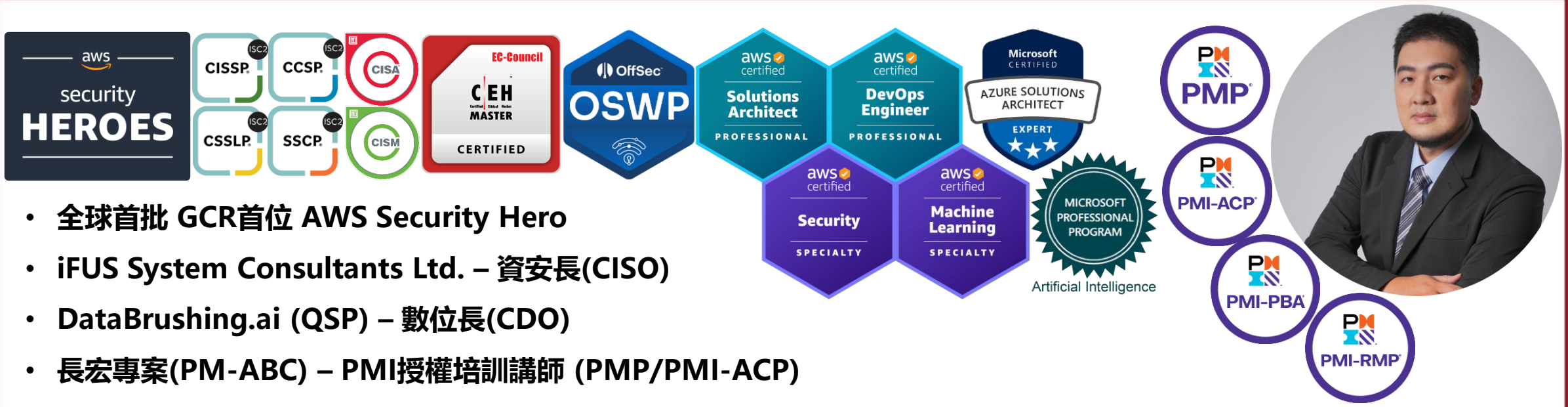
Secure by Default

用Serverless實作
零信任的Port Knocking

林家瑋 (Ray Lin)
2025/04

林家瑋 (Ray Lin), ray.lin@ifus.tw



- **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**

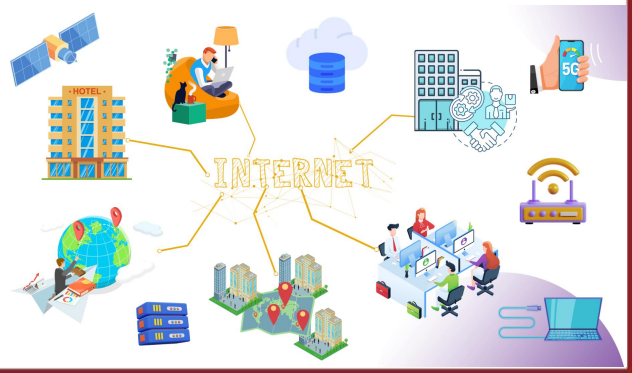
現在的網路使用情境越趨複雜

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

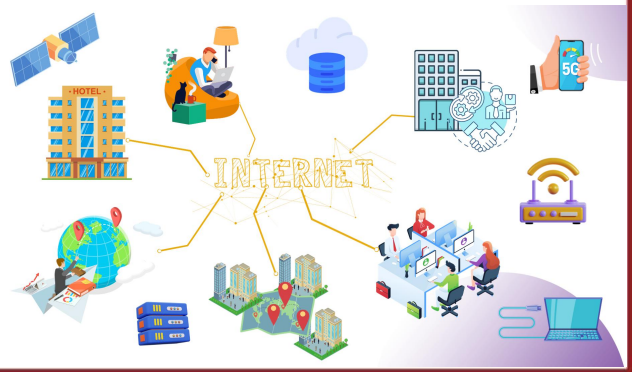
- 基本理念：永不信任，始終驗證 (Never Trust, Always Verify)

