Security & Identity

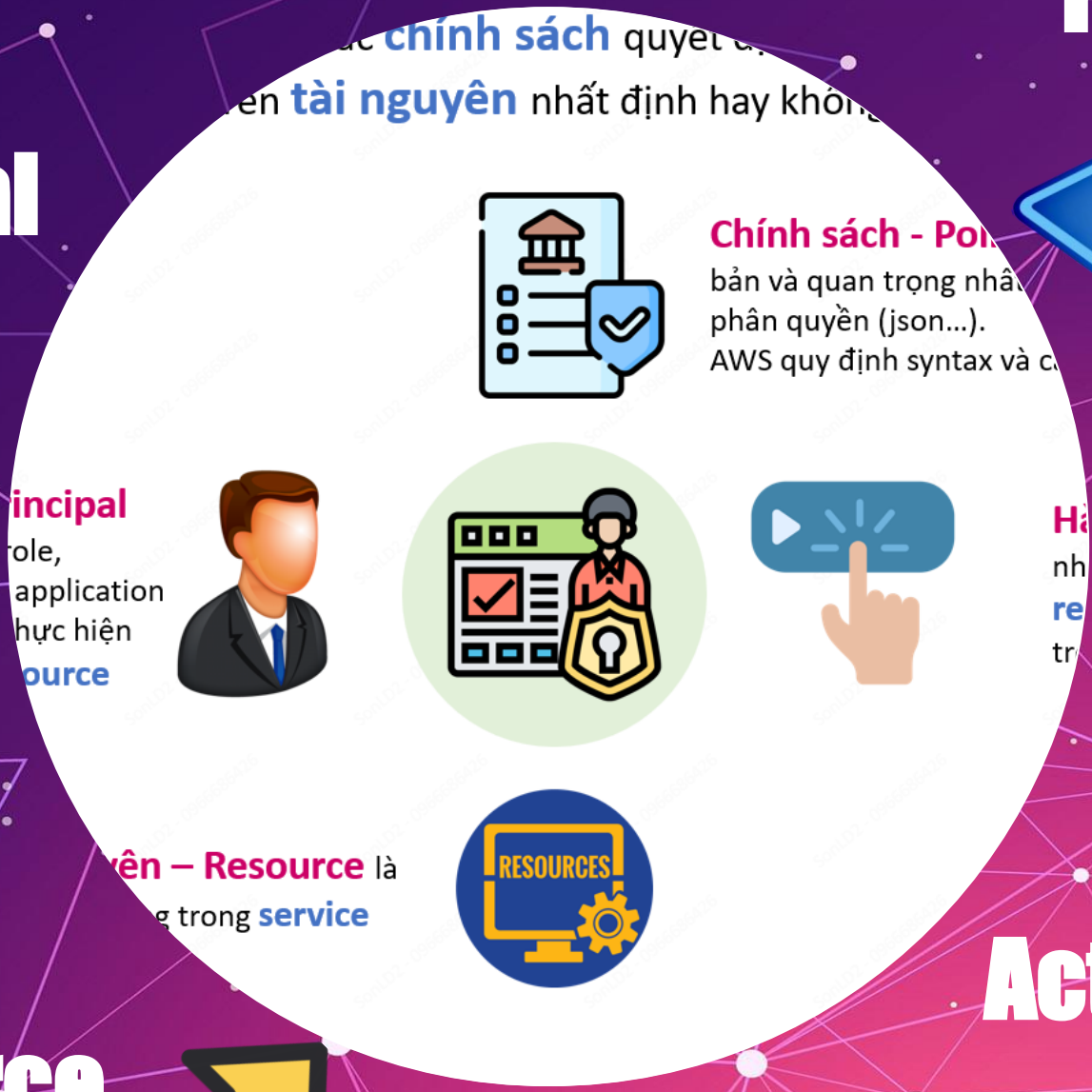
IAM Basic

Principal

Policy

Resource

Action



amazon web services™

Amazon Web Service - Training

PERMISSION GRANT

Phân quyền là tạo ra một tập hợp các **chính sách** quyết định việc một **chủ thể** được phép thực thi một hay nhiều **hành động** trên **tài nguyên** nhất định hay không

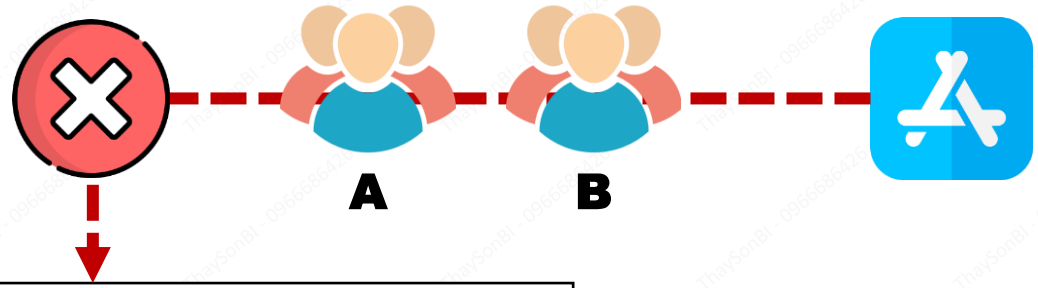
Chính sách - Policy là đơn vị cơ bản và quan trọng nhất trong quá tình phân quyền (json…).
AWS quy định syntax và cấu trúc cụ thể

Chủ thể - Principal
bao gồm user, role, federated user, application sẽ gửi yêu cầu thực hiện **action** trên **resource**

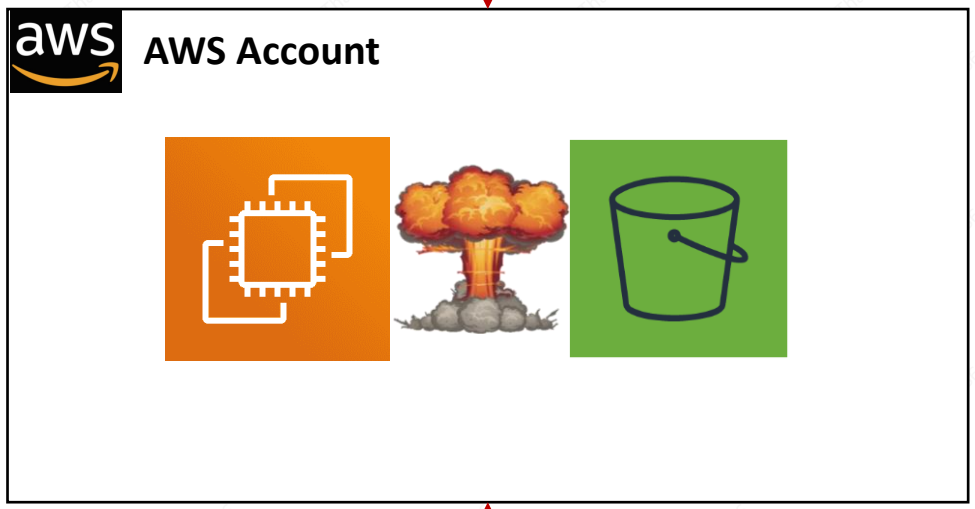
Hành động - Action là những hành động thực hiện trên **resource** được định nghĩa sẵn trong từng service

