Devops on AWS for beginner

Instructor – Linh Nguyen

Engineering Consultant, AWS Cloud Solution Architect

Ôn lại kiến thức về AWS

Mục tiêu chương này sẽ nhằm hệ thống hoá lại các kiến thức về AWS đã được giới thiệu ở level Associate.
Phần nào các bạn chưa nắm chắc có thể Google hoặc ôn lại các khoá tương ứng.

"Không có việc gì khó, chỉ sợ không biết làm!"

Global architect of AWS

AWS có mặt ở những khu vực nào?

Quy mô của AWS

- 31 Regions
- 99 Availability zones
- 450+ Points of Presence
- 400+ Edge Locations and 13 Regional Edge Caches

Ngoài ra:

- Có mặt tại 245 Countries
- 32 Local zones
- 115 Direct Connect Locations

*Nguồn: https://aws.amazon.com/about-aws/global-infrastructure/

Định nghĩa region

Region là một khái niệm để mô tả một khu vực vật lý trên thế giới mà AWS cung cấp các dịch vụ điện toán đám mây. Mỗi AWS Region là một khu vực độc lập với cơ sở hạ tầng và các dịch vụ.

Mỗi region sẽ bao gồm nhiều Availability Zone (AZ).

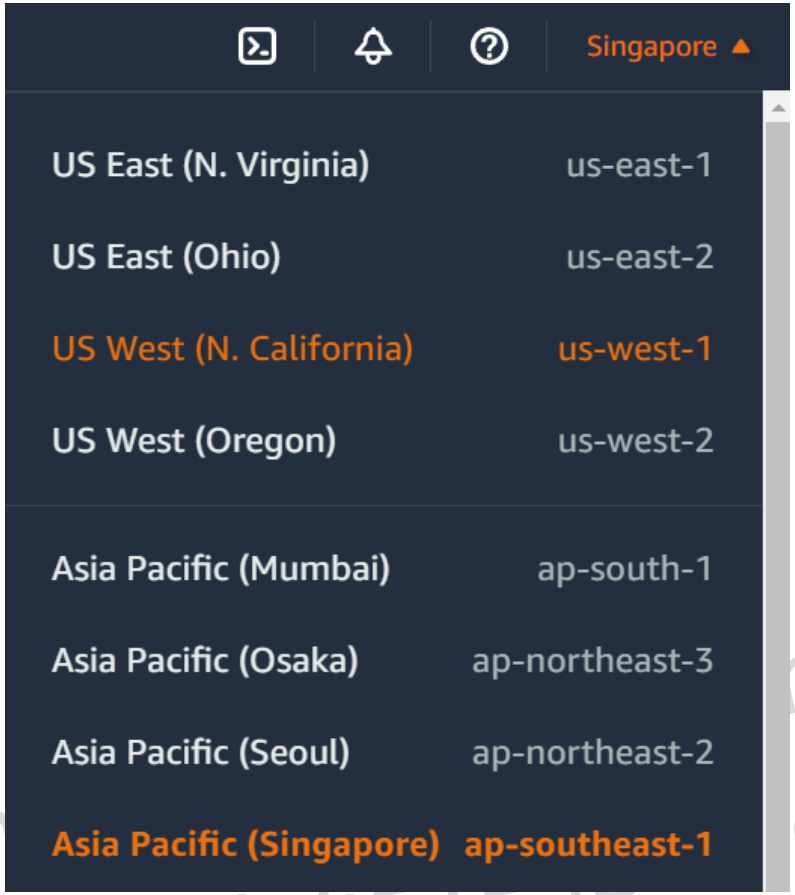
Lựa chọn region

Việc lựa chọn region để triển khai hệ thống dựa trên:

- Tuân thủ compliance (tiêu chuẩn ngành, luật pháp v.v)
- Gần người dùng để mang lại trải nghiệm tốt nhất (giảm độ trễ).
- Dịch vụ cần sử dụng có ở region đó không?
- Giá cả của các dịch vụ.

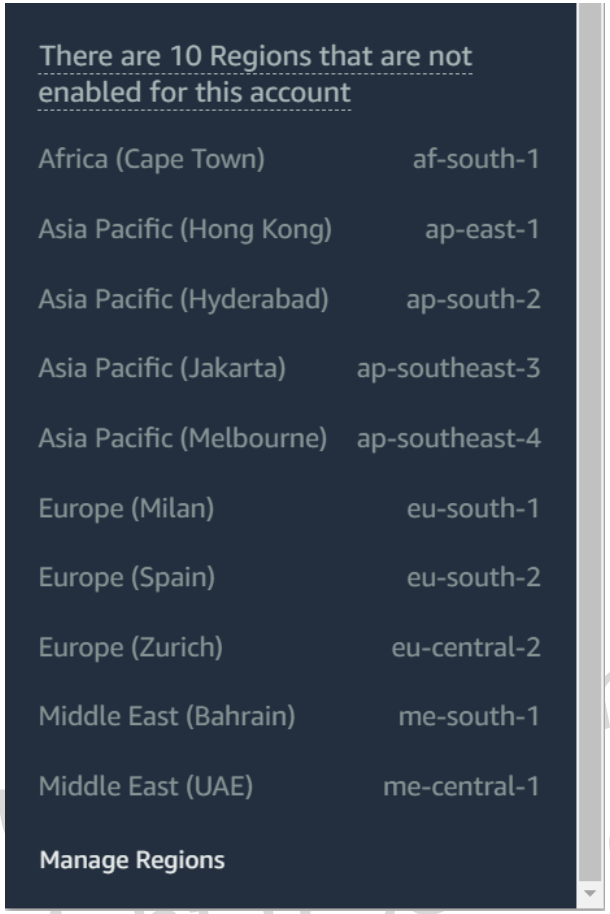
Tiêu chí chọn region cho hệ thống

Switch sang đúng region trước khi bắt đầu bất kỳ thao tác nào



Tiêu chí chọn region cho hệ thống

Một số region không available by-default, cần enable để có thể sử dụng.



Private region – Ex China region

AWS có mặt tại China tuy nhiên không thể trực tiếp switch sang region này trên Console. Cần phải đăng ký với AWS một account riêng biệt và tách biệt hoàn toàn với các account thông thường.

Availability Zone là gì?

Một Availability Zone (AZ) là một trung tâm dữ liệu hoặc một nhóm các trung tâm dữ liệu nằm trong cùng một khu vực vật lý, nhưng được phân bổ và vận hành hoàn toàn độc lập. Mỗi AZ có thể có các tài nguyên đám mây như máy chủ ảo, ổ cứng, network, security, các dịch vụ khác nhau, cùng với các tài nguyên hỗ trợ khác như hệ thống cấp điện.

Việc sử dụng nhiều Availability Zone giúp đảm bảo tính khả dụng (HA) cao cho ứng dụng, tăng tính bảo mật và bảo đảm dữ liệu được lưu trữ và xử lý an toàn. Nếu một AZ bị sự cố hoặc ngừng hoạt động, các tài nguyên đám mây được triển khai tại các AZ khác vẫn có thể hoạt động bình thường, giúp đảm bảo rằng dịch vụ của bạn vẫn hoạt động một cách liên tục và đáng tin cậy.

Availability Zone là gì?

Mỗi region của AWS thường có ít nhất 3 AZs.

VD: ở region Singapore(ap-southeast) sẽ có các zone:

- ap-southeast-1a
- ap-southeast-1b
- ap-southeast-1c

Hầu hết các service của AWS đều hỗ trợ triển khai trên Multi-AZ để đảm bảo nâng cao High Avalibility của hệ thống.

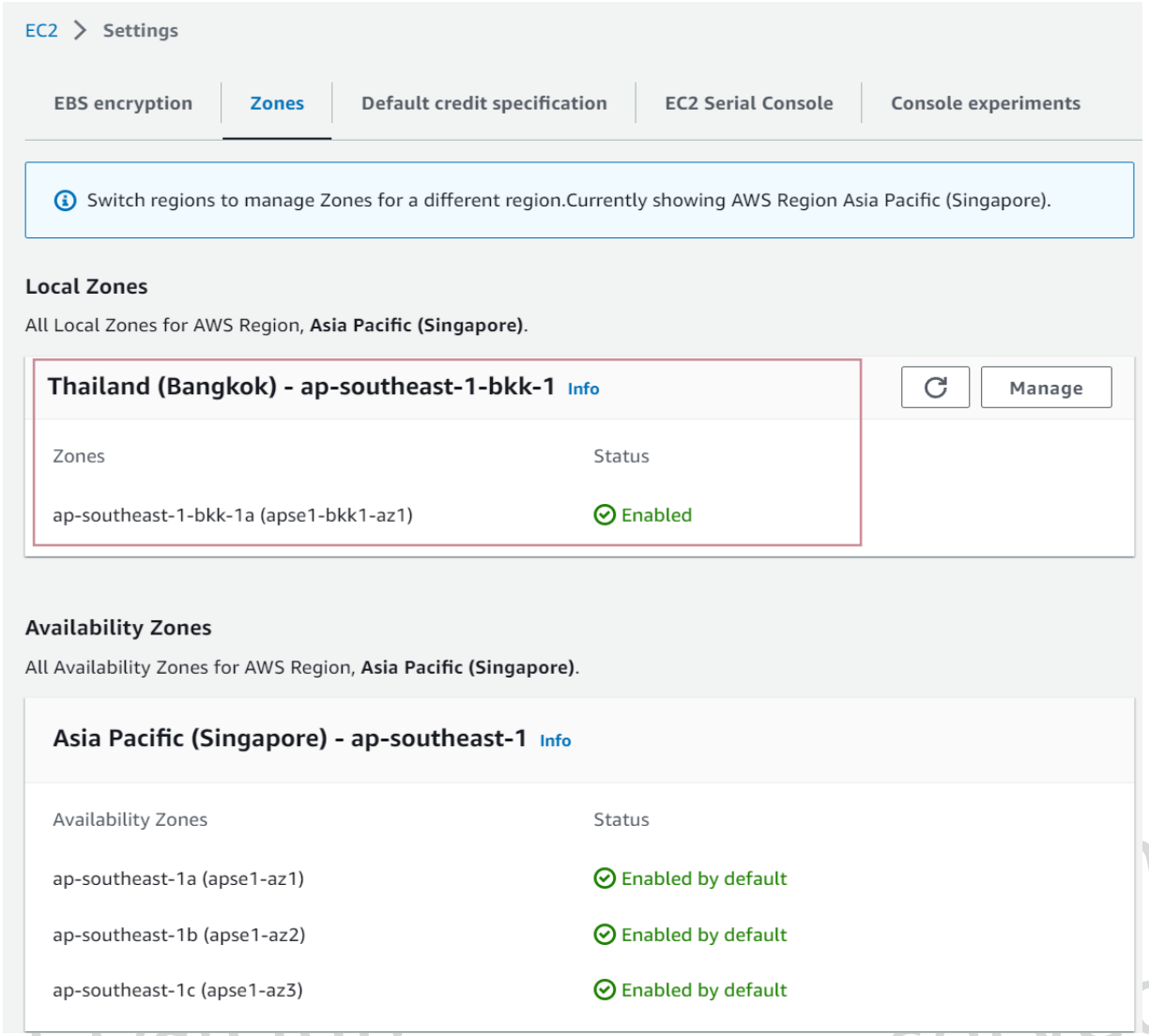
Local Zone

AWS Local Zones are a type of infrastructure deployment that places compute, storage, database, and other select AWS services close to large population and industry centers.

https://aws.amazon.com/about-aws/global-infrastructure/localzones/locations/

Local Zone

Enable local zone trên console
*Chỉ bật khi thật sự có nhu cầu.

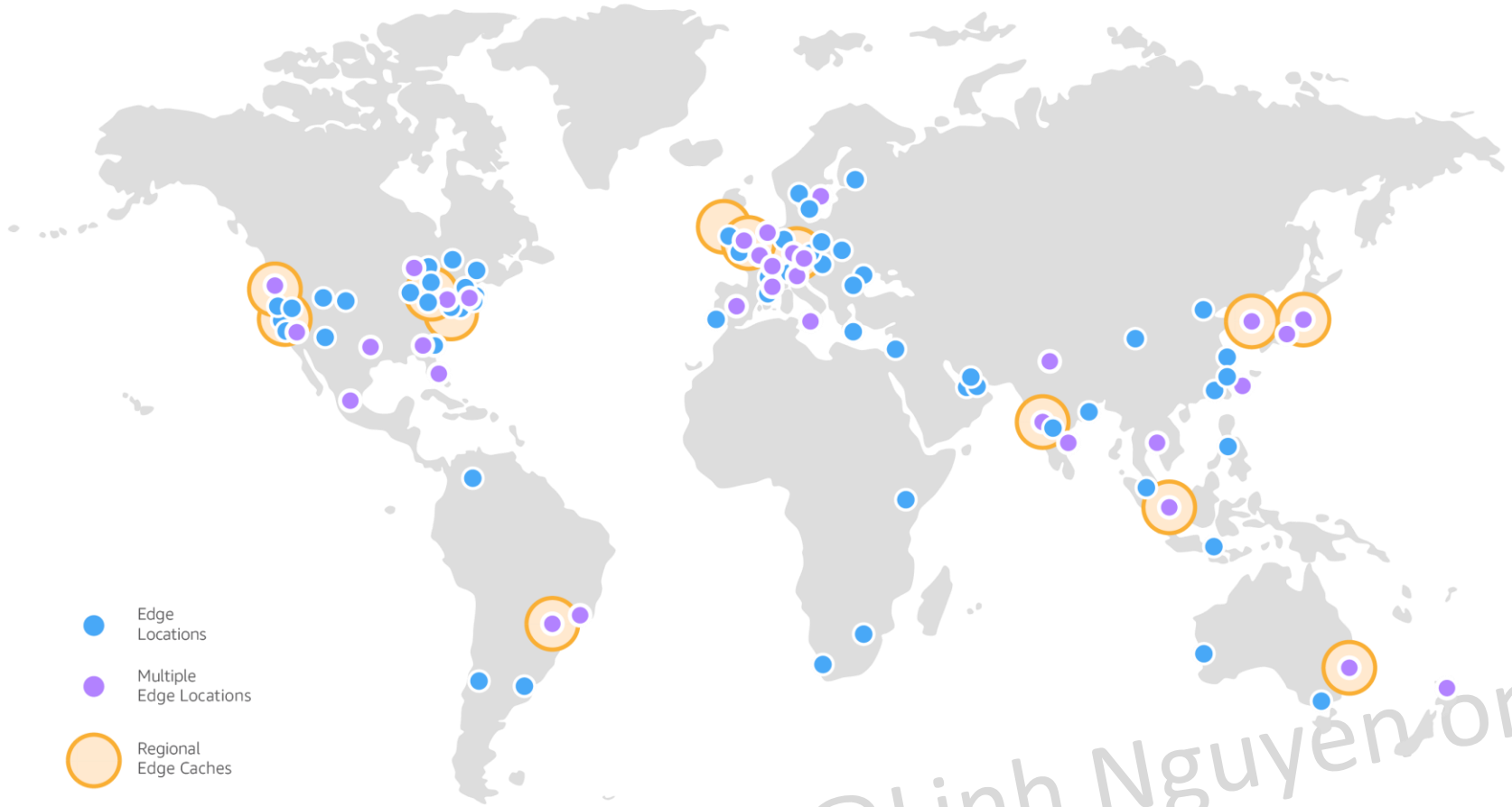


Edge location

AWS Edge Location là một mạng lưới các điểm phân phối (Point of Presense) trên thế giới, nơi các dịch vụ AWS, như Amazon CloudFront và Amazon Route 53, cung cấp các tính năng xử lý và phân phối nội dung (CDN) đến người dùng cuối.

