* Acloudguru Test 1

- API Call log 를 확인하기 위해서는 Cloudtrail 을 씀
- S3-IA 와 S3 의 처리량, 지연시간은 동일함
- Life cycle 의 사용 목적
    - 일정기간 데이터를 업로드한 후 더이상 필요없을 경우
    - 일정기간 액세스되나 그 다음에는 보존 목적이 더 큰 데이터일 경우
    - 업로드에 실패한 multipart upload 나 만료된 객체 삭제가 필요한 경우
- CloudWatch 의 default 수집주기는 5 분이지만, 최소 1 분까지 가능함
- S3 는 Redirect Website 를 지원함
- S3 는 Multi part uploads 를 통해 S3 Transfer Acceleration 이 가능함
- AWS 암호화 방식
    - 서버측 암호화
        - SSE-S3 : S3 의 고유한 키로 암호화되며 주기적으로 마스터키를 바꾸어 사용
        - SSE-KMS : AWS KMS 관리형 키를 통한 서버측 암호화방식으로 키가 사용된 때와 사용 주체에 대한 감사 추적이 가능함
        - SSE-C : 고객이 제공한 암호화 키로 서버측 암호화를 실시함, S3 는 제공된 암호화 키를 저장하지 않지만, HMAC 값을 저장하여 위/변조 여부를 검증함, 암호화 키를 손실하면 객체를 손실
            - 객체 데이터만 암호화
            - 암호화 키에 대한 제어권을 유지하고 싶다면 사용하는 것이 좋음
        - SSE-S3 vs SSE-KMS : SSE-S3 는 마스터키를 AWS 가 관리하고, KMS 는 데이터 키를 AWS 가 관리하지만, 고객 마스터키는 사용자가 관리해야 하며, 사용 감시 및 추적이 가능함
    - 클라이언트측 암호화
        - CMK 를 사용하여 암호화
        - 클라이언트의 마스터 키를 사용하여 암호화, 이 경우 마스터키를 클라이언트가 관리해야함
- Glacier 에서 오브젝트를 복원할 때는 S3 API 혹은 AWS Console 을 이용해야함
- EC2 의 SLA 는 99.95%
- S3-IA 의 오브젝트 최소 사이즈는 128KB
- S3 멀티파트 업로드 파트의 크기는 5MB ~ 5GB(오브젝트 최대 크기는 5TB)
- S3 에 특정 오브젝트가 반드시 CRR 이 되어야 한다면 그 오브젝트의 subset 에만 CRR 를 허용해 줄 수 있음(소스 설정 가능)
- CLB 는 IPv6 를 제공함

- S3 는 HTTPS 를 이용하여 SSL, HTTP Endpoint 에 접근할 수 있음
- Versioning 이 활성화된 Bucket 은 소유자만이 지울 수 있음
- 계정당 S3 Buckt 은 기본적으로 최대 100 개까지 생성 가능
- CloudWatch 의 경우 최대 2 주까지 보관
- S3 에 데이터를 보관할 때는 KMS 보단 SSE-S3 가 훨씬 안전함
- CRR 은 S3 오브젝트의 Metadata 와 ACL 을 복제함
- S3 는 IPv6 를 지원함
- Glacier 에서 데이터를 가져오는데 걸리는 시간은 3~5 시간임
- S3 스탠다드 클래스의 최소 사이즈는 1 Byte

* Acloudguru Test 2
- Multi AZ 가 활성화된 상태에서는 Primary RDS 가 아닌 Standby 가 Backup 실시
- workload 가 중단되거나 재시작되어도 되는 서비스일 경우(단기간에 폭발적인 사용량이 필요한 경우), Spot instance 를 사용하는 것이 좋음
- 같은 리전 내에서 S3 - > EC2 데이터 이동시 요금이 따로 없음
- RDS instanace 는 업그레이드시 일시적으로 사용불가능하며 이는 몇분간 지속됨(단일 AZ 의 경우)
- EMR 은 Root level access 가 가능함
- S3 Static hosting 시 버킷이름.리전.amazonaws.com 순으로 domain name 을 설정해야함
- 기존재하는 DB 를 암호화하는 설정은 존재하지 않으므로 DB 를 새로 생성하여 migration 해야함
- infrastructure 를 다른 리전에 복사 및 배포하고 싶을 경우, Cloudformation 을 사용해야함
- Storage Gateway with Cached Volume 은 자주 사용되는 데이터만 Cache 하고 나머지 데이터를 S3 에 저장함
- Reserved instance 를 사용하다가 나중에 다시 사용해야할 경우, 스냅샷을 떠놓고 종료해야 함
- S3 RRS 는 99.99%의 가용성과 내구성을 보장하며, 재생성이 쉬운 데이터를 보관함
- 각 서비스들의 설정 변경을 감독, 관리하고 싶은 경우 AWS Config 를 사용하면 됨
- Read Replica, Elastic Cache 까지 썼음에도 병목현상이 발생한다면 DB 파티셔닝 후 다수의 DB instance 로 분산하는 것이 좋음
- Read Replica 는 동기식 복제를 지원하지 않음(Asynchronous)
*** Ephemeral : 단명하는, 짧은
- RDS 가 Standby Replica 로 Failover 되는 요건 3 가지 : Compute Unit fail, 네트워크 연결 끊김, AZ 가용성 상실

- EBS SSD 볼륨은 1GiB ~ 16TiB
- Read Replica 의 Multi-AZ 복사는 불가능
- RDS 가 삭제될 때, automatic backup 은 자동으로 삭제되며, final snapshot 이 생성되어 남음(설정을 활성화했을 경우)
- EC2 메타 데이터 얻는 법 : curl http://169.254.169.254/latest/meta-data/public-hostname
- Read Replica 는 MySQL, PostgreSQL, MariaDB, Aurora, Oracle 서비스만 가능(MPMAO)
- Multi-AZ RDS Standby 에서는 동기식 복제를 지원함