- 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

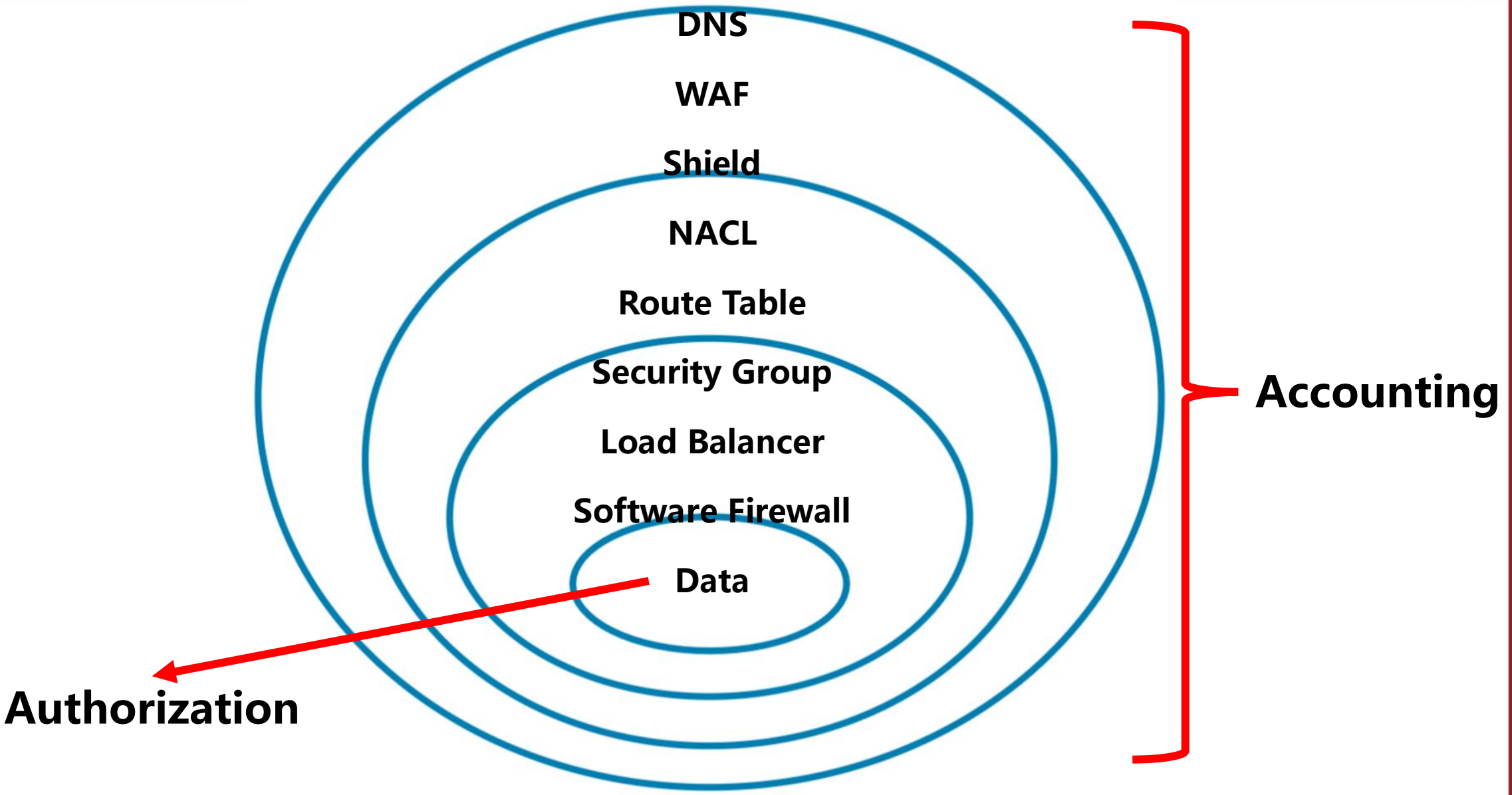
```
{
        "Version": "2012-10-17",
        "Statement": {
                "Effect": "Deny",
                "Action": "*",
                "Resource": "*",
                "Condition": {
                        "NotIpAddress": {"aws:SourceIp": "203.0.113.0/24"}
                }
        }
}
```

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



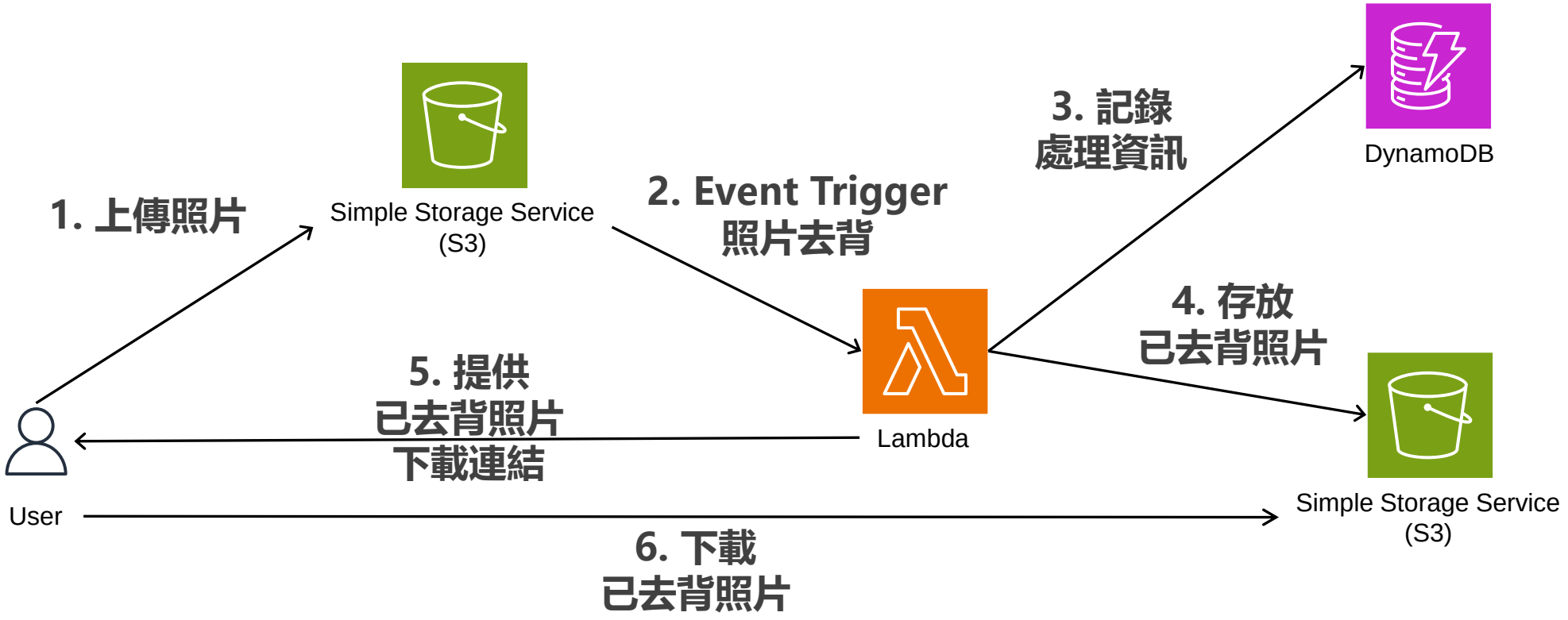
Secure by Default & Port Knocking

- 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)

