

IAM Advanced

Nội dung



- STS
- Directory Services
- Organization, Landing Zone
- RAM
- AWS System Manager
- AWS Trusted Advisor

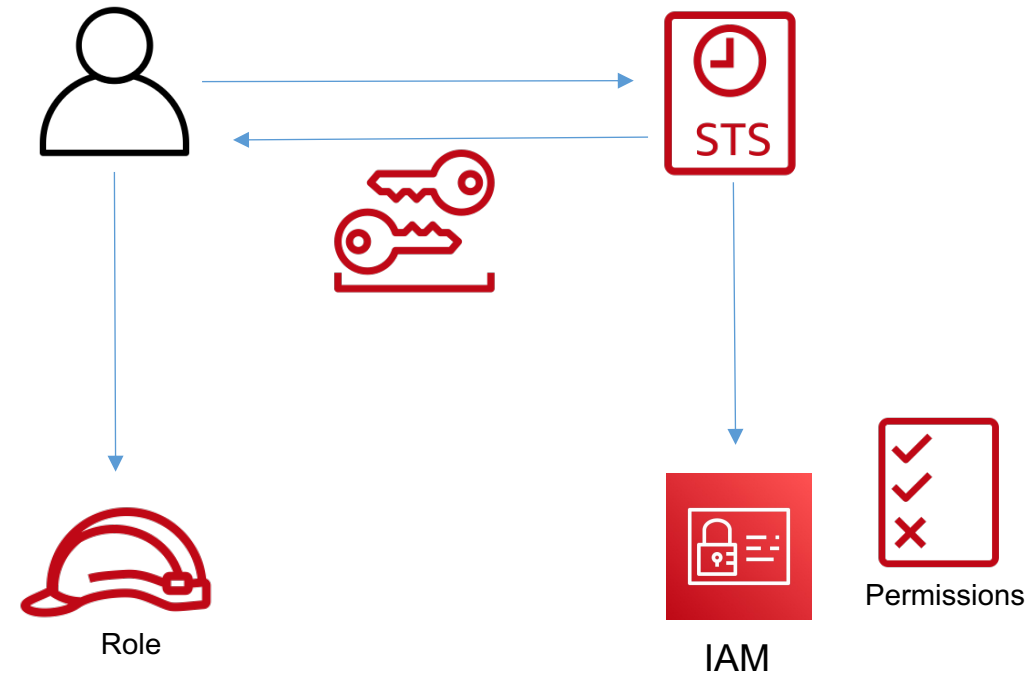
STS

STS – Security Token Service

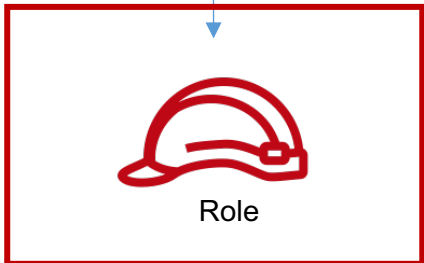
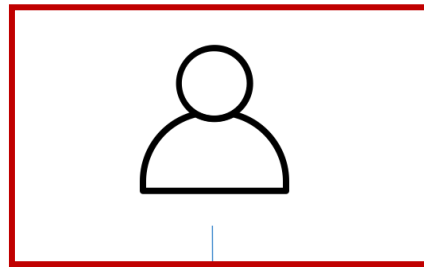
- STS cho phép gán quyền tạm để truy cập vào các AWS resources
- STS cung cấp Token cho các thực thể cần truy cập AWS resources trong khoảng thời gian 15 phút ~ 1 giờ.
- **AssumeRole**
 - Sử dụng trong cùng một AWS account hoặc chéo account (Cross Account)
- **AssumeRoleWithSAML**
 - Sử dụng để cung cấp Token cho các users đăng nhập qua các hệ thống xác thực nội bộ (IdP) sử dụng SAML
- **AssumeRoleWithWebIdentity**
 - Sử dụng để cung cấp Token cho các users đăng nhập qua các hệ nhà cung cấp Web Identity (Facebook, Google, Amazon, Microsoft...)

Assume Role sử dụng STS

- Định nghĩa Role với tiêu chí quyền tối thiểu (Least privilege permission)
- Định nghĩa một thực thể (user) có quyền sử dụng Role này
- Sử dụng STS để lấy credentials và để truy cập resources với quyền hạn của Role (AssumeRole)
- Credentials sẽ có hiệu lực trong khoảng 15 phút tới 1 giờ, sau đó cần refresh lại để lấy credentials mới



Assume Role sử dụng STS (cont.)



