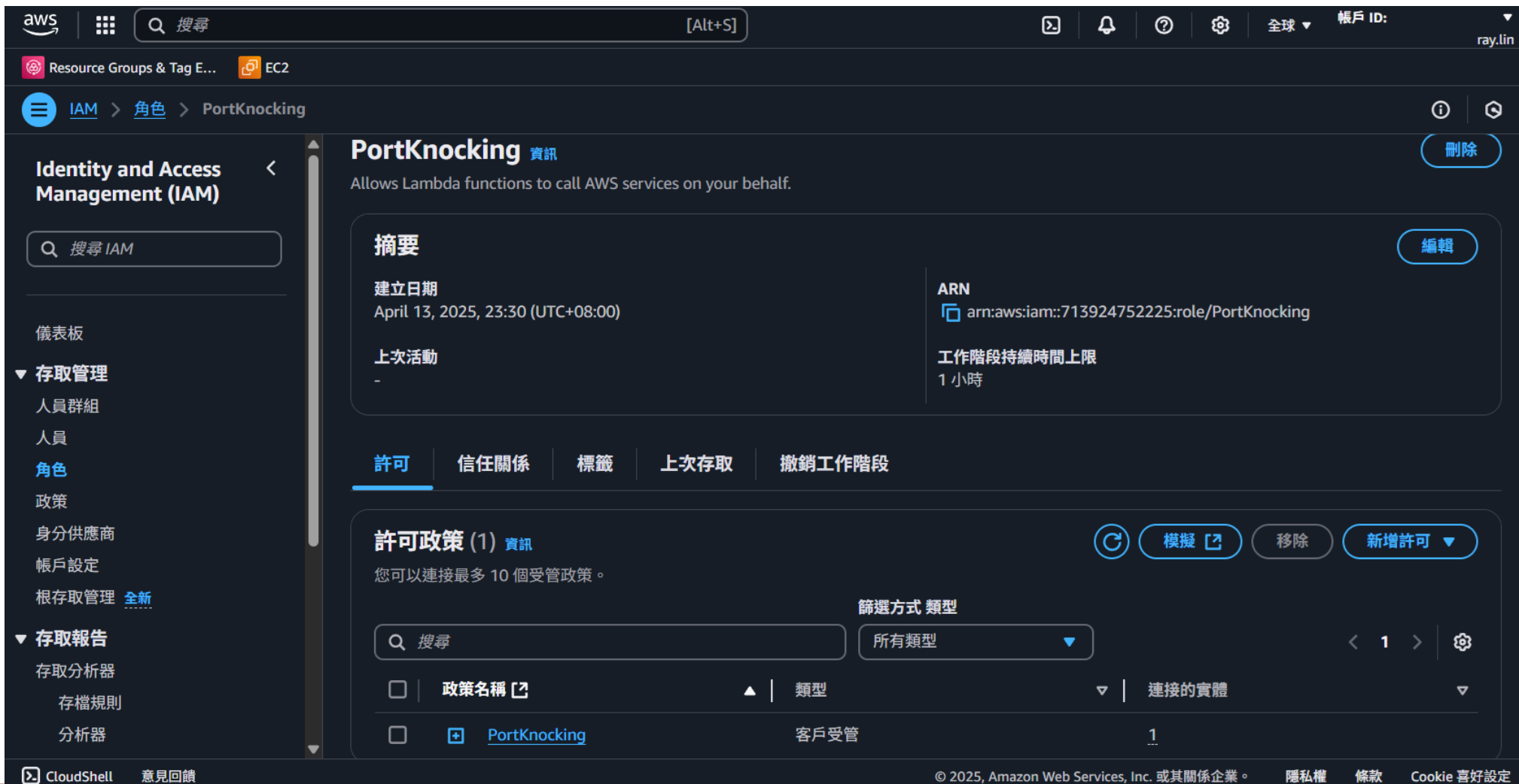
PortKnocking

建立Lambda要使用的IAM Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource": "*"
    }
  ]
}
```



將IAM Policy新增到Lambda的角色



The screenshot shows the AWS IAM console interface. The left sidebar contains the navigation menu with sections like 'Identity and Access Management (IAM)', '存取管理' (Access Management), and '存取報告' (Access Reports). The main content area displays the 'PortKnocking' role details, including its summary, creation date, and ARN. Below the summary, there are tabs for '許可' (Permissions), '信任關係' (Trust Relationships), '標籤' (Tags), '上次存取' (Last Accessed), and '撤銷工作階段' (Revoke Session). The '許可' tab is active, showing a list of permissions with a table containing columns for '政策名稱' (Policy Name), '類型' (Type), and '連接的實體' (Connected Entity). The table lists the 'PortKnocking' policy as a '客戶受管' (Managed by AWS) policy.