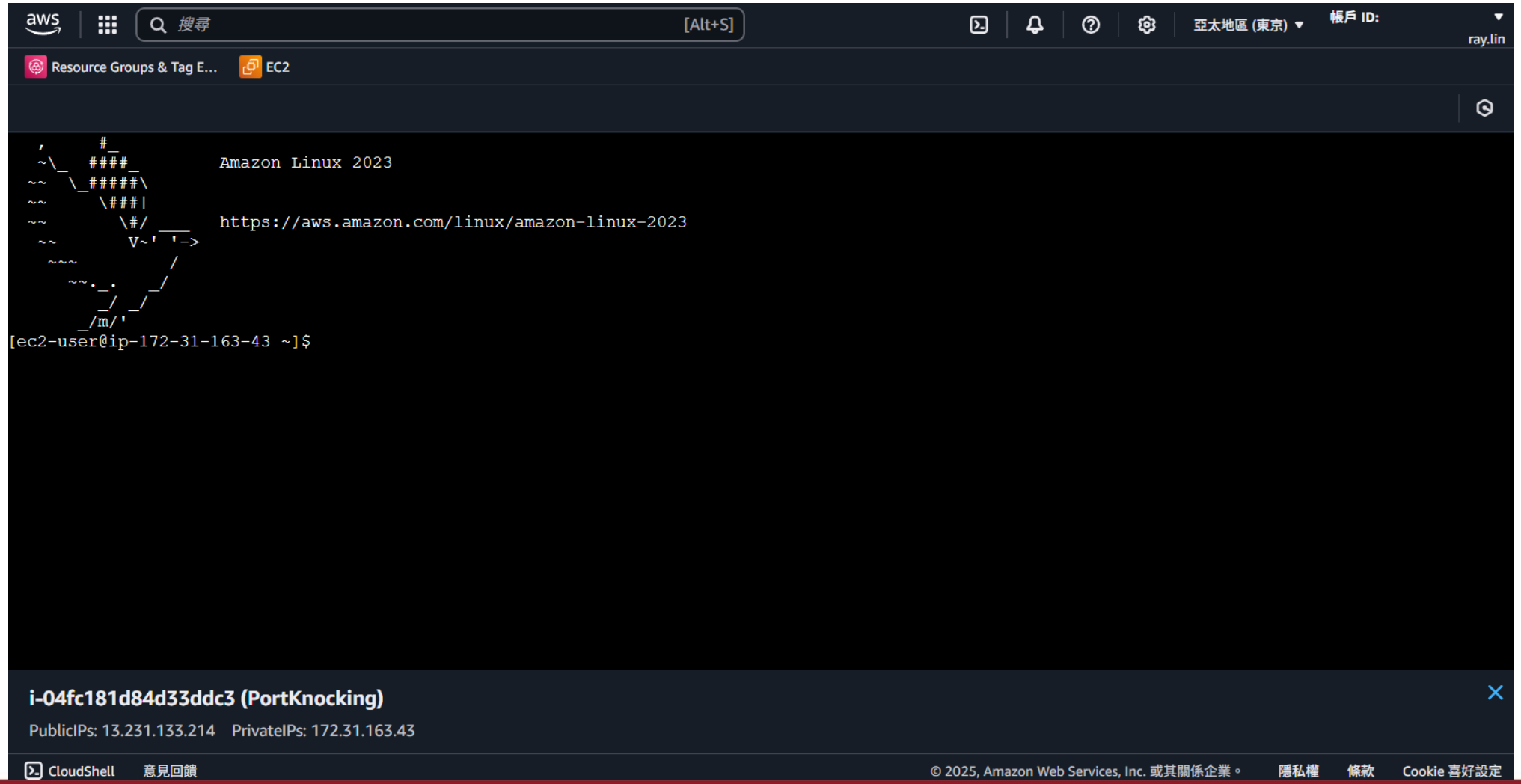


星爺曾經說過

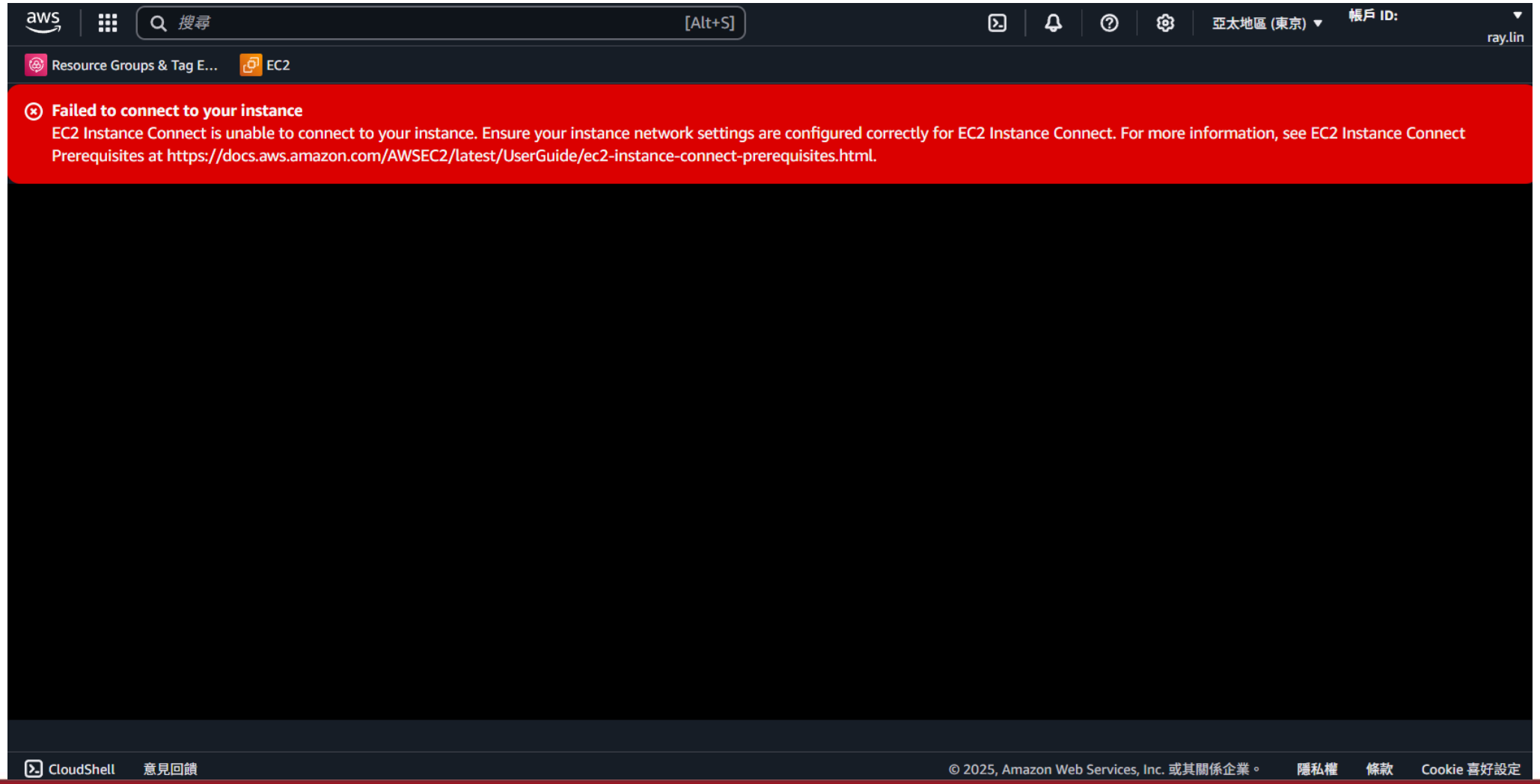
Port Knocking模擬

- 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

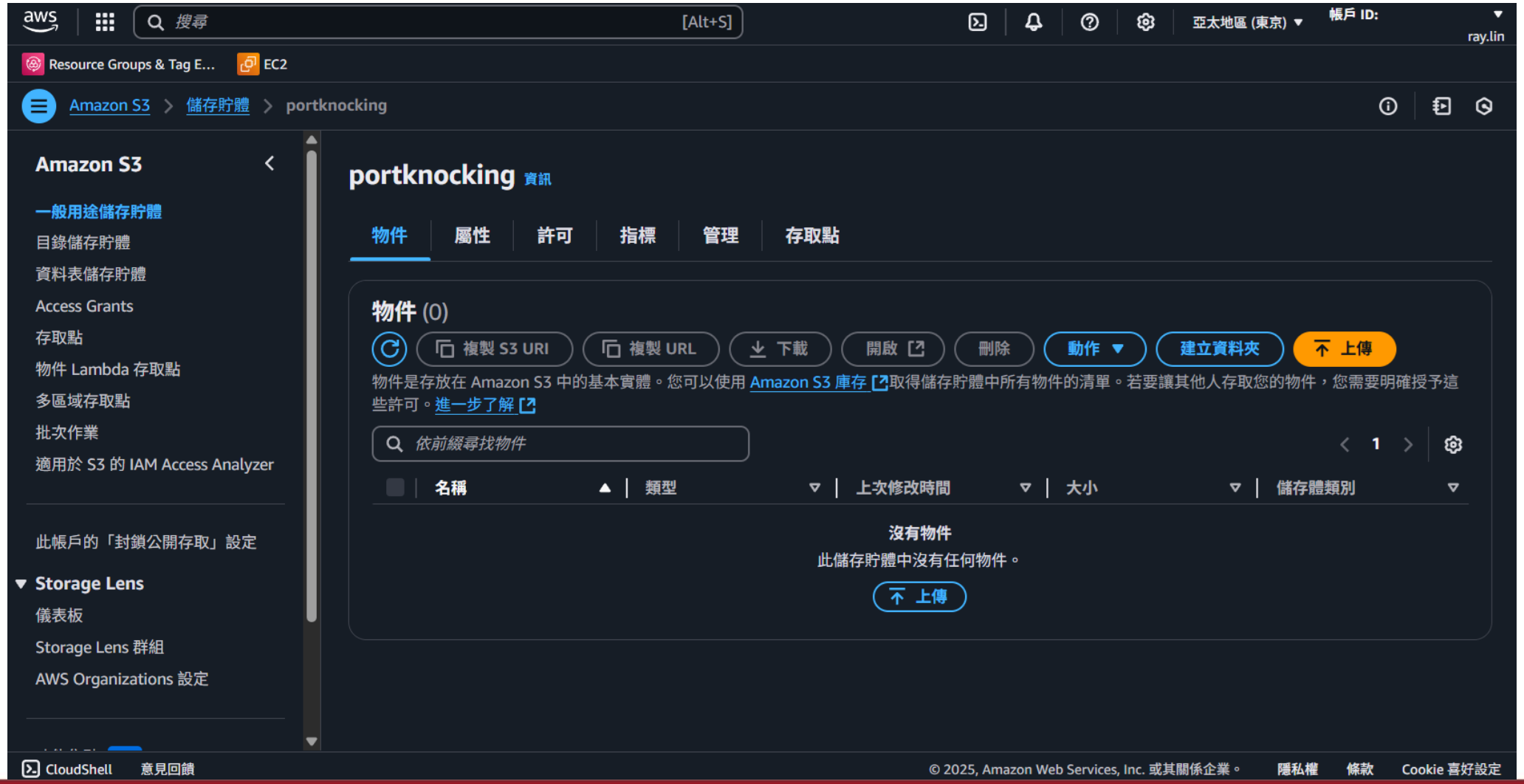
啟動AWS EC2，測試SSH是否正常連線



