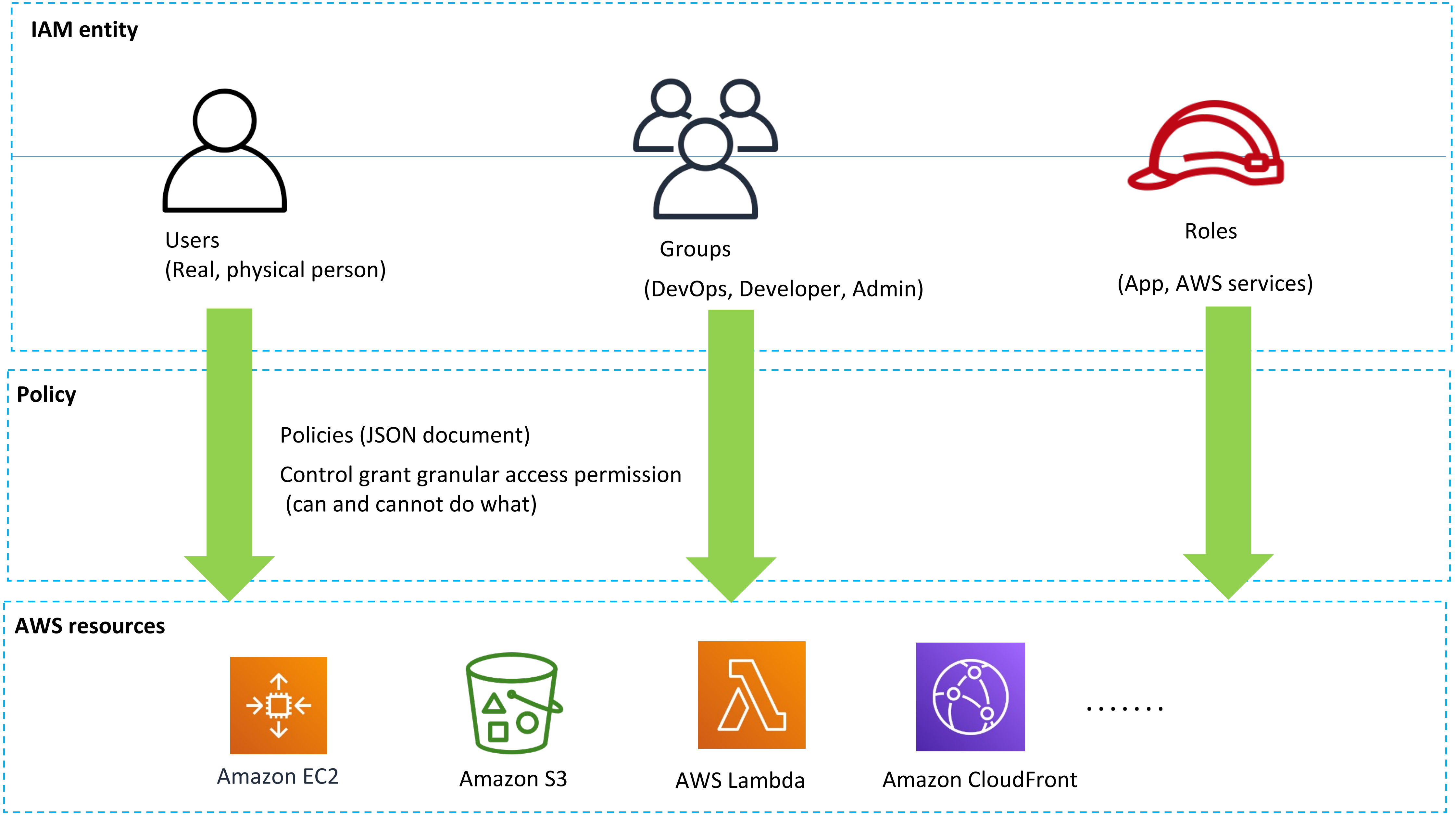
CloudNut
Learn Clouds in a Nutshell

Giới thiệu về IAM

Dịch vụ IAM?

- IAM viết tắt của **Identity Access Management**
- Là dịch vụ quản lý phân quyền, xác thực và là dịch vụ Core của AWS
- Các thực thể IAM (IAM entity): Users, Groups, Roles
- Tất cả các khía cạnh về Security của AWS đều nằm ở việc quản lý, phân quyền của IAM
- Các thực thể IAM (IAM Identity) được gắn với mội Policy để xác định quyền hạn của thực thể này
- Policy được viết dưới dạng JSON



IAM entity

Users
(Real, physical person)

Groups

(DevOps, Developer, Admin)

Roles

(App, AWS services)

Policy

Policies (JSON document)

Control grant granular access permission
(can and cannot do what)

AWS resources

Amazon EC2

Amazon S3

AWS Lambda

Amazon CloudFront

…….

