AWS IAM

Quản lý Định danh và Truy cập

AWS Identity and Access Management (IAM) là một dịch vụ web cho phép quản lý an toàn quyền truy cập đến các tài nguyên AWS. IAM giúp bảo vệ môi trường cloud của bạn bằng cách đảm bảo rằng chỉ các thực thể được phép mới có thể tương tác với các dịch vụ và dữ liệu của bạn.

Người dùng

Nhóm

Vai trò

Chính sách

Ngày tạo báo cáo: 2025-10-07

IAM RECAP - Tổng quan

AWS IAM là gì?

AWS Identity and Access Management (IAM) là một dịch vụ web cho phép kiểm soát an toàn quyền truy cập vào tài nguyên AWS.

Nó đảm bảo nguyên tắc đặc quyền tối thiểu và bảo mật toàn diện cho môi trường cloud của bạn.

Hàm chức năng chính

- **Định danh (Authentication)**: Xác định *ai* có thể truy cập vào tài nguyên AWS
- **Tác quyền (Authorization)**: Xác định *giảm* họ có thể thực hiện *trên những tài nguyên*

Nguyên tắc bảo mật

Nguyên tắc đặc quyền tối thiểu: Chỉ cấp quyền cần thiết cho việc thực hiện một tác vụ cụ thể

IAM giúp bạn áp dụng nguyên tắc này, giảm thiểu các rủi ro bảo mật bằng cách đảm bảo rằng chỉ các thực thể được ủy quyền mới có thể tương tác với các dịch vụ và dữ liệu của bạn.

Tại sao IAM quan trọng?

- Bảo vệ môi trường cloud của bạn khỏi truy cập trái phép
- Cho phép bạn quản lý quyền truy cập một cách tập trung
- Hỗ trợ việc tuân thủ các chính sách bảo mật và quy định
- Giúp bạn quản lý các khóa truy cập và quyền một cách hiệu quả

Thành phần chính của IAM

AWS IAM dựa trên bốn thành phần chính hoạt động cùng nhau để quản lý quyền truy cập đến tài nguyên.

Người dùng (Users)

Đại diện cho một người hoặc ứng dụng tương tác với AWS.

- Có thông tin đăng nhập riêng (tên người dùng và mật khẩu hoặc khóa truy cập)
- Thực hiện các hành động cụ thể trên tài nguyên AWS

Nhóm (Groups)

Tập hợp các người dùng IAM, đơn giản hóa quản lý quyền.

- Cho phép gán quyền cho nhiều người dùng cùng một lúc
- Khi thêm người dùng vào nhóm, họ tự động kế thừa tất cả các quyền của nhóm

Vai trò (Roles)

Các danh tính với quyền hạn có thể được đảm nhận tạm thời.

- Không liên kết vĩnh viễn với người dùng cụ thể
- Thiết kế để được đảm nhận bởi các thực thể đáng tin cậy
- Phục vụ nguyên tắc đặc quyền tối thiểu

Chính sách (Policies)

Các tài liệu JSON định nghĩa quyền được cấp cho người dùng, nhóm hoặc vai trò.

- Chỉ định các hành động được phép hoặc bị từ chối
- Áp dụng cho các tài nguyên cụ thể
- Có thể được gắn vào danh tính hoặc tài nguyên

Đây là các khối building block của chiến lược bảo mật IAM của bạn

Người dùng và Nhóm trong IAM

Người dùng IAM

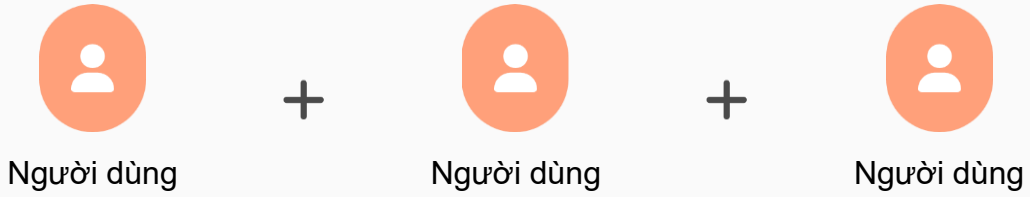
- Đại diện cho một người hoặc ứng dụng tương tác với AWS
- Mỗi người dùng có thông tin đăng nhập riêng (tên người dùng và mật khẩu, hoặc khóa truy cập)
- Thông tin đăng nhập này được sử dụng để xác thực danh tính

