↑ 목록으로 ← 이전 단원 다음 단원 →

4단원. **AWS** 실습

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

Q1. EC2 인스턴스 생성 시 결정해야 할 주요 항목을 설명하세요.

★★★

답안 EC2 인스턴스 생성 시에는 먼저 OS와 기본 소프트웨어가 담긴 **AMI**를 선택하고, 워크로드 특성(CPU 집약적, 메모리 집약적, 범용 등)에 맞는 인스턴스 타입을 결정합니다. 이후 인스턴스가 위치할 **VPC**와 서브넷(퍼블릭 또는 프라이빗)을 지정하고, 트래픽 접근을 제어할 보안 그룹을 설정하며, SSH 접속에 사용할 키 페어를 생성하거나 선택합니다. 스토리지 항목에서는 **EBS** 볼륨의 크기와 타입(범용 SSD, 프로비저닝된 IOPS 등)을 결정하고, 필요시 초기 설정 스크립트를 자동 실행하는 **User Data**를 등록합니다. 마지막으로 인스턴스에 부여할 IAM 역할을 지정해 다른 AWS 서비스에 접근할 권한을 안전하게 위임합니다.

관련 개념 AMI, 키 페어, EBS, User Data, IAM 역할

Q2. 보안 그룹과 네트워크 **ACL(NACL)**의 차이를 설명하세요.

★★★

답안 보안 그룹은 인스턴스 단위(ENI 단위)로 동작하는 가상 방화벽으로 상태 저장 **(Stateful)** 방식이기 때문에, 인바운드 요청을 허용하면 그에 대한 응답 트래픽은 아웃바운드 규칙과 무관하게 자동으로 허용됩니다. 또한 허용(Allow) 규칙만 설정할

수 있고 거부(Deny) 규칙은 지정할 수 없습니다. 네트워크 **ACL**은 서브넷 단위로 동작하며 상태 비저장(**Stateless**) 방식이기 때문에 인바운드와 아웃바운드 규칙을 각각 명시적으로 설정해야 하고, 허용과 거부 규칙을 모두 지정할 수 있으며 규칙 번호 순서대로 평가됩니다. 실무에서는 보안 그룹으로 인스턴스 단위의 세밀한 접근 제어를 하고, NACL로 서브넷 단위의 넓은 범위의 차단(예: 특정 악성 IP 대역 전체 차단)을 보완적으로 사용합니다.

관련 개념 Stateful/Stateless, ENI, 서브넷 단위 제어, 규칙 우선순위, 인바운드/아웃바운드

> **Q3. VPC**에서 퍼블릭 서브넷과 프라이빗 서브넷을 설계하는 방법을 설명하세요. ★★★

답안 퍼블릭 서브넷은 라우팅 테이블에 인터넷 게이트웨이(**IGW**)로 향하는 경로(0.0.0.0/0 → IGW)가 설정되어 있어 외부 인터넷과 직접 통신이 가능한 서브넷으로, 로드밸런서나 배스천 호스트처럼 외부에서 접근이 필요한 리소스를 배치합니다. 프라이빗 서브넷은 IGW로 향하는 직접 경로가 없어 외부에서 직접 접근할 수 없는 서브넷으로, 데이터베이스나 내부 애플리케이션 서버처럼 보안이 중요한 리소스를 배치합니다. 프라이빗 서브넷의 리소스가 외부로 나가는 트래픽(예: 패키지 업데이트)이 필요할 경우, 퍼블릭 서브넷에 위치한 **NAT** 게이트웨이를 경유하도록 라우팅 테이블을 구성해 외부 요청은 가능하지만 외부에서의 인바운드 접근은 차단하는 구조로 설계합니다. 이러한 구조는 일반적으로 웹(퍼블릭)-앱(프라이빗)-DB(프라이빗)의 다계층 아키텍처로 확장됩니다.

