

SAA-C03 오답 노트

기출 풀이 중 헷갈렸던 개념 정리 · 2026-08-28

1 EC2 컴퓨팅 요금 · 구매 모델

옵션	할인	약정	언제 쓰나 (키워드)
On-Demand	없음	없음	"예측 불가", "단기", "스파이크성", 약정 회피
Spot	최대 ~90%	없음	"중단돼도 됨", "내결함성", "배치", "스테이트리스", "유연한 시작/종료", dev/test + 비용 최우선
Reserved Instance	최대 ~72%	1년 / 3년	"24/7 상시", "예측 가능한 꾸준한 부하", "장기"
Savings Plans	최대 ~72%	1년 / 3년 (\$/h)	RI와 같은 상황인데 더 유연 (패밀리/리전/Lambda-Fargate 커버)
Dedicated Host	—	선택	"소켓/코어 기반 BYOL 라이선스", 물리 서버에 라이선스 묶임

RI vs Savings Plans

- RI — "이 타입(m5.large)을 1년 쓸게" → 특정 스펙에 묶임. Standard RI는 마켓플레이스 판매 가능.
- Compute Savings Plans — 가장 유연. EC2 + Fargate + Lambda, 리전+패밀리 무관.
- EC2 Instance Savings Plans — 특정 리전+패밀리 내로 한정, 대신 할인을 약간 큼.

판단 흐름 — 중단 OK & 비용 최우선 → Spot / 1년+ 꾸준 → RI-Savings Plans (Lambda-Fargate도면 Compute SP) / 소켓·코어 BYOL → Dedicated Host / 나머지 예측 불가·단기 → On-Demand

DB(RDS-ElastiCache-Redshift-OpenSearch)에도 Reserved Instance 개념 동일. DB에 "Spot"이 보이면 오답.

2 스토리지 큰 분류

유형	서비스	접근 방식
블록	EBS, 인스턴스 스토어	하나의 EC2에 디스크로 부착
파일	EFS, FSx 4종	여러 서버가 네트워크로 마운트 (NFS / SMB)
객체	S3, Glacier	HTTP API (키-값)

3 EBS 볼륨 타입 & Multi-Attach

타입	특징 / 용도
io1 / io2 (Provisioned IOPS SSD)	IOPS 직접 지정 → 볼륨 크기와 무관하게 일관·예측 가능한 저지연 . 비즈니스 크리티컬. Multi-Attach 지원 (io1/io2 only)
gp3 / gp2 (범용 SSD)	일반 워크로드 기본값. gp3가 신형(기본 3,000 IOPS). Multi-Attach 미지원
st1 (처리량 최적화 HDD)	처리량(MB/s) 최적화 → 빅데이터·로그 등 대용량 순차 . 랜덤 I/O·저지연엔 부적합. Multi-Attach 미지원
sc1 (Cold HDD)	가장 저렴, 접근 드문 대용량

"consistent, low-latency" → io1/io2 | **Multi-Attach**(같은 AZ 내 여러 Nitro 인스턴스 동시 연결) → io1/io2 + 클러스터 인식 파일시스템 필요

4 파일 스토리지 — EFS vs FSx

Amazon EFS

- **Linux 전용** (NFS), POSIX 호환
- 여러 AZ의 다수 EC2 동시 마운트, 용량 자동 무한 확장
- 키워드: "Linux", "다중 AZ 공유", "POSIX", "자동 확장"

Amazon FSx — 4종

종류	프로토콜 / OS	키워드
FSx for Windows File Server	SMB / Windows	"SMB" , "Windows 파일 공유", "Active Directory 통합"
FSx for Lustre	고성능 병렬 (Linux)	"HPC" , "머신러닝 학습", "S3 연동 고속 처리", 수백 GB/s
FSx for NetApp ONTAP	NFS + SMB + iSCSI	"온프레 NetApp", "NFS-SMB 둘 다", 중복제거·스냅샷
FSx for OpenZFS	NFS (Linux)	"온프레 ZFS 이전", ZFS 스냅샷·클론