在S3上傳一個PortKnocking檔案

aws

搜尋

[Alt+S]

亞太地區 (東京)

帳戶 ID: ray.lin

Resource Groups & Tag E... EC2

☰

☰

☰

☑ 上傳成功

如需詳細資訊，請參閱檔案和資料夾資料表。

✕

上傳：狀態

關閉

ⓘ 當您離開此頁面之後，將無法再使用以下資訊。

摘要

目的地

s3://portknocking

已成功

☑ 1 個檔案, 0 B (0%)

失敗

⋯ 0 個檔案, 0 B (0%)

檔案和資料夾

組態

檔案和資料夾 (1 合計, 0 B)

🔍 依名稱尋找

< 1 >

名稱	資料夾	類型	大小	狀態	錯誤
PortKnocking.txt	-	text/plain	0 B	☑ 已成功	-

CloudShell

意見回饋

© 2025, Amazon Web Services, Inc. 或其關係企業。

隱私權

條款

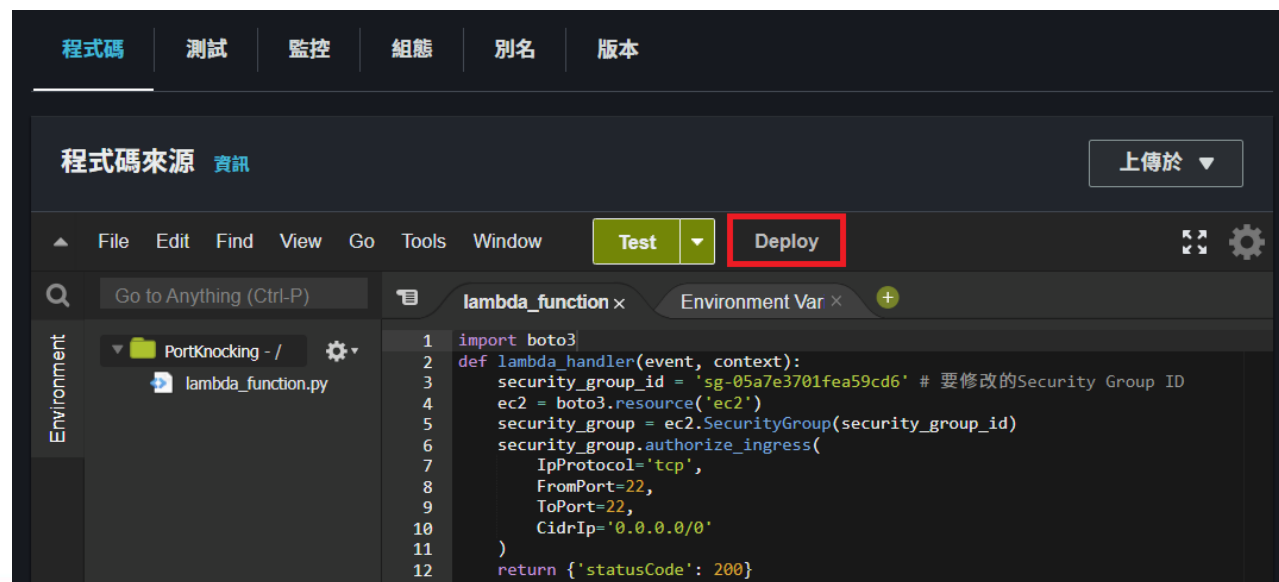
Cookie 喜好設定

30-60秒左右，測試SSH是否正常連線

The screenshot shows the AWS CloudShell interface. At the top, there's a navigation bar with the AWS logo, a search bar, and a user profile. Below this, the 'Resource Groups & Tag Editor' and 'EC2' tabs are visible. The main area is a terminal window with a dark background. It displays the Amazon Linux 2023 logo, which consists of a stylized 'A' made of hash symbols and a tilde. To the right of the logo, the text 'Amazon Linux 2023' is shown. Below the logo, the URL 'https://aws.amazon.com/linux/amazon-linux-2023' is displayed. The terminal prompt is '[ec2-user@ip-172-31-163-43 ~]\$'.

