

AWS Practitioner Skill Builder

Module 3 / 4 Study

Module 3

Module 3

Topic : 고가용성 (High Availability)

- 시스템이나 서비스가 계속 이용가능한 상태로 유지되는 것
- 예시 : 현금 자동화 인출기 (ATM)

ChatGPT

물론입니다! 고가용성은 시스템이나 서비스가 계속해서 이용 가능하고 작동하는 능력을 나타냅니다. 이를 이해하기 쉬운 예시로는 ATM(자동화된 현금인출기)가 있습니다.

일반적으로 은행의 ATM은 고가용성을 유지해야 합니다. 왜냐하면 사람들이 24시간 동안 언제든지 현금을 인출할 수 있어야 하기 때문입니다. 만약 ATM이 고장나거나 다른 이유로 작동을 멈춘다면, 이는 고객들에게 큰 불편을 주게 될 것입니다.

따라서 은행은 고가용성을 유지하기 위해 여러 가지 방법을 사용합니다. 예를 들어, 여러 대의 ATM을 설치하여 한 대가 고장나도 다른 ATM을 이용할 수 있게 합니다. 또한 정기적인 점검과 유지보수를 통해 잠재적인 문제를 사전에 예방하고, 백업 시스템을 갖추어 장애 발생 시 빠르게 대응할 수 있도록 합니다.

이러한 조치들은 ATM이 항상 고객들에게 서비스를 제공할 수 있도록 하여 고가용성을 확보하는데 도움이 됩니다.

ATM 은 우리가 원할 때, 원하는 시간에 언제든지 이용할 수 있어야 한다.

그러기 위해서는 ATM 은 사람들이 언제든지 이용할 수 있는 상태를 유지해야 한다.

이처럼 AWS는 여러 리전, 여러 가용영역 (AZ)을 제공하여 언제 어디서든 원하는 시간에 언제든지 이용할 수 있는 상태를 유지한다.

Module 3

Topic : AWS 리전

- 서비스, 데이터 및 애플리케이션에 적합한 리전을 결정할 때 다음 네 가지 비즈니스 요소를 고려해야 함.

데이터 거버넌스 및 법적 요구 사항 준수

회사와 위치에 따라 특정 영역에서 데이터를 실행해야 할 수도 있습니다. 예를 들어 회사에 모든 데이터를 영국 내부에 유지해야 한다는 규정이 있는 경우 런던 리전을 선택합니다. 모든 회사에 위치 기반 데이터 규정이 있는 것은 아니므로 다른 세 가지 요소에 더 집중해야 할 수도 있습니다.

고객과의 근접성

고객과 가까운 리전을 선택하면 고객에게 콘텐츠를 더 빠르게 제공하는 데 도움이 됩니다. 예를 들어 본사는 워싱턴 DC에 있고 고객 중 다수가 싱가포르에 거주하고 있다고 가정합니다. 인프라를 본사와 가까운 버지니아 북부 리전에서 실행할지, 고객과 가까운 싱가포르 리전에서 실행할지 고려해야 합니다.

리전 내에서 사용 가능한 서비스

경우에 따라 고객에게 제공하려는 기능이 가장 가까운 리전에 없을 수도 있습니다. AWS는 새로운 서비스를 개발하고 기존 서비스의 기능을 확장하며 혁신을 주도하고 있습니다. 그러나 AWS가 전 세계에서 새로운 서비스를 제공할 수 있으려면 경우에 따라 각 리전마다 물리적 하드웨어를 구축해야 할 수도 있습니다.

개발자가 Amazon Braket (AWS 양자 컴퓨팅 플랫폼)을 사용하는 애플리케이션을 빌드하기를 원한다고 가정해 보겠습니다. 이 과정이 작성된 시점에는 아직 Amazon Braket이 전 세계 모든 AWS 리전에서 제공되지 않으므로 개발자는 이미 서비스를 제공하는 리전 중 하나에서 이 플랫폼을 실행해야 합니다.