調整AWS SG，確認SSH無法連線

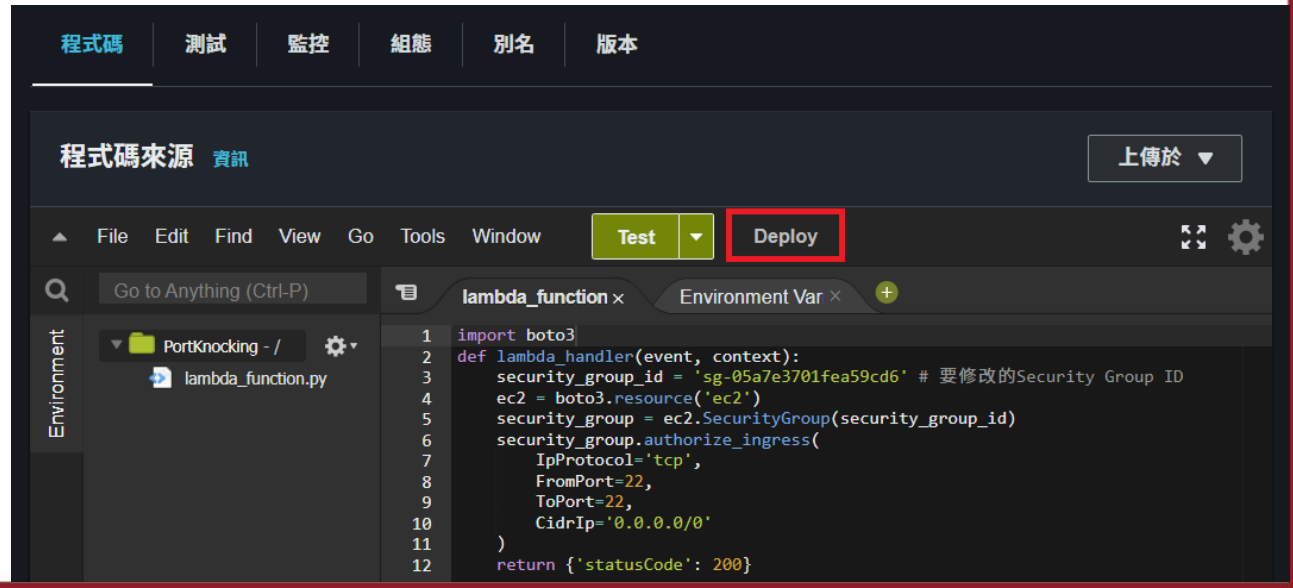


建立AWS S3 Bucket



在Lambda建立Python程式碼並Deploy

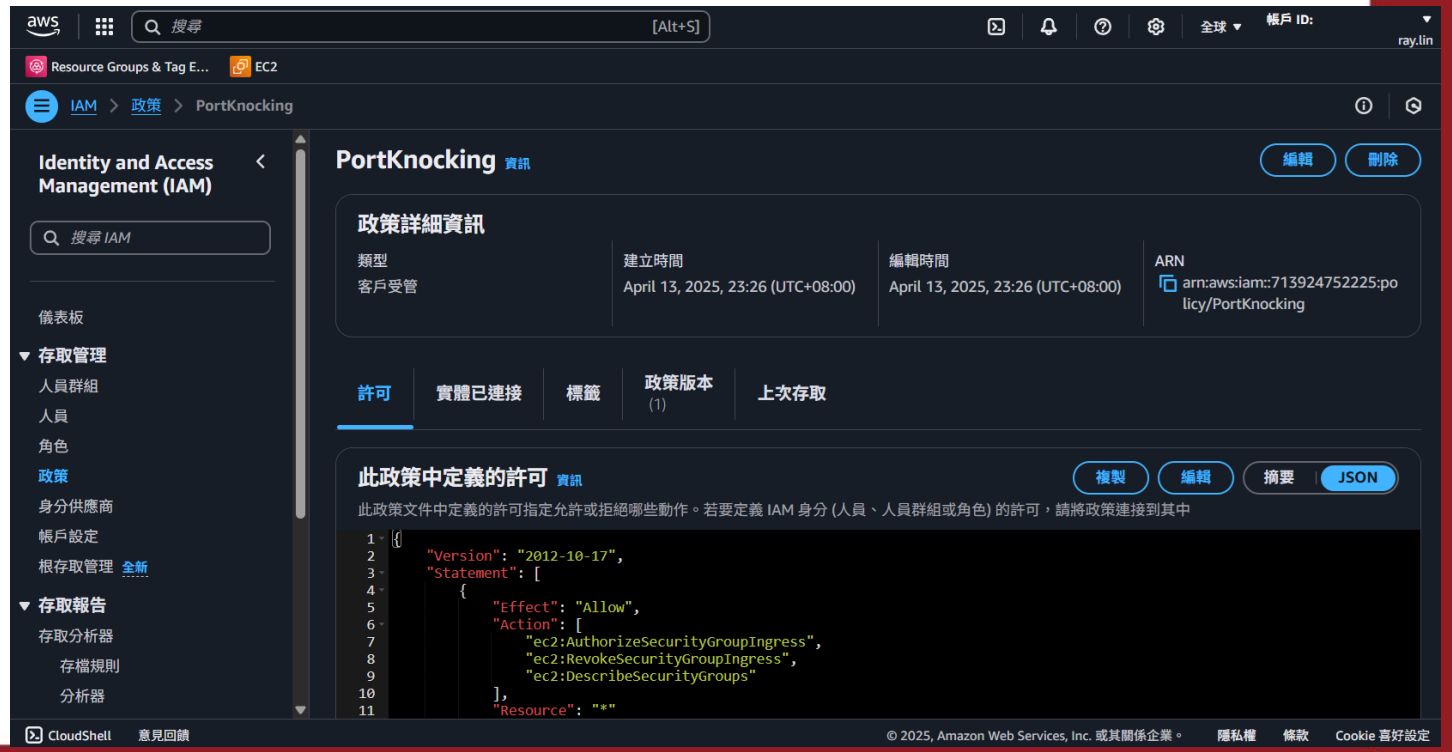
```
import boto3
def lambda_handler(event, context):