Mỗi Edge Location là một trung tâm dữ liệu nhỏ và được quản lý bởi AWS, có khả năng đáp ứng các yêu cầu địa phương từ các máy khách của người dùng cuối. Edge Locations hoạt động như bộ đệm cho nội dung được phân phối bởi các dịch vụ AWS, giúp giảm thiểu độ trễ và tăng tốc độ truy cập cho người dùng cuối.

Edge location



Nguồn: https://aws.amazon.com/cloudfront/features

Introduction to AWS main services

Tổng quan về các dịch vụ trên AWS

**Các dịch vụ trong danh sách này được sắp xếp theo 2 tiêu chí:*

- *Mức độ phổ biến trong các dự án thực tế (service nào hay dùng được đưa lên đầu)*
- *Độ khó tăng dần (service nào dễ tiếp cận được đưa lên trước)*

**Danh sách chỉ là 1 phần nhỏ, không phải tất cả dịch vụ của AWS.*

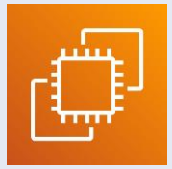
**Những dịch vụ trong khung màu xanh là những dịch vụ thường được sử dụng.*

**Không cần phải nhớ hết các service cũng như biểu tượng (vì google có).*

**Khoá DevOps này chỉ tập trung sử dụng các dịch vụ liên quan Compute, Database, Container, Network, Security, Deployment.*

Tổng quan về các dịch vụ trên AWS

Computing & Container


Amazon Elastic Compute Cloud (Amazon EC2)


AWS Elastic Beanstalk


AWS Lambda


Amazon EC2 Auto Scaling


Amazon Elastic Container Registry (Amazon ECR)


Amazon Elastic Container Service (Amazon ECS)


Amazon Elastic Kubernetes Service (Amazon EKS)


AWS Fargate

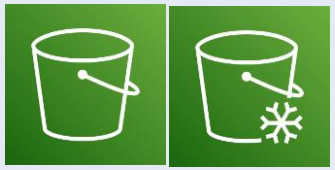

VMware Cloud on AWS


AWS Outposts family

Tổng quan về các dịch vụ trên AWS

Storage


Amazon Elastic Block Store (Amazon EBS)


Amazon Simple Storage Service (Amazon S3)


Amazon Elastic File System (Amazon EFS)


AWS Storage Gateway


Amazon FSx for Lustre


Amazon FSx


Amazon FSx for Windows File Server


AWS Snowmobile


AWS Snowball


CloudEndure Disaster Recovery


AWS Backup

Tổng quan về các dịch vụ trên AWS

Networking


Amazon Virtual Private Cloud (Amazon VPC)


Amazon CloudFront


AWS Cloud Map


AWS Client VPN


AWS Transit Gateway


AWS PrivateLink

Amazon Route 53


Elastic Load Balancing


AWS Global Accelerator


AWS Site-to-Site VPN


AWS Direct Connect

Tổng quan về các dịch vụ trên AWS

Database


Amazon Aurora


Amazon ElastiCache


Amazon DynamoDB


Amazon Neptune


Amazon Quantum Ledger Database (Amazon QLDB)


Amazon Relational Database Service (Amazon RDS)


Amazon DocumentDB (with MongoDB compatibility)


Amazon MemoryDB for Redis


Amazon Keyspaces (for Apache Cassandra)

Tổng quan về các dịch vụ trên AWS

Security & Identity


AWS Identity and Access Management (IAM)


AWS Key Management Service (AWS KMS)


AWS Secrets Manager


Amazon Cognito


AWS WAF


AWS Certificate Manager (ACM)


AWS Firewall Manager


AWS Shield


AWS Directory Service


Amazon GuardDuty


Amazon Inspector


Amazon Cloud Directory


AWS Artifact


Amazon Macie


AWS CloudHSM

Tổng quan về các dịch vụ trên AWS

Management & Governance


AWS Config


AWS Management Console

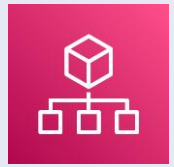

AWS CloudTrail


AWS Control Tower


AWS OpsWorks


AWS Systems Manager


AWS Trusted Advisor


AWS Organizations


AWS CloudFormation


AWS Well-Architected Tool


AWS Budgets


AWS Cost Explorer

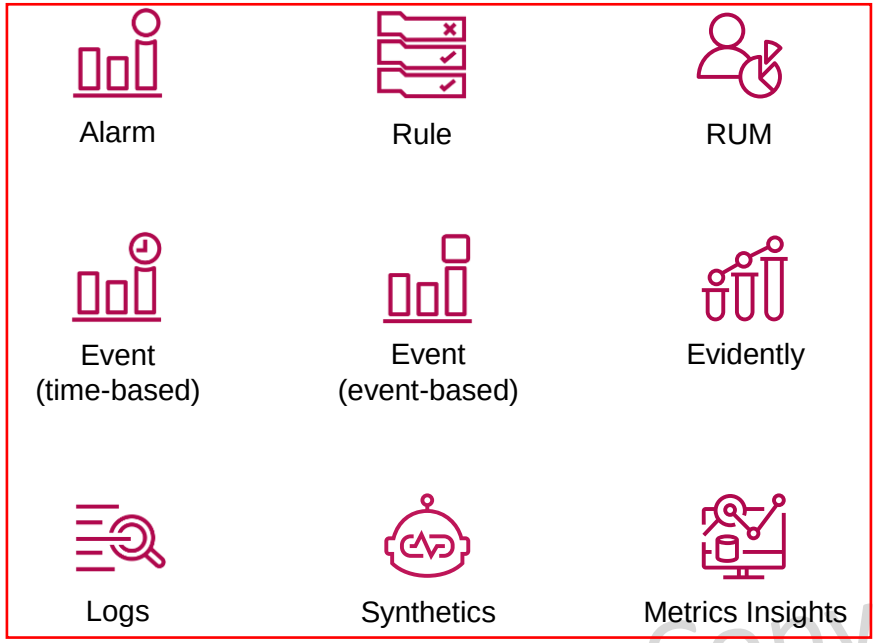

AWS Cost & Usage Report


AWS Resource Explorer

Tổng quan về các dịch vụ trên AWS

Monitoring

Amazon CloudWatch



AWS CloudTrail

Tổng quan về các dịch vụ trên AWS

Messaging, Application integration

Amazon Simple Email Service (Amazon SES)

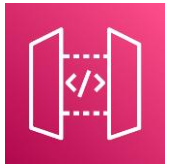
Amazon Simple Notification Service (Amazon SNS)

Amazon Simple Queue Service (Amazon SQS)

Amazon MQ

AWS AppSync

Amazon EventBridge



Amazon API Gateway

Tổng quan về các dịch vụ trên AWS

Deployment & Automation


AWS Cloud9


AWS CodeBuild


AWS CodeCommit


AWS CodeDeploy


AWS CodePipeline

CICD


AWS X-Ray


AWS Cloud Development Kit (AWS CDK)


AWS CodeArtifact


AWS CloudShell

Tổng quan về các dịch vụ trên AWS

Migration

AWS Database Migration Service (AWS DMS)

AWS Application Discovery Service

AWS Transfer Family

AWS DataSync

AWS Migration Hub

AWS Server Migration Service (AWS SMS)

AWS Application Migration Service

AWS Migration Evaluator

AWS Mainframe Modernization

Tổng quan về các dịch vụ trên AWS

Big data & Data analytic


Amazon Redshift


Amazon QuickSight


AWS Lake Formation


AWS Data Pipeline


Amazon Managed Streaming for Apache Kafka


AWS Data Exchange


AWS Glue DataBrew


Amazon FinSpace

Tổng quan về các dịch vụ trên AWS

AI & Machine learning


Amazon Fraud Detector


Amazon Kendra


Amazon CodeGuru


Amazon SageMaker Studio Lab


TensorFlow on AWS


Amazon Polly


Amazon Rekognition


Amazon SageMaker


Amazon Translate


AWS DeepComposer


AWS Deep Learning AMIs


AWS Deep Learning Containers


AWS DeepLens


AWS DeepRacer

Tổng quan về các dịch vụ trên AWS

Other: *Ask Google for more information* ☺

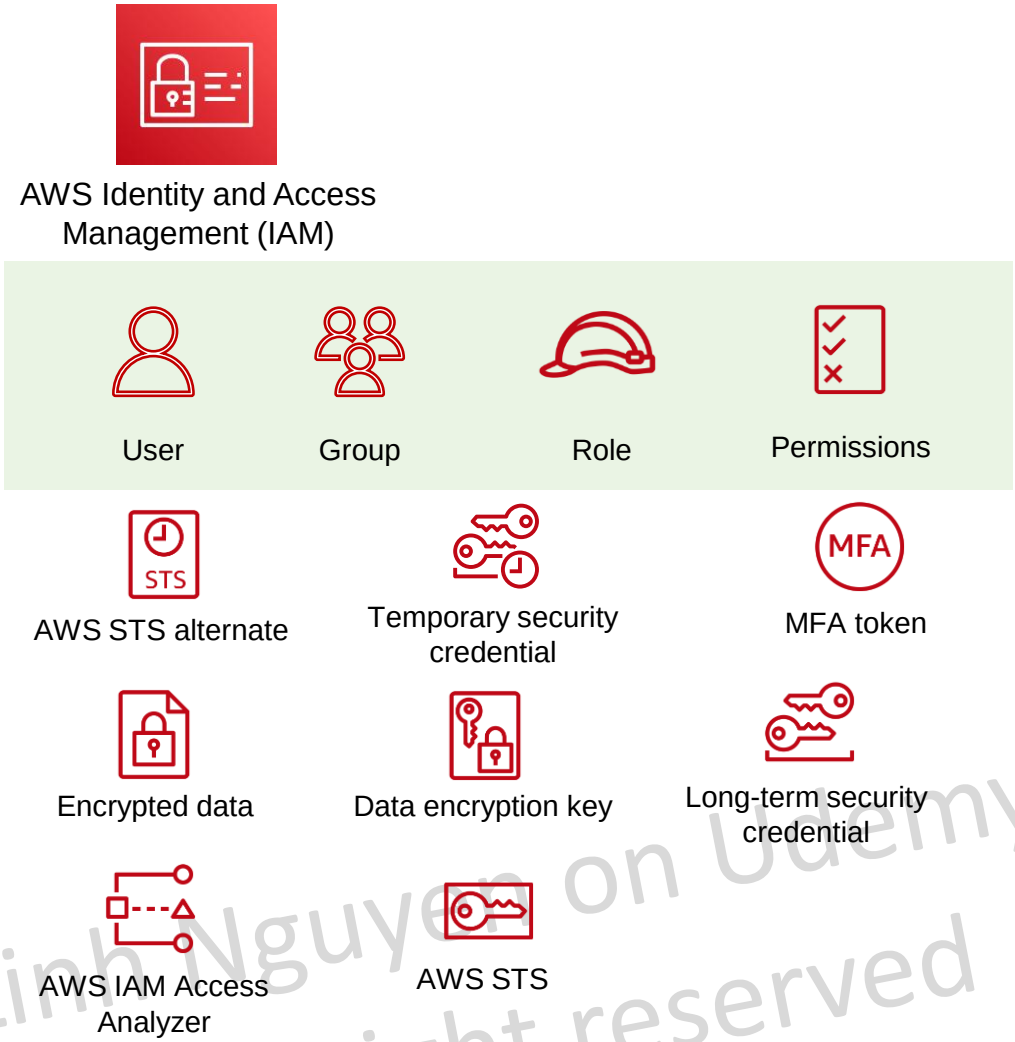
- *IoT*
- *Media Services*
- *Game*
- *Quantum technologies*
- *Robotics*
- *Satellite*
- *VR & AR*
- *Blockchain*