요금

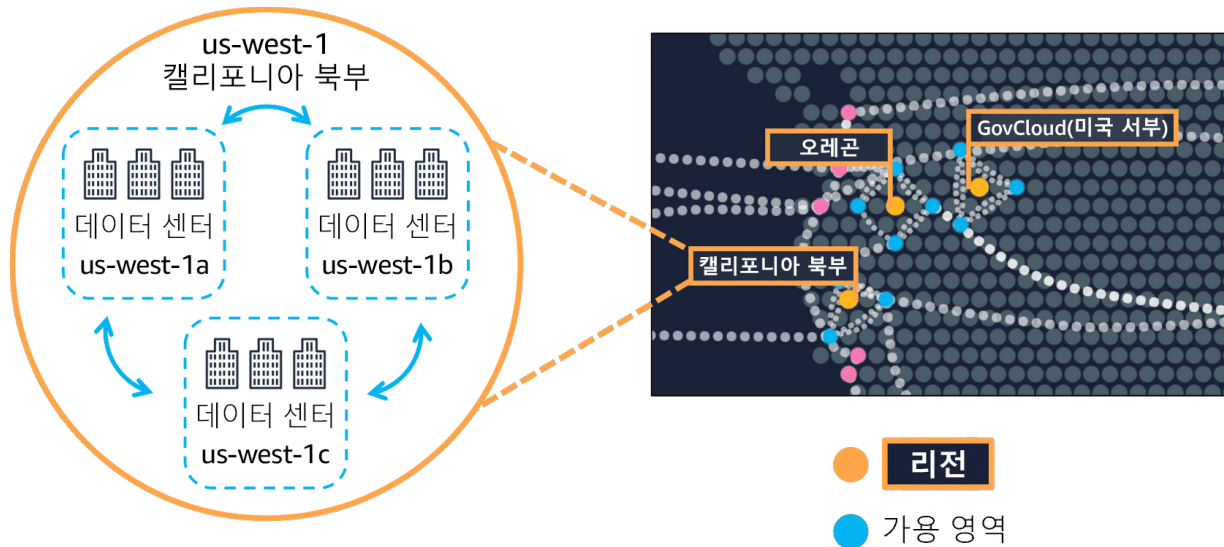
미국과 브라질 모두에서 애플리케이션을 실행할 것을 고려한다고 가정해 보겠습니다. 브라질의 세제 때문에 상파울루 리전은 오레곤 리전과 비교하여 동일한 워크로드를 실행하는 데 50% 더 많은 비용이 소요될 수 있습니다.

요금을 결정하는 몇 가지 요인에 대해 더 자세히 배울 예정이지만, 지금은 서비스 비용이 리전마다 다를 수 있음을 알고 있으면 됩니다.

Module 3

Topic : AWS 가용영역

- 리전 내의 단일 데이터 센터 또는 데이터 센터 그룹



- 서로 수십 ~ 수백 KM가 떨어져 있습니다.

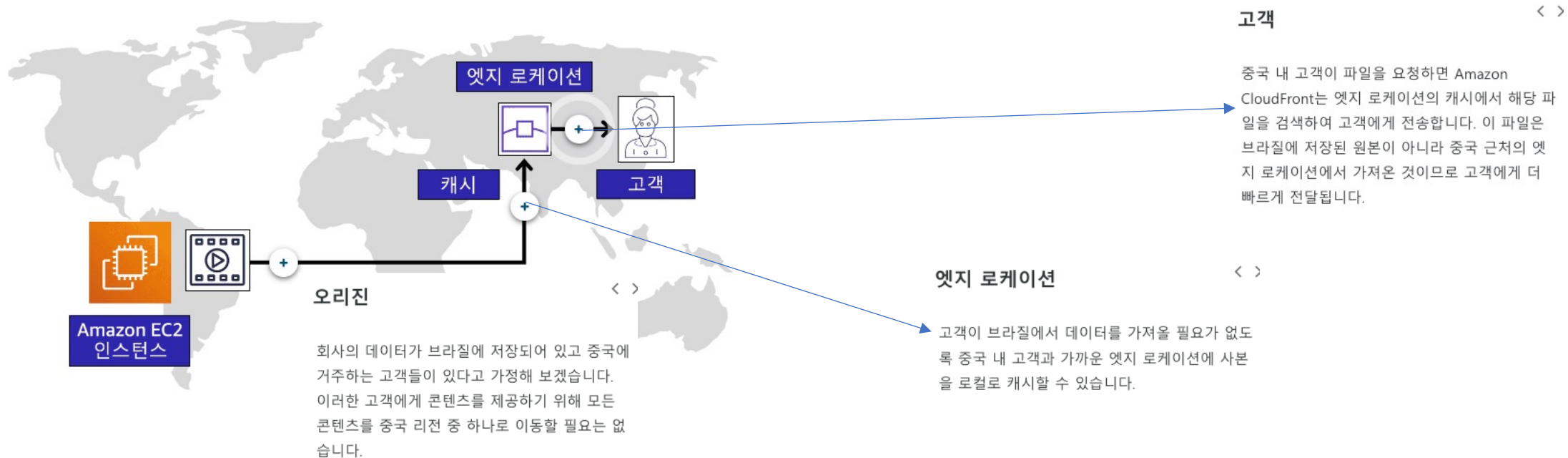
- 이 간격은 가용 영역 간의 지연 시간(콘텐츠가 요청된 시점과 수신된 시점 간의 차이)이 짧을 정도로 충분히 가깝음.

