IAM Organization

CodeStar Academy

Nội dung chính

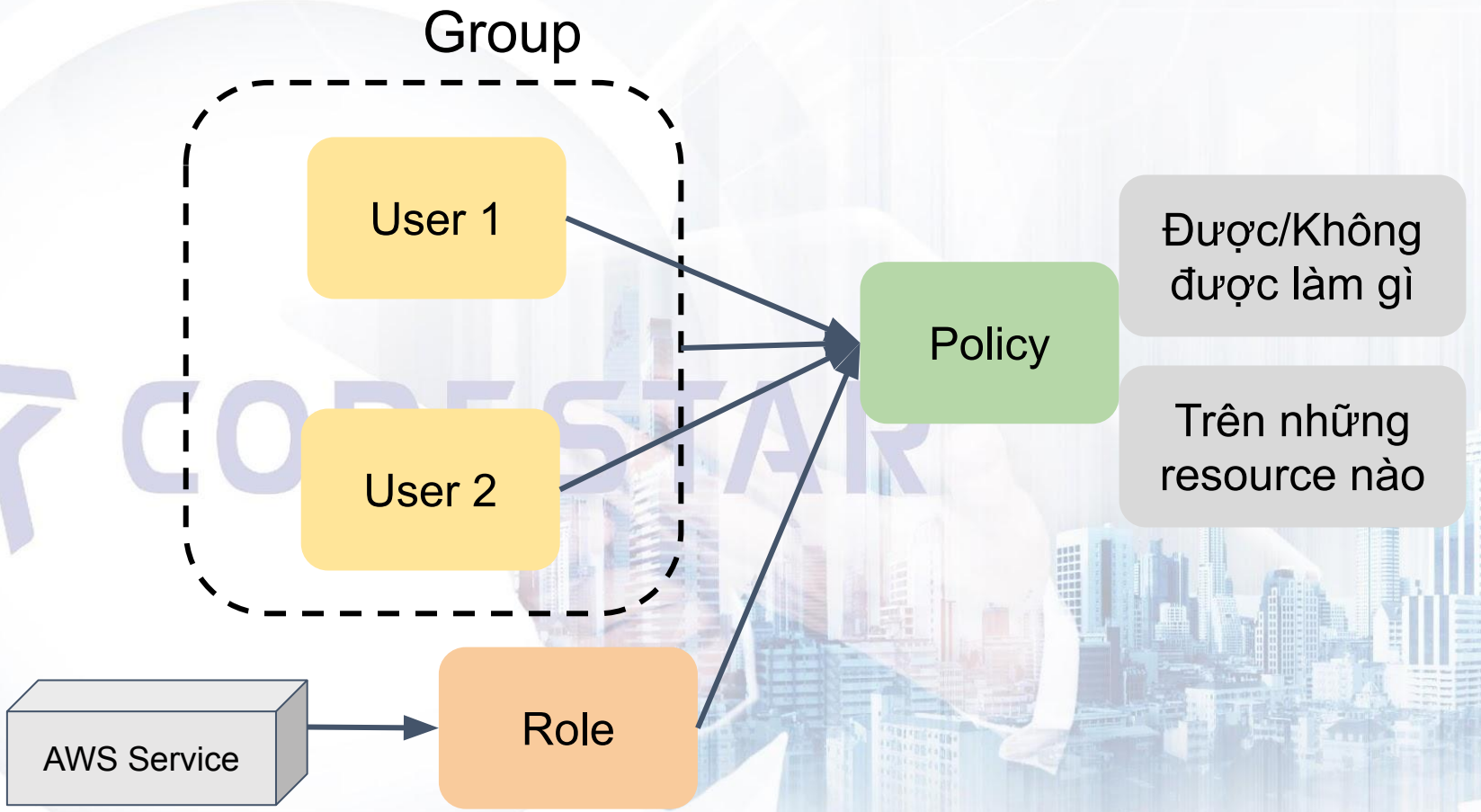
IAM

Organization

IAM

Các khái niệm trong IAM:

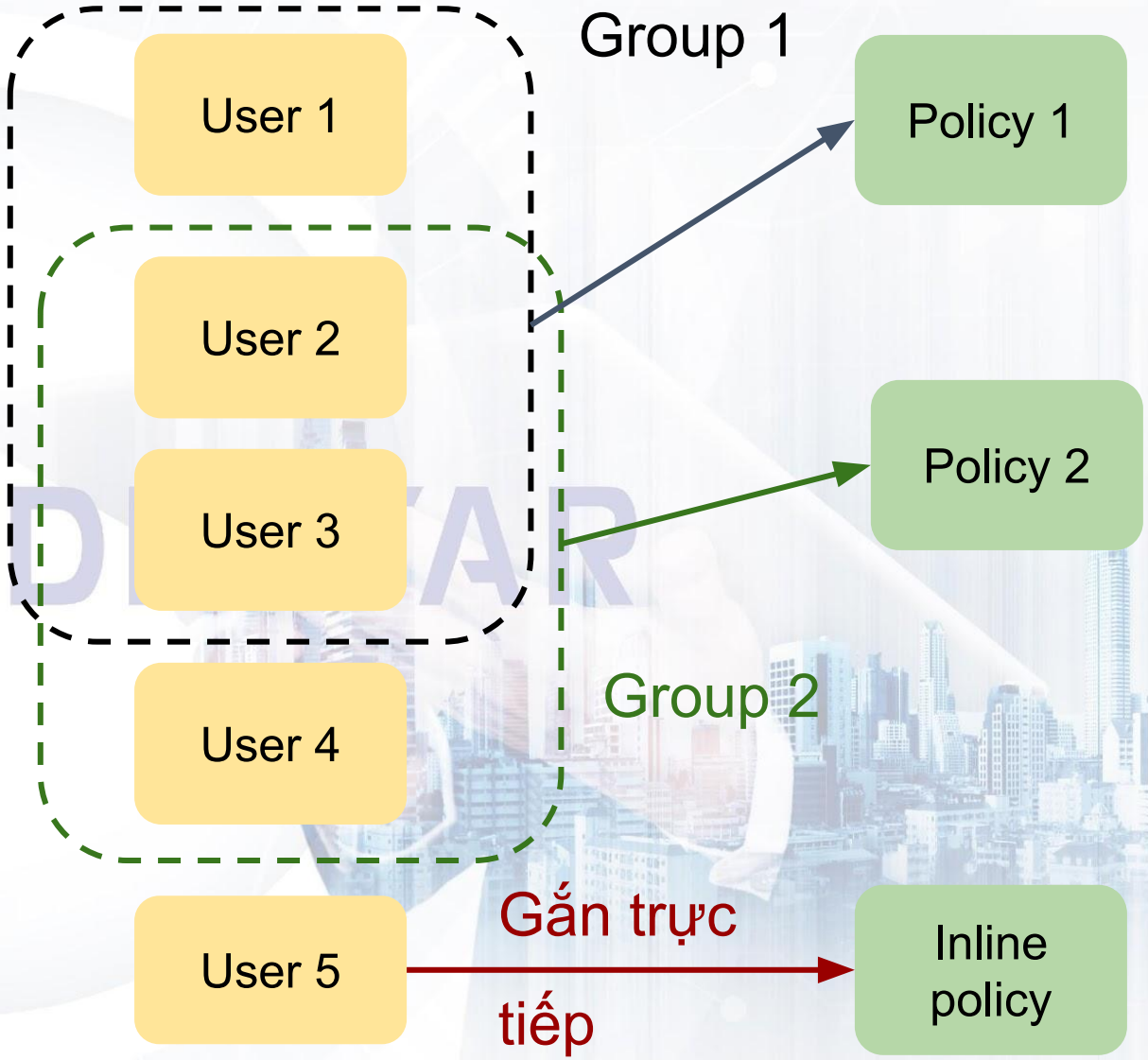
- Group
- User
- Role
- Policy



IAM

User vs Group

- Một User có thể được nằm trong nhiều Group hoặc không nằm trong Group nào.



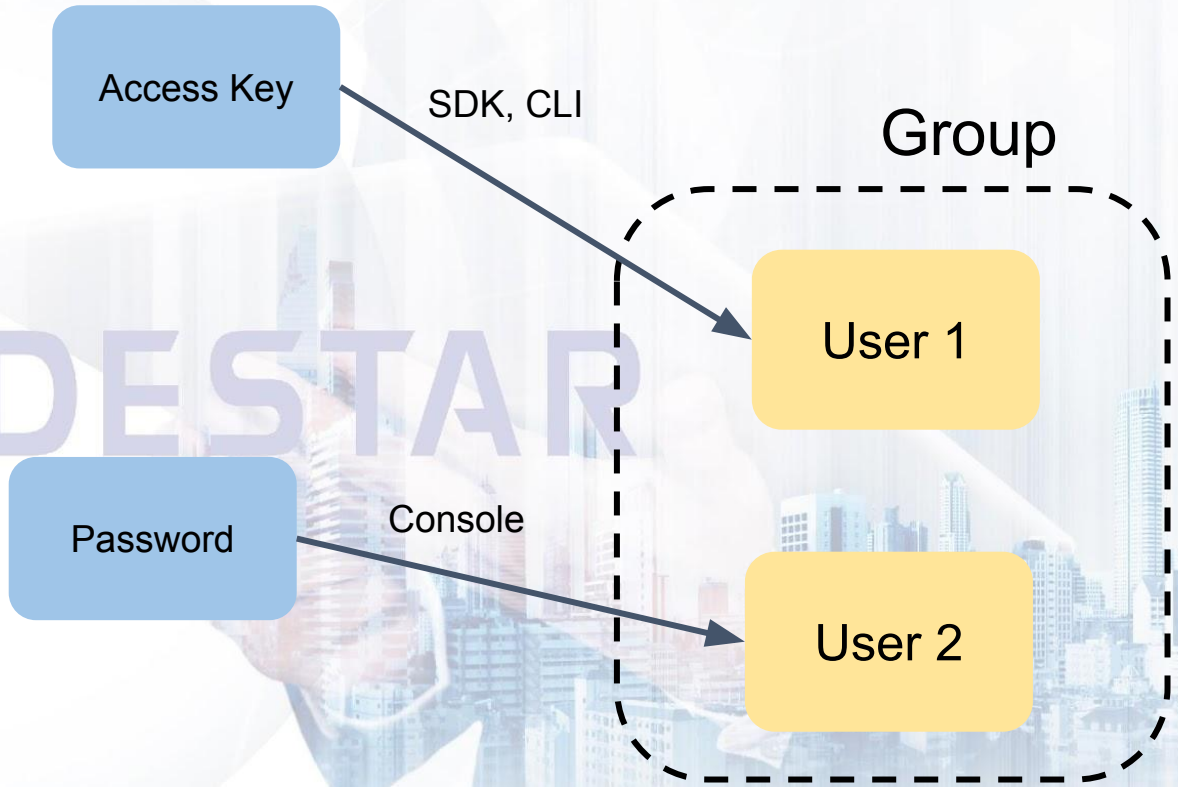
IAM

User sử dụng Security Credentials

- User có một số phương thức sử dụng chủ yếu:

+ Thông qua password để đăng nhập vào Console
+ Thông qua Access Key/Secret Key để xác thực khi sử dụng API/SDK
+ Có thể tạo SSH để sử dụng trên máy tính cá nhân cho 1 số dịch vụ.