Review AWS Knowledge

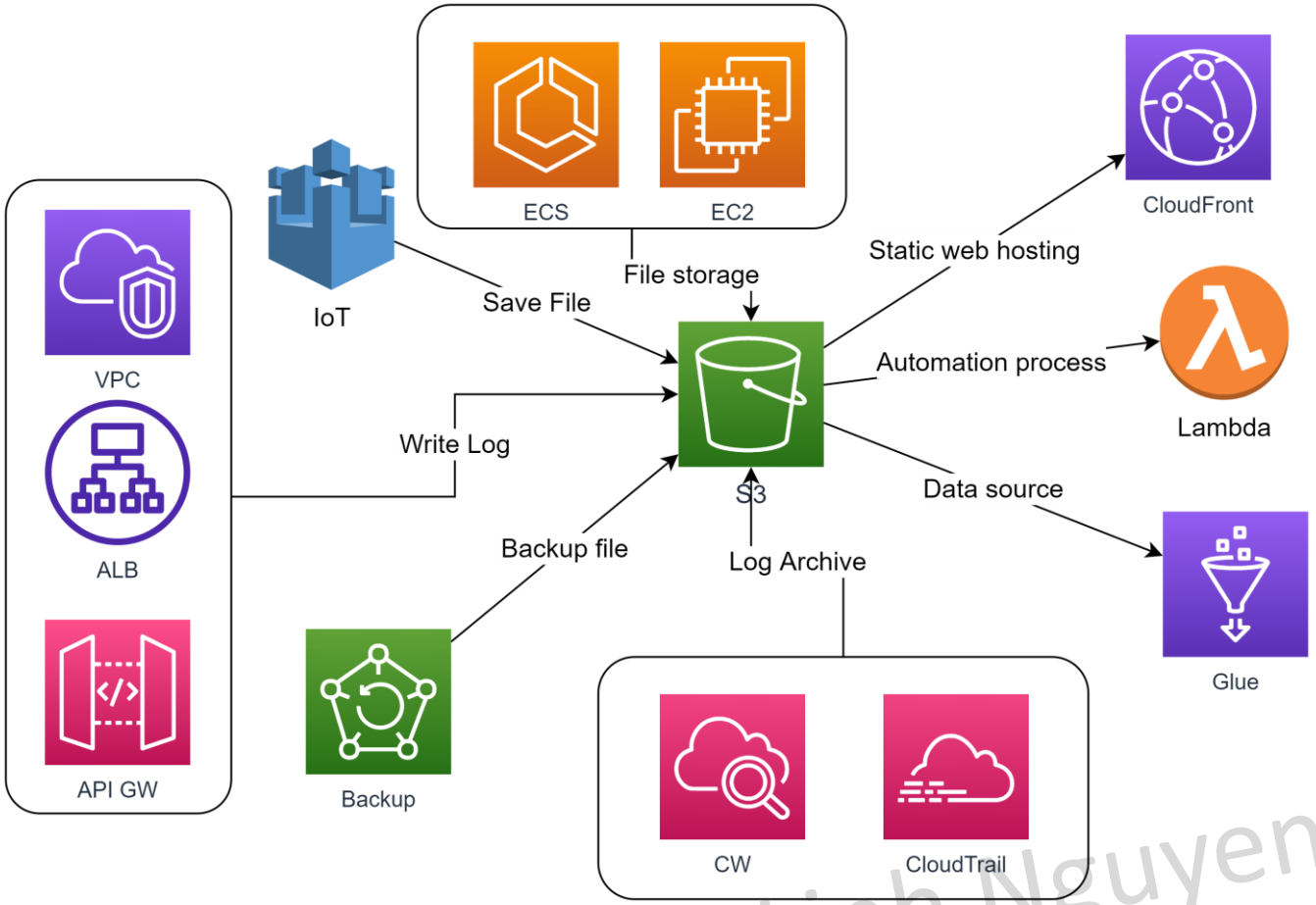
IAM Concepts

Để có thể thiết kế & xây dựng hệ thống trên AWS đảm bảo tiêu chí về Security cũng như không gặp trouble, chúng ta cần nắm vững các concept cơ bản của IAM bao gồm:

- User
- Group
- Role
- Permission (Policy)

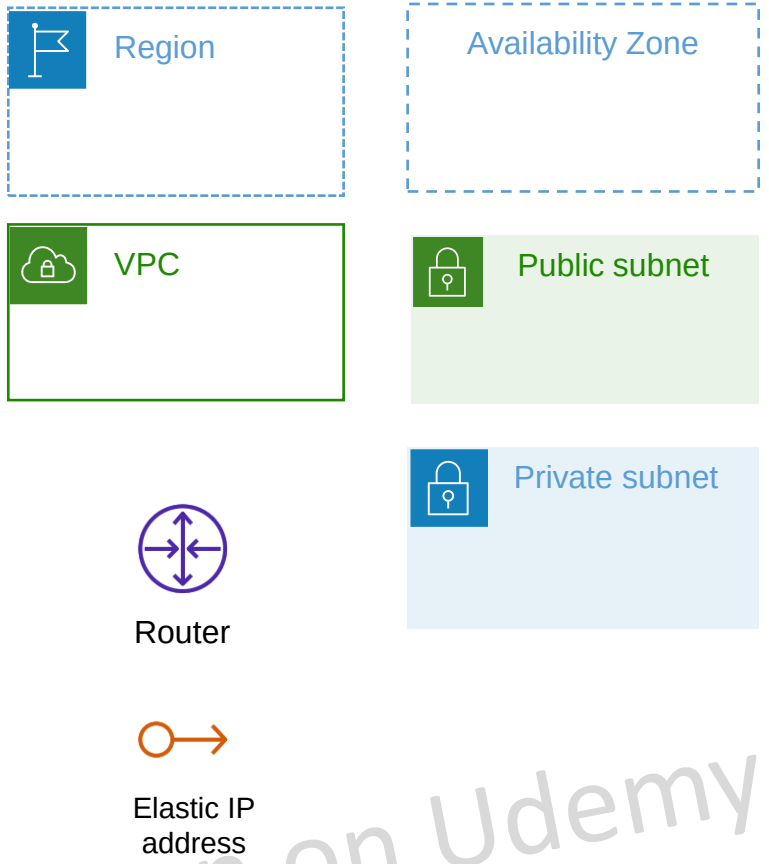


Simple Storage Service (S3)



VPC & Networking

- VPC: Một mạng ảo được tạo ra ở cấp độ region.
- Subnet: Một dải IP được định nghĩa nằm trong VPC. Mỗi subnet phải được quyết định Availability Zone tại thời điểm tạo ra.
- IP Address: IP V4 hoặc V6 được cấp phát. Có 2 loại là Public IP và Private IP.
- Routing: xác định traffic sẽ được điều hướng đi đâu trong mạng.
- Elastic IP: IP được cấp phát riêng, có thể access từ internet (public), không bị thu hồi khi instance start -> stop.



