AWS Cloud for beginner

Instructor: Linh Nguyen

(Engineering Consultant, AWS Cloud Solution Architect)

Level: Beginner

“Không có việc gì khó, chỉ sợ không biết làm”

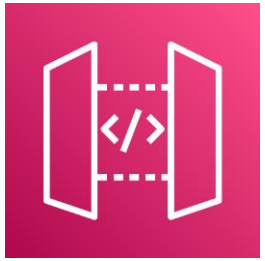
API Gateway & Cognito

Target

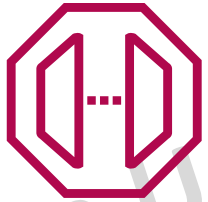
- Hiểu được API Gateway là gì? Tính năng, usecases
- API Gateway Pricing model
- Authentication for API Gateway
- Kết hợp API Gateway & Lambda để tạo một REST API đơn giản.
- API Gateway Advanced options
- Cognito là gì? Usecase
- Kết hợp Cognito làm Authorzer cho API Gateway.

API Gateway là gì?

Một dịch vụ API Gateway được cung cấp bởi AWS. Nó cung cấp một cách đơn giản để xây dựng, quản lý và bảo mật các **RESTful API** hoặc **WebSocket**. AWS API Gateway là một dịch vụ quan trọng trong kiến trúc dựa trên các dịch vụ của AWS (**AWS-based microservices architecture**) và thường được sử dụng cùng với các dịch vụ AWS khác như AWS Lambda, EC2, S3, Amazon DynamoDB.



Amazon API Gateway

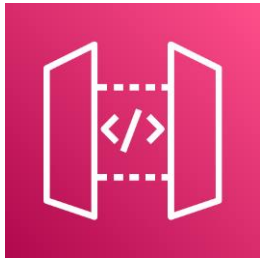


Endpoint

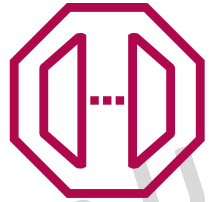
API Gateway là gì?

AWS API Gateway cung cấp các tính năng:

- Cho phép thiết kế và phát triển API RESTful hoặc WebSocket thông qua web GUI.
- Điều phối các yêu cầu API đến các hệ thống hoặc dịch vụ khác nhau.
- Authen/Author request tới các API.
- Quản lý và giám sát các yêu cầu API, vd số lượng request, response time...
- AWS API Gateway cũng cung cấp các tính năng bảo mật, bao gồm chứng thực và ủy quyền các yêu cầu API và mã hóa secure communication giữa các hệ thống khác nhau.