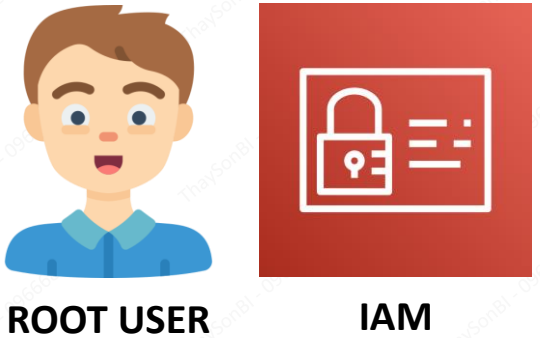
Tài nguyên – Resource là một đối tượng trong **service**

IAM

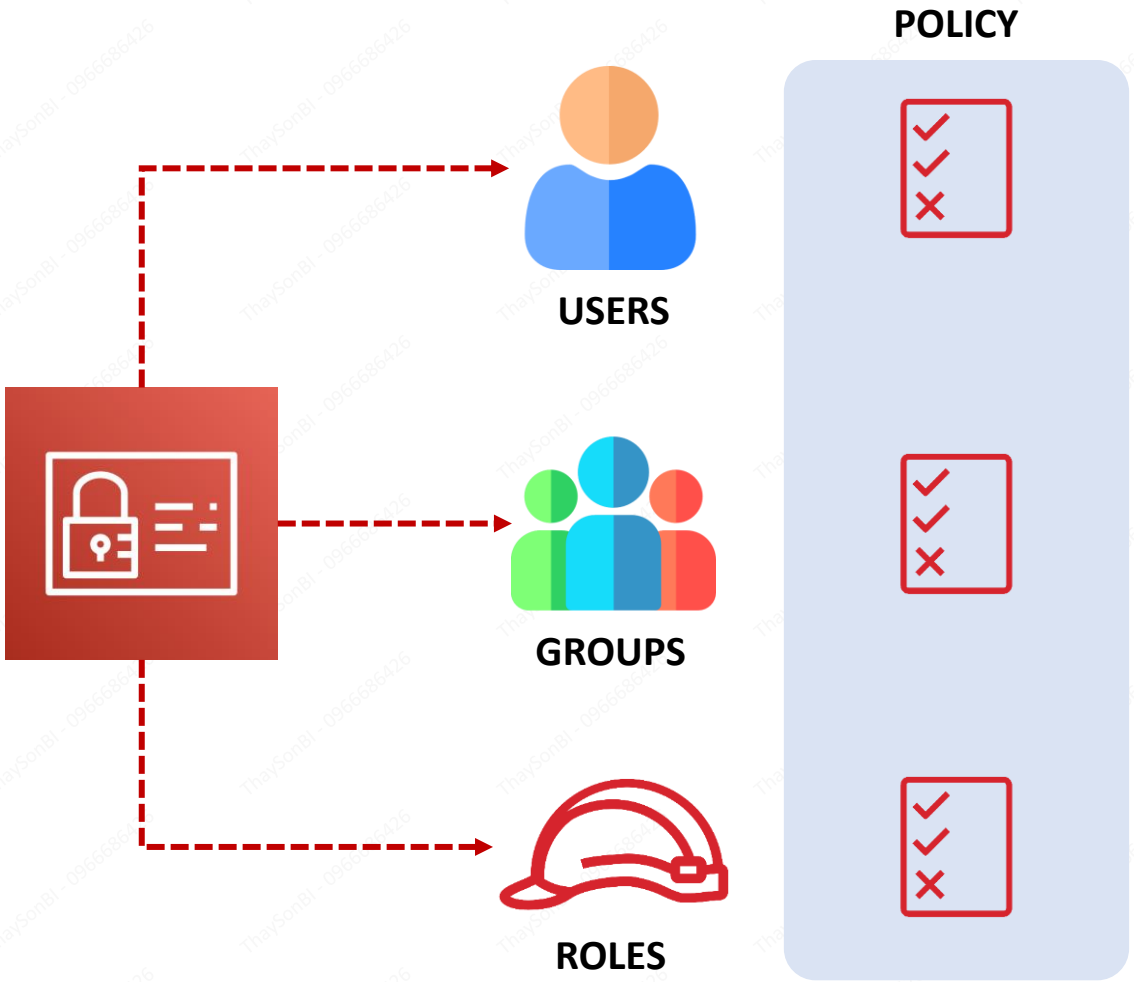


IAM có **toàn bộ** các quyền hạn trên Account AWS mà Root User có





IAM COMPONENT



Những định danh đại diện cho **ai đó** hoặc **ứng dụng** cần **truy cập** vào account của bạn

Đại diện cho **một nhóm** người dùng (**users**) mà **có chung** những đặc điểm nhất định (DEV team, HR, FINN, RISK…)

Những định danh có thể được dùng bởi **AWS Service** hoặc để gán cho các truy cập **từ bên ngoài** vào account của bạn

ALLOW hoặc **DENY** quyền truy cập vào các **dịch vụ AWS** hoặc tính năng của các dịch vụ đó

SUMMARY

KHÔNG mất phí

Là dịch vụ **Global** / **Global Resilience**

ALLOW hoặc **DENY** các đối tượng trên Account của nó

Không thể tác động lên **account khác**

Có thể kết hợp **Identity federation** và **MFA**

Statement

Security & Identity

IAM Policies

Deny

Allow

Merge

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "FirstStatement",
      "Effect": "Allow",
      "Action": ["iam:ChangePassword"],
      "Resource": "*"
    },
    {
      "Sid": "SecondStatement",
      "Effect": "Allow",
      "Action": "s3:ListAllMyBuckets",
      "Resource": "*"
    },
    {
      "Sid": "ThirdStatement",
      "Effect": "Allow",
      "Action": [
        "s3:List*",
        "s3:Get*"
      ],
      "Resource": [
        "arn:aws:s3:::confidential-data",
        "arn:aws:s3:::confidential-data/*"
      ],
      "Condition": {"Bool": {"aws:MultiFactorAuth
```

amazon web services™

Amazon Web Service - Training

POLICY DOCUMENT

Sid: Mã hoặc cụm từ mô tả statement này dùng để làm gì

Statement + 1 + 2

Condition: Tùy chọn giúp kiểm soát khi nào chính sách có hiệu lực

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "FirstStatement",
      "Effect": "Allow",
      "Action": ["iam:ChangePassword"],
      "Resource": "*"
    },
    {
      "Sid": "SecondStatement",
      "Effect": "Allow",
      "Action": "s3:ListAllMyBuckets",
      "Resource": "*"
    },
    {
      "Sid": "ThirdStatement",
      "Effect": "Allow",
      "Action": [
        "s3:List*",
        "s3:Get*"
      ],
      "Resource": [
        "arn:aws:s3:::confidential-data",
        "arn:aws:s3:::confidential-data/*"
      ],
      "Condition": {"Bool": {"aws:MultiFactorAuthPresent": "true"}}
    }
  ]
}
```