VPC & Networking - components


Flow logs


VPN connection


Internet gateway


Peering connection

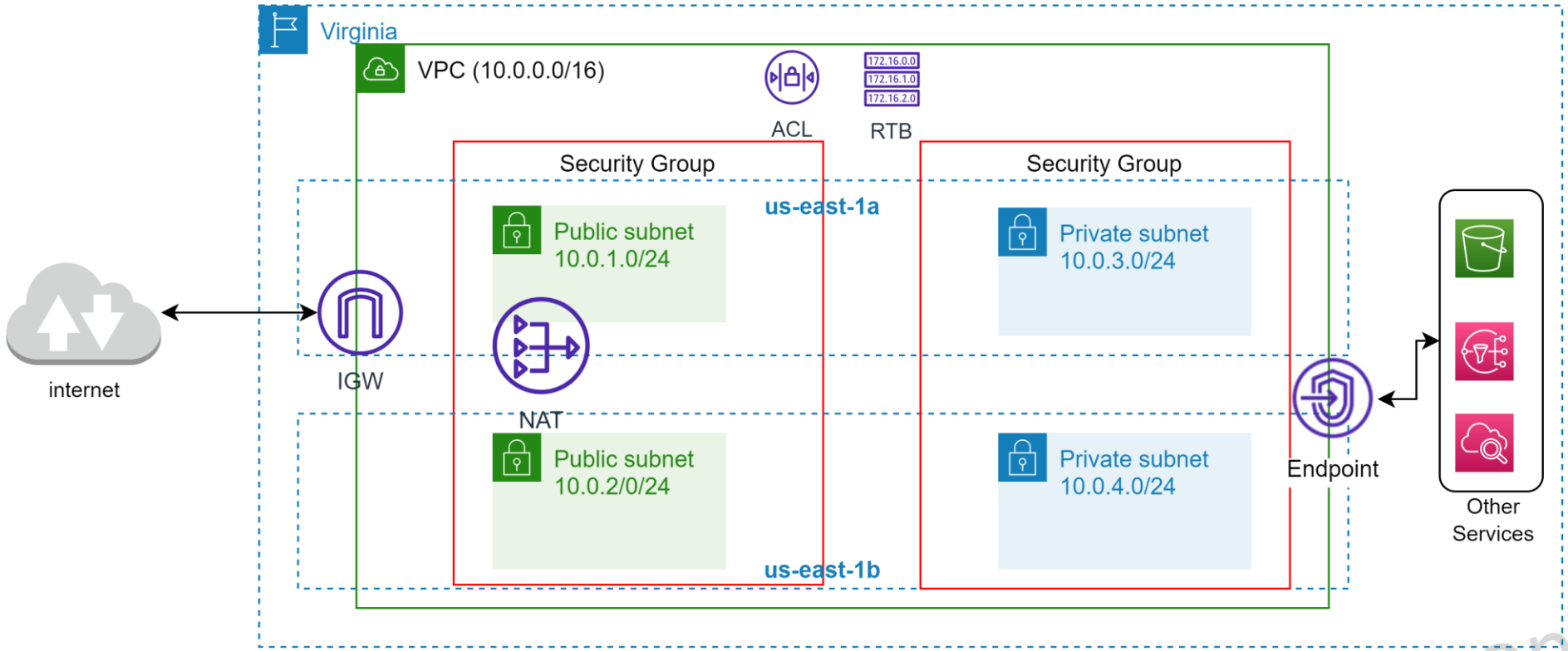

NAT gateway


Transit Gateway

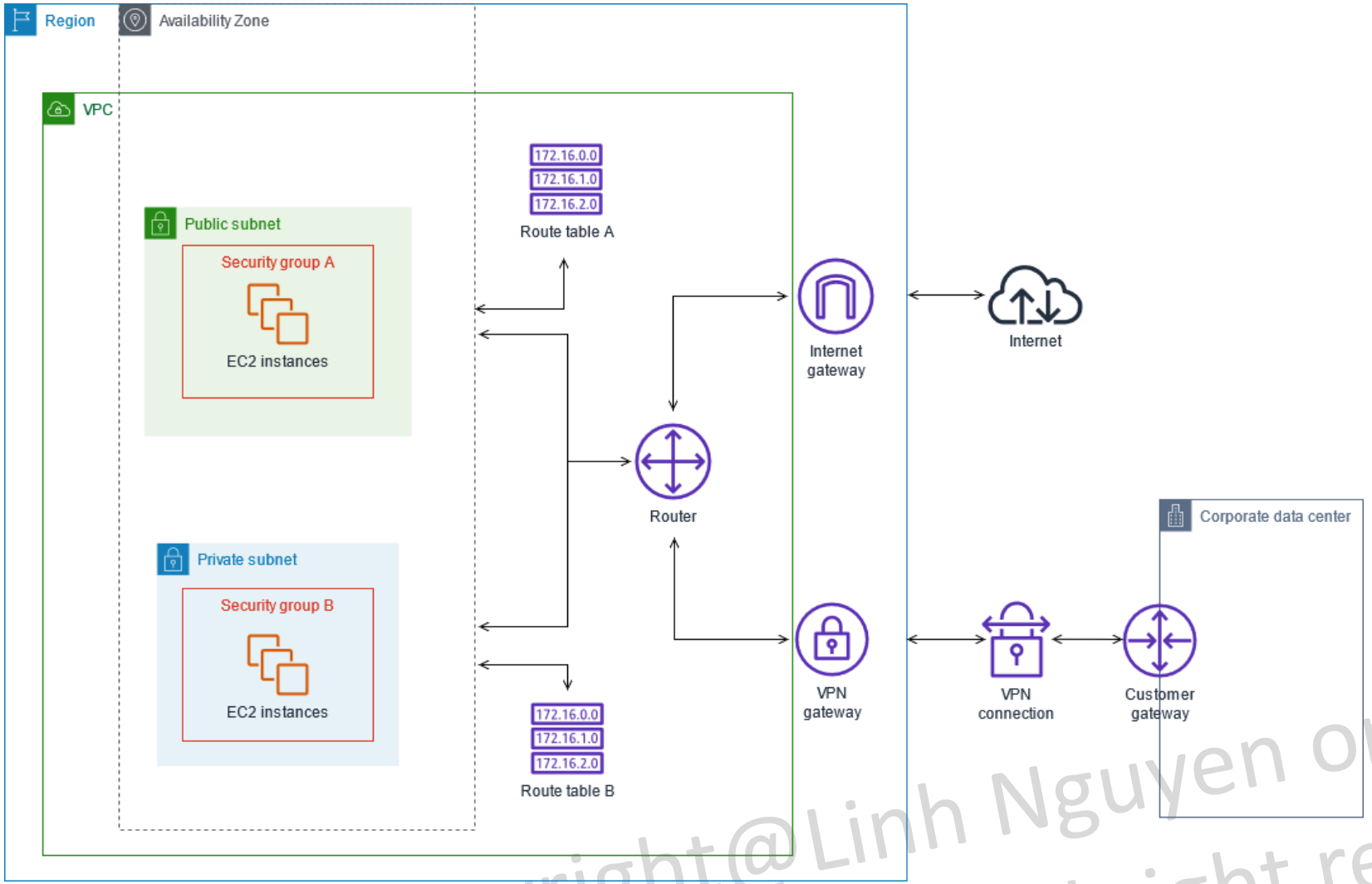

Elastic network interface


Endpoints

VPC & Networking – Standard design for a VPC



VPC & Networking – Route table



VPC & Networking – Standard design for Security Groups

Security Group

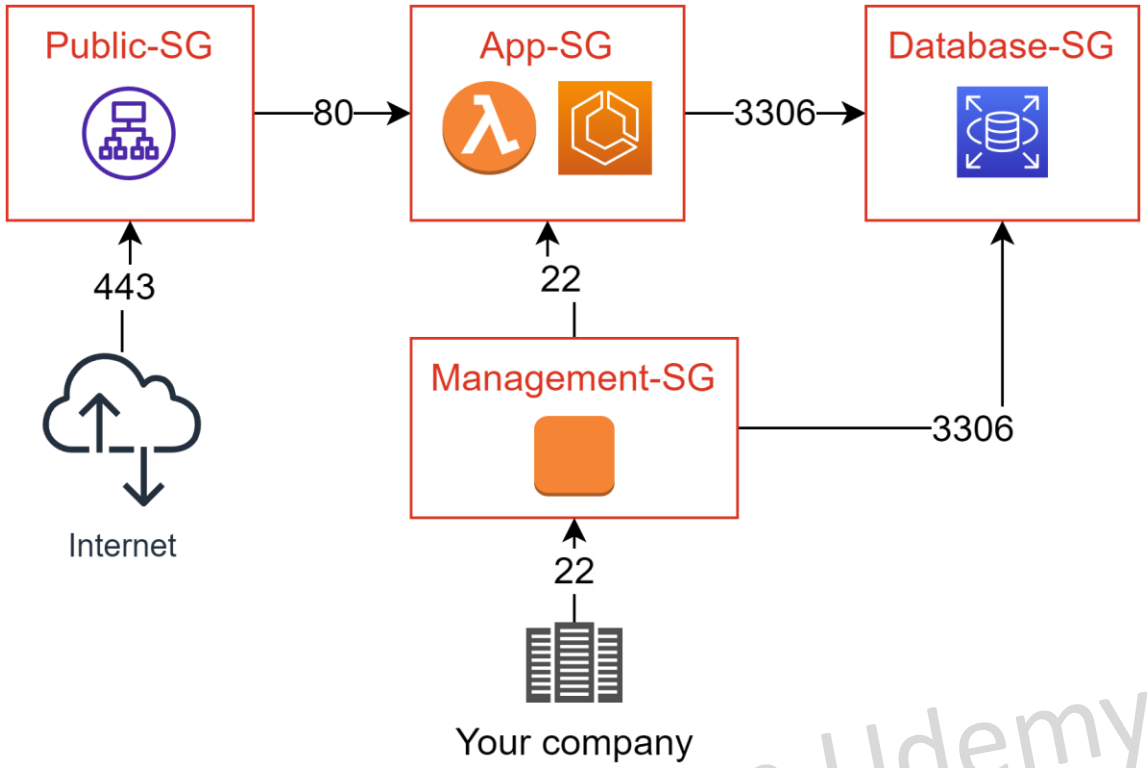
Thường được dùng để gom nhóm các resource có chung network setting (in/out, protocol, port).

Khi thiết kế cần quan tâm tới tính tái sử dụng, dễ quản lý.

Source của một Security Group có thể là CIDR hoặc id của một Security Group khác.

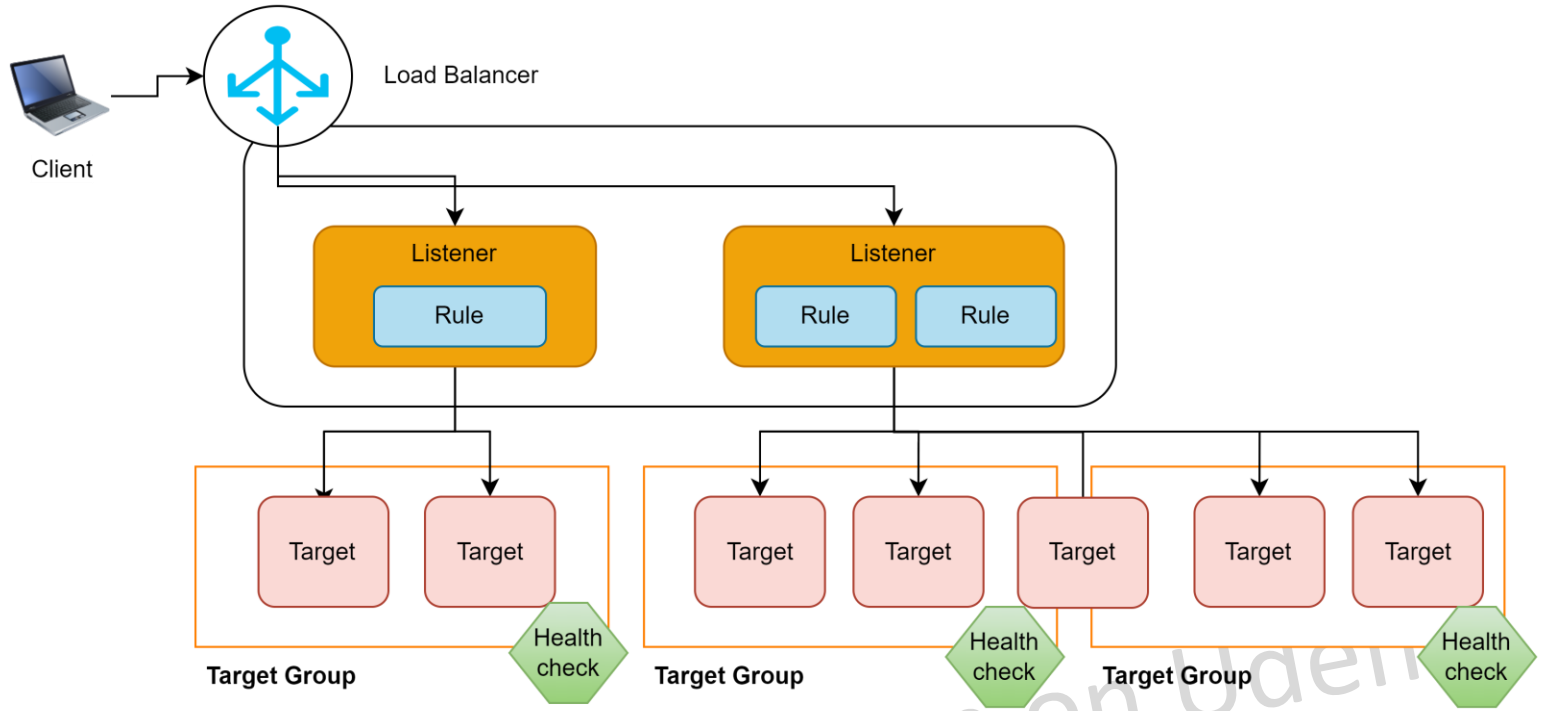
Rule của Security Group là stateful và không có deny rule.

*Statefull có nghĩa là nếu Inbound cho phép traffic đi vào thì khi request tới sẽ nhận được response mà không cần explicit allow Outbound. Khác với Network ACL.



Load Balancing

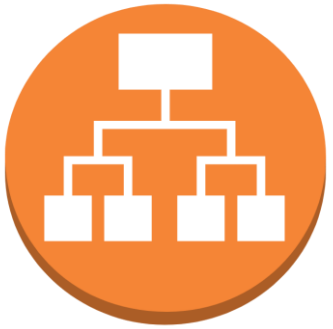
- Load Balancer cho phép setting các listener (trên 1 port nào đó vd HTTP:80, HTTPS:443)
- Mỗi Listener cho phép cấu hình nhiều rule.
- Request sau khi đi vào listener, được đánh giá bởi các rule sẽ được forward tới target group phù hợp.
- Target group có nhiệm vụ health check để phát hiện và loại bỏ target un-healthy.



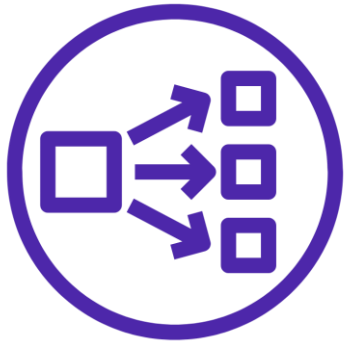
Load Balancing

Có 4 loại load balancer chính:

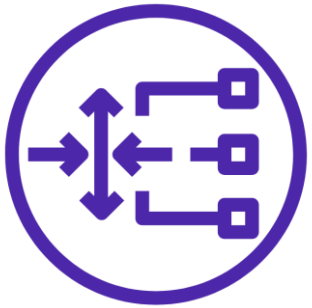
- Application LB
- Network LB
- Gateway LB
- Classic LB



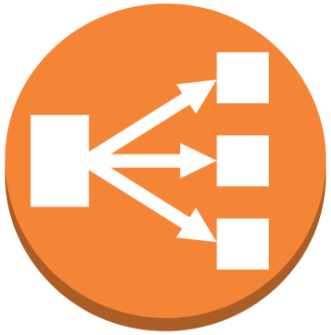
Application Load Balancer



Network Load Balancer

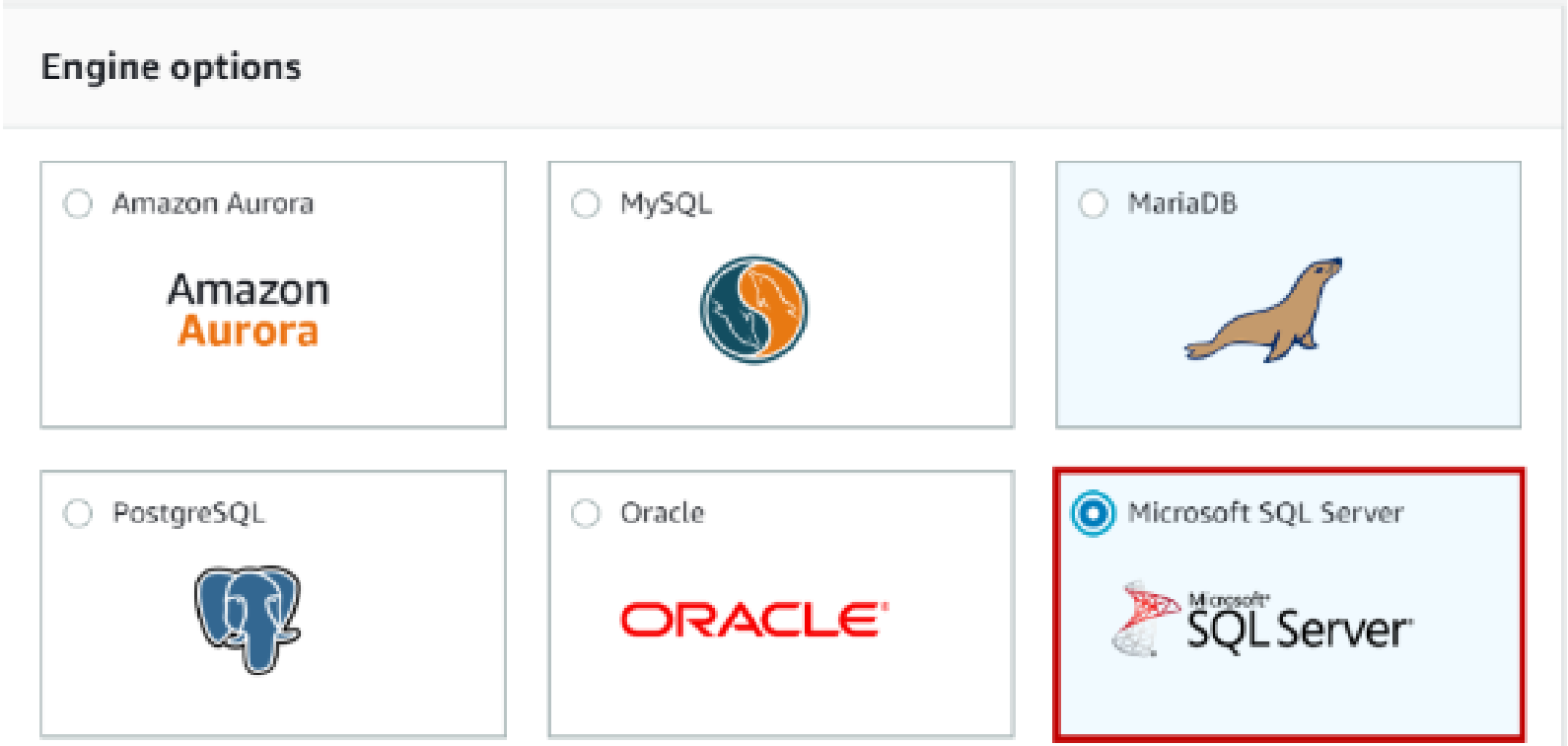


Gateway Load Balancer

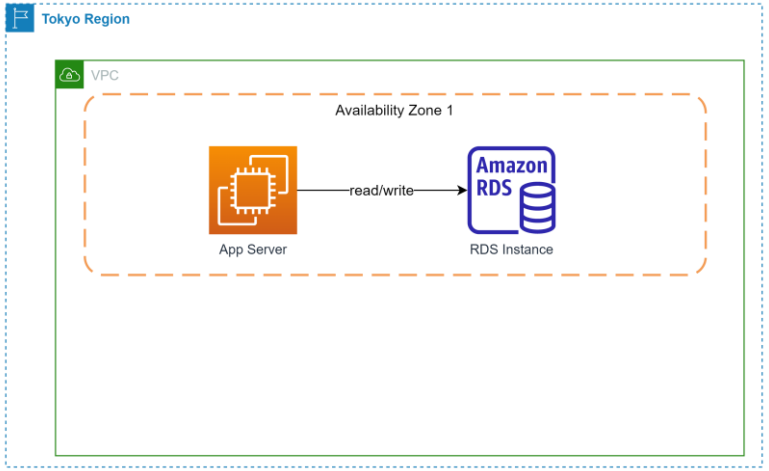


Classic Load Balancer

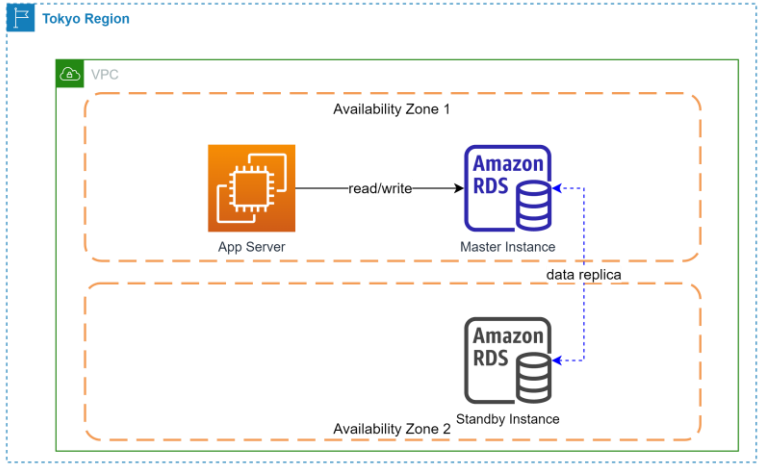
Relational Database Service (RDS)



