

3단원. **AWS** 핵심 서비스

대상: 전공자 · 정보처리기사 취득자 | 목적: 인프라 직무(네트워크·클라우드·시스템·보안) 기술 면접 대비
중요도: ★★★ 최빈출 · ★★ 자주 출제 · ★ 기본 개념

Q1. EC2란 무엇이며 주요 구성 요소를 설명하세요. ★★★

답안 **EC2(Elastic Compute Cloud)**는 AWS의 대표적인 IaaS 서비스로, 가상 서버(인스턴스)를 필요한 만큼 생성해 사용할 수 있는 컴퓨팅 서비스입니다. 인스턴스를 생성할 때는 CPU·메모리 사양을 결정하는 인스턴스 타입, OS와 초기 소프트웨어가 담긴 **AMI(Amazon Machine Image)**, 트래픽을 제어하는 보안 그룹, 그리고 데이터를 저장하는 **EBS** 볼륨을 함께 설정합니다. 인스턴스는 온디맨드, 예약 인스턴스, 스팟 인스턴스 등 다양한 과금 방식으로 사용할 수 있으며, 특정 AZ에 배치되기 때문에 고가용성을 위해서는 여러 AZ에 걸쳐 인스턴스를 분산 배치하는 것이 일반적입니다.

관련 개념 AMI, EBS, 보안 그룹, 인스턴스 타입, 탄력적 IP(EIP)

Q2. S3의 특징과 스토리지 클래스를 설명하세요. ★★★

답안 **S3(Simple Storage Service)**는 파일을 객체(Object) 단위로 저장하는 오브젝트 스토리지 서비스로, 사실상 무제한에 가까운 확장성과 높은 내구성(설계상 매우 높은 데이터 내구성)을 제공합니다. 데이터는 버킷(**Bucket**)이라는 논리적 컨테이너 안에 키-값 형태로 저장되며, 파일 시스템처럼 계층 구조를 갖지는 않지만 접두어(Prefix)를 이용해 폴더처럼 관리할 수 있습니다. 접근 빈도에 따라 표준 스토리지, 접근 빈도가 낮은 데이터용 클래스, 장기 보관용 아카이브 클래스 등 여러 스토리

지 클래스를 선택할 수 있어 비용을 최적화할 수 있으며, 정적 웹사이트 호스팅, 백업, 로그 저장, 빅데이터 원본 저장소 등 다양한 용도로 사용됩니다.

관련 개념 오브젝트 스토리지, 버킷 정책, 수명주기 정책(Lifecycle), 버저닝, 내구성/가용성

Q3. VPC란 무엇이며 왜 필요한가요? ★★★

답안 **VPC(Virtual Private Cloud)**는 AWS 클라우드 내에 사용자가 논리적으로 격리된 가상 네트워크 공간을 구성할 수 있게 해주는 서비스로, IP 대역(CIDR), 서브넷, 라우팅 테이블, 게이트웨이 등을 자유롭게 설계할 수 있습니다. VPC가 필요한 이유는 각 리소스를 원하는 네트워크 구조로 격리하고 접근을 통제함으로써 보안성을 확보하고, 온프레미스 네트워크와 유사한 방식으로 퍼블릭/프라이빗 영역을 구분해 트래픽 흐름을 세밀하게 관리할 수 있기 때문입니다. VPC 내부는 서브넷 단위로 나뉘며, 인터넷 게이트웨이를 통해 외부와 통신하는 퍼블릭 서브넷과, 외부에서 직접 접근이 불가능한 프라이빗 서브넷으로 구성해 다계층 아키텍처(웹-앱-DB)를 설계하는 것이 일반적입니다.