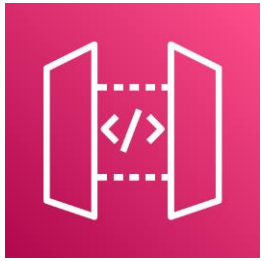
Amazon API Gateway



Endpoint

Đặc trưng của API Gateway

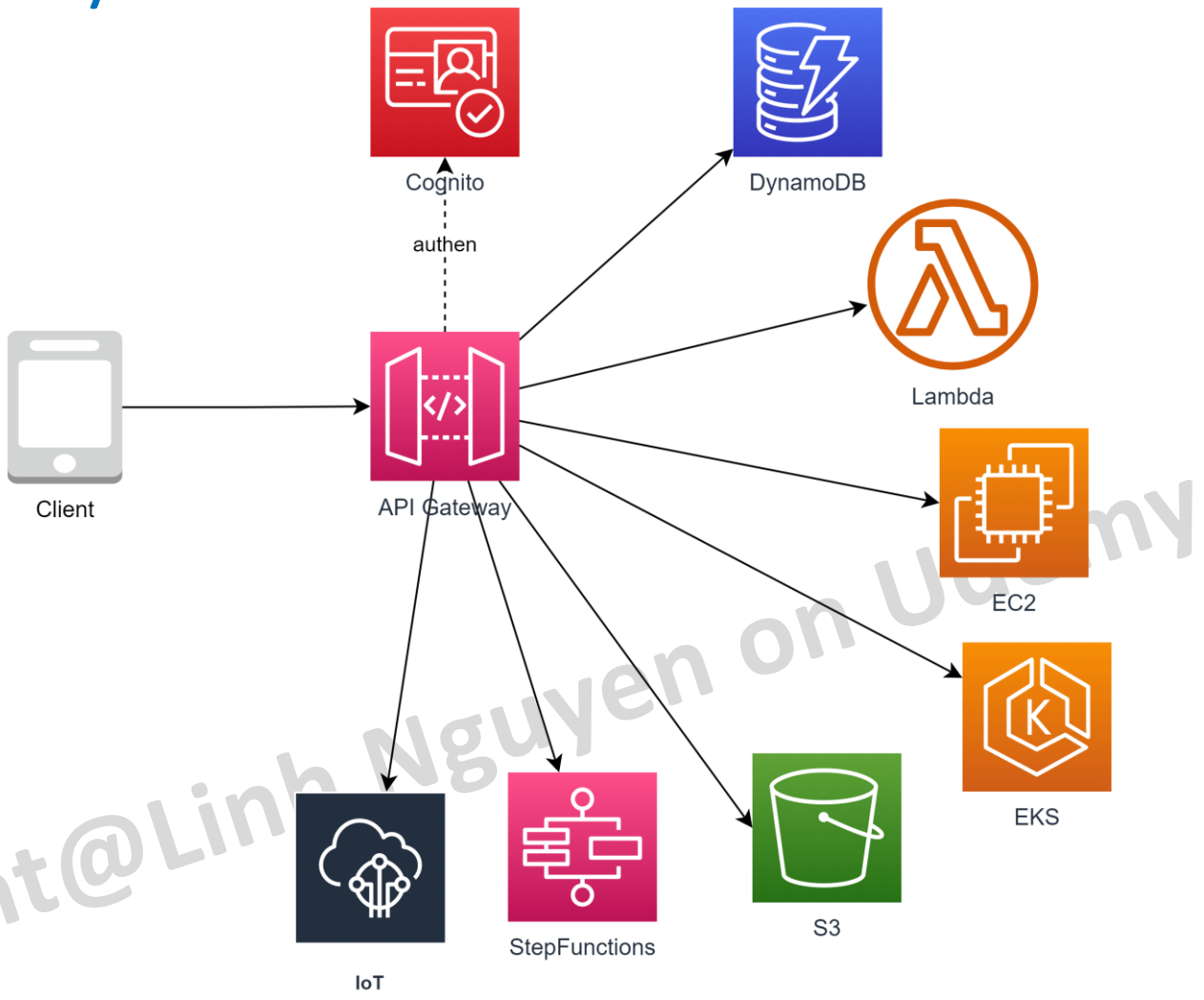
- Là một fully managed service của AWS.
- Khả năng scale và High Availablity không giới hạn.
- Zero idle cost
- Easy to setup
- Dễ dàng kết hợp với các dịch vụ khác như CloudWatch, WAF cho mục đích monitor & security.



Amazon API Gateway

Hệ sinh thái API Gateway

API Gateway là một service chủ yếu có nhiệm vụ nhận request của client sau đó forward tới các service phía sau.



Khi nào nên sử dụng API Gateway?

API Gateway phù hợp cho những bài toán sau

- Kiến trúc Micro-service sử dụng lambda làm backend
- Backend API cho hầu hết các use case (web API, IoT)
- Gateway nhận data trực tiếp từ client sau đó lưu vào DynamoDB (DB First)
- Web Socket cho những hệ thống realtime communication.