Effect: Thực hiện (Allow) hoặc loại trừ (Deny) những gì

Action/NotAction: Thực hiện hoặc không được thực hiện hành động cụ thể nào

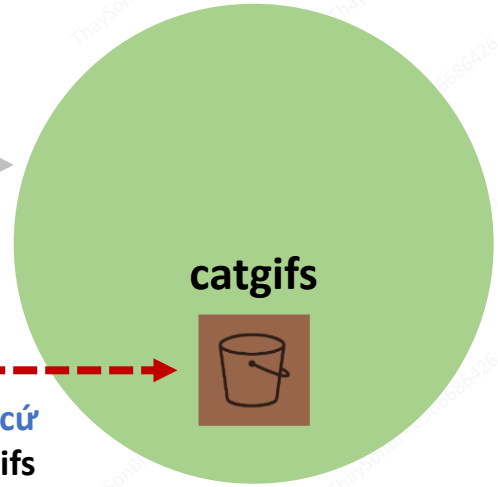
Resource: Tác động lên những đối tượng nào

POLICY ORDER

Action: s3:* và Resource: *

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "FullAccess",
            "Effect": "Allow",
            "Action": ["s3:*"],
            "Resource": ["*"]
        },
        {
            "Sid": "DenyCatBucket",
            "Action": ["s3:*"],
            "Effect": "Deny",
            "Resource": ["arn:aws:s3:::catgifs", "arn:aws:s3:::catgifs/*" ]
        }
    ]
}
```

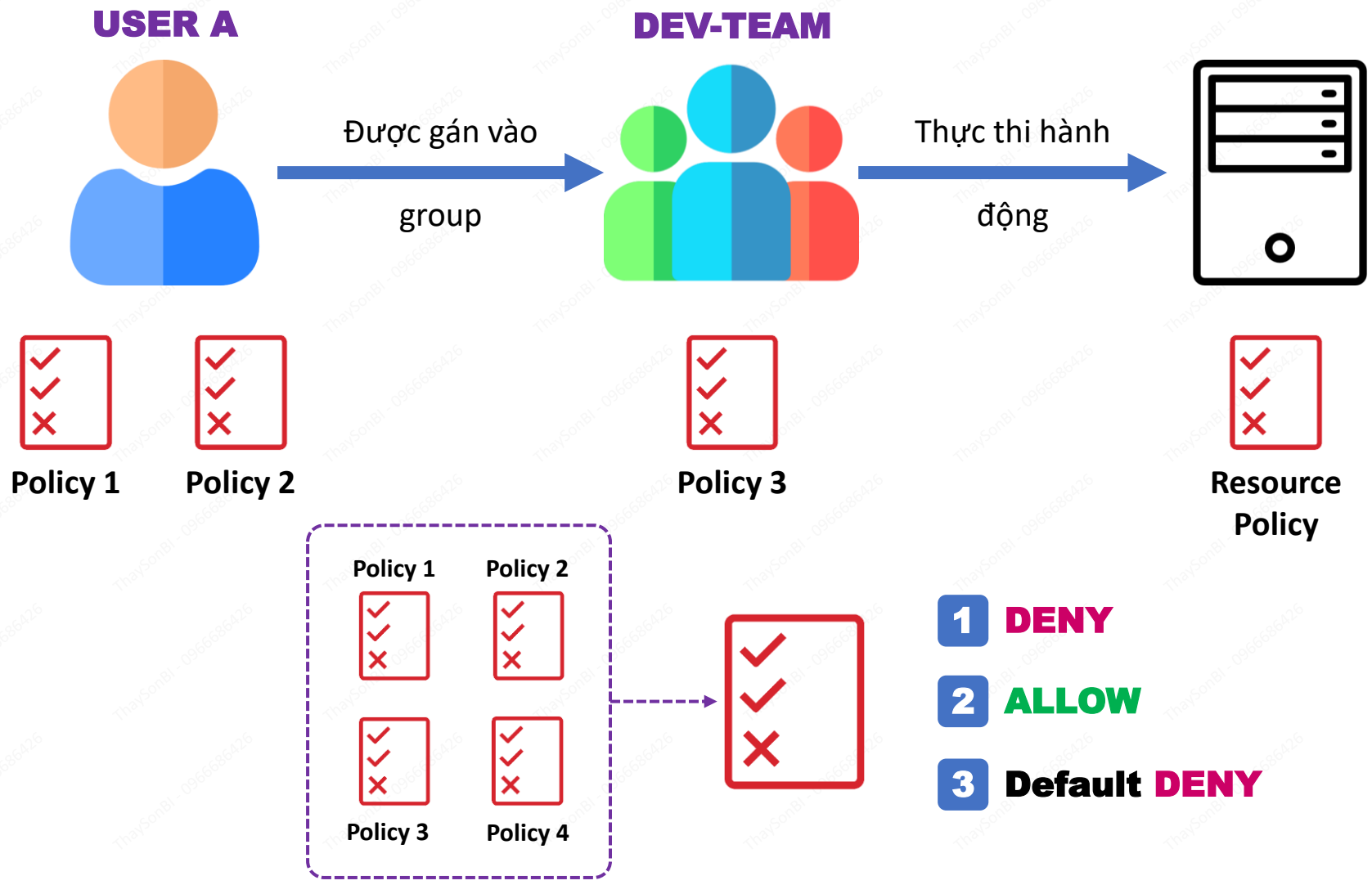
Được phép thực hiện **bất cứ thao tác S3 nào** trên mọi bucket



Không được phép thực hiện **bất cứ thao tác S3 nào** trên bucket **Catgifs**

1. **DENY**
2. **ALLOW**
3. **Default DENY**

MERGE


USER A
DEV-TEAM
Được gán vào
group
Thực thi hành
động
Policy 1
Policy 2
Policy 3
Resource Policy
Policy 1
Policy 2
Policy 3
Policy 4
1 DENY
2 ALLOW
3 Default DENY

