* Acloudguru Mega Quiz

- IPv6 를 지원하는 네트워크 구성요소는 인터넷 게이트웨이와 외부 전용 인터넷 게이트웨이
- Cloudformation 실패시 스택 삭제 방지 방법 : disable-rollback
- Cloudformation 과 Lambda, EC2 는 SSM parameter Store 를 지원
- IAM : PassRole 은 다른 계정으로의 역할 전달 및 AWS 서비스로의 역할 전달 담당
- ElastiCache 는 Pub / Sub, Sorted Set, 인 메모리 데이터 스토어에는 적합하지만, 관계형 데이터는 부적합
- 기본 데이터 암호화(설정시)는 EBS, S3, EFS 가 지원하며 Memcached 는 지원하지 않음

* Sysops administrator exam 1

- CloudWatch 의 3 가지 표시 항목은 OK, Alarm, Insfficietn Data
- RDS 에서 일관된 읽기를 사용하면 모든 쓰기 작업의 업데이트를 반영하여 최신 데이터로 응답
- Trusted Advisor Business, Enterprise 고객은 알림과 프로그래밍 방식 액세스 사용이 가능함
- CloudWatch 를 워크플로우 일부로 사용할 경우 선택 가능 유형은 Lambda, kinesis, SQS, SNS
- S3 에서 의도된 삭제를 방지하는 방법은 CRR 과 복제본 소유자 변경
- ELB 는 트래픽 플로우가 있을 때만 지표를 보고함
- Batch 컴퓨팅 환경
    - 관리형 : 인스턴스 타입, vCPU 와 같은 요구사항 지정 가능
    - 비관리형
- Federation Access 를 구성할 때 보안 자격증명을 요청하고 로그인 URL 을 구성하는데 사용하는 프로토콜 및 API Call 은 SAML 2.0, AssumeRoleWithSAML
- 범용 SSD 는 최대 3000 IOPS 의 버스트 기능을 지원하며, 최대 16000 IOPS 가능
- RDS 를 삭제할 경우 Automated backup 만 삭제됨
- 지역을 떠나서 가장 빠른 응답시간을 요구하는 경우, 지연 기반 라우팅이 최적
- ElastiCache 서비스를 구성할 때 일반적인 스왑파일 크기는 램 크기와 동일
- 인스턴스를 가장 빠르게 업그레이드(메모리 사용량 증대와 같은)하는 방법은 인스턴스 중단 및 수정 후 재시작
- DynamoDB Streams 는 모든 DynamoDB 테이블에서 수정 순서를 캡쳐하고 24 시간 동안 로그에 저장
- EC2 인스턴스에서 스캔을 수행할 경우 Amazon 은 권한을 얻는 것이 우선
- Aurora 의 클러스터에는 클러스터 엔드포인트가 있으며 이를 통해 기본 인스턴스에 연결(리더가 아님)
- R/R 을 만들기 위해서는 자동 백업이 활성화되어야 있어야 함

- http://169.254.169.254/latest/meta-data/
- Elastic Beanstalk 의 App 배포 방식
    - 한 번에 모두 : 새 버전을 모든 인스턴스에 동시에 배포, 배포가 수행되는 동안 환경에 있는 모든 인스턴스 중지
    - 롤링 : 새 버전을 배치로 분할하여 배포, 각 배치는 배포단계동안 서비스에서 제외되므로 환경 용량 감소
    - 추가 배치를 사용한 롤링 : 새 버전을 배치로 배포하지만, 새로운 배치의 인스턴스를 시작하여 용량 유지
    - 변경 불가능 : 새 버전을 새로운 인스턴스 그룹에 배포
- RDS R/R 이 네트워크 이슈 혹은 복제 이슈로 싱크가 되지 않을 경우 봐야 하는 메트릭은 ReplicaLag
    - 추가로 ReplicaLag 는 읽기 전용 복제본이 원본 데이터베이스보다 뒤쳐지는 시간을 나타냄
- RPO / RTO 가 0 이 되려면 모든 기능을 갖춘 복제본을 배포해야 하며 Multi-Site Active-Active 구성을 사용해야 함
- Autoscaling 은 키 페어가 삭제되었거나, AS 그룹을 찾지 못할 경우, 관련 보안그룹이 없을 경우 새 인스턴스를 시작하지 않음
- ELB 내 서버에 문제가 생길 경우, 해당 인스턴스로의 라우팅을 중지하고 기존 로드밸런싱 알고리즘을 기반으로 새로운 인스턴스 선택
- RDS 의 장애조치 프로세스 : RebootDBInstance API 를 호출하거나 인스턴스를 재부팅하고 장애조치로 재부팅을 선택하여 테스트

