

câu 270

-----Service-----

***)Gateway VPC endpoint**

-chỉ hỗ trợ S3 và DynamoDB, không hỗ trợ Secrets Manager.

***)Permissions Boundaries**

-chỉ giới hạn quyền của IAM Role/User chứ không kiểm soát toàn bộ tài khoản như SCP.

***)AWS Config**

-AWS Config là một dịch vụ cho phép bạn đánh giá, kiểm tra và đánh giá cấu hình của các tài nguyên AWS. AWS Config liên tục theo dõi và ghi lại cấu hình của tài nguyên AWS, đồng thời cho phép bạn tự động đánh giá các cấu hình đã ghi lại so với cấu hình mong muốn.

-chỉ theo dõi và cảnh báo về các tài nguyên không tuân thủ, không ngăn chặn tài nguyên bị tạo ra sai quy chuẩn.

-Conformance packs giúp quản lý việc tuân thủ cấu hình của các tài nguyên AWS ở quy mô lớn bằng cách sử dụng một khung làm việc chung và mô hình đóng gói. Bạn có thể sử dụng các conformance packs dựng sẵn để quét lỗ hổng bảo mật, chẳng hạn như CIS Operating System Security Configuration Benchmarks hoặc Amazon Inspector Rules for Linux Instances. Ngoài ra, bạn cũng có thể tạo conformance packs tùy chỉnh để quét lỗ hổng trong các thư viện ngôn ngữ lập trình.

-ec2-managedinstance-applications-required là một AWS Config Rule kiểm tra xem các phiên bản EC2 được quản lý (Managed Instances) có cài đặt các ứng dụng bắt buộc hay không.

***)Amazon Inspector**

-là một dịch vụ quét bảo mật tự động của AWS, giúp phát hiện lỗ hổng bảo mật (CVE) và đánh giá tuân thủ trên các tài nguyên như Amazon EC2, AWS Lambda, và Amazon ECR (Elastic Container Registry).

-Mối liên hệ giữa Amazon Inspector, Security Hub và IAM Management Console

1. Amazon Inspector

- Tự động quét bảo mật EC2, Lambda, ECR để phát hiện lỗ hổng (CVE) và đánh giá tuân thủ.
- Gửi kết quả quét đến Security Hub để quản lý tập trung.

2. AWS Security Hub

- Thu thập, tổng hợp và phân tích dữ liệu bảo mật từ nhiều dịch vụ AWS, bao gồm Amazon Inspector.
- Cung cấp bảng điều khiển bảo mật tập trung giúp quản lý và khắc phục lỗ hổng.

3. IAM Management Console

- Quản lý quyền truy cập của Amazon Inspector và Security Hub thông qua IAM Role & Policies.
- Đảm bảo chỉ tài khoản hoặc dịch vụ được ủy quyền mới có thể quét, xem và xử lý kết quả bảo mật.

-Bạn cần cấu hình Amazon Inspector agent để sử dụng gói quy tắc CVE, đây là tập hợp các quy tắc giúp kiểm tra lỗ hổng bảo mật và các rủi ro trên các phiên bản EC2 của bạn. Bạn cũng cần cài đặt một thư viện tích hợp bổ sung để kích hoạt giao tiếp giữa Amazon Inspector agent và Security Hub. Security Hub là một dịch vụ cung cấp cái nhìn tổng quan về trạng thái bảo mật trong AWS, giúp bạn kiểm tra môi trường AWS theo các tiêu chuẩn bảo mật của ngành và các phương pháp tốt nhất. Các lựa chọn khác hoặc không chính xác, hoặc không đầy đủ để đáp ứng yêu cầu này.

-Amazon Inspector cung cấp khả năng quét liên tục và quét khi đẩy các image container trong Amazon ECR.

- Các phát hiện từ Amazon Inspector có thể được đẩy đến AWS Security Hub, một bảng điều khiển tập trung để quản lý các phát hiện bảo mật.
- Có thể tạo các quy tắc bao gồm (inclusion rules) trong Amazon ECR để chỉ quét các kho lưu trữ cụ thể, loại trừ các kho lưu trữ không cần quét.

-Amazon Inspector không thể tạo các quy tắc bao gồm trong chính nó, và AWS Config không phải là bảng điều khiển tập trung phù hợp để hiển thị các phát hiện bảo mật.

***)AWS CloudTrail**

-Công dụng chính:

- Ghi lại tất cả hoạt động API trên AWS (ai làm gì, khi nào, ở đâu?).
- Lưu log vào S3, CloudWatch Logs hoặc EventBridge để giám sát & phân tích.
- Dùng để điều tra sự cố bảo mật, kiểm tra compliance.

-Sử dụng AWS CLI, chạy lệnh `aws kms get-key-rotation-status` với tham số `--key-id` để kiểm tra ngày luân phiên của CMK.

-Sự kiện KeyRotation không tồn tại trong AWS CloudTrail.

-TerminateInstances là sự kiện xảy ra khi một Amazon EC2 Instance bị tắt và xóa vĩnh viễn.

-AssumeRoleWithSAML là sự kiện xảy ra khi một người dùng xác thực bằng SAML (Security Assertion Markup Language) để assume một IAM Role trong AWS.

-AWS CloudTrail Insights là một tính năng trong AWS CloudTrail giúp phát hiện và cảnh báo về các hoạt động API bất thường trong tài khoản AWS.

Chức năng chính:

- Phát hiện hành vi bất thường: Xác định các thay đổi đột ngột trong khối lượng hoặc loại API gọi.
- Giám sát các sự kiện quan trọng: Như tăng đột biến các yêu cầu IAM, thay đổi quyền hạn, hoặc truy cập dịch vụ bất thường.
- Cung cấp ngữ cảnh chi tiết: Hiển thị dữ liệu về thời gian, người thực hiện và hành động cụ thể.
- Tích hợp với CloudWatch: Có thể gửi cảnh báo khi phát hiện hoạt động bất thường.

Lợi ích:

- Tự động phát hiện sự cố bảo mật hoặc lỗi cấu hình.
- Giúp điều tra nhanh hơn bằng cách phân tích xu hướng API.
- Hỗ trợ tuân thủ bảo mật và quản lý rủi ro AWS.

CloudTrail Insights không dùng để bắt sự kiện cụ thể như đăng nhập thất bại, mà chỉ phát hiện bất thường tổng thể.

-AWS CloudTrail Lake là một tính năng của AWS CloudTrail cho phép lưu trữ, truy vấn và phân tích dữ liệu sự kiện nhật ký trong AWS một cách tập trung.

Chức năng chính:

- Lưu trữ dữ liệu nhật ký lâu dài trong một hồ dữ liệu bảo mật.
- Truy vấn sự kiện bằng SQL mà không cần thiết lập cơ sở dữ liệu riêng.
- Phân tích xu hướng và điều tra bảo mật từ các sự kiện CloudTrail.
- Tích hợp với các công cụ bảo mật như GuardDuty và Security Hub.

Lợi ích:

- Dễ dàng điều tra sự kiện bảo mật AWS.
- Tìm kiếm nhanh và linh hoạt với truy vấn SQL.
- Không cần thiết lập cơ sở hạ tầng riêng để quản lý nhật ký.

-CloudTrail Log File Integrity Validation giúp phát hiện bất kỳ thay đổi nào trong log files, đảm bảo log không bị chỉnh sửa hoặc xóa bởi hacker.

-Trong AWS CloudTrail, prefix là một tiền tố (folder ảo) được sử dụng khi lưu trữ log trong Amazon S3. Nó giúp tổ chức và truy vấn log dễ dàng hơn. Cấu trúc lưu trữ CloudTrail logs trên S3 Mặc định, log được lưu theo định dạng:

s3://<bucket-name>/AWSLogs/<account-id>/CloudTrail/<region>/<year>/<month>/<day>/

Ví dụ:

s3://my-cloudtrail-bucket/AWSLogs/123456789012/CloudTrail/us-east-1/2024/03/27/

***)CloudWatch**

-Công dụng chính:

- Thu thập, giám sát & phân tích log từ ứng dụng, hệ thống & AWS services.
- Hỗ trợ cảnh báo khi phát hiện lỗi hoặc bất thường.
- Dùng để giám sát ứng dụng & hạ tầng theo thời gian thực.

-CloudWatch Events không tạo sự kiện khi CMK được tự động xoay vòng. CloudWatch không có rule nào để phát hiện CMK rotation.

-Bằng cách cấu hình query logging và gửi nhật ký đến CloudWatch Logs, kỹ sư bảo mật có thể dễ dàng phân tích dữ liệu và sử dụng CloudWatch Contributor Insights để tạo các chuỗi thời gian hiển thị các truy vấn DNS phổ biến nhất. Giải pháp này tự động hóa quá trình ghi nhật ký và phân tích, giảm thiểu chi phí vận hành.

-CloudWatch Logs Insights là một công cụ phân tích log mạnh mẽ trong Amazon CloudWatch, cho phép truy vấn, lọc và trực quan hóa dữ liệu log từ Amazon CloudWatch Logs. Tính năng chính:

- Truy vấn log nhanh chóng bằng ngôn ngữ truy vấn mạnh mẽ.
- Tìm kiếm và lọc log theo thời gian thực, giúp phát hiện sự cố nhanh hơn.
- Trực quan hóa dữ liệu log với biểu đồ và bảng thống kê.
- Tích hợp với CloudWatch Dashboards để giám sát toàn diện.

-CloudWatch không thể trực tiếp gọi các công việc AWS Batch từ các phát hiện IAM Access Analyzer. Bạn sẽ cần sử dụng một dịch vụ khác như EventBridge hoặc SNS để kích hoạt công việc Batch.

-CloudWatchAgentServerPolicy cung cấp đúng các quyền cần thiết để EC2 instance có thể gửi log tới CloudWatch.

-Metric Filter trong AWS CloudWatch được sử dụng để trích xuất thông tin có ý nghĩa từ log dữ liệu và chuyển đổi chúng thành CloudWatch Metrics.

Cách hoạt động:

1. Phân tích log (từ CloudWatch Logs).
2. Xác định mẫu tìm kiếm (filter pattern).
3. Tạo CloudWatch metric dựa trên dữ liệu khớp với filter.

-CloudWatch Alarm trong AWS là một tính năng giúp giám sát số liệu (metrics) và tự động kích hoạt hành động khi một ngưỡng (threshold) nhất định bị vượt qua.

📌 Cách hoạt động:

1. Chọn một metric (ví dụ: CPU Utilization, số lần đăng nhập thất bại).
2. Định nghĩa điều kiện kích hoạt (ví dụ: CPU > 80% trong 5 phút).
3. Chọn hành động khi alarm kích hoạt (gửi thông báo SNS, tự động scale EC2, dừng instance...).

-CloudWatch không thể tải lên hoặc quản lý bằng chứng thủ công từ on-premises.

***)AWS Key Management Service (AWS KMS)**

-AWS Key Management Service (AWS KMS) là dịch vụ quản lý khóa mã hóa được AWS cung cấp. Nó giúp tạo, quản lý và kiểm soát việc sử dụng các khóa mã hóa để bảo vệ dữ liệu trên AWS.

-Lợi ích chính:

- Mã hóa dữ liệu cho nhiều dịch vụ AWS như S3, RDS, Secrets Manager.
- Quản lý quyền truy cập bằng IAM và chính sách KMS.
- Tự động xoay vòng khóa để tăng cường bảo mật.

AWS KMS giúp bảo vệ dữ liệu với mã hóa mạnh mẽ và kiểm soát truy cập linh hoạt.

-AWS KMS không tạo một CMK(Customer Managed Key) mới khi xoay vòng.CMK rotation chỉ thay đổi vật liệu khóa (key material) bên trong CMK chứ không tạo một CMK mới.

-Customer Managed CMK (khóa do khách hàng quản lý) và Custom Key Store (kho lưu trữ khóa tùy chỉnh) để có thể nhập khẩu vật liệu khóa của riêng mình.

- Customer Managed CMK cho phép công ty kiểm soát hoàn toàn việc quản lý khóa, bao gồm việc đặt ngày hết hạn và xóa khóa.
- Custom Key Store cho phép công ty sử dụng vật liệu khóa của riêng mình.

-Chức năng lên lịch xóa khóa (Schedule Key Deletion) trong AWS KMS cho phép bạn chỉ định thời gian chờ trước khi xóa Customer Master Key (CMK).

- Thời gian chờ tối thiểu là 7 ngày và tối đa là 30 ngày.
- Trong thời gian chờ, CMK sẽ không thể được sử dụng để mã hóa hoặc giải mã dữ liệu.

-SSE-KMS (Server-Side Encryption with AWS KMS keys) cho phép mã hóa dữ liệu trên Amazon S3 bằng các khóa quản lý bởi AWS KMS.

-AWS KMS Encrypt có thể chủ động mã hóa dữ liệu trước khi đẩy lên S3 bucket. Quá trình này gọi là Client-Side Encryption (CSE)

-SSE-KMS (Server-Side Encryption with AWS KMS keys) cho phép mã hóa dữ liệu trên Amazon S3 bằng các khóa quản lý bởi AWS KMS.Quá trình mã hóa diễn ra trên dịch vụ

-Key ID và ARN đều có thể được sử dụng để tham chiếu đến một CMK hợp lệ, nên đây không phải nguyên nhân gây lỗi.

-Alias (bí danh) là một cách hợp lệ để tham chiếu đến một CMK, nên việc sử dụng alias không gây ra lỗi.

-Key Policy trong AWS là một tập hợp các quy tắc xác định ai có quyền sử dụng và quản lý một AWS KMS key (Khóa quản lý trong AWS Key Management Service - KMS).

- ♦ Chức năng chính:
 - Kiểm soát quyền truy cập vào KMS key.
 - Xác định ai có thể mã hóa, giải mã dữ liệu hoặc quản lý khóa.
 - Được viết bằng JSON, tương tự IAM Policy.
- ♦ Các thành phần quan trọng:
 - Principal: Ai có quyền truy cập (IAM user, role, service, account).
 - Action: Hành động được phép (ví dụ: kms:Encrypt, kms:Decrypt, kms:DescribeKey).
 - Resource: Khóa KMS được áp dụng.
 - Condition: Điều kiện hạn chế truy cập (ví dụ: chỉ từ VPC hoặc tài khoản cụ thể).

-Grant trong AWS KMS (Key Management Service) là một cơ chế cấp quyền sử dụng Customer Master Key (CMK) cho các dịch vụ hoặc người dùng khác mà không cần chỉnh sửa chính sách chính của CMK.

Chức năng của Grant trong AWS KMS:

- Cho phép các thực thể được chỉ định (Principal) thực hiện các thao tác nhất định trên CMK (ví dụ: mã hóa, giải mã).
- Giúp quản lý quyền truy cập tạm thời hoặc có kiểm soát mà không cần thay đổi chính sách chính sách IAM.
- Có thể bị thu hồi (Revoke) bất cứ lúc nào nếu không còn cần thiết.

Theo tài liệu AWS KMS, grant token được trả về trong phản hồi của CreateGrant phải được sử dụng trong các lệnh mã hóa/giải mã cho đến khi grant được phổ biến hoàn toàn (thường mất vài giây).

Grant token từ phản hồi CreateGrant phải được truyền cho người dùng để sử dụng ngay lập tức.

***)AWS CloudHSM**

-AWS CloudHSM là một dịch vụ quản lý phần cứng bảo mật (HSM - Hardware Security Module) giúp bạn tạo và quản lý khóa mã hóa một cách an toàn.

- ♦ Đặc điểm chính:
 - ✓ Cung cấp HSM chuyên dụng tuân thủ tiêu chuẩn FIPS 140-2 cấp 3.
 - ✓ Hỗ trợ mã hóa, ký số, quản lý khóa mà AWS không thể truy cập.
 - ✓ Tích hợp với AWS KMS, database encryption, TLS/SSL offloading.
 - ✓ Đáp ứng các yêu cầu bảo mật và tuân thủ cao như PCI DSS, HIPAA.

🔧 Khi nào dùng?