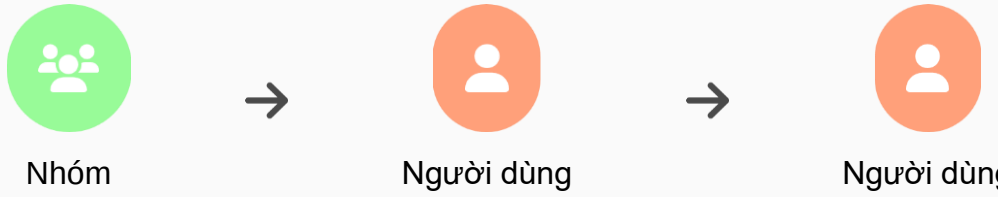
Ví dụ: Một nhà phát triển, một ứng dụng CI/CD, hoặc một người quản trị hệ thống

Nhóm IAM

- Là một tập hợp các người dùng IAM
- Gán quyền cho nhóm thay vì từng người dùng riêng lẻ là phương pháp được khuyến nghị
- Khi bạn thêm một người dùng vào một nhóm, họ tự động kế thừa tất cả các quyền được gán cho nhóm

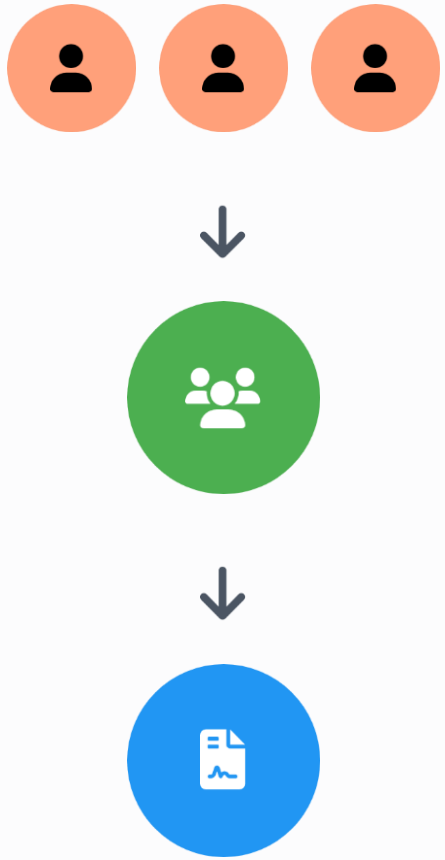
Ví dụ: Nhóm "Nhà phát triển", "Quản trị viên", hoặc "Hợp tác bên ngoài"





Thực tiễn tốt nhất cho Người dùng và Nhóm

Hướng dẫn phân quyền



Thực tiễn tốt nhất: Gán các chính sách vào nhóm thay vì từng người dùng riêng lẻ

Lợi ích của phương pháp này

- **Quản lý quyền truy cập đơn giản hơn**
  Thay vì phải quản lý quyền cho từng người dùng riêng lẻ, bạn chỉ cần quản lý quyền cho nhóm
- **Bảo đảm tính nhất quán**
  Khi bạn thêm một người dùng vào một nhóm, họ tự động kế thừa tất cả các quyền được gán cho nhóm
- **Thêm hoặc xóa người dùng dễ dàng**
  Bạn có thể thêm hoặc xóa người dùng khỏi nhóm mà không cần lo lắng về việc quản lý quyền riêng lẻ

Ví dụ thực tế

- **Trước:** Bạn có 10 người dùng và mỗi người cần 5 quyền khác nhau. Bạn phải quản lý 50 phân quyền riêng lẻ.
- **Sau:** Bạn tạo 2 nhóm với 5 quyền mỗi nhóm, sau đó thêm người dùng vào các nhóm. Bạn chỉ cần quản lý 10 phân quyền.

Cơ chế hoạt động của IAM

Khi một thực thể (chính thể) gửi một yêu cầu đến một dịch vụ AWS, hệ thống IAM xác định liệu yêu cầu đó nên được phép hay bị từ chối. Quá trình này bao gồm xác thực danh tính của chính thể và đánh giá tất cả các chính sách quyền hạn liên quan.

1. Yêu cầu

Người dùng, vai trò hoặc dịch vụ AWS gửi yêu cầu để thực hiện một hành động trên tài nguyên AWS.