* Acloudguru Test 3
- AWS Migration Service 를 이용할 경우, 동시에 Migration 가능한 VM 의 갯수는 50 개
- S3 의 read-after-wirte consistency 는 new object 에만 해당함(PUTS and DELETE 는 eventual consistency)
- VPC Peering 은 Edge-to-Edge routing 이 불가능(중간에서 양쪽의 VPC 를 연결하여 통신케 하는 것이 불가능)
- Autoscaling 사용 중 특정 시간에 사용량이 급증하는 경우 Proactive cyclic scaling 이 적절
- CloudHSM 은 SSL offload 를 목적으로 사용하므로 Network Latency 를 최소화하기 위해 EC2 주변에 두는 것이 좋음
    - KMS 대신 CloudHSM 을 써야하는 경우 : VPC 고성능 암호화가 필요한 경우, 키가 사용자의 독점적 제어 하에 다른 하드웨어 내에 저장되어있음, 애플리케이션과 통합되어있음
- S3 업로드시 edge location 에 직접 쓰는 것이 가능(Transfer Acceleration)
- SQS 는 최소 한번 메시지를 전달하지만 순서를 보장하지 못 하고, 중복전송을 할 가능성이 있음
- IAM 을 이용해 EC2 의 Root Account 에 접근하는 것을 막을 수 없음(Root account 는 모든 서비스에 접근 가능)
- VPC Peering 이 인접 VPC 에 대한 Routing Table 필요
- VPC Peering 은 두 VPC 간 두 개의 Peering 을 생성할 수 없으며, 다른 Region 의 VPC 이 가능하고, CIDR block 이 충돌하는 경우 사용 불가능
- Cloudtrail 은 계정의 활동을 감시,추적하는 기능을 함(+API)
- SQS 의 긴폴링과 짧은 폴링에 대한 차이점을 알아야 함
    - 짧은 폴링 구성은 Receive Message Wait Time 을 0 초로 만드는 것임
    - 짧은 폴링을 쓸 경우, 처리되지 못하는 메시지가 발생할 수 있음

    - SQS Standard 는 FIFO 를 보장하지 않음
- EC2 instance Type 선택시, I/O Operation 갯수와 메모리 사용량을 고려해야함
- EC2 를 껐다 켜도 Elastic IP 는 떨어지지 않음
- S3 Object 의 최소 사이즈는 0bytes 임(즉 빈 파일을 올릴 수 있음)
- Well Architected Framework 란 AWS 의 실례에 얼마나 부합하는가임
- SQS 메시지의 표시되는 시간이 끝나면 다른 인스턴스에 의해 활용가능해짐
- AWS 의 Well Architected Framework 의 구성요소는
보안,신뢰성,성능,비용최적화임(가용성은 없음)
- EBS 의 스냅샷은 S3 에 저장되기 때문에 안전함. 굳이 Glacier 로 옮길 필요없이
스냅샷을 자주 생성해주는 것이 좋음
- Auto Scaling 은 순간적 트래픽을 감당하기 위한 솔루션이 아님
- EFS 를 활성화하기 위해 EC2 와 EFS 의 Security group 에 포트를 열고, 리눅스에
chmod 명령어를 실행하여 권한을 줌

* 추가 테스트 1
- Autoscaling 생성 후 '예악된 작업'에서 예악된 시간에 정책 적용 가능
- DB 의 접근을 제어하고 싶을 땐 DB 에 IAM 을 적용하면 가능
- 사용가능 예산을 설정하고 초과시 알람을 보내는 서비스는 AWS Budget
- Error: No supported authentication methods available
    - 이 에러가 뜰 경우, 로그인시 ID 와 private key 를 확인해야 함
- Cloudwatch 의 기본 수집시간은 5 분이지만, 확장모니터링을 통해 1 분까지 가능
- Lambda 는 기본적으로 암호화를 수행하지 않으므로 Lambda 생성시 KMS 를 이용하여
암호화하여야 함
- RDS 와 Dynamo DB
    - Schema 가 flexible 한 경우 RDS 를 사용
    - Scale up/down 은 RDS 가 아닌 Dynamo DB 가능
    - RDS 는 다음과 같은 이유로 확장성(Scale up/down)이 떨어짐
        - 데이터를 정상화하고 디스크에 쓰려면 여러 개의 쿼리가 필요한 여러
테이블에 저장한다.
        - 일반적으로 ACID 준수 트랜잭션 시스템의 성능 비용을 발생시킨다.
        - 고가의 조인을 이용하여 조회 결과의 필요한 뷰를 재조립한다.
    - DynamoDB is not a totally schemaless database since the very
definition of a schema is just the model or structure of your data.
    -
https://docs.aws.amazon.com/ko_kr/amazondynamodb/latest/developerguide/bp
-general-nosql-design.html
    - RDBMS 의 경우, 세부적인 구현이나 성능을 걱정하지 않고 유연성을 목적으로
설계. 일반적으로 쿼리 최적화가 스키마 설계에 영향을 미치지 않지만, 정규화가 아주 중요

- DynamoDB 의 경우, 가장 중요하고 범용적인 쿼리를 가능한 빠르고 저렴하게 수행할 수 있도록 스키마를 설계. 사용자의 데이터 구조는 사용자 비즈니스 사용 사례의 특정 요구 사항에 적합

- 온프레미스에서 사용하던 고유의 IP 를 가져오기 위해서는 ROA(Route Origin Authorization)을 사용하여 Amazon ASN 이 해당 주소를 광고하도록 허용하게 함

- Dynamo DB 의 Cache 역할은 DAX 가 맡음

- EBS 의 성능이 내결함성보다 더 중요할 경우 RAID 0 을 사용함

- AWS 내부가 아닌 외부에서 AWS 에 access 할 수 있도록 하기 위해 SAML(SSO)을 연동하면 됨

- RDS 내 보다 면밀한 모니터링을 위해서는 Enhanced Monitoring 을 하는 것이 좋음

- 실행 후에도 SQS 에 메시지가 남아 있다면 메시지를 지우지 않은 것

- Redshift 에서 쿼리 큐를 정의하는 방식은 WLM(Workload management)가 있음

- Redshift 에서 클러스터와 VPC 외부의 COPY, UNLOAD 트래픽을 모니터링하기 위해서는 Enhanced VPC routing 을 사용해야함

- API Gateway 에는 트래픽 쏠림으로 인한 병목현상을 막아주는 Throttling Limit 기능이 존재

- Memory utilization, disk swap utilization, disk space utilization, page file utilization, log collection 은 custom monitoring 항목

  - EC2 에 에이전트를 설치하고 해당 항목을 감시해야 함

- ELB 를 쓰지 않으려면, EC2 에 공인 IP 를 할당하고 스크립트로 헬스체크를 하고 Failover 하는 것이 좋음

- Cloudfront 의 Signed URL

  - RTMP 를 사용할 경우 Signed Cookie 를 지원하지 않으므로 사용
  - 개별 파일에 대한 액세스를 제공하려는 경우
  - 클라이언트가 Cookie 를 지원하지 않을 경우

- Cloudfront 의 Signed Cookie

  - HLS 형식의 비디오 파일 전체 또는 웹 사이트의 구독자 영역에 있는 파일 전체 등 제한된 파일 여러 개에 대한 액세스 권한을 제공하려는 경우
  - 현재의 URL 을 변경하고 싶지 않은 경우

- EBS 스냅샷이 진행되는 동안 EBS 의 읽기 및 쓰기는 영향을 받지 않음

- Autoscaling 에서 종료되는 순서

  - 인스턴스가 가장 많은 가용영역에서 종료
    - 종료할 인스턴스를 결정하고 종료 중인 온디맨드 또는 스팟 인스턴스의 할당 전략, 현재 선택된 인스턴스 유형, 최저가 N 개 스팟 풀 배포에 나머지 인스턴스를 맞춤
  - 오래된 시작 1.구성 2. 템플릿을 쓰는 인스턴스 중에서 종료