- 👉 Khi cần kiểm soát tuyệt đối khóa mã hóa (thay vì AWS quản lý như KMS).
- 👉 Khi yêu cầu bảo mật bắt buộc sử dụng HSM vật lý chuyên dụng.

***)Amazon Security Lake**

+)Amazon Security Lake, khi được cấu hình với tài khoản quản trị viên được ủy quyền trong AWS Organizations, cung cấp một giải pháp tập trung để tổng hợp, tổ chức và ưu tiên dữ liệu bảo mật từ nhiều nguồn, bao gồm:

- Dịch vụ AWS,
- Giải pháp từ AWS Marketplace,
- Hệ thống on-premises (tại chỗ).

+)Bằng cách kích hoạt Security Lake cho toàn bộ tổ chức và thêm các tài khoản AWS cần thiết, giải pháp này giúp tập trung hóa việc thu thập và phân tích log.

+)CloudHSM cho phép bạn kiểm soát hoàn toàn các khóa mã hóa của mình, bao gồm:

- Khóa đối xứng (AES)
- Khóa bất đối xứng (RSA)
- SHA-256, SHA-512
- Mã hóa dựa trên Hash
- Chữ ký số (RSA)

Ngược lại, AWS Key Management Service (KMS) là dịch vụ lưu trữ khóa đa tenant (nhiều người dùng chung) được sở hữu và quản lý bởi AWS.

***)Amazon GuardDuty**

-Amazon GuardDuty là dịch vụ phát hiện mối đe dọa (threat detection) trên AWS, giúp phân tích log dữ liệu và phát hiện hoạt động đáng ngờ trong tài khoản AWS của bạn.

-Phát hiện tấn công: Như brute force, tài khoản AWS bị xâm nhập, dữ liệu bị đánh cắp.

-Phân tích tự động: Dựa trên AI/ML và threat intelligence.

-Tích hợp với Security Hub & EventBridge: Giúp tự động hóa phản ứng bảo mật.

-Các phát hiện của GuardDuty chỉ tự động được gửi đến Security Hub nếu tích hợp GuardDuty với Security Hub được kích hoạt trong cùng một tài khoản và cùng một khu vực (Region). Điều này có nghĩa là tài khoản bảo mật (security tooling account), đóng vai trò là quản trị viên được ủy quyền cho cả GuardDuty và Security Hub, phải bật tích hợp GuardDuty với Security Hub trong từng tài khoản thành viên và từng khu vực nơi GuardDuty được kích hoạt. Nếu không, các phát hiện từ GuardDuty sẽ không hiển thị trong Security Hub.

-Impact: IAMUser/AnomalousBehavior là một phát hiện cho thấy hành vi bất thường từ một người dùng IAM trong tài khoản AWS của bạn.

***)AWS Systems Manager**

-AWS Systems Manager là một dịch vụ giúp tự động hóa và quản lý tài nguyên AWS.

-Bạn có thể sử dụng Systems Manager để giám sát các chính sách bucket S3 nhằm phát hiện quyền ghi công khai bằng cách sử dụng State Manager association, chạy một tài liệu được xác định trước có tên AWS-FindS3BucketWithPublicWriteAccess. Tài liệu này kiểm tra từng S3 bucket trong tài khoản và báo cáo bất kỳ bucket nào có quyền ghi công khai được bật.

-AWS Systems Manager (SSM) có khả năng thu thập thông tin chi tiết về phần mềm đang chạy trên các EC2 instances, bao gồm phiên bản của các framework được cài đặt. SSM có thể nhanh chóng quét hàng loạt instances để tìm phiên bản cụ thể của phần mềm mà không cần cấu hình phức tạp.

-AWS Systems Manager Inventory tự động thu thập thông tin về cấu hình phần mềm và phần cứng trên các EC2 instances hoặc máy chủ on-premises.

♦ Chức năng chính:

- ✓ Ghi nhận thông tin phần mềm: Hệ điều hành, ứng dụng, bản vá, service, v.v.
- ✓ Truy vấn và lọc dữ liệu: Dễ dàng tìm kiếm các phần mềm dựa trên tên, phiên bản.
- ✓ Tích hợp với AWS Systems Manager Automation: Hỗ trợ khắc phục lỗi tự động.
- ✓ Tăng cường bảo mật: Xác định nhanh các phần mềm lỗi thời hoặc có lỗ hổng bảo mật.

***)AWS Systems Manager Session Manager**

-AWS Systems Manager Session Manager là công cụ giúp truy cập an toàn vào EC2 instances mà không cần SSH hoặc RDP.

-Không cần mở cổng SSH (22) hoặc RDP (3389) → Giảm rủi ro bảo mật.

-Tích hợp IAM → Quản lý quyền truy cập chặt chẽ.

-Ghi log phiên làm việc vào S3 hoặc CloudWatch → Dễ kiểm tra & giám sát.

-Hỗ trợ cả Linux & Windows.

-Ví dụ: Dùng Session Manager để truy cập EC2 từ AWS Console mà không cần key SSH.

-Cách hoạt động:

1. Người dùng đăng nhập vào AWS Console hoặc sử dụng AWS CLI.
2. Gửi yêu cầu kết nối tới AWS Systems Manager (SSM).
3. SSM Agent trên EC2 nhận yêu cầu, xác thực IAM Role.
4. Kết nối an toàn được thiết lập giữa AWS Console và EC2 thông qua SSM mà không cần SSH/RDP.
5. Ghi log phiên làm việc vào Amazon S3 / CloudWatch (nếu được bật).

Người dùng → AWS Console → AWS Systems Manager → SSM Agent trên EC2 → Kết nối Terminal (Bảo mật)

***)EC2 Instance Connect**

-EC2 Instance Connect là công cụ giúp truy cập EC2 Linux thông qua SSH từ AWS Console.

-Chỉ hỗ trợ Amazon Linux & Ubuntu.

-Không cần SSH key, sử dụng IAM permissions.

-Gửi public SSH key tạm thời để đăng nhập an toàn.

-Ví dụ: Khi không có SSH key nhưng cần truy cập nhanh vào EC2, có thể dùng EC2 Instance Connect từ AWS Console.

-EC2 Instance Connect (Dùng SSH nhưng không cần key)

-Cách hoạt động:

1. Người dùng mở AWS Console hoặc sử dụng EC2 Instance Connect CLI.
2. AWS gửi SSH Key tạm thời đến EC2 Instance.
3. Người dùng kết nối SSH vào EC2 bằng key tạm thời.
4. Khi phiên kết thúc, key SSH bị xóa.

Người dùng → AWS Console → EC2 Instance Connect → EC2 (Qua SSH tạm thời)

***)AWS Trusted Advisor**

-AWS Trusted Advisor là công cụ tư vấn giúp bạn tối ưu hóa tài nguyên AWS bằng cách kiểm tra và đề xuất cải thiện hiệu suất, bảo mật, chi phí, độ tin cậy và giới hạn dịch vụ.

-Các loại kiểm tra chính:

- Cost Optimization – Đề xuất cắt giảm chi phí (ví dụ: EC2 dư thừa, S3 không dùng).

- Security – Kiểm tra lỗ hổng bảo mật (ví dụ: S3 public, IAM không an toàn).
- Fault Tolerance – Đề xuất cải thiện độ tin cậy (ví dụ: backup, Multi-AZ).
- Performance – Kiểm tra hiệu suất (ví dụ: cấu hình EC2, RDS).
- Service Limits – Cảnh báo giới hạn AWS (ví dụ: số lượng EC2, VPC).

-IAM Trusted Advisor là một tính năng của AWS Trusted Advisor giúp kiểm tra và đề xuất cải thiện bảo mật IAM trong tài khoản AWS. **Các kiểm tra quan trọng của IAM Trusted Advisor:**

- Quyền admin không cần thiết → Xác định IAM users/roles có quyền quá rộng.
- Không sử dụng MFA → Cảnh báo nếu IAM users không bật Multi-Factor Authentication (MFA).
- Access key cũ hoặc không sử dụng → Đề xuất xóa hoặc xoay vòng access key lâu ngày không hoạt động.
- Root account đang sử dụng access key → Cảnh báo nếu tài khoản root có access key (nên xóa để tăng bảo mật).

***)Amazon EventBridge**

-Công dụng chính:

- Dịch vụ bus sự kiện giúp kích hoạt hành động tự động khi có sự kiện AWS.
- Nhận sự kiện từ AWS CloudTrail, CloudWatch Logs, hoặc ứng dụng rồi gửi đến Lambda, SNS, SQS...
- Dùng để tự động hóa, tích hợp giữa các dịch vụ AWS & bên thứ ba.

-Ví dụ Kết hợp:

1. CloudTrail ghi nhận sự kiện xóa S3 bucket.
2. Sự kiện này được gửi đến EventBridge, kích hoạt AWS Lambda để cảnh báo.
3. CloudWatch Logs theo dõi & phân tích log để tìm dấu hiệu bất thường.

-Tóm lại:

- CloudTrail = Ghi log hoạt động API.
- CloudWatch Logs = Giám sát & phân tích log hệ thống & ứng dụng.
- EventBridge = Xử lý sự kiện & tự động hóa dựa trên log từ các dịch vụ khác.

-Amazon EventBridge tích hợp sẵn với ACM để theo dõi các sự kiện liên quan đến chứng chỉ, bao gồm cả việc chứng chỉ sắp hết hạn.

-Bằng cách sử dụng mẫu định sẵn, bạn có thể dễ dàng cấu hình một quy tắc để kích hoạt cảnh báo khi chứng chỉ sắp hết hạn và gửi thông báo qua Amazon SNS.

***)AWS Control Tower**

-AWS Control Tower là dịch vụ giúp thiết lập và quản lý môi trường AWS đa tài khoản theo các tiêu chuẩn và thực tiễn tốt nhất. Nó cung cấp:

- Landing Zone: Môi trường AWS được thiết lập sẵn với bảo mật và quản trị.
- Guardrails: Các chính sách bảo mật và quy tắc kiểm soát.
- Account Factory: Tự động hóa việc tạo tài khoản AWS mới theo chuẩn.
- Dashboard: Giao diện giám sát và quản lý tập trung.

-Chức năng chính:

- Thiết lập tài khoản tự động theo cấu trúc tổ chức chuẩn.
- Quản lý chính sách tập trung bằng Guardrails (giới hạn bảo mật & tuân thủ).
- Theo dõi và giám sát trạng thái tuân thủ trong toàn bộ môi trường AWS.

Nói ngắn gọn, AWS Control Tower giúp tự động hóa và đơn giản hóa việc quản lý nhiều tài khoản AWS theo tiêu chuẩn an toàn.

-Nó phù hợp cho doanh nghiệp muốn quản lý nhiều tài khoản AWS một cách an toàn, tuân thủ quy định.

***)CloudFront**

-CloudFront geo restriction cho phép công ty hạn chế quyền truy cập vào nội dung dựa trên vị trí địa lý của người dùng.

- Bằng cách thêm một danh sách từ chối (deny list) các quốc gia mà công ty không có giấy phép phân phối, công ty có thể ngăn chặn việc truy cập hình ảnh từ các quốc gia đó.
- Đây là một cách hiệu quả để hạn chế phân phối hình ảnh theo yêu cầu pháp lý.

-Tùy chọn Restrict Viewer Access trong CloudFront được sử dụng để hạn chế quyền truy cập vào nội dung bằng cách yêu cầu chữ ký URL hoặc cookie, không phải để hạn chế truy cập dựa trên vị trí địa lý.

-CloudFront signed URL là cách bảo mật nhất để cung cấp quyền truy cập tạm thời và có kiểm soát đến các tệp tin trong bucket S3.URL được ký có thể được cấu hình để hết hạn sau một khoảng thời gian nhất định, đảm bảo rằng quyền truy cập chỉ được cấp trong thời gian ngắn.CloudFront cũng hỗ trợ sử dụng tên miền tùy chỉnh (ví dụ: example.com), đáp ứng yêu cầu về việc tải xuống từ tên miền tùy chỉnh.

-Chọn "Restrict Bucket Access" trong cài đặt nguồn gốc của CloudFront sẽ tự động tạo một origin access identity (OAI) và cập nhật chính sách bucket S3 để chỉ cho phép CloudFront truy cập vào bucket.

-Để bảo vệ nội dung video được phát trực tiếp thông qua CloudFront, cách đơn giản nhất và hiệu quả nhất là sử dụng signed cookies. Signed cookies cho phép người dùng truy cập nội dung được bảo vệ mà không cần thay đổi URL, đồng thời đảm bảo rằng chỉ người dùng đã xác thực mới có thể truy cập.

-Lambda@Edge là tính năng của AWS giúp chạy AWS Lambda function tại các edge locations của Amazon CloudFront, giảm độ trễ và tối ưu hiệu suất cho người dùng toàn cầu.
Chức năng chính:

Xử lý request và response gần người dùng → Giảm thời gian phản hồi.

Tùy chỉnh nội dung động → Thay đổi HTTP headers, redirect, kiểm tra xác thực.

Chạy logic serverless mà không cần máy chủ backend.

Trường hợp sử dụng:

- Tăng tốc website bằng cách thay đổi cache key trước khi CloudFront lưu trữ nội dung.
- Thực hiện xác thực JWT hoặc kiểm tra bảo mật ngay tại edge.
- Redirect URL động hoặc rewrite path trước khi gửi request về origin.

Tóm lại: Lambda@Edge giúp xử lý yêu cầu gần người dùng hơn, giảm tải backend, tối ưu hiệu suất & bảo mật.

-AWS WAF không thể được sử dụng làm nguồn gốc (origin) của CloudFront. AWS WAF chỉ hoạt động như một lớp bảo vệ trước khi yêu cầu đến được origin.

-Việc tạo một CloudFront distribution và cấu hình ALB làm origin có thể giúp giảm tải cho máy chủ Tomcat bằng cách cung cấp nội dung đã được cache cho người dùng cuối. Ngoài ra, CloudFront cũng giúp bảo vệ trước các cuộc tấn công DDoS bằng cách lọc lưu lượng độc hại ngay tại các edge locations.

-SecurityHeadersPolicy là chính sách tiêu đề phản hồi được quản lý sẵn bởi AWS, bao gồm các tiêu đề bảo mật quan trọng để chống tấn công man-in-the-middle:

- Strict-Transport-Security (HSTS): Bắt buộc kết nối HTTPS, ngăn chặn downgrade attack.
- X-Content-Type-Options: Chống MIME sniffing.
- X-Frame-Options: Chống clickjacking.
- Content-Security-Policy: Giảm thiểu XSS.
- Ưu điểm:
 - Không cần viết code (như Lambda@Edge).
 - Dễ triển khai: Chỉ cần gắn policy vào CloudFront distribution.
 - Tự động cập nhật khi AWS thêm tính năng mới.

***)AWS Fargate**

-AWS Fargate: Một tùy chọn của ECS (và EKS) giúp chạy container không cần quản lý server. Với Fargate, AWS tự động quản lý hạ tầng, giúp đơn giản hóa việc triển khai và mở rộng container mà không cần quan tâm đến EC2 instances.

***)AWS Elastic Load Balancers (ELB)**

-AWS Elastic Load Balancers (ELB) không thể gửi nhật ký truy cập (access logs) trực tiếp đến CloudWatch Logs. ELB chỉ có thể gửi nhật ký truy cập đến S3. Do đó, đáp án này không khả thi.

***)AWS Network Load Balancer (NLB)**

-AWS Network Load Balancer (NLB) là một dịch vụ cân bằng tải hoạt động ở tầng 4 (Transport Layer) của mô hình OSI, giúp phân phối lưu lượng TCP, UDP, và TLS đến các Amazon EC2 instances, containers, hoặc on-premises servers.

-Đặc điểm chính của AWS NLB:

- Hiệu suất cao: Xử lý hàng triệu yêu cầu mỗi giây với độ trễ cực thấp.
- IP tĩnh & Elastic IP: Dễ dàng gán IP cố định cho NLB.
- Sticky Sessions (cố định phiên): Duy trì kết nối với backend cụ thể.
- Tích hợp AWS Auto Scaling: Tự động mở rộng hoặc thu hẹp quy mô.
- Zonal Failover: Hỗ trợ cân bằng tải đa vùng sẵn sàng (Multi-AZ).