SMB / Windows → FSx for Windows (EFS는 Linux만!) | NFS / Linux / 다중 AZ → EFS | ML · HPC → FSx for Lustre

5 S3 스토리지 클래스

클래스	가용성	검색 속도 / 용도
S3 Standard	3-AZ	ms 즉시. 자주 액세스
S3 Standard-IA	3-AZ	ms 즉시. 가용성·내구성 그대로 + 저장 단가 ↓ (검색 요금 있음). 30일+ 뜸하게
S3 One Zone-IA	1-AZ	ms 즉시. 저렴하지만 그 AZ 손상 시 데이터 손실. 재생성 가능한 데이터만
S3 Intelligent-Tiering	3-AZ	접근 패턴을 모를 때 . 오브젝트당 모니터링 수수료
Glacier Instant Retrieval	3-AZ	ms 즉시. 분기 1회 수준 접근
Glacier Flexible Retrieval	3-AZ	분~수시간
Glacier Deep Archive	3-AZ	복원 최대 12시간 . 최저가 아카이브

"즉시 액세스 + 가용성 그대로 + 비용 ↓" → Standard-IA. Glacier류-One Zone-IA는 여기서 탈락.
 접근 패턴 명확(예: 30일 경계) → Standard로 시작 후 라이프사이클로 IA 전환. **패턴 불명확** → Intelligent-Tiering.

라이프사이클 예시

- 0~180일 Standard → 180일 후 Standard-IA → 360일 후 Glacier Instant Retrieval(즉시 필요) → 5년 후 Deep Archive(감사자 12h 내 검색 = 느려도 됨)

6 S3 우발 삭제 방지 · Object Lock

버킷 우발 삭제 방지

- Versioning** — 덮어쓰기·삭제해도 이전 버전 보존
- MFA Delete** — 버전 영구 삭제 / 버전 관리 끄기에 추가 MFA 인증 요구 (Versioning과 짝)
- IAM 정책** — 버킷에 붙는 건 "버킷 정책". 사용자는 업로드·수정을 해야 하므로 권한 조이기가 목적 아님. 우발 삭제 방지의 직접 수단 X
- 읽기 전용 ACL** — 업로드·수정 막힘 → 요구사항 위반

WORM (일정 기간 삭제 금지) + 이후 자동 삭제

Object Lock(+ Versioning 필수) + 기본 보존 기간 + 라이프사이클 만료(expiration)
 "보호"는 라이프사이클이 아니라 **Object Lock**의 역할. 라이프사이클은 전환·만료만 함.

Object Lock 모드	의미
Governance	특정 IAM 권한 보유자는 우회(삭제) 가능
Compliance	루트 포함 누구도 잠금 기간 내 삭제·변경 불가 (되돌릴 수 없음)

Backup Vault Lock도 동일: "어떤 사용자도 N년간 삭제 불가" → **compliance 모드** (governance는 "any user" 조건 불충족)

스냅샷 우발 삭제 방지

- "권한 안 건드리고 최소 노력" → **EBS Snapshot Lock**. IAM Deny는 "권한 변경"이라 조건 위반. Recycle Bin은 삭제 자체를 막지 못함(복구만).

7 KMS 키 종류

키 종류	사용자 교체 제어	정책 제어	비용
AWS owned	X (안 보임)	X	무료
AWS managed (aws/서비스)	X (연 1회 고정)	X	무료 (사용료만)
Customer managed	✓	✓	키당 월 \$1 + 사용료
Customer managed (imported)	수동만	✓	동일

"키를 생성·교체·비활성화·정책을 내가 완전히 제어" → 무조건 **Customer managed key** (SSE-KMS). SSE-S3-AWS managed는 제어 불가.