    security_group_id = 'sg-05a7e3701fea59cd6' # 要修改的Security Group ID
    ec2 = boto3.resource('ec2')
    security_group = ec2.SecurityGroup(security_group_id)
    security_group.authorize_ingress(
        IpProtocol='tcp',
        FromPort=22,
 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



新增S3"PUT"觸發條件

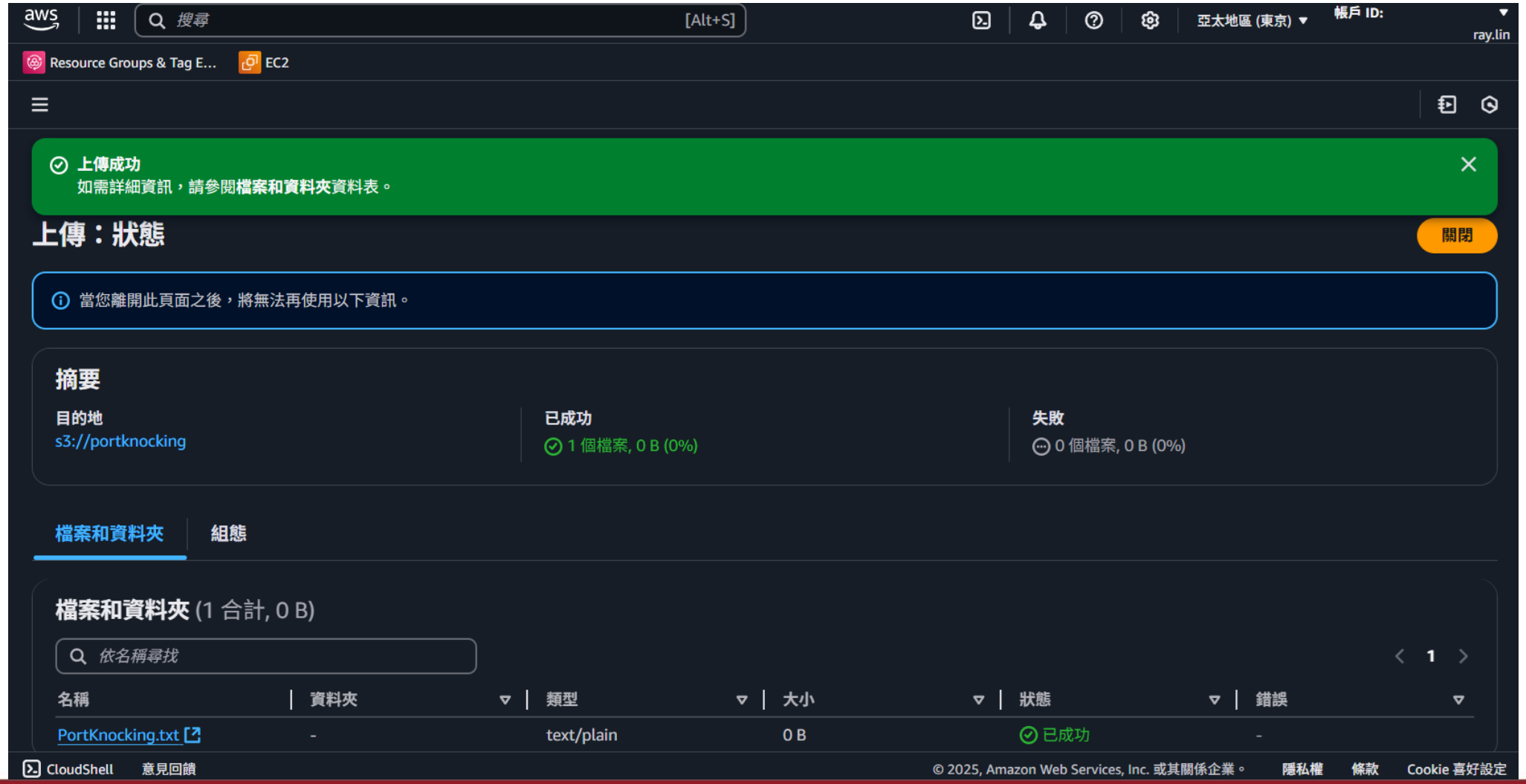
建立Lambda要使用的IAM Policy

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