在Lambda建立Python程式碼並Deploy

```
import boto3
def lambda_handler(event, context):
    security_group_id = 'sg-05a7e3701fea59cd6' # 要修改的Security Group ID
    ec2 = boto3.resource('ec2')
    security_group = ec2.SecurityGroup(security_group_id)
    security_group.revoke_ingress(
        IpProtocol='tcp',
        FromPort=22,
        ToPort=22,
        CidrIp='0.0.0.0/0'
    )
    return {'statusCode': 200}
```



新增S3 "所有物件刪除事件" 觸發條件

The screenshot shows the AWS Lambda console interface for adding a new trigger. The breadcrumb navigation indicates the path: **Lambda** > **新增觸發條件** (Add Trigger).

新增觸發 (Add Trigger)

觸發組態 (Trigger Configuration)

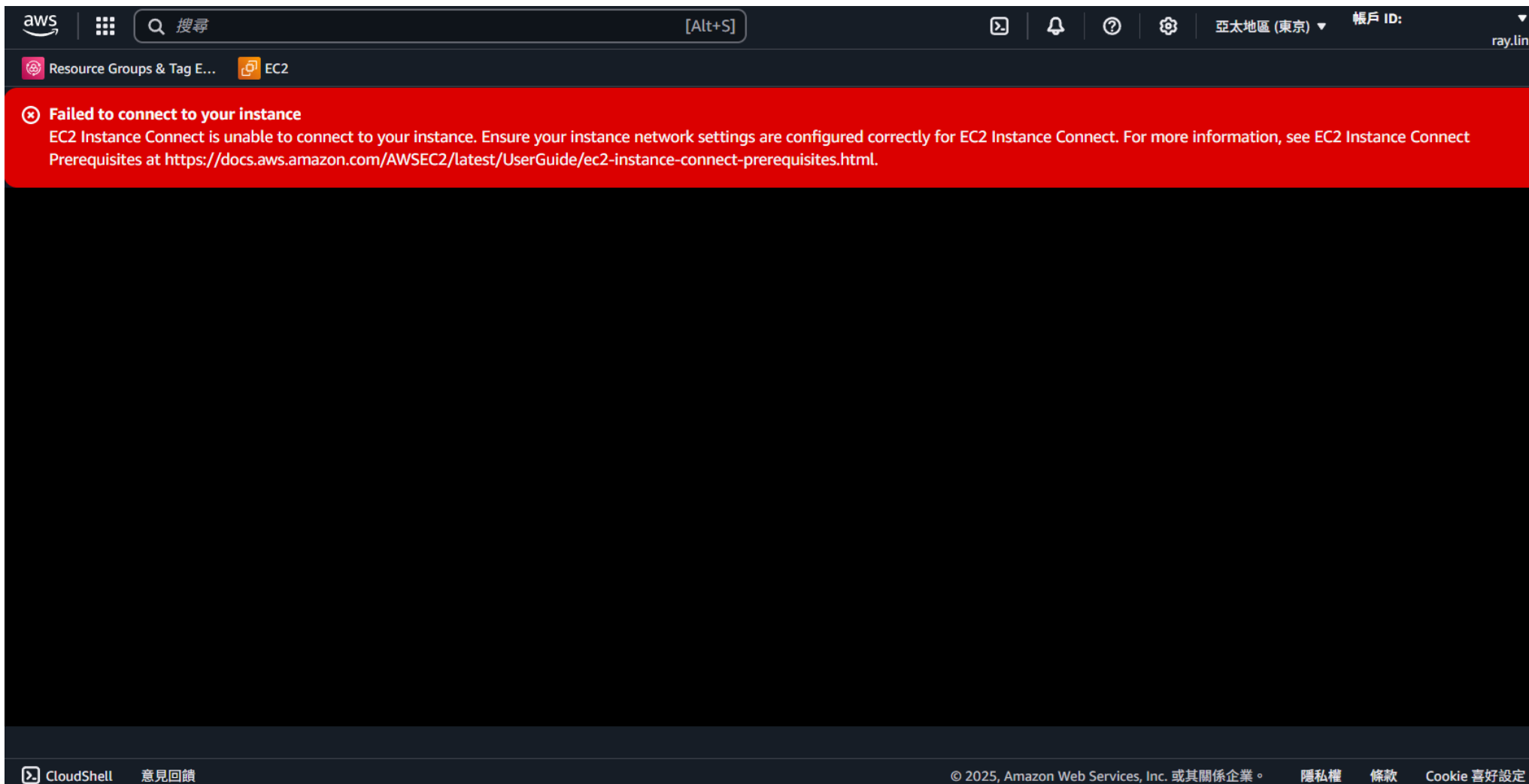
- 觸發組態** (Trigger Configuration): S3, asynchronous, storage.
- 儲存貯體** (Bucket): s3/portknocking. (Note: 儲存貯體必須與函數位於相同的區域。)
- 事件類型** (Event Type): 所有物件刪除事件 (All Objects Deleted).
- 字首 - 選用** (Prefix - Optional): PortKnocking.
- 尾碼 - 選用** (Suffix - Optional): (Empty).

At the bottom, there are links for **CloudShell**, **意見回饋** (Feedback), and a footer with copyright information: © 2025, Amazon Web Services, Inc. 或其關係企業。 (or its affiliates).

在S3刪除PortKnocking檔案

The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with the AWS logo, a search bar, and various icons. Below the navigation bar, there's a breadcrumb trail showing 'Resource Groups & Tag E...' and 'EC2'. The main content area has a green banner at