-Ứng dụng: Thích hợp cho API, game, VoIP, ứng dụng tài chính yêu cầu độ trễ thấp. 🚀

-Trạng thái InService trong ngữ cảnh của Network Load Balancer (NLB) có nghĩa là máy chủ đích (target instance) đã vượt qua health checks và sẵn sàng nhận lưu lượng truy cập từ NLB. Khi một máy chủ đích ở trạng thái này, NLB sẽ phân phối lưu lượng đến nó. Nếu máy chủ đích không vào được trạng thái InService, điều này thường có nghĩa là health checks đang thất bại, và máy chủ đó sẽ không nhận được lưu lượng từ NLB.

***)Amazon S3 Glacier**

-Amazon S3 Glacier là một dịch vụ lưu trữ đám mây của AWS, chuyên dùng để lưu trữ dữ liệu ít truy cập với chi phí thấp. Nó phù hợp cho việc lưu trữ lâu dài, như sao lưu, lưu trữ tài liệu hoặc dữ liệu tuân thủ quy định.

-Amazon S3 Glacier với Vault Lock policy. Đây là giải pháp phù hợp nhất để đáp ứng yêu cầu lưu trữ dữ liệu trong 7 năm mà không thể thay đổi hoặc xóa. S3 Glacier được thiết kế cho việc lưu trữ dài hạn với chi phí thấp, và Vault Lock policy cho phép khóa dữ liệu để đảm bảo tuân thủ các yêu cầu pháp lý.

***)AWS Secrets Manager**

-AWS Secrets Manager là một **dịch vụ quản lý thông tin bí mật** (secrets), giúp lưu trữ, quản lý và truy xuất **một cách an toàn các thông tin nhạy cảm** như:

- Mật khẩu cơ sở dữ liệu
- Khóa API
- Thông tin xác thực khác

-Để xoay vòng thông tin đăng nhập của cơ sở dữ liệu mỗi 30 ngày, giải pháp an toàn và hiệu quả nhất là lưu trữ thông tin đăng nhập trong AWS Secrets Manager và cấu hình xoay vòng tự động mỗi 30 ngày. Secrets Manager có thể tự động xoay vòng thông tin đăng nhập cả trong bí mật (secret) lẫn trong cơ sở dữ liệu, đồng thời sử dụng AWS KMS để mã hóa thông tin đăng nhập.

***)AWS Security Hub**

-AWS Security Hub mặc định chỉ tổng hợp các phát hiện (findings) trong cùng một Region. Để nhận được findings từ tất cả các Regions, bạn cần một cơ chế để thu thập và định tuyến dữ liệu từ các Regions khác về tài khoản Security Hub chuyên dụng.

-Custom Action trong AWS Security Hub là các hành động tùy chỉnh do người dùng thiết lập để phản hồi các phát hiện bảo mật theo nhu cầu cụ thể.

Ví dụ về Custom Action:

1. Gửi cảnh báo đến CloudWatch Logs – Lưu trữ phát hiện để phân tích sau.
2. Kích hoạt AWS Lambda – Tự động hóa phản ứng, như cô lập một máy chủ bị tấn công.
3. Gửi thông báo đến SNS – Cảnh báo nhóm bảo mật qua email hoặc tin nhắn.
4. Tạo vé sự cố trong hệ thống ITSM – Tích hợp với Jira, ServiceNow để theo dõi và xử lý.

-AWS Security Hub không hỗ trợ tải lên hoặc quản lý bằng chứng thủ công từ on-premises.

***)Amazon ECR (Elastic Container Registry)**

-Amazon ECR (Elastic Container Registry) là một dịch vụ của AWS giúp lưu trữ, quản lý và triển khai các container images một cách an toàn.

-Đặc điểm chính:

- Private & Public Registry: Hỗ trợ cả registry riêng tư và công khai.

- Tích hợp với AWS: Dễ dàng tích hợp với Amazon ECS, EKS, và AWS Lambda.
- Bảo mật: Hỗ trợ IAM, encryption, và vulnerability scanning.
- Tối ưu hóa hiệu suất: Hỗ trợ caching và tăng tốc pull image.

-Ứng dụng:

- Lưu trữ container images cho Kubernetes, Docker Swarm.
- Tích hợp CI/CD để tự động hóa triển khai container.

-Tính năng chính:

- Lưu trữ hình ảnh container: Hỗ trợ Docker và OCI (Open Container Initiative).
- Bảo mật: Tích hợp IAM để kiểm soát quyền truy cập, hỗ trợ quét lỗ hổng bảo mật.
- Tích hợp AWS: Kết hợp dễ dàng với ECS, EKS, Lambda và các dịch vụ AWS khác.
- Hiệu suất cao: Hỗ trợ caching để tăng tốc độ pull image.

-Tóm lại ECR giúp bạn lưu trữ và quản lý hình ảnh container một cách an toàn, tiết kiệm và tích hợp tốt với hệ sinh thái AWS.

-Tính năng quét cơ bản của ECR không cung cấp khả năng quét liên tục và không tích hợp trực tiếp với AWS Security Hub.

***)AWS RAM (Resource Access Manager)**

-AWS RAM (Resource Access Manager) là dịch vụ cho phép chia sẻ tài nguyên AWS giữa các tài khoản AWS khác nhau một cách an toàn mà không cần phải sao chép dữ liệu.

-Tài nguyên có thể chia sẻ qua AWS RAM:

- VPC Subnets (cho phép nhiều tài khoản dùng chung VPC).
- Transit Gateway (kết nối mạng giữa nhiều VPC).
- License Manager (chia sẻ giấy phép phần mềm).
- Route 53 Resolver Rules (chia sẻ quy tắc DNS).

***)AWS Nitro Enclaves**

AWS Nitro Enclaves là một tính năng của Amazon EC2, giúp tạo ra môi trường tính toán cô lập, an toàn để xử lý dữ liệu nhạy cảm mà không bị truy cập từ bên ngoài, ngay cả từ hệ điều hành chính của EC2.

-Đặc điểm chính của Nitro Enclaves:

- Cô lập hoàn toàn: Không có quyền truy cập mạng, không có lưu trữ vĩnh viễn, không truy cập từ hệ điều hành EC2.
- Bảo mật cao: Chỉ giao tiếp với EC2 thông qua vsock (virtual socket), giúp hạn chế rủi ro tấn công.
- Tích hợp AWS KMS: Giải mã dữ liệu bằng AWS Key Management Service (KMS) mà không để lộ khóa.
- Sử dụng Nitro Hypervisor: Tận dụng công nghệ Nitro để tạo enclave từ tài nguyên EC2 mà không ảnh hưởng đến hiệu suất chính.
- Dùng để xử lý dữ liệu nhạy cảm: Chạy các ứng dụng xử lý dữ liệu y tế, tài chính, khóa mã hóa, chứng thực giao dịch, AI bảo mật, v.v.

***)AWS CloudFormation**

-AWS CloudFormation là một dịch vụ giúp tự động hóa việc triển khai và quản lý hạ tầng AWS bằng cách sử dụng mẫu (template) dưới dạng tệp YAML hoặc JSON.

-“aws cloudformation validate-template” chỉ kiểm tra cú pháp của mẫu CloudFormation, không kiểm tra tuân thủ các tiêu chuẩn bảo mật.

-CloudFormation Template là một tệp JSON hoặc YAML dùng để định nghĩa hạ tầng AWS dưới dạng code. Nó mô tả các tài nguyên AWS (EC2, S3, RDS, IAM, v.v.) mà bạn muốn tạo và quản lý bằng AWS CloudFormation.

Cấu trúc chính của template:

- Resources (bắt buộc): Xác định tài nguyên AWS cần tạo.
- Parameters: Định nghĩa giá trị động (VD: loại instance).
- Outputs: Xuất thông tin sau khi stack triển khai.
- Conditions: Điều kiện tạo tài nguyên.

Lợi ích:

Tự động hóa hạ tầng (IaC).

Dễ dàng triển khai, cập nhật và rollback.

Quản lý tài nguyên nhất quán, giảm lỗi cấu hình. 🚀

-Trong AWS CloudFormation, Stack là một tập hợp các tài nguyên AWS được tạo, quản lý và xóa cùng nhau thông qua một CloudFormation template.

Cách hoạt động:

1. Viết template (định nghĩa tài nguyên như EC2, S3, IAM, v.v.).
2. Tạo Stack từ template → CloudFormation tự động triển khai tài nguyên.
3. Cập nhật hoặc xóa Stack để thay đổi hoặc gỡ bỏ tài nguyên.

Lợi ích:

- Tự động hóa hạ tầng (IaC - Infrastructure as Code).
- Dễ dàng quản lý & triển khai hàng loạt.
- Rollback nếu lỗi xảy ra.

-Tóm lại: Template là kế hoạch, còn Stack là triển khai thực tế của kế hoạch đó.

***)AWS CloudFormation Guard (cfn-guard)**

-AWS CloudFormation Guard (cfn-guard) là công cụ giúp xác thực và thực thi quy tắc bảo mật trên các tệp CloudFormation. Nó cho phép bạn viết các policy rules để kiểm tra xem cấu hình hạ tầng có tuân thủ các tiêu chuẩn bảo mật, chi phí và best practices hay không.

-Cách hoạt động:

1. Viết quy tắc trong Guard Rules (ví dụ: bắt buộc S3 Bucket phải bật mã hóa).
2. Chạy cfn-guard validate để kiểm tra CloudFormation template.
3. Nếu vi phạm, Guard sẽ báo lỗi và đề xuất sửa đổi.

-Lợi ích:

- Đảm bảo compliance tự động.
- Giúp phát hiện lỗi cấu hình sớm trước khi triển khai.
- Tích hợp CI/CD để kiểm tra liên tục.

-Lệnh “cfn-guard” là công cụ dòng lệnh trong AWS CloudFormation Guard dùng để kiểm tra xem một CloudFormation template có tuân thủ các quy tắc bảo mật và cấu hình không.

***)Amazon Route 53**

-Amazon Route 53 là dịch vụ DNS (Domain Name System) được quản lý của AWS, giúp phân giải tên miền thành địa chỉ IP để kết nối với ứng dụng.

-Tính năng chính:

- Quản lý tên miền: Đăng ký, chuyển và quản lý tên miền.
- DNS Routing: Định tuyến lưu lượng theo nhiều phương thức (Weighted, Latency, Geolocation...).

- Health Checks & Failover: Giám sát trạng thái máy chủ và tự động chuyển hướng khi có sự cố.
- Hỗ trợ DNSSEC: Tăng cường bảo mật bằng chữ ký số.
- Tích hợp với AWS: Kết nối dễ dàng với S3, CloudFront, ELB...

-Amazon Route 53 Resolver query logging là dịch vụ được thiết kế để ghi lại tất cả các truy vấn DNS trong VPC.

-DNS sinkhole là một kỹ thuật chuyển hướng lưu lượng độc hại hoặc không mong muốn đến một đích đến khác, chẳng hạn như một máy chủ "black hole" hoặc "honeypot". Bằng cách sửa đổi hosted zone trong Route 53 và tạo một DNS sinkhole cho địa chỉ IP độc hại, Kỹ sư Bảo mật có thể chặn bot độc hại không thể tiếp cận instance EC2 trên subnet công cộng. Các tùy chọn khác hoặc là không hiệu quả hoặc không phù hợp để chặn bot độc hại.

***)Amazon Macie**

-Amazon Macie là dịch vụ bảo mật dữ liệu trên AWS, sử dụng machine learning để phát hiện, phân loại và bảo vệ dữ liệu nhạy cảm trong Amazon S3.

-Tính năng chính:

- Phát hiện dữ liệu nhạy cảm: Tự động tìm kiếm PII (Personally Identifiable Information), thông tin tài chính, bảo mật...
- Quét và phân loại dữ liệu: Xác định nội dung trong S3 và cảnh báo về dữ liệu có nguy cơ rò rỉ.
- Tích hợp với AWS Security Services: Kết nối với AWS CloudTrail, EventBridge, Security Hub để giám sát và phản hồi sự cố.
- Báo cáo và trực quan hóa: Hiển thị kết quả quét qua AWS Console hoặc gửi cảnh báo đến hệ thống bảo mật.

***)Amazon Athena**

-Amazon Athena là một dịch vụ truy vấn dữ liệu serverless, cho phép bạn sử dụng SQL để truy vấn trực tiếp dữ liệu trong Amazon S3 mà không cần thiết lập cơ sở dữ liệu.

-Tính năng chính:

- Truy vấn dữ liệu bằng SQL: Hỗ trợ ANSI SQL để phân tích dữ liệu trong S3.
- Không cần quản lý hạ tầng: Hoạt động serverless, không yêu cầu cài đặt hoặc quản lý cơ sở dữ liệu.
- Tích hợp với AWS Glue: Có thể sử dụng AWS Glue Data Catalog để quản lý schema.
- Thanh toán theo truy vấn: Chỉ trả phí cho dung lượng dữ liệu quét, giúp tối ưu chi phí.

***)AWS IAM Access Analyzer**

-AWS IAM Access Analyzer là một công cụ giúp bạn xác định quyền truy cập không mong muốn vào tài nguyên AWS. Nó tự động phân tích các chính sách IAM, S3, KMS, Lambda, SQS và các dịch vụ khác để phát hiện xem có bất kỳ tài nguyên nào được chia sẻ ngoài tổ chức của bạn hay không. Điều này giúp tăng cường bảo mật và đảm bảo tuân thủ chính sách truy cập.

-IAM Access Analyzer không giám sát đăng nhập Console, mà tập trung vào phân tích quyền IAM.

***)AWS Shield Advanced**

-AWS Shield Advanced là một dịch vụ bảo vệ chống tấn công DDoS nâng cao dành cho các ứng dụng chạy trên AWS. Nó cung cấp khả năng phát hiện, giảm thiểu tấn công theo thời gian thực, phân tích lưu lượng, hỗ trợ 24/7 từ AWS DDoS Response Team (DRT), và bảo hiểm chi phí phát sinh do tấn công.

-AWS Shield Standard (miễn phí) bảo vệ chống lại các cuộc tấn công DDoS lớp 3/4 phổ biến.

-AWS Shield Advanced (trả phí) cung cấp bảo vệ nâng cao, giảm thiểu tấn công phức tạp hơn.

-Bạn có thể tạo một Amazon CloudWatch alarm để giám sát các số liệu của Shield Advanced, chẳng hạn như:

- DDoSAttackBitsPerSecond
- DDoSAttackPacketsPerSecond
- DDoSAttackRequestsPerSecond

Điều này giúp bạn nhận được cảnh báo nếu tài khoản của mình bị tấn công DDoS.

***)AWS Service Catalog**

-AWS Service Catalog là một dịch vụ giúp các tổ chức quản lý, triển khai và kiểm soát danh mục các tài nguyên AWS đã được phê duyệt. Nó cho phép quản trị viên tạo và quản lý các danh mục chứa Amazon EC2, RDS, S3, Lambda, v.v., giúp đảm bảo rằng người dùng chỉ có thể triển khai các tài nguyên tuân thủ chính sách của tổ chức.

-Lợi ích chính:

- Kiểm soát & Quản lý: Định nghĩa các danh mục dịch vụ chuẩn để đảm bảo tuân thủ bảo mật và chi phí.
- Tự động hóa & Triển khai dễ dàng: Người dùng có thể triển khai các dịch vụ được phê duyệt mà không cần kiến thức chuyên sâu về AWS.
- Bảo mật & Tuân thủ: Giúp doanh nghiệp kiểm soát quyền truy cập và tránh việc sử dụng tài nguyên không được phép.

-Ứng dụng thực tế: Doanh nghiệp có thể sử dụng AWS Service Catalog để cung cấp các mẫu hạ tầng tiêu chuẩn, giúp nhân viên dễ dàng triển khai ứng dụng mà vẫn đảm bảo tính bảo mật và tối ưu chi phí.