2. Xác thực

AWS xác minh danh tính của chính thể đã gửi yêu cầu, bao gồm việc kiểm tra thông tin đăng nhập (tên người dùng, mật khẩu, khóa truy cập, v.v.).

3. Đánh giá chính sách

IAM xác định và đánh giá tất cả các chính sách liên quan áp dụng cho chính thể và tài nguyên.

4. Quyết định

Based on the evaluation of all policies, IAM makes a final decision to allow or deny the request.

Loại chính sách được đánh giá:

Chính sách dựa trên danh tính
Chính sách gắn vào người dùng, nhóm hoặc vai trò

Chính sách dựa trên tài nguyên
Chính sách gắn trực tiếp vào tài nguyên AWS

Ranh giới quyền hạn
Hạn chế tối đa các quyền có thể được cấp

SCP (Service Control Policies)
Quản lý quyền hạn ở cấp tổ chức

Chính sách phiên
Chính sách áp dụng cho phiên đăng nhập cụ thể

Mô hình luồng xử lý IAM

1. Yêu cầu

Người dùng hoặc dịch vụ gửi yêu cầu đến AWS

2. Xác thực

AWS xác minh danh tính của người gửi yêu cầu

3. Đánh giá ngữ cảnh

IAM thu thập thông tin về yêu cầu như hành động, tài nguyên, IP nguồn

4. Đánh giá chính sách

IAM đánh giá tất cả các chính sách liên quan đến người dùng và tài nguyên

5. Quyết định cuối cùng

IAM đưa ra quyết định cuối cùng: cho phép hoặc từ chối yêu cầu

Chi tiết về quyết định cuối cùng

- **Quyết định cho phép (Allow)**: Khi ít nhất một chính sách cho phép hành động và không có chính sách nào từ chối
- **Quyết định từ chối (Deny)**: Khi một chính sách cụ thể từ chối hành động hoặc không có chính sách nào cho phép

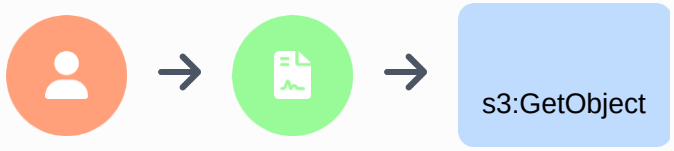
Chính sách dựa trên danh tính

Định nghĩa

Chính sách dựa trên danh tính là các chính sách bạn gắn vào một danh tính IAM (người dùng, nhóm hoặc vai trò). Chúng xác định các quyền mà danh tính đó có.

Các chính sách này cho phép bạn kiểm soát những hành động mà danh tính có thể thực hiện, trên những tài nguyên nào và trong những điều kiện nào.

Cách hoạt động



Danh tính IAM → Chính sách → Quyền truy cập tài nguyên

Thành phần chính

- **Danh tính**: Người dùng, nhóm hoặc vai trò
- **Hành động**: Ví dụ: s3:GetObject
- **Tài nguyên**: Ví dụ: bucket S3 cụ thể
- **Điều kiện**: Ví dụ: Địa chỉ IP nguồn

Ví dụ trường hợp sử dụng:

Cho phép một nhóm các nhà phát triển đọc các đối tượng từ một bucket S3 cụ thể.

Ví dụ về chính sách dựa trên danh tính

Tình huống sử dụng

Đối tượng: Nhóm nhà phát triển

Tài nguyên: Bucket S3 cụ thể

Hành động: Đọc các đối tượng

Bạn muốn cho phép nhóm nhà phát triển của bạn truy cập và đọc các file trong bucket S3 của bạn, nhưng không muốn họ có quyền ghi hoặc xóa bất kỳ thứ gì.