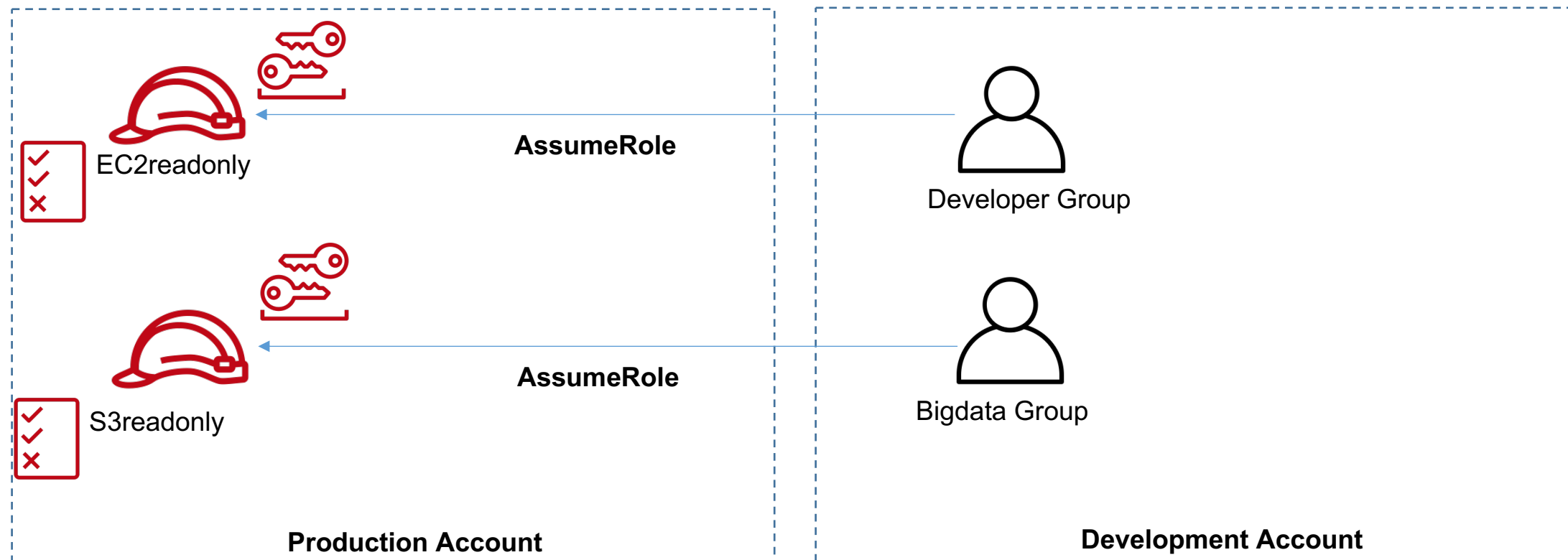
Trusted Policy

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "AWS": "arn:aws:iam::1234567890:user/hoa.nh"  
      },  
      "Action": "sts:AssumeRole",  
      "Condition": {} } ] ] }
```

Permission Policy

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

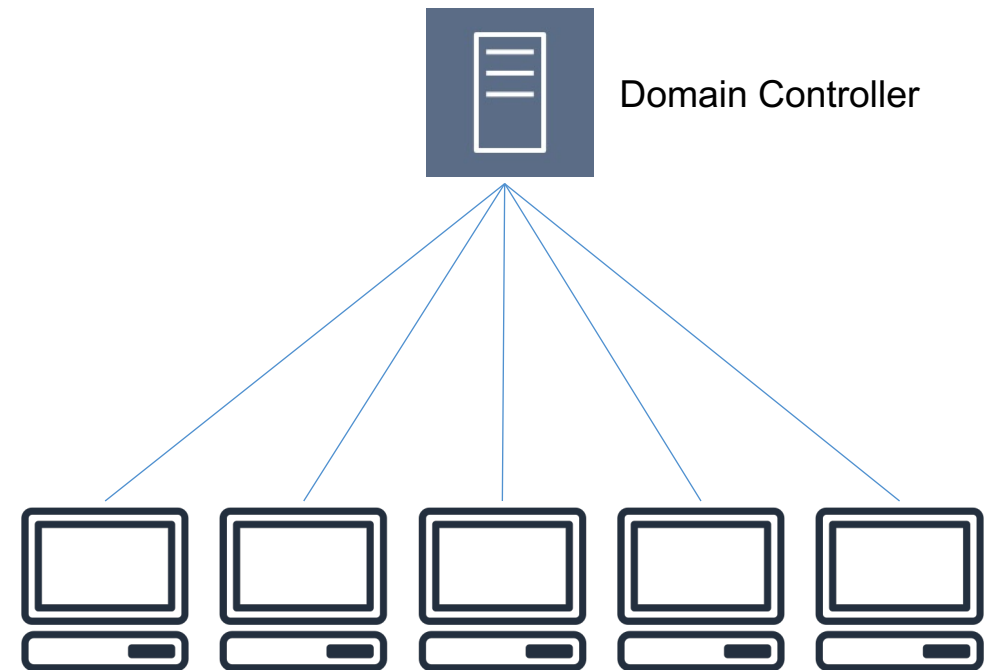
Cross account access sử dụng STS



Directory Service

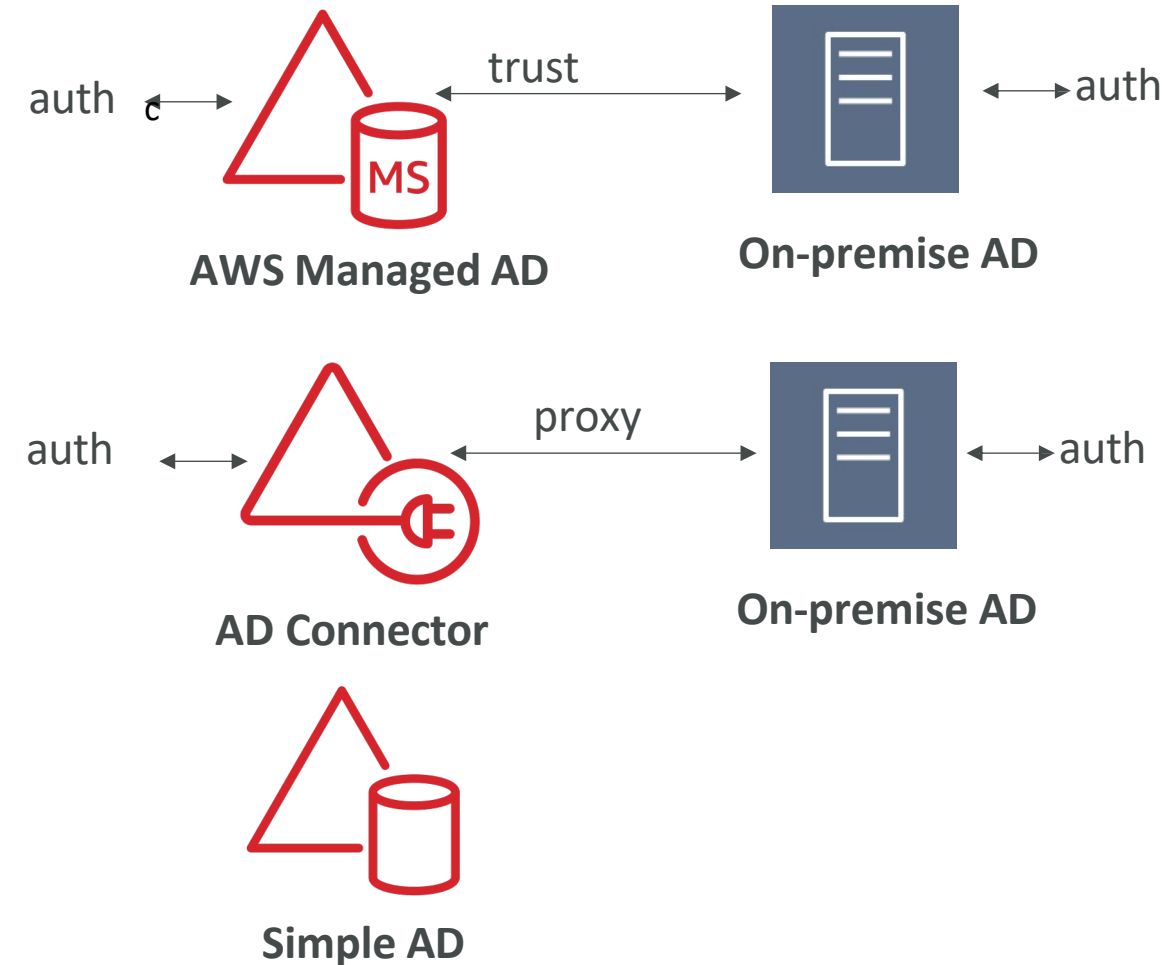
Microsoft Active Directory

- Quản lý tập trung users, các chính sách (policy), security trong các tổ chức, công ty.
- Các đối tượng (objects) được quản lý bao gồm: user account, computer, printers, file servers...
- Các objects được tổ chức dưới dạng **tree**
- Nhóm các **tree** được gọi là **forest**



AWS Directory Service

- AWS Managed Microsoft AD
 - Microsoft Active Directory đặt (hosted) trên AWS
- AD Connector
 - Sử dụng Microsoft AD có sẵn tại hạ tầng On-premise
- Simple AD
 - Standalone managed directory
 - Cung cấp một số tính năng tương tự Microsoft AD



AWS Organizations

AWS Organizations

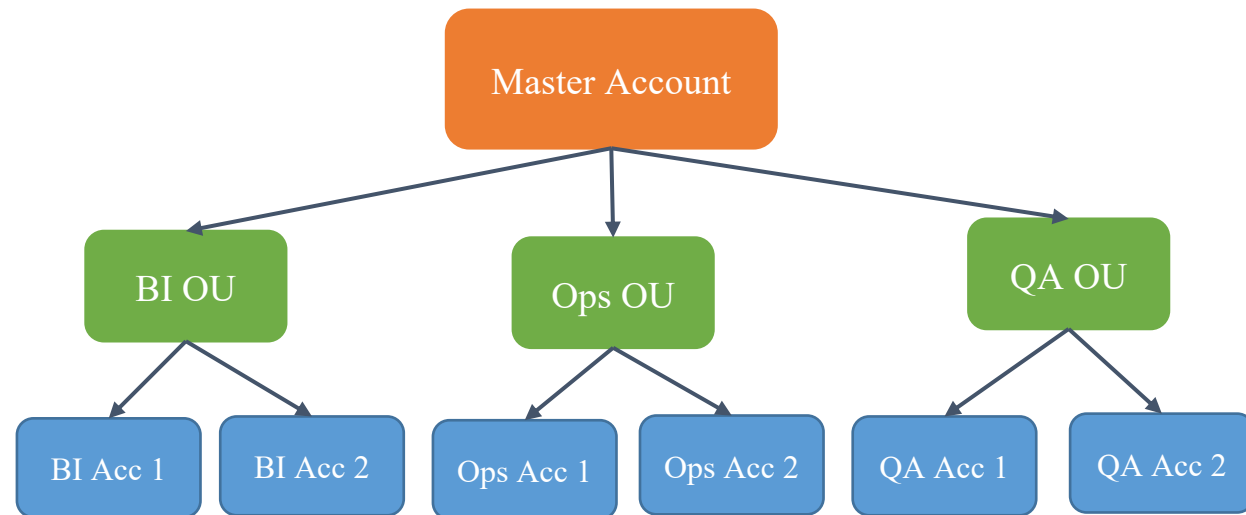
- Cho phép quản lý nhiều AWS accounts
- Bao gồm 1 AWS account chính gọi là master. Các accounts còn lại là account thành viên (member accounts)
- Hợp nhất Billing (consolidated billing) từ các accounts thành viên.
- Có các benefit từ việc sử dụng tài nguyên nhiều (tài nguyên sử dụng được tính từ tất cả các account thành viên – aggregate usages)