관련 개념 인터넷 게이트웨이, NAT 게이트웨이, 라우팅 테이블, 배스천 호스트, 다계층 아키텍처

Q4. IAM 정책을 작성할 때 최소 권한 원칙을 어떻게 적용하나요? ★★★

답안 최소 권한 원칙은 사용자나 역할에게 업무 수행에 반드시 필요한 권한만 부여하고 그 이상은 허용하지 않는 보안 원칙입니다. 실무에서는 먼저 관리형 정책 중 광범위한 권한을 가진 `AdministratorAccess` 같은 정책 대신, 필요한 서비스와 액션만 명시한 사용자 지정(**Customer Managed**) 정책을 작성합니다. 정책 문서에서는 `Effect`(허용/거부), `Action`(허용할 API 동작), `Resource`(대상 리소스의 ARN)를 구체적으로 명시하며, 가능하다면 특정 리소스 ARN이나 조건(`Condition`, 예: 특정 IP 대역에서만 접근 허용)을 추가해 범위를 더욱 좁힙니다. 또한 정기적으로 IAM Access Analyzer 등을 통해 실제 사용되지 않는 과도한 권한을 점검하고 축소하는 것이 모범 사례입니다.

관련 개념 관리형 정책 vs 사용자 지정 정책, ARN, Condition 키, Access Analyzer

Q5. 오토스케일링 그룹(**ASG**)의 동작 원리를 설명하세요. ★★★

답안 오토스케일링 그룹(**ASG**)은 CloudWatch 지표(예: 평균 CPU 사용률)를 기준으로 **EC2** 인스턴스 수를 자동으로 증가시키거나 감소시키는 기능입니다. ASG는 최소 용량, 최대 용량, 원하는 용량(Desired Capacity)을 설정하며, 시작 템플릿(Launch Template)을 통해 새로 생성될 인스턴스의 AMI, 인스턴스 타입, 보안 그룹 등을 미리 정의해둡니다. 스케일링 정책은 CPU 사용률이 특정 임계치를 초과하면 인스턴스를 추가하는 동적 스케일링, 특정 시간대에 미리 용량을 조정하는 예약 스케일링, 목표 지표 값을 유지하도록 자동 조절하는 목표 추적 스케일링 등이 있습니다. ASG는 일반적으로 로드밸런서와 연동되어, 새로 생성된 인스턴스가 자동으로 대상 그룹에 등록되고 헬스체크를 통과해야 트래픽을 받도록 구성합니다.

관련 개념 Launch Template, 목표 추적 스케일링, Desired Capacity, 대상 그룹(Target Group), 쿨다운

> **Q6. ALB(Application Load Balancer)**와 오토스케일링을 연동하는 아키텍처를 설명하세요. ★★★

답안 일반적인 연동 구조는 사용자 요청이 **ALB**로 먼저 도착하고, ALB는 등록된 대상 그룹(**Target Group**) 내의 여러 EC2 인스턴스로 트래픽을 분산합니다. ALB는 주기적으로 각 인스턴스에 헬스체크 요청을 보내 응답이 정상인 인스턴스에만 트래픽을 전달하고, 비정상 인스턴스는 자동으로 대상에서 제외합니다. 이 대상 그룹은 오토스케일링 그룹(**ASG**)과 연결되어 있어서, ASG가 트래픽 증가에 따라 새 인스턴스를 생성하면 자동으로 대상 그룹에 등록되고, 인스턴스를 종료할 때도 자동으로 대상 그룹에서 제거됩니다. 이러한 구조를 통해 트래픽 변화에 유연하게 대응하면서도 특정 인스턴스 장애가 전체 서비스 장애로 이어지지 않는 고가용성 아키텍처를 구현할 수 있으며, 여러 AZ에 걸쳐 인스턴스를 분산 배치하면 AZ 장애에도 대응할 수 있습니다.

관련 개념 Target Group, 헬스체크, 크로스 존 로드밸런싱, Multi-AZ 배포

> **Q7.** 배스천 호스트(**Bastion Host**)란 무엇이며 왜 사용하나요? ★★

답안 배스천 호스트는 프라이빗 서브넷에 있는 서버들에 직접 접근할 수 없는 상황에서 안전하게 접속하기 위한 중계 서버로, 퍼블릭 서브넷에 위치해 외부에서 SSH나 RDP로 접속할 수 있는 유일한 진입점 역할을 합니다. 관리자는 먼저 배스천 호스트에 접속한 뒤, 그곳을 경유해 프라이빗 서브넷의 인스턴스에 접속함으로써 프라이빗 리소스를 외부에 직접 노출하지 않고도 관리할 수 있습니다. 보안을 강화하기 위해 배스천 호스트의 보안 그룹은 특정 관리자 IP 대역에서만 접근을 허용하도록 제한하는 것이 일반적이며, 최근에는 배스천 호스트를 별도로 운영하지 않고 **AWS Systems Manager Session Manager**를 이용해 SSH 포트를 아예 열지 않고도 안전하게 접속하는 방식이 권장되기도 합니다.