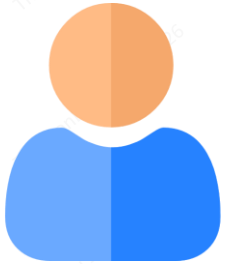
POLICY TYPES

AWS mặc định và không thể xóa ← AWS Managed

Customer Managed → **Thêm/Sửa/Xóa** do người dùng

Có thể **được dùng lại**

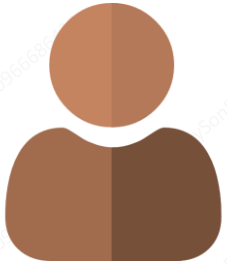
Managed Policy

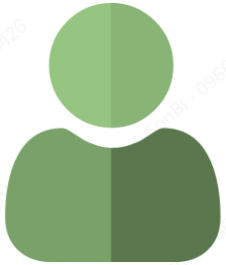


Inline Policy

Giảm sự phức tạp trong việc quản lý

Inline Policy





Inline Policy

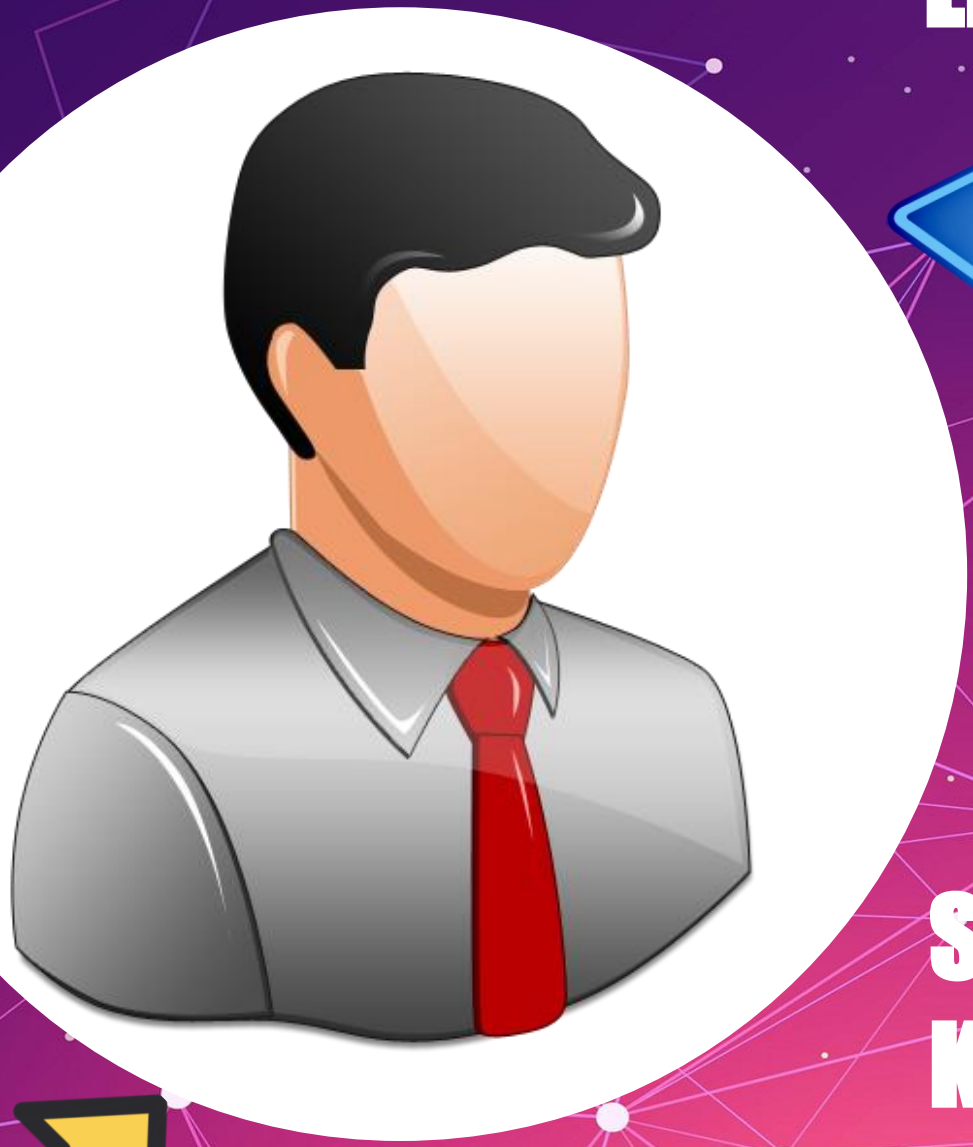
Dùng trong trường hợp **ngoại lệ** hoặc **đặc biệt**

Security & Identity

IAM Users

Principal

Limited



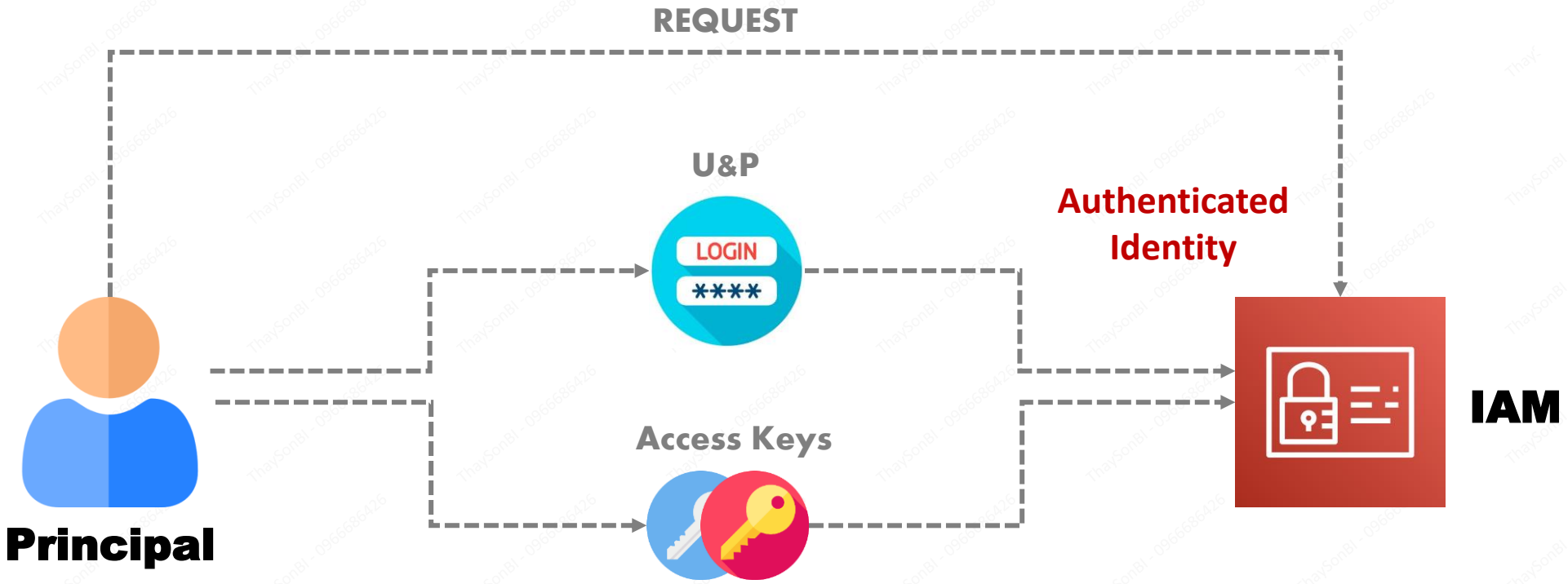
Secret Key

Access Key

amazon web services™

Amazon Web Service - Training

IAM - USERS



IAM Users là những **định danh** được sử dụng cho bất cứ **yêu cầu long-term** nào truy cập **vào AWS**.

Ví dụ: Con người, ứng dụng, tài khoản dịch vụ

AMAZON RESOURCE NAME

ARN được sử dụng để **định danh** cho các **tài nguyên** trong môi trường **AWS**.
Cung cấp quyền **truy cập, xác thực và sử dụng** cho các tài khoản

arn : partition : service : region : account-id : resource-id