-AWS Service Catalog portfolio là một tập hợp các products (sản phẩm) trong AWS Service Catalog, giúp tổ chức quản lý và kiểm soát việc triển khai tài nguyên AWS theo quy định. Portfolio cho phép quản trị viên nhóm các sản phẩm, cấp quyền truy cập cho người dùng hoặc nhóm, và áp dụng các chính sách bảo mật và quản trị.

-Bạn có thể sử dụng Service Catalog để quản lý tập trung các dịch vụ CNTT được triển khai phổ biến, giúp đảm bảo các yêu cầu về quản trị và tuân thủ nhất quán, đồng thời cho phép người dùng nhanh chóng triển khai các dịch vụ CNTT đã được phê duyệt mà họ cần.

***)Amazon Cognito**

-Amazon Cognito là dịch vụ của AWS giúp xác thực và quản lý người dùng cho ứng dụng web và di động. Nó hỗ trợ đăng nhập bằng tài khoản email, số điện thoại, hoặc các nền tảng bên thứ ba như Google, Facebook, Apple.

-Thành phần chính của Amazon Cognito:

1. User Pools – Cung cấp hệ thống đăng nhập, xác thực người dùng, hỗ trợ MFA (xác thực hai yếu tố).
2. Identity Pools – Cấp quyền truy cập tạm thời vào AWS services (S3, DynamoDB...) sau khi xác thực.

-Amazon Cognito có thể tích hợp với ADFS thông qua SAML, cho phép nhân viên xác thực bằng thông tin đăng nhập hiện có của họ.

-Sử dụng Amazon Cognito identity pool và SDK yêu cầu thay đổi ứng dụng, điều này không phù hợp với yêu cầu của bài toán.

***)AWS Software Development Kit (SDK)**

-AWS SDK (Software Development Kit) là bộ công cụ phát triển phần mềm giúp lập trình viên tích hợp và tương tác với các dịch vụ AWS bằng cách sử dụng các ngôn ngữ lập trình phổ biến như Python, Java, JavaScript, C#, Go, Ruby, PHP, v.v.

♦ Chức năng chính:

✓ Cung cấp API để dễ dàng gọi dịch vụ AWS như S3, EC2, Lambda, DynamoDB, IAM...

✓ Hỗ trợ xác thực AWS IAM, giúp bảo mật khi truy cập dịch vụ.

✓ Quản lý phiên bản và lỗi khi giao tiếp với AWS.

✓ Tích hợp với AWS CLI và AWS CloudFormation để tự động hóa hạ tầng.

***)AWS Systems Manager Parameter Store**

-AWS Systems Manager Parameter Store là một dịch vụ giúp lưu trữ, quản lý và truy xuất cấu hình hoặc thông tin bí mật một cách an toàn cho các ứng dụng và tài nguyên AWS.

-Tính năng chính:

- Lưu trữ giá trị dưới dạng key-value: Hỗ trợ chuỗi văn bản, danh sách, và dữ liệu bí mật.
- Bảo mật cao: Mã hóa với AWS KMS để bảo vệ thông tin nhạy cảm (ví dụ: mật khẩu, API keys).
- Tích hợp với AWS Services: Dễ dàng truy xuất thông qua Lambda, EC2, ECS, CloudFormation.
- Hỗ trợ versioning & auditing: Theo dõi lịch sử thay đổi và kiểm soát truy cập với IAM.

AWS Parameter Store giúp quản lý cấu hình và thông tin bí mật một cách bảo mật, linh hoạt và dễ tích hợp trong hệ sinh thái AWS.

-không hỗ trợ xoay vòng tự động như AWS Secrets Manager.

-AWS Systems Manager Parameter Store là dịch vụ tiết kiệm chi phí nhất để lưu trữ thông tin nhạy cảm dưới dạng secure string parameters.

***)Amazon Kinesis Data Firehose**

-Amazon Kinesis Data Firehose là một dịch vụ truyền dữ liệu theo thời gian thực giúp thu thập, biến đổi và tải dữ liệu trực tiếp vào các dịch vụ AWS như S3, Redshift, Elasticsearch, Splunk mà không cần quản lý máy chủ.

Tính năng chính:

- Dữ liệu streaming liên tục: Tự động thu thập và gửi dữ liệu theo thời gian thực.
- Biến đổi dữ liệu: Hỗ trợ chuyển đổi, nén, mã hóa và định dạng dữ liệu trước khi lưu trữ.
- Tích hợp với AWS: Kết nối dễ dàng với S3, Redshift, OpenSearch, Splunk...
- Không cần quản lý hạ tầng: Hoàn toàn serverless, AWS tự động scale theo nhu cầu.

Tóm lại : Kinesis Data Firehose là lựa chọn lý tưởng để truyền dữ liệu lớn theo thời gian thực đến các dịch vụ lưu trữ và phân tích, mà không cần quản lý phức tạp. 🚀

-Replay messages: Kinesis lưu trữ dữ liệu trong 24h-365 ngày (tùy cấu hình), cho phép phát lại message.

-Persist logs: Có thể tích hợp với Amazon S3/Firehose để lưu trữ lâu dài.

***)Amazon Elasticsearch**

-Amazon OpenSearch Service (trước đây là Amazon Elasticsearch Service) là dịch vụ tìm kiếm và phân tích dữ liệu do AWS cung cấp, giúp bạn lưu trữ, tìm kiếm và phân tích dữ liệu log, monitoring, và security analytics một cách mạnh mẽ và theo thời gian thực.

-Tính năng chính:

- ✓ Tìm kiếm dữ liệu nhanh chóng trên lượng dữ liệu lớn.
- ✓ Hỗ trợ phân tích log và giám sát hệ thống (thường dùng với Kibana hoặc OpenSearch Dashboards).
- ✓ Tích hợp với AWS services như CloudWatch, Kinesis, S3, Lambda.
- ✓ Tự động mở rộng & bảo mật cao, hỗ trợ IAM, VPC, và encryption.

-Khi nào nên dùng OpenSearch Service?

- ♦ Khi cần tìm kiếm dữ liệu nhanh trên hệ thống lớn (logs, analytics, full-text search).
- ♦ Khi muốn phân tích và trực quan hóa log từ CloudTrail, CloudWatch Logs, hoặc ELB.
- ♦ Khi cần giám sát hệ thống và phát hiện sự cố theo thời gian thực.

***)IAM Organizations**

-IAM Organizations là một dịch vụ của AWS giúp quản lý và kiểm soát nhiều tài khoản AWS trong một tổ chức. Nó cho phép:

- Tạo và quản lý nhiều tài khoản AWS trong một tổ chức.
- Áp dụng chính sách kiểm soát tập trung bằng Service Control Policies (SCPs) để giới hạn quyền truy cập trên tất cả hoặc một nhóm tài khoản.
- Thiết lập thanh toán tập trung để quản lý chi phí dễ dàng hơn.
- Tự động áp dụng cài đặt bảo mật và tuân thủ trên tất cả tài khoản con.

-IAM Organizations giúp quản lý tài nguyên và bảo mật hiệu quả hơn trong môi trường doanh nghiệp.

***)Amazon Simple Queue Service (Amazon SQS)**

-Amazon Simple Queue Service (Amazon SQS) là một dịch vụ hàng đợi tin nhắn có khả năng mở rộng cao, giúp tách biệt các thành phần của hệ thống phân tán.

-Đặc điểm chính:

- Gửi, nhận và lưu trữ tin nhắn giữa các thành phần của ứng dụng mà không cần chúng phải hoạt động đồng thời.
- Hỗ trợ hai loại hàng đợi:
 - Standard Queue: Đảm bảo khả năng mở rộng cao, có thể xử lý số lượng lớn tin nhắn nhưng không đảm bảo thứ tự tuyệt đối.
 - FIFO Queue: Đảm bảo tin nhắn được xử lý đúng thứ tự và không trùng lặp.
- Bảo mật: Hỗ trợ mã hóa dữ liệu và kiểm soát truy cập với IAM.
- Tích hợp dễ dàng: Hoạt động với AWS Lambda, Amazon SNS, Amazon ECS và các dịch vụ AWS khác.

SQS giúp cải thiện hiệu suất, tăng khả năng chịu lỗi và giảm độ phức tạp trong các hệ thống phân tán.

-Amazon SQS là một dịch vụ hàng đợi tin nhắn được quản lý đầy đủ, cho phép bạn tách rời và mở rộng quy mô các vi dịch vụ, hệ thống phân tán và ứng dụng không máy chủ. SQS có thể gửi tin nhắn đến các thành phần tiêu thụ (consumers) bằng cách đợi chúng truy vấn hàng đợi để lấy tin nhắn. Tuy nhiên, SQS không thể trực tiếp gửi thông báo đến địa chỉ

email của nhóm bảo mật. Bạn sẽ cần sử dụng một dịch vụ khác như SNS hoặc SES để gửi email thông báo.

***)AWS Transit Gateway**

-AWS Transit Gateway là một dịch vụ của Amazon Web Services (AWS) giúp kết nối nhiều VPC (Virtual Private Cloud) và mạng tại chỗ (on-premises) thông qua một cổng trung tâm. Nó hoạt động như một bộ định tuyến trung tâm, giúp đơn giản hóa việc quản lý mạng, giảm số lượng kết nối cần thiết và cải thiện hiệu suất.

-Lợi ích chính:

- Đơn giản hóa kết nối: Thay vì thiết lập nhiều kết nối VPC Peering phức tạp, chỉ cần kết nối tất cả VPC vào Transit Gateway.
- Tích hợp on-premises: Dễ dàng kết nối với mạng tại chỗ thông qua VPN hoặc Direct Connect.
- Quản lý tập trung: Dễ kiểm soát và bảo mật lưu lượng mạng từ một điểm duy nhất.
- Hiệu suất cao: Hỗ trợ băng thông lớn và tối ưu hóa luồng lưu lượng giữa các mạng.

-Transit Gateway phù hợp cho các tổ chức có nhiều VPC hoặc cần tích hợp với hạ tầng on-premises mà vẫn muốn đơn giản hóa kiến trúc mạng.

***)AWS Firewall Manager**

-AWS Firewall Manager là dịch vụ giúp quản lý tập trung các quy tắc bảo mật trên nhiều tài khoản và tài nguyên AWS. Nó tự động áp dụng và kiểm soát các chính sách tường lửa như AWS WAF, AWS Shield Advanced, và AWS Network Firewall trên toàn bộ tổ chức AWS.

-Lợi ích chính:

- Quản lý quy tắc tường lửa trên nhiều tài khoản và VPC.
- Tự động áp dụng chính sách bảo mật khi có tài nguyên mới.
- Tích hợp với AWS WAF, Shield, và Network Firewall để bảo vệ ứng dụng.

Nó giúp đảm bảo tuân thủ bảo mật và giảm công sức quản lý bảo vệ mạng trên AWS.

***)Amazon Detective**

-Amazon Detective là một dịch vụ của AWS giúp phân tích, điều tra và trực quan hóa hoạt động đáng ngờ trong tài khoản AWS. Nó tự động thu thập dữ liệu từ nhiều nguồn như GuardDuty, CloudTrail, VPC Flow Logs, sau đó sử dụng machine learning để phát hiện các mẫu bất thường.

-Chức năng chính:

- Phân tích các sự kiện bảo mật: Điều tra các hoạt động đáng ngờ, như đăng nhập bất thường hoặc truy cập trái phép.
- Trực quan hóa dữ liệu: Hiển thị thông tin dưới dạng biểu đồ, giúp dễ dàng nhận biết các xu hướng bất thường.
- Tích hợp với GuardDuty: Hỗ trợ phân tích sâu hơn các phát hiện của GuardDuty để xác định mức độ rủi ro.
- Tự động thu thập dữ liệu: Không cần thiết lập thủ công, Amazon Detective tự động tổng hợp thông tin từ các dịch vụ AWS.

-Lợi ích:

- Giảm thời gian điều tra bằng cách cung cấp ngữ cảnh đầy đủ về các sự kiện bảo mật.
- Không cần cấu hình phức tạp, hoạt động tự động với dữ liệu có sẵn từ AWS.

- Hỗ trợ bảo mật nâng cao cho các nhóm bảo mật và quản trị viên AWS.

***)Amazon EC2 Image Builder**

-Amazon EC2 Image Builder là một dịch vụ giúp tự động tạo, kiểm tra và triển khai các Amazon Machine Images (AMI) và container images một cách dễ dàng.

-Chức năng chính:

- Tạo AMI và container images tự động theo lịch trình.
- Kiểm tra bảo mật và tuân thủ trước khi triển khai.
- Cập nhật hình ảnh định kỳ để luôn có bản mới nhất.

-Lợi ích:

- Tiết kiệm thời gian so với tạo AMI thủ công.
- Tăng cường bảo mật với kiểm tra tích hợp.
- Tự động hóa quy trình giúp quản lý image hiệu quả hơn.

***)Direct Connect**

-AWS Direct Connect là một dịch vụ cho phép bạn thiết lập kết nối mạng chuyên dụng từ trung tâm dữ liệu của bạn đến AWS. Thay vì sử dụng Internet công cộng, Direct Connect cung cấp một đường truyền riêng, giúp tăng tốc độ, giảm độ trễ và đảm bảo kết nối ổn định hơn khi truy cập các dịch vụ AWS. Nó đặc biệt hữu ích cho các doanh nghiệp có khối lượng dữ liệu lớn cần truyền tải thường xuyên giữa hệ thống on-premise và AWS.

***)AWS Step Functions**

-AWS Step Functions là dịch vụ giúp xây dựng và quản lý quy trình làm việc (workflow) dựa trên trạng thái. Nó cho phép tự động hóa các tác vụ bằng cách kết nối nhiều dịch vụ AWS theo trình tự nhất định.

-Đặc điểm chính:

- Orchestration: Điều phối Lambda, ECS, S3, DynamoDB, v.v.
- State Machine: Hoạt động theo mô hình máy trạng thái với các bước tuần tự.
- Kiểm soát luồng: Hỗ trợ quyết định, lặp, chờ, gọi API...
- Không máy chủ: Không cần quản lý hạ tầng, tự động mở rộng.

-Ứng dụng phổ biến:

- Xử lý dữ liệu, kiểm tra tự động.
- Quản lý luồng công việc DevOps.
- Tích hợp nhiều dịch vụ AWS theo quy trình.

-Tóm gọn: AWS Step Functions giúp tự động hóa & điều phối các dịch vụ AWS theo quy trình linh hoạt, đáng tin cậy. 🚀

-AWS Step Functions không tự kiểm tra tài nguyên nhưng có thể điều phối Lambda hoặc gọi API AWS để thực hiện kiểm tra.

-State Machine (máy trạng thái) là một quy trình làm việc được mô hình hóa dưới dạng một tập hợp các trạng thái (states). Nó xác định cách các tác vụ được thực thi, quyết định luồng điều khiển và xử lý lỗi.

***)AWS Batch**

-AWS Batch là dịch vụ quản lý xử lý theo lô (batch computing) trên AWS. Nó giúp chạy khối lượng công việc lớn một cách tự động, có thể mở rộng, mà không cần quản lý cơ sở hạ tầng.

Đặc điểm chính:

- Tự động cấp phát tài nguyên: Tối ưu hóa CPU/GPU/RAM theo nhu cầu.
- Hỗ trợ xử lý song song: Chạy nhiều tác vụ đồng thời.
- Tích hợp với AWS ECS, EC2, và Fargate: Hỗ trợ môi trường Docker.
- Dùng cho công việc lớn: Như xử lý dữ liệu, mô phỏng khoa học, AI/ML.

Lưu ý: AWS Batch không phù hợp cho xử lý theo sự kiện hoặc thời gian thực (nên dùng Lambda hoặc Step Functions).

-AWS Batch là một dịch vụ cho phép bạn chạy các khối lượng công việc tính toán theo lô trên AWS. Batch được thiết kế cho các công việc có quy mô lớn, chạy lâu dài và có thể hưởng lợi từ việc xử lý song song cũng như cung cấp tài nguyên điện toán động. Tuy nhiên, Batch không phù hợp cho các quy trình làm việc theo sự kiện và thời gian thực yêu cầu phản hồi ngay lập tức.

***)AWS API Gateway**

-AWS API Gateway là một dịch vụ quản lý API giúp tạo, bảo mật và giám sát RESTful APIs và WebSocket APIs để kết nối với các dịch vụ backend như Lambda, EC2, DynamoDB.