Lợi ích của chính sách dựa trên danh tính

- Đơn giản hóa quản lý quyền cho nhiều người dùng cùng lúc
- Cho phép bạn kiểm soát cụ thể các hành động mà nhóm có thể thực hiện
- Facilite theo dõi và giám sát hoạt động của nhóm

Triển khai chính sách

1. Tạo một nhóm IAM cho nhà phát triển

→ Điều này giúp bạn quản lý các quyền cho tất cả nhà phát triển cùng lúc

2. Tạo một chính sách IAM với quyền đọc S3

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::my-example-bucket",
        "arn:aws:s3:::my-example-bucket/*"
      ]
    }
  ]
}
```

3. Gắn chính sách đến nhóm IAM

→ Chính sách này sẽ áp dụng cho tất cả các thành viên của nhóm

Bây giờ, tất cả các nhà phát triển trong nhóm có thể đọc các đối tượng từ bucket S3 "my-example-bucket" mà không cần quyền ghi hoặc xóa bất kỳ thứ gì.

Chính sách dựa trên tài nguyên

Chính sách dựa trên tài nguyên là gì?

Chính sách dựa trên tài nguyên là các chính sách gắn trực tiếp vào tài nguyên AWS (ví dụ: bucket S3, hàng đợi SQS, khóa KMS).

Các chính sách này xác định những người dùng hoặc tài khoản nào được phép thực hiện các hành động trên tài nguyên đó.

Khác biệt với chính sách dựa trên danh tính

- Chính sách dựa trên tài nguyên gắn trực tiếp vào **tài nguyên** thay vì gắn vào danh tính
- Cho phép các thực thể từ **các tài khoản AWS khác** truy cập tài nguyên
- Quản lý quyền truy cập dựa trên **nguyên tắc đích** thay vì nguyên tắc nguồn

Cách hoạt động

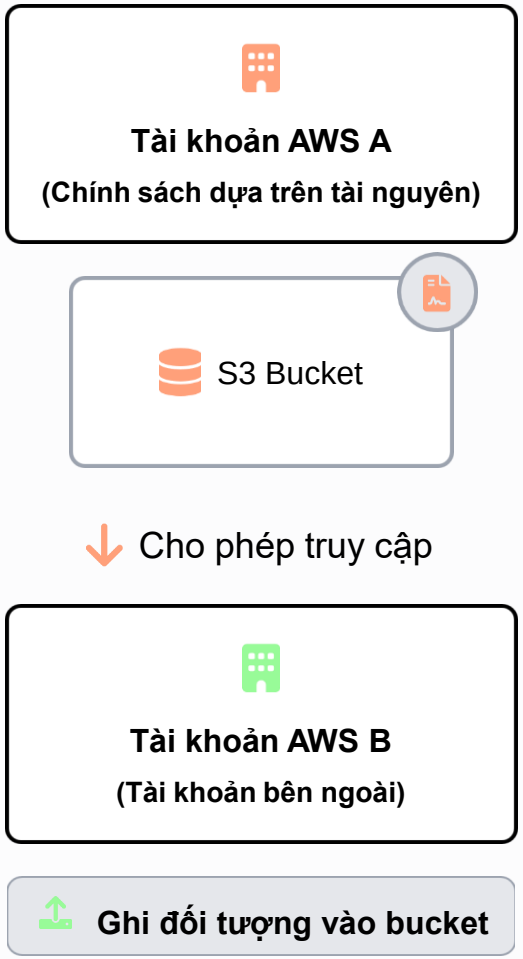
Ví dụ trường hợp sử dụng

Cho phép một tài khoản AWS bên ngoài ghi các đối tượng vào bucket S3 của bạn:

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": {"AWS": "account-id-ngoai"}, "Action": ["s3:PutObject"], "Resource": "arn:aws:s3:::my-bucket/*" } ] }
```