- Quản lý policy tập trung (tuân thủ – MFA, audit logs...)

Multi Account Strategies

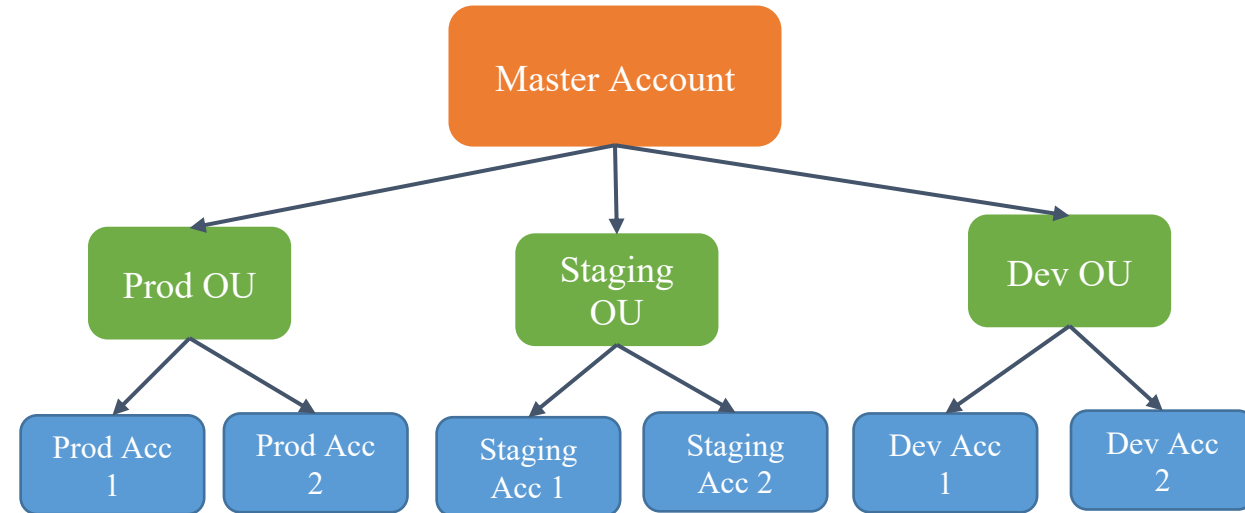
- Chiến lược chia các accounts theo tiêu chí:
 - Theo phòng ban (Departments Ex: BI/Ops/QA)
 - Theo bộ phận trả phí (Cost center Ex: HQ/Branch Office)
 - Theo dự án (Projects), theo môi trường (Environments Ex: Prod/Staging/Dev)
- Đánh tags để quản lý các tài nguyên (Tagging)
- Bật Cloud Trail trên tất cả accounts sau đó gửi logs tập trung về S3 phục vụ Audit
- Tạo Admin role cho các tác vụ quản lý

Organizational Units (OU)

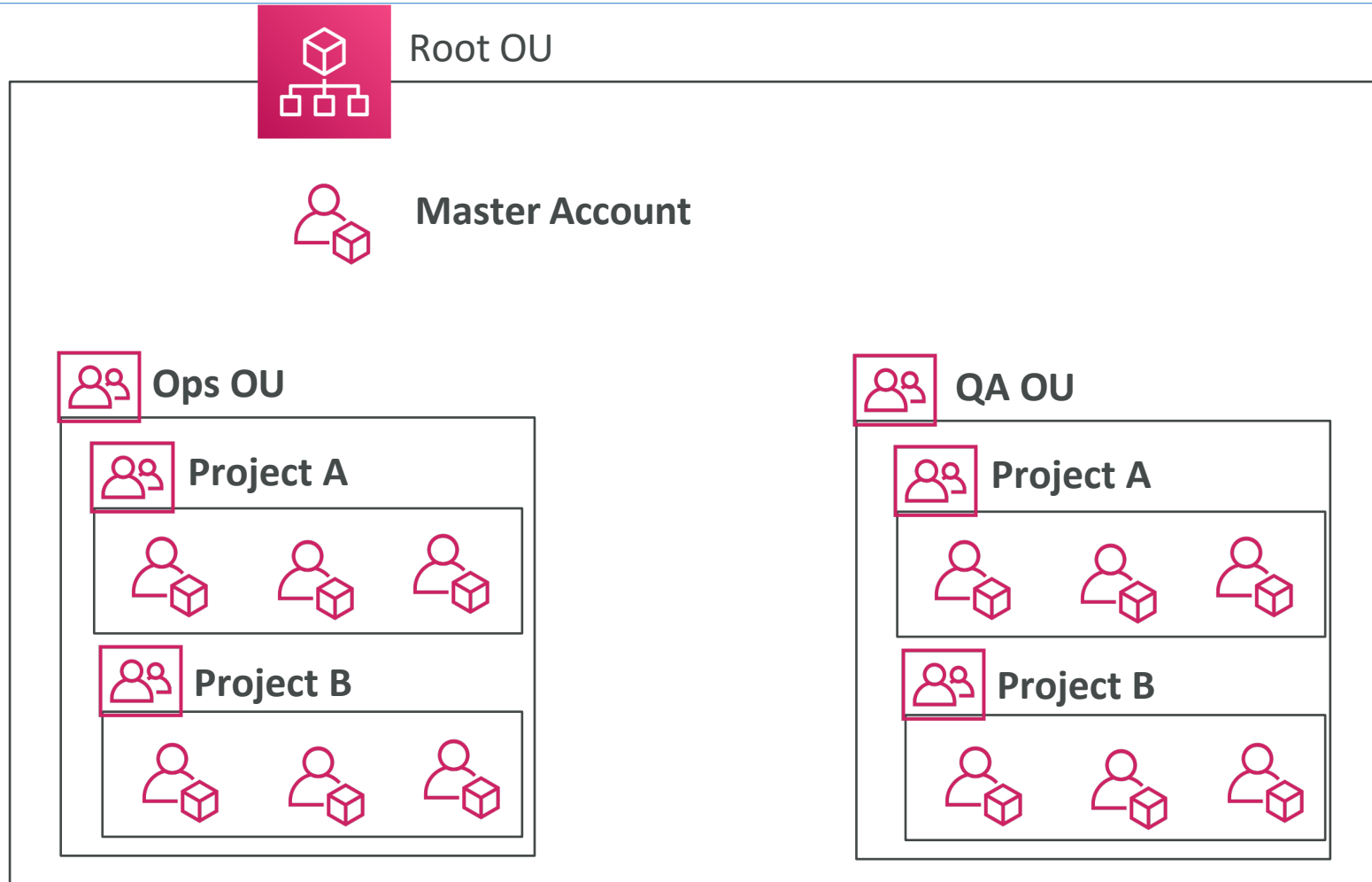
Department Unit



Environmental Unit



AWS Organizations

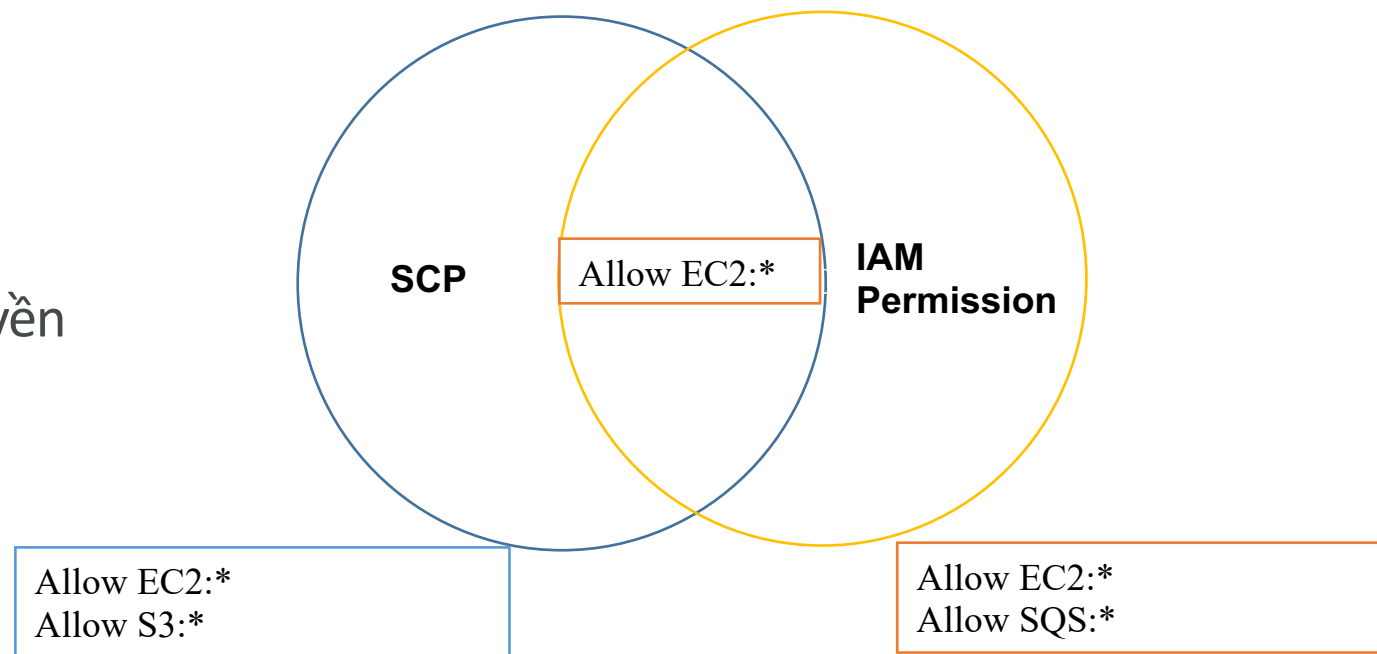


Service Control Policy (SCP)

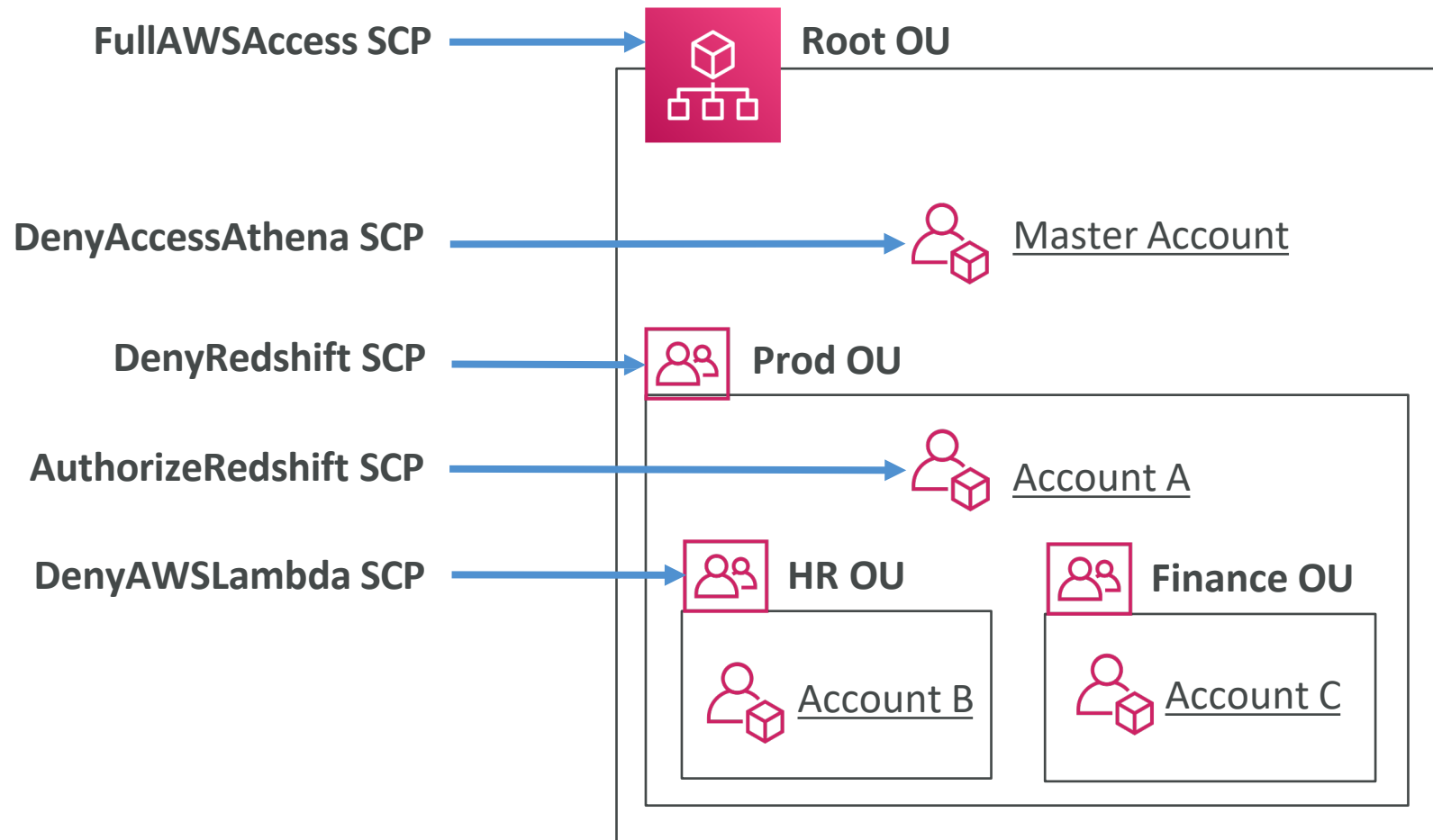
- Whitelist hoặc blacklist IAM actions
- Chỉ apply được ở OU hoặc Account level. Không apply được cho Master Account
- SCP được apply cho tất cả Users, Role của account (bao gồm cả Root account)
- SCP không ảnh hưởng tới service-linked roles
 - Service-linked role là các role được định nghĩa sẵn, và dùng cho để cho các service cụ thể có thể có quyền truy cập tới services khác
- SCP must have an explicit Allow (does not allow anything by default)

Service Control Policy (SCP)

- Định nghĩa tối đa các permission mà một thực thể (IAM identities) trong một account có thể có.