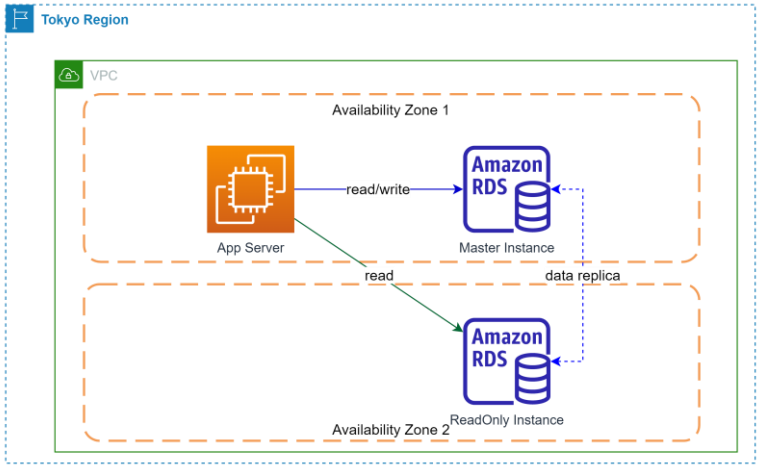
Các mô hình triển khai RDS



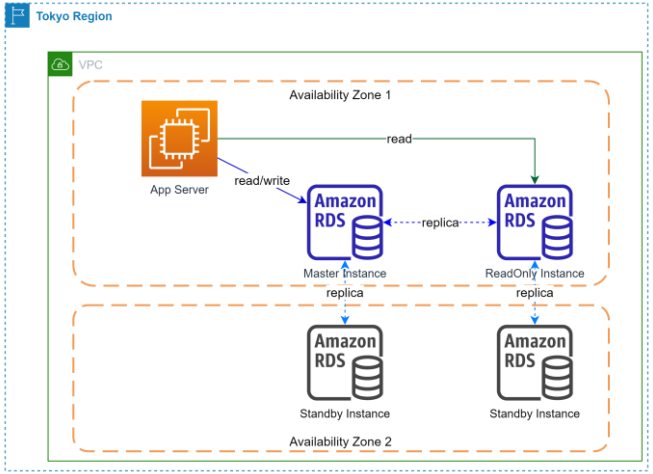
Single Instance



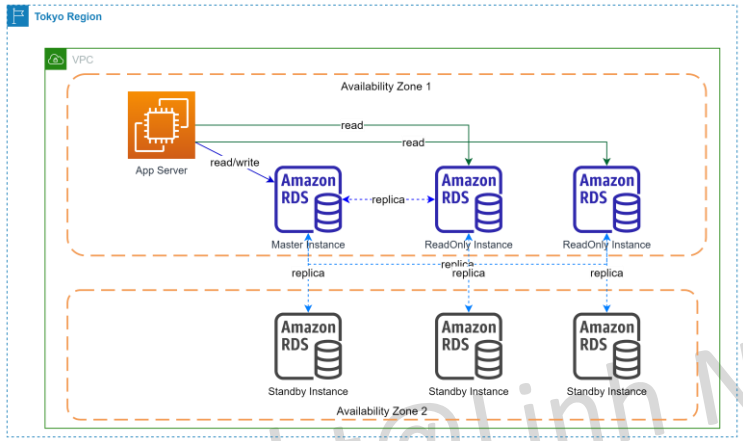
Single Instance + Multi AZ



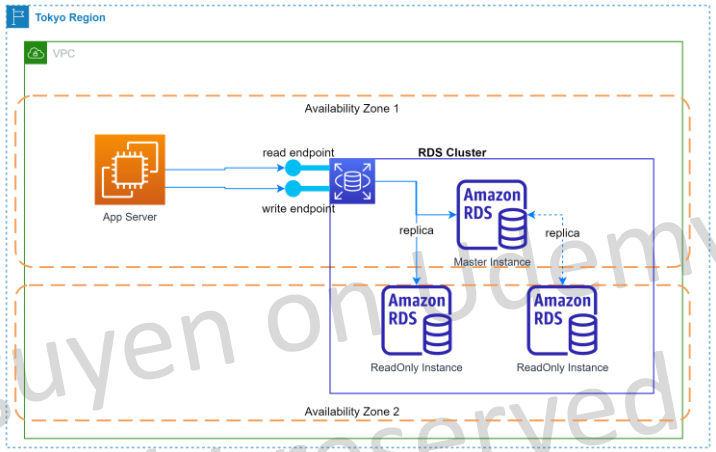
Master – Read replica



Master – Read replica + Multi AZ



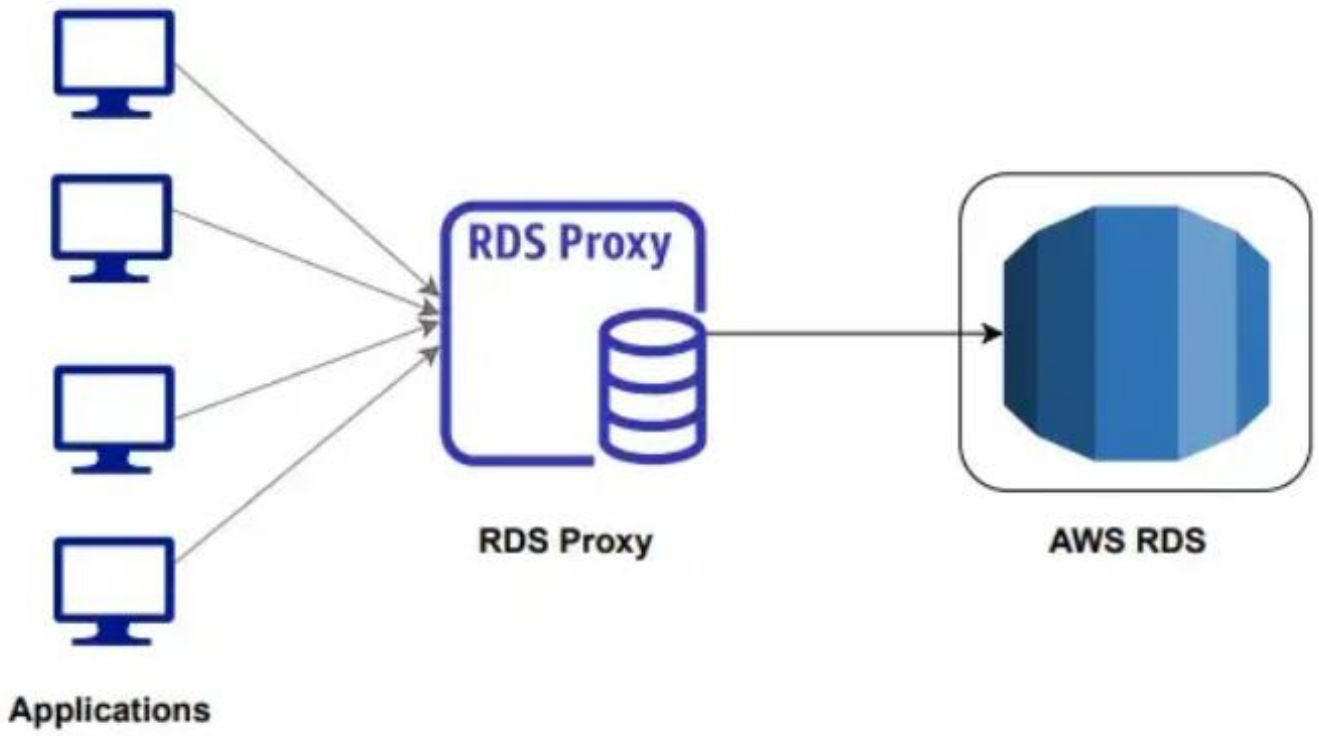
Master + Multi Read + Multi AZ



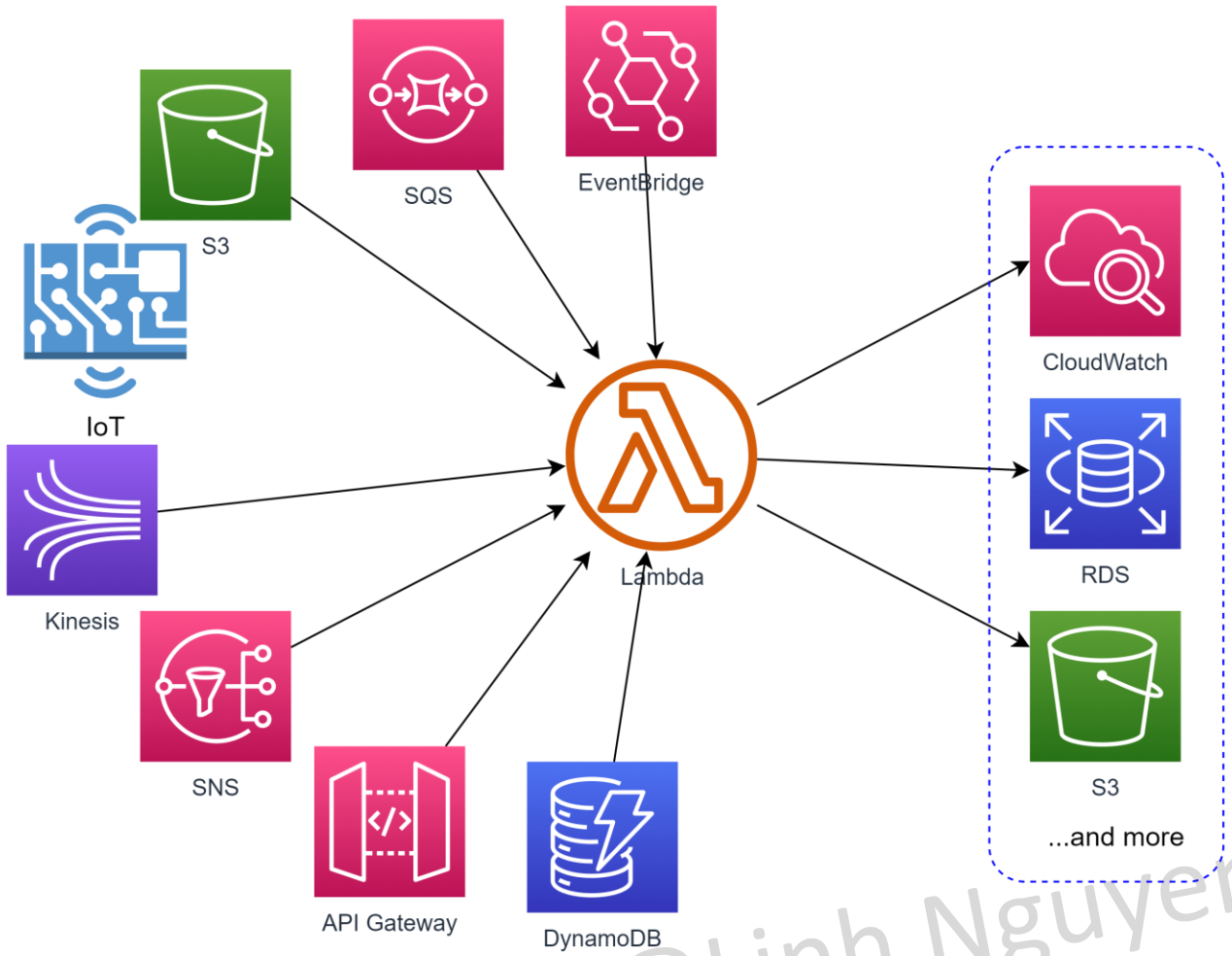
RDS - Cluster Endpoint

Relational Database Service (RDS)