8 데이터 전송 · 마이그레이션 수단

온라인 파일 / 객체

서비스	키워드
AWS DataSync	온프레 NFS/SMB/HDFS ↔ S3/EFS/FSx. 증분·스케줄·검증. "대량 + 지속/반복 동기화" , 에이전트 설치 OK
CLI <code>s3 sync</code> / <code>s3 cp</code>	TLS 기본. "소량(수십~수백 GB) + 일회성" , 명령 한 줄, 에이전트 없이
S3 Transfer Acceleration	CloudFront 엣지 경우 장거리 업로드 가속 . "전 세계 지사 → S3", "대륙 간"
S3 Multipart Upload	큰 객체 병렬 조각 업로드. "100MB~5TB 단일 객체"

오프라인 (Snow 패밀리)

서비스	키워드
Snowcone (~8TB)	소형·휴대, 엣지, 열악한 환경
Snowball Edge (~80TB)	"수십 TB~PB + 회선 부족/느림 + 기한 촉박"
Snowmobile (~100PB)	엑사바이트급, 데이터센터 통째로

판단 공식 — 인터넷 전송 시간 계산 → 며칠~몇 주면 Snowball, 몇 시간이면 온라인.

하이브리드 (온프레에서 계속 접근)

Storage Gateway 종류	키워드
S3 File Gateway	온프레 NFS/SMB 마운트 → 뒤는 S3. "앱은 그대로 파일 접근, 데이터는 S3에"
FSx File Gateway	SMB + 온프레 저지연 로컬 캐시
Volume Gateway	iSCSI 블록 볼륨, S3에 스냅샷 백업
Tape Gateway (VTL)	가상 테이프 → Glacier. "기존 백업 SW 테이프"

DataSync vs Storage Gateway — 옮기고 끝 = DataSync / 온프레에서 계속 쓰면서 = Storage Gateway

데이터베이스

서비스	키워드
AWS DMS	"최소 다운타임 DB 마이그레이션" , CDC로 소스 운영 유지
AWS SCT	이종 엔진 스키마·코드 변환 (Oracle → PostgreSQL). DMS와 짝
RDS 스냅샷 / read replica	같은 엔진 이전, 리전 간 DR

실시간 스트리밍

서비스	키워드
Kinesis Data Streams	실시간 버스, 소비자 직접 개발 , ms 지연, 재처리·순서. 샤드 관리
Kinesis Data Firehose	S3 / Redshift / OpenSearch로 자동 배달 (관리형, 코드 X). 버퍼링·재시도·변환. "최소 운영 부담"
Amazon MSK	관리형 Kafka. "이미 Kafka 씀"

전용 네트워크 경로

서비스	키워드
Direct Connect	전용 물리 회선(인터넷 우회). "일관된 저지연", "대량을 인터넷 영향 없이", "장기 하이브리드"

Site-to-Site VPN	인터넷 위 IPsec. "빠르게 구축", "임시/백업 경로", 저비용
DX + VPN	전용 회선 위에 암호화까지

9 네트워킹 · 엣지

API Gateway

- 프라이빗 VPC 리소스(프라이빗 서브넷 ECS 등)에 접근 → VPC Link (Private Integration) 필수. API Gateway는 VPC 밖 관리형 서비스라 보안 그룹을 못 붙임. (REST API는 VPC Link → NLB → 프라이빗 서브넷)
- 글로벌 분산 사용자 + 지연 감소 → Edge-optimized 엔드포인트 (CloudFront 엣지 자동 배치 → AWS 백본망)
- Regional = 특정 리전 서빙 / Private = VPC 내부 전용

CloudFront 프라이빗 콘텐츠

- Signed URLs — 개별 파일, 쿠키 미지원 클라이언트
- Signed cookies — 여러 파일, URL을 바꿀 수 없는 클라이언트

실시간 UDP/TCP 글로벌 + 자동 페일오버

- Global Accelerator + NLB. 정적 애니캐스트 IP, 네트워크 레벨 수 초 내 페일오버.
- CloudFront = HTTP 전용(UDP 불가) / ALB = L7(HTTP만) / Route 53 페일오버 = DNS 캐싱 때문에 느림

리전 근처 저지연 배치

서비스	위치 / 접근	용도
Local Zones	대도시(리전 밖) / 일반 인터넷	일반 앱의 지역 저지연, 규제 회피 (single-digit ms)
Wavelength	통신사 5G 엣지 / 5G 캐리어 망	모바일 5G 기기 초저지연 (AR/VR, 게임, 자율주행). 일반 인터넷 사용자 접근 X
Outposts	고객 데이터센터 / 사내망	데이터 레지던시, 온프레 통합
CloudFront	전 세계 엣지 / 일반 인터넷	콘텐츠 캐싱·전달 (앱 호스팅 X)