Ví dụ về chính sách dựa trên tài nguyên

Tình huống sử dụng



Chính sách Bucket S3

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      },
      "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl"
      ],
      "Resource": "arn:aws:s3:::my-example-bucket/*"
    }
  ]
}
```

Điểm chính

- Chính sách này được gắn trực tiếp vào bucket S3 (tài nguyên)
- Cho phép tài khoản AWS bên ngoài (123456789012) thực hiện hành động

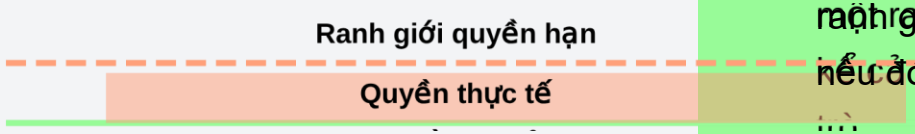
Ranh giới quyền hạn (Permission Boundaries)

Ranh giới quyền hạn là gì?

Một cơ chế bảo mật bổ sung trong IAM dùng để giới hạn quyền tối đa mà một danh tính (người dùng, nhóm hoặc vai trò) có thể có.

Cách hoạt động

- Tạo một "lớp bảo vệ bổ sung" xung quanh các quyền của danh tính
- Ngăn chặn việc mở rộng quyền vượt quá những gì đã được xác định trong ranh giới
- Hỗ trợ việc tuân thủ nguyên tắc đặc quyền tối thiểu



Lợi ích

- Giúp kiểm soát phân quyền và giảm thiểu rủi ro quyền hạn quá mức
- Thêm lớp bảo vệ bổ sung cho môi trường cloud của bạn
- Cho phép bạn thiết lập giới hạn cứng cho các quyền cụ thể
- Hỗ trợ việc quản lý quyền truy cập một cách hiệu quả và an toàn

Ví dụ sử dụng

Kết hợp với IAM Roles

Bạn có thể kết hợp ranh giới quyền hạn với các vai trò IAM để tạo ra các giải pháp bảo mật đa lớp. Ví dụ: một vai trò có thể được phép thực hiện hầu hết các hành động trên S3, nhưng một ranh giới quyền hạn có thể ngăn chặn việc xóa bucket S3, kể cả nếu đó là một hành động được phép trong chính sách vai trò.

IAM Role - Vai trò trong IAM

Vai trò IAM là gì?

Vai trò IAM là một danh tính IAM với các chính sách quyền được thiết kế để cấp quyền tạm thời cho các thực thể đáng tin cậy.

Không giống như người dùng hoặc nhóm, vai trò không được liên kết với người dùng cụ thể nào.

Các đặc điểm chính

- **Không liên kết vĩnh viễn**: Không giống như người dùng hoặc nhóm, vai trò không được liên kết với người dùng cụ thể nào
- **Chấp nhận tạm thời**: Được thiết kế để được giả định (assume) tạm thời bởi các thực thể đáng tin cậy
- **Quyền truy cập tạm thời**: Cung cấp thông tin xác thực bảo mật tạm thời, hỗ trợ nguyên tắc đặc quyền tối thiểu
- **Thực thể đáng tin cậy**: Có thể được giả định bởi người dùng IAM, ứng dụng, dịch vụ AWS hoặc người dùng федерated

Ví dụ minh họa

Vai trò IAM như "laissez-passer tạm thời"

Giả sử bạn là một người thăm dò (entity of trust). Thay vì cần có các khóa truy cập vĩnh viễn của riêng bạn, bạn nhận được một laissez-passer tạm thời (vai trò) mà cấp cho bạn quyền truy cập vào một tòa nhà (bộ phận) cụ thể.

Khi thời hạn hết hoặc laissez-passer được trả lại, quyền truy cập bị hủy bỏ.

Lợi ích của Vai trò IAM

- **Phân tách trách nhiệm**: Tách biệt danh tính người dùng khỏi quyền truy cập cụ thể
- **Quản lý quyền truy cập**: Thay vì chia sẻ khóa truy cập dài hạn, bạn cấp quyền tạm thời
- **Phân quyền dựa trên nhiệm vụ**: Cung cấp quyền truy cập dựa trên nhu cầu cụ thể của một nhiệm vụ

Các loại vai trò phổ biến

Vai trò Dịch vụ

Vai trò được tạo ra bởi các dịch vụ AWS để thực hiện các hành động trên tài nguyên của bạn.

- Cho phép dịch vụ AWS thực hiện các hành động cụ thể
- Thuộc tính chính: Service

Assume a Role - Đảm nhận vai trò

Quy trình đảm nhận vai trò

1. Thực thể