- 다음 결제 시한이 가장 가까워오는 인스턴스 중에서 종료
- 온프레미스에서 이미 메시지 큐 서비스를 사용하고 있다면 MQ 로 넘어가는 것이 유리함
- 오로라에는 Endpoint 가 있어 트래픽을 분산할 수 있음
- 애플리케이션이 EBS 에 저장할 데이터 각각을 암호화하는 것은 불가능하므로 KMS 를 사용하여 암호화하여야 함

* 추가 테스트 2(EBS)
- Provisioned IOPS SSD 는 IOPS 중심이므로 Input/Output 이 적은 경우에서는 적합하지 않음(Cold HDD 가 더 적합)
- Cold HDD 는 입출력 빈도가 적은 대규모 스토리지의 볼륨에 적합
- Lambda 의 배포방법(기존 Lambda 함수에서 새로운 Lambda 함수로)
    - Canary : 트래픽이 2 번에 걸쳐 이동하여 2 번째 이동에서 이동할 트래픽 비율, 간격을 정할 수 있음
    - Linear : 트래픽을 동일한 비율로 이동시키며 증분간 간격이 돌이하고, 비율과 간격시간을 정할 수 있음
    - All-at-once : 한 번에 이동
- RDS 가 Failover 되는 4 가지 경우
    - AZ 가용성 상실
    - 네트워크 연결 끊김
    - 컴퓨팅 유닛 실패
    - 스토리지 Fail
- AWS IoT Core
    - AWS 에 연결된 디바이스들이 AWS Service 와 쉽게 상호작용하도록 돕는 서비스
- EC2 에 호스팅된 Database(Raid array)를 백업시 다운타임을 최소화하는 방법
    - 모든 RAID array 로 쓰기 작동을 멈춤
    - 모든 cache 를 disk 에 flush 함
    - EC2 가 RAID 에 쓰기작업을 하지 않는지 확인
    - RAID 에 대한 모든 디스크 관련 활동을 중지하는 단계를 수행한 후 스냅샷 생성
- 기본적으로 data at rest 를 암호화하는 솔루션은 Storage Gateway 와 Glacier
- PFS 가 지원되는 솔루션은 Cloudfront 와 ELB
- Internet Gateway 는 VPC 와 연결되며 라우팅은 서브넷과 연관되어있음
- DAX 는 Cache 이므로 Dynamo DB 의 읽기 성능과 관련이 있음
- 다른 서브넷간의 통신을 확인하려면 ACL,Security Group 을 확인해야 함
- SQS 의 메시지 보관 최대 일수는 14 일임(Application crash = 앱이 멈춤으로 해석하자)

- 앱의 문제로 메시지가 13 일간 쌓여있다하더라도 앱이 다시 시작만 한다면 바로 처리 가능
- AWS 의 책임 범위(보안)는 Facility, underlying network infrastructure, Phsycial security of hardware, virtualization infrastructure
- EBS 의 특징
    - EBS 를 생성할 경우, 다른 AZ 가 아닌 해당 AZ 에만 자동으로 복제됨
    - EBS 는 해당 AZ 에만 어느 EC2 든 연결할 수 있음
    - 서비스 사용중인 상태에서 volume type(gp2, io1, standard), size, IOPS 를 바꿀 수 있음
    - EBS 스냅샷은 S3 에 저장됨
- API Gateway 는 받거나 처리한 양만큼은 요금을 지불하면 됨
- SNI(Server Name Indication)
    - 여러 도메인을 하나의 IP 주소로 연결하는 TLS 의 확장 표준 중 하나(인증서에서 사용하는 방식)
    - 이 SNI 를 사용하게 되면 하나의 웹서버에서 여러 도메인의 웹사이트를 서비스하는 경우에도 인증서를 사용한 HTTPS 활성화가 가능
    - AWS 에서는 Application Load balancer 와 Cloudfront 사용 가능
- S3 Static web hosting 을 Route 53 에 연결하기 위해서는 둘의 이름이 같고 등록된 도메인이어야 함
- AWS 의 decoupled Architecture 기술은 SQS 와 SWF, SNS, SES
- ENI 의 'warm attach'는 이미 실행중인 인스턴스에 ENI 를 붙일 때 나타남
- SQS queue 에서 메시지를 실행하기만 하고 지우지 않으면 그 메시지가 queue 로 돌아가 다시 실행됨
- S3 에서 사용 가능한 Event Notification Service 는 SQS, SNS, Lambda
- BLOB Data 는 크므로 DynamoDB 에 적합하지 않으며, 큰 메타 데이터는 S3 에 저장하고 작은 메타 데이터는 DynamoDB 에 저장하는 게 좋음
- 데이터가 80TB 가 넘을 땐 Snow ball 이 아닌 Snowball Edge 를 사용해야 함
- Cognito 는 AWS Resource 에 대한 접근이 아닌 유저 인증에 사용되는 서비스이며, 임시 권한을 주는 서비스는 STS 임
- AWS SSO 가 STS 를 이용하여 권한을 발급함
- EBS volume 의 백업을 자동화하기 위해서는 DLM(Data Lifecycle Manager)를 쓰는 것이 좋음
- Autoscaling cool down 정책
    - scaling action 이 발동되기 전에는 launch 나 termination 을 하지 않음
    - 기본값은 300 초임
    - cool down 은 scale out 후 발동되는 것

- EC2 의 경우 Region 당 20 개가 한계이며 별도의 요청이 있으면 그 이상의 생성이 가능
- EBS 의 경우 오로지 Single AZ 의 다수의 Facility 에 중복 저장됨
- S3 에 데이터를 보내기 전에 KMS 나 자체 암호화방식을 통해 암호화해야 함
- datawarehouse 로서 기능하는 S3 서비스는 Glacier
- AWS 에서의 DR scenario 로 Pilot light 가 사용됨
- 확장성과 탄력성을 위해서는 ELB 와 Route 53(Weighted Routing Policy)를 사용하는 것이 바람직
- RDS Failover 도 CNAME 이 Standby 로 이동
- SQS 와 SNS 는 비동기적인 Function call 은 지원하지 않음
- Geolocation routing 은 사용자의 지역을 기반으로 Routing 해주는 Route 53 의 기능