* Sysops administrator exam 2
- Read Replica 를 업데이트할 수 있도록 변경하기 위해서는 read_only parameter 를 0 으로 변경해야 함
- OpsWorks Stack 을 구성할 때의 5 가지 수명주기 이벤트는 Shutdown, Setup, Configure, Undeploy, Deploy
- RDS R/R 은 자동백업이 활성화되어있아야 사용 가능
- RDS DB 인스턴스를 모니터링하기 위해서는 RDS Event 와 CloudWatch 가 필요
- ELB 에서 페이지를 로드하는 시간이 굉장히 느리다면 Latency Report 를 보는 것이 좋음
- S3 버킷에서 503 코드를 반환하는 이유는 과도한 트래픽을 조절하기 위해 응답을 제한하는 것
- 태그를 리소스에 적용하여 리소스 소유자 식별 가능
- DynamoDB 의 각 쓰기 용량 단위는 초당 최대 1KB 의 쓰기 1 을 나타냄, 각 항목이 4KB 일 경우 쓰기 4 용량이 필요

- SQS 내 Dead Letter Queue 를 통해 처리하지 못한 메시지를 확인하고 처리가 실패한 이유를 알 수 있음
- Xen HyperVisor 는 AWS 의 책임 소재
- 온프레미스에서 EFS 에 접근할 수 있는 연결 유형은 VPN, Direct Connect
- 읽기 복제본을 생성하고 동기화하기 위해 AWS 에서 지원하는 MySQL 엔진은 InnoDB
- API Gateway 는 많은 요청으로 인해 API 가 가득 차는 것을 방지 하기 위해 토큰 버킷 알고리즘을 통해 API 요청을 조절함
- ELB 를 사용할 때, 사이트 연결이 끊어지고 시간 초과 오류가 발생한다면 idle timeout 을 늘려주면 됨
- 인스턴스 프로파일은 IAM 역할을 위한 컨테이너로 EC2 인스턴스에 대한 역할 정보 전달에 사용
- Fn::GetAtt 는 URL 을 식별할 수 있도록 DNS 이름 제공
- Cloudformation 의 DependsOn 속성을 통해 특정 리소스가 생성된 이후에 다른 리소스가 생성될 수 있도록 가능
- CloudWatch Event 를 사용하여 AWS Lambda 를 일정에 따라 실행하도록 설정할 수 있음
- VPN 사용시 고객 게이트웨이를 추가로 구성하면 이중화가 가능
- 다른 DNS 서비스에서 호스팅하던 것을 Route 53 으로 옮길 경우, name server 설정을 변경해야 함
- DB 를 강제 Failover 하기 위해서는 기본 DB 인스턴스를 재부팅하고 'Rebooting with Failover' 설정
- DynamoDB 에서 400 Bad Reqeust 를 받는 경우는 프로비져닝된 용량보다 더 많은 읽기 / 쓰기 요청을 하기 때문
- Direct Connect 의 Public/Private Virtual Interface 차이
    - Public : S3 와 같은 AWS 외부 서비스와 연결하기 위한 인터페이스
    - Private : VPC 내 서비스와 연결하기 위한 인터페이스
- Autoscaling 의 수명주기후크를 사용하면 인스턴스를 시작/종료할 때 인스턴스를 일시중지하여 사용자 지정 작업을 할 수 있음
- Autoscaling 의 상태 확인 유예기간을 늘리면 서버가 실행하기 위해 준비하는 시간을 연장할 수 있음
- Elastic Beanstalk 의 블루/그린 배포는 별도의 환경을 배포한 후 두 환경의 CNAME 을 변경하여 가동중지를 막는 배포임

* Sysops administrator exam 3
- CloudTrail 의 추적 유형은 모든 지역과 단일 지역이 있음
- 인스턴스 상태 확인