```
arn:partition:service:region:account-id:resource-id
arn:partition:service:region:account-id:resource-type/resource-id
arn:partition:service:region:account-id:resource-type:resource-id
```

Bucket

```
arn:aws:s3:::catgifs
arn:aws:s3:::catgifs/*
```

Các đối tượng trong Bucket

USER CHARACTERISTICS

5000 IAM Users cho mỗi 1 Account AWS

IAM User có thể nằm trong **10 groups khác nhau**

Đó có thể là một **xung đột** trong thiết kế

Tăng trưởng theo **ứng dụng** (mỗi apps có user riêng)

IAM Roles và **Identity Federatiom**
…có thể giải quyết vấn đề

Merge Policy

Many User

Security & Identity

IAM Groups

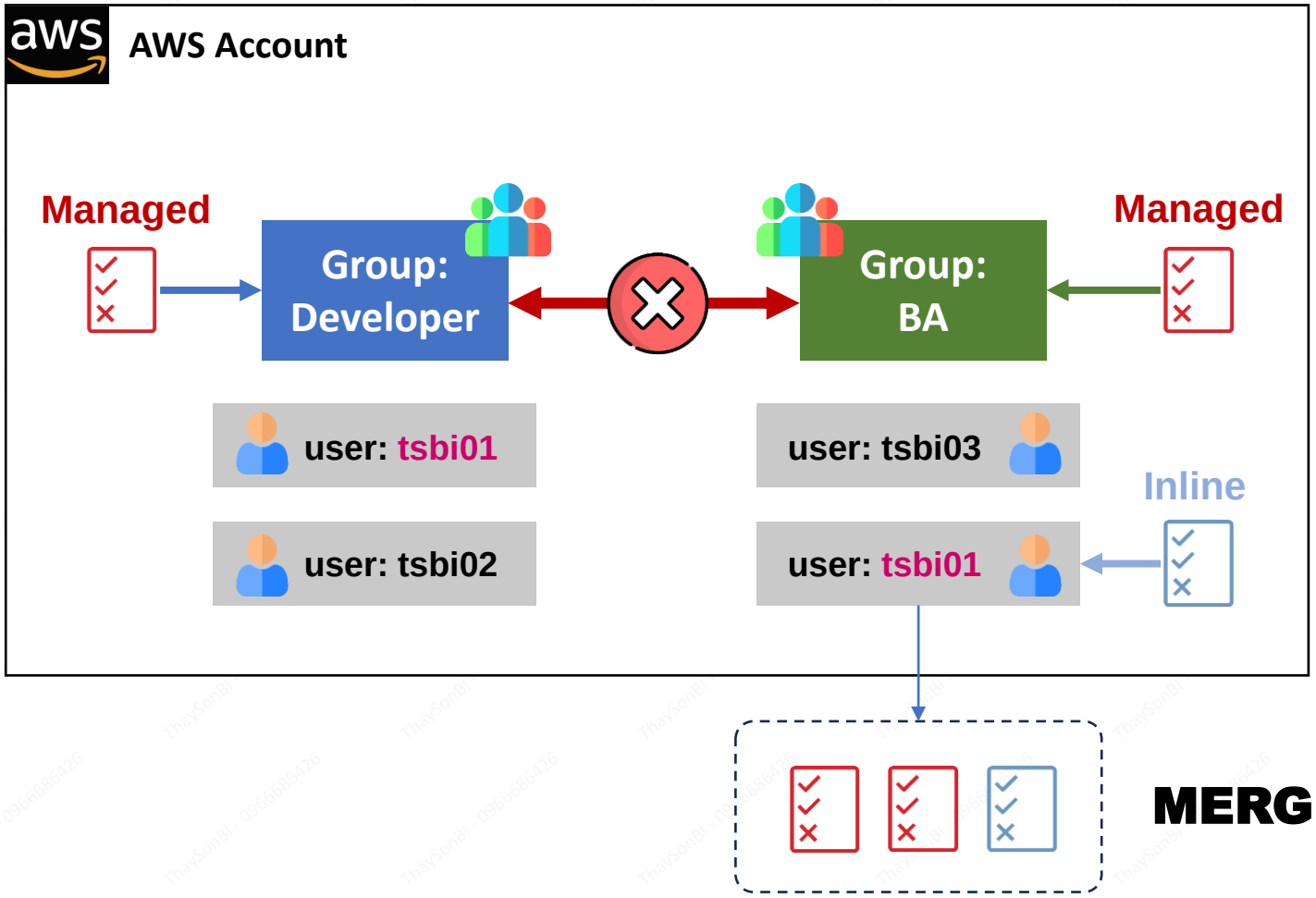
300 Groups

amazon web services™

Amazon Web Service - Training