=> User dùng cấp cho một người dùng, 1 cá nhân sử dụng.



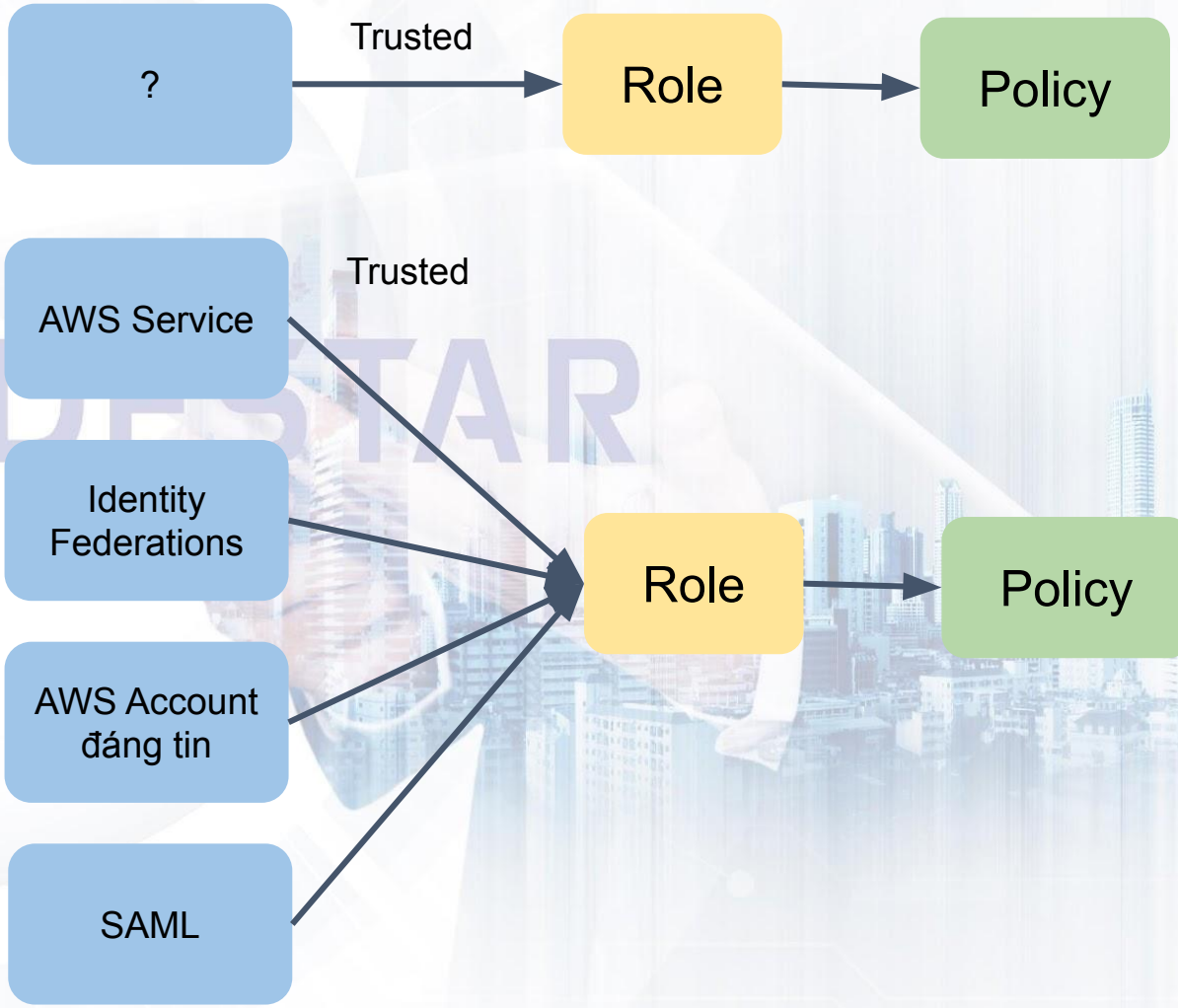
IAM

Role:

Role cho phép một đơn vị là Trusted Entity nào đó sử dụng và cấp quyền.

Trusted Entity này có thể là

+ Một AWS Service đáng tin cậy
+ Một IdF đáng tin như Facebook/Gmail của công ty
+ Một AWS Account nào
+ Một format xác thực phổ biến như SAML

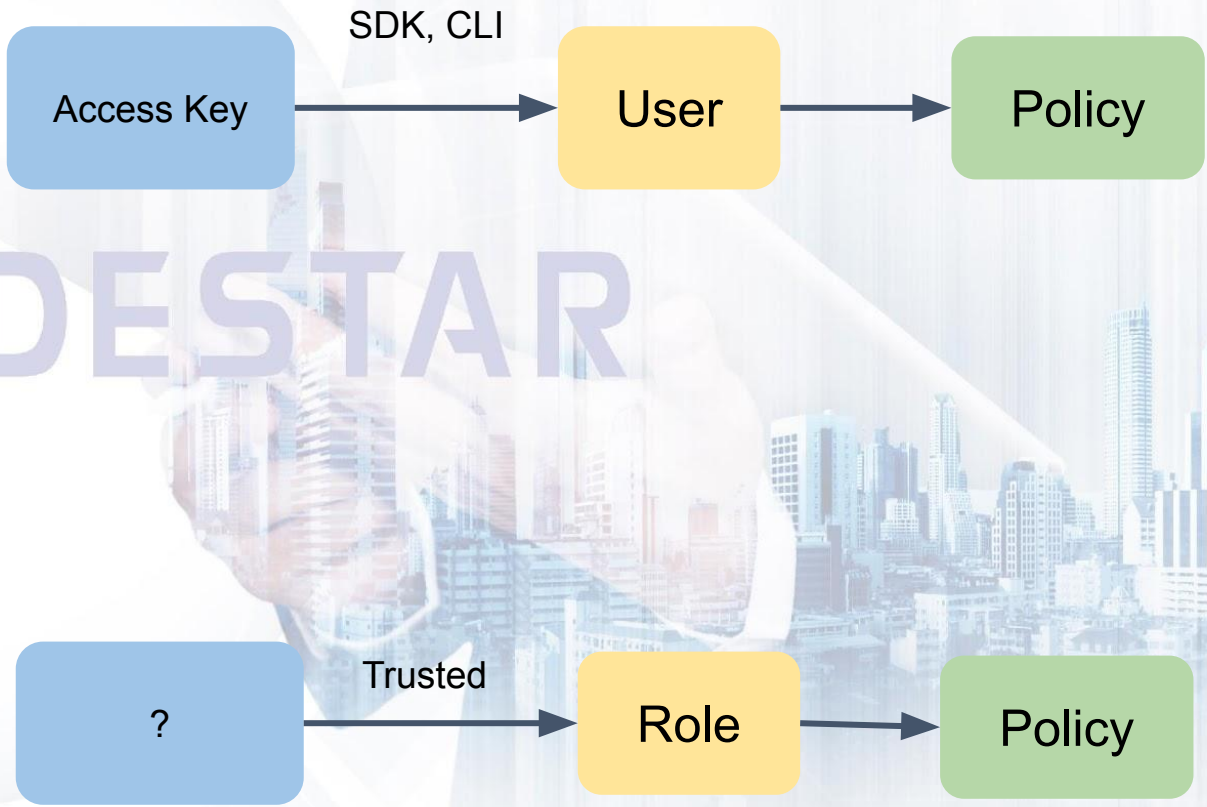


IAM

Role vs User

User thường được sử dụng cho **đối tượng là người**, cần nhập các yếu tố xác thực.

Role thường được sử dụng cho các đối tượng **mang tính tự động, hàng loạt**, như các EC2 instance, Tất cả user trong Account X, …



IAM

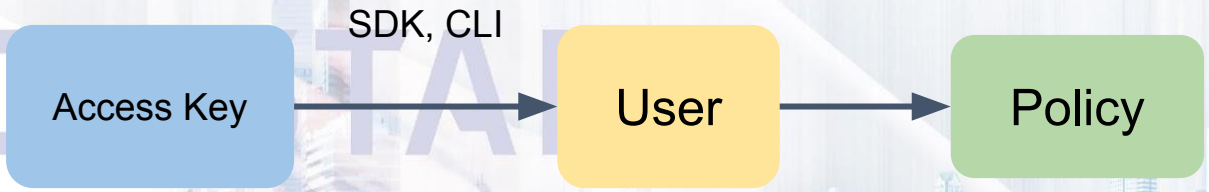
Use-case với Role

- Cho người khác vào xem tài khoản của mình.
- Cho một dịch vụ tương tác với dịch vụ khác trong tài khoản của mình
- Cho phép một bên thứ 3 tương tác vào tài khoản của mình.

IAM

Use-case với User

- Cấp quyền cho các developer trong dự án
- Cấp quyền cho instance nhưng không phải từ EC2 (non-EC2 instance.
- Nhóm các quyền theo Group
- Cần sử dụng Code để đưa Code lên AWS hoặc lấy Code về.



IAM

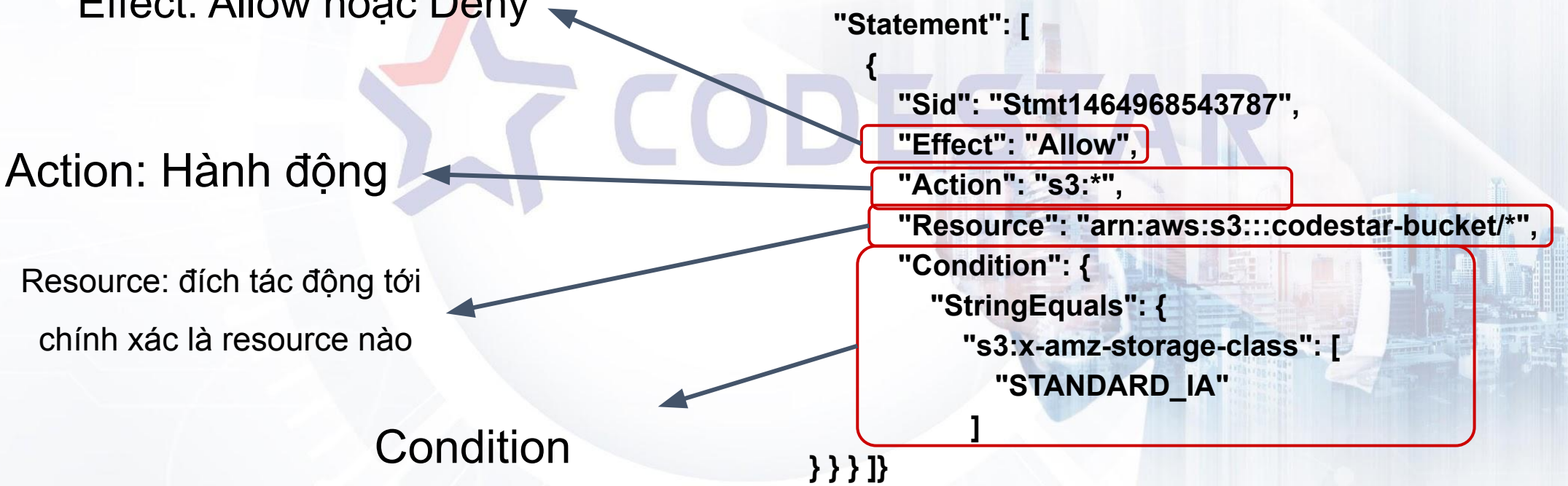
Policy

Effect: Allow hoặc Deny

Action: Hành động

Resource: đích tác động tới chính xác là resource nào

Condition



```
{
   "Version": "2012-10-17",
   "Id": "Access-S3",
   "Statement": [
      {
         "Sid": "Stmt1464968543787",
         "Effect": "Allow",
         "Action": "s3:*",
         "Resource": "arn:aws:s3:::codestar-bucket/*",
         "Condition": {
            "StringEquals": {
               "s3:x-amz-storage-class": [
                  "STANDARD_IA"
               ]
} } } ]}
```