-Tính năng chính:

- ✓ Proxy API: Chuyển tiếp yêu cầu đến các dịch vụ AWS hoặc HTTP endpoint.
- ✓ Xác thực & bảo mật: Hỗ trợ IAM, Lambda Authorizer, Cognito, API Key.
- ✓ Tích hợp với AWS Lambda: Xử lý API serverless mà không cần máy chủ.
- ✓ Quản lý lưu lượng & caching: Hỗ trợ throttling, rate limiting, CloudFront caching.

-Ứng dụng thực tế:

- 🚀 Xây dựng RESTful API cho ứng dụng web & mobile.
- 🚀 Làm API Gateway trong kiến trúc Microservices.
- 🚀 Kết nối frontend với backend serverless (Lambda + DynamoDB).
- 💡 Tóm lại: AWS API Gateway giúp dễ dàng tạo, quản lý và bảo mật APIs với khả năng mở rộng cao! 🚀

***)AWS DynamoDB**

-Amazon DynamoDB là một cơ sở dữ liệu NoSQL được quản lý hoàn toàn, cung cấp hiệu suất cao, độ trễ thấp, và khả năng mở rộng linh hoạt.

- ♦ Đặc điểm chính
 - Không cần quản lý máy chủ (serverless).
 - Tốc độ nhanh với độ trễ dưới 10ms.
 - Tự động mở rộng theo nhu cầu.
 - Hỗ trợ sao lưu & phục hồi dữ liệu.
 - Tích hợp với AWS Lambda, IAM, Kinesis, v.v.
- ♦ Cấu trúc dữ liệu
 - Table (Bảng): Tập hợp dữ liệu giống như bảng trong SQL.
 - Item (Mục): Một bản ghi (giống như một hàng).
 - Attribute (Thuộc tính): Dữ liệu trong từng mục (giống như cột).

- Primary Key: Dùng để xác định duy nhất một mục (Partition Key hoặc Partition Key + Sort Key).
- ♦ Các chế độ sử dụng
 1. On-Demand Mode: Thanh toán theo lượng sử dụng, phù hợp với tải không ổn định.
 2. Provisioned Mode: Cấu hình trước số lượng đọc/ghi, phù hợp với tải ổn định.

-On-Demand Backup là tính năng sao lưu thủ công trong Amazon DynamoDB, giúp bạn lưu trữ trạng thái bảng tại một thời điểm nhất định mà không ảnh hưởng đến hiệu suất.

♦ Đặc điểm chính:

- ✓ Không ảnh hưởng hiệu suất: Sao lưu diễn ra trong nền, không làm chậm ứng dụng.
- ✓ Toàn bộ dữ liệu: Sao lưu toàn bộ bảng, bao gồm dữ liệu và cài đặt.
- ✓ Giữ vô thời hạn: Không tự động xóa, bạn phải xóa thủ công khi không cần.
- ✓ Khôi phục dễ dàng: Có thể tạo bảng mới từ bản sao lưu.

Sử dụng tính năng sao lưu theo yêu cầu (on-demand backup) của DynamoDB để tạo kế hoạch sao lưu.

***)Amazon Redshift**

-Amazon Redshift là một dịch vụ kho dữ liệu (Data Warehouse) trên AWS, được thiết kế để xử lý các truy vấn phân tích dữ liệu lớn một cách nhanh chóng và hiệu quả.

-Đặc điểm chính:

- Hiệu suất cao: Sử dụng kiến trúc lưu trữ cột (Columnar Storage) và tối ưu hóa truy vấn để tăng tốc phân tích dữ liệu.
- Tích hợp tốt với AWS: Hỗ trợ nhập dữ liệu từ S3, RDS, DynamoDB, Kinesis và tích hợp với AWS Glue, QuickSight.
- Tự động mở rộng: Có thể mở rộng linh hoạt với Redshift Spectrum để truy vấn dữ liệu trực tiếp từ S3 mà không cần tải vào Redshift.
- Chi phí tối ưu: Cung cấp tùy chọn RA3 nodes giúp lưu trữ tách biệt với tài nguyên tính toán, giảm chi phí.

Redshift thường được sử dụng cho phân tích dữ liệu lớn, báo cáo kinh doanh, và machine learning.

***)AWS DataSync**

-AWS DataSync là dịch vụ giúp tự động hóa và tăng tốc di chuyển dữ liệu giữa on-premises (tại chỗ) và AWS storage hoặc giữa các dịch vụ lưu trữ AWS với nhau.

♦ Đặc điểm chính:

- ✓ Di chuyển dữ liệu nhanh hơn (lên đến 10 Gbps).
- ✓ Tự động hóa quy trình sao chép, đồng bộ dữ liệu.
- ✓ Mã hóa & bảo mật trong quá trình truyền tải.
- ✓ Hỗ trợ nhiều nguồn đích, bao gồm Amazon S3, EFS, FSx và on-premises NFS/SMB.

♦ Cách sử dụng:

1. Cài đặt DataSync Agent nếu di chuyển từ on-premises.
2. Cấu hình Source (Nguồn) và Destination (Đích).
3. Thiết lập Lịch trình đồng bộ hoặc sao chép một lần.
4. Theo dõi trạng thái qua AWS Console hoặc CloudWatch.

♦ Khi nào nên dùng?

- ✓ Di chuyển dữ liệu on-premises lên AWS (ví dụ: từ NAS sang S3).
- ✓ Sao chép dữ liệu giữa các dịch vụ AWS (ví dụ: từ EFS sang FSx).
- ✓ Tự động đồng bộ dữ liệu định kỳ.

***)Amazon Elastic MapReduce (EMR)**

-Amazon EMR là dịch vụ xử lý dữ liệu lớn (Big Data) trên AWS, sử dụng framework như Apache Hadoop, Spark, Presto để phân tích và xử lý dữ liệu nhanh chóng.

-Tính năng chính:

- ✓ Xử lý dữ liệu quy mô lớn theo mô hình phân tán.
- ✓ Tích hợp với S3, DynamoDB, RDS để lưu trữ dữ liệu.
- ✓ Hỗ trợ nhiều framework: Hadoop, Spark, Hive, Presto, HBase...
- ✓ Tự động mở rộng & tối ưu chi phí (chỉ trả tiền theo tài nguyên sử dụng).

-Khi nào nên dùng Amazon EMR?

- ◆ Khi cần phân tích dữ liệu lớn (Big Data Analytics).
- ◆ Khi chạy machine learning, AI, hoặc xử lý log ở quy mô lớn.
- ◆ Khi cần xử lý ETL (Extract, Transform, Load) từ nhiều nguồn dữ liệu khác nhau.

-----Config-----

***)IAM**

-Điều kiện IAM (aws:PrincipalTag và aws:ResourceTag): Các điều kiện này cho phép bạn kiểm soát quyền truy cập dựa trên các tag, giúp việc quản lý quyền truy cập trở nên linh hoạt và có thể mở rộng.

-Access Key và Secret Key là cặp thông tin xác thực (credentials) trong AWS IAM, giúp người dùng hoặc ứng dụng xác thực và thực hiện API request đến AWS.

- ◆ Access Key ID (AKIA...) → Giống như username, dùng để nhận diện.
- ◆ Secret Access Key → Giống như mật khẩu, dùng để xác thực (không thể xem lại sau khi tạo).

***)IAM Role**

-MaxSessionDuration là một thuộc tính của IAM Role, không phải một điều kiện khóa. Nó xác định thời gian tối đa của phiên làm việc (tính bằng giây) cho IAM Role, có thể từ 3600 đến 43200 giây (1 đến 12 giờ). Thuộc tính này có thể được đặt khi tạo hoặc chỉnh sửa role, nhưng không thể sử dụng như một điều kiện trong chính sách IAM.

-IAM Role (Vai trò IAM)

- Là một định danh IAM cấp quyền cho dịch vụ AWS hoặc người dùng giả lập (assume) để thực hiện tác vụ.
- Không có thông tin đăng nhập như username/password hay access key.
- Thường dùng cho EC2, Lambda, CloudFormation, ECS, v.v.

Ví dụ: Một EC2 Instance Role có thể truy cập S3 mà không cần lưu credentials trên máy ảo.

-AssumeRole là cơ chế cho phép một entity (user, service, AWS account khác) tạm thời nhận quyền hạn của một IAM Role để thực hiện các tác vụ mà không cần có quyền trực tiếp.

-Để một IAM Role có thể bị assume, nó phải có **Trust Policy** cho phép dịch vụ/người dùng đó giả lập nó.

-IAM InfrastructureDeployment thường là một IAM Role được tạo ra để triển khai hạ tầng trong AWS. Vai trò này thường được cấp quyền để tạo, sửa đổi và quản lý tài nguyên AWS như EC2, EBS, RDS, S3, Lambda, v.v.

Mục đích sử dụng:

- ✓ Tự động hóa triển khai hạ tầng bằng AWS CloudFormation, Terraform, CDK.
- ✓ Quản lý tài nguyên AWS mà không cần dùng thông tin đăng nhập cá nhân.
- ✓ Phân quyền theo nguyên tắc least privilege để đảm bảo bảo mật.

Tóm lại: InfrastructureDeployment là IAM Role giúp triển khai hạ tầng AWS một cách bảo mật và tự động! 🚀

-Execution Role là IAM Role mà AWS Lambda sử dụng khi thực thi hàm. Role này xác định hàm Lambda có quyền truy cập vào dịch vụ AWS nào.

♦ Vai trò của Execution Role

- ✓ Cấp quyền cho Lambda đọc/ghi dữ liệu từ các dịch vụ AWS như S3, DynamoDB, SQS, CloudWatch Logs,...
- ✓ Chạy với nguyên tắc "least privilege" (chỉ cấp quyền cần thiết).
- ✓ Không ảnh hưởng đến quyền của người gọi hàm Lambda.

-IAMSystemAdministrator là một chính sách IAM được thiết kế để cấp quyền quản trị hệ thống trong AWS. Chính sách này cho phép người dùng hoặc vai trò IAM có quyền quản lý tài nguyên AWS, bao gồm tạo, sửa đổi và xóa các dịch vụ như EC2, S3, RDS, IAM, v.v.

Các quyền chính của IAMSystemAdministrator:

- Quản lý EC2: Khởi động, dừng, khởi động lại và xóa phiên bản EC2.
- Quản lý S3: Tạo, sửa, xóa bucket và đối tượng S3.
- Quản lý IAM: Tạo, sửa, xóa người dùng, nhóm và vai trò IAM.
- Quản lý RDS: Tạo và quản lý cơ sở dữ liệu.

Chính sách này không nhất thiết cấp quyền quản trị toàn bộ tài khoản AWS, vì có thể bị giới hạn bởi SCP (Service Control Policy) hoặc IAM Permission Boundaries trong AWS Organizations.

***)IAM Policy (Chính sách IAM)**

-IAM Policy:

- Là tập hợp các quy tắc xác định ai được phép làm gì trên tài nguyên AWS.
- Chính sách có thể đính kèm vào IAM Role, IAM User, IAM Group.
- Gồm 3 phần chính:
 - Action (hành động được phép, ví dụ: s3:ListBucket)
 - Resource (tài nguyên áp dụng, ví dụ: arn:aws:s3:::my-bucket)
 - Effect (Allow hoặc Deny)

Ví dụ: Một IAM Policy có thể cho phép EC2 đọc dữ liệu từ S3.

-Quy tắc đánh giá chính sách IAM:

1. Explicit Deny (Từ chối rõ ràng) → Luôn được ưu tiên.
2. Explicit Allow (Cho phép rõ ràng) → Được áp dụng nếu không có "Deny".
3. Implicit Deny (Từ chối ngầm định) → Nếu không có "Allow", thì mặc định bị từ chối.

-aws:ResourceOrgID:

- Dùng để kiểm soát quyền truy cập vào tài nguyên (resource) dựa trên ID của tổ chức AWS Organizations mà tài nguyên đó thuộc về.
- Ví dụ: Chỉ cho phép truy cập vào Amazon S3 bucket nếu bucket đó thuộc tổ chức của công ty.

-aws:PrincipalOrgID:

- Dùng để kiểm soát quyền truy cập dựa trên ID của tổ chức AWS Organizations mà người dùng hoặc dịch vụ (principal) thuộc về.
- Ví dụ: Chỉ cho phép người dùng hoặc dịch vụ từ tổ chức của công ty truy cập vào tài nguyên AWS.

***)IAM Managed Policy**

-AWS Managed Policy – Chính sách do AWS tạo sẵn, được cập nhật và bảo trì bởi AWS

-AmazonEC2FullAccess : cấp toàn quyền quản lý Amazon EC2, bao gồm:

- ✓ Tạo, xóa, khởi động, dừng EC2 instances
- ✓ Quản lý EBS volumes, AMIs, Security Groups, Elastic Load Balancer
- ✓ Quyền truy cập vào Auto Scaling

-AmazonDynamoDBFullAccess : cấp toàn quyền quản lý Amazon DynamoDB, bao gồm:

- ✓ Tạo, xóa, chỉnh sửa bảng (tables)
- ✓ Thực hiện CRUD (Create, Read, Update, Delete) dữ liệu
- ✓ Quản lý chỉ mục (indexes), backup, replication

-AmazonVPCFullAccess : Cấp toàn quyền quản lý Amazon VPC, bao gồm:

- ✓ Tạo, sửa, xóa VPCs, Subnets, Route Tables
- ✓ Cấu hình Internet Gateway, NAT Gateway, VPN
- ✓ Quản lý Security Groups & Network ACLs

***)IAM Group**

-IAM Groups là một nhóm người dùng IAM trong AWS, giúp quản lý quyền tập trung thay vì gán từng quyền riêng lẻ cho từng người dùng.

Cách hoạt động:

- Gom nhiều IAM Users vào một nhóm có cùng vai trò hoặc quyền hạn.
- Gán quyền (IAM Policies) cho nhóm, và tất cả thành viên trong nhóm sẽ có các quyền đó.
- Dễ dàng quản lý và cập nhật quyền, chỉ cần chỉnh sửa nhóm thay vì từng người dùng.

Lợi ích:

- Quản lý quyền hiệu quả hơn, giảm công việc thủ công.
- Tăng cường bảo mật, tránh cấp quyền quá mức cho từng cá nhân.
- Dễ dàng thêm/xóa người dùng, mà không cần chỉnh sửa quyền từng người.

***)IAM Config Rule**

-IAM Config restricted-ssh trong IAM giúp hạn chế quyền truy cập SSH vào các máy ảo (VM instances) dựa trên các điều kiện bảo mật cụ thể.

Cách hoạt động:

- Chỉ cho phép SSH từ những tài khoản hoặc nhóm được cấp quyền cụ thể.

- Kiểm soát dựa trên IAM policies, thay vì chỉ dựa vào SSH key truyền thống.
- Có thể áp dụng điều kiện như IP nguồn, thời gian, hoặc yêu cầu sử dụng OS Login.

Quy tắc này được kích hoạt khi có thay đổi trong cấu hình nhóm bảo mật không tuân thủ quy định. Nó kiểm tra xem các nhóm bảo mật đang được sử dụng có chứa quy tắc inbound cho phép lưu lượng SSH không hạn chế hay không. Nếu phát hiện vi phạm, AWS Config có thể sử dụng tính năng khắc phục để gửi thông báo đến một **chủ đề Amazon Simple**

Notification Service

***)IAM Access Advisor**

-Là công cụ trong AWS giúp kiểm tra quyền sử dụng của IAM User, Group, Role hoặc Service Role. IAM Access Advisor không cung cấp thông tin chi tiết về người dùng liên kết cụ thể.

-Chỉ hiển thị lần cuối vai trò được truy cập, nhưng không cho biết ai đã truy cập hoặc mục đích sử dụng. Nó cũng không hiển thị thời gian chính xác của lần truy cập, chỉ có ngày.