Người dùng, ứng dụng hoặc dịch vụ AWS cố gắng đảm nhận vai trò

2. Xác thực
IAM xác thực danh tính của thực thể và quyền hạn của nó để đảm nhận vai trò

3. AWS STS
AWS Security Token Service (STS) tạo ra thông tin xác thực tạm thời với quyền hạn của vai trò

AWS Security Token Service

- Dịch vụ STS tạo ra thông tin xác thực tạm thời cho các vai trò IAM
- Có thể cấp quyền hạn tùy chỉnh cho mỗi phiên
- Hỗ trợ cả cho người dùng IAM và các dịch vụ AWS

Thông tin xác thực tạm thời

Hạn sử dụng
Thông tin xác thực tạm thời có thời hạn sử dụng (mặc định 1 giờ, có thể được cấu hình)

Lợi ích
- Thực hiện **nguyên tắc đặc quyền tối thiểu**
- Tránh việc chia sẻ khóa truy cập dài hạn
- Cung cấp quyền truy cập tạm thời cho các ứng dụng hoặc dịch vụ

Các tình huống sử dụng IAM Role

Truy cập giữa tài khoản

Cho phép người dùng từ một tài khoản AWS truy cập vào tài nguyên của một tài khoản khác mà không cần chia sẻ khóa truy cập.

- Tạo vai trò trong tài khoản đích
- Gán chính sách quyền cho vai trò
- Người dùng từ tài khoản nguồn đảm nhận vai trò

Ứng dụng ideal: Tổ chức đa tài khoản hoặc hợp tác giữa các tài khoản

Xác thực liên kết

Cho phép người dùng xác thực thông qua một nhà cung cấp xác thực bên thứ ba (IdP) để truy cập vào tài nguyên AWS.

- Tạo vai trò федерated trong IAM
- Configure nhà cung cấp xác thực bên thứ ba
- Đảm nhận vai trò sau khi xác thực thành công

Ứng dụng ideal: Tích hợp với các hệ thống xác thực hiện có như Active Directory, Okta, hoặc Google

Quyền cho dịch vụ AWS

Cho phép bạn cấp quyền cho các dịch vụ AWS khác nhau để thực hiện các hành động trên tài nguyên của bạn.

- Tạo vai trò dịch vụ
- Chọn dịch vụ AWS (như Lambda, EC2, S3)
- Gán quyền cần thiết cho vai trò

Ứng dụng ideal: Khi bạn muốn cho phép một dịch vụ AWS truy cập vào tài nguyên khác của bạn

IAM Roles giúp bạn áp dụng nguyên tắc đặc quyền tối thiểu bằng cách cung cấp quyền tạm thời cho các thực thể cần thiết

Logique đánh giá chính sách

Nguyên tắc đánh giá chính sách IAM

Từ chối ngầm định mặc định

Mặc định, tất cả các yêu cầu đều bị từ chối ngầm định trừ khi có chính sách cụ thể cấp quyền.

Cho phép rõ ràng

Một câu lệnh Allow

Quy tắc ưu tiên trong đánh giá chính sách

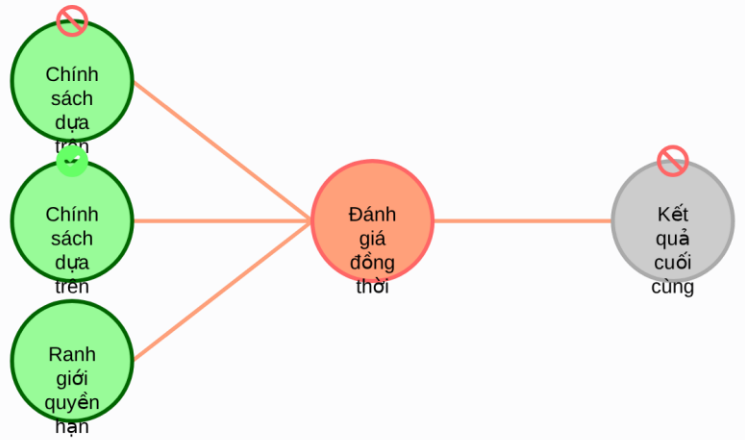
Các quy tắc cơ bản

Trong IAM, cách đánh giá chính sách quyết định xem một yêu cầu được phép hay bị từ chối. IAM đánh giá tất cả các chính sách liên quan đồng thời để đưa ra quyết định cuối cùng.

Quy tắc ưu tiên

- **Từ chối rõ ràng luôn được ưu tiên hơn cho phép rõ ràng**
- Chỉ cần tìm thấy một câu lệnh Từ chối trong bất kỳ chính sách nào, yêu cầu sẽ bị Từ chối
- Nếu không có câu lệnh Cho phép nào nhưng cũng không có Từ chối nào, yêu cầu bị Từ chối ngụ ý
- Thứ tự đánh giá các chính sách không ảnh hưởng đến quyết định cuối cùng

Luồng đánh giá



Ví dụ đánh giá

Từ chối rõ ràng
Trong chính sách

Cho phép rõ ràng
Trong chính sách

Không xác định
Không có câu lệnh

Kết luận: Trong cùng một ngữ cảnh, **từ chối rõ ràng** luôn được

Cấu trúc chính sách IAM

Cấu trúc chính sách IAM dạng JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::my-example-bucket",
        "arn:aws:s3:::my-example-bucket/*"
      ],
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "203.0.113.0/24"
        }
      }
    }
  ]
}
```