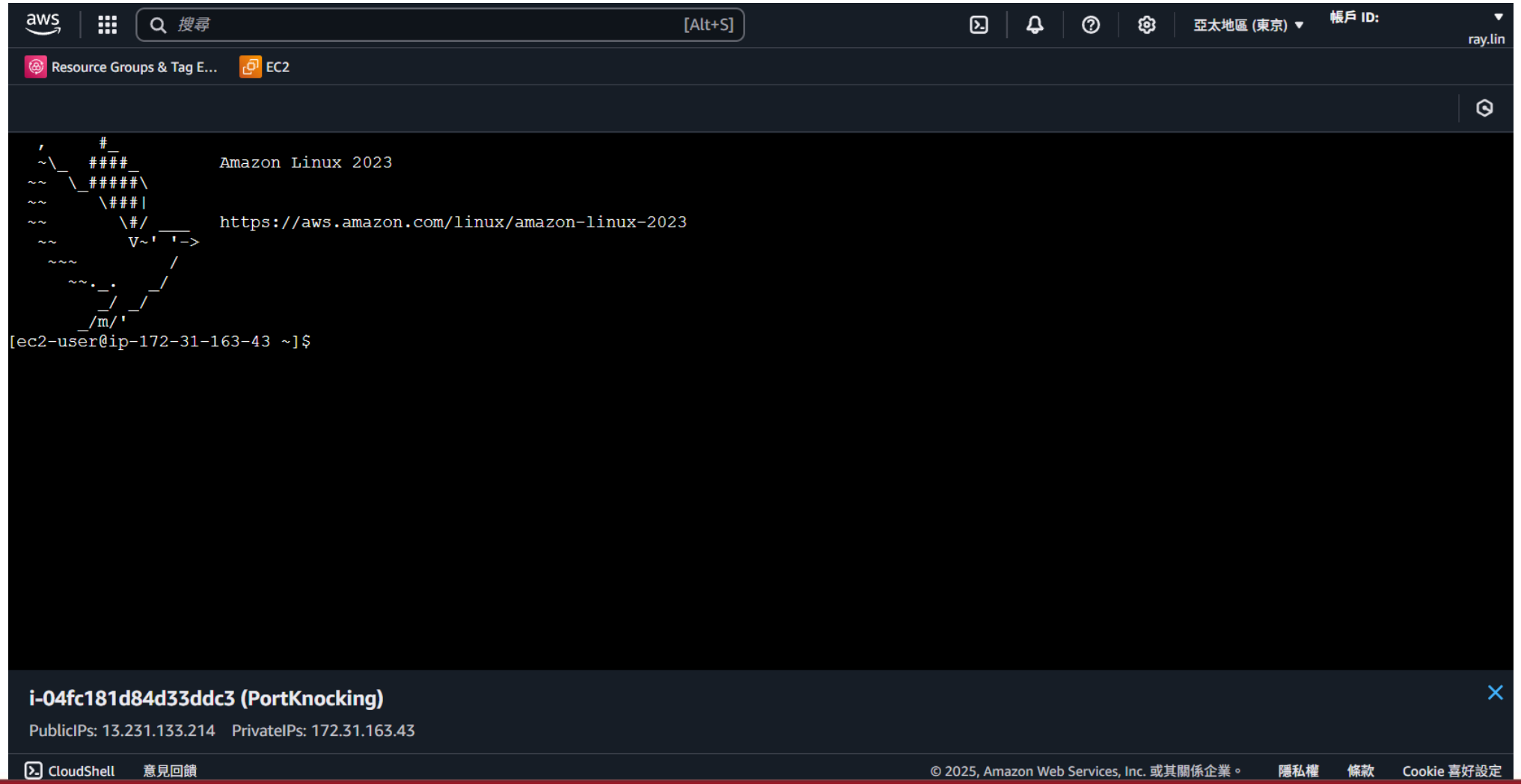


將IAM Policy新增到Lambda的角色

在S3上傳一個PortKnocking檔案

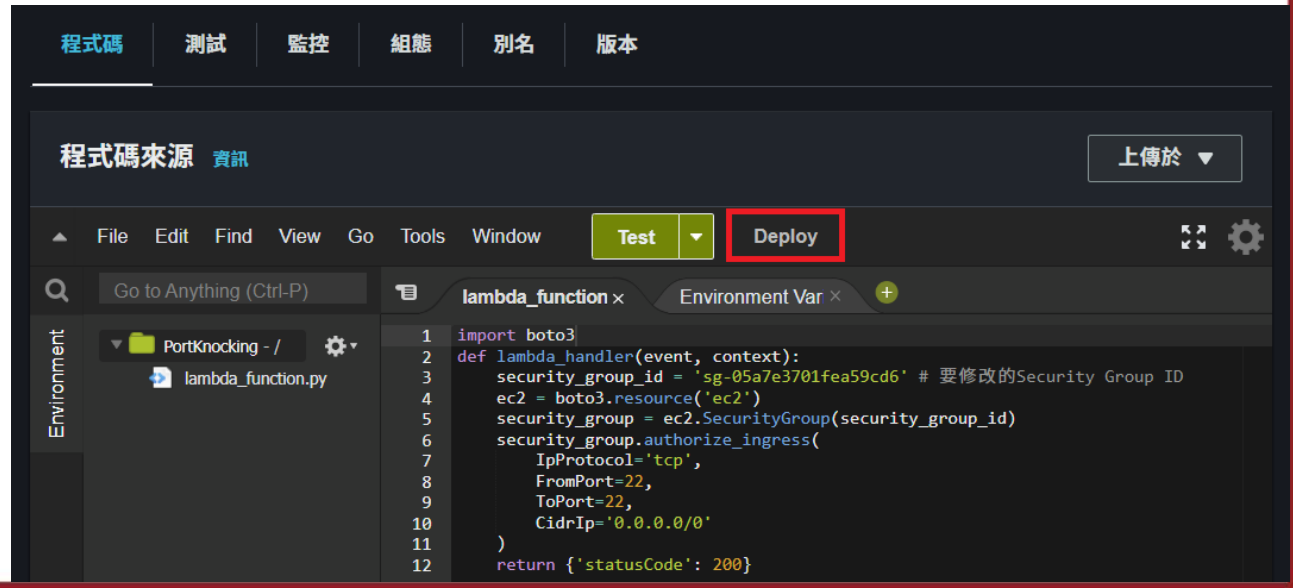


30-60秒左右，測試SSH是否正常連線

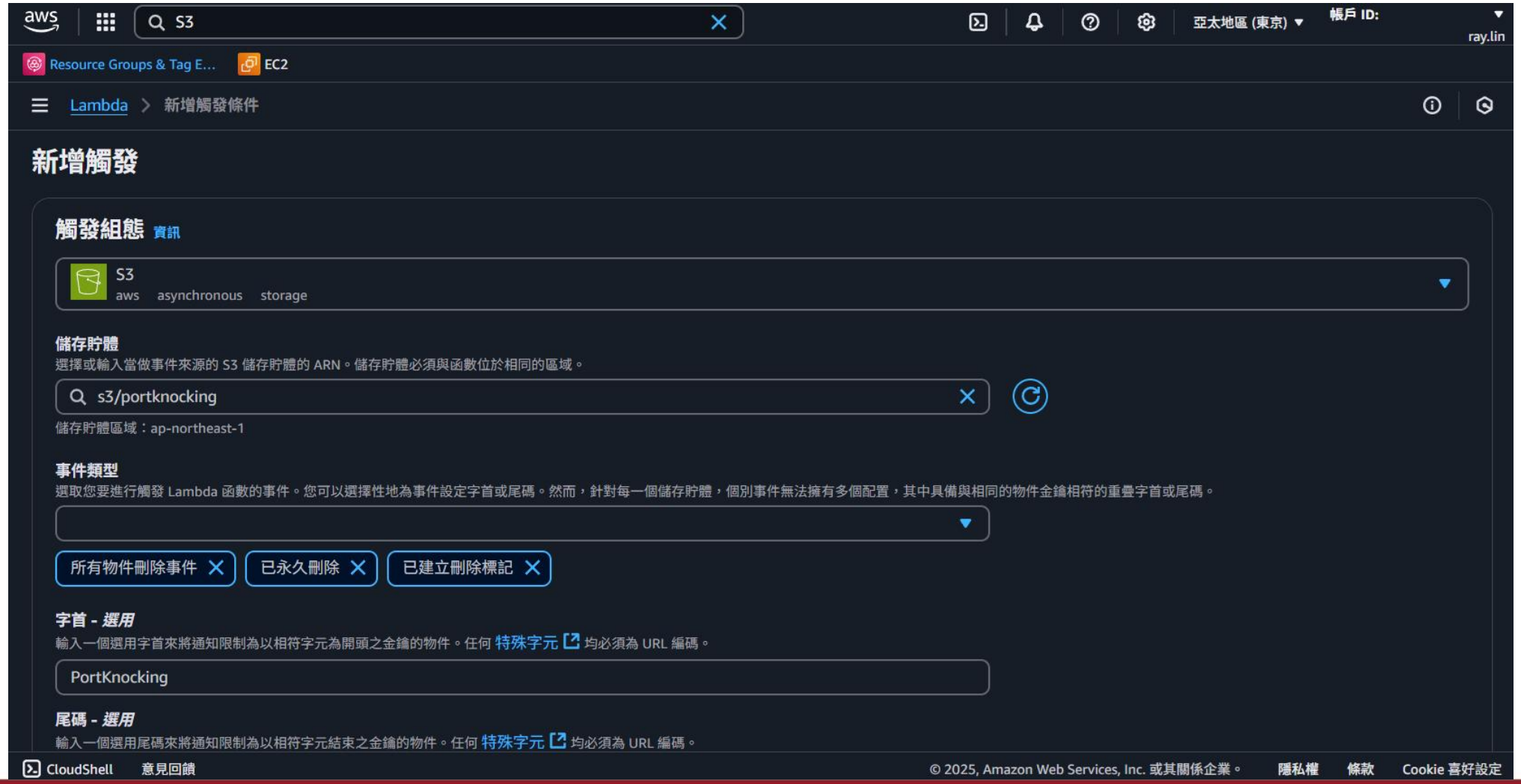


在Lambda建立Python程式碼並Deploy

