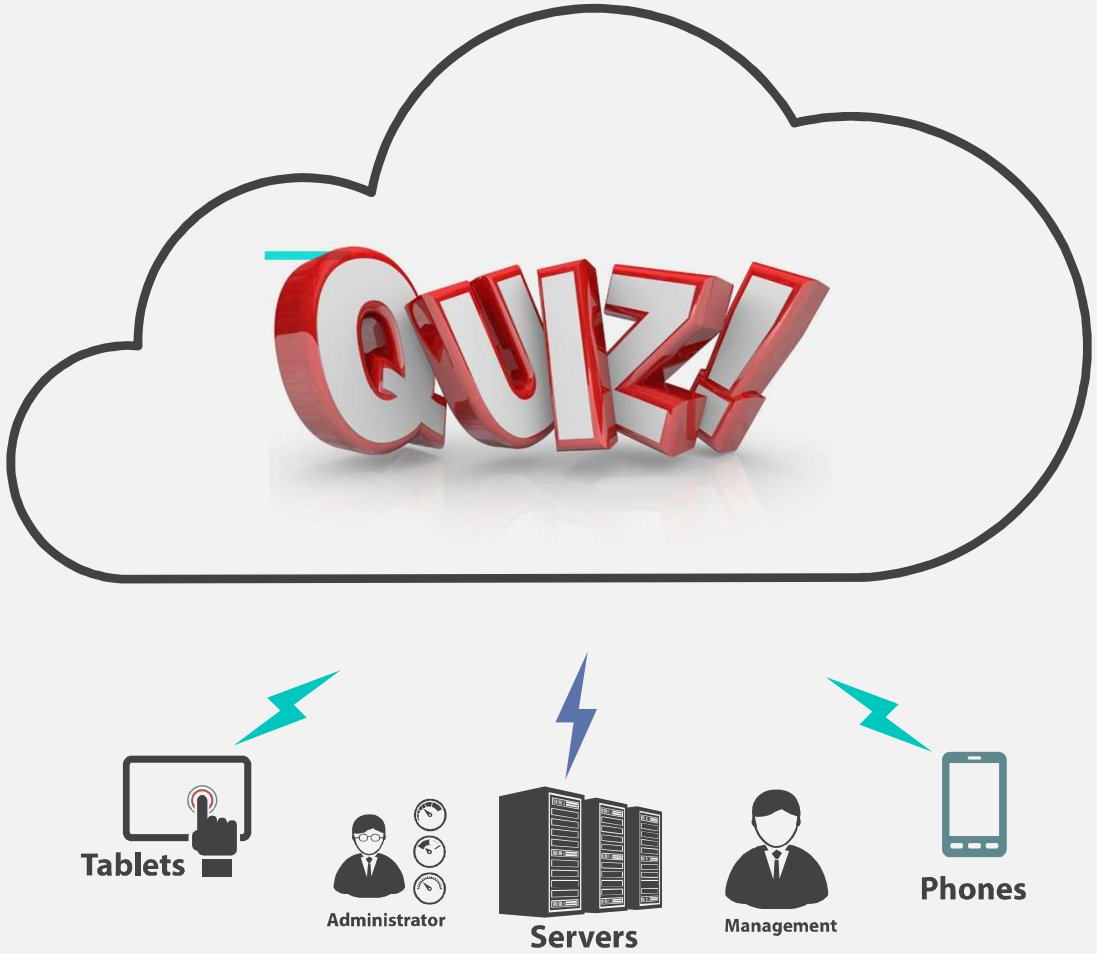
클라우드 아키텍처 구조

AWS Monitoring & Security Services

MEGAZONE CLOUD


QUIZ!
Tablets
Administrator
Servers
Management
Phones

Quiz

#1

다음 중 Amazon CloudFront를 가장 잘 설명한 것은 무엇인가?

① 하이브리드 클라우드 방식으로 인프라를 실행할 수 있도록 지원하는 서비스

② 컨테이너용 서버리스 컴퓨팅 엔진

③ 대기열을 통해 소프트웨어 구성 요소 간에 메시지를 보내고 받을 수 있는 서비스

④ 글로벌 콘텐츠 전송 서비스

Quiz

#2

다음 중 Amazon CloudFront에서 사용자가 어느 위치에 있든지 콘텐츠를 더 빠르게 전송하기 위해 콘텐츠 복사본을 캐싱하는 데 사용하는 사이트는 무엇인가?