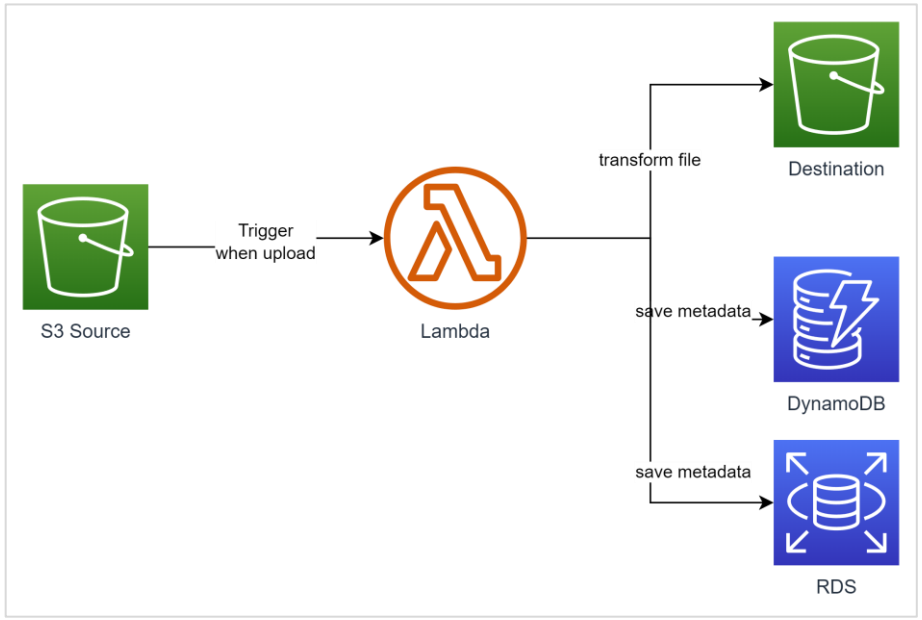
RDS Proxy



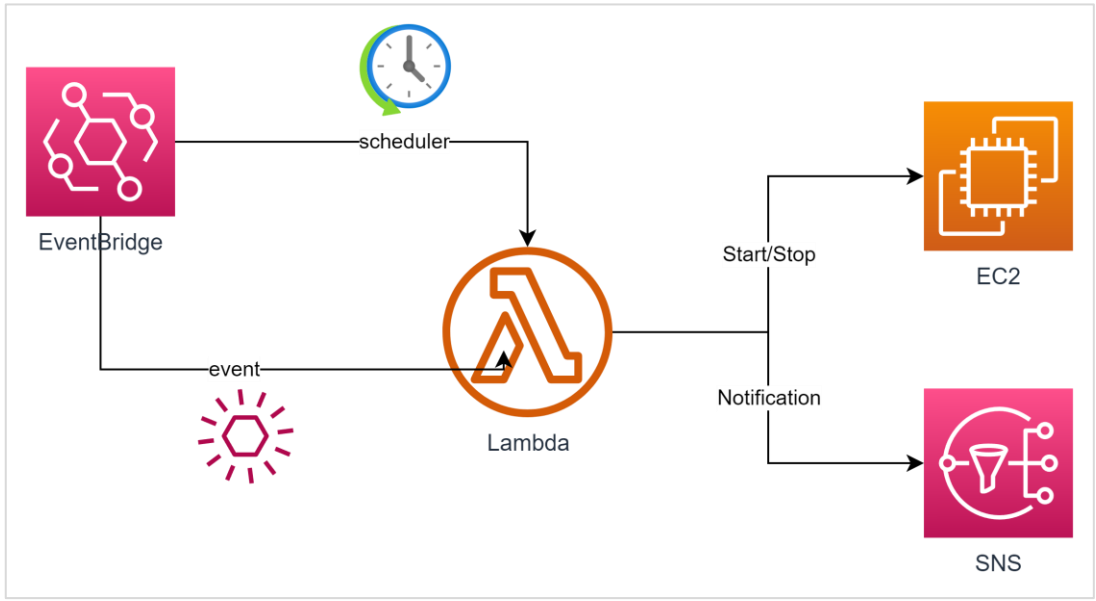
Serverless Architect (API Gateway, Cognito, Lambda)



Serverless Architect (API Gateway, Cognito, Lambda)

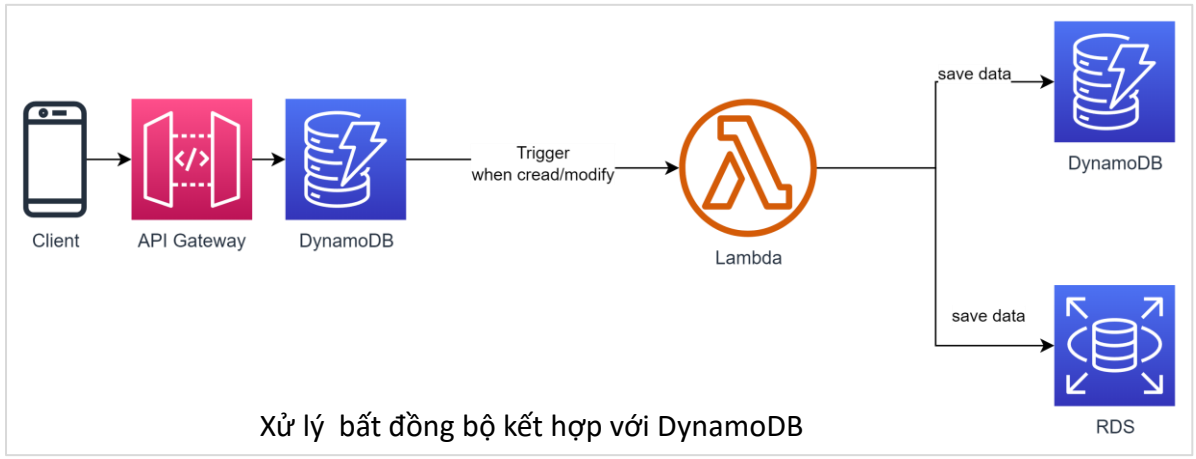


Tự động xử lý file được upload lên s3

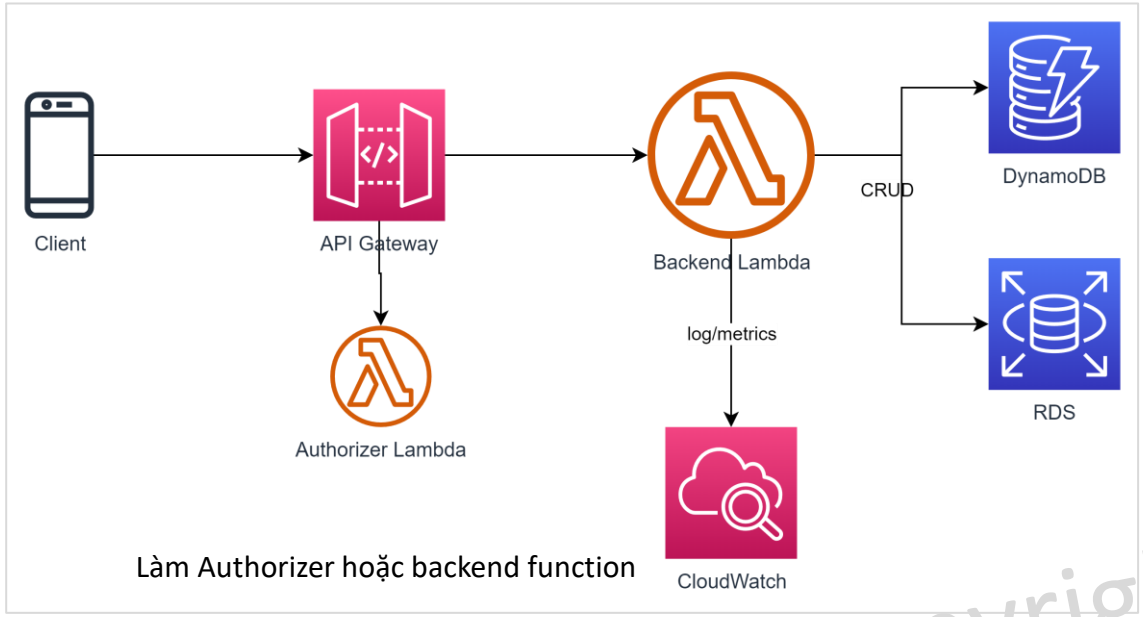


Chạy các task đơn giản theo lịch

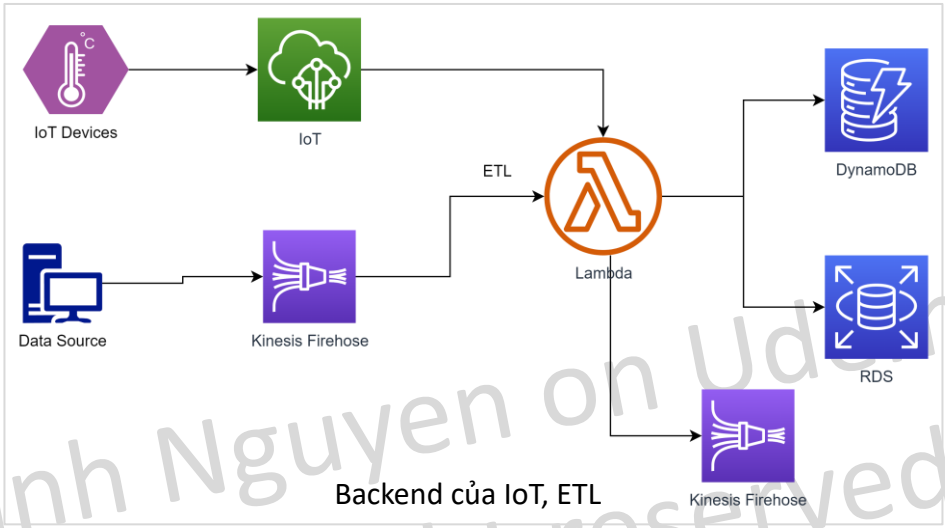
Serverless Architect (API Gateway, Cognito, Lambda)



Xử lý bất đồng bộ kết hợp với DynamoDB

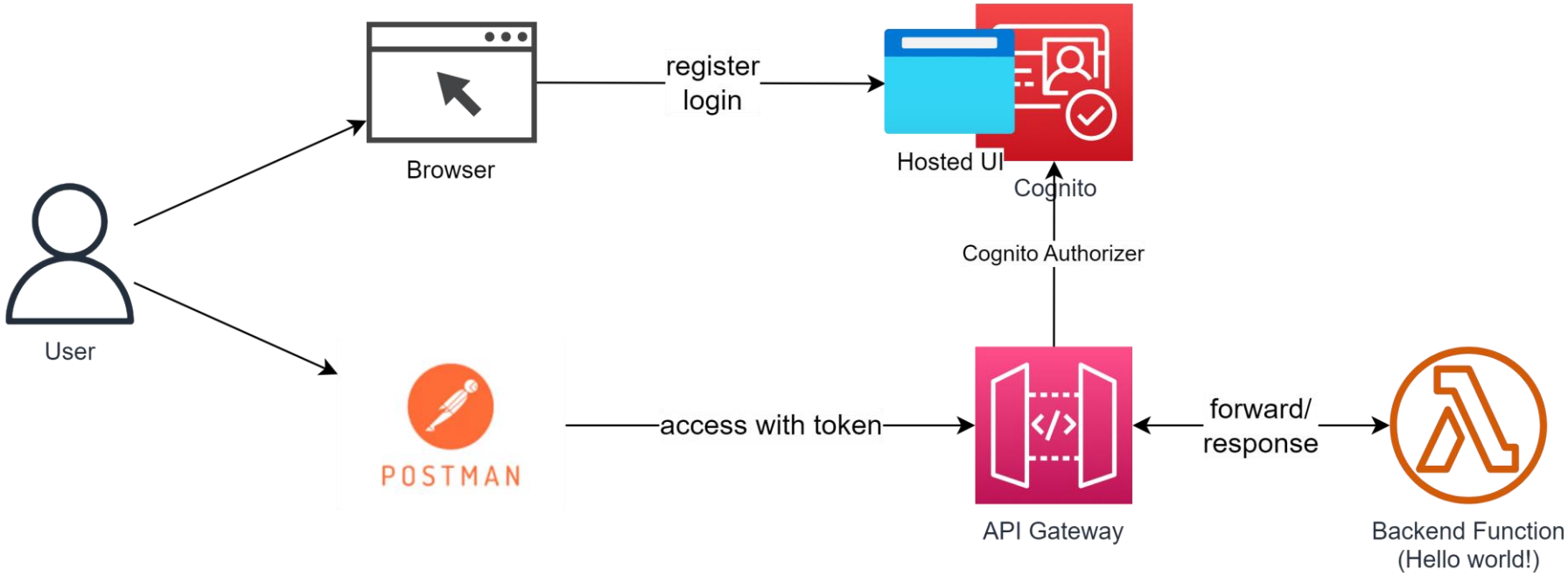


Làm Authorizer hoặc backend function



Backend của IoT, ETL

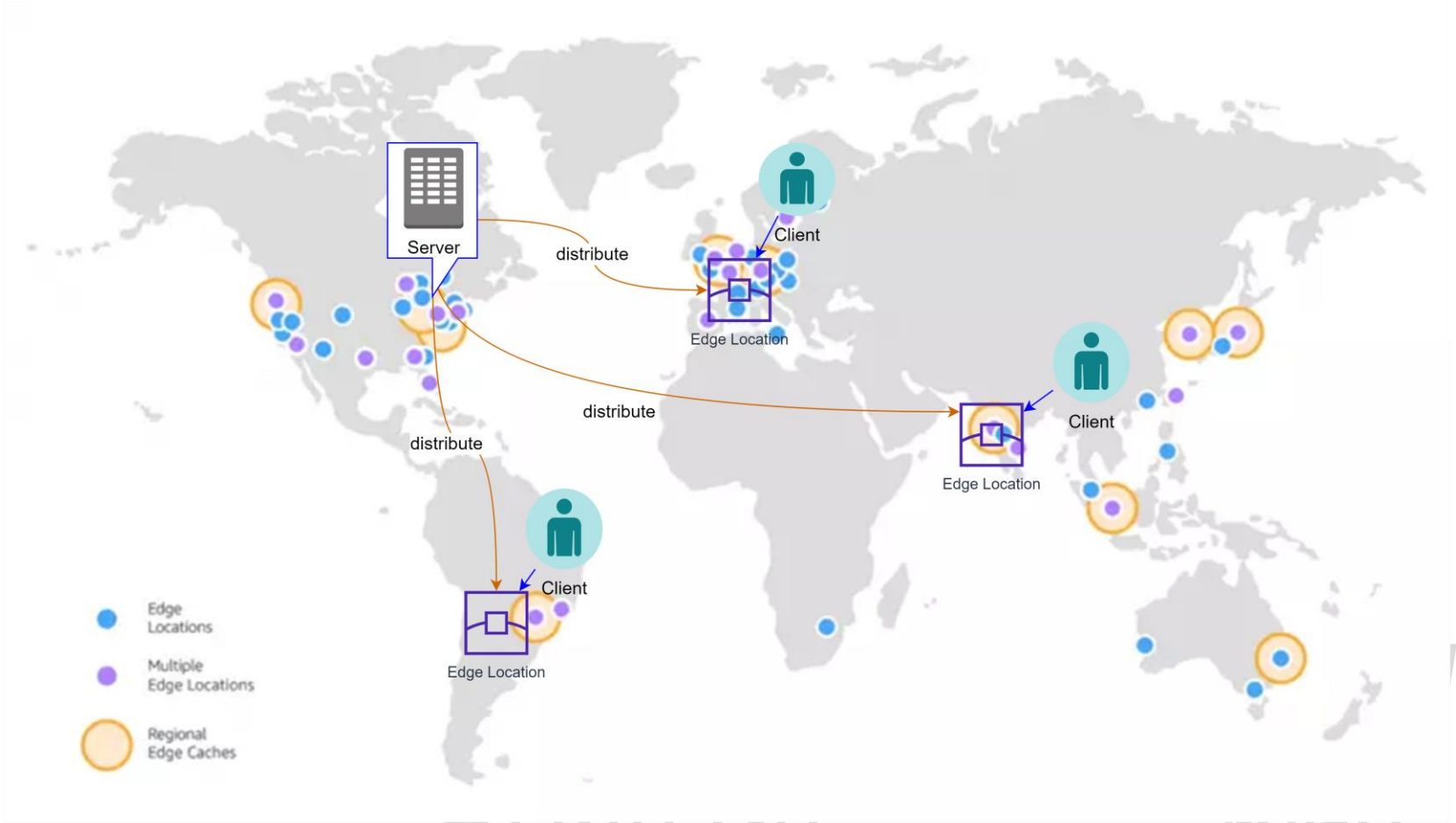
Serverless Architect (API Gateway, Cognito, Lambda)