IAM

Multi Statement Policies

Trong Policy, chúng ta có thể thêm nhiều Statement khác nhau. Permission sẽ thỏa mãn:

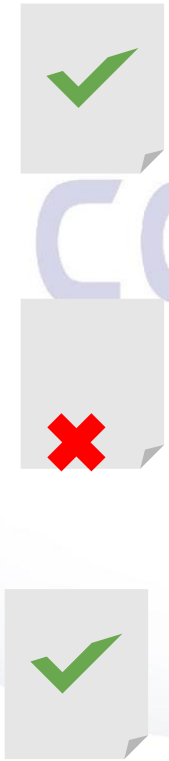
- Nếu Request thỏa mãn tối thiểu một Statement Deny thì sẽ không được cấp phép hoạt động.
- Request không có Statement Deny nào, thì chỉ cần thỏa mãn ít nhất một trong các Statement Allow là có thể được cấp phép.

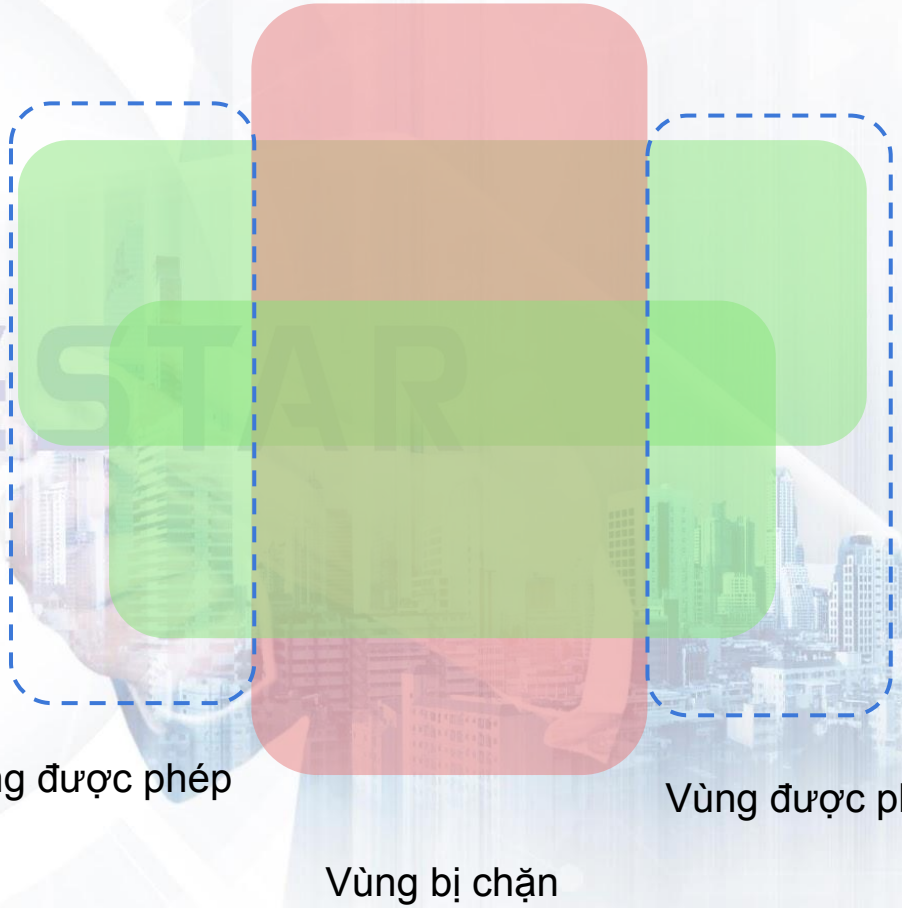
```
{
   "Version": "2012-10-17",
   "Id": "Allow-PutObject-S3",
   "Statement": [
      {
         "Sid": "Stmt1464968543787",
         "Effect": "Allow",
         "Action": "s3:PutObject",
         "Resource": "arn:aws:s3:::codestar-bucket/*.png"
      },
      { ... },
      { ... }
]}
```

IAM

```
{
   "Version": "2012-10-17",
   "Id": "S3-Allow-bucket-policy",
   "Statement": [
      { … },  A
      { ... },  B
      { … },  C

]}
```





IAM

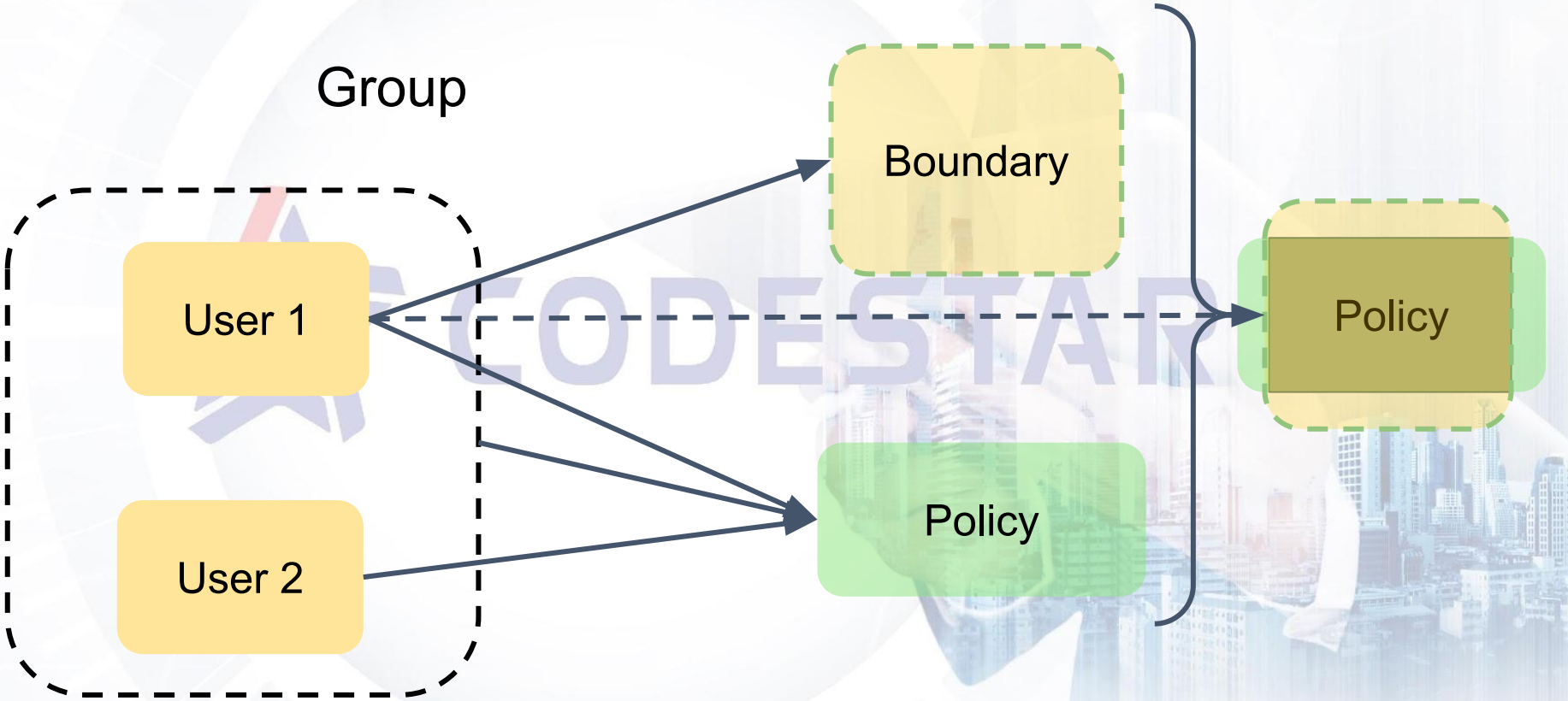
Một số khái niệm bổ sung trong IAM:

- **MFA:** Xác thực đa yếu tố
- **Boundary**: Thành phần giới hạn quyền người dùng/Role.

  Use case:

+ Glới hạn quyền hạn dành cho người dùng khi kết hợp vào nhiều nhóm Group khác nhau.
+ Cắt quyền cho một nhóm người dùng cụ thể.