- SCP sẽ không thực hiện việc cấp quyền (grant permission)



Tính phân cấp của SCP (SCP hierarchy)

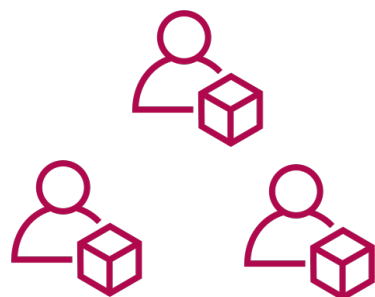


- **Master Account**
 - Can do anything
 - (no SCP apply)
- **Account A**
 - Can do anything
 - EXCEPT access Redshift (explicit Deny from OU)
- **Account B**
 - Can do anything
 - EXCEPT access Redshift (explicit Deny from Prod OU)
 - EXCEPT access Lambda (explicit Deny from HR OU)
- **Account C**
 - Can do anything
 - EXCEPT access Redshift (explicit Deny from Prod OU)

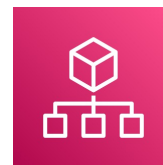
AWS RAM

RAM – Resource Access Manager

- Cho phép chia sẻ tài nguyên (resources) với các tài khoản AWS
- Có thể chia sẻ tài nguyên với bất kỳ AWS account nào trong cùng một Organization



Individual Account



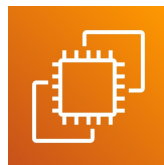
AWS Organizations

Resource Access Manager

- Các tài nguyên (AWS services) có thể được chia sẻ sử dụng RAM



Amazon VPC



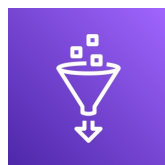
Amazon EC2



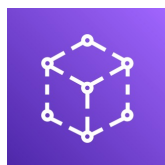
Amazon Aurora



EC2 Image Builder



AWS Glue



AWS App Mesh



AWS License Manager

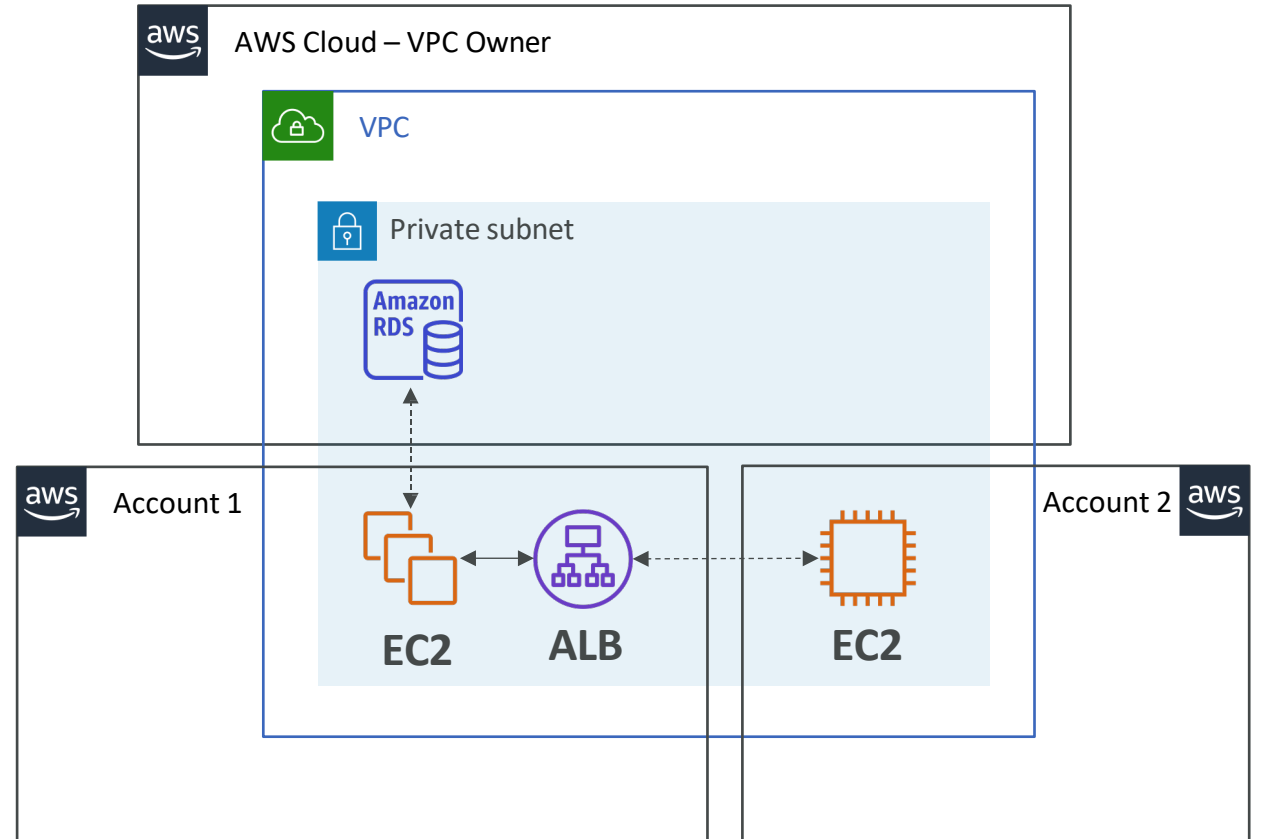


AWS CodeBuild

Reference: <https://docs.aws.amazon.com/ram/latest/userguide/shareable.html>

Resource Access Manager

- Mỗi account tham gia:
 - Chịu trách nhiệm về phần quản lý tài nguyên của account đó