① 리전
② 가용 영역
③ 엣지 로케이션
④ 오리진

Quiz

#3

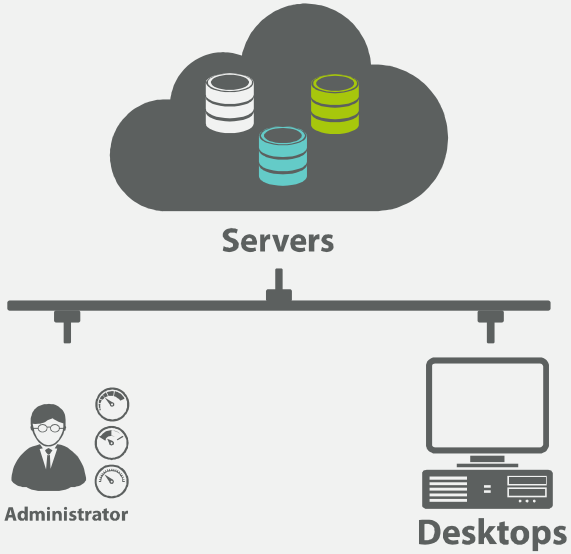
다음 중 도메인 이름의 DNS 레코드를 관리하는 데 사용되는 서비스는 무엇인가?

① Amazon Virtual Private Cloud

② AWS Direct Connect

③ Amazon CloudFront

④ Amazon Route 53



Index

01. 수업 목표

02. Amazon CloudWatch

03. AWS CloudTrail

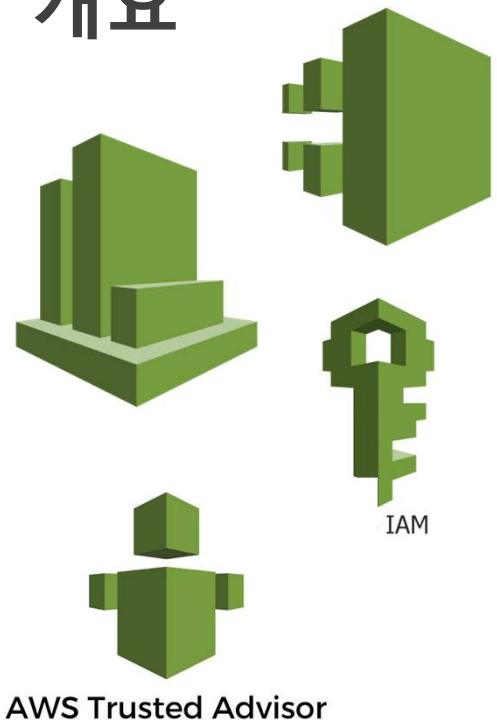
04. AWS Trusted Advisor

05. AWS Shared Responsibility Model

06. AWS IAM

수업 목표

개요



- Amazon CloudWatch에 대한 이해
- AWS CloudTrail에 대한 이해
- AWS Trusted Advisor에 대한 이해
- AWS Shared Responsibility Model 이해
- AWS IAM에 대한 이해

Amazon CloudWatch

AWS CloudWatch

What's AWS CloudWatch

- Is a web service.
- Enables client to monitor and manage various metrics and configure alarm actions based on data from those metrics.
- Uses metrics to represent the data points for client's resources.
- AWS services send metrics to CloudWatch.
- CloudWatch then uses these metrics to create graphs automatically that show how performance has changed over time.