***)AWS Organizations**

-Cấu trúc của AWS Organizations giúp đơn giản hóa quá trình tích hợp và chuẩn hóa dữ liệu nhật ký, tạo nên một giải pháp hiệu quả để đáp ứng các yêu cầu đã đề ra. Việc sử dụng Amazon Athena để truy vấn dữ liệu log còn giúp nâng cao khả năng phân tích và phản ứng với các phát hiện bảo mật trên toàn bộ tổ chức.

***)AWS Regions**

-là các trung tâm dữ liệu độc lập của AWS trên toàn cầu.

-Cấu trúc phân tán: Giúp tăng cường bảo mật, hiệu suất và độ tin cậy.

-Gồm nhiều Availability Zones (AZs): Giúp dự phòng và chống lỗi.

-Dữ liệu không tự động di chuyển giữa Regions: Để tuân thủ quy định và bảo mật.

-Ví dụ:

- us-east-1 (N. Virginia) – Khu vực phổ biến với nhiều dịch vụ mới.
- ap-southeast-1 (Singapore) – Gần Đông Nam Á, giúp giảm độ trễ.

***)ABAC (Attribute-Based Access Control)**

-ABAC (Attribute-Based Access Control) trong AWS là cách kiểm soát quyền dựa trên thẻ (tags) và thuộc tính, thay vì chỉ dựa vào IAM roles hoặc policies tĩnh.

-Cách hoạt động của ABAC:

- Dùng thẻ (tags) trên AWS resources, IAM users, IAM roles.
- IAM policies sử dụng điều kiện (Condition) để cấp quyền dựa trên tags.
- Cho phép linh hoạt hơn so với phương pháp RBAC (Role-Based Access Control).

***)RBAC (Role-Based Access Control)**

-RBAC (Role-Based Access Control) là mô hình kiểm soát truy cập trong AWS, cấp quyền dựa trên vai trò (role) thay vì người dùng cụ thể.

♦ Cách hoạt động:

- ❶ Tạo IAM Role với các quyền cụ thể (ví dụ: quyền truy cập S3, RDS, EC2, v.v.).
- ❷ Gán Role cho người dùng, nhóm hoặc dịch vụ AWS (như Lambda, EC2, ECS).
- ❸ Người dùng/dịch vụ assume role để có quyền truy cập tài nguyên theo chính sách IAM.

♦ Lợi ích của RBAC:

- ✓ Bảo mật cao → Hạn chế quyền theo nguyên tắc Least Privilege (Chỉ cấp quyền cần thiết).
- ✓ Quản lý dễ dàng → Gán quyền theo vai trò thay vì từng người dùng.
- ✓ Linh hoạt → Một người có thể assume nhiều role khác nhau tùy vào tác vụ.

*)Amazon S3 Bucket

- Chính sách bucket S3 không hỗ trợ hạn chế truy cập dựa trên vị trí địa lý (geo restriction).
- S3 Object Lock chỉ ngăn các đối tượng bị ghi đè hoặc xóa bởi bất kỳ người dùng nào, bao gồm cả root user trong tài khoản AWS của bạn. Nó không ngăn các đối tượng bị thay đổi bằng các phương tiện khác, chẳng hạn như thay đổi metadata hoặc cài đặt mã hóa. Hơn nữa, S3 Object Lock yêu cầu bạn bật tính năng versioning (phiên bản hóa) trên bucket của mình, điều này sẽ làm phát sinh thêm chi phí lưu trữ cho việc lưu trữ nhiều phiên bản của một đối tượng.
- S3 Object Lock trong chế độ governance sẽ không ngăn chặn bất kỳ ai thay đổi hoặc xóa dữ liệu. S3 Object Lock trong chế độ governance hoạt động tương tự như chế độ compliance, ngoại trừ việc người dùng có quyền IAM cụ thể có thể thay đổi hoặc xóa các đối tượng bị khóa.
- S3 Bucket policy: Điều kiện "s3:x-amz-server-side-encryption":"IAM:kms" đảm bảo rằng các đối tượng được tải lên phải được mã hóa.
- S3 Bucket policy: điều kiện "s3:x-amz-server-side-encryption-aws-kms-key-id":"arn:aws:kms:*:1111122222233333:key/*" trong S3 bucket policy được sử dụng để bắt buộc tất cả các đối tượng mới tải lên phải được mã hóa bằng AWS KMS CMK cụ thể.
- s3:x-amz-server-side-encryption-aws-kms-key-id: Xác định rằng chỉ những đối tượng sử dụng mã hóa KMS CMK mới được phép lưu trữ trong S3.

arn:aws:kms:*:11111222223333:key/*: Chỉ định rằng chỉ các khóa KMS thuộc tài khoản 11111222223333 mới được phép sử dụng để mã hóa dữ liệu.

- S3 Intelligent-Tiering là một lớp lưu trữ trong Amazon S3 tự động di chuyển dữ liệu giữa các tầng lưu trữ dựa trên tần suất truy cập, giúp tối ưu hóa chi phí mà không ảnh hưởng đến hiệu suất.

Cách hoạt động:

- Dữ liệu mới tải lên được lưu trong tầng Truy cập thường xuyên.
- Nếu dữ liệu không được truy cập trong 30 ngày, nó sẽ tự động chuyển sang tầng Truy cập ít thường xuyên để giảm chi phí.
- Nếu dữ liệu được truy cập lại, nó sẽ quay về tầng Truy cập thường xuyên ngay lập tức.
- Có thể bổ sung các tầng lưu trữ sâu hơn cho dữ liệu ít dùng hơn (Archive Access, Deep Archive Access).

Lợi ích:

- Tối ưu hóa chi phí tự động mà không cần quản lý thủ công.
- Dữ liệu luôn sẵn sàng với độ trễ thấp, phù hợp với workload không thể đoán trước.
- Bạn có muốn biết khi nào nên sử dụng S3 Intelligent-Tiering không?

- S3 Lifecycle Rule là một tính năng trong Amazon S3 giúp tự động chuyển đổi lớp lưu trữ hoặc xóa dữ liệu theo lịch trình để tối ưu hóa chi phí và quản lý dữ liệu hiệu quả.

Cách hoạt động:

- Chuyển đổi lớp lưu trữ: Tự động di chuyển dữ liệu từ S3 Standard sang S3 Intelligent-Tiering, Glacier, hoặc Deep Archive sau một khoảng thời gian nhất định.
- Xóa dữ liệu tự động: Xóa các đối tượng cũ hoặc không cần thiết sau một thời gian xác định.

Lợi ích:

- Giảm chi phí lưu trữ bằng cách di chuyển dữ liệu không thường xuyên truy cập sang lớp rẻ hơn.
- Tự động hóa quản lý dữ liệu, không cần thao tác thủ công.
- Tuân thủ chính sách lưu trữ, giúp quản lý dữ liệu hiệu quả hơn.

-Trong AWS S3, nếu một policy có cả quyền deny và allow, quyền deny luôn được ưu tiên cao hơn. Trong trường hợp này, quyền deny ban đầu đã từ chối tất cả người dùng, và quyền allow sau đó không thể ghi đè lên quyền deny.

***)Amazon ECS**

-Amazon ECS (Elastic Container Service): Dịch vụ quản lý container do AWS cung cấp, giúp chạy, dừng và quản lý Docker containers trên cụm máy chủ. ECS hỗ trợ cả EC2 launch type (chạy trên EC2) và Fargate launch type (chạy serverless).

-là một dịch vụ serverless, nghĩa là bạn không có quyền truy cập trực tiếp vào các container instances (máy chủ vật lý hoặc EC2 instances) để cài đặt hoặc cấu hình bất kỳ phần mềm nào. Do đó, việc tải xuống và cấu hình CloudWatch agent trên các container instances là không khả thi.

-Amazon ECS tích hợp sẵn trình điều khiển nhật ký awslogs, cho phép bạn dễ dàng gửi nhật ký từ các container đến Amazon CloudWatch. Bằng cách chỉ định các tham số như awslogs-group (nhóm nhật ký đích) và awslogs-region (khu vực CloudWatch), bạn có thể đảm bảo rằng nhật ký từ tất cả các container sẽ được thu thập và lưu trữ trong nhóm nhật ký CloudWatch đã có sẵn. Đây là cách đơn giản, hiệu quả và được khuyến nghị khi sử dụng Amazon ECS với Fargate.

-AMI (Amazon Machine Image) là một hình ảnh máy ảo được đóng gói sẵn trên AWS, chứa hệ điều hành, phần mềm, cấu hình và các thành phần khác cần thiết để khởi chạy một phiên bản Amazon EC2 (Elastic Compute Cloud). AMI đóng vai trò như một "khuôn mẫu" để tạo ra các phiên bản EC2.

***)Amazon EC2**

-EC2InstanceProfileForImageBuilder: Là IAM Instance Profile mặc định dành cho EC2 Image Builder. Cung cấp quyền để EC2 chạy quá trình tạo và kiểm tra AMI.

-EC2InstanceProfileForImageBuilderECRContainerBuilds: Dành riêng cho EC2 Image Builder khi tạo container images trong Amazon ECR. Bổ sung quyền so với EC2InstanceProfileForImageBuilder để làm việc với Amazon Elastic Container

-AmazonSSMManagedInstanceCore : Là IAM Policy cấp quyền cơ bản cho EC2 sử dụng AWS Systems Manager (SSM). Cho phép EC2 được quản lý qua SSM, mà không cần SSH hoặc RDP.

***)Amazon EBS**

- Sử dụng AWS Management Console hoặc AWS CLI để bật mã hóa mặc định cho volume EBS trong mỗi Region AWS mà công ty hoạt động.

- Enable encryption by default for EBS volumes:
 - Tính năng này tự động mã hóa tất cả volume EBS mới được tạo trong các Region được chỉ định.
 - Không cần thao tác thủ công từ người dùng hoặc can thiệp của Lambda.
 - Giảm thiểu chi phí vận hành (không cần giám sát, cảnh báo hay xử lý sự cố).
 - Áp dụng cho cả EC2 instances và EMR clusters.

***)Perfect Forward Secrecy (PFS)**

-Perfect Forward Secrecy (PFS) là một tính năng bảo mật đảm bảo rằng ngay cả khi khóa riêng tư của chứng chỉ bị rò rỉ, các phiên mã hóa trước đó vẫn không thể bị giải mã. Điều này đáp ứng yêu cầu của công ty về việc đảm bảo an toàn cho lưu lượng TLS trước đây và hiện tại.

***)AWS Site-to-Site VPN**

-Cung cấp kết nối an toàn giữa trung tâm dữ liệu tại chỗ và AWS bằng cách sử dụng mã hóa IPsec.

-Đáp ứng yêu cầu mã hóa dữ liệu.

***)AWS Direct Connect**

-Cung cấp kết nối mạng riêng, ổn định và có độ trễ thấp giữa trung tâm dữ liệu tại chỗ và AWS.

-Đáp ứng yêu cầu về độ trễ thấp cho cơ sở dữ liệu nhạy cảm.

***)Cross-account**

-Cross-account trong AWS là cơ chế cho phép tài nguyên hoặc người dùng từ một tài khoản AWS truy cập tài nguyên trong một tài khoản AWS khác. Điều này thường được thực hiện bằng cách sử dụng IAM roles, resource-based policies, hoặc AWS Organizations để cấp quyền truy cập an toàn giữa các tài khoản mà không cần chia sẻ thông tin đăng nhập.

***)Network Access Control List (NACL)**

Network Access Control List (NACL) là một bộ lọc bảo mật tùy chọn trong AWS giúp kiểm soát lưu lượng vào và ra của subnet trong Amazon VPC.

-Chức năng chính:

- Hoạt động như một tường lửa theo quy tắc (rule-based firewall) kiểm soát lưu lượng dựa trên địa chỉ IP, giao thức và cổng.
- Hỗ trợ cả Allow (cho phép) và Deny (từ chối) lưu lượng.

-Đặc điểm:

- Áp dụng theo subnet (tất cả instances trong subnet đó sẽ tuân theo NACL).
- Đánh giá theo thứ tự quy tắc số thứ tự (rule với số thấp hơn được ưu tiên).
- Là stateless, tức là nếu có một rule cho phép inbound traffic, thì outbound traffic cũng cần rule tương ứng.

-So sánh với Security Group:

- NACL bảo vệ subnet, trong khi Security Group bảo vệ instance.
- NACL là stateless, còn Security Group là stateful (nếu inbound được phép thì outbound tự động được phép).

NACL thích hợp cho việc kiểm soát lưu lượng ở cấp độ subnet và bổ sung bảo mật cho Security Group.

-NACL hoạt động dựa trên địa chỉ IP (CIDR blocks) chứ không phải dựa trên các NACL khác. Do đó, việc tham chiếu đến NACL2 trong quy tắc của NACL3 là không hợp lệ.

***)Lambda**

-AWS Lambda:

- Là một dịch vụ serverless của AWS cho phép bạn chạy mã mà không cần quản lý máy chủ.
- Lambda thực thi mã dựa trên các sự kiện kích hoạt, chẳng hạn như thay đổi dữ liệu trong S3, cập nhật DynamoDB, hoặc yêu cầu API Gateway.

-Lambda IAM (AWS IAM Role for Lambda):

- IAM (Identity and Access Management) là dịch vụ quản lý quyền trong AWS.
- Lambda IAM role là một vai trò (role) IAM được gán cho một Lambda function để cấp quyền truy cập vào các dịch vụ AWS khác (ví dụ: đọc từ S3, ghi vào DynamoDB, gửi logs lên CloudWatch).

***)VPC**

-VPC Endpoint là một thành phần trong AWS Virtual Private Cloud (VPC) giúp kết nối riêng tư từ VPC đến các dịch vụ AWS mà không cần đi qua Internet.

Tính năng chính:

- Bảo mật cao: Dữ liệu không đi qua internet, giảm rủi ro tấn công.
- Hiệu suất tốt hơn: Giảm độ trễ so với kết nối qua internet.
- Tiết kiệm chi phí: Tránh chi phí băng thông NAT Gateway hoặc VPN.


Hai loại chính:

- Interface Endpoint: Kết nối qua AWS PrivateLink, hỗ trợ hầu hết các dịch vụ AWS.
- Gateway Endpoint: Dành cho S3 và DynamoDB, định tuyến thông qua VPC Route Table.

VPC Endpoint giúp kết nối an toàn và nhanh chóng từ VPC đến các dịch vụ AWS, không cần Internet hoặc địa chỉ IP công khai.

-VPC Peering, một tính năng của AWS Virtual Private Cloud (VPC) cho phép kết nối trực tiếp hai VPC với nhau để trao đổi dữ liệu một cách riêng tư.

-Virtual Private Gateway (VGW) là một thành phần trong AWS dùng để kết nối Amazon VPC với mạng on-premises thông qua VPN hoặc AWS Direct Connect.

 Cách hoạt động:

1. VGW được gán vào VPC để làm điểm cuối VPN.
2. Kết nối với Customer Gateway (CGW) ở phía on-premises.
3. Dữ liệu truyền qua kết nối VPN hoặc Direct Connect để đảm bảo an toàn.

***)Audit Manager**

-AWS Audit Manager là dịch vụ giúp tự động hóa quy trình đánh giá tuân thủ bằng cách thu thập và phân tích bằng chứng từ các dịch vụ AWS.

Chức năng chính:

- Tạo đánh giá tuân thủ theo tiêu chuẩn như ISO 27001, PCI DSS, HIPAA.
- Tự động thu thập dữ liệu từ AWS để giảm công việc kiểm toán thủ công.

- Tạo báo cáo kiểm toán giúp chứng minh tuân thủ với các quy định.

Lợi ích:

- Giảm thời gian kiểm toán, giúp doanh nghiệp dễ dàng đáp ứng tiêu chuẩn bảo mật.
- Tự động thu thập bằng chứng, tránh sai sót thủ công.
- Dễ dàng tích hợp với các dịch vụ AWS để theo dõi liên tục.

-AWS Audit Manager giúp bạn liên tục kiểm tra việc sử dụng AWS để đơn giản hóa cách quản lý rủi ro và tuân thủ các quy định, tiêu chuẩn ngành. Audit Manager giúp đánh giá xem các chính sách, quy trình và hoạt động của bạn (còn gọi là các control) có hoạt động như mong đợi hay không.