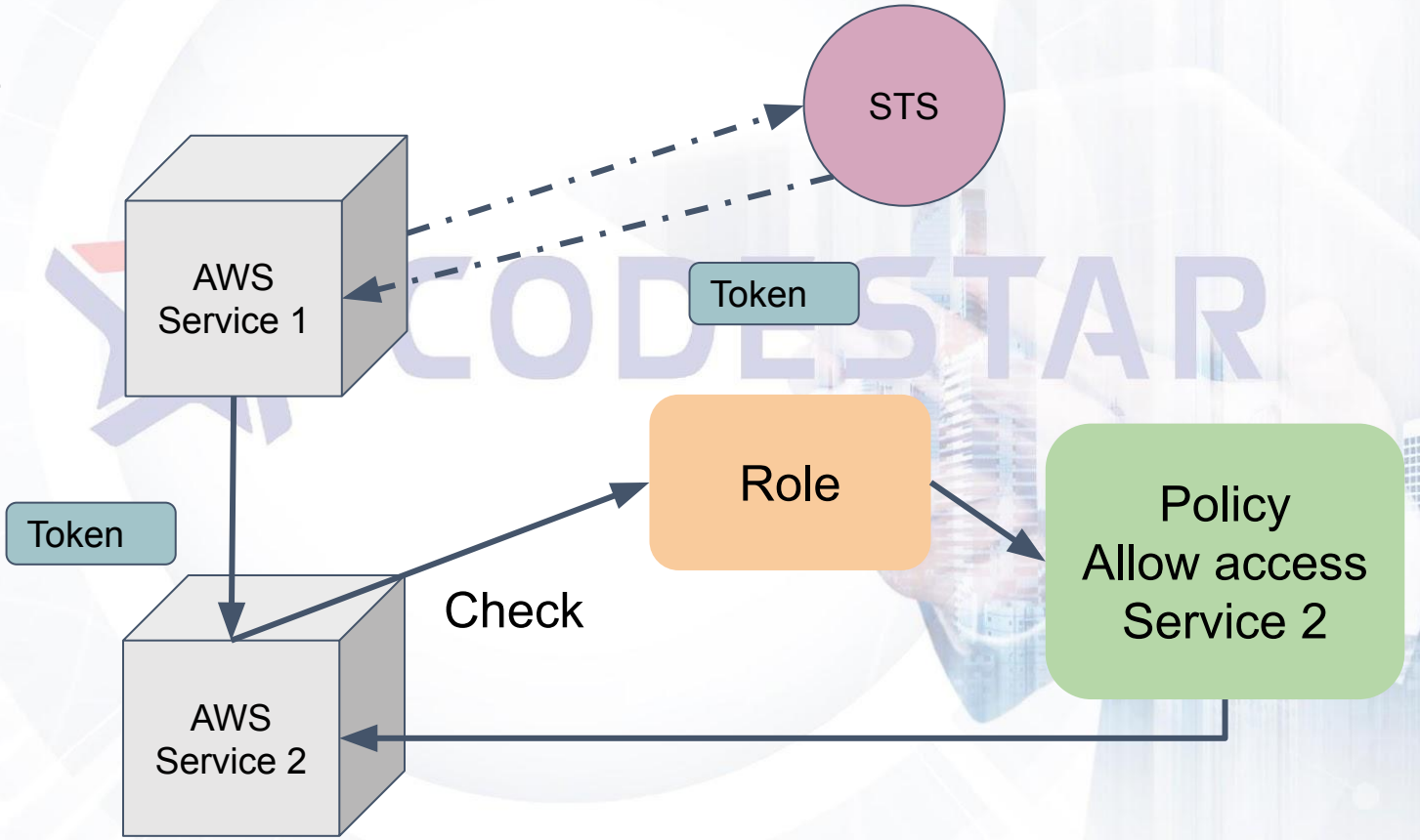
IAM



IAM

STS Temporary access token cho 15 phút - 12h

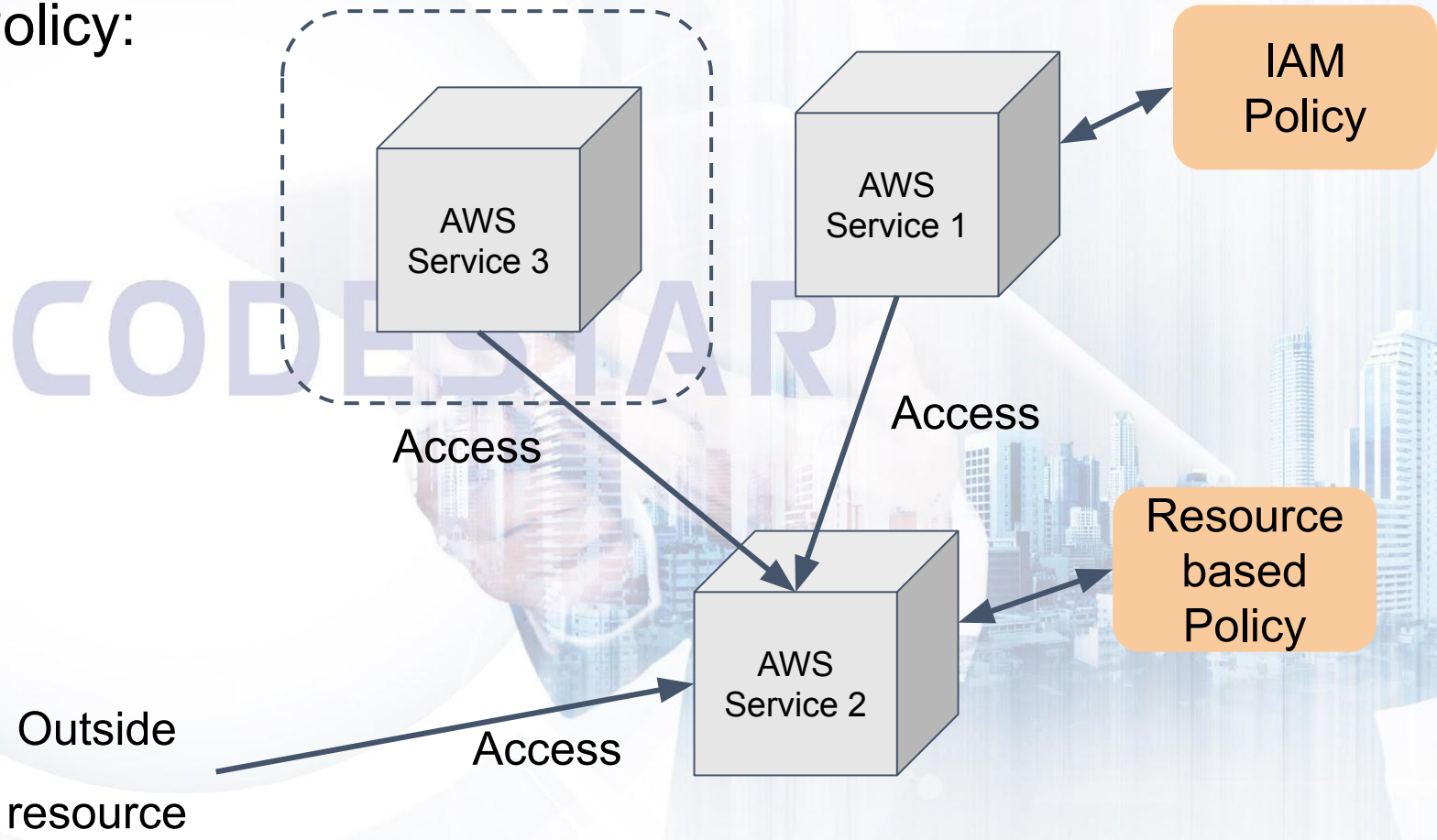
AssumeRole



IAM

Các loại resource based Policy:

- S3
- SQS
- SNS
- VPC Endpoint Policy
- Lambda
- …



IAM

Policy

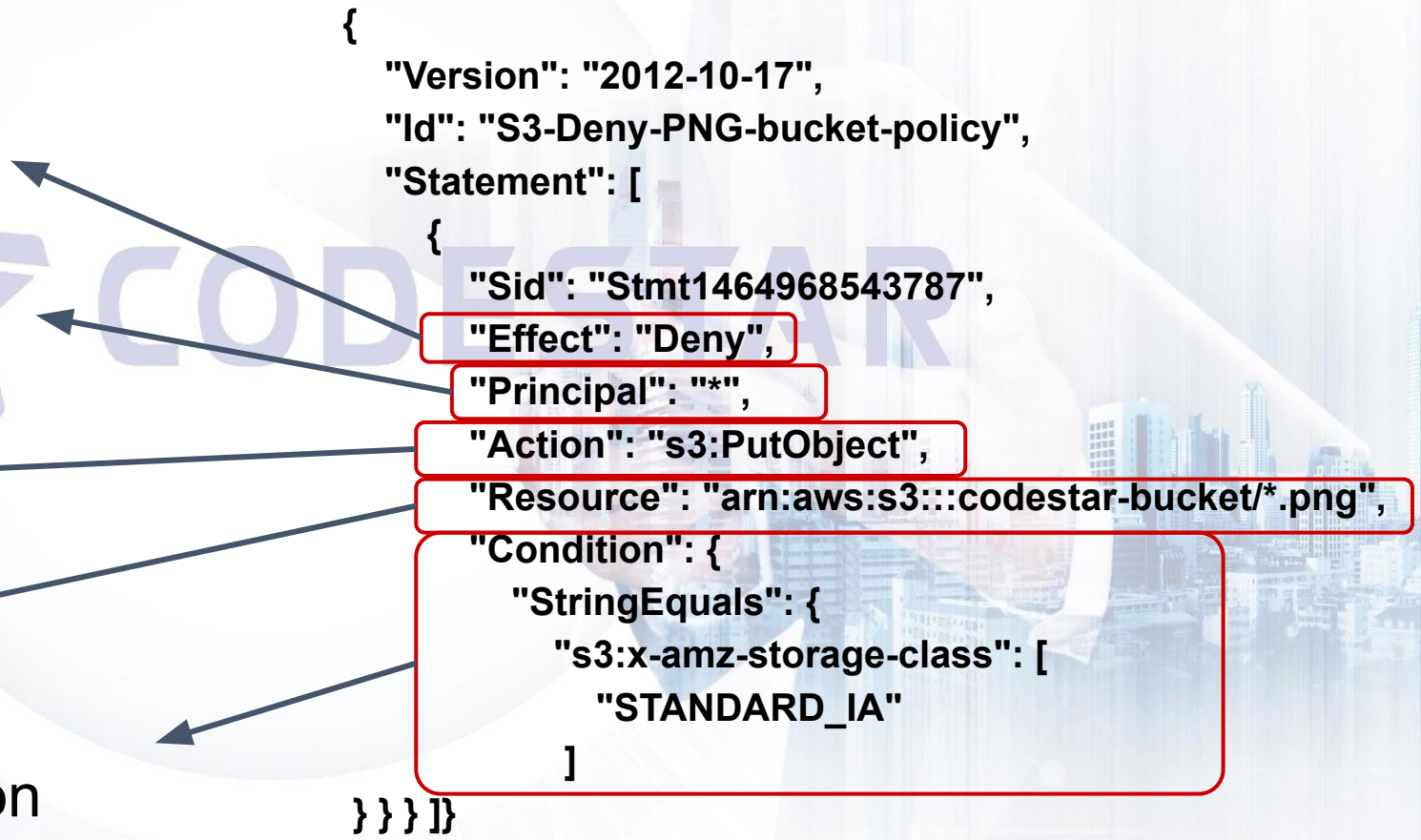
Effect: Allow hoặc Deny

Principal: Tác động tới đối tượng nào

Action: Hành động

Resource: đích tác động tới chính xác là resource nào

Condition



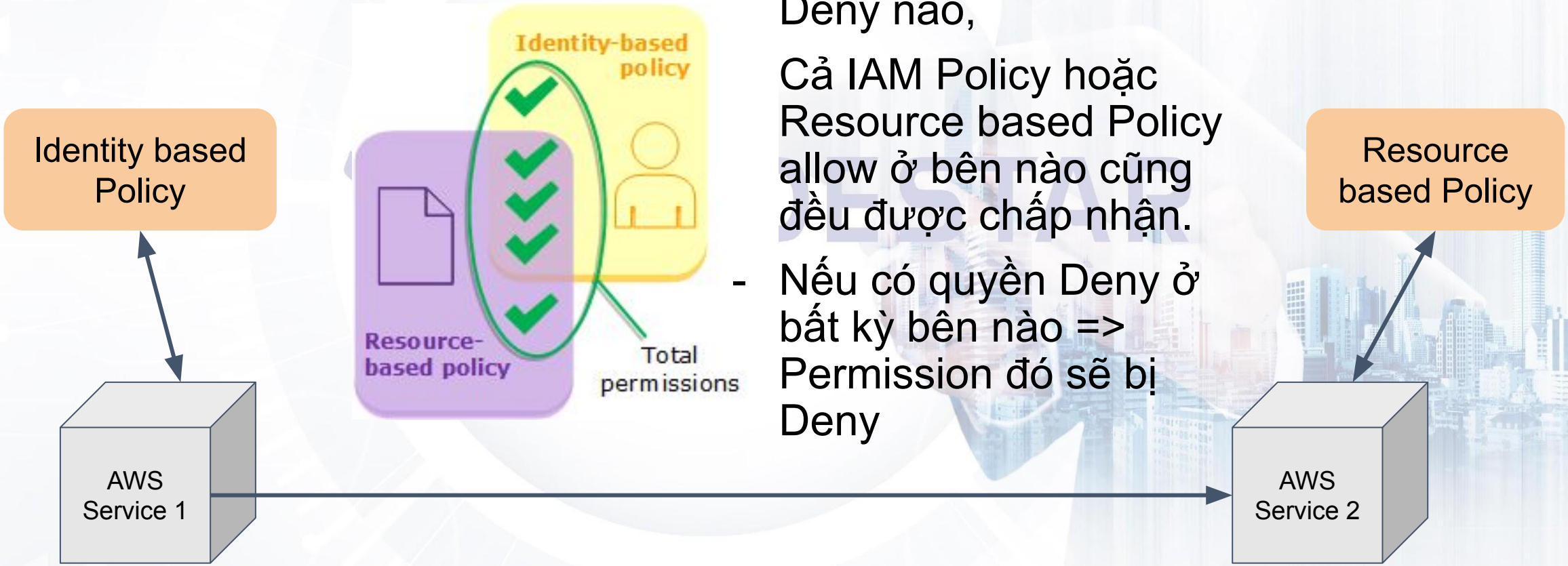
```
{
   "Version": "2012-10-17",
   "Id": "S3-Deny-PNG-bucket-policy",
   "Statement": [
     {
       "Sid": "Stmt1464968543787",
       "Effect": "Deny",
       "Principal": "*",
       "Action": "s3:PutObject",
       "Resource": "arn:aws:s3:::codestar-bucket/*.png",
       "Condition": {
         "StringEquals": {
           "s3:x-amz-storage-class": [
             "STANDARD_IA"
           ]
} } } ]}
```

IAM

Kết hợp quyền:

- Nếu không có quyền Deny nào,

  Cả IAM Policy hoặc Resource based Policy allow ở bên nào cũng đều được chấp nhận.
- Nếu có quyền Deny ở bất kỳ bên nào => Permission đó sẽ bị Deny

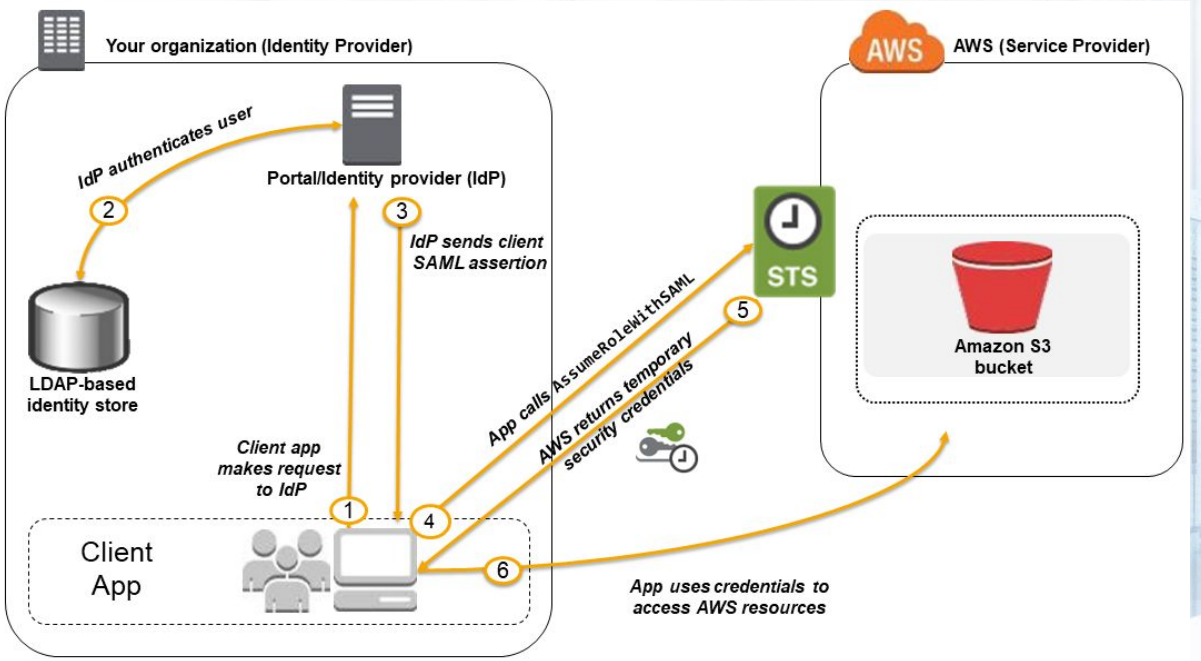


IAM

Identity Federation

- Khi tạo ra Role với Trusted Entity sử dụng SAML, chúng ta có thể thiết lập một hệ thống custom authentication nội bộ để thao tác trên AWS (thông qua STS).

***Use case**: Công ty có một hệ thống xác thực tự build. Công ty muốn tạo một App, đăng nhập vào tài khoản của công ty cấp và có thể truy xuất file trên S3.*



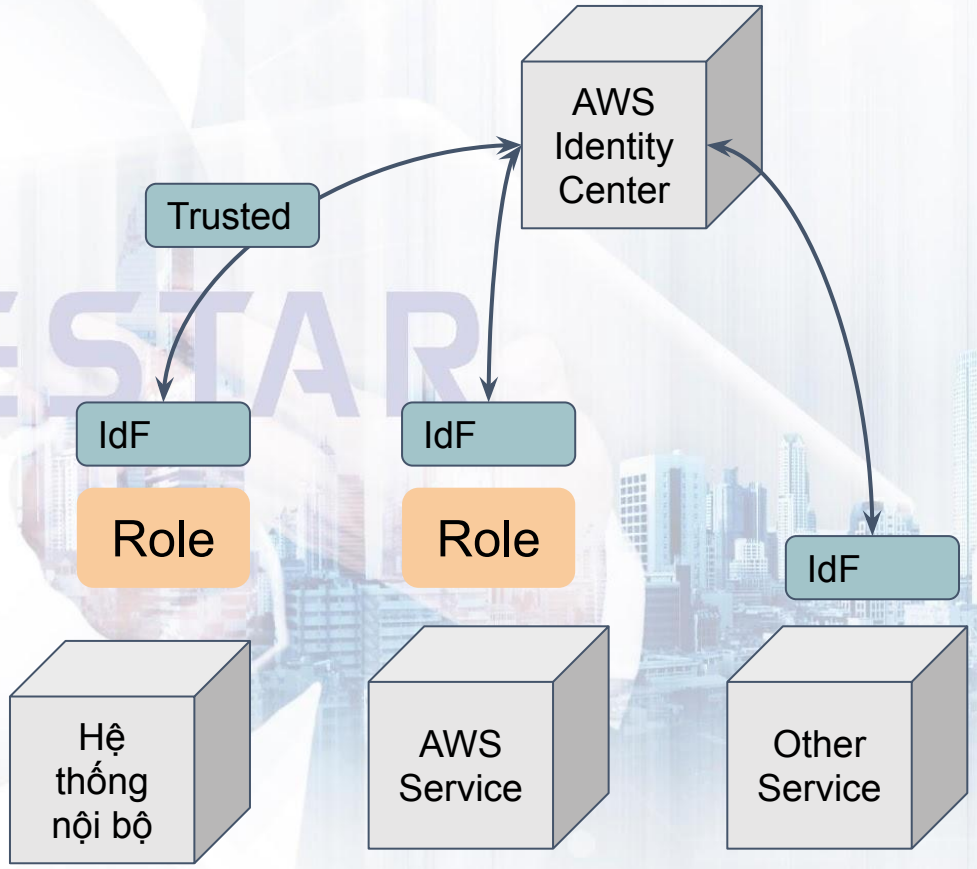
IAM

AWS Identity Center - SSO

AWS Identity Center là một dịch vụ SSO cho phép tách biệt luồng xác thực người dùng.

AWS Identity Center cho phép các Service khác (Service Provider), sử dụng phương thức truy cập của mình.

Use case: *Công ty muốn xây dựng 1 hệ thống xác thực cho nội bộ, để sử dụng cho các Service/App của công ty/truy cập vào các tài nguyên trên AWS.*

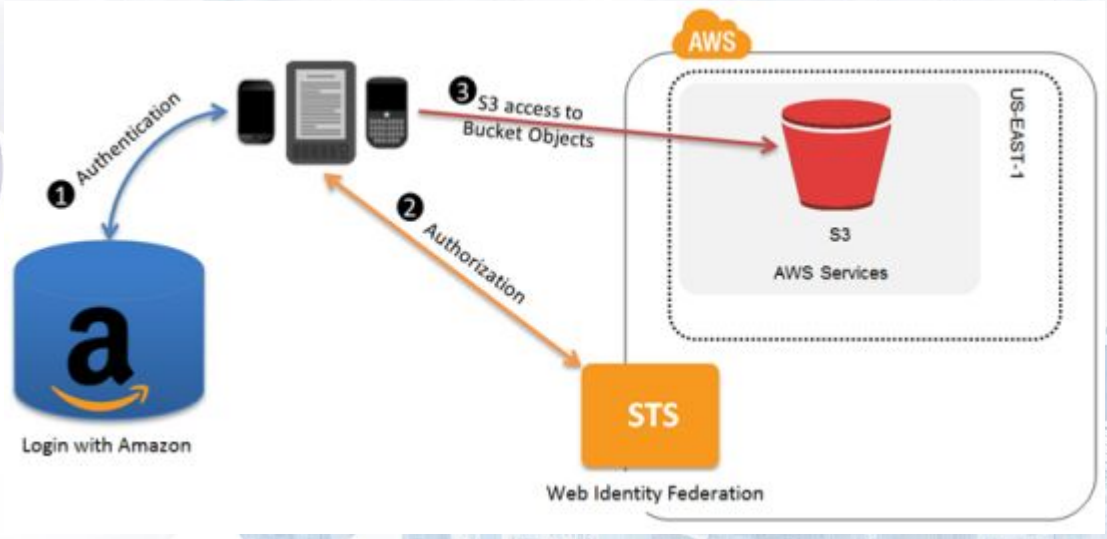


IAM

AssumeRole with Web Identity

Use case:

Công ty muốn build một App, sử dụng Gmail công ty. Sau khi đăng nhập vào Gmail công ty, có thể thao tác tới S3