    - 시스템 상태 확인
        - 네트워크 연결 끊김
        - 시스템 전원 중단
        - 물리적 호스트의 소프트웨어 문제
        - 물리적 호스트의 하드웨어 문제
    - 인스턴스 상태 확인
        - 시스템 상태 확인 실패
        - 잘못된 네트워크 구성
        - 메모리 모두 사용
        - 파일 시스템 손상
        - 호환되지 않는 커널
- 인스턴스 스토어 볼륨은 재부팅해도 데이터가 손실되지 않음
- AWS Health API 를 사용하기 위해서는 Enterprise 혹은, Business 지원이 필요
- Trusted Advisor 의 5 가지 구성요소는 비용 최적화, 서비스 제한, 성능, 보안, 내결함성(고가용성 없음!!!!!!!!!!!)
- Opswork 에서 'Manage' Level 은 스택 액세스는 불가능하지만 앱 배포 및 스택 보기는 가능
- RDS 배포에 사용가능한 OS 패치 및 DB 업데이트를 보는데 RDS API, AWS CLI, RDS Console 로 가능
- 다음 3 가지 사항이 충족되면 중단된 스팟 인스턴스를 중지하도록 할 수 있음
    - 스팟 인스턴스 요청 유형이 'Persistent'
    - 스팟 집합 요청의 유형이 maintain
    - EBS 볼륨일 경우
- RDS 다중 배포는 단일 리전에서만 가능하며, 오로라는 읽기 복제본은 다른 리전도 가능
- Cloudformation 생성 후 S3 에 저장된 버킷이 삭제되지 않도록 하려면 버킷 정책 내 DeletionPolicy 속성을 사용하면 됨
- Redshift, RDS, Redis 는 자동백업 제공
- RDS Failover 시 원래 기본 인스턴스가 종료되고 다른 Standby 가 생성됨
- Lambda 함수 내에 환경변수를 사용하면 코드를 변경하지 않고도 설정을 함수 코드 및 라이브러리에 동적으로 전달 가능
- ELB 고급 설정에 사용가능한 설정은 Response Timeout, Unhealthy Threshold, Healthy Threshold
- CloudWatch 를 사용하여 모니터링시 데이터를 검색할 권한을 줄 경우 GetMetricStatistics 를 주어야 함
- Memcached 의 SwapUsage 값이 50MB 가 초과할 경우 ConnectionOverHead 값을 높이는 것이 좋음

- Visibility timeout 을 늘리게 되면 다른 소비자가 접근하여 처리하는 중복 현상을 줄일 수 있음
- Cloudformation 변경 세트 : 스택을 업데이트해야 하는 경우 변경사항을 구현하기 전에 변경 사항이 실행중인 리소스에 미치는 영향을 확인할 수 있음
- AD 자격증명을 통해 콘솔에 로그인할 경우 AssumeRoleWithSAML API 를 호출함
- Redshift 는 데이터의 증분을 정기적으로 생성하며 S3 에 저장함
- Memcahced 의 CPU 사용률 메트릭은 최대 90%임
- 결제 보고서에 태그를 표시하려면 결제 콘솔의 '비용 할당 태그' 섹션에 태그를 활성화해야 함
- 프라이빗 키를 분실했을 경우 인스턴스를 중지하고 루트 볼륨을 분리한 뒤, 새로운 인스턴스를 생성하여 키페어를 생성하고 authorized_keys 를 임시 인스턴스에 대한 authorized_keys 의 새 퍼블릭 키로 업데이트
- Lambda 가 VPC 리소스에 액세스할 수 있는 ENI 를 가질 경우 NAT Gateway 를 통해 인터넷에 액세스함
- IAM Role 에서 활성 세션 취소를 누르면 AWSRevokeOlderSessions 이라는 역할을 연결하여 모든 세션에 대한 액세스를 즉시 거부할 수 있음

* Sysops administrator exam 4
- 리소스가 모범 사례를 준수하는지 확인할 때는 Trusted Advisor 가 나음(Inspector 는 취약점 점검용)
- 용량이 80TB 를 넘을 때는 Snowball Edge 가 더 효율적
- SQS 대기열의 메시지 수를 확인한 후 Auto Scaling 그룹이 추가 EC2 를 시작할 수 있도록 가능
- Redshift 의 모든 COPY 및 UNLOAD 트래픽을 모니터링할 경우 Enhanced VPC Routing 사용
- SSM 의 파라미터 스토어를 이용해 Cloudformation 의 AMI 를 변경할 수 있음
- 온프레미스 서버에 CloudWatch Agent 를 설치하여 모니터링 가능
- S3 인벤토리는 S3 버킷의 규정 준수, 요구사항에 따른 복제 및 암호화 상태를 감사 후 보고 가능
- Geoproximity Routing Policy 는 사용자의 지리적 위치와 리소스에 따라 트래픽을 리소스로 라우팅 가능
- Autoscaling Group 에서 그룹 크기를 업데이트하지 않고 인스턴스를 종료하는 명령어
    - terminate-instance-in-auto-scaling-group --no-should-decrement-desired-capacity
- Pilot Light ???
- Cloudformation 의 CreationPolicy 을 사용하면 지정된 수신호를 전달받기 전까지 리소스의 상태가 생성 완료로 변하지 않음