* 추가 테스트 3(Storage)
- non-default subnet 은 public ipv4, DNS hostname 을 받지 않음
- aws appsync 는 데이터 기반의 웹 및 모바일 애플리케이션을 빌드하거나 빌드하기를 원하나 실시간 업데이트와 오프라인 작업이 필요할 경우 유용
- IAM Group 에 새로운 정책을 추가하고 싶을 경우 그룹을 새로 만들고 유저를 추가한 후 해당 그룹에 정책을 적용하는 것이 좋음
- EC2 가 인터넷에 접근이 되지 않을 경우 두 가지를 살펴야 함
    - EIP or Public IP 를 갖고 있는지
    - 라우팅 테이블이 제대로 되어있는지
- Kinesis Data Firehose : 스트리밍 데이터를 S3, Redshift, Elasticsearch Service 등의 대상으로 전송하기 위한 관리형 서비스(전송 전문 서비스)
- SWF 에서 Worker 는 작업을 받아 처리하고 결과를 반환하며, Decider 는 여러 작업의 조정을 제어하는 프로그램임
- EC2 Placement Group
    - 클러스터 : 인스턴스를 가용 영역 안에 서로 근접하게 패킹하여 지연시간을 낮춤
    - 분산 : 인스턴스 그룹을 다른 기본 하드웨어로 분산하여 상호 오류를 줄임
- Redshift 는 열단위 데이터 처리와 데이터 분석을 통한 Reporting 이 가능함
- Data in transit 은 SSL 혹은 client-side encryption 을 통해 가능하며, Data at rest 는 SSE-S3,SSE-KMS,SSE-C and CMK,Client master key 를 통해 가능
- EC2 재부팅시 변화
    - EC2 는 physical host computer 를 가지고 있으며, EC2 가 멈출 경우 다른 host computer 로 이동함
    - ENI 와 Elastic IP 는 떨어지지 않으며 변화 없음
    - 요금은 running, stopping(최대절전모드로) 상태로 변환중인 경우에만 청구

- 예약 인스턴스의 경우, 'terminated' 상태여도 요금이 부과됨
- Glacier 에서 신속한 검색이 필요할 경우, Expeidted Retrieval 을 사용한 후 , provisioned retrieval capacity 를 사용하면 검색용량이 보장됨
- Lambda monitoring metric
    - Invocations - 5 분 기간 동안 함수가 호출된 횟수
    - Duration - 평균, 최소, 최대 실행 시간
    - 오류 수 및 성공률(%) - 오류 수 및 오류 없이 완료된 실행의 비율
    - Throttles - 동시 사용자 한도로 인해 실행에 실패한 횟수
    - IteratorAge - 스트림 이벤트 소스에서 Lambda 가 배치의 마지막 항목을 받아 함수를 호출했을 때 해당 항목의 수명
    - DeadLetterErrors - Lambda 가 배달 못한 편지 대기열에 쓰려고 시도했으나 실패한 이벤트 수
- VPC Peering 의 기능 중 다음 2 가지는 불가능함
    - Transit Gateway : A VPC 가 Peering 된 B VPC 를 통해 C VPC 로 갈 수 없음
    - Edge to Edge Routing : Peering 을 통해 다른 서비스로의 이동이 불가능함
- 이미 생성된 Autoscaling 의 시작구성은 변경할 수 없음
- Active-Standby 구성은 Primary Service 와 Secondary Service 를 분할하여 Primary 장애시 Secondary 로 넘어갈 수 있도록 할 때 사용해야 함
- Autoscaling 에서 설정한 EC2 갯수의 한도에 도달할 경우 더 이상 EC2 를 생성하지 않음
- ElastiCache 는 쿼리 결과를 캐싱함으로써 효율을 향상시킴
- EC2 병목현상의 경우, 충분한 수의 ENI or IP 가 할당되지 않았거나 subnet 을 분산시키지 않았을 경우임
- VPC 내 IP 대역은 /16 ~ /28 사이이며, 새로운 서브넷을 생성하면 main route table 에 연계됨(172.16.0.0/16)

* 추가 테스트 4(Storage)
- S3 에서 모든 액세스 요청에 대한 자세한 정보를 확인하고 싶다면 Server Access Log 를 사용 가능
- Cloudwatch 는 메모리 사용 관련 지표가 없으므로 인스턴스 내 스크립트를 통해 지표를 생성하고 Cloudwatch 로 보내야 함
- Elastic MAP Reduce 의 정의
- Stopped EC2 의 EBS Volume 은 요금 부과됨
- batch 는 다수의 batch computing job 을 처리하기 위한 서비스

- AWS Step function 은 patch management, infrastructure selection, and data synchronization 와 같은 Serverless
  Serverless Service 를 자동화시키는 서비스
- Cloudformation 은 AWS infrastructure 의 Versioning, Provisioning, modeling 을 가능케 함
- Flow log 는 특정 Instance 에 사용될 수 없음
- S3 Select : 버킷 내 오브젝트의 데이터 처리 및 분석을 돕는 툴
- Athena : S3 의 데이터를 쿼리하기 위한 서비스
- Redshift Spectrum : S3 의 exabyte 급 데이터 처리를 가능하게 함
- Magnetic Volume 은 접근 빈도가 적고 비용이 적게 들어야 하는 워크로드에 적합
- Provisioned IOPS SSD 는 영구적이고 지연시간이 낮은 퍼포먼스가 필요할 경우 적합
- Dynamo DB 에 과부하가 발생하면 Dynamo DB Autoscaling 을 사용하면 가능함
- Redshift 의 가용성을 높이기 위해서는 cross-region snapshot copy 를 활성화하면 됨
- DynamoDB Stream 과 Lambda 를 통합하여 table activity 를 감지한 후 Lamabda 를 트리거할 수 있음
- SQS 의 중복문제를 궁극적으로 해결하고 싶을 경우, SWF 를 쓰는 것이 좋음
- RDS 가 Failover 되어 도메인이 변경될 경우, Route 53 내에서 바뀌는 것은 CNAME 임
- 확장모니터링의 경우, 인스턴스 내 에이전트에서 정보를 받기 때문에 메모리 관련 정보를 얻음
    - RDS child process, OS Process 확인 가능
- SSL/TLS 인증서를 안전하게 import 할 수 있게 도와주는 서비스는 ACM, IAM cert store
- S3 static host 의 경우, 버킷이름.s3-website-ap-지역.amazonaws.com
- CloudTrail 은 AWS 서비스들의 API Call log 를 확인함
- volume check 가 insufficient-data 일 경우, 상태 체크가 진행 중이기 때문
- EBS 스토리지는 'Low-Latency access'가 가능
- CLB 에서 기존 연결이 열려 있는 상태에서 등록 취소 중이거나 비정상 상태인 인스턴스로의 요청 전송을 중지하려면 Connection draining 을 써야함

* 추가 테스트 5(EBS, Storage, EC2)
- Kinesis Stream 을 통해 데이터를 전송할 수 있는 서비스는 S3, Dynamo DB, Redshfit, EMR, Kinesis Firehose
- AWS Glue : 관리형 ETL 을 제공하며, 데이터 카탈로그를 통해 데이터를 자동으로 프로파일링하고 ETL 코드를 추천하여 소스 데이터를 대상 스키마로 변환함