IAM - GROUPS

IAM Group chứa các IAM User



- Inline
- Managed
- **Not** Principle
- Group **N-N** User
- Have **no** default
- **300** Groups

Step by Step

Easily

Hands On

Create IAM User & Group

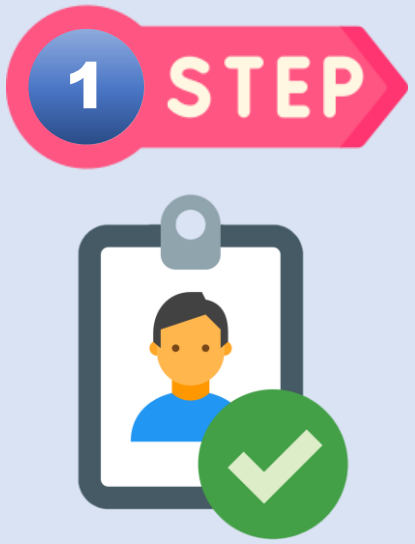
Practice

Funy

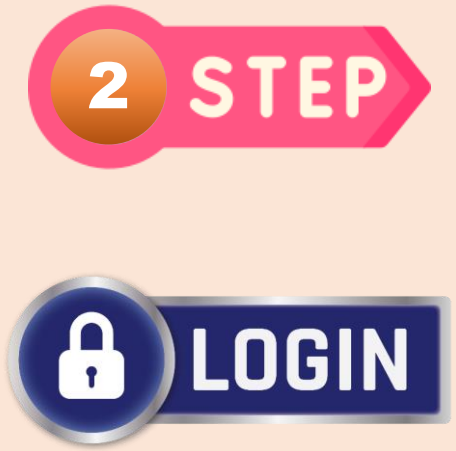
amazon web services™

Amazon Web Service - Training

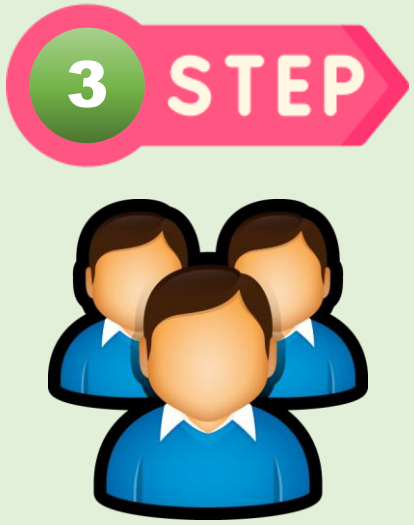
MAIN STEPS



Create IAM **User** and attach **Policy**



Test **Login** to new **User**



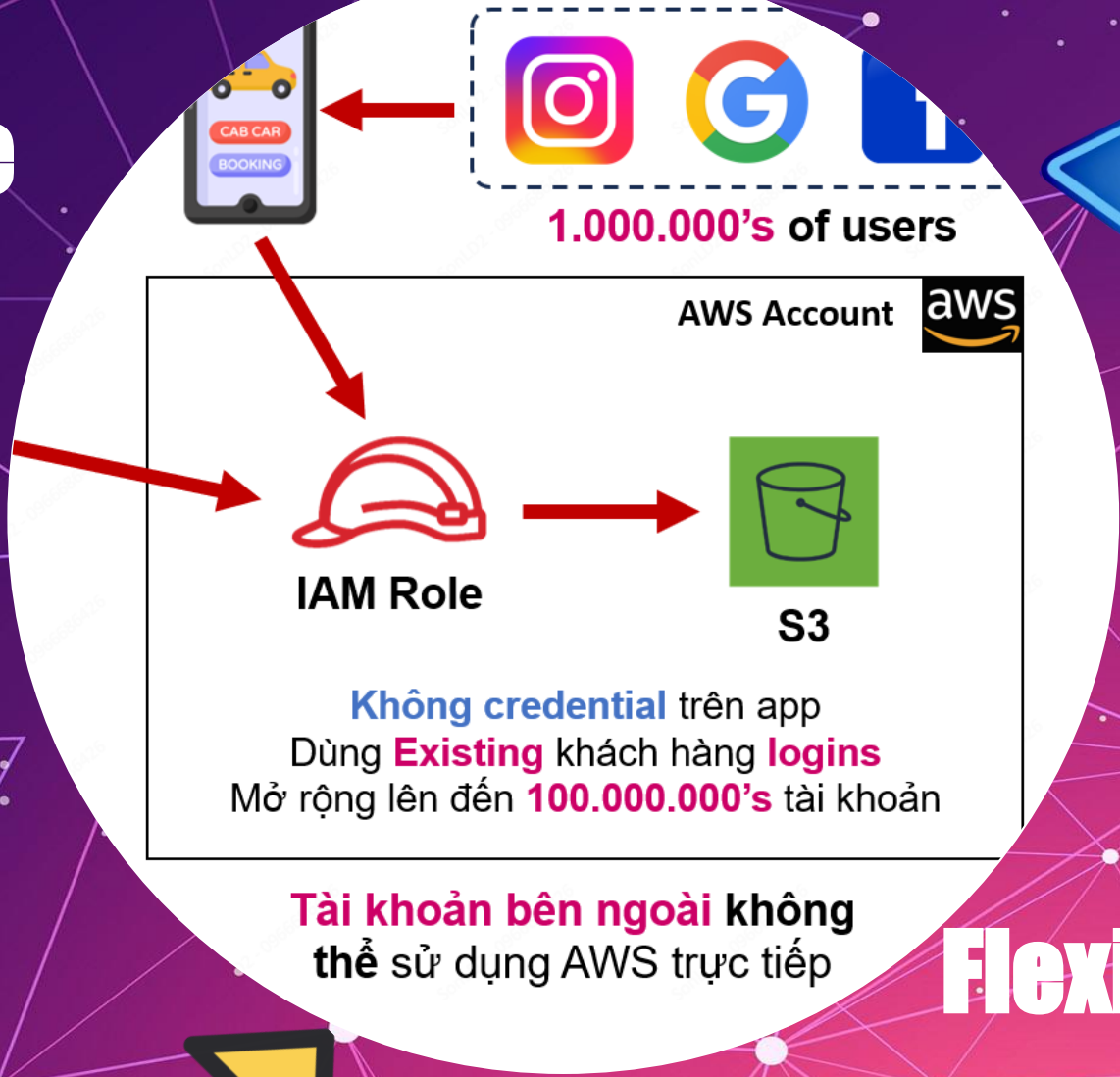
Create **IAM Group** and add user to this group

Temporary

Assume

Security & Identity

IAM Roles



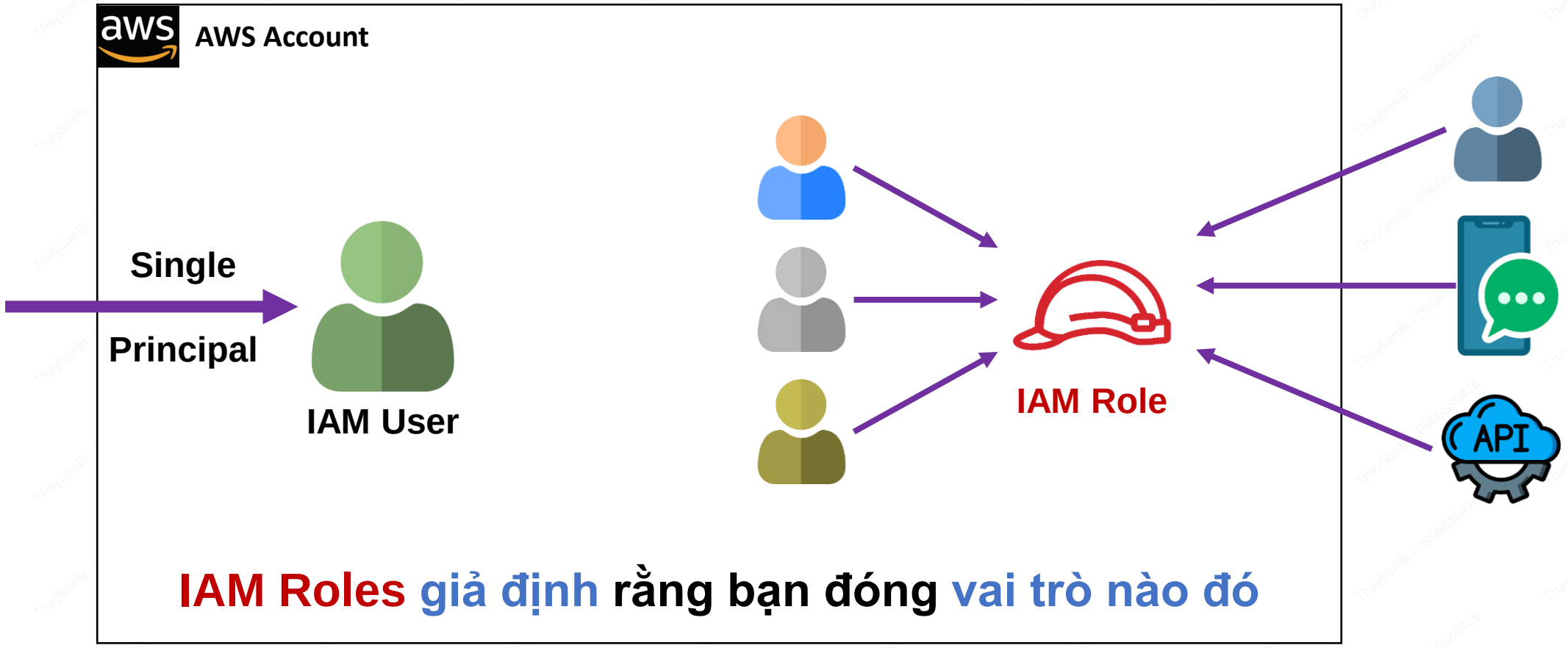
Flexibility

User

amazon web services™