- EC2 인스턴스 <인스턴스 ID>가 VPC 에 있습니다.로드 밸런서 구성 업데이트에 실패했습니다
    - ELB 와 Autoscaling 이 동일한 네트워크에 없을 경우 발생
- 프로비져닝 IOPS SSD 볼륨의 크기와 IOPS 의 최대 비율은 50:1
- DynamoDB 글로벌 테이블은 다중 리전, 다중 마스터 베이스를 배포할 수 있도록 지원
- Route 53 은 다음 3 가지 모니터링 가능
    - 엔드포인트 모니터링
    - Healthcheck 모니터링
    - CloudWatch 모니터링
- Autoscaling 에서 Terminate 스케일링 프로스세를 일시적으로 중지하게 도면 AZRebalance 가 영향을 받아 AG 가 최대 10% 커질 수 있음
- 버전관리와 MFA 가 활성화되어 있는 버킷을 삭제할 경우 2 가지 중 하나를 수행해야 함
    - 버킷 정책에서 MFA 삭제가 필요한 정책 제거, 삭제 마커와 객체 버전을 제거
    - 루트 계정 소유자가 버킷에서 MFA 및 버전관리를 일시 중단하도록 함, 현재 객체 버전을 만료하고 이전 버전을 영구적으로 제거하도록 수명주기 작성

* Sysops administrator exam 5
- Multi Site 는 AWS 의 DR 솔루션 중 가장 빠르고 비쌈
- S3 요청에 대한 HTTP 503 응답이 크게 증가한다는 것은 버전이 무수히 많은 객체가 하나 이상 버킷에 존재한다는 것
- 인스턴스가 pending 상태 이후 종료된다면 다음과 같은 경우임
    - EBS 볼륨제한 도달
    - EBS 스냅샷 손상
    - KMS 키에 액세스할 권한 없음
    - AMI 에 필요한 부분이 없음
- Cloudformation 에서 cfn-signal 은 EC2 인스턴스가 성공적으로 생성 또는 업데이트되었는지 여부를 Cloudformation 에 보냄
- 표준 예약 인스턴스는 기간동안 인스턴스 유형을 수정할 수 없음
- 사용자 지정 지표를 AWS CLI 또는 API 를 통해 Cloudwatch 에 업로드할 수 있음
- NLB 는 초당 수백만 건의 요청을 자동으로 확장할 수 있음
- Glacier 아카이브에 직접 업로드는 불가능, Snowball 을 사용하거나 다른 유형으로 업로드한 이후 수명주기 규칙을 이용
- 예산 제한의 경우, Cloudwatch 에서 청구 경보를 설정하면 편리함
- 인터넷 게이트웨이는 IPv4, IPv6 를 지원함
- Cloudwatch 에서 리전간 데이터를 집계할 수 없음

- Virtual Private Gateway 를 이용하여 하나 이상의 VPC 를 Direct Connect 로 연결 가능(?????????????????????? - transit gateway)
- CLB 에서 TCP 를 사용하면 헤더를 수정할 수 없음(HTTP)
- CLB 에서 지원하는 보안기능은 SSL 인증서, SSL 협상, 백엔드 서버 인증
- VPC 에서 새로운 서브넷이 필요한데 IP 가 부족한 경우 VPC 에 보조 CIDR 블록을 추가하면 가능
- 보조 CIDR 블록의 최대 갯수는 4 개
- Cloudfront 에는 캐시 통계 보고서, 상위 25 개 참조자 보고서, 인기 객체 보고서, 사용보고서가 있음
- EBS 의 볼륨에 남아있는 디스크 스토리지의 양은 사용자 정의 메트릭
- Route 53 개인 호스팅의 경우, A 레코드를 생성하고 데이터베이스 IP 를 연결
- DB 보안그룹은 EC-Classic 에 관한 정보