- 그러나 리전의 한 부분에서 재해가 발생할 경우 여러 가용 영역이 영향을 받을 가능성을 줄일 만큼 멀리 떨어져 있습니다.

Module 3

Topic : 엣지 로케이션

- Amazon CloudFront가 더 빠른 콘텐츠 전송을 위해 고객과 가까운 위치에 콘텐츠 사본을 캐시하는 데 사용하는 사이트
- CDN : Content Delivery Network의 약자, 전 세계 고객과 더 가까운 곳에 데이터 복사본을 캐싱하는 작업, AWS 에서는 이를 CloudFront라는 서비스로 명칭



Module 3

Topic : 리소스 프로비저닝 방법

AWS Management Console

Amazon 서비스 액세스 및 관리를 위한 웹 기반 인터페이스입니다. 최근에 사용한 서비스에 빠르게 액세스하고 이름, 키워드 또는 약어로 다른 서비스를 검색할 수 있습니다. 콘솔에는 작업을 수행하는 프로세스를 단순화할 수 있는 마법사 및 자동화된 워크플로가 포함되어 있습니다.

또한 AWS 콘솔 모바일 애플리케이션을 사용하여 리소스 모니터링, 경보 보기, 결제 정보 확인 등의 작업을 수행할 수 있습니다. 여러 ID가 동시에 AWS 콘솔 모바일 앱에 로그인할 수 있습니다.

AWS 명령줄 인터페이스(AWS CLI)

AWS CLI를 사용하면 하나의 도구를 통해 명령줄에서 직접 여러 AWS 서비스를 제어할 수 있습니다. AWS CLI는 Windows, macOS 및 Linux 사용자가 사용할 수 있습니다.

AWS CLI를 사용하면 스크립트를 통해 서비스 및 애플리케이션이 수행하는 작업을 자동화할 수 있습니다. 예를 들어 Amazon EC2 인스턴스를 시작하고 Amazon EC2 인스턴스를 특정 Auto Scaling 그룹에 연결하는 등의 작업을 명령을 사용해 수행할 수 있습니다.

소프트웨어 개발 키트(SDK)

SDK를 사용하면 프로그래밍 언어 또는 플랫폼용으로 설계된 API를 통해 AWS 서비스를 보다 간편하게 사용할 수 있습니다. SDK를 통해 AWS 서비스를 기존 애플리케이션과 함께 사용하거나 AWS에서 실행할 완전히 새로운 애플리케이션을 생성할 수 있습니다.

SDK를 사용하기 시작하는 데 도움이 되도록 AWS는 지원되는 각 프로그래밍 언어에 대한 설명서와 샘플 코드를 제공합니다. 지원되는 프로그래밍 언어에는 C++, 자바, .NET 등이 있습니다.

Module 3

Topic : 리소스 프로비저닝 방법

AWS Elastic Beanstalk

AWS Elastic Beanstalk에서는 사용자가 코드 및 구성 설정을 제공하면 Elastic Beanstalk이 다음 작업을 수행하는 데 필요한 리소스를 배포

- 용량 조정
- 로드 밸런싱
- 자동 조정
- 애플리케이션 상태 모니터링

AWS CloudFormation

AWS CloudFormation을 사용하여 인프라를 코드로 취급

즉, AWS Management Console을 사용하여 개별적으로 리소스를 프로비저닝하는 대신 코드 줄을 작성하여 환경을 구축 가능

AWS CloudFormation은 리소스를 안전하고 반복 가능한 방식으로 프로비저닝하므로 수작업을 수행하거나 사용자 지정 스크립트를 작성할 필요 없이 인프라 및 애플리케이션을 빈번히 구축할 수 있음

이 서비스는 스택을 관리할 때 수행해야 할 적절한 작업을 결정하고 오류를 감지하면 변경 사항을 자동으로 롤백함

Module 4

Module 4

Topic : VPC (Virtual Private Cloud)

AWS 서비스를 사용하는 수백만 명의 고객을 상상해 보십시오. 또한 이들 고객이 생성한 Amazon EC2 인스턴스와 같은 수백만 개의 리소스를 상상해 보십시오.