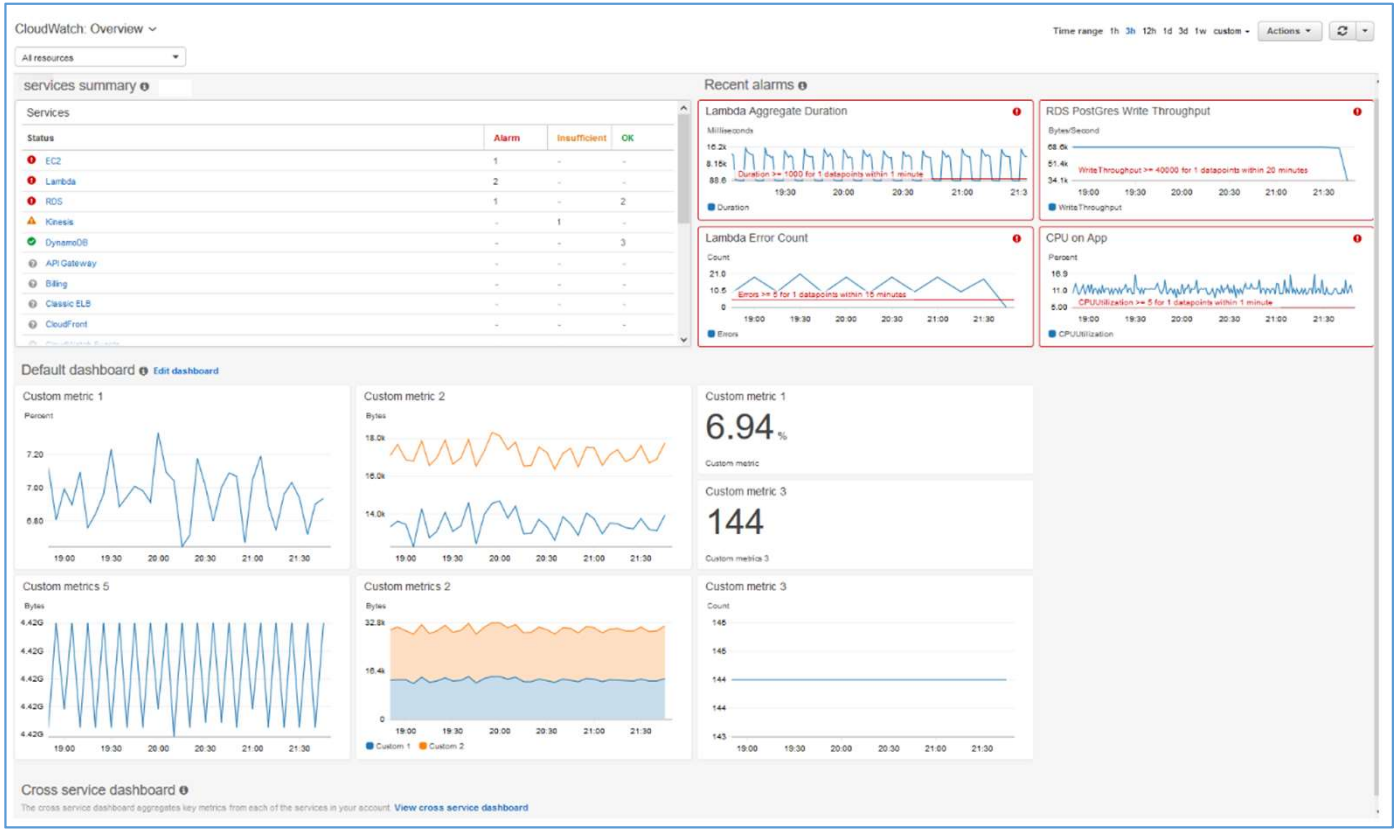
CloudWatch Alarms

- Automatically perform actions if the value of metric has gone above or below a predefined threshold.
- For example,
  - A company's developers use Amazon EC2 instances for application development or testing purposes.
  - If the developers occasionally forget to stop the instances, the instances will continue to run and incur charges.
- In this scenario, you could create a CloudWatch alarm
  - Automatically stops an Amazon EC2 instance when the CPU utilization percentage has remained below a certain threshold for a specified period.
  - When configuring the alarm, can specify to receive a notification whenever this alarm is triggered.

AWS CloudWatch

Amazon CloudWatch

CloudWatch dashboard



https://docs.aws.amazon.com/ko_kr/AmazonCloudWatch/latest/monitoring/GettingStarted.html

AWS CloudTrail

AWS CloudTrail

What's AWS CloudTrail ?

- Records API calls for your account.
- The recorded information includes :
  - The identity of the API caller
  - The time of the API call
  - The source IP address of the API caller.
- As a "trail" of breadcrumbs (or a log of actions) that someone has left behind them.

AWS CloudTrail

What's AWS CloudTrail ?

- It can use API calls to provision, manage, and configure AWS resources.
- With CloudTrail, it can view a complete history of user activity and API calls for applications and resources.
- Events are typically updated in CloudTrail **within 15 minutes** after an API call.
- It can filter events by specifying the time and date that an API call occurred, the user who requested the action, the type of resource that was involved in the API call, and more.

AWS CloudTrail

AWS CloudTrail event

What happened?

Who made the request?

When did this occur?

How was the request made?

