**TÀI LIỆU VỀ AWS API GATEWAY TRÊN AWS CLOUD**

**Mục Lục**

1. **Giới Thiệu**
   * 1.1. **AWS API Gateway là gì?**
   * 1.2. **Ưu điểm của AWS API Gateway**
2. **Kiến Trúc Cơ Bản của AWS API Gateway**
   * 2.1. **Endpoint và API Gateway**
   * 2.2. **Integration và Resource Mapping**
3. **Tạo và Quản Lý API trên AWS API Gateway**
   * 3.1. **Bước 1: Tạo mới một API**
   * 3.2. **Bước 2: Cấu hình Resource và Method**
   * 3.3. **Bước 3: Cấu hình Integration**
   * 3.4. **Bước 4: Deploy API**
4. **Quản Lý Quyền Truy Cập với AWS Identity and Access Management (IAM)**
   * 4.1. **Quản lý Người Dùng và Nhóm**
   * 4.2. **Kết hợp với AWS Lambda và AWS Cognito**
5. **Quản Lý Thông Tin và Đơn Thư mục (Throttling và API Keys)**
   * 5.1. **Quy định giới hạn Request (Throttling)**
   * 5.2. **Sử dụng API Keys để Kiểm soát Quyền Truy Cập**
6. **Giám sát và Theo dõi với AWS CloudWatch**
   * 6.1. **Đặt Metrics và Logs**
   * 6.2. **Sử dụng AWS X-Ray để theo dõi API**
7. **Bảo mật API với Chữ Ký và Mã Hóa**
   * 7.1. **Sử dụng HTTPS**
   * 7.2. **Chữ Ký và Xác Minh Chữ Ký (Signature and Signature Verification)**
8. **Tổng Kết và Hướng Dẫn Thêm**
   * 8.1. **Tổng Kết**
   * 8.2. **Hướng Dẫn Thêm và Tài Nguyên Tham Khảo**

**1. Giới Thiệu**

**1.1. AWS API Gateway là gì?**

AWS API Gateway là dịch vụ quản lý và triển khai API (Application Programming Interface) trên AWS Cloud. Nó giúp tạo ra các endpoint HTTP hoặc HTTPS cho các ứng dụng, cho phép chúng tương tác với các dịch vụ khác trên nền tảng AWS hoặc bên ngoài.

**1.2. Ưu Điểm của AWS API Gateway**

* **Dễ sử dụng:** Giao diện quản lý đơn giản, giúp người phát triển dễ dàng tạo và quản lý API.
* **Mở rộng linh hoạt:** Tích hợp tốt với nhiều dịch vụ AWS khác nhau và hỗ trợ nhiều loại kiến trúc API.
* **Bảo mật mạnh mẽ:** Cung cấp các tính năng bảo mật như xác thực, ủy quyền và quản lý khóa API.

**2. Kiến Trúc Cơ Bản của AWS API Gateway**

**2.1. Endpoint và API Gateway**

* **Endpoint:** Địa chỉ URL mà các ứng dụng khác có thể gửi các request HTTP hoặc HTTPS đến.
* **API Gateway:** Dịch vụ quản lý các endpoint, định tuyến request đến các tài nguyên khác nhau và thực hiện các hành động xử lý.

**2.2. Integration và Resource Mapping**

* **Integration:** Liên kết các endpoint của API với các dịch vụ khác trên AWS hoặc bên ngoài.
* **Resource Mapping:** Xác định cách request và response được chuyển đổi giữa các endpoint và các dịch vụ.

**3. Tạo và Quản Lý API trên AWS API Gateway**

**3.1. Bước 1: Tạo mới một API**

Truy cập AWS Console, chọn AWS API Gateway, và thực hiện bước tạo mới API.

**3.2. Bước 2: Cấu Hình Resource và Method**

Xác định các resource (tài nguyên) mà API của bạn sẽ hỗ trợ, và các HTTP methods (GET, POST, PUT, DELETE, v.v.) được ánh xạ tới resource đó.

**3.3. Bước 3: Cấu Hình Integration**

Liên kết resource với các dịch vụ khác nhau bằng cách cấu hình integration. Điều này có thể là AWS Lambda, Amazon S3, hoặc bất kỳ dịch vụ nào hỗ trợ HTTP.

**3.4. Bước 4: Deploy API**

Sau khi cấu hình xong, triển khai API để tạo ra các endpoint và cho phép ứng dụng khác truy cập.

**4. Quản Lý Quyền Truy Cập với AWS Identity and Access Management (IAM)**

**4.1. Quản Lý Người Dùng và Nhóm**

Sử dụng IAM để tạo người dùng và nhóm, và cấu hình quyền truy cập vào API Gateway.

**4.2. Kết Hợp với AWS Lambda và AWS Cognito**

Tích hợp với AWS Lambda để thực hiện logic xử lý, và sử dụng AWS Cognito để quản lý danh tính và xác thực người dùng.

**5. Quản Lý Thông Tin và Đơn Thư mục (Throttling và API Keys)**

**5.1. Quy Định Giới Hạn Request (Throttling)**

Sử dụng cơ chế throttling để kiểm soát số lượng request mà một client có thể gửi trong một khoảng thời gian nhất định.

**5.2. Sử Dụng API Keys để Kiểm Soát Quyền Truy Cập**

Tạo và quản lý API keys để kiểm soát quyền truy cập vào API, đặc biệt là khi sử dụng cho các ứng dụng bên ngoài.

**6. Giám Sát và Theo Dõi với AWS CloudWatch**

**6.1. Đặt Metrics và Logs**

Sử dụng AWS CloudWatch để giám sát và theo dõi các metric quan trọng, cũng như xem logs của request và response.

**6.2. Sử Dụng AWS X-Ray để Theo Dõi API**

Kích hoạt AWS X-Ray để theo dõi các bước thực hiện của request khi đi qua các dịch vụ.

**7. Bảo Mật API với Chữ Ký và Mã Hóa**

**7.1. Sử Dụng HTTPS**

Kích hoạt HTTPS để bảo vệ dữ liệu truyền tải giữa client và API Gateway.

**7.2. Chữ Ký và Xác Minh Chữ Ký (Signature and Signature Verification)**

Thực hiện chữ ký và xác minh chữ ký để đảm bảo tính toàn vẹn và xác thực của request.

**8. Tổng Kết và Hướng Dẫn Thêm**

**8.1. Tổng Kết**

AWS API Gateway cung cấp một giải pháp mạnh mẽ cho việc quản lý và triển khai API trên AWS Cloud. Nó giúp đơn giản hóa quy trình, tăng tính mở rộng và cung cấp nhiều tính năng bảo mật.

**8.2. Hướng Dẫn Thêm và Tài Nguyên Tham Khảo**

Để biết thêm chi tiết và hướng dẫn thực hành, hãy tham khảo tài liệu chính thức của AWS API Gateway tại <https://docs.aws.amazon.com/apigateway/>.