* Sysops administrator exam 6
- EC2 Enhanced networking
    - Elastic network adapter 를 통해 최대 100Gbps 의 속도를 지원(ENA)
    - intel 82599 Virtual Function 인터페이스
- Route 53 은 2xx and 3xx 에 대한 상태 코드를 반환함
- DNS 서비스에 등록된 기존 부모 도메인을 재사용하면서 새 웹페이지에 리디렉션되게 만드는 것은 하위 도메인에 대한 Route 53 호스팅 영역을 생성하면 가능
- EBS Cold HDD 를 쓰는 것보다 EFS 를 쓰는 것이 비용이 더 많이 듦
- DiskReadOps 는 지정된 기간동안 인스턴스에 사용 가능한 모든 인스턴스 스토어 볼륨에서 완료된 읽기 작업을 계산하는 지표로 인스턴스 볼륨이 없으면 값이 0
- Cloudformation 은 일수 서비스를 제대로 생성하지 못하면 기본적으로 스택을 롤백
    - --on-failure 는 스택 작성에 실패할 경우 수행할 조치를 결정하는 매개변수
- 인스턴스가 적재되어있는 서브넷을 삭제하려 할 경우 인스턴스가 종료될 때까지 삭제되지 않음
- CLB 인증서 교체 방법
    - aws iam get-server-certificate 명령어를 사용하여 인증서를 가져옴
    - aws elb set-load-balancer-listener-ssl-certi 를 이용하여 로드 밸런서에 새 인증서 추가
- ACM 이 제공하고 ELB 에 배포된 인증서는 자동으로 갱신이 가능
- AWS Config 는 다음 이벤트에 알림을 보냄
    - 리소스의 구성 항목 변경
    - 리소스의 스냅샷 생성 시작
    - 리소스의 규칙 준수 여부

    - 리소스에 대한 구성 기록이 계정에 전달되었을 때
    - 규칙에 대한 평가를 시작할 때
- 클라우드 보안 사례를 따랐는지 점검할 경우 Trusted Advisor 가 좋음
- CloudWatch 는 리전간 데이터를 집계할 수 없으며, 세부 모니터링이 활성화된 EC2 인스턴스에 대한 통계는 집계 가능
- Cognito 자격증명 풀은 인증된 사용자가 리소스에 액세스를 할 수 있는 권한을 제공하며 각 권한은 IAM Role 을 통해 제어
- ELB 의 액세스 로깅은 선택적 기능이며 로그를 캡쳐하고 S3 에 저장
- VPC Flow Log 는 네트워크 인터페이스를 오가는 IP 트래픽을 캡쳐하는 기능
- KMS 에 암호화키를 저장 가능
- EBS 볼륨으로의 데이터 전송이 성능을 저하시키면 EBS 최적화 볼륨 사용
- EC2 내에서 발생하는 여러 활동에 대한 보고서, 통신 세부정보, 보안채널 사용, 실행중인 프로세스 정보 등을 수집하는 것은 Inspector
- 서비스 사용 및 비용에 대한 분석을 제공하는 보고서는 Cost Optimize monitor
- SSM
    - 리소스 및 인스턴스를 구성하고 관리하기 위한 워크플로우 구축
    - 사용자 지정 워크플로우 생성
    - CloudWatch Events 를 사용하여 워크플로에 대한 알림 받기
    - 자동화 진행 및 실행 상황 모니터링
- 스택을 업데이트 하는 두가지 방법
    - 직접 업데이트
    - 변경 세트 작성 및 실행
- AWS 가 제공하는 보안사항은 웹사이트에 자세히 제공됨
- CloudWatch Events 를 사용하여 AWS Health 이벤트 상태의 변화를 감지하고 이벤트가 규칙에 지정한 값과 일치하면 하나의 작업을 호출함

* Sysops administrator exam 7
- VPC 를 삭제하기 전에 VPC 와 연결된 모든 게이트웨이와 리소스를 분리하거나 삭제해야함(보안그룹과 라우팅 테이블은 제외)
- Cloudformation StackSets 은 단일 작업으로 여러 계정 및 리전에서 스택을 생성, 업데이트, 삭제할 수 있도록 스택 기능을 확장
- AWS Directory Service 는 AD 를 사용하여 Single Sign On 기능활성화 가능
- CLB 에서 제공하는 두 가지 추가적인 지표는 SurgeQueueLength(보류)와 SpiiloverCount(거부)
- AWS CLI 에서 put-metric-data 명령을 사용하여 사용자 지정 지표를 CloudWatch 로 푸시할 수 있음