CloudTrail Insights

- Within CloudTrail, can also enable CloudTrail Insights.
- Allows CloudTrail to automatically detect ***unusual*** API activities in AWS account.
- For example, CloudTrail Insights might detect that a higher number of Amazon EC2 instances than usual have recently launched in account.
- It can then review the full event details to determine which actions need to take next.

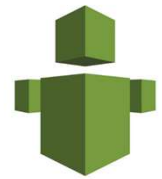
AWS Trusted Advisor

AWS Trusted Advisor

What's AWS Trusted Advisor ?

- Is a web service.
- Inspects AWS environment and provides real-time recommendations in accordance with AWS best practices.
- Compares its findings to AWS best practices in five categories:
  - Cost optimization
  - Performance
  - Security
  - Fault tolerance
  - Service limits.

AWS Trusted Advisor



What's AWS Trusted Advisor ?

- For the checks in each category, offers a list of recommended actions and additional resources to learn more about AWS best practices.
- The guidance can benefit company at all stages of deployment.
- For example, AWS Trusted Advisor assist :
  - Creating new workflows
  - Developing new applications.
  - Making ongoing improvements to existing applications and resources.

AWS Trusted Advisor

AWS Trusted Advisor dashboard

- The green check : the number of items for which it detected no problems.
- The orange triangle : the number of recommended investigations.
- The red circle : the number of recommended actions.

Quiz

#1

다음 중 Amazon CloudWatch를 사용하여 수행할 수 있는 작업은 무엇인가? (2개 선택)

① 리소스 활용도 및 성능 모니터링

② AWS 환경 개선을 위한 실시간 권장 사항 받기

③ 5개 범주에서 인프라를 AWS 모범 사례와 비교

④ 단일 대시보드에서 지표에 액세스

⑤ 비정상적인 계정 활동을 자동 감지

Quiz

#2

다음 중 오픈 액세스 권한을 확인하여 Amazon S3 버킷의 보안을 검토할 수 있는 서비스는 무엇인가?