- Management Console 을 통해 Glacier 로 직접 업로드하는 것은 불가능
- Spot Instance 는 사용 후 첫 1 시간 이내에 AWS 에 의해 종료되면 요금을 부과하지 않고, 그 이후에 AWS 에 의해 종료되면 초단위까지 부과됨
- Trusted Advisor 는 비용 최적화, 성능, 보안, 내결함성, 서비스 한도 등을 체크하여 사용자에게 알려줌
- Auto Scaling 에서 Cloudwatch 와 같은 alarm 값을 이용하여 scale up/down 하는 것은 Step 과 Simple
    - Target 은 그룹의 평균 CPU 사용률, 평균 네트워크 입/출력, 대상그룹 LB 요청 갯수를 기준으로 삼음
    - 일련의 조정 과정(set of scaling adjustment)는 Step Scaling 이 되어야 함
- S3 - client 암호화는 KMS 를 이용한 암호화 혹은 사용자의 마스터키로 암호화해야 함
- 지속적인 IOPS 성능을 요구하는 경우(잠깐이 아닌) Provisioned SSD EBS 가 나음
- EBS 를 암호화하면 다음 4 가지가 적용됨
    - EBS 와 Instance 사이의 데이터 암호화
    - 이 EBS 에서 생성된 스냅샷 암호화
    - 그 스냅샷을 통해 생성한 EBS
    - EBS 내부 데이터
- Schema Conversion Tool 을 사용하여 소스 스키마를 타켓 DB 의 스키마로 변형한 후, Database Migration Service 로 데이터 변형 가능
- SQS 내에서 지워지지 않은 메시지로 인해 App 이 충돌나는 경우는 그 메시지를 처리했던 EC2 가 아닌 다른 EC2 가 처리해서 그런 경우(Visibility timeout 이후)
- 비밀 액세스 키와 액세스 키 ID 는 API 호출시 사용되며, 콘솔에 접속하고자 할 때는 암호를 제공하고 암호를 시스템 관리자에게 제공해야 함
- Aurora Failover
    - Read Replica 가 있는 경우 : CNAME 이 정상 복제본을 가리키도록 변경되며, 해당 복제본이 승격됨
    - Read Replica 가 없는 경우 : 동일한 AZ 에 새 인스턴스를 하나 생성시도, 생성이 어려운 경우 다른 AZ 에 생성 시도
- CloudHSM 은 키 또는 자격 증명에 대한 액세스 권한을 가지지 않으므로 자격 증명을 분실할 경우 키 복구 불가
- AMI 를 생성 및 다른 Region 에 옮길 때 IAM 을 적용할 수 없음
- Cloudtrail 은 기본적으로 S3-SSE 를 이용하여 로그 파일을 암호화함
- https://docs.aws.amazon.com/ko_kr/AWSEC2/latest/UserGuide/EBSVolumeTypes.html#EBSVolumeTypes_gp2(볼륨 타입)

- RDS 의 설정을 수정해야 할 경우 Parameter Group 사용
- EBS 는 S3 의 Client Encryption 과 마찬가지로 KMS(CMK, 사용자 마스터 키)를 사용하여 암호화함
- API Gateway 는 오로지 HTTPS endpoints 만을 게시함
- https://docs.aws.amazon.com/ko_kr/AmazonS3/latest/dev/lifecycle-transition-general-considerations.html (S3 수명주기)
    - Standard 에서 IA, One ZONE_IA 로 가려면 30 일을 기다려야 함
- EBS 의 스냅샷의 경우, 하나의 스냅샷을 유지하면서 변경된 부분만 증분함(하나의 스냅샷만이 유지됨)
- 예약 인스턴스의 경우, 비용을 아끼려면 마켓플레이스에 팔거나 인스턴스를 종료시켜야 함

* 추가 테스트 6 (RDS, IAM, EC2)
- Redis 는 AUTH 커맨드를 통해 사용자에게 비밀번호를 요구한 후 Redis 명령어를 사용할 수 있게 할 수 있음
  (비밀번호를 요구하기 위해서는 --auth-token parameter 를 포함시켜야 함)
- 람다의 timeout 은 15 분이 최대
- CRR 의 조건
    - Versioning 이 활성화되어있어야 함
    - Source 와 Destination 가 다른 Region 이어야 함
    - S3 가 오브젝트를 복사할 권한이 있어야 함
- EIP 는 다음과 같은 경우 과금되지 않음
    - EC2 에 연결되어있는 경우
    - 그 EC2 가 running 인 경우
    - 하나의 EIP 만 연결되어있는 경우
- VPC 는 멀티캐스트 혹은 브로드캐스트를 지원하지 않음
- AWS Organization 은 트리구조로 되어 있으며 여러 조직의 여러 계정을 관리할 수 있음
    - 그룹을 만들고 계정 생성을 자동화하고 해당 그룹에 정책을 적용/관리할 수 있음
    - 여러 계정의 서비스 사용을 중앙에서 제어하는 SCP(Service Control Policies) 사용가능
- Cache-Control max-age 가 0 이면 캐시되는 시간이 없어 원본 서버로 감
- Public dataset 은 무료
- ECS 는 웹서버 배포를 자동으로 하지 않음(Elastic Beanstalk 가 자동으로 수행)
- IPv6 송신 전용 게이트웨이는 Egress-only Internet gateway
- Cloudformation 에서는 Resource 섹션만 필수 섹션임

- 모바일 앱과 같은 외부 어플이 AWS 서비스를 요청해야할 경우 Access Key 를 전달하는 것보다 Web Identity Federation 을 써야함
- SAML 2.0 연동은 SSO 을 이용하여 조직의 모든 사용자에게 IAM 사용자를 생성하지 않고도 사용자가 AWS 콘솔에 로그인하거나 API 작업을 호출할 수 있도록 도움
- Multi-AZ 는 standby 를 다른 Region 이 아닌 같은 Region 내에 둠
- Vertical Scaling 은 Instance 의 성능을 끌어올리는 것이고, Horizontal Scaling 은 숫자를 늘리는 것
- Spot Instance 는 사용 후 첫 1 시간 이내에 AWS 에 의해 종료되면 요금을 부과하지 않고, 그 이후에 AWS 에 의해 종료되면 초단위까지 부과됨
  (Reserved Instance 는 실행 여부와 상관없이 시간당 요금이 부과됨)
- EC2 에서 Cloudwatch 로 로그 데이터를 전송하는 것은 CloudWatch Logs agent
- Lambda 는 CodeDeploy, Code pipeline 을 통해 빠르게 배포할 수 있음
- Elastic beanstalk 의 application file 은 S3 에 쌓고 로그는 선택적으로 S3 혹은 Cloudwatch Log 에 쌓임
- ENI 에는 고정된 MAC 주소가 지정됨
- SQS queue size 를 트리거하는 Autoscaling 을 구성하여 queue 에 기반하여 EC2 숫자 조절 가능(EC2 인스턴스당 대기열 메시지 수 측정)
- 블루/그린 배포의 특징
- 예약 인스턴스의 경우, 인스턴스 실행 여부와 관계없이 매 시간 요금이 청구됨, 판매하는 것이 답임