 - Không thể thay đổi các tài nguyên (resources) của các account khác
- Sử dụng shared network
- Các ứng dụng của các accounts khác nhau có thể nói chuyện được với nhau.



Resource Cost for sharing VPC


- VPC của owner chịu chi phí cho NAT Gateway, VPC endpoint, Virtual Private Gateway
- Các accounts thành viên (được share) thì sẽ chịu chi phí cho các resources tạo ra từ các accounts này.

IAM Policies

Amazon Resource Name (ARN)

- ARN begin pattern:

arn:partition:service:region:account_id



aws|aws-cn s3|ec2|rds us-east-1|eu-west-1 123456789012

- Ví dụ:

arn:aws:iam::123456789012:user/mark

arn:aws:s3:::my_bucket/image.jpeg

arn:aws:dynamodb:us-east-1:123456789012:tables/mytables

- End with:

resource

resource_type/resource/qualifier

resource_type/resource:qualifier

resource_type:resource

resource_type:resource:qualifier

IAM Policies

- Sử dụng JSON document để định nghĩa các permissions
- Có 2 loại policy
 - **Identity policy:** Attach vào một thực thể (IAM identities) để định nghĩa quyền (permission) của thực thể đó. Ex: User, group, role
 - **Resource policy:** Attach vào một resources (s3, DynamoDB...) để định nghĩa xem thực thể nào có quyền truy cập vào resources này.

IAM Policies

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    1 {  
      ...  
    },  
    2 {  
      ...  
    },  
    3 {  
      ...  
    }  
  ]  
}
```