API Gateway Pricing

API Gateway là một dịch vụ có idle cost = 0. Người dùng chỉ trả tiền cho chi phí chạy thực tế, cụ thể

Với REST API

- Số lượng request (Vd Singapore region:$ 4.25/1M requests)
- Data transfer out ($/GB)
- Caching size tính theo GB/hour

Với Web socket

- Message number (đối với Web socket). Vd $1.15/1M message với block 32KB.
- Connection minutes: $0.288/1M connection minutes

Authentication cho API Gateway

API Gateway cung cấp 2 phương thức authen tích hợp trực tiếp (authorizer) thường được sử dụng đó là:

- **Cognito Authorizer**

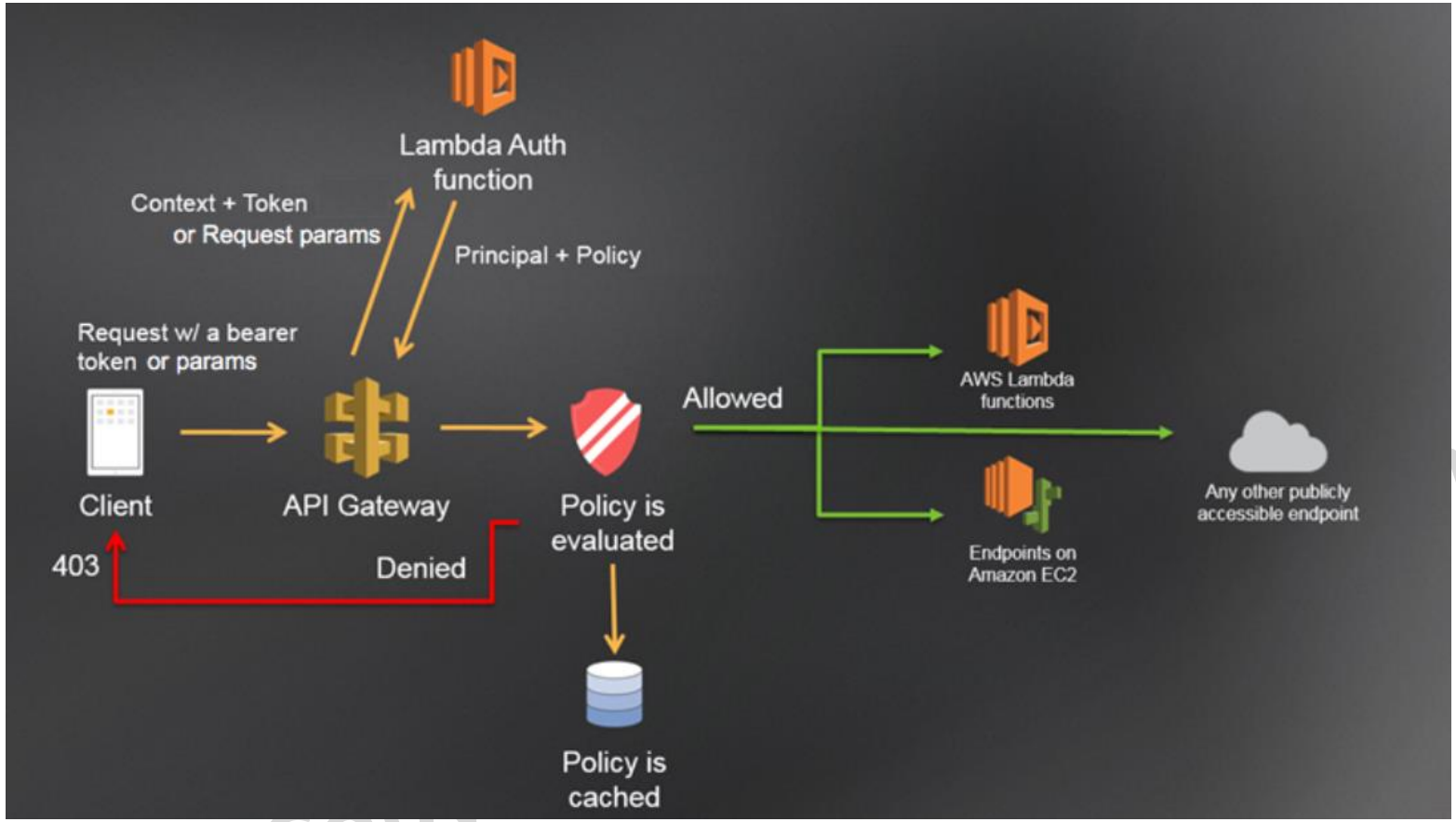
Liên kết trực tiếp với một Cognito User Pool sử dụng làm authorizer. Khi access API, client passing trực tiếp token lấy được thông qua login với Cognito, API Gateway sẽ check token và allow access nếu token hợp lệ.