* 추가테스트 7 (Networking, Storage, Database)
- autoscaling 으로 충분히 대응이 되지 않을 경우, scheduled autoscaling 을 사용하여 대응
- ALB 는 동적 포트 맵핑을 이용하여 단일 서비스에서 여러 작업을 진행할 수 있음
  - 경로 기반 라우팅
  - 호스트 기반 라우팅
  - 네이티브 HTTP/2
  - 리디렉션
  - 고정 응답
  - Lambda 함수를 대상으로 사용
  - HTTP 헤더 기반 라우팅
  - HTTP 방법 기반 라우팅
- Autoscaling 은 기본적으로 기본모니터링이 활성화되어있으며 CLI 로 생성할 경우 세부모니터링이 기본 활성화됨

- Inspector 는 배포된 애플리케이션의 보안 및 준수를 개선하는 자동화 보안 평가 서비스
- AWS Device Farm 은 여러 기기에서 Android, iOS 및 웹 앱을 한꺼번에 테스트하고 상호 작용하거나 실시간으로 문제를 재현하는 앱 테스트 서비스
- EMR 은 Hadoop 프레임워크를 사용하여 데이터를 처리하고 분석하므로 스트리밍에는 사용되지 않으며, Kinesis Video Stream 은 분석, 기계학습 및 기타 처리를 위해 연결된 장치에서 AWS 로 동영상을 안전하게 스트리밍하므로 Kinesis data stream 에는 포함되지 않음
- 신속하고 대규모 확장을 위한 DB 는 RDS 보다는 Dynamo DB
- Cloudwatch 로그 파일에 저장하기 위한 유효한 옵션
    - CloudWatch log
    - splunk
    - S3 사용자 정의 스크립트
- DynamoDB Stream 을 이용하여 item level change 의 리스트를 유지하고 24 시간 내 발생한 item level change list 를 제공할 수 있음
- Autoscaling 의 조정 정책(아래 두 개 모두 예측 불가능한 상황에 적합)
    - 대상 추적 조정 정책 : 조정 지표를 선택하고, 대상 값을 설정(CPU 활용도, 네트워크 인터페이스에서 받은/보낸 평균 바이트 수, 대상그룹 내 대상별 요청 수
    - 단순 및 단계 조정 정책 : 조정 프로세스를 트리거하는 CloudWatch 경보에 대한 조정 지표와 임계값을 선택하고 위반시 조정 방법을 결정
- Kinesis data analytics 는 표준 SQL 을 사용하여 처리하고 Firehose 는 SQL 쿼리를 실행할 수 없음
- 모든 VPC 를 연결하기 위해서는 지역간 Peering 을 사용하고 풀 메시 구조로 구현함
- Redshift 는 아직 Multi-AZ 를 지원하지 않으며, 단일 AZ 내 데이터를 3 부식 복제하여 가지고 있으며 연속/증분 백업을 제공
- Cloudformation stackset : 단일계정으로 여러 리전에 리소스를 생성할 때 사용하는 서비스
- Proxy Protocl(TCP)와 X-forwared-for 를 쓰면 클라이언트 IP 전달 가능
- MFA 는 console 접속시, API 사용시 인증 가능
- 응용 프로그램 계층 내에서 정보를 저장하고 세션을 유지하기 위해서는 Sticky session 과 Elasticache 를 씀
- DynamoDB 사용 여부에 관계없이 프로비저닝된 처리량에 대해 요금 부과, 읽기가 많은 작업에 대해 보다 경제적임
- Cloudfront 접근제어는 사용자가 서명된 URL 을 사용하여 파일에 액세스하고 OAI 를 작성한 후 S3 버킷의 파일에 대한 액세스를 OAI 에 제한하도록 구성해야 함

- EBS 볼륨의 성능을 향상시키기 위해서는 프로비져닝된 볼륨을 사용하고 RAID 0 배열에 여러 볼륨을 추가하는 것
- DynamoDB 는 RDS, Redshift 와 달리 백업, 유지보수기간, 업데이트 등을 처리할 필요가 없어 운영상 오버헤드가 적음
- API Gateway 는 다른 개발자 액세스를 측정하고 제한할 수 있음

* 추가 테스트 8 (Computing, Storage)
- Autoscaling 은 각 AZ 의 인스턴스 수가 균형을 이루지 않을 경우 재조정을 시도함
    - 먼저 인스턴스가 없는 AZ 에서 인스턴스를 생성한 후, 나머지 AZ 에서 같은 수의 인스턴스를 종료함
- Redshift 의 클러스터와 데이터 저장소 간에 데이터 처리시, VPC EndPoint 와 Enhanced Routing 을 사용하면 인터넷을 거치지 않고 처리 가능
- EC2-Classic 에서 시작된 인스턴스는 종료되거나 중지될 때 Private IPv4 주소가 해제됨
- KMS 는 CMK 를 사용하며 IAM 콘솔에서 감사 가능한 마스터 키를 생성, 회전 및 비활성화할 수 있음
- 스키마가 자주 변경된다는 것은 스키마를 쉽게 변경할 수 있음을 의미함(NoSQL)
- S3 는 덮어 쓰기 및 삭제시 최종 일관성을 제공하지만 RDS 는 읽기 후 쓰기 일관성을 제공함
- EFS 는 Direct Connect 또는 VPN 을 이용하여 여러 AZ, Resion, VPC 등에 공유 가능(계층적 구조 사용)
- Egress Only Internet Gateway 는 IPv4, IPv6 모두 지원함
- EBS 는 요구 사항 증가시 자동으로 증가하지 않으므로, 볼륨크기를 늘린다음 파일 시스템을 확장해야 함
    - EFS 의 장점이기도 함
- DB 는 암호화된 스냅샷에서 암호화된 마스터 DB 를 생성할 수 있으며 지역에 따라 다른 암호화키로 읽기복제본을 만들 수 있음
- 하나의 IAM 역할을 하나의 작업 정의에만 적용할 수 있으므로 다른 작업 Role 을 별도로 만들어 작업 정의를 만드는 것이 좋음
- 암호화된 스냅샷을 공유하기 위해서는 CMK 키를 암호화하고 CMK 키와 스냅샷을 다른 계정과 공유해야 함
- AWS 가 인스턴스를 프로비저닝과 관리를 담당하고 고객이 개발만을 집중하고자 할 경우 API Gateway 와 Lambda 가 유용
- S3 는 필요한 성능을 알아서 늘리며 접두어 또한 S3 내부 성능 조절 기능
- Burstable Instance 는 CPU 성능을 향상시킨 유형임
- DB 를 프로비져닝할 때는 Provisined SSD 가 나음(io1)