이러한 모든 리소스에 경계가 없으면 네트워크 트래픽이 제한 없이 리소스 간에 흐를 수 있습니다. AWS 리소스에 경계를 설정하는 데 사용할 수 있는 네트워킹 서비스가 [Amazon Virtual Private Cloud\(Amazon VPC\)](#)입니다.

Amazon VPC를 사용하여 AWS 클라우드의 격리된 섹션을 프로비저닝할 수 있습니다. 이 격리된 섹션에서는 사용자가 정의한 가상 네트워크에서 리소스를 시작할 수 있습니다.

한 Virtual Private Cloud(VPC) 내에서 여러 서브넷으로 리소스를 구성할 수 있습니다. 서브넷은 리소스(예: Amazon EC2 인스턴스)를 포함할 수 있는 VPC 섹션입니다.

Module 4

Topic : Internet GateWay

인터넷의 퍼블릭 트래픽이 VPC에 액세스하도록 허용하려면 **인터넷 게이트웨이**를 VPC에 연결합니다.

인터넷 게이트웨이는 VPC와 인터넷 간의 연결입니다. 인터넷 게이트웨이는 고객이 커피숍에 들어가기 위해 사용하는 출입문과 비슷한 것으로 생각할 수 있습니다. 인터넷 게이트웨이가 없으면 아무도 VPC 내의 리소스에 액세스할 수 없습니다.

Module 4

Topic : 가상 프라이빗 게이트웨이

VPC 내의 비공개 리소스에 액세스하려면 **가상 프라이빗 게이트웨이**를 사용할 수 있습니다.

다음은 가상 프라이빗 게이트웨이 작동 방식의 예입니다. 인터넷은 집과 커피숍 사이의 도로로 생각할 수 있습니다. 이 도로를 보디가드와 함께 지나간다고 가정해 보십시오. 다른 고객과 동일한 도로를 사용하고 있지만 추가 보호 계층이 있습니다.

보디가드는 주변의 다른 모든 요청으로부터 인터넷 트래픽을 암호화(또는 보호)하는 가상 프라이빗 네트워크 (VPN) 연결과 같습니다.

가상 프라이빗 게이트웨이는 보호된 인터넷 트래픽이 VPC로 들어오도록 허용하는 구성 요소입니다. 커피숍까지 가는 도로에는 추가적인 보호 기능이 있지만 다른 고객과 동일한 도로를 사용하고 있기 때문에 교통 체증이 발생할 수 있습니다.

가상 프라이빗 게이트웨이를 사용하면 VPC와 프라이빗 네트워크(예: 온프레미스 데이터 센터 또는 회사 내부 네트워크) 간에 가상 프라이빗 네트워크(VPN) 연결을 설정할 수 있습니다. 가상 프라이빗 게이트웨이는 승인된 네트워크에서 나오는 트래픽만 VPC로 들어가도록 허용합니다.

Module 4

Topic : AWS Direct Connect

[AWS Direct Connect](#)는 데이터 센터와 VPC 간에 비공개 전용 연결을 설정하는 서비스입니다. 커피숍과 직접 연결되는 복도가 있는 아파트 건물이 있다고 가정하면, 아파트 입주자만 이 복도를 사용할 수 있습니다.

이 사설 복도는 AWS Direct Connect와 동일한 유형의 전용 연결을 제공하며, 입주민은 다른 고객도 함께 사용하는 공공 도로를 거칠 필요 없이 커피숍에 들어갈 수 있다.

AWS Direct Connect가 제공하는 비공개 연결은 네트워크 비용을 절감하고 네트워크를 통과할 수 있는 대역폭을 늘리는 데 도움이 된다

Module 4

Topic : Subnet



퍼블릭 서브넷에는 온라인 상점의 웹 사이트와 같이 누구나 액세스할 수 있어야 하는 리소스가 포함되며, 프라이빗 서브넷에는 고객의 개인 정보 및 주문 내역이 포함된 데이터베이스와 같이 프라이빗 네트워크를 통해서만 액세스할 수 있는 리소스가 포함된다.