- **Lambda Authorizer** (custom authorizer)

Khi sử dụng loại authorizer này, bạn sẽ tự implement logic authen trên Lambda. Có 2 hình thức là authen dựa vào TOKEN (JWT) hoặc request parameter based (VD username/password).

Authentication cho API Gateway

Mô hình sử dụng Lambda làm authorizer

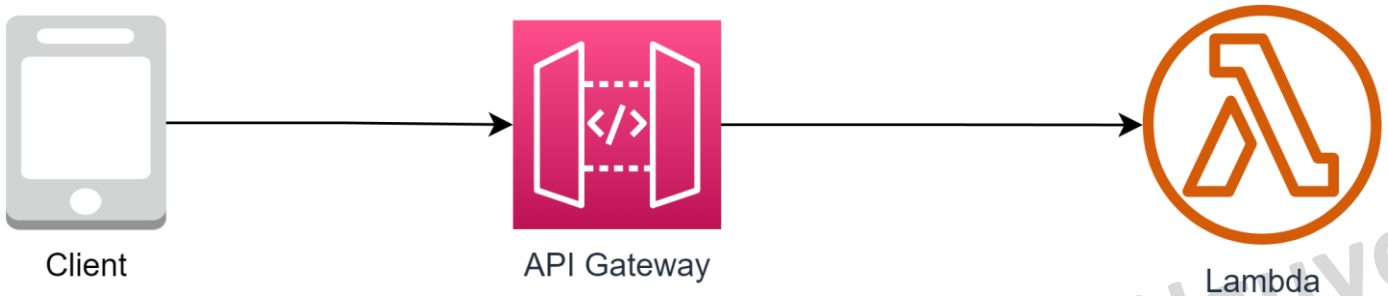


Nguồn: https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-use-lambda-authorizer.html

Lab 1 – API Gateway + lambda backend

Yêu cầu: Tạo 1 API Gateway có chức năng nhận request từ client, forward tới Lambda backend xử lý sau đó response.

Sơ đồ hệ thống:



Lab 1 – API Gateway + lambda backend

Steps:

1. Tạo một Lambda function với code mẫu (Python)
2. Tạo một API Gateway
3. Tạo resource & path vd /calculate method POST, forward sang lambda
4. Deploy API Gateway thành một stage vd **dev**
5. Sử dụng Postman để test API

API Gateway advanced option

- Throttle
- API Key
- Stage and Canary deployment
- Custom domain

Giới thiệu Cognito

Cognito là gì?

AWS Cognito là một dịch vụ quản lý **danh tính** và **xác thực** người dùng của Amazon Web Services (AWS). Dịch vụ này cho phép bạn tạo ra các ứng dụng web và di động an toàn với khả năng xác thực người dùng, phân quyền, và đăng nhập với nhiều tùy chọn như user account, Social login hoặc đăng nhập qua Identity Provider.

Amazon Cognito

Tính năng của Cognito

Tính năng cơ bản của Cognito

- Đăng ký & Xác thực người dùng sd username/pw/email hoặc tài khoản mạng xã hội.
- Phân quyền người dùng vào các ứng dụng hoặc tài nguyên
- Xác thực email/số điện thoại.
- Tích hợp với các dịch vụ khác (API Gateway, Lambda) để xây dựng ứng dụng.
- Hỗ trợ cho ứng dụng di động (iOS,Android) thông qua SDK
- Cognito sync: sync data giữa các mobile device với nhau
- Advanced Security: giám sát & phân tích truy cập của user để phát hiện và ngăn chặn truy cập bất thường (optional).