- Cloudformation TemplateURL 은 생성 or 업데이트와 같은 스택동작에 대해 설정하는 매개변수(템플릿이 어디에 쓰일지 결정 + IAM)
- Direct Connect 은 한 지역 내 모든 AZ 에 연결할 수 있음
- ALB 는 로드밸런서에서 생성된 쿠키만을 지원하며 쿠키의 이름은 AWSALB 임
- 사용자들로 하여금 EFS 를 사용하게 하려면 각 사용자에 대한 하위 디렉토리를 만들고 사용자에게 읽기 - 쓰기 - 실행권한을 부여함
- Hadoop 클러스터와 ASG 를 동시에 사용하며 인스턴스가 종료되지 않게 하려면 인스턴스 보호기능을 사용함
- ALB 는 Cross-zone load balancing 이 기본 활성화되어있으며 사설 인스턴스로 LB 하기 위해서는 공용 서비스넷이 필요함
- ECS 서비스에서 한 컨테이너가 다른 컨테이너의 데이터에 액세스하지 못하도록 막으려면 각 작업에 대한 IAM Role 을 만드는 것이 좋음
- Spot 인스턴스가 인터럽트 발생시 할 수 있는 동작은 중지와 최대 절전 모드
- 단일 인스턴스에는 하나의 역할만을 부여할 수 있음(하나의 작업에는 하나의 역할만 부여 가능)
    - 추가적으로 IAM 역할을 만들어 부여하는 것은 불가능

* 추가 테스트 9 (Computing, Storage, Newtork/Contents)
- EC2 의 향상된 네트워킹을 사용하기 위해서 VPC 에서 시작하여야 하고, HVM AMI 에서 시작해야함
- ASG 를 사용하는 것보다 Cloudfront 를 사용해 캐싱하는 것이 더 효율적
- Elastic Beanstalk 는 장기간 실행되는 작업 프로세스와 RDS 를 사용하는 프로그램에 좋음(SQS, RDS)
- 다운타임을 최소화하면서 일관된 스냅샷을 만드는 가장 좋은 방법은 EBS unmount 후 스냅샷 찍고 다시 mount
- Lambda 내 환경변수로 저장할 땐 KMS 를 활용하는 암호화 helper 는 사용하는 것이 좋음
- EBS 처리량 최적화 HDD 는 트래픽이 적은 소규모 DB 의 경우 충분함
- 비디오 제공 서비스에서 피크 시간 대에 느려지면 Cloudfront 를 사용하는 것이 좋음
    - Cloudfront 는 정적,동적,비디오 캐시가 가능
- ELB 의 SSL 협상을 위한 정책 2 가지는 predefined security policies 와 custom security policies 임
- Connection draining 이 활성화된 경우 커넥션이 종료될 때까지 기다리며, 새로운 대체 인스턴스를 시작하기 전에 유지중인 인스턴스를 먼저 종료함
    - Autoscaling 은 관리자에게 알람을 보내지 않음

- 온프레미스 AD 로 디렉터리 요청을 하기 위해서는 AD Connector 가 필요하며 IAM Role 을 생성해 권한을 정의함
- PrivateLink 를 사용하면 VPC 를 지원하는 AWS 서비스, 다른 계정에서 호스팅하는 서비스에 연결 가능
- 낮은 대기시간 및 높은 네트워크 처리량을 보장하는 EC2 디자인은 향상된 네트워킹과 Placement Group
- IGW 는 대역폭에 대한 제한이 없음
- 프록시 프로토콜은 L4 단계에서 실행하는 것으로 웹계층에서는 소용 없음
- AWS Directory service 는 AD connector 를 사용하여 온프레미스 AD 사용자와 그룹에 할당할 수 있으며 IAM 정책에 따라 사용자 액세스 제어
- CloudWatch Logs 는 로그 데이터를 사용하여 애플리케이션 및 시스템을 모니터링할 수 있음

* 추가 테스트 11
- Step function : 서버 워크 플로우를 조정하고 람다 실행 한계 내에서 지원되지 않는 작이 실행을 여러 단계로 나누거나 실행중인 Worker 를 호출하여 결합
- Cloudformation 의 기능 2 가지
    - direct update : 업데이트를 즉시 배포하는 기능
    - change set : 적용되는 변경사항을 Preview 해볼 수 있음
- Cloudfront RMTP 는 파일을 S3 에 저장함
- 전용 호스트는 기존 서버 소프트웨어 라이센스를 사용할 수 있으며 요금이 호스트별로 부과됨
- Route 53 multi-value answer 는 DNS 쿼리 응답에 최대 8 개의 레코드를 반환
- EC2 유형의 ECS 만이 운영체제에 액세스 가능
- 모든 EBS(EC2 Instance 아님)은 암호화를 지원
- CloudTrail 이 지원하는 2 가지 이벤트
    - 데이터 이벤트
    - 관리 이벤트
- Autoscaling 은 손상된 인스턴스가 확인될 경우 이를 종료한 후!!! 새로운 인스턴스로 교체함
- 람다함수가 VPC 내부 리소스에 액세스하려면 서브넷 ID 와 보안 그룹 ID 가 필요
- ECS 내 인스턴스들이 연결이 끊긴 것으로 표시될 경우
    - 컨테이너 인스턴스가 컨테이너 에이전트에서 실행되고 있는지 확인
    - IAM Instance Profile 에 권한이 있는지 확인
- Read Replica 는 배포될 AZ 를 지정할 수 있고, 4 개 이상의 인스턴스를 포함할 수 없으며 복제는 비동기식

- ALB 는 Cognito 와 통합되어 OIDC ID 공급자 인증을 지원함
- DynamoDB 의 경우, 읽기/쓰기 용량을 결정해야 하며 Lambda, Kinesis 는 용량을 결정하지 않음
- DynamoDB 의 모범사례
    - 항목 크기를 작게 유지
    - 데이터 / 시간에 기반한 작업이 필요한 경우 일별/주별/월별 테이블 생성
    - 액세스가 빈번한 테이블과 적은 테이블 구분
    - S3 에 400KB 를 초과하는 객체를 저장하고 DynamoDB 에서 포인터 사용
- 암호화된 스냅샷을 공유하기 위해서는 사용자 지정 키와 스냅샷 사용 권한을 공유해야 함
- API Gateway 와 Cloudfront 을 결합하면 세계 각지에서 API 요청 및 응답을 가능한 빠르게 전달 가능
- S3 버킷의 유효한 엔드포인트
    - <bucket>.s3.amazonaws.com/object
    - s3.<region>.amazonaws.com/bucket
- S3 정적 웹 호스팅 주소 : 버킷이름.s3-website-ap-northeast-1.amazonaws.com
- IAM Group 은 IAM 정책에서 주체로 식별될 수 없음