- Một policy là danh sách các statements
- Mỗi statement sẽ tương ứng với một API request

IAM Policies – Identity policy

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

- **Sid** là một id được đặt tùy ý.
- **Effect** là cho phép (**Allow**) hoặc từ chối (**Denied**)
- **Action** là hành động
- **Resource** là hành động được thực hiện trên resource nào?

IAM Policies – Resource base policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ResourceBasePolicy",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::cloudnut",
        "arn:aws:s3:::cloudnut/*"
      ],
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/hoa.nh"
        ]
      }
    }
  ]
}
```

- **Sid** là một id được đặt tùy ý.
- **Effect** là cho phép (**Allow**) hoặc từ chối (**Denied**)
- **Action** là hành động
- **Resource** là hành động được thực hiện trên resource nào?
- **Principal** là đối tượng được áp dụng policy này

Identity and Resource based policy



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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ResourceBasePolicy",
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::cloudnut",
        "arn:aws:s3:::cloudnut/*"
      ],
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/hoa.nh"
        ]
      }
    }
  ]
}
```

Policy Generator: <https://awspolicygen.s3.amazonaws.com/policygen.html>

Identity vs Resource based policy

Đặc điểm	Identity Policy	Resource base policy
Gắn vào đối tượng (Attach to)	IAM users, group or Role	Resources (S3, SQS, SNS...)
Gán quyền cho (Grant permission to)	Entities (Users/Group/Role) được gắn policy	Entities được chỉ định truy cập
Quản lý Policy	Inline và manage policy	Inline policy

IAM Condition

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NotIpAddress": {
        "aws:SourceIp": [
          "192.0.2.0/24",
          "203.0.113.0/24"
        ]
      }
    }
  },
}
```

aws:SourceIp: Giới hạn Client IP có thể tạo lời gọi API hoặc truy cập vào Console

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowOnlyInsideEU",
      "Effect": "Allow",
      "Action": [
        "ec2:*",
        "rds:*",
        "dynamodb:*"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": [
            "eu-central-1",
            "eu-west-1"
          ]
        }
      }
    }
  ]
}
```