Mô hình kiến trúc Serverless đơn giản kết hợp với Cognito

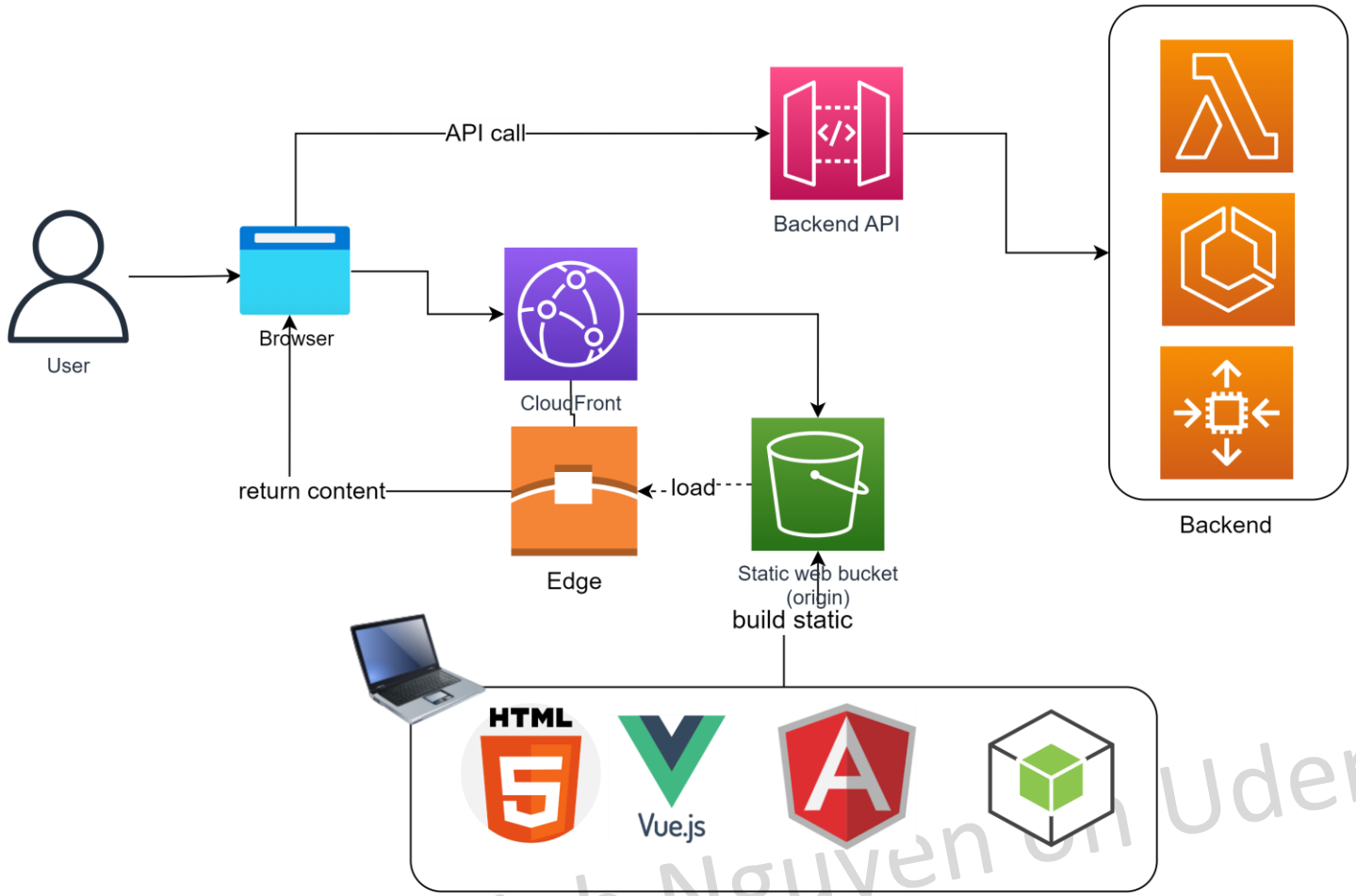
Content Delivery Network

Khi có CDN, tài nguyên của server sẽ được cache trên các máy chủ Edge, request của user tới một tài nguyên trên CloudFront sẽ được redirect tới máy chủ Edge gần nhất.



Content Delivery Network

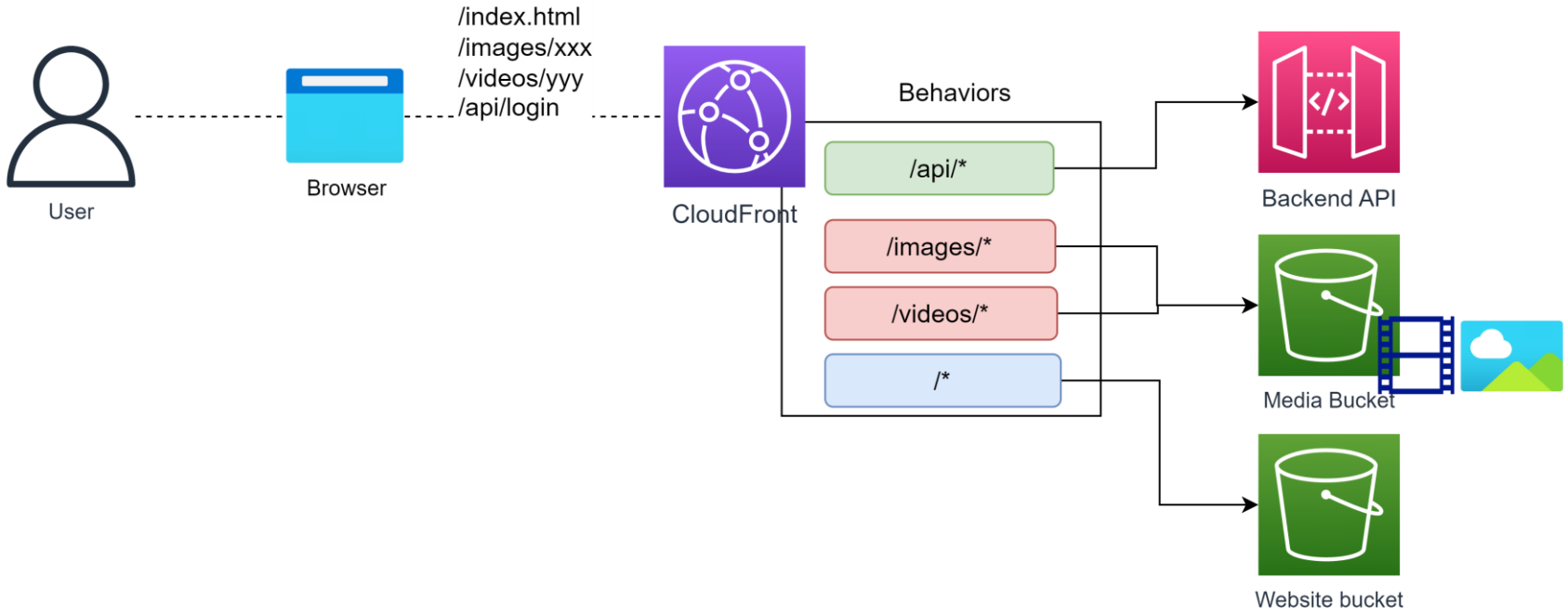
Website static (chỉ gồm HTML/css/js...) có thể được deploy lên S3 kết hợp với CloudFront.
Hâu hết các framework hiện nay như Angular, Vue, Nodejs đều hỗ trợ build website thành dạng satic chỉ gồm HTML, css, javascript để deploy lên S3.



Content Delivery Network

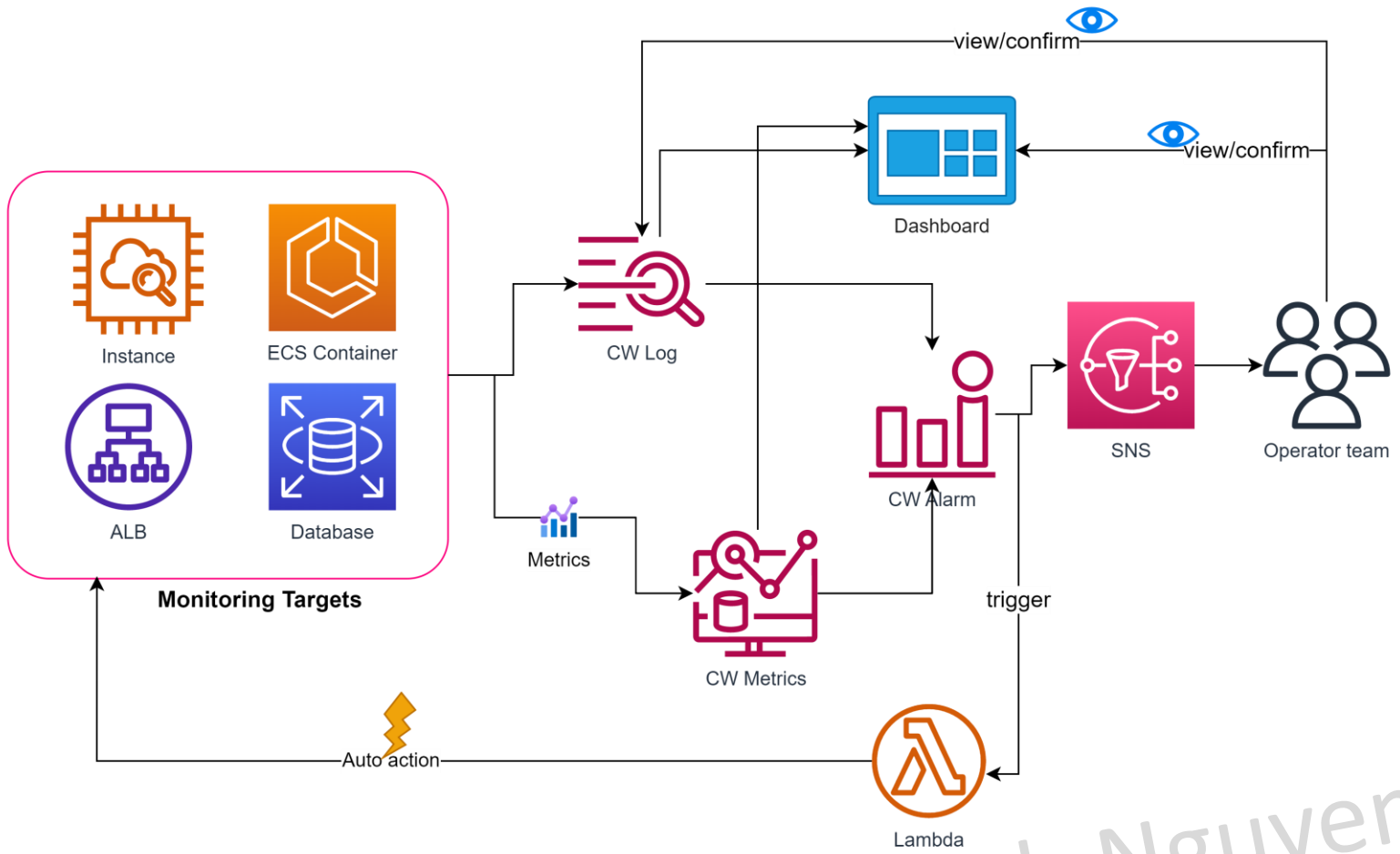
Bằng việc cấu hình các behavior khác nhau, CloudFront giúp điều hướng request của người dùng tới đúng origin mong muốn.

*Lưu ý khi setting behavior cần quan tâm tới thứ tự trước sau của các behavior, vì khi match 1 path rồi sẽ không đánh giá path tiếp theo.



Thứ tự của các behavior rất quan trọng, trong hình nếu để / lên trên cùng, sẽ làm các behavior bên dưới bị sai lệch.