Amazon Cognito

Pricing của Cognito

Pricing của Cognito dựa trên

- Số lượng Monthly Active User. VD ở Singapore là $0.0055/MAU (càng lên cao càng rẻ)
- User sign in thông qua SAML hoặc OIDC: $0.015/MAU
- Tính năng Advance Security: $0.05/MAU nếu enable
- SMS trong trường hợp gửi message MFA: Tuỳ theo khu vực.

Amazon Cognito

Hạn chế của Cognito

- Số lượng User trên 1 user pool: 40M (contact AWS nếu muốn tăng)
- Số lượng user pool tối đa: default 1,000, max 10,000
- Custom attribute: 50

Hạn chế về tần suất Admin API call vd:

- UserCreation: 50 RPS. Tăng thêm 10RPS cho mỗi 1 triệu MAU
- AdminUserRead: 120 RPS. Tăng thêm 40 RPS cho mỗi 1 triệu MAU
- RevokeToken: 120 RPS. Tăng thêm 40 RPS cho mỗi 1 triệu MAU
- UserUpdate: 25 RPS không thể tăng thêm.
- ...

Amazon Cognito

See more at: https://docs.aws.amazon.com/cognito/latest/developerguide/limits.html

Hạn chế của Cognito

Lưu ý về cơ chế verify token của Cognito

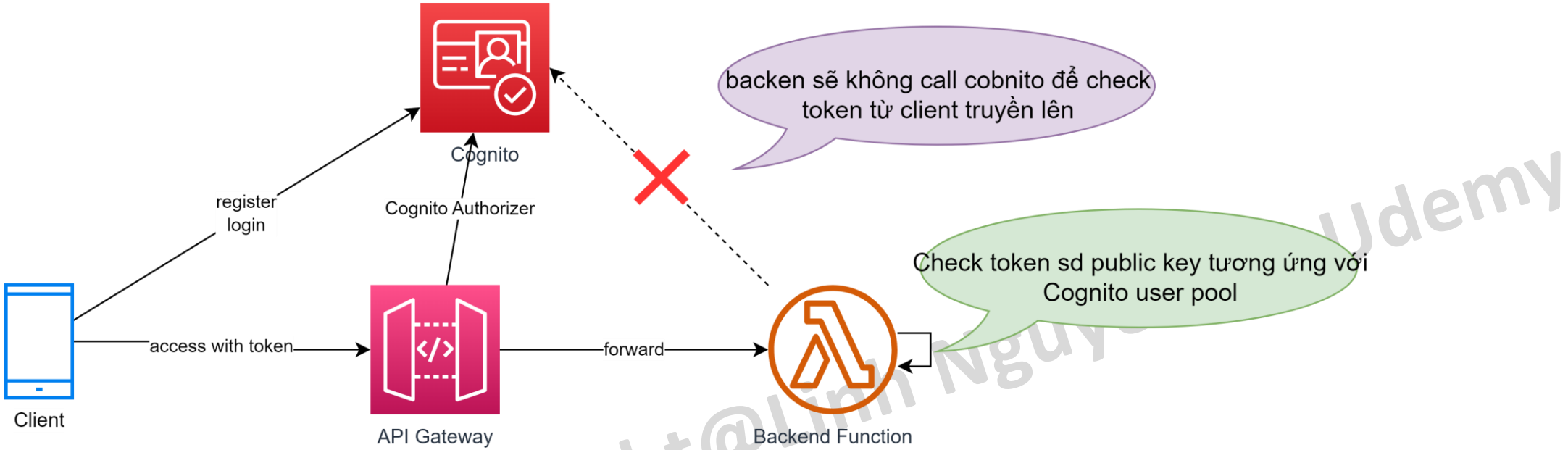
JWT token do Cognito phát hành thông thường sẽ dùng client side verify (sử dụng Public Key do Cognito cung cấp. **Lưu ý AWS không cung cấp private key của Cognito*).

Việc này đồng nghĩa với việc nếu user logout thì access-token vẫn có hiệu lực cho tới khi expired (vd 30 min).