- 인스턴스 무제한 모드 : Unlimited 모드는 성능 순간 확장 가능 인스턴스에 사용할 수 있는 크레딧 구성
- Redshift 는 CRR 기능이 없으며, 스냅샷을 다른 리전으로 자동 복사하도록 클러스터 구성 가능
- CloudTrail 사용시 로그 파일 전송 후 무결성을 검증하기 위해서는 로그 파일 무결성 검증을 사용하면 가능
- DLM 을 사용하면 EBS 볼륨을 백업하기 위해 만든 스냅샷의 생성, 보존, 삭제를 자동화할 수 있음
- CloudWatch Agent 를 통해 웹서버의 로그를 Cloudwatch 로 전송 가능
- CloudWatch Events(다음과 같은 이벤트가 발생하는 경우 CloudWatch Events 로 이벤트를 보냄) + 람다로 이용 가능
    - EBS 볼륨 이벤트 : 볼륨 생성, 볼륨 삭제, 볼륨 연결
    - EBS 스냅샷 이벤트 : 스냅샷 생성, 스냅샷 복사, 스냅샷 공유 - > 스냅샷 생성시 람다 함수를 트리거하여 다른 리전으로 복사
    - EBS 볼륨 수정 이벤트 : 수정될 때 전달, 저장,로깅,아카이빙은 되지 않음
    - 람다를 이용한 이벤트 처리 : EBS 와 CloudWatch 이벤트를 통해 데이터 백업 워크플로우 자동화 가능(IAM, 람다, Events 필요)
- Cloudfront 에서 파일이 만료되기 전에 파일을 제거하는 방법
    - 엣지 캐시에서 파일 무효화
    - 파일 버전 관리를 사용하여 서로 다른 이름을 가진 여러 버전의 파일 제공
- Aurora Service 는 Aurora Auto Scaling 을 통해 워크로드 증가 처리 가능
- DynamoDB 는 온디맨드 백업 기능을 제공
- 하이브리드 클라우드 아키텍쳐인 환경에서 데이터 일부를 클라우드로 옮길 경우 Snowball 보다는 File Gateway 로 옮기고 Glacier 로 옮기는 것이 나음
- RDS 리소스를 관리하기 위해 루트 계정을 사용하지 말 것

* Sysops administrator exam 8
- MFA Delete 활성화시 객체 버전을 영구히 삭제하거나 버킷의 버전 관리 상태를 변경해야 함
- User data 를 이용하는 것보다 AMI 에 필요한 모듈을 포함시키는 것이 적은 시간 내에 작동 가능
- DB 인스턴스에 연결할 수 없는 3 가지 이유
    - 로컬 방화벽에서 적용되는 액세스 규칙과 인스턴스 보안그룹의 IP 규칙이 일치하지 않음
    - 아직 DB 인스턴스가 생성중
    - 보안그룹에 허용이 되어있지 않음

    - 네트워크에서 지정한 포트를 열지 않음
- Cost & Usage Report 는 사용을 추적하고 예상요금을 제공함
- RDS 암호화 제한
    - 암호화는 생성시에만 활성화, 다만 스냅샷을 생성하여 암호화된 사본 생성 가능
    - 암호화된 인스턴스를 비암호화하는 것은 불가능
    - 암호화된 읽기 복제본은 소스 DB 인스턴스와 동일한 키로 암호화해야 함
    - 암호화되지 않은 DB 인스턴스의 암호화된 읽기 복제본 보유는 불가
    - 다른 리전으로 암호화된 스냅샷을 복사하려면 대상 리전의 KMS 키 식별자를 지정해야함, KMS 키는 리전 고유이기 때문
    - 비암호화된 스냅샷 혹은 백업으로 암호화된 인스턴스로 복원 불가
- 모든 계정에 걸쳐 AWS 에서 리소스를 생성할 시 태그가 일관되게 적용되도록 할 겨우
    - Cloudformation 리소스 태그 속성을 사용하여 생성시 특정 리소스 유형에 태그 적용
    - AWS 서비스 카탈로그를 사용하여 프로비져닝된 리소스에 고유식별자로 태그 지정
- WAF 와 ALB 만 통합 가능
- IAM 의 AWS 관리형 정책과 고객 관리형 정책 구별
- CodeDeploy 는 EC2, 온프레미스 인스턴스, 람다에 대한 애플리케이션 배포를 자동화하는 서비스
- RDS 성능 향상은 인스턴스 유형 변경을 통한 스케일 업과 읽기 복제본을 통한 스케일 아웃
- CloudWatch 의 1 초 간격 사용자 지정 지표
    - AWS 는 콘솔을 통해 사용자 정의 지표를 게시할 수 없음
    - 데이터 세분성이 1 초인 고해상도 메트리 게시
- CMK 에 대한 액세스 제어하는 기본적인 방법은 Key Policy
- 로드밸런서가 생성한 쿠키 이름은 AWSELB
- 삭제 대기 중인 CMK 는 어떠한 암호화 작업에도 사용되지 않으며, 삭제 대기중인 CMK 의 백업키를 교체하지 않음
- 스택이 삭제된 이후에도 배포된 인스턴스를 유지할 경우 DeletionPolicy 스택 리소스의 속성을 'Retain'
- RDS 에 대한 연결을 SSL 을 사용하여 암호화 가능
- 실행중인 EC2 에서 Auto Scaling 그룹 생성 가능
- RDS 콘솔에서 OS 패치 프로세스의 취약점을 확인할 수 있음
- 프록시 프로토콜은 연결을 요청한 소스에서 연결이 요청된 대상으로 연결정보를 전달하는데 사용되는 프로토콜
- Redshift 는 연결 로그, 사용자 로그, 사용자 활동 로그를 기록함