Ngoài ra, Audit Manager không chỉ thu thập bằng chứng từ môi trường AWS của bạn, mà còn cho phép tải lên và quản lý tập trung bằng chứng từ môi trường on-premises hoặc đa đám mây.

-bằng cách tạo một đánh giá trong AWS Audit Manager, kỹ sư bảo mật có thể:

- Sử dụng framework có sẵn hoặc tùy chỉnh chứa các control liên quan đến chính sách công ty.
- Tải lên bằng chứng thủ công từ môi trường on-premises và thêm vào đánh giá.
- Thu thập tự động bằng chứng từ tài nguyên AWS.
- Tạo báo cáo đánh giá bao gồm tất cả các bằng chứng từ cả hai nguồn.

***)AWS Cost**

-AWS Cost Explorer chỉ cung cấp thông tin về chi phí, không cung cấp chi tiết về các hoạt động triển khai hoặc cấu hình lại tài nguyên.

-AWS Cost Anomaly Detection tập trung vào việc phát hiện bất thường trong chi phí, không cung cấp thông tin chi tiết về các hoạt động cụ thể của người dùng.

***)Security Groups (SG)**

-Security Groups (SG) trong AWS là tường lửa ảo kiểm soát lưu lượng vào (inbound) và ra (outbound) của các tài nguyên như EC2, RDS, Lambda (vPC-enabled).

-Đặc điểm chính:

- Chỉ cho phép (Allow Rules), không có Deny Rules.
- Stateful: Nếu một request đi ra, response tự động được cho phép quay lại.
- Áp dụng ở cấp độ instance (không phải subnet).
- Mỗi SG có thể gán cho nhiều instance, mỗi instance có thể có nhiều SG.

-Cách hoạt động:

- Inbound Rules: Xác định ai có thể truy cập vào instance (VD: chỉ cho phép SSH từ IP cụ thể).
- Outbound Rules: Xác định instance có thể kết nối ra ngoài hay không (VD: cho phép HTTP ra Internet).

***)Inline policy**

-Inline policy là một chính sách được gắn trực tiếp vào một người dùng, nhóm hoặc vai trò cụ thể. Nó phù hợp khi bạn muốn áp dụng một chính sách riêng biệt cho một người dùng cá nhân mà không ảnh hưởng đến các người dùng khác.

***)SAML (Security Assertion Markup Language)**

-SAML (Security Assertion Markup Language) trong AWS là một tiêu chuẩn xác thực liên kết (federated authentication) cho phép người dùng đăng nhập vào AWS bằng danh tính từ nhà cung cấp danh tính (IdP) bên ngoài, như Active Directory, Okta, hoặc Google Workspace.

-Cách hoạt động:

1. Người dùng đăng nhập vào IdP (ví dụ: Active Directory).
2. IdP xác thực và gửi SAML assertion chứa thông tin danh tính & quyền.
3. AWS nhận SAML assertion, cấp temporary credentials thông qua AWS STS (Security Token Service).
4. Người dùng có thể truy cập AWS với vai trò được gán.

-Lợi ích:

- SSO (Single Sign-On) → Người dùng có thể đăng nhập AWS mà không cần tạo tài khoản IAM.
- Bảo mật & quản lý tập trung → Danh tính và quyền được quản lý từ IdP. Hỗ trợ truy cập tạm thời → Không cần lưu trữ key dài hạn.

=>SAML giúp tích hợp dễ dàng AWS với hệ thống quản lý danh tính doanh nghiệp, nâng cao bảo mật & tiện lợi.

***)Giải thích ngắn về các bước cấu hình SAML với Amazon Cognito và API Gateway**

① Cấu hình SAML Identity Provider trong Amazon Cognito để ánh xạ thuộc tính sang Amazon Cognito User Pool

- Thêm SAML Identity Provider (IdP) vào Cognito User Pool.
- Ánh xạ các thuộc tính SAML (attributes) từ IdP (ví dụ: email, username) sang các thuộc tính của Cognito User Pool.

② Cấu hình SAML Identity Provider để thêm Amazon Cognito User Pool làm bên phụ thuộc (Relying Party)

- Trong IdP, khai báo Cognito User Pool như một Relying Party để xác thực danh tính.
- Cung cấp Assertion Consumer Service URL (ACS URL) của Cognito để IdP gửi SAML assertions khi người dùng đăng nhập.

③ Cập nhật API Gateway để sử dụng bộ ủy quyền COGNITO_USER_POOLS

- Cấu hình API Gateway để sử dụng Cognito User Pool Authorizer.
- Khi client gọi API, API Gateway sẽ xác thực JWT Token do Cognito phát hành.
- Nếu hợp lệ, API Gateway cho phép truy cập tài nguyên backend.



Tóm lại:

Bước này giúp xác thực người dùng với SAML IdP, đồng bộ thông tin vào Cognito, và bảo vệ API bằng Cognito User Pool Authorizer! 🔒🚀

***)Cron Schedule Expression**

-Biểu thức cron trong AWS giúp tạo lịch trình tự động cho các dịch vụ như Amazon EventBridge (CloudWatch Events), AWS Lambda, Step Functions,...

♦ Cú pháp Cron AWS:

cron(Minutes Hours Day-of-month Month Day-of-week Year)

***)Runbook**

-Runbook trong AWS Systems Manager Automation là một tập hợp các bước hướng dẫn được xác định trước để tự động hóa các tác vụ quản lý và vận hành trên AWS.

-Chức năng của Runbook trong SSM Automation:

- Tự động hóa các tác vụ như vá lỗi, khắc phục sự cố, triển khai ứng dụng, sao lưu dữ liệu.
- Hỗ trợ AWS Lambda, AWS API, AWS CLI và tích hợp với các dịch vụ khác.
- Có thể được kích hoạt thủ công hoặc tự động thông qua EventBridge, AWS Lambda, hoặc Security Hub.

Ví dụ: Một runbook có thể tự động cô lập một EC2 bị xâm nhập bằng cách dừng phiên SSH, gắn cờ bảo mật, và gửi cảnh báo qua SNS.

-----**NOTE**-----

***)AWS đánh giá yêu cầu truy cập**

+)Khi AWS đánh giá yêu cầu truy cập, nó kết hợp cả resource-based policy (ví dụ: bucket policy của S3) và identity-based policy (ví dụ: IAM user policy, IAM role policy) để xác định có cho phép hay từ chối hành động hay không.

Theo tài liệu AWS:

"Nếu có một explicit allow (cho phép rõ ràng) trong resource-based policy hoặc identity-based policy, thì AWS sẽ cấp quyền truy cập vào tài nguyên."

Do đó:

- Nếu bucket policy có điều kiện kiểm tra giá trị của tag, điều kiện này sẽ không có tác dụng nếu identity-based policy của principal có explicit allow cho hành động PutObject mà không có điều kiện nào.
- Explicit allow trong identity-based policy sẽ ghi đè điều kiện trong bucket policy và cấp quyền cho principal tải đối tượng lên.

***)Phân biệt cơ bản giữa IAM Role và IAM Policy**

-Khác nhau cơ bản về mục đích:

- IAM Role = "Ai thực thi hành động?"
- IAM Policy = "Hành động nào được phép?"
 - ➔ IAM Role sử dụng IAM Policy để kiểm soát quyền truy cập!

***)Quy tắc tạo Role trước, rồi mới gán Policy áp dụng cho hầu hết các dịch vụ AWS cần assume IAM Role để thực thi tác vụ.**

***)Kiểm tra nguồn/đích (Source/Destination Check)**

- "Bạn phải vô hiệu hóa kiểm tra nguồn/đích nếu instance chạy các dịch vụ như dịch địa chỉ mạng (NAT), định tuyến hoặc tường lửa."

- Vô hiệu hóa kiểm tra Nguồn/Đích cho phép thiết bị bảo mật ảo định tuyến lưu lượng không phải gửi đến hoặc xuất phát từ chính nó.

- Mặc định, kiểm tra này được bật trên tất cả các EC2 instances, và nó ngăn chặn việc chuyển tiếp lưu lượng không khớp với địa chỉ IP hoặc MAC của instance.

-Đối với một thiết bị bảo mật ảo hoạt động như bộ định tuyến hoặc tường lửa, nếu không vô hiệu hóa kiểm tra này, nó sẽ loại bỏ lưu lượng mà đáng lẽ phải định tuyến.

-Thiết bị bảo mật ảo (virtual security appliance) thường được triển khai dưới dạng một instance EC2 trong môi trường AWS. Đây là cách phổ biến để triển khai các giải pháp bảo mật như tường lửa, hệ thống phát hiện xâm nhập (IDS), hoặc hệ thống ngăn chặn xâm nhập (IPS) trong AWS.

-EC2 là nền tảng tính toán chính của AWS, nên các thiết bị ảo hóa (bao gồm cả thiết bị bảo mật) thường được triển khai trên EC2 để tận dụng khả năng mở rộng, linh hoạt và tích hợp sâu với các dịch vụ AWS khác như VPC, security groups, và network ACLs.

***)Bastion host**

-Một bastion host là một máy chủ được thiết kế đặc biệt để cung cấp quyền truy cập an toàn vào các tài nguyên trong mạng riêng tư. Từ góc độ bảo mật, các đặc điểm chính của một bastion host bao gồm:

1. Vị trí: Bastion host thường được đặt trong một subnet công cộng (public subnet) để có thể truy cập từ bên ngoài, nhưng nó được bảo vệ bởi các biện pháp bảo mật nghiêm ngặt.
2. Mục đích: Nó hoạt động như một cổng kết nối (gateway) vào mạng riêng tư, cho phép người dùng truy cập an toàn vào các máy chủ bên trong thông qua các giao thức như SSH hoặc RDP.
3. Bảo mật: Bastion host phải được bảo mật và giám sát chặt chẽ vì nó là điểm tiếp xúc trực tiếp với internet và có nguy cơ bị tấn công cao.

***)Hao mòn mã hóa (Cryptographic Wear-out) trong AWS**

-Cryptographic Wear-out là tình trạng khóa mã hóa bị suy yếu do sử dụng quá nhiều lần, làm tăng nguy cơ bị tấn công.

-Nguyên nhân:

- Dùng cùng một khóa mã hóa cho nhiều dữ liệu trong thời gian dài.
- Tấn công mật mã học có thể khai thác mô hình lặp lại trong dữ liệu được mã hóa.

***)Phạm vi ảnh hưởng (Blast Radius) trong AWS**

-Blast Radius là mức độ thiệt hại khi có sự cố bảo mật hoặc lỗi hệ thống xảy ra.

-Ví dụ:

- Một tài khoản AWS bị tấn công → Nếu không phân tách quyền hạn, toàn bộ hệ thống có thể bị ảnh hưởng.
- Một VPC bị lỗi → Nếu các dịch vụ không được cô lập, toàn bộ ứng dụng có thể bị gián đoạn.

-Cách giảm thiểu trong AWS:

- IAM Least Privilege – Hạn chế quyền truy cập ở mức tối thiểu cần thiết.
- Multi-Account Strategy – Phân tách hệ thống thành nhiều tài khoản AWS.
- Network Segmentation – Dùng VPC, Security Groups, NACLs để cô lập tài nguyên.

***)Cross-account**

Để cho phép truy cập liên tài khoản vào tài nguyên bằng IAM Roles, cần thực hiện các bước sau:

1. Tạo một IAM Role trong tài khoản AWS chứa tài nguyên (Trusting Account) và chỉ định tài khoản AWS chứa IAM user (Trusted Account) là thực thể đáng tin cậy trong trust policy của role đó. Điều này cho phép người dùng từ tài khoản được tin cậy assume role và truy cập tài nguyên trong tài khoản tin cậy.
2. Đảm bảo rằng IAM user có quyền assume role trong tài khoản của họ. Điều này có thể được thực hiện bằng cách tạo một identity policy cho phép hành động sts:AssumeRole và gán policy này cho IAM user hoặc nhóm của họ.
3. Đảm bảo rằng không có Service Control Policies (SCPs) trong tổ chức sở hữu tài nguyên có thể từ chối hoặc hạn chế quyền truy cập vào hành động sts:AssumeRole hoặc role đó. SCPs được áp dụng cho tất cả các tài khoản trong tổ chức và có thể ghi đè bất kỳ quyền nào được cấp bởi IAM policies.

***)Để cho phép truy cập liên tài khoản vào một KMS key**, key policy của KMS key phải cấp quyền cho tài khoản hoặc thực thể bên ngoài, và IAM policy của tài khoản hoặc thực thể bên ngoài phải ủy quyền cho key policy.

Trong trường hợp này, hàm Lambda mới trong tài khoản phát triển cần sử dụng KMS key trong tài khoản bảo mật, vì vậy:

- Key policy của KMS key phải cho phép IAM role của hàm Lambda mới trong tài khoản phát triển truy cập
- IAM role của hàm Lambda mới trong tài khoản phát triển phải có IAM policy cho phép truy cập KMS key trong tài khoản bảo mật

***)Auto Scaling**

-Auto Scaling sử dụng AMI để tạo ra các phiên bản EC2 mới khi cần mở rộng hệ thống.

-AMI là một bản sao chứa hệ điều hành, ứng dụng, cấu hình... giúp đảm bảo rằng mỗi instance trong nhóm Auto Scaling đều khởi chạy từ cùng một cấu hình chuẩn.

-Cách hoạt động:

1. Bạn tạo một AMI chứa hệ thống và ứng dụng cần thiết.
2. Khi Auto Scaling cần mở rộng (scale-out), nó sẽ sử dụng AMI này để tạo phiên bản EC2 mới.
3. Khi cần thu nhỏ (scale-in), nó sẽ tự động tắt bớt các phiên bản dư thừa.

Tóm lại: AMI giúp Auto Scaling triển khai các instance một cách đồng nhất và tự động.

***)Termination Protection**

-Termination Protection là một tính năng bảo vệ Amazon EC2 instances và Auto Scaling Groups (ASG) khỏi bị vô tình xóa.



Cách hoạt động:

- Khi bật Termination Protection, bạn không thể xóa instance bằng AWS Console hoặc CLI mà không tắt bảo vệ trước.
- Áp dụng cho EC2 Instances và Auto Scaling Groups.

***)Phân biệt cơ bản NAT Gateway và Internet Gateway (IGW)**

Đặc điểm	NAT Gateway	Internet Gateway (IGW)
Chức năng	Cho phép các instance trong mạng riêng (private subnet) truy cập Internet hoặc các dịch vụ AWS nhưng không cho phép inbound traffic từ Internet .	Cho phép các instance trong mạng công khai (public subnet) có thể gửi và nhận lưu lượng trực tiếp từ Internet.
Hướng lưu lượng	Outbound only (chỉ gửi đi) từ private subnet ra Internet.	Bidirectional (2 chiều), hỗ trợ cả inbound và outbound.
Gắn với subnet	Chỉ dành cho private subnet .	Chỉ dành cho public subnet .
Cách sử dụng	Các instance trong private subnet cần NAT Gateway để truy cập Internet (ví dụ: cập nhật hệ điều hành, tải gói phần mềm).	Các instance trong public subnet cần Internet Gateway để có địa chỉ IP công khai và truy cập Internet trực tiếp.
Yêu cầu Elastic IP	Có (NAT Gateway cần Elastic IP).	Không (chỉ cần gán vào VPC).
Tính khả dụng	Single-AZ , cần tạo nhiều NAT Gateway nếu muốn HA (High Availability).	High Availability mặc định trên toàn VPC.

***)Các yếu tố có thể ảnh hưởng đến kết nối outbound từ một máy chủ trong private subnet ra Internet.**

- Các quy tắc outbound của Network ACL trên private subnet và cả quy tắc inbound & outbound trên public subnet phải cho phép lưu lượng đi qua.
- Nhóm bảo mật (Security Group) được áp dụng cho Application Load Balancer và NAT Gateway cũng phải cho phép lưu lượng từ private subnet.
- Đường 0.0.0.0/0 trong bảng định tuyến của private subnet phải trỏ đến NAT Gateway trong public subnet, không phải Internet Gateway.