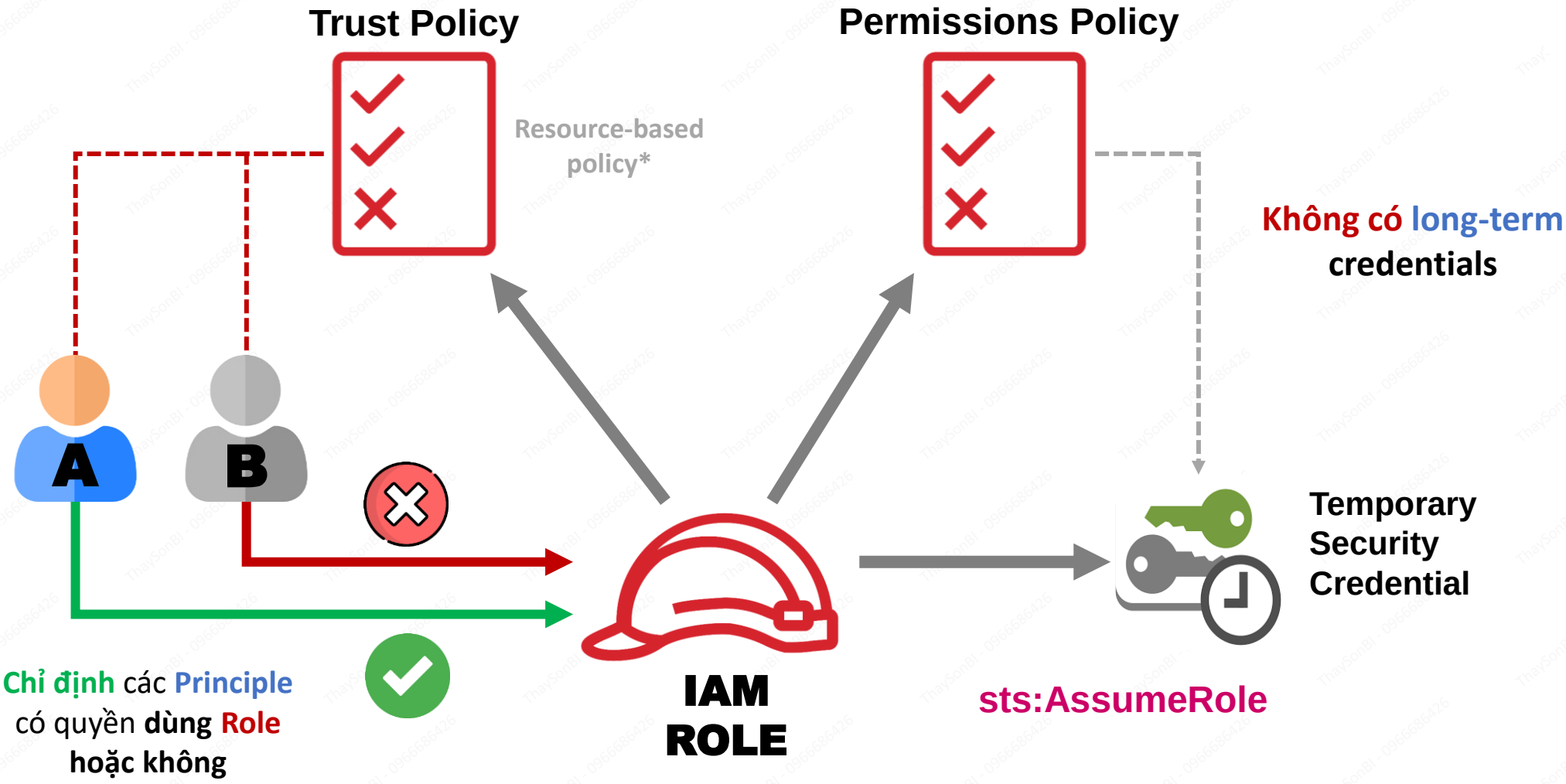
Amazon Web Service - Training

IAM - ROLES



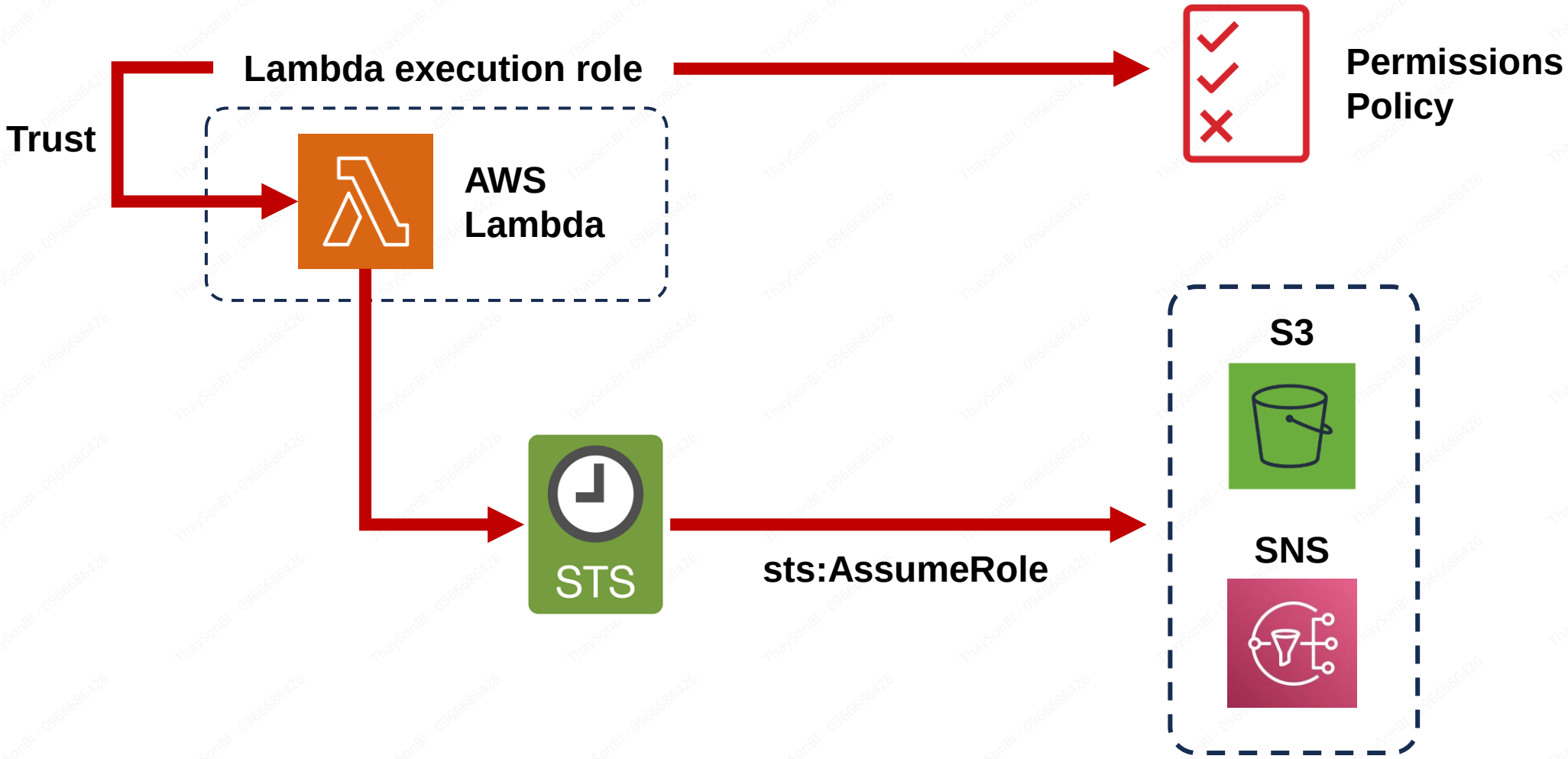
IAM Roles giả định rằng bạn đóng vai trò nào đó

IAM - ROLES

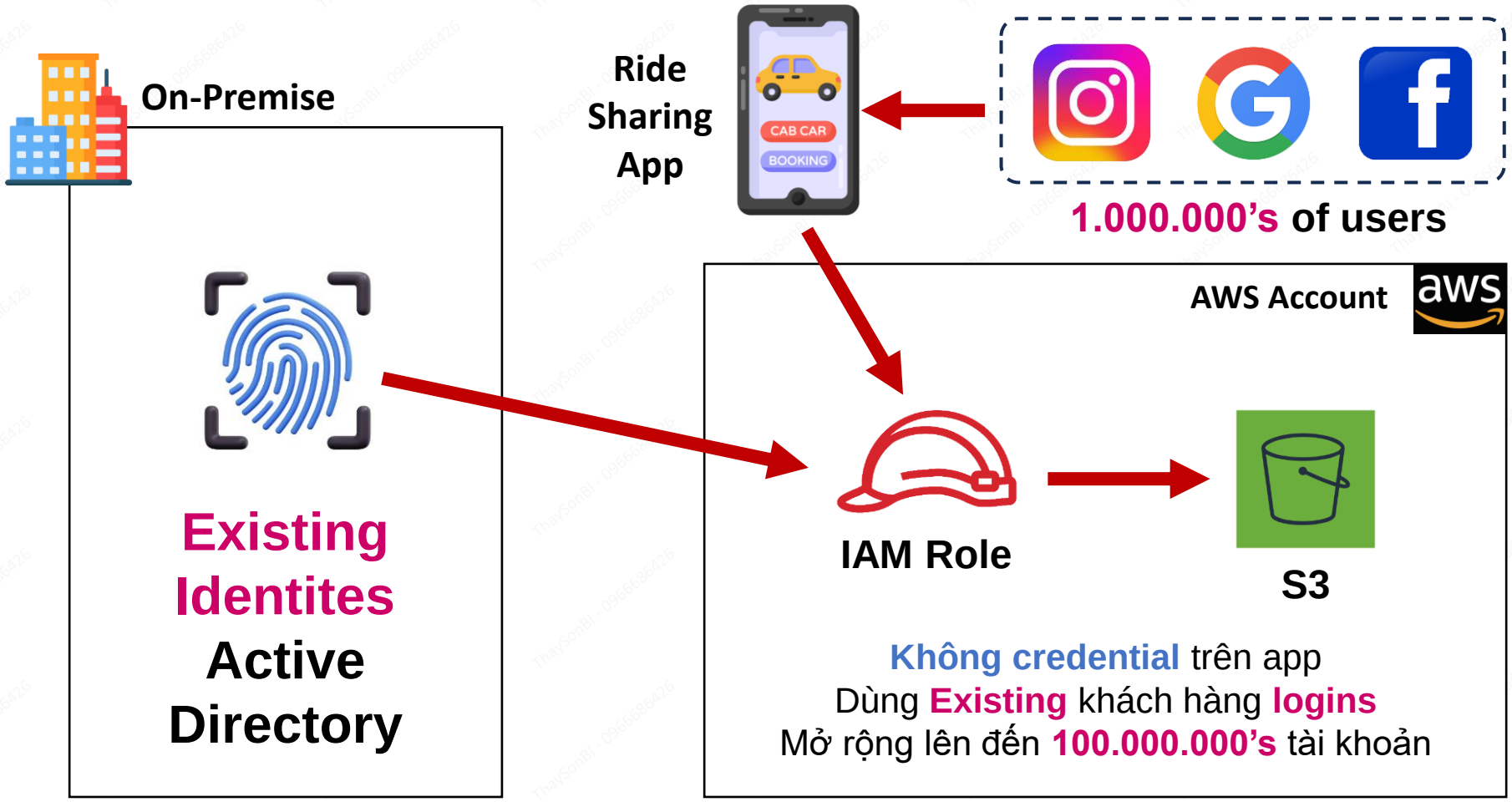


Resource-based policy*: Là 1 inline policy gắn với 1 resource. Cho phép principle ngoài account sử dụng tài nguyên trong account

IAM - ROLES


Lambda execution role
Trust
AWS
Lambda
Permissions
Policy
STS
sts:AssumeRole
S3
SNS

IAM - ROLES



Single Sign-On hoặc **>5000** đối tượng **cần định danh**

Tài khoản bên ngoài không thể sử dụng AWS trực tiếp

Step by Step

Easily

Hands On

Install CLI Windows

Practice

Funy

amazon web services™

Amazon Web Service - Training

MAIN STEPS

Install **CLI** in AWS Website

Open and configure **CLI** in your Windows

Test configure **success** and connect to AWS

Step by Step

Easily

Hands On

Install CLI Linux

Practice

Funy

amazon web services™

Amazon Web Service - Training

MAIN STEPS

Create EC2 instance with Linux

Using script to download & run CLI

Test configure success and delete instance

Step by Step

Easily

Hands On

Access Key for CLI

Practice

Funy

amazon web services™

Amazon Web Service - Training

MAIN STEPS

AWS
Command Line Interface

1 STEP

Login AWS account and IAM console

2 STEP

Create a new IAM user

3 STEP

Generate access key from new IAM user

4 STEP

Using command line to access AWS using access & secret key