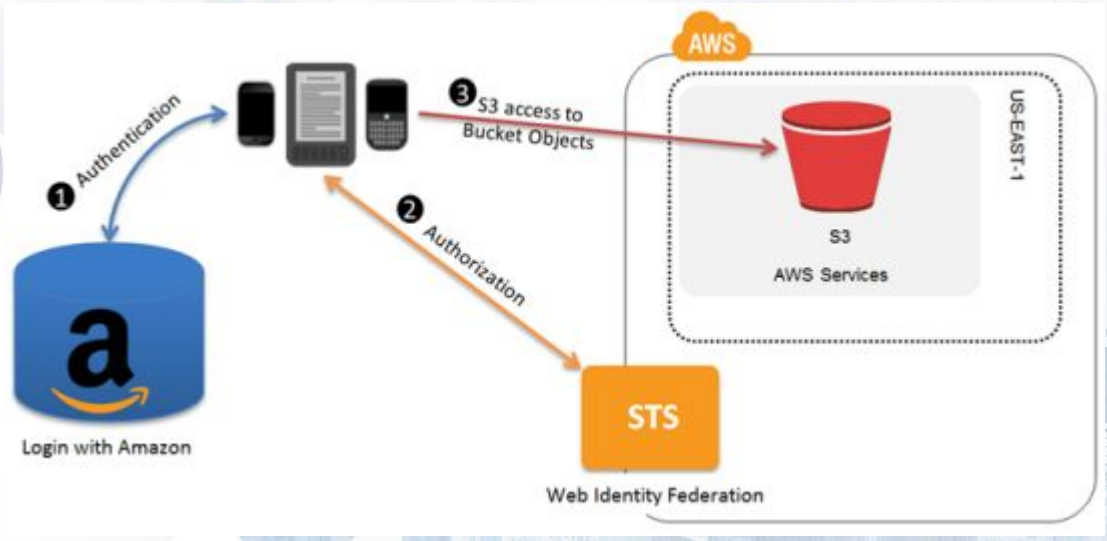
IAM

AssumeRole with Web Identity

AssumeRole có thể được thực hiện thông qua một bên thứ 3.

Tại đó, bên thứ 3 đã thực hiện xác thực bằng IdF trên AWS.

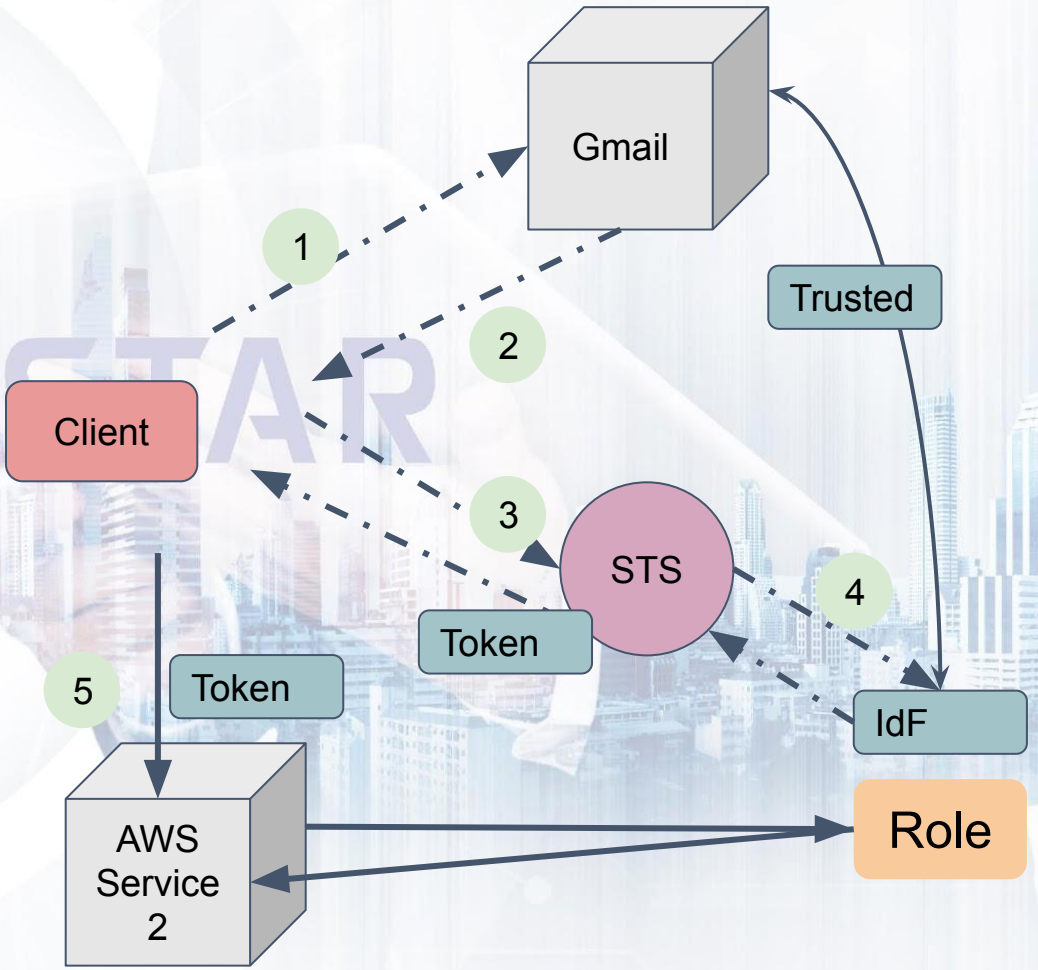
Khi chúng ta đăng nhập bằng cơ chế xác thực của bên thứ 3 (như Facebook, Gmail, Amz, …), service sẽ gửi về Đối tượng đăng nhập (Service 1) một thông tin đăng nhập, gửi lên STS, xác thực với IdF -> cho phép sử dụng Role.



IAM

AssumeRole with Web Identity

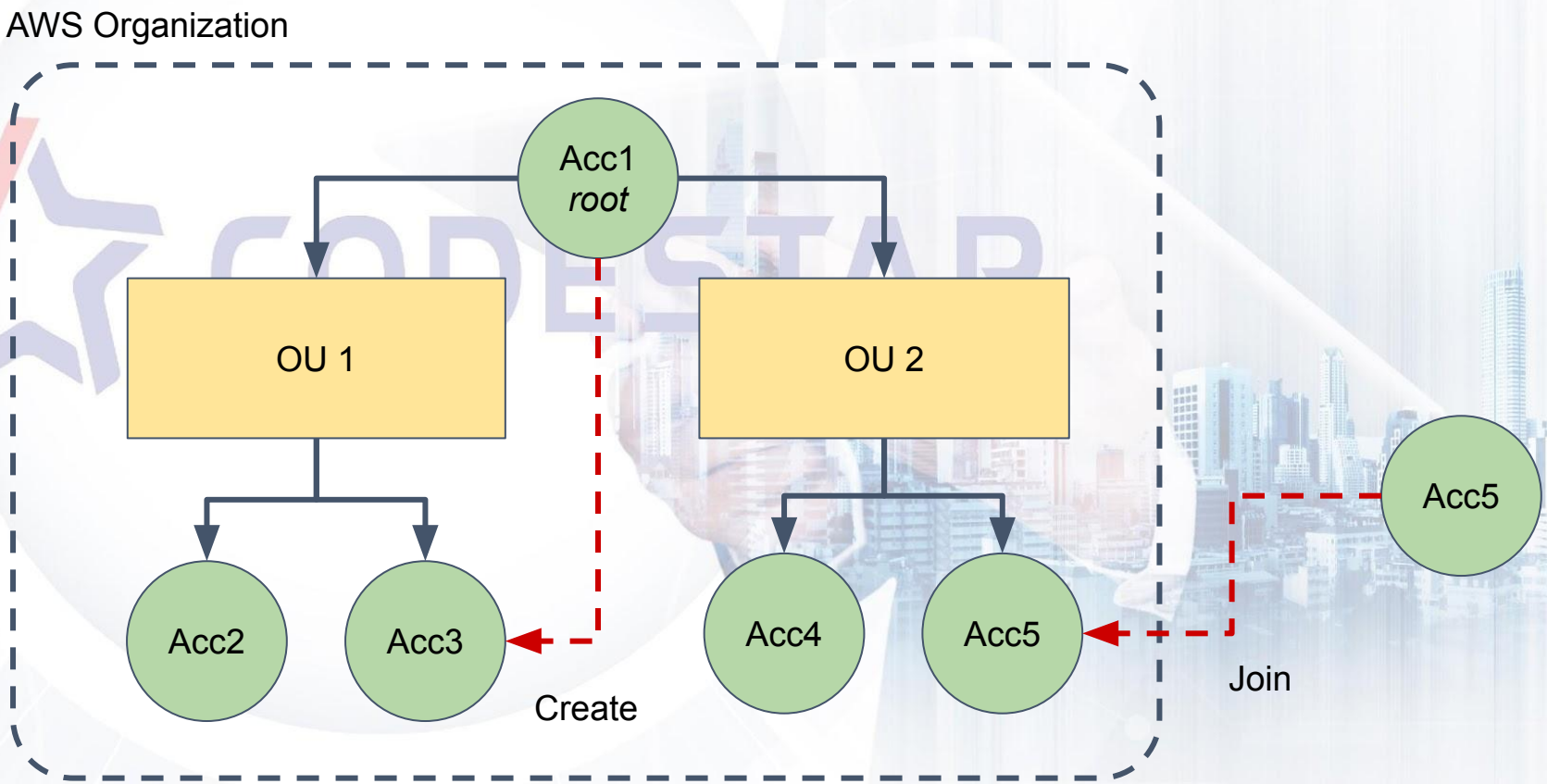
1. Phía client -> Show màn hình Web Identity để người dùng đăng nhập.
2. Phía client sẽ nhận được token. Gửi lên AWS STS để AssumeRole và nhận về STS Token (session token)
3. Phía client sử dụng Token này để thao tác với AWS.



Organization

Organization:

Dịch vụ hỗ trợ quản lý multi-account trong các chiến lược quản lý tổng thể.