관련 개념 CIDR, 서브넷, 라우팅 테이블, 인터넷 게이트웨이, NAT 게이트웨이

Q4. IAM의 역할과 주요 구성 요소(사용자, 그룹, 역할, 정책)를 설명하세요. ★★★

답안 **IAM(Identity and Access Management)**은 AWS 리소스에 대한 인증과 인가를 관리하는 서비스로, "누가 어떤 자원에 어떤 작업을 할 수 있는가"를 정의합니다. 사용자(**User**)는 개별 계정으로 사람이나 애플리케이션에 발급되며, 그룹(**Group**)은 여러 사용자를 묶어 동일한 권한을 일괄 부여할 때 사용합니다. 역할(**Role**)은 특정 개체(EC2 인스턴스, 다른 AWS 계정, Lambda 등)가 일시적으로 위임받아 사용하는 권한 집합으로, 고정된 자격 증명을 코드에 하드코딩하지 않고 안전하게 권한을 위임할 수 있습니다. 정책(**Policy**)은 JSON 형식으로 허용/거부할 작

업과 리소스를 명시한 문서로, 최소 권한 원칙(Least Privilege)에 따라 필요한 권한만 부여하는 것이 보안 모범 사례입니다.

관련 개념 최소 권한 원칙, 역할 기반 접근제어(RBAC), Assume Role, 정책 문서(JSON), MFA

Q5. RDS란 무엇이며 자체 구축 DB 대비 장점을 설명하세요. ★★

답안 **RDS(Relational Database Service)**는 MySQL, PostgreSQL, MariaDB 등 관계형 데이터베이스 엔진을 관리형으로 제공하는 서비스로, AWS가 백업, 패치, 장애 복구, 스케일링 같은 운영 작업을 대신 처리해줍니다. 자체 구축(EC2에 DB 설치) 대비 장점은 자동 백업과 스냅샷, 장애 발생 시 대기 인스턴스로 자동 전환하는 **Multi-AZ** 구성, 읽기 부하 분산을 위한 읽기 전용 복제본(**Read Replica**) 생성이 쉽다는 점입니다. 또한 마이너 버전 패치나 보안 업데이트가 자동화되어 운영 부담이 크게 줄어듭니다. 다만 관리형 서비스이기 때문에 OS 레벨 접근이나 특정 엔진 설정에 대한 세밀한 커스터마이징에는 제약이 있을 수 있습니다.

관련 개념 Multi-AZ, Read Replica, 자동 백업, 관리형 서비스, 패치 관리

Q6. AWS의 CloudFront(CDN)는 어떤 역할을 하나요? ★★

답안 **CloudFront**는 AWS의 **CDN(Content Delivery Network)** 서비스로, 전 세계에 분산된 엣지 로케이션(Edge Location)에 콘텐츠를 캐싱해 사용자와 물리적으로 가까운 위치에서 콘텐츠를 제공함으로써 지연시간을 줄이고 원본 서버(**Origin**)의 부하를 경감합니다. 정적 파일(이미지, CSS, JS)뿐 아니라 동적 콘텐츠도 배포할 수 있으며, S3나 EC2, 온프레미스 서버를 오리진으로 지정할 수 있습니다. 또한 HTTPS 처리를 엣지에서 담당하고, DDoS 방어나 WAF와 연동해 보안을 강화할 수 있으며, 오리진으로 향하는 요청 수를 줄여 비용 절감 효과도 있습니다. 글로벌 서비스를 운영할 때 사용자 경험 개선을 위한 필수 구성 요소로 자주 언급됩니다.

관련 개념 엣지 로케이션, 캐시 무효화(Invalidation), 오리진, TTL, WAF 연동

Q7. Route 53의 역할과 라우팅 정책을 설명하세요. ★★

답안 **Route 53**은 AWS의 **DNS(도메인 네임 시스템)** 서비스로, 도메인 이름을 IP 주소로 변환해주는 역할과 함께 도메인 등록, 헬스체크, 트래픽 라우팅 기능을 제공합니다. 다양한 라우팅 정책을 지원하는데, 단순히 하나의 리소스로 연결하는 단순 라우팅, 여러 리소스에 가중치를 부여해 트래픽을 분산하는 가중치 기반 라우팅, 사용자와 가장 가까운 리전으로 연결하는 지연시간 기반 라우팅, 그리고 장애 발생 시 자동으로 대기 리소스로 전환하는 장애조치(**Failover**) 라우팅이 있습니다. 헬스체크 기능과 결합하면 특정 엔드포인트에 장애가 발생했을 때 자동으로 정상 엔드포인트로 트래픽을 우회시킬 수 있어고가용성 아키텍처 구축에 활용됩니다.