① Amazon CloudWatch

② AWS CloudTrail

③ AWS Trusted Advisor

④ Amazon GuardDuty

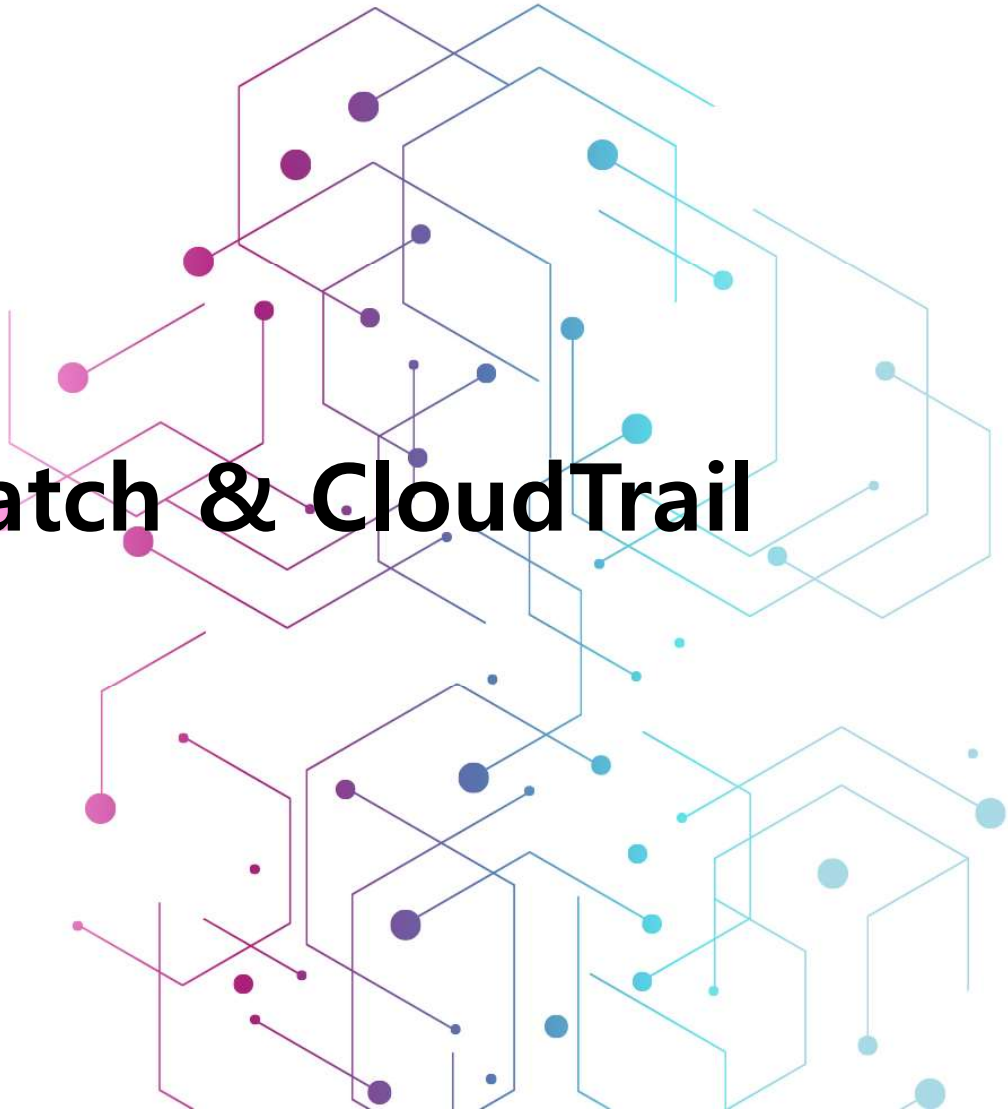
Quiz

#3

다음 중 AWS Trusted Advisor 대시보드의 범주에 포함되는 항목은 무엇인가? (2개 선택)