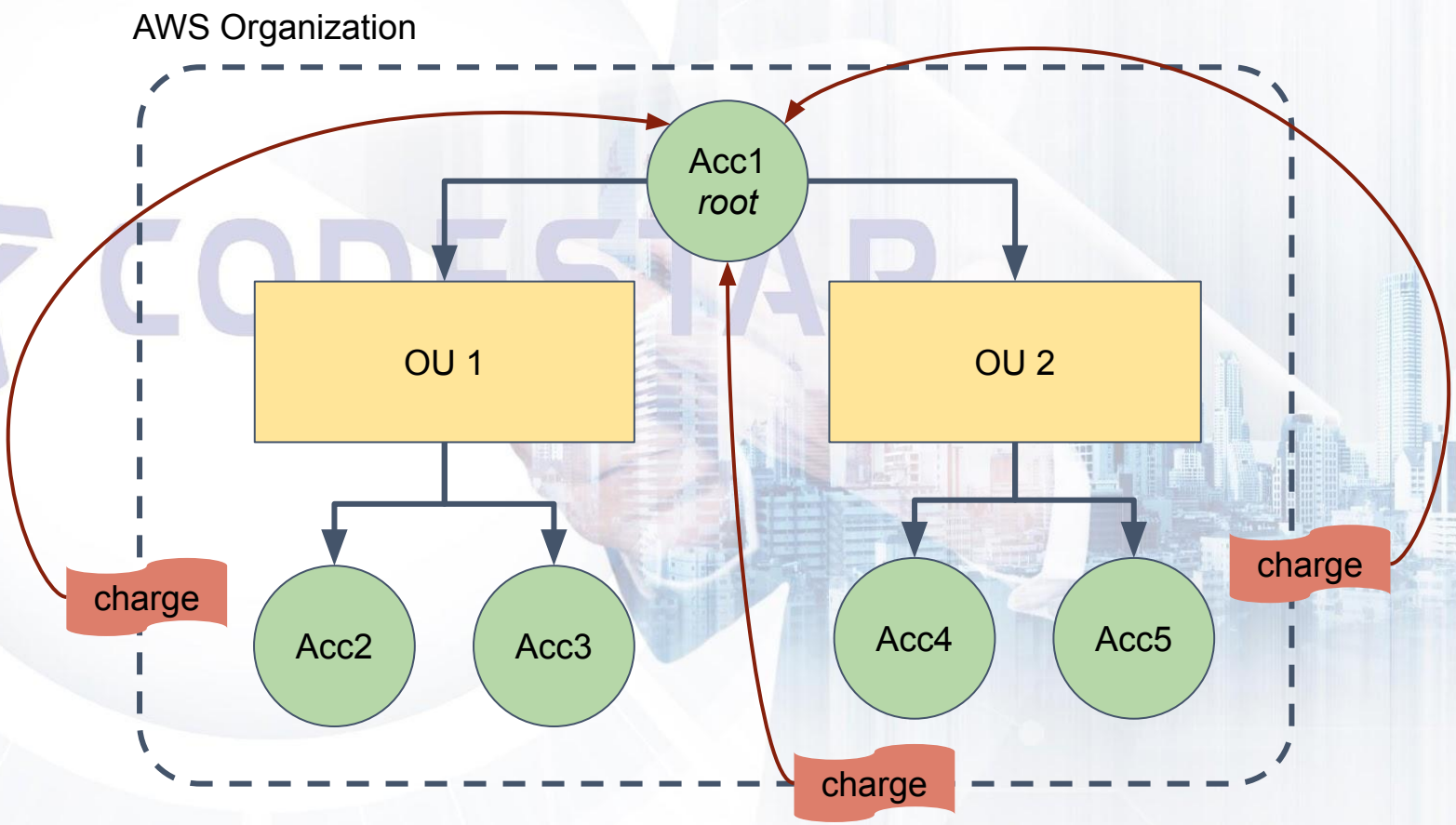


Organization

Consolidated Billing:

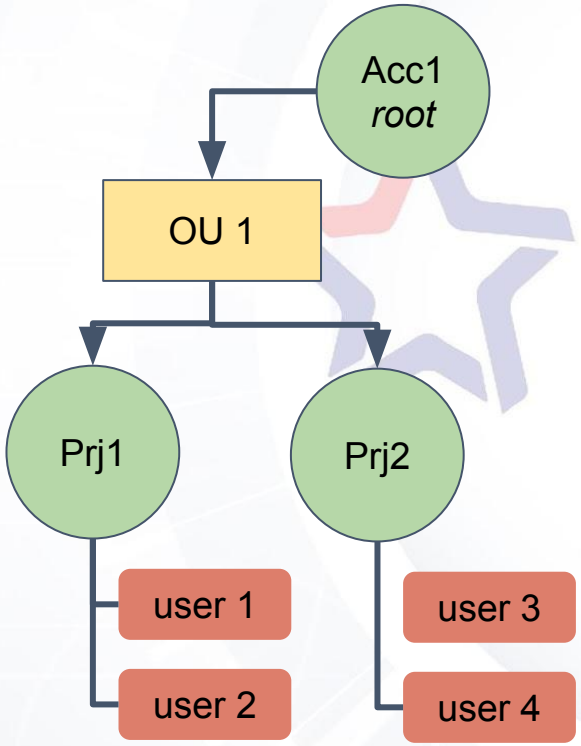
Các Account bên dưới sử dụng tiền sẽ được đưa vào Billing của Acc1.

Lưu ý: Credit của các Account bên dưới cũng được sử dụng luôn.

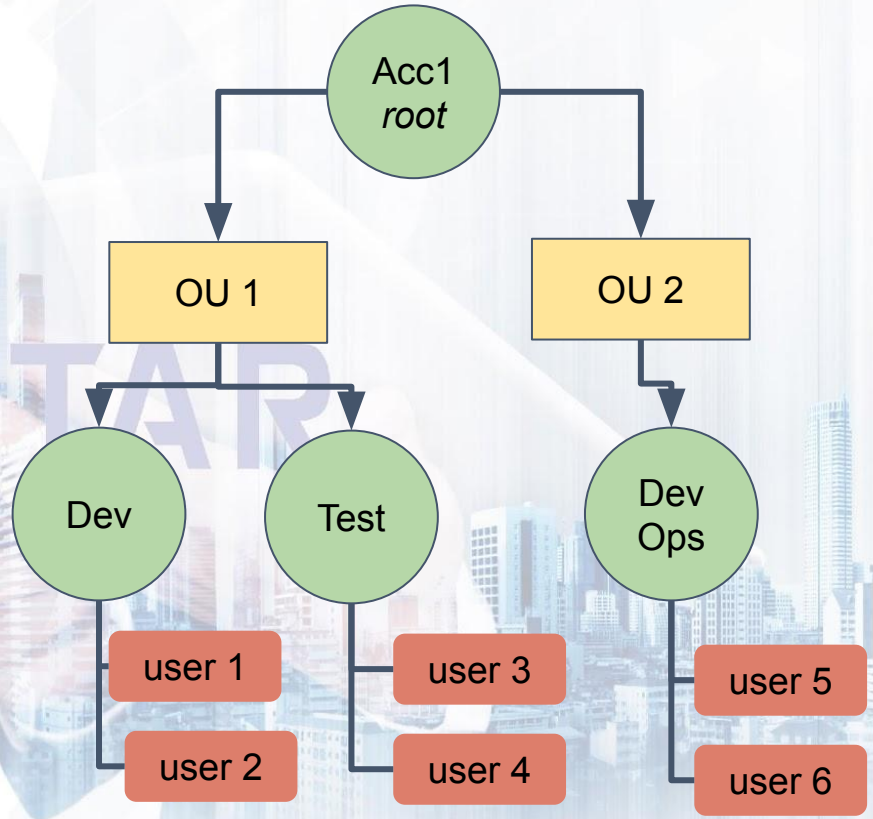


Organization

Một số cách chia dự án



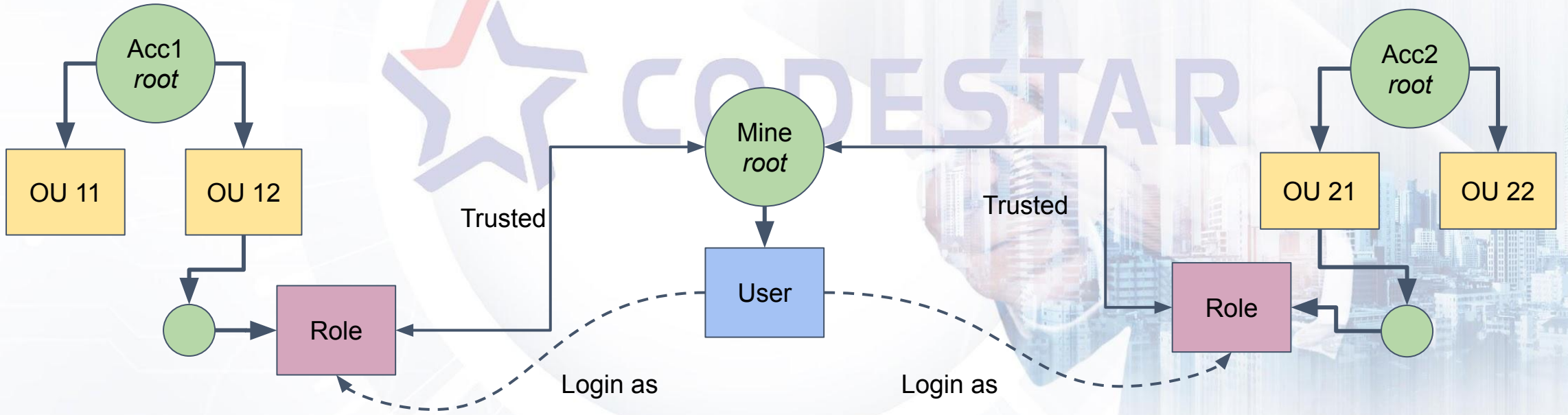
Phân chia theo project



Phân chia theo phòng ban/chức năng

Organization

Use case: Sử dụng Account cá nhân truy cập tài nguyên trên các Organization khác nhau



Organization 1

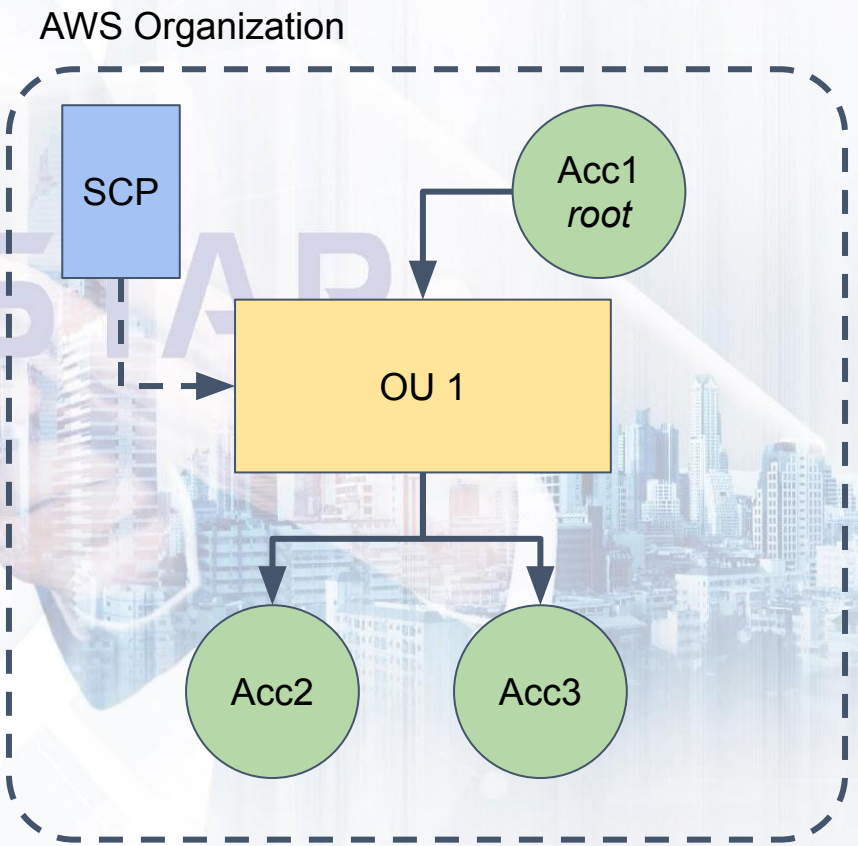
Organization 2

Organization

Service Control Policy (SCP)

SCP có thể hiểu là Permission Boundary của một OU và các Account nằm trong OU đó.