VPC 내에서 서브넷은 서로 통신할 수 있습니다. 예를 들어 퍼블릭 서브넷에 있는 Amazon EC2 인스턴스가 프라이빗 서브넷에 있는 데이터베이스와 통신하는 애플리케이션이 있을 수 있다.

Module 4

Topic : 네트워크 ACL (액세스 제어 목록)

네트워크 ACL (액세스 제어 목록)은 서브넷 수준에서 인바운드 및 아웃바운드 트래픽을 제어하는 가상 방화벽입니다.

각 AWS 계정에는 기본 네트워크 ACL이 포함됩니다.

VPC를 구성할 때 계정의 기본 네트워크 ACL을 사용하거나 사용자 지정 네트워크 ACL을 생성할 수 있습니다.

계정의 기본 네트워크 ACL은 기본적으로 모든 인바운드 및 아웃바운드 트래픽을 허용하지만 사용자가 자체 규칙을 추가하여 수정할 수 있습니다.

사용자 지정 네트워크 ACL은 사용자가 허용할 트래픽을 지정하는 규칙을 추가할 때까지 모든 인바운드 및 아웃바운드 트래픽을 거부하며 또한 모든 네트워크 ACL에는 명시적 거부 규칙이 있습니다. 이 규칙은 패킷이 목록의 다른 모든 규칙과 일치하지 않으면 해당 패킷이 거부되도록 합니다.

Module 4

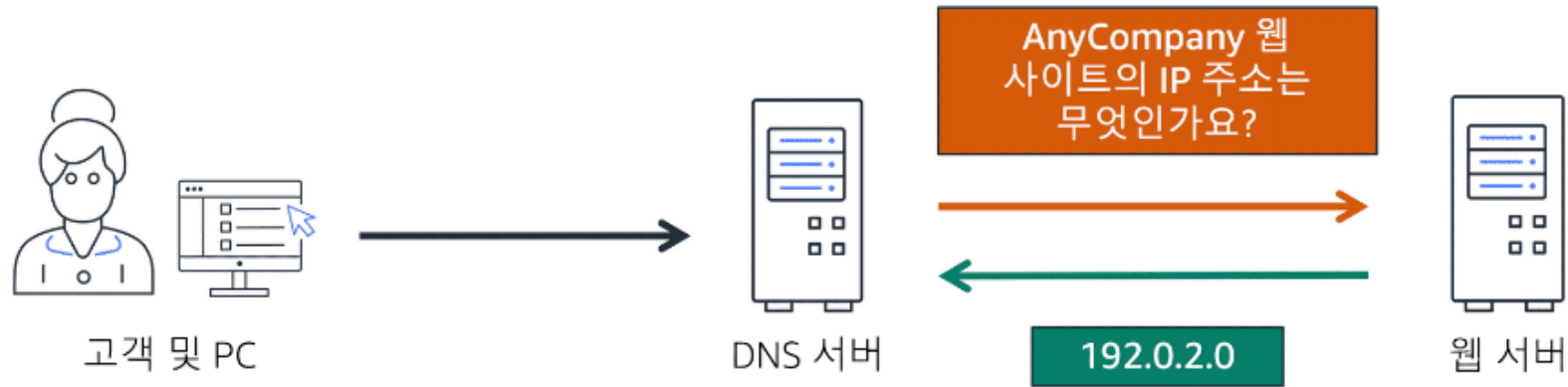
Topic : 보안 그룹

보안 그룹은 Amazon EC2 인스턴스에 대한 인바운드 및 아웃바운드 트래픽을 제어하는 가상 방화벽

기본적으로 보안 그룹은 모든 인바운드 트래픽을 거부하고 모든 아웃바운드 트래픽을 허용하며, 사용자 지정 규칙을 추가하여 허용 또는 거부할 트래픽을 구성할 수 있다

Module 4

Topic : Route 53



Amazon Route 53는 DNS 웹 서비스이며, 개발자와 비즈니스가 최종 사용자를 AWS에서 호스팅 되는 인터넷 애플리케이션으로 라우팅할 수 있는 안정적인 방법을 제공

Amazon Route 53는 사용자 요청을 AWS에서 실행되는 인프라(예: Amazon EC2 인스턴스 및 로드 밸런서)에 연결하며, 사용자를 AWS 외부의 인프라로 라우팅할 수 있습니다.

Route 53의 또 다른 기능에는 도메인 이름의 DNS 레코드를 관리하는 기능도 있습니다.