Nếu hệ thống có nhu cầu revoke access-token đã phát hành khi user có các hành động như change password, log-out thì không thể thực hiện với Cognito. Tất nhiên có thể workaround sử dụng các kỹ thuật Caching/DB.

Hạn chế của Cognito

Lưu ý về cơ chế verify token của Cognito



Lab 2- Cognito basic operation

Yêu cầu

- Login to AWS -> Cognito
- Tạo một user pool với các thông tin cơ bản
- Username, cho phép dùng email đã verify làm username
- Cho phép tuỳ chọn username (user có thể change)
- Tạo thử một user
- Tạo thử một group, gán user vào group

Lab 3- Sử dụng Cognito Hosted UI

- Tạo một App Client (nếu chưa tạo). *Chú ý bật Implicit grant
- Cấu hình Hosted UI của Cognito User pool.
- Sử dụng Hosted UI để tiến hành Login, Lấy access token
- Sử dụng JWT Tool để decrypt token xem bên trong có gì.

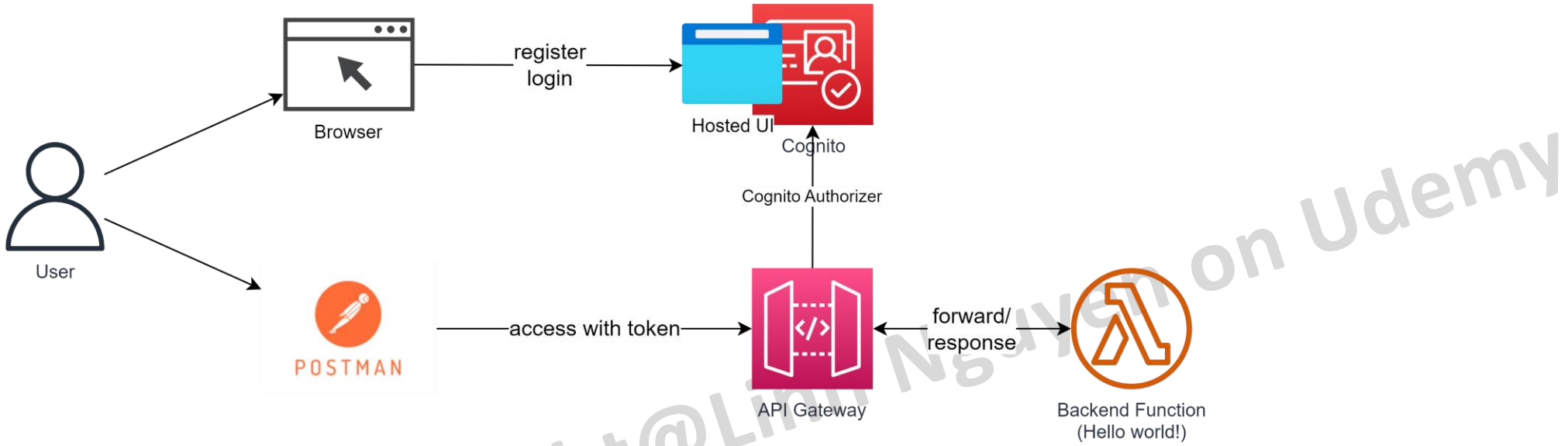
Lab 4- Combine Cognito with API Gateway

Yêu cầu đã có một API Gateway chạy được với method đơn giản

- Cấu hình Authorizer cho API Gateway sử dụng Cognito user pool đã tạo
- Sử dụng hosted UI (Lab3) để login và lấy token.
- Thử truy cập API mà không có token -> Access Denied
- Thử truy cập API có token lấy được từ step trước -> Allow.

Lab 4- Combine Cognito with API Gateway

Sơ đồ hệ thống



Clear resources

Trên AWS console, thực hiện các steps sau:

1. Lambda có Idle cost = 0, có thể xoá hoặc giữ lại để tham khảo.
2. API Gateway có Idle cost = 0, có thể xoá hoặc giữ lại để tham khảo.
3. Cognito User pool: Có thể giữ lại tham khảo do vẫn nằm trong free tier.