```
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}
```

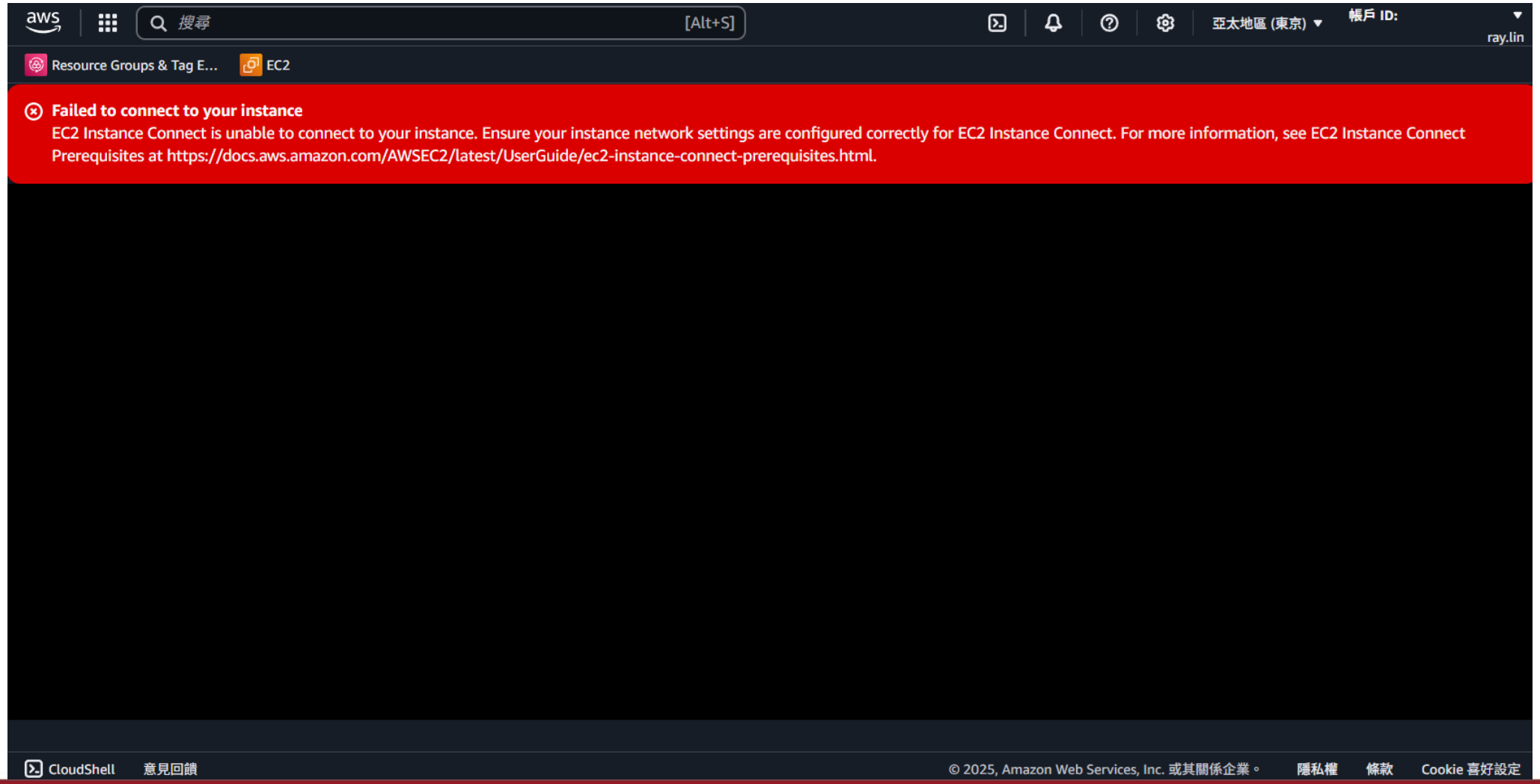


新增S3"所有物件刪除事件"觸發條件



在S3刪除PortKnocking檔案

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