Aws:RequestedRegion: Giới hạn region tại đó có thể tạo lời gọi API hay truy cập vào console

IAM Condition

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "StartStopIfTags",
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:DescribeTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:instance/*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Project": "DataAnalytics",
          "aws:PrincipalTag/Department": "Data"
        }
      }
    }
  ]
}
```

Restrict dựa vào tags

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAllActionsForEC2",
      "Effect": "Allow",
      "Action": "ec2:*",
      "Resource": "*"
    },
    {
      "Sid": "DenyStopAndTerminateWhenMFAIsNotPresent",
      "Effect": "Deny",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {
        "BoolIfExists": {"aws:MultiFactorAuthPresent": false}
      }
    }
  ]
}
```

Force MFA

Knowledge Check

Account ID: 123456789012

Identity-based policies

John Smith
Can List, Read
On Resource X

Carlos Salazar
Can List, Read
On Resource Y,Z

Mary Major
Can List, Read, Write
On Resource X,Y,Z

Zhang Wei
No policy

Resource-based policies

Resource X
John Smith: Can List, Read
Mary Major: Can List, Read

Resource Y
Carlos Salazar: Can List, Write
Zhang Wei: Can List, Read

Resource Z
Carlos Salazar: Denied access
Zhang Wei: Allowed full access

1. **John Smith** có những permission gì?
2. **Carlos Salazar** có những permission gì?

IAM Permission Boundaries

- Chỉ support cho users và roles (not groups)
- Tính năng nâng cao, cho phép giới hạn quyền tối đa một thực thể (user, role) có thể có