10 보안 · 거버넌스 서비스 역할

서비스	역할
AWS Config	리소스 구성 규정 준수 추적 + 자동 수정 (암호화 여부, 퍼블릭 접근 등). "미준수 리소스 식별 + 자동 교정"
Amazon Inspector	취약점 스캔 (CVE, 패치 누락, 네트워크 도달성)
Amazon Macie	S3 민감 데이터(PII) 발견·분류 (여권·카드 번호 등)
Amazon GuardDuty	위험 탐지 (악성 IP, 이상 API 호출, 크립토마이닝)
Security Hub	위 결과들 집계·대시보드

크로스 계정 접근(다른 AWS 계정 리소스) → IAM Role + trust policy + AssumeRole. 액세스 키를 저장하는 선택지는 거의 항상 오답.

비밀번호·자격 증명 자동 교체 → Secrets Manager (RDS 통합). Parameter Store는 교체 기능 없음(단순 저장).

루트 사용자 보안 → ① 액세스 키 삭제 ② MFA ③ 강력한 비밀번호. 루트는 IAM 그룹·정책 대상이 아님.

11 분석 서비스

- "S3에 있는 데이터를 즉시 SQL로 애드혹 분석" → Glue Crawler + Athena (서버리스). 인프라 0.
- 스트리밍 분석 → Kinesis / 대규모 반복 ETL → Glue Jobs:EMR
- Firehose = 목적지로 자동 배달(관리형, 코드 X) | Data Streams = 실시간 버스, 소비자 직접 개발
- Redshift = OLAP 데이터 웨어하우스 (OLTP:웹앱 성능과 무관 → 함정 오답)

12 DynamoDB 용량 모드 & 테이블 클래스

구분	선택 기준
Provisioned	부하 예측 가능·구준함 → RCU/WCU 지정 (가장 저렴). 간헐적·짧아도 provisioned + Auto Scaling
On-demand	부하 급변·예측 불가
Reserved Capacity	provisioned를 1~3년 상시 대량으로 → 선결제 할인. 주 몇 시간짜리엔 낭비
Standard 클래스	자주 액세스
Standard-IA 클래스	자주 안 읽는 대용량 (저장 단가 ↓, 읽기·쓰기 요금 ↑)

"온디맨드 모드 + RCU/WCU 지정" 같은 보기는 모순 설정 → 오답 (온디맨드는 용량 미지정)

13 자주 나오는 판단 패턴 요약

DB 옮기나?

```

|-- 예 -> DMS (+ 엔진 다르면 SCT)
|-- 아니오
  |-- 실시간 스트림?          -> Kinesis (적재만이면 Firehose)
  |-- 온프레미스에서 계속 접근? -> Storage Gateway
  |-- 옮기고 끝
    |-- 회선으로 며칠+ (수십 TB~) -> Snowball
    |-- 대량 파일, 반복 동기화     -> DataSync
    |-- 소량, 일회성               -> aws s3 sync / cp
    |-- 전 세계 -> S3 빠른 업로드  -> S3 Transfer Acceleration
  |-- 회선 자체 필요             -> Direct Connect(전용) / VPN(인터넷 위)
  
```

공유 파일 시스템?

```

|-- Windows / SMB          -> FSx for Windows File Server
|-- Linux / NFS 일반        -> EFS
|-- HPC / ML / 초고성능     -> FSx for Lustre
|-- NFS + SMB 동시          -> FSx for NetApp ONTAP
  
```

"코드 변경 최소 + 복원력 개선"

-> 엔진 유지 RDS Multi-AZ + ALB / Auto Scaling 웹 tier
(엔진 바꾸는 보기 = DynamoDB / Aurora 다른 엔진 -> 오답)

"신뢰성 / 가용성 최대화"

-> 모든 계층 이중화: Multi-AZ RDS + ALB + Multi-AZ ASG
(인스턴스 수 줄이기 / Spot 사용 보기 -> 오답)