----------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.

*)**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.

*)**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.

*)**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.

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

*)**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.

*)**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.
*)**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 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.

*)**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.

*)**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

*)**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.

*)**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.

*)**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.

*)**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.

*)**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 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.

*)**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.

----------Config----------

*)**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.

*)**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).

*)**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.

*)**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.

*)**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)**

----------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.