① 안정성
② 성능
③ 확장성
④ 탄력성
⑤ 내결함성

Lab1. Using CloudWatch & CloudTrail



AWS Shared Responsibility Model

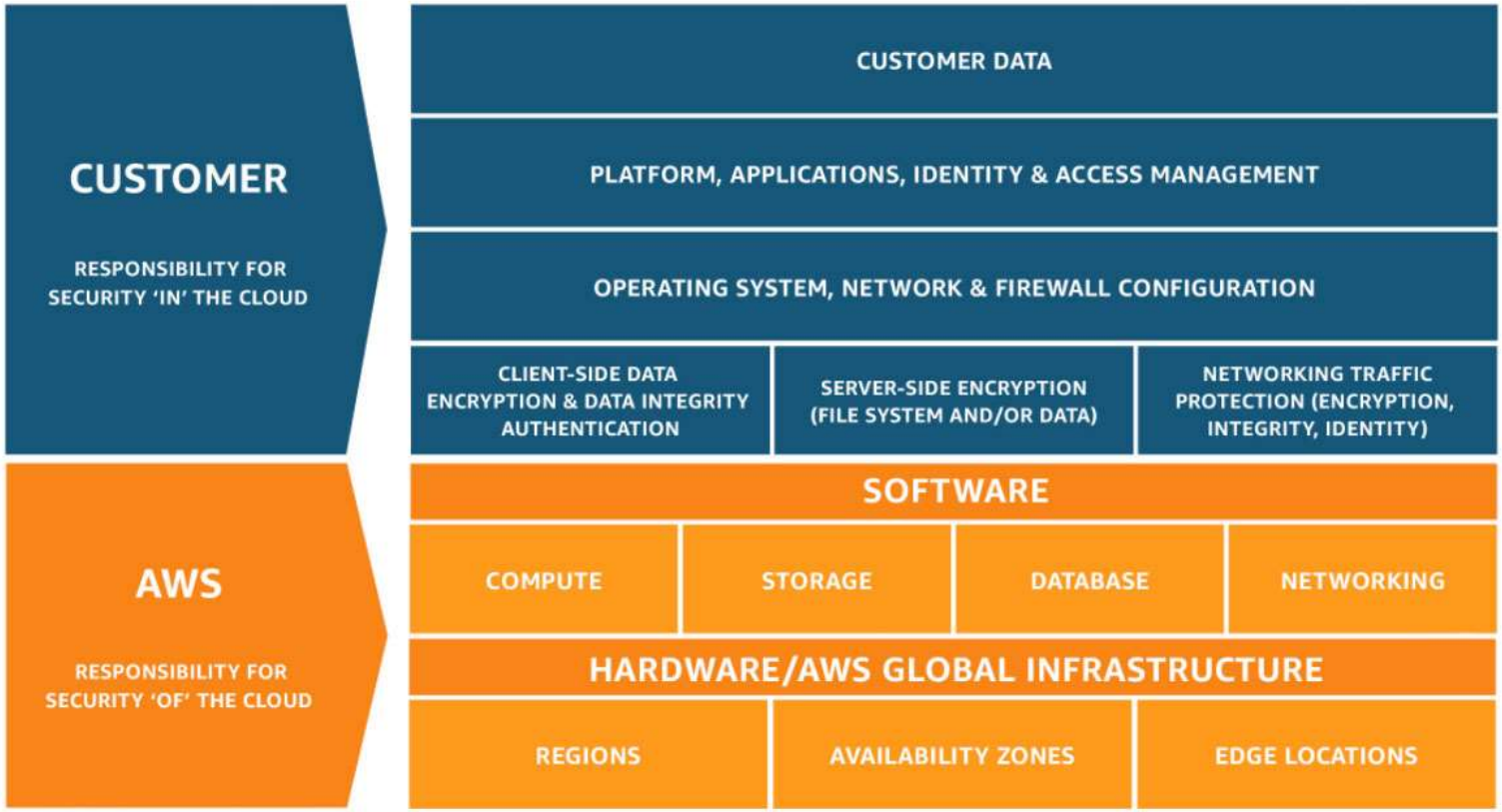
AWS Shared Responsibility Model

What's AWS Shared Responsibility Model

- Who is responsible for keeping AWS resources secure?
  - The customer
  - or AWS
- The answer is both.
- Divides into :
  - Customer responsibilities (commonly referred to as ***security in the cloud***)
  - AWS responsibilities (commonly referred to as ***security of the cloud***).

AWS Shared Responsibility Model

What's AWS Shared Responsibility Model



AWS Shared Responsibility Model

Knowledge Check

Which tasks are the responsibilities of customers? (Select TWO.)

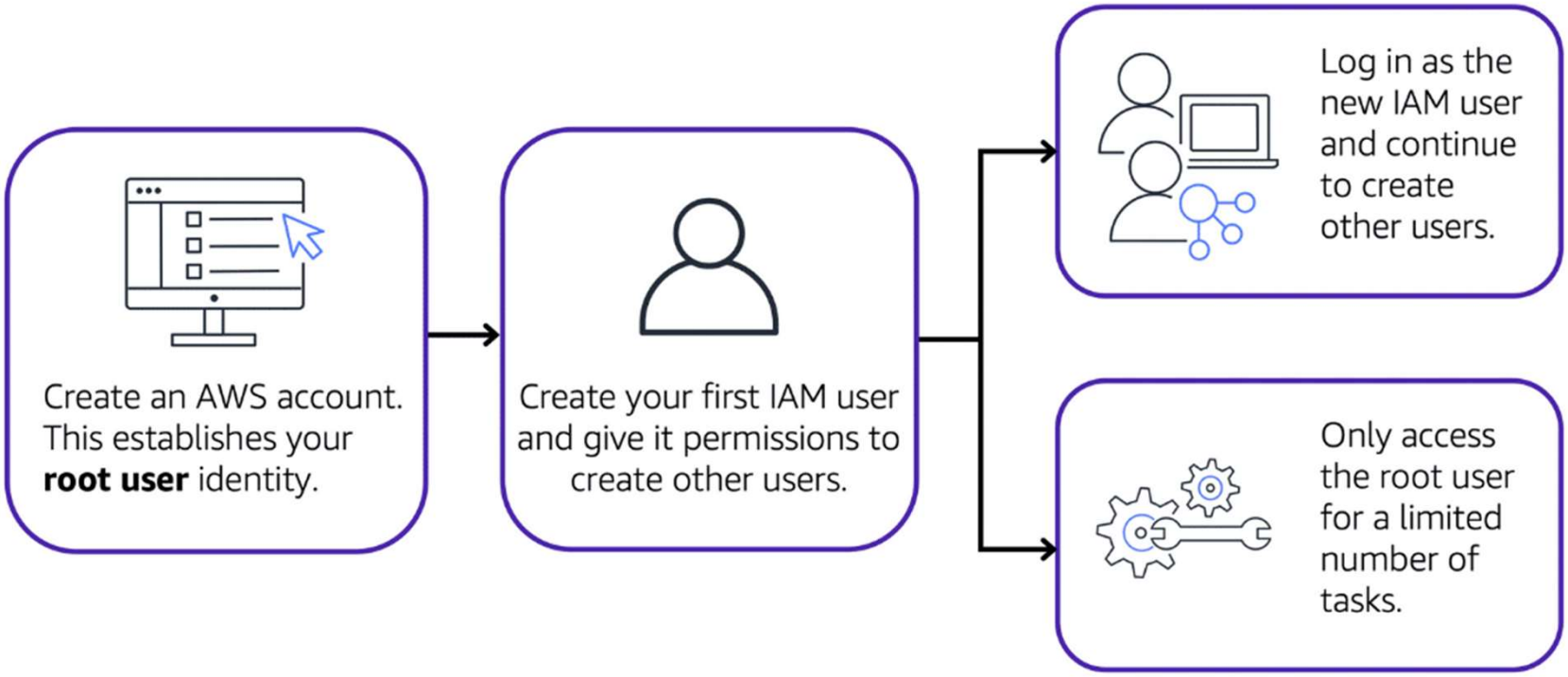
① Maintaining network infrastructure
② Patching software on Amazon EC2 instances
③ Implementing physical security controls at data centers
④ Setting permissions for Amazon S3 objects
⑤ Maintaining servers that run Amazon EC2 instances