관련 개념 Session Manager, 점프 서버, SSH 터널링, 프라이빗 서브넷 접근 제어

Q8. **VPC** 피어링과 **VPC** 엔드포인트의 차이를 설명하세요. ★★

답안 **VPC** 피어링은 서로 다른 두 VPC 간에 프라이빗 네트워크 연결을 맺어 마치 같은 네트워크에 있는 것처럼 서로 통신할 수 있게 해주는 기능으로, 인터넷을 거치지 않고 VPC와 VPC를 직접 연결할 때 사용합니다. 다만 피어링은 전이적(transitive)이지 않아서 A-B, B-C가 피어링되어 있어도 A와 C는 직접 통신할 수 없다는 제약이 있습니다. **VPC** 엔드포인트는 VPC 내부에서 인터넷 게이트웨이나 NAT 게이트웨이를 거치지 않고 S3, DynamoDB 같은 AWS 서비스에 프라이빗하게 직접 접근할 수 있게 해주는 기능으로, 프라이빗 서브넷에서도 인터넷 경유 없이 AWS 서비스를 안전하게 이용할 수 있게 해줍니다. 두 기능 모두 트래픽을 인터넷에 노출시키지 않아 보안성과 지연시간 측면에서 이점이 있습니다.

관련 개념 전이적 라우팅 제약, Gateway 엔드포인트, Interface 엔드포인트, Transit Gateway

---

Q9. **EC2** 인스턴스에서 **EBS** 볼륨과 스냅샷을 활용한 백업 전략을 설명하세요. ★★

답안 **EBS(Elastic Block Store)**는 EC2 인스턴스에 연결되는 네트워크 기반 블록 스토리지로, 인스턴스와 독립적으로 존재하기 때문에 인스턴스가 종료되어도 데이터를 유지할 수 있습니다(설정에 따라 다름). 백업 전략의 핵심은 **EBS** 스냅샷으로, 특정 시점의 볼륨 상태를 S3에 증분 방식으로 저장하며 이후 스냅샷은 이전 스냅샷과의 변경분만 저장해 비용과 시간을 절약합니다. 스냅샷을 이용하면 동일한 볼륨을 다른 AZ나 리전에 복제해 새로운 인스턴스를 생성할 수 있어 재해복구나 환경 복제에 활용됩니다. 실무에서는 **AWS Backup**이나 수명주기 정책을 이용해 정기적인 스냅샷 생성과 오래된 스냅샷의 자동 삭제를 자동화하는 것이 일반적입니다.

관련 개념 증분 스냅샷, AWS Backup, 볼륨 복제, 리전 간 복제, 수명주기 정책

> **Q10. 3**계층(웹-앱-**DB**) 아키텍처를 **AWS**로 설계한다면 어떻게 구성하나요? ★★★

답안 먼저 사용자 트래픽을 받는 웹 계층은 퍼블릭 서브넷에 ALB를 배치하고, 그 뒤에 오토스케일링 그룹으로 관리되는 웹 서버 EC2 인스턴스를 여러 AZ에 걸쳐 배치합니다. 애플리케이션 계층은 프라이빗 서브넷에 위치시켜 외부에서 직접 접근할 수 없도록 하고, 웹 계층에서만 트래픽이 유입되도록 보안 그룹을 설정하며, 필요시 내부 로드밸런서로 트래픽을 분산합니다. 데이터베이스 계층은 더 깊은 프라이빗 서브넷에 RDS를 Multi-AZ로 구성해 배치하고, 애플리케이션 계층에서만 접근 가능하도록 보안 그룹을 제한합니다. 전체적으로 각 계층은 서로 다른 서브넷과 보안 그룹으로 격리되어 있으며, 외부에서 접근 가능한 것은 웹 계층뿐이라는 것이 이 아키텍처의 핵심 보안 설계 원칙입니다.

관련 개념 다계층 아키텍처, 서브넷 분리, 보안 그룹 체이닝, Multi-AZ RDS, 최소 노출 원칙