Thành phần chính của một chính sách IAM

Version

Phiên bản ngôn ngữ chính sách. Luôn nên sử dụng "2012-10-17" cho các chính sách mới.

Statement

Một khối chứa một hoặc nhiều câu lệnh quyền. Mỗi câu lệnh mô tả một tập hợp các quyền.

Sid (Statement ID)

Một định danh tùy chọn cho câu lệnh, dùng để phân biệt giữa các câu lệnh trong cùng một chính sách.

Effect

Xác định xem câu lệnh có cho phép (Allow

Ví dụ về cấu trúc chính sách IAM

```
" Version ":  "2012-10-17" ,
" Statement ":  [
    {
        " Sid ":  "VisualEditor0" ,
        " Effect ":  "Allow" ,
        " Action ":  [
            "s3:GetObject" ,
            "s3:ListBucket"
        ] ,
        " Resource ":  [
            "arn:aws:s3:::my-example-bucket" ,
            "arn:aws:s3:::my-example-bucket/*"
        ] ,
        " Condition ":  {
            " IpAddress ":  {
                " aws:SourceIp ":  "203.0.113.0/24"
            }
        }
    }
]
```

Version
Phiên bản ngôn ngữ chính sách. Luôn sử dụng "2012-10-17" cho các chính sách mới.

Statement
Một khối chứa một hoặc nhiều câu lệnh quyền.

Sid (Statement ID)
Một định danh tùy chọn cho câu lệnh.

Effect
Xác định xem câu lệnh có cho phép (Allow) hay từ chối (Deny) quyền truy cập.

Action
Liệt kê các hành động cụ thể của AWS mà chính sách cho phép hoặc từ chối.

Resource
Xác định các tài nguyên AWS mà hành động được áp dụng.

Condition
(Tùy chọn) Xác định các điều kiện mà quyền phải được đáp ứng

Tổng kết và Thực tiễn tốt nhất

Điểm chính về AWS IAM

- IAM là dịch vụ quản lý định danh và truy cập an toàn cho tài nguyên AWS
- Thành phần chính: Người dùng, Nhóm, Vai trò, và Chính sách
- Chính sách dựa trên danh tính và tài nguyên tạo nên quyền truy cập
- Quy tắc đánh giá chính sách quyết định việc chấp nhận hoặc từ chối quyền

Vai trò quan trọng của IAM

IAM đảm bảo nguyên tắc đặc quyền tối thiểu, giảm thiểu rủi ro bảo mật bằng cách:

- Quản lý quyền truy cập một cách tập trung
- Cho phép bạn kiểm soát ai có thể truy cập và làm gì
- Đảm bảo rằng chỉ các thực thể được ủy quyền mới có thể tương tác với các dịch vụ và dữ liệu

Thực tiễn tốt nhất cho IAM

- **Quản lý nhóm thay vì người dùng riêng lẻ**: Gắn các chính sách vào nhóm thay vì từng người dùng riêng lẻ để đơn giản hóa việc quản lý quyền
- **Áp dụng nguyên tắc đặc quyền tối thiểu**: Chỉ cấp quyền cần thiết cho việc thực hiện một tác vụ cụ thể
- **Sử dụng vai trò cho các ứng dụng và dịch vụ**: Thay vì sử dụng khóa truy cập dài hạn, hãy sử dụng vai trò để cung cấp quyền truy cập tạm thời
- **Đặt giới hạn cho quyền truy cập**: Sử dụng ranh giới quyền hạn (Permission Boundaries) để thêm lớp bảo vệ bổ sung

Kết luận

Quản lý IAM một cách hiệu quả là khía cạnh quan trọng của bảo mật trong môi trường AWS. Bằng cách hiểu rõ về các thành phần và cơ chế hoạt động của IAM, bạn có thể thiết lập một hệ thống quyền truy cập an toàn và hiệu quả cho môi trường cloud của mình.