Monitoring



Monitoring

Amazon CloudWatch

Alarm

Rule

Event (time-based)

Event (event-based)

Logs

Metrics Insights

RUM

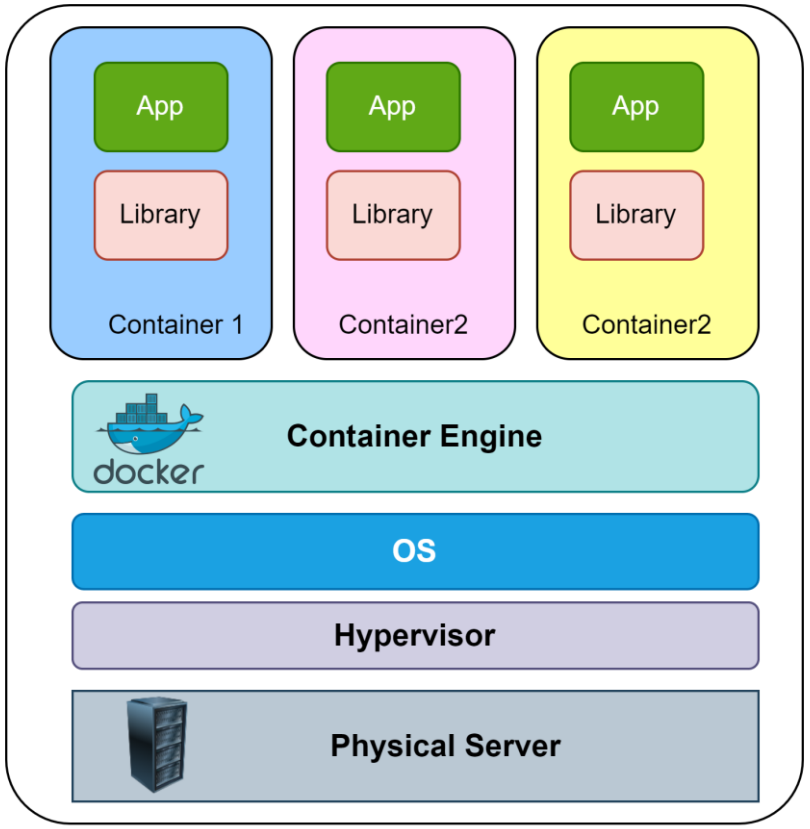
Cross-account observability

Evidently

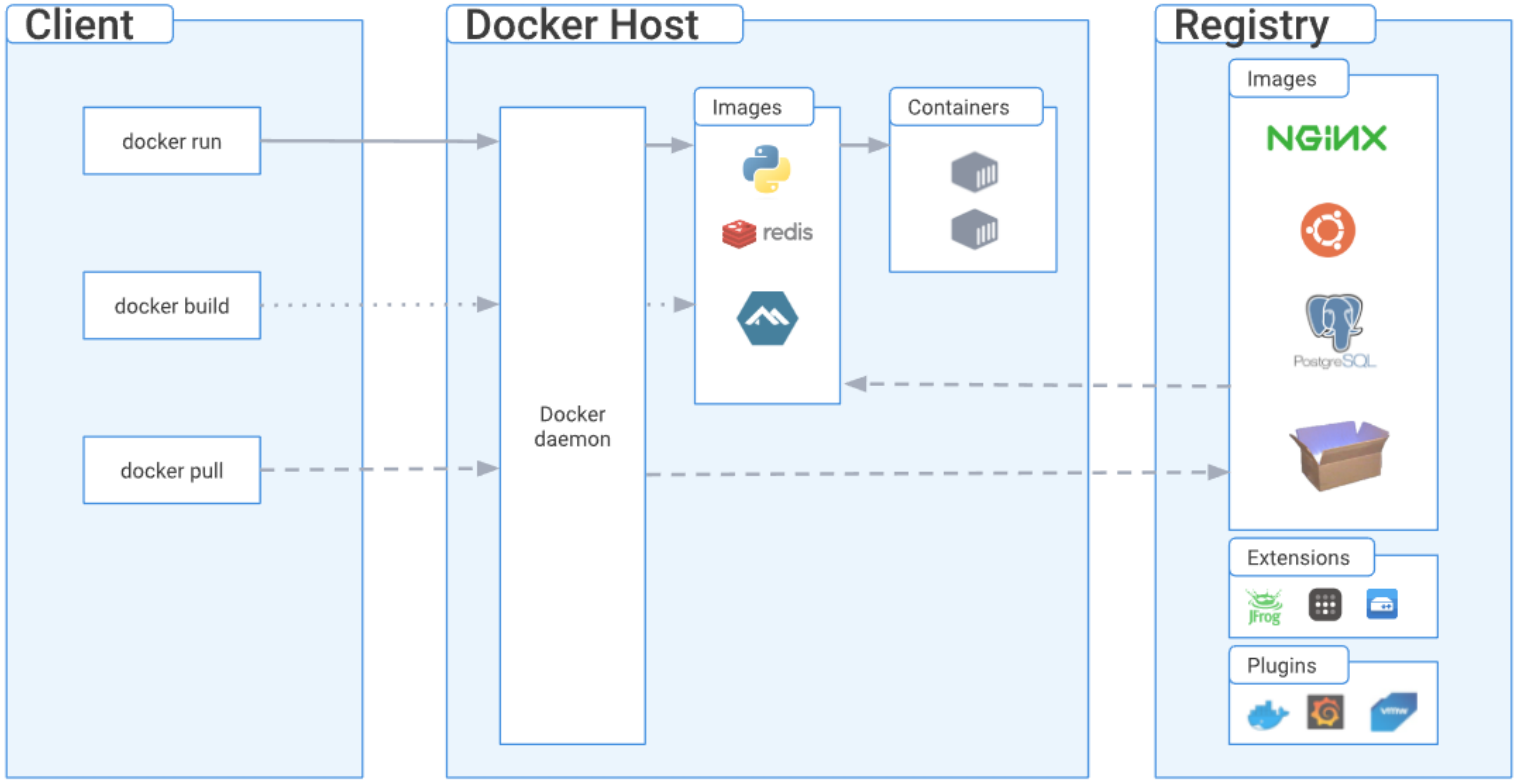
Data protection

Synthetics

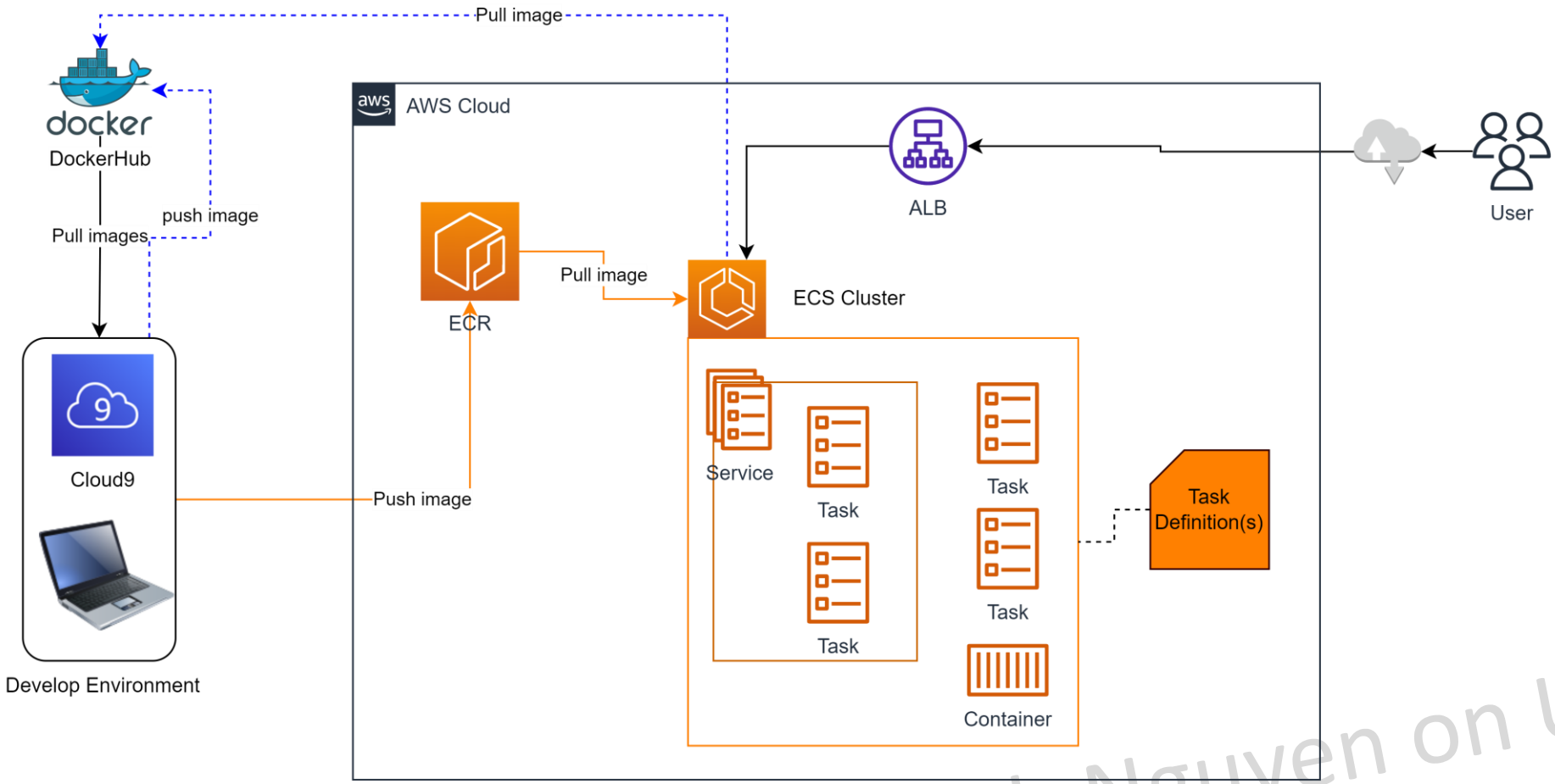
Container, ECS, ECR



Containers Architect

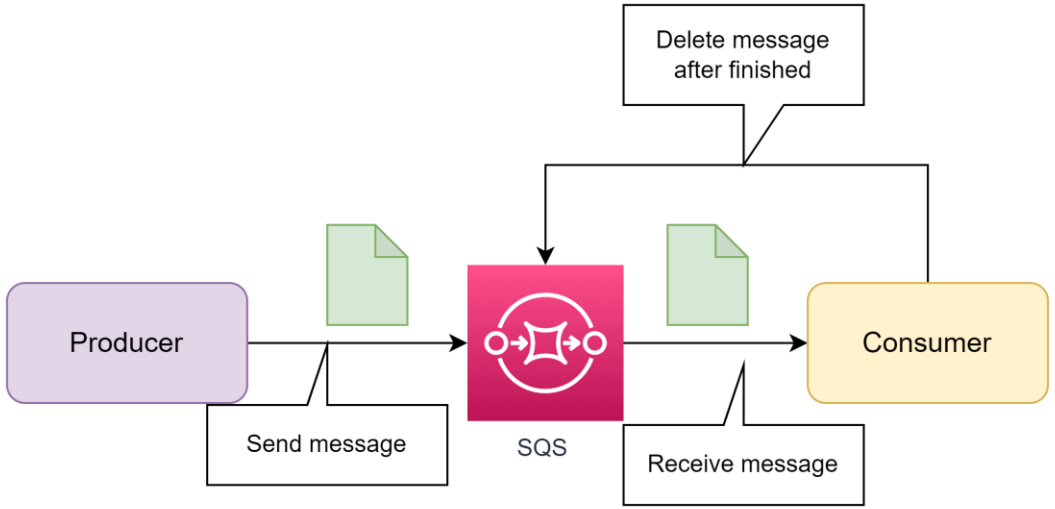


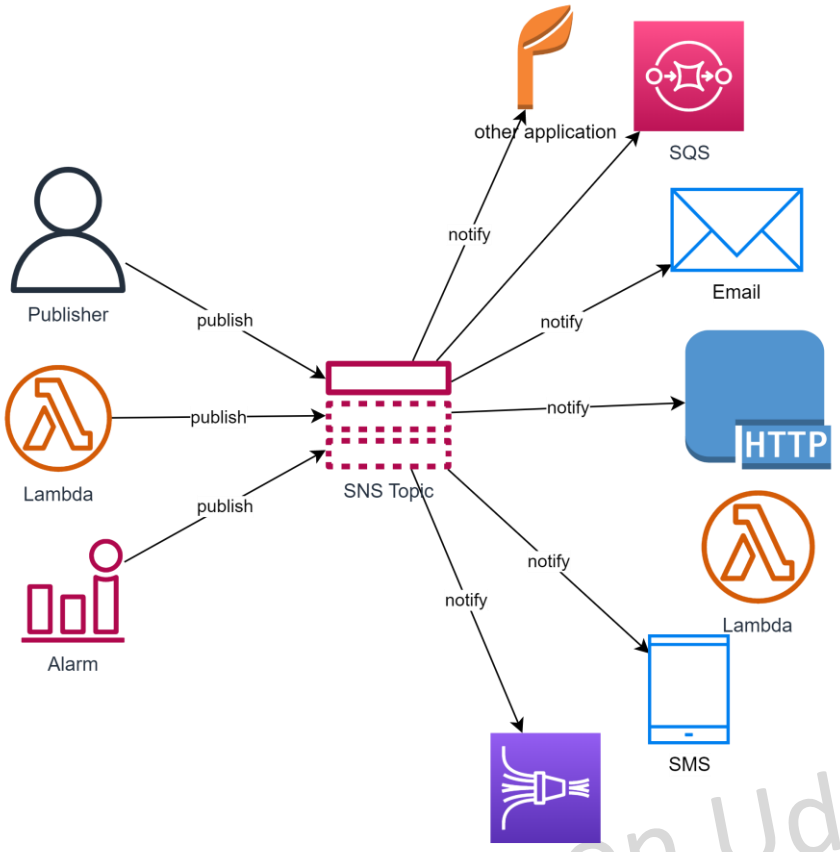
Container, ECS, ECR



Triển khai hệ thống sử dụng Docker, ECS, ECR

Decoupling, Messaging





Thanks you and see you in next chapter!