AWS Identity and Access Management (IAM)

What's AWS IAM

- Enables to manage access to AWS services and resources securely.
- Gives the flexibility to configure access based on company's specific operational and security needs.
- Using a combination of IAM features :
  - IAM users, groups, and roles
  - IAM policies
  - Multi-factor authentication

AWS account root user



Best Practice : root user

- ***Do not use*** the **root user** for everyday tasks.
- Instead, use the root user to create your first **IAM user** and assign it permissions to create other users.
- Then, continue to create other IAM users, and access those identities for performing regular tasks throughout AWS.
- ***Only use*** the root user when need to perform a limited number of tasks that are only available to the root user.
- Examples of these tasks include changing root user email address and changing AWS support plan.

IAM Users

- Represents the person or application that interacts with AWS services and resources.
- Consists of a name and credentials.
- By default, when create a new IAM user in AWS, it has no permissions associated with it.
- To allow the IAM user to perform specific actions in AWS, such as launching an Amazon EC2 instance or creating an Amazon S3 bucket, must grant the IAM user the necessary permissions.

IAM Policies

- Are **a document** that allows or denies permissions to AWS services and resources.
- Enable to customize users' levels of access to resources.
- For example, can allow users to access all of the Amazon S3 buckets within AWS account, or only a specific bucket.

Best Practice : IAM policies

- Follow the security principle of **least privilege** when granting permissions.
- By following this principle, help to prevent users or roles from having more permissions than needed to perform their tasks.

IAM Groups

- Are a collection of IAM users.
- When assign an IAM policy to a group, all users in the group are granted permissions specified by the policy.

IAM Roles

- Are an identity that can assume to gain temporary access to permissions.
- Before an IAM user, application, or service can assume an IAM role, they must be granted permissions to switch to the role.
- When someone assumes an IAM role, they abandon all previous permissions that they had under a previous role and assume the permissions of the new role.

Multi-factor authentication

- Have ever signed in to a website that required to provide multiple pieces of information to verify your identity?
- You might have needed to provide your password and then a second form of authentication, such as a random code sent to your phone.

Lab2. IAM User, Group 생성 및 역할 다루기

Quiz

#1

다음 중 IAM 정책을 가장 잘 설명한 것은 무엇인가?

① AWS 계정에 추가 보호 계층을 제공하는 인증 프로세스
② AWS 서비스 및 리소스에 대한 권한을 부여하거나 거부하는 문서
③ 임시로 권한에 액세스하기 위해 수임할 수 있는 자격 증명
④ AWS 계정을 처음 만들면 설정되는 자격 증명

Quiz

#2

만일 직원이 여러 Amazon S3 버킷을 생성하기 위해 임시 액세스 권한이 필요하다면, 다음 중 이 작업에 가장 적합한 옵션을 무엇인가?

① AWS 계정 루트 사용자
② IAM 그룹
③ IAM 역할
④ 서비스 제어 정책(SCP)

Quiz

#3

다음 중 최소 권한 원칙을 가장 잘 설명한 것은 무엇인가?

① IAM 사용자를 하나 이상의 IAM 그룹에 추가
② 액세스 제어 목록에서 패킷의 권한을 확인
③ 특정 작업을 수행하는 데 필요한 권한만 부여
④ 하나 이상의 디바이스에서 시작하는 서비스 거부 공격을 수행