- Kinesis Data Stream 은 서버측암호화를 통해 CMK 를 사용하여 데이터를 저장하기 전에 자동으로 암호화함

* 추가 테스트 1

- AWS 의 리소스 변경사항을 확인하고 구성규식 및 준수 여부를 확인하는 서비스는 AWS Config
- Cloudwatch 가 수신하고 집계하는 데이터의 최소 단위는 1 초
- RDS 의 Describe Event 를 통해 Failover 시 이벤트를 생성할 수 있음
- NACL 은 AZ 가 아닌 서브넷과 연결되어 있음
- DR 솔루션 중 Multi Site 가 가장 비싸며 Pilot Light 가 가장 저렴
- 여러 AZ 에 걸쳐 최소 및 최대 사이즈를 1 로 한 Autoscaling 을 Bastion Host 로 구성하면 가용성을 높일 수 있음
- S3 에 저장된 객체를 다른 사람과 공유할 경우, 가장 안전한 방법은 Pre signed URL
- S3 의 ACL 에 다른 AWS 계정의 읽기 / 쓰기 권한을 부여할 수 있음
- Auto Scaling AddToLoadBalancer 를 일시 중단한 경우 일시 중단한 기간 인스턴스는 ELB 에 수동으로 등록해야함
    - AS 와 ELB 가 연결된 상태임
- Windows 기반 인스턴스 스토어 AMI 는 EBS 기반 AMI 로 변환 불가
- 매일 일정시간동안 사용되는 인스턴스는 Scheduled Reserved Instance 가 좋음
- AS 의 예약된 작업의 시간은 고유해야함, 각 작업이 겹칠 경우 충돌이 발생
- 인스턴스의 인터페이스에 다중의 탄력적 IP 를 설정하여 사용 가능
- 지리적으로 나뉘었다 하더라도 성능관련해서는 지연 시간 기반이 맞는듯
- ELB 에 고정 IP 주소를 지정할 수 없음
- Memcached 의 Evicition 이 높을 경우 Scale out and up 이 답
- Cloudwathc 의 데이터 보존 기간 확인
- S3 에서 호스팅된 애플리케이션이 DynamoDB 에 액세스할 경우 데이터에 액세스하기 위한 API 키 유지 방법
    - 웹 자격 증명 연동을 사용하여 사용자를 인증하고 임시 자격 증명을 통해 올바른 DynamoDB 자격 증명에 액세스 가능
- RDS Oracle 을 사용할 경우, 매일 자동 백업을 사용하여 백업하고 파일 레벨 백업을 S3 로 보완
- 청구 금액이 할당된 예산을 초과할 경우 알림을 보내려면 Cloudwatch 사용