the top stating '已成功刪除的物件' (Objects successfully deleted) and '查看下方的詳細資訊。' (View details below). Below this, a blue banner states '當您離開此頁面之後，將無法再使用以下資訊。' (After you leave this page, you will no longer be able to use the following information). The main section is titled '摘要' (Summary) and shows a table with three columns: '來源' (Source), '已成功刪除' (Successfully deleted), and '無法刪除' (Cannot delete). The '來源' column shows 's3://portknocking-1'. The '已成功刪除' column shows '1 個物件' (1 object). The '無法刪除' column shows '0 個物件' (0 objects). Below the summary, there are two tabs: '無法刪除' (Cannot delete) and '組態' (Configuration). The '無法刪除' tab is selected, showing a section titled '無法刪除 (0)' (Cannot delete (0)). Below this, there's a search bar and a table with columns: '名稱' (Name), '資料夾' (Folder), '類型' (Type), '上次修改時間' (Last modified time), '大小' (Size), and '錯誤' (Error). The table is empty, and a message at the bottom states '沒有無法刪除的物件。' (No objects cannot be deleted).

30-60秒左右，測試SSH是否無法連線



歡迎加我好友



Email: ray.lin@ifus.tw

台灣敏捷部落(TAT) - DevSecOps Taiwan

- 每個月免費線上分享
 - 每月固定一場 👉 1~2小時分享
 - 不定期快閃 👉 0.5~1小時分享
- 每季一次系列講座(3月/6月/9月/12月)
 - 從零開始的跨雲生活系列
- 社群分享主題與交流方向
 1. Agile / Waterfall / Hybrid
 2. DevSecOps (DevOps + Security)
 3. AI + Security
 4. Cybersecurity
 5. Cloud (AWS / Azure / GCP / SaaS)



林家瑋|大Ray@DevSecOps社長

DevSecOps Taiwan (2000+)



https://bit.ly/AG3_DevSecOps

Email: ray.lin@ifus.tw