SCP giúp quản lý tập trung Maximum available Permission cho các tài khoản nằm trong Organization.



Organization

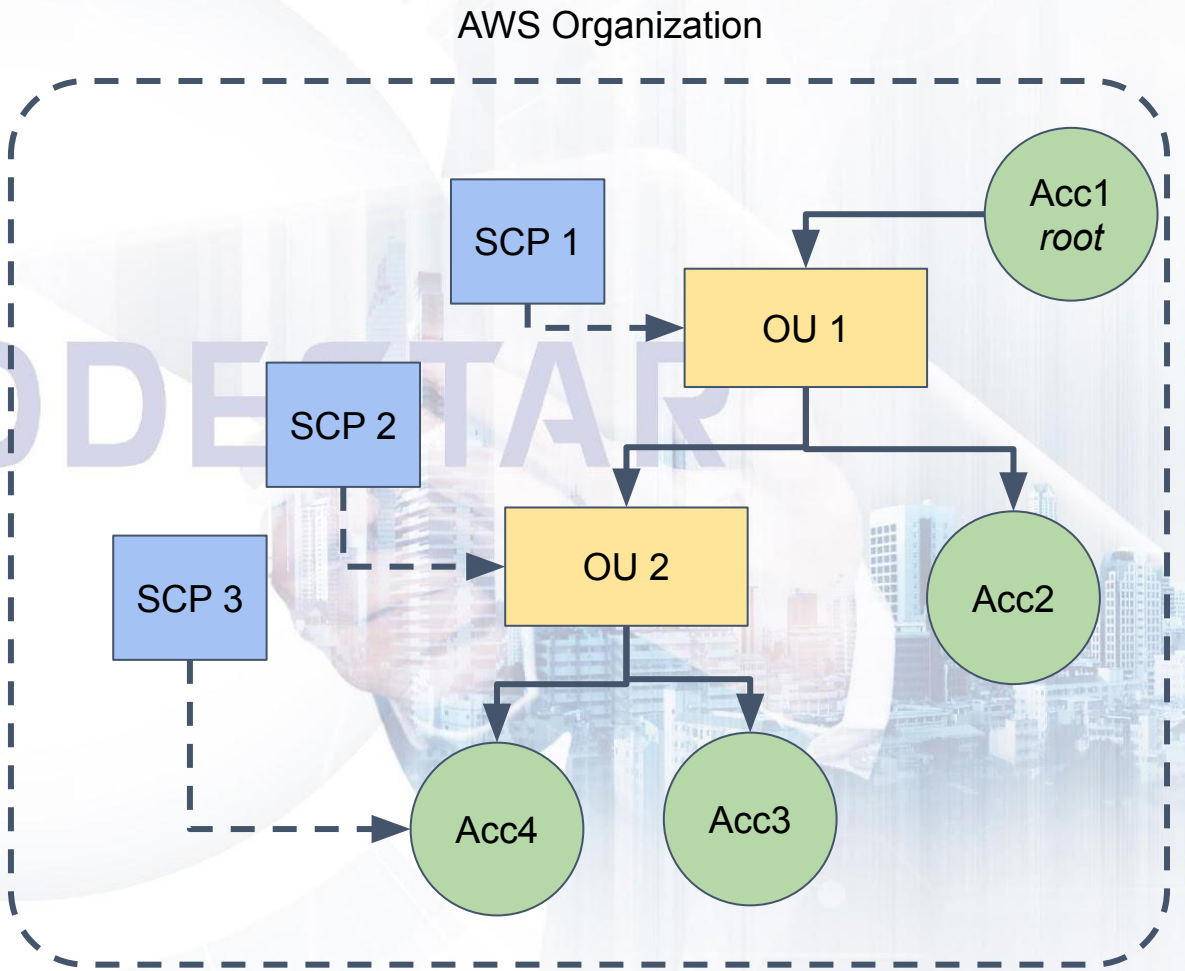
Service Control Policy (SCP)

Permission của một Account sẽ chịu tác động toàn bộ SCP của OU phía trên.

Acc2 chịu tác động của SCP1

Acc3 chịu tác động của SCP1 và SCP2 (giao của 2 SCP)

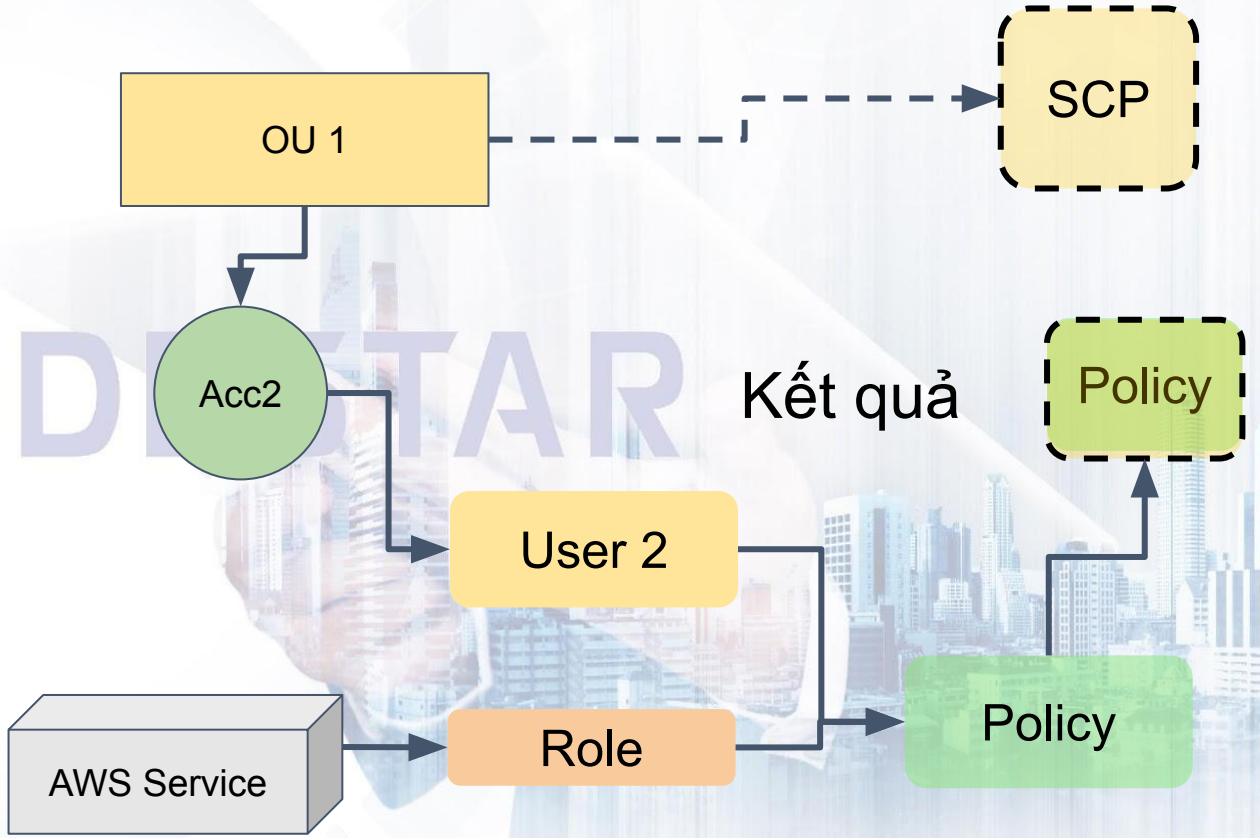
Acc4 chịu tác động của SCP1,2 và 3



Organization

Service Control Policy (SCP)

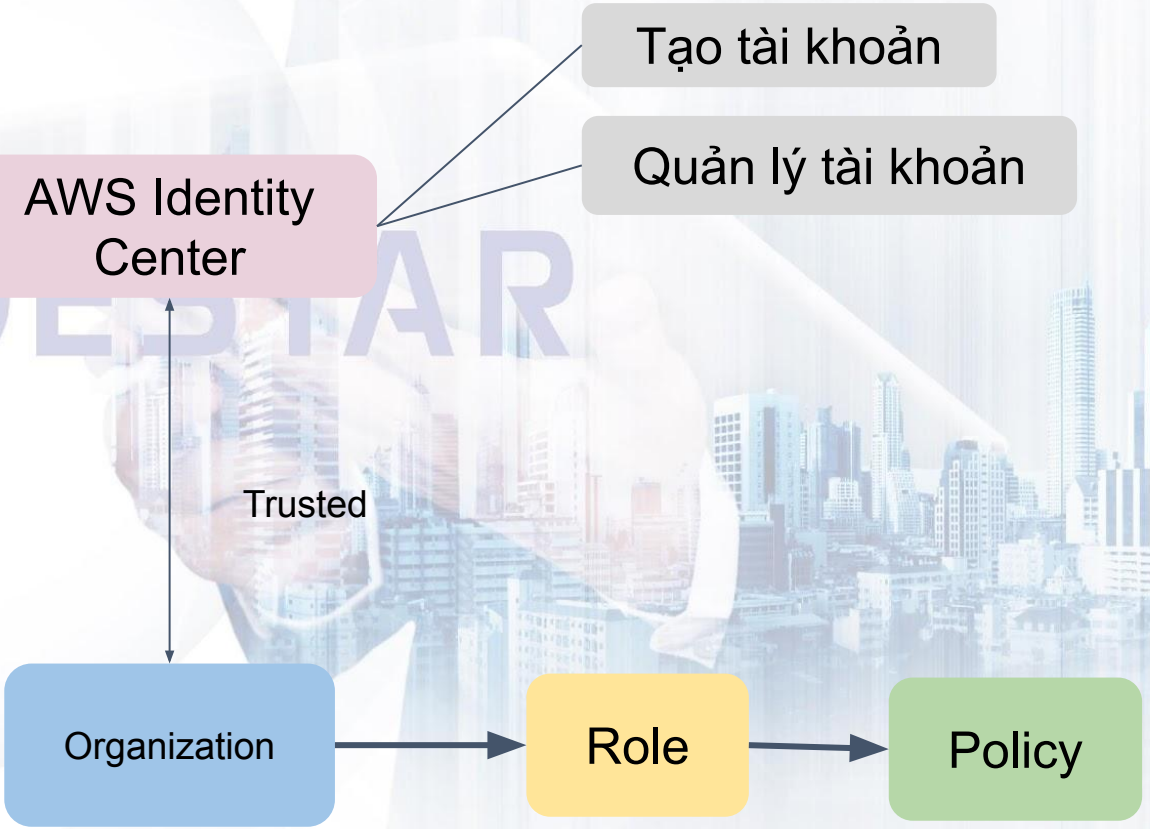
Lưu ý: SCP tác động tới toàn account nằm trong OU. Để xác định quyền có được cấp không, cần có thêm Identity-based Policy hoặc Resource-based Policy.



Organization

Use case sử dụng Role với Organization

- Tạo Role chung
- Sử dụng Role



CODESTAR

THANK YOU