관련 개념 DNS, 헬스체크, 가중치 기반 라우팅, 지연시간 기반 라우팅, Failover 라우팅

Q8. AWS의 공유 책임 모델(Shared Responsibility Model)을 설명하세요. ★★★

답안 공유 책임 모델은 클라우드 환경에서 보안 책임이 **AWS**와 고객 사이에 나뉘어 있다는 것을 명시한 원칙입니다. AWS는 "클라우드 자체의 보안(**Security OF the Cloud**)"을 책임지는데, 여기에는 데이터센터의 물리적 보안, 하드웨어, 네트워크 인프라, 가상화 계층 등이 포함됩니다. 반면 고객은 "클라우드 내부의 보안(**Security IN the Cloud**)"을 책임지는데, 여기에는 OS 패치, 애플리케이션 보안 설정, 데이터 암호화, IAM 권한 관리, 보안 그룹 및 네트워크 ACL 설정 등이 포함됩니다. 서비스 모델(IaaS/PaaS/SaaS)에 따라 고객이 책임지는 범위가 달라지며, 관리형 서비스일수록 AWS가 더 많은 부분을 책임집니다. 실제 보안 사고의 상당수가 고객 측 설정 실수(예: 잘못된 S3 버킷 권한)에서 발생하기 때문에 면접에서 중요하게 다뤄집니다.

관련 개념 Security of/in the Cloud, IAM, 데이터 암호화, 보안 그룹, 컴플라이언스

Q9. AWS Lambda란 무엇이고 어떤 경우에 사용하나요? ★★

답안 **Lambda**는 AWS의 대표적인 서버리스(**FaaS**) 서비스로, 서버를 직접 프로비저닝하지 않고 이벤트가 발생했을 때 정의된 함수 코드를 실행해주는 컴퓨팅 서비스입니다. S3 파일 업로드, API Gateway를 통한 HTTP 요청, DynamoDB 데이터 변경, 스케줄(EventBridge) 등 다양한 이벤트 트리거에 반응해 실행되며, 실행 시간만큼만 과금되어 트래픽이 없을 때는 비용이 발생하지 않습니다. 이미지 리사이징, 실시간 데이터 처리, 간단한 API 백엔드 등 짧고 이벤트 기반인 작업에 적합하지만, 최대 실행 시간 제한과 콜드 스타트 지연이 있어 장시간 실행되는 배치 작업이나 상시 연결이 필요한 서비스에는 적합하지 않습니다.

관련 개념 FaaS, 이벤트 트리거, API Gateway, 콜드 스타트, EventBridge

Q10. CloudWatch는 어떤 역할을 하며 왜 중요한가요? ★★

답안 **CloudWatch**는 AWS 리소스와 애플리케이션의 모니터링 및 로깅을 담당하는 서비스로, EC2의 CPU/메모리 사용률, RDS의 커넥션 수, Lambda의 실행 시간 등 다양한 메트릭을 수집하고 시각화합니다. 특정 임계치를 초과하면 알람(**Alarm**)을 발생시켜 SNS를 통해 담당자에게 통지하거나, 오토스케일링과 연동해 자동으로 인스턴스를 증설·축소할 수 있습니다. 또한 **CloudWatch Logs**를 통해 애플리케이션 로그를 중앙에서 수집·검색할 수 있어 장애 발생 시 원인 분석에 활용됩니다. 인프라 운영에서 장애를 조기에 감지하고 자동 대응 체계를 구축하는 핵심 도구이기 때문에, 실무 면접에서는 "어떤 지표를 어떻게 모니터링할 것인지"를 함께 묻는 경우가 많습니다.

관련 개념 메트릭, 알람(Alarm), CloudWatch Logs, 오토스케일링 연동, SNS