Các tính năng của dịch vụ IAM

- Quản lý phân quyền tập trung cho tài khoản AWS
- Chia sẻ quyền hạn (permission) cho các tài khoản AWS khác
- Kiểm soát bụi mịn (Granular Permissions) chi tiết tới từng action
- Identity Federation (Active Directory, Facebook, LinkedIn…)
- Xác thực nhiều lớp (Multifactor Authentication)
- Thiết lập Password policy cho các tài khoản
- Hỗ trợ tích hợp với nhiều dịch vụ khác của AWS

IAM best practice

- Một người dụng thật (real user) ánh xạ với một IAM user
- Không sử dụng **Root user** cho các hoạt động quản trị thông thường
- Không bao giờ được nhúng IAM credentials vào trong source code
- Không sử dụng credentials của Root user
- Luôn luôn yêu cầu xác thực nhiều lớp (Multi-factor authentication)
- Luôn luôn áp dụng nguyên tắc **Quyền tối thiểu (Least Priviledge Principle)**

Knowledge Check

Which of the following is not a component of IAM?

A. Roles

B. Users

C. Groups

D. Organization Units

Knowledge Check

What is the default level of access a newly created IAM User is granted?

A. Read-only access to all AWS services.

B. No access to any AWS services.

C. Administrator access to all AWS services.

D. Power user access to all AWS services.

Knowledge Check

What is an additional way to secure the AWS accounts of both the root account and new users alike?

A. Implement Multi-Factor Authentication for all accounts.

B. Store the access key id and secret access key of all users in a publicly accessible plain text document on S3 of which only you and members of your organization know the.

C. Configure the AWS Console so that you can only log in to it from a specific IP Address range.

D. Configure the AWS Console so that you can only log in to it from your internal network IP address range.

Knowledge Check

A ___________ is a document that provides a formal statement of one or more permissions.

A. User

B. Group

C. Role

D. Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1638835896200",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket",
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::cloudnut.vn"
    }
  ]
}
```

Policy Generator tool:
https://awspolicygen.s3.amazonaws.com/policygen.html
Policy Evaluation:
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html

Knowledge Check

Q3: You are a security administrator working for a hotel chain. You have a new member of staff who has started as a systems administrator, and she will need full access to the AWS console. You have created the user account and generated the access key id and the secret access key. You have moved this user into the group where the other administrators are, and you have provided the new user with their secret access key and their access key id. However, when she tries to log in to the AWS console, she cannot. Why might that be?

A. You have not applied the "log in from console" policy document to the user. You must apply this first so that they can log in.

B. Your user is trying to log in from the AWS console from outside the corporate network. This is not possible.

C. You have not yet activated multi-factor authentication for the user, so by default they will not be able to log in.Tell her to log out and try logging back in again.

D. You cannot log in to the AWS console using the Access Key ID / Secret Access Key pair. Instead, you must generate a password for the user, and supply the user with this

Knowledge Check

Q3: You are a security administrator working for a hotel chain. You have a new member of staff who has started as a systems administrator, and she will need full access to the AWS console. You have created the user account and generated the access key id and the secret access key. You have moved this user into the group where the other administrators are, and you have provided the new user with their secret access key and their access key id. However, when she tries to log in to the AWS console, she cannot. Why might that be?

A. You have not applied the "log in from console" policy document to the user. You must apply this first so that they can log in.

B. Your user is trying to log in from the AWS console from outside the corporate network. This is not possible.

C. You have not yet activated multi-factor authentication for the user, so by default they will not be able to log in.Tell her to log out and try logging back in again.

D. You cannot log in to the AWS console using the Access Key ID / Secret Access Key pair. Instead, you must generate a password for the user, and supply the user with this

Knowledge Check

CloudNut
Learn Clouds in a Nutshell

Q3: You are a security administrator working for a hotel chain. You have a new member of staff who has started as a systems administrator, and she will need full access to the AWS console. You have created the user account and generated the access key id and the secret access key. You have moved this user into the group where the other administrators are, and you have provided the new user with their secret access key and their access key id. However, when she tries to log in to the AWS console, she cannot. Why might that be?

A. You have not applied the "log in from console" policy document to the user. You must apply this first so that they can log in.

B. Your user is trying to log in from the AWS console from outside the corporate network. This is not possible.

C. You have not yet activated multi-factor authentication for the user, so by default they will not be able to log in.Tell her to log out and try logging back in again.

D. You cannot log in to the AWS console using the Access Key ID / Secret Access Key pair. Instead, you must generate a password for the user, and supply the user with this