***)Edge Locations**

-Edge Locations trong AWS là các trạm biên (các trung tâm dữ liệu phân tán toàn cầu) được sử dụng chủ yếu bởi Amazon CloudFront và AWS Global Accelerator để cung cấp nội dung và dịch vụ nhanh hơn cho người dùng.

-Chức năng chính:

- Lưu trữ và phân phối nội dung tĩnh/dữ liệu cache gần người dùng → Giảm độ trễ.
- Xử lý request của CloudFront → Tăng tốc website và ứng dụng.
- Hỗ trợ Lambda@Edge để thực thi logic serverless gần người dùng hơn.

-Tóm lại: Edge Locations giúp cải thiện hiệu suất và giảm độ trễ khi người dùng truy cập nội dung từ AWS. 🚀

-Các **Edge Locations phổ biến** trong AWS thường được sử dụng để cải thiện hiệu suất và giảm độ trễ khi phân phối nội dung hoặc xử lý request gần người dùng hơn. Dưới đây là một số **dịch vụ AWS sử dụng Edge Locations** phổ biến:

1. Amazon CloudFront
 2. AWS Global Accelerator
 3. AWS Shield & AWS WAF
 4. Lambda@Edge: Cho phép chạy AWS Lambda gần người dùng để xử lý request/responses nhanh hơn. Ứng dụng trong redirect URL, xác thực, nén dữ liệu, v.v.
- Tóm lại: Các dịch vụ trên sử dụng Edge Locations để tối ưu hiệu suất, tăng cường bảo mật và cải thiện trải nghiệm người dùng toàn cầu.

***)RPO (Recovery Point Objective)**

-RPO (Recovery Point Objective) là mức dữ liệu tối đa có thể mất trong trường hợp xảy ra sự cố, tính từ thời điểm sao lưu gần nhất.

Hiểu đơn giản:

RPO = Khoảng thời gian tối đa dữ liệu có thể không được cập nhật trước khi hệ thống khôi phục.

Ví dụ: Nếu RPO là 1 giờ, có thể mất dữ liệu tối đa của 1 giờ trước sự cố.

***)Hạ tầng bất biến (Immutable Infrastructure)**

-Hạ tầng bất biến (Immutable Infrastructure) trong AWS là mô hình triển khai mà các tài nguyên cơ sở hạ tầng (như server, container, máy ảo) không thay đổi sau khi được tạo. Nếu cần cập nhật, hệ thống sẽ tạo một bản mới thay vì chỉnh sửa tài nguyên hiện có.

-Đặc điểm chính:

- Không thay đổi sau khi triển khai → Nếu có cập nhật, tạo mới hoàn toàn và thay thế.
- Tự động hóa bằng IaC (Infrastructure as Code) như Terraform, CloudFormation, hay AWS CDK.
- Dễ dàng rollback: Nếu có lỗi, chỉ cần quay lại phiên bản trước.
- Giảm lỗi do cấu hình tay → Mọi thứ đều được mã hóa và kiểm soát chặt chẽ.

-Ví dụ trong AWS:

- Amazon Machine Image (AMI): Tạo AMI mới thay vì cập nhật server hiện có.
- AWS Auto Scaling với Launch Templates: Tạo instance mới từ template thay vì cập nhật tại chỗ.
- Serverless với AWS Lambda: Triển khai phiên bản mới của function thay vì chỉnh sửa trực tiếp.

-Lợi ích:

- Ổn định & dễ kiểm soát vì mọi thay đổi đều có lịch sử rõ ràng.
- Bảo mật tốt hơn do loại bỏ lỗi cấu hình hoặc phần mềm cũ.
- Tự động hóa mạnh mẽ giúp giảm thời gian triển khai.

=>Ứng dụng nhiều trong DevOps và CI/CD để đảm bảo hạ tầng linh hoạt, đáng tin cậy.

***)Break Glass User**

-Break Glass User trong AWS là một tài khoản có quyền admin cao nhất, thường được sử dụng trong các tình huống khẩn cấp khi tài khoản chính hoặc hệ thống IAM gặp sự cố.

-Mục đích:

- Cung cấp quyền truy cập khẩn cấp khi các tài khoản IAM thông thường bị khóa hoặc lỗi.
- Giúp khắc phục sự cố bảo mật hoặc cấu hình sai nghiêm trọng.

-Đặc điểm:

- Là tài khoản root hoặc IAM user đặc biệt với quyền quản trị tối đa.
- Không sử dụng thường xuyên và chỉ kích hoạt khi cần thiết.
- Bảo vệ nghiêm ngặt, thường được lưu trữ an toàn (ví dụ: vault, MFA).

-Best Practices:

- Không sử dụng hàng ngày, chỉ truy cập khi thật sự cần thiết.
- Bật MFA và lưu trữ thông tin an toàn.
- Giám sát & ghi log mọi hoạt động khi tài khoản này được sử dụng.
- Tự động hóa quy trình quản lý quyền để giảm rủi ro lạm dụng.

=>Break Glass User là phương án dự phòng quan trọng để đảm bảo khả năng khôi phục và bảo mật trong AWS.

***)Phân biệt cơ bản giữa các cơ chế kiểm soát truy cập trong AWS**

Loại Chính Sách	Áp dụng cho đối tượng nào?	Mô tả
IAM Policy	IAM Users, IAM Groups, IAM Roles	Quy định quyền của từng người dùng/role trong một tài khoản AWS cụ thể.
SCP (Service Control Policy)	AWS Accounts, Organizational Units (OU) trong AWS Organizations	Giới hạn quyền tối đa của tài khoản AWS, không cấp quyền trực tiếp.
Resource-based Policy	AWS Resources (S3 Bucket, SQS, SNS, Lambda, v.v.)	Kiểm soát quyền truy cập trực tiếp vào tài nguyên mà không cần IAM.
Permission Boundary	IAM Users, IAM Roles	Giới hạn quyền tối đa mà một IAM Policy có thể cấp cho user/role.
Session Policy	Tạm thời áp dụng khi user/role assume role	Giới hạn quyền trong một phiên session IAM STS.

***)Ứng cứu sự cố**

-Tài liệu của AWS nêu rõ rằng bạn có thể tạo một AMI mới mà không chứa thông tin xác thực có khả năng bị xâm phạm và tạo một IAM Role với các quyền phù hợp. Sau đó, bạn có thể tạo một launch template cho Auto Scaling Group để tham chiếu đến AMI mới và IAM Role. Đây là phương pháp an toàn nhất để khắc phục các vấn đề bảo mật mà không gây gián đoạn cho ứng dụng.

-Instance đang chờ chạy trong subnet us-east-1b và là instance duy nhất trong subnet này.
=>Cập nhật outbound network ACL cho subnet us-east-1b để từ chối rõ ràng tất cả các kết nối như là rule đầu tiên. Thay thế security group hiện tại bằng một security group mới chỉ cho phép kết nối từ một security group chặn đoán. Cập nhật outbound network ACL cho subnet us-east-1b để xóa rule deny all. Khởi chạy một instance EC2 mới có công cụ chặn

đoán. Gán security group mới cho instance EC2 mới. Sử dụng instance EC2 mới để điều tra instance đáng ngờ.

-Một kỹ sư bảo mật cần triển khai một giải pháp giám sát liên tục để tự động thông báo cho nhóm bảo mật của công ty về các instance bị xâm phạm thông qua một danh sách email phân phối

=>Giải pháp:

- Kích hoạt GuardDuty:
 - GuardDuty là dịch vụ phát hiện mối đe dọa thời gian thực, có thể nhận diện các instance bị xâm phạm (như phát tán malware, kết nối đến địa chỉ độc hại).
 - Tích hợp sẵn với AWS Security Hub và EventBridge.
- Tạo SNS topic + email distribution list
 - SNS hỗ trợ gửi thông báo qua email cho nhóm bảo mật khi có sự cố.
 - Đơn giản, dễ triển khai nhanh
- EventBridge rule cho GuardDuty findings
 - EventBridge lọc các phát hiện high severity từ GuardDuty và kích hoạt SNS topic.
 - Đảm bảo chỉ các sự cố nghiêm trọng được thông báo.

-Công ty phát hiện ra rằng một hoặc nhiều EC2 instances đã bị xâm nhập và đang trích xuất dữ liệu đến một S3 bucket bên ngoài tổ chức của công ty trong AWS Organizations. Một kỹ sư bảo mật phải triển khai giải pháp ngăn chặn việc rò rỉ dữ liệu này mà vẫn đảm bảo quy trình xử lý dữ liệu của EC2 tiếp tục hoạt động.

=>Áp dụng SCP (Service Control Policy) lên tài khoản AWS để chỉ cho phép các hành động S3 nếu giá trị của các điều kiện aws:ResourceOrgID và aws:PrincipalOrgID khớp với giá trị của công ty.

***)Triển khai an toàn**

-Tài liệu của AWS nêu rõ rằng bạn có thể triển khai các hàm Lambda bên trong VPC và gắn một security group vào các hàm Lambda. Sau đó, bạn có thể chỉ cấp quyền truy cập outbound đến phạm vi CIDR của VPC và cập nhật security group của instance cơ sở dữ liệu để cho phép lưu lượng từ security group của Lambda. Đây là phương pháp an toàn nhất để đáp ứng các yêu cầu.

-Các bước triển khai end-to-end encryption in transit:

1. CloudFront → ALB: HTTPS (dùng ACM certificate)
2. ALB → EC2: Có thể HTTP (trong VPC đã an toàn) hoặc HTTPS
3. Ứng dụng → DynamoDB: Luôn dùng HTTPS
4. Client → CloudFront: Redirect HTTP → HTTPS

-Giới hạn IAM KMS Customer Master Key (CMK) chỉ hoạt động với Amazon S3

Yêu cầu chính:

- Giới hạn CMK chỉ được sử dụng bởi Amazon S3
- Tuân thủ chính sách "mỗi dịch vụ dùng CMK riêng"
2. Tại sao chọn B:
 - kms:ViaService là điều kiện đặc biệt trong KMS key policy:

```
"Condition": {
  "StringEquals": {
    "kms:ViaService": "s3.amazonaws.com"
```

- ```
}
}
```
- Chỉ cho phép sử dụng CMK khi request đến từ dịch vụ S3
  - Ngăn các dịch vụ khác (như EC2, EBS...) sử dụng CMK này

-Sau khi triển khai chính sách yêu cầu mọi hành động tới EC2 yêu cầu 2FA, quản trị viên nhận được báo cáo rằng người dùng không thể thực hiện các lệnh Amazon EC2 bằng AWS CLI:

=>Hướng dẫn người dùng chạy lệnh CLI `aws sts get-session-token` và cung cấp các tham số xác thực đa yếu tố (`--serial-number` và `--token-code`). Sử dụng các giá trị này để thực hiện các lệnh API/CLI tiếp theo.

-Một kỹ sư bảo mật cần tạo cảnh báo sẽ thông báo cho công ty trước khi một KMS key bị xóa. Kỹ sư bảo mật đã cấu hình tích hợp giữa AWS CloudTrail và Amazon CloudWatch:

=>Tạo một Amazon EventBridge rule để phát hiện các API calls `DisableKey` và `ScheduleKeyDeletion` của KMS. Tạo một AWS Lambda function để gửi thông báo Amazon SNS tới công ty. Thêm Lambda function làm target của EventBridge rule.

-Một công ty có nhiều tài khoản trên AWS Cloud. Người dùng trong tài khoản Developer cần truy cập vào một số tài nguyên cụ thể trong tài khoản Production.

=>Tạo cross-account access bằng một IAM role trong tài khoản Production. Cấp các quyền phù hợp cho role này. Cho phép người dùng trong tài khoản Developer `assume role` này để truy cập tài nguyên Production.

-Yêu cầu bảo mật của công ty:

- Bảo vệ quyền riêng tư người dùng: Dữ liệu truyền tải phải được mã hóa bằng các công nghệ tăng cường bảo mật (ví dụ: Perfect Forward Secrecy - PFS).
- Không ảnh hưởng đến chức năng của HIDS: Giải pháp phải đảm bảo HIDS agent vẫn có thể giám sát lưu lượng để phát hiện xâm nhập.

=>Vấn đề cần giải quyết:

- Mâu thuẫn tiềm ẩn:
  - Nếu sử dụng mã hóa end-to-end (từ client tới server), HIDS agent sẽ không thể giải mã và phân tích lưu lượng.
  - Nếu tắt mã hóa giữa ALB và EC2 instance để HIDS hoạt động, dữ liệu sẽ bị truyền ở dạng plaintext (không mã hóa), vi phạm yêu cầu bảo mật.

→ Cần một giải pháp cân bằng: vừa mã hóa dữ liệu người dùng, vừa cho phép HIDS giám sát lưu lượng.

=>Bằng cách tạo một listener trên ALB không kích hoạt các cipher suite hỗ trợ PFS và sử dụng kết nối mã hóa với máy chủ bằng cipher suite ECDHE, bạn có thể đảm bảo rằng các tác nhân HIDS có thể ghi lại lưu lượng truy cập trên EC2 instance mà không ảnh hưởng đến quyền riêng tư của người dùng.

-Để ngăn người dùng truy cập trực tiếp vào Application Load Balancer và chỉ cho phép truy cập thông qua CloudFront, hãy thực hiện các bước sau:

- 1) Cấu hình CloudFront để thêm một HTTP header tùy chỉnh vào các yêu cầu gửi đến Application Load Balancer.
- 2) Cấu hình Application Load Balancer chỉ chuyển tiếp các yêu cầu có chứa HTTP header

tùy chỉnh.

③(Tùy chọn) Yêu cầu HTTPS để tăng cường bảo mật cho giải pháp này.

-Một công ty sử dụng AWS Organizations và có các workload production trên nhiều tài khoản AWS khác nhau. Một kỹ sư bảo mật cần thiết kế một giải pháp để giám sát chủ động các hành vi đáng ngờ trên tất cả các tài khoản chứa workload production.

=>Kích hoạt AWS Security Hub trên từng tài khoản production. Trong tài khoản logging chuyên dụng, tổng hợp tất cả findings Security Hub từ các tài khoản production. Khắc phục sự cố bằng cách sử dụng Amazon EventBridge để gọi một hàm AWS Lambda tùy chỉnh từ các findings Security Hub. Cấu hình hàm Lambda để gửi thông báo đến SNS topic.

-Kỹ sư bảo mật cần xây dựng một chính sách IAM theo nguyên tắc least privilege để thay thế các chính sách IAM quản lý bởi AWS hiện đang gắn với các role đang có quá nhiều đặc quyền.

=>Trong AWS CloudTrail, tạo một trail cho các sự kiện quản lý. Chạy script với các chính sách IAM quản lý bởi AWS hiện có. Sử dụng IAM Access Analyzer để tạo chính sách IAM mới dựa trên hoạt động truy cập trong trail. Thay thế các chính sách IAM quản lý bởi AWS hiện có bằng chính sách IAM mới được tạo cho role.

=>Operationally efficient (Hiệu quả vận hành):

- IAM Access Analyzer tự động phân tích hoạt động từ CloudTrail và tạo policy least privilege → tiết kiệm thời gian so với cách thủ công.
- Không cần phải chạy script nhiều lần và sửa lỗi từng bước như phương án D.
- Bảo mật:
  - Policy được tạo dựa trên hoạt động thực tế của script → đảm bảo đủ quyền nhưng không dư thừa.
  - Thay thế các policy full-access bằng policy tối thiểu → giảm rủi ro bảo mật.

### **\*)Quyền cơ bản để Lambda ghi nhật ký vào CloudWatch Logs**

-Để một hàm AWS Lambda ghi nhật ký vào CloudWatch, nó cần có execution role với các quyền IAM sau:

- ◆ 1. Quyền cần thiết trong IAM Policy

```
{
 "Effect": "Allow",
 "Action": [
 "logs:CreateLogGroup", // Tạo nhóm nhật ký (nếu chưa tồn tại)
 "logs:CreateLogStream", // Tạo luồng nhật ký mới
 "logs:PutLogEvents" // Ghi log vào luồng nhật ký
],
 "Resource": "arn:aws:logs:*:*:log-group:/aws/lambda/*:*"
}
```