* 추가 테스트 12
- 사용자지정 보안그룹은 기본적으로 모든 인바운드 트래픽이 거부되며, 모든 IP 주소로의 트래픽을 허용하는 아웃바운드 규칙 존재
- ELB 는 가중치 라우팅 정책을 지원하지 않으며, 같은 유형의 인스턴스를 쓰는 것이 성능 문제를 해결하는 방법
- AWS 의 관리형 쿠버네티스는 EKS 로 애플리케이션 구축에 집중하면서 인프라 관리를 처리할 수 있음
- 온프레미스의 디렉토리 서비스를 이용하려면 AD Connector 와 IAM Role 을 사용하면 가능
- ASG 내에서 정의된 시작 구성은 편집할 수 없으므로 다시 시작해야 함
- 인스턴스 스토어 볼륨은 시작할 때만 지정 가능
- RDS 를 특정시점으로 복원할 경우, 마지막 5 분까지 복원할 수 있으며, 기본 DB 보안그룹이 적용됨
- 기본이 아닌 VPC 인스턴스에는 프라이빗이 할당되며, 기본 VPC 인스턴스에는 퍼블릭 및 프라이빗 DNS 가 할당됨
- AWS Batch 는 컴퓨팅 작업을 프로비져닝, 관리 모니터링 및 확장하기 위한 서비스
- ELB Access Log 는 DynamoDB 에 전달하도록 구성할 수 없음

- SQS 에서 한 메시지가 처리되다가 완료되지 않으면 Visibility time out 이후에 선택 가능

* 덤프 오답
- ECS 사용시 각 작업들의 권한을 제한하고 싶다면 'task'에 IAM Role 을 적용하면 가능
- IAM, 웹 자격연동, SAML 등이 STS 를 사용하여 임시 자격을 부여함
- S3 의 encryption at rest 에는 SSE-S3, KMS, C-KEY 뿐만 아니라 client-side own master key 도 포함
- IAM 의 정의 : '허용'해줄 정책(Policy)을 생성(Create)하고 '부여'해줄 대상(Role)을 정함(Attach)
- EBS-optimized Instance 는 EBS I/O 를 위한 추가 전용 용량을 제공함
- Cloudfront 의 OAI 확인
- EBS 암호화 방법 : EBS 에서 Snapshot 을 생성(이 때 암호화 불가), 스냅샷을 이용하여 암호화 볼륨 생성
- Lambda 를 트리거하는 서비스 : SNS, S3, SES, SQS, Kinesis, Cognito, Cloudfront, Dynamo DB
- EC2 전용 호스트(Dedicated Host) : 고객 전용의 EC2 인스턴스 용량을 갖춘 물리 서버, 전용 호스트를 통해 Server 의 기존 소켓당, 코어당 VM 당 라이센스 사용 가능
    - 인스턴스와 차이점 : 전용 호스트는 자동 인스턴스 복구 지원하지 않음, 소켓 코어 등의 표시 여부를 제공
- SWF 의 정의
- Read replica 가능한 RDS : MySQL, PostgreSQL, MariaDB, Oracle, Aurora
- Autoscaling 은 EC2 상태확인, ELB 상태확인, 사용자 지정 상태 확인을 통해 인스턴스의 상태를 확인하며 비정상 인스턴스 발생시 조정 정책 이후 자동으로 비정상 인스턴스를 삭제
- Session data 를 Dynamo DB 에 저장하여 보다 빠르게 검색 가능케 함
- DynamoDB 는 TTL 을 가지고 있어 일정시간 만료 후 삭제할 수 있으며, Pipeline 을 통해 S3 로 전송 가능
- SNS 의 endpoint 로는 Lambda, SQS, HTTP/S, Email-JSON, SMS 가 있음
- S3 Client Encryption 의 경우 마스터 키로 암호화하거나 CMK 를 쓰는 방법이 있는데 마스터 키 암호화는 마스터 키와 암호화되지 않은 데이터가 S3 로 전송되지 않음
- S3 glacier 도 multipart upload 지원
- RDS DB Instance Storage
    - 범용 SSD
    - Provisioned IOPS
    - Magnetic

- ELB 는 IGW 가 연결되어있는 public subnet 을 쓰도록 설정되어야 함(Security Group + ACL)
- S3 Transfer Acceleration 은 거리가 먼 클라이언트와 S3 간에 파일을 빠르고 쉽게 전송할 수 있게 해줌
- API Gateway 는 Lambda authorizer 를 이용하여 API 메서드에 대한 Access 를 제어할 수 있음
- AWS Autoscaling 으로 제어 가능한 것
    - ECS
    - EC2 Spot fleet
    - EMR Cluser
    - DynamoDB 의 글로벌 보조 인덱스의 프로비저닝된 읽기 및 쓰기
    - Aurora 복제본
- OpenID 와 같은 외부 자격 공급자는 보통 웹 자격증명과 관련 있음
- Cloudfront 에서 오래된 객체가 검색될 경우 2 가지 방법 : S3 객체 무효화, 버전 관리 사용
- CLB 는 Single AZ 가능
- SSE-C : 자체 암호화키는 유지하고 싶지만, 클라이언트 암호화 라이브러리를 구현하고 싶지 않은 경우
- Cloudwatch logs 는 EC2, CloudTrail, S3 등에서 로그 파일을 모니터링, 수집 저장하여 중앙집중화시키는 서비스
- 서비스가 독립적으로 확장된다는 것의 의미 : 별도의 Load Balancer?
- S3 Life Cycle 은 30 일 이내에 Standard 에서 Standard-IA 로 30 일 내에 옮기게 되면 30 일치 요금을 물게 됨(가능하긴 하다는 뜻)
- 보안그룹이 여러 개일 경우 먼저 것을 먹음
- S3 의 일관성 모델 중요!!!!!(Read and Write for new object, eventually consistency for PUT and DELETE)
- AWS Consolidated Billing 을 통해 조직별 결제 통합관리 가능
- (자동기능)S3 쿼리시 성능을 극대화하기 위해 접두사로 추가된 4 자 16 진수를 사용함(exampleawsbucket/c34a-2019-14-03-15-00-01/cust1248473/photo7.jpg)
- ELB 을 위한 공용 서브넷 2 개, 웹서버용 2 개, DB 용 2 개가 좋음
- 람다 환경 변수는 코드를 변경하지 않고 함수 코드와 라이브러리에 설정을 동적으로 전달함
    - 각자 다른 데이터베이스에 다른 정보를 참조하기 위해 사용 가능
    - 환경변수를 사용하는 Lambda 함수를 생성 또는 업데이트시 KMS 를 사용하여 암호화
- S3 는 각 리전 내 최소 3 개의 AZ 를 운영하며 복제함

- 인스턴스를 프로비저닝하거나 관리하지 않고 소프트웨어 개발에 집중하고 새로운 기능을 배치하고자 할 때는 API Gateway 와 Lambda
- 부서당 AWS 계정을 만든 상태에서 단일 Direct Connect 회로를 주문하면 가상 인터페이스를 구성하고 부서 계정번호로 태그를 걸면 가능
- VPC Peering의 경우 기본적으로 NACL에서 거부