Example:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:*",
        "cloudwatch:*",
        "ec2:*"
      ],
      "Resource": "*"
    }
  ]
}
```

IAM Permission Boundary

+

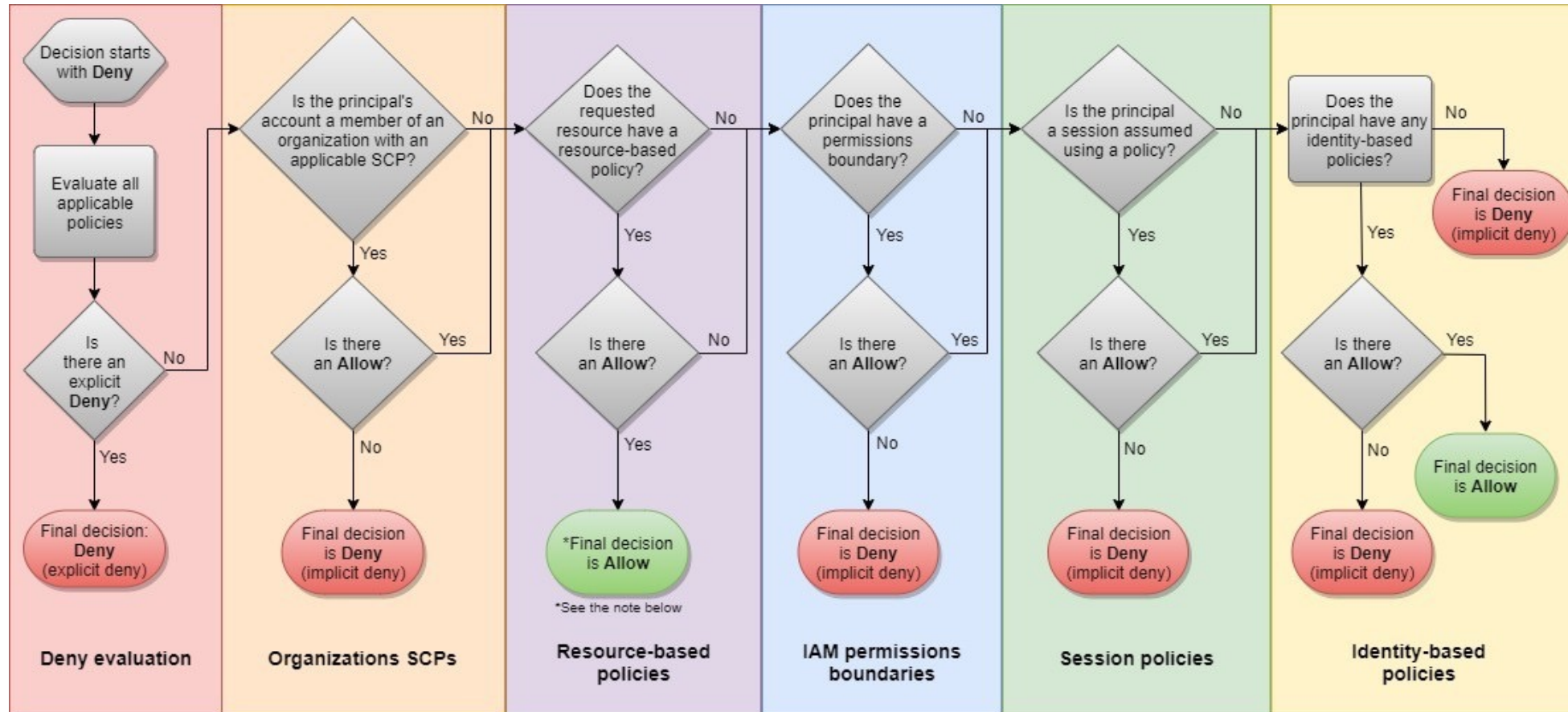
```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "iam:CreateUser",
    "Resource": "*"
  }
}
```

**IAM Permissions
Through IAM Policy**

=

No Permissions

IAM Policy Evaluation Logic



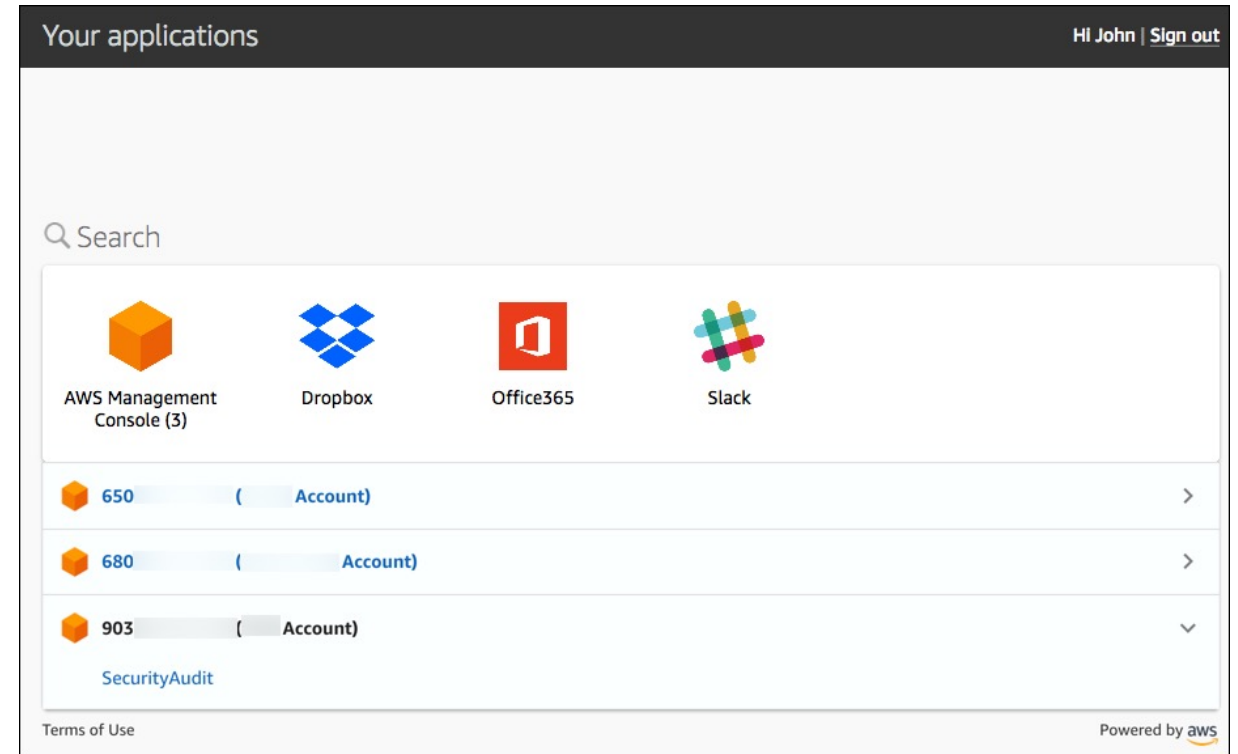
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html

- User: IAM => s3 full access
- SCP => whitelist {
 - Ec2:*
 - RDS:*
 - S3:*
- }
- S3: Bucket Policy {
 - Allow: bao.vq
- }
- Identity Policy => hoa.nh {
- }

AWS Single Sign On (SSO)

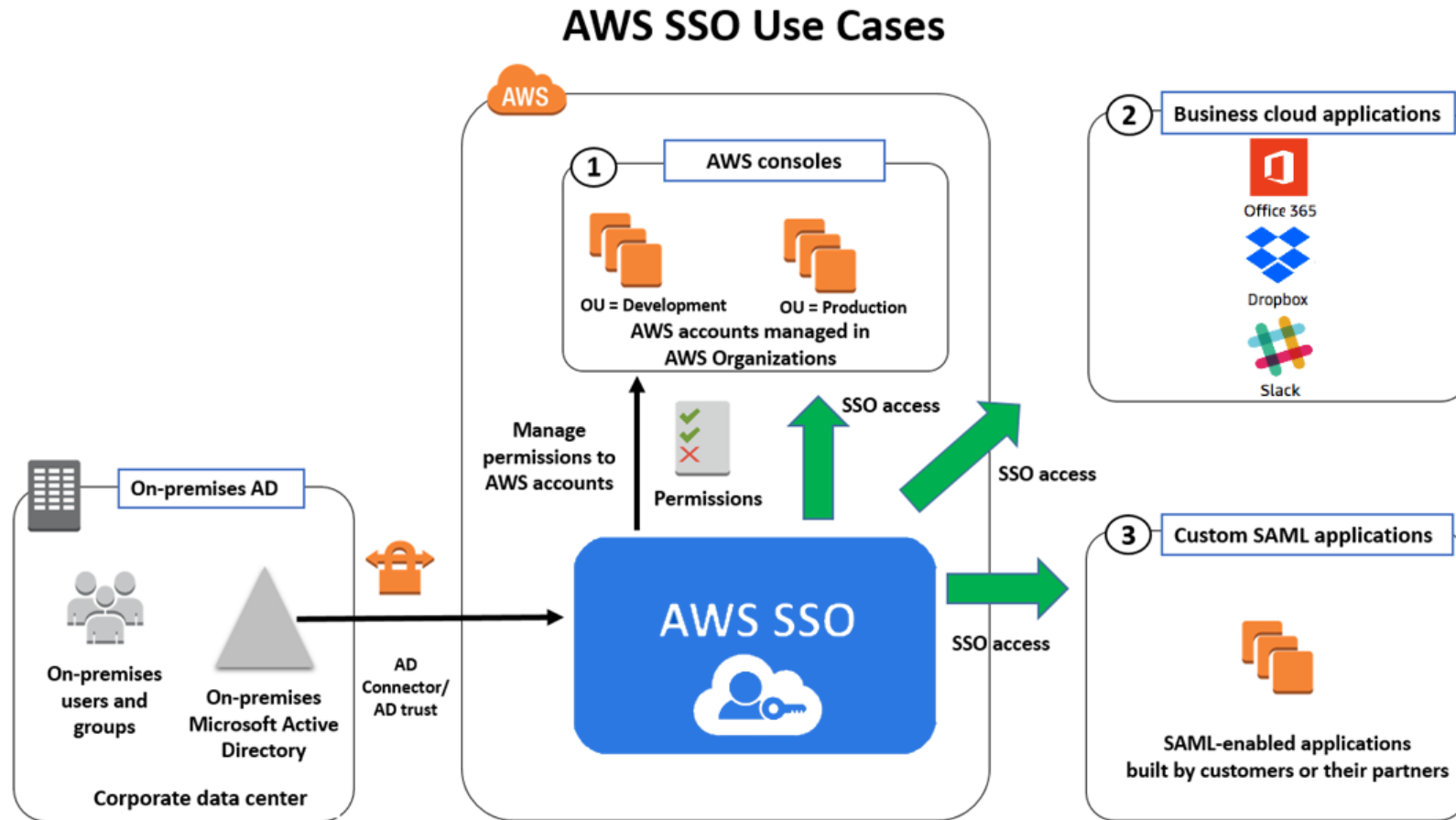
AWS SSO

- Quản lý tập trung SSO cho nhiều tài khoản AWS và ứng dụng.
- Có thể tích hợp với AWS organization
- Quản lý quyền tập trung.
- Audit tập trung sử dụng Cloudtrail



<https://aws.amazon.com/vi/blogs/security/introducing-aws-single-sign-on/>

AWS SSO – Use cases



AssumeRoleWithSAML vs SSO