* 추가 테스트 2

- S3 액세스 거부는 4xx 에러(403) 반환
- 정적 MAC 주소는 ENI 생성을 통해 얻을 수 있음, ENI 의 MAC 은 변경되지 않음

- Autoscaling 의 조정 프로세스에는 재부팅이 존재하지 않음, AZRebalance 는 존재
- ELB 의 가용영역은 콘솔에서 즉시 추가 가능
- Autoscaling 은 Replacehealthy, AZRebalance, AddToLoadBalacner 등을 지원
- EC2 인스턴스 연결시간 초과 오류 : 보안그룹, 라우팅 테이블, CPU 사용량, ACL
- EC2 인스턴스 호스트 키를 찾을 수 없음 : 각 OS 별 고유 이름 적지 않음
- AWS Organization 의 경우, 마스터 계정이 기존 계정을 초대해야 통합 결제가 가능
- AMI 의 경우, 권한까지 복사되지 않음
- EBS 볼륨에 대해 IOPS 가 0 이고 비어 있지 않은 대기열이 있다면 볼륨을 사용할 수 없다는 뜻
- Opsworks 의 구조 : 스택 > 레이어 > 인스턴스
- OS, 네트워크, 방화벽 구성은 고객의 책임
- EBS 의 경우, DLM 을 활성화하면 자동 백업이 가능
- 짧은 기간의 Spike 의 경우, 온디맨스 인스턴스를 사용하는 것이 바람직
- Aurora 에서 읽기복제본을 사용할 경우, 리더 엔드포인트를 가리키게 되어있음(클러스터 엔드포인트는 DB 인스턴스)
- MySQL, PostgreSQL, MariaDB 만이 리전간 읽기 전용 복제본을 지원(oracle 불가)

* 추가 테스트 3
- 1~2 분 단위 모니터링은 세부모니터링으로 가능하며, CloudWatch Event 를 통해 인스턴스 재시작 가능
- 일괄처리 작업은 스팟 인스턴스가 적합(주중, 주말 가끔 실행 작업)
- CloudFormation 을 업데이트할 경우, WaitOnResourceSignals(UpdatePolicy) 속성을 사용하면 업데이트 중 새 인스턴스의 신호를 대기함
- MFA Delete 가 활성화된 경우, 객체 버전을 영구히 삭제하거나 버킷의 버전 관리 상태를 변경해야 함
- CloudFormation 의 기본 동작은 오류시 롤백
- 인스턴스의 종료 이유는 설명 내 상태전환이유 항목에서 확인 가능
- 보호되지 않은 키 파일 오류 : 개인 키 파일에 잘못된 권한이 있음
- VPN 을 사용하는 경우, Virtual Private Gateway 에 대한 라우팅 테이블이 있어야 함
- Cloudwatch, 청구 경보를 통해 지출 한도 초과시 메일 전송 가능

* 추가 테스트 4
- S3 의 리소스에서 특정 작업을 수행하려면 리소스를 소유한 계정과 IAM 계정이 소속된 상위 계정 권한 모두 필요
- ELB Source 보안 그룹에 액세스할 수 있는 EC2 의 보안그룹 생성시 ELB 로만 접속 가능

- 스냅샷에서 새로운 볼륨 생성시 볼륨 크기는 줄일 수 없음
- VPC 와 온프레미스 데이터 센터가 겹치면 통신 불가능!!
- Cloudwatch 에 의해 트리거하여 SNS 을 통해 이메일로 알람을 받을 수 있음
- ELB health check 는 인스턴스 상태만을 확인하기 때문에, ELB 활동에 대한 정보는 제공하지 않음
- Cloudfront 502 에러는 원본 서버 연결 에러
- Autoscaling 시 인스턴스에 사용자 지정 지표를 삽입해야하는 경우, PutMetricData 권한으로 IAM 을 생성하고 시작구성을 수정
- 클러스터 배치그룹은 단일 영역 내의 그룹
- 스택 생성 실패시 수행할 작업은 DO_NOTHING, ROLLBACK, DELETE
    - 기본 정책은 ROLLBACK
    - DO_NOTHING 은 수동으로 오류 정정
- ElastiCache 의 CurrConenctions 은 그저 커넥션 숫자만을 표시

* 추가 테스트 5
- ELB 의 액세스 로그에는 backend_processing_time 을 통해 대기시간을 확인할 수 있음(인스턴스 지연 확인)
- AMI 는 다른 리전에서 액세스할 수 있도록 허용 불가능
- Cloud HSM 은 비대칭 키를 지원함
- RDS 는 콘솔을 통해 패치 프로세스(유지 관리 상태)를 확인할 수 있음
- RDS multi-AZ 는 Standby 의 경우 실행하지는 않음 -ㅅ-;;
- RDS 인스턴스 스토리지 확장시(혹은 DB 업데이트 실행시) 이벤트 순서
    1. Standby 에서 스토리지 확장(DB 업데이트) 수행
    2. Standby 를 Primary 로 승격
    3. 기존 Primary 를 Standby 로 격하 후 Standby 수행
- 알람 동작을 테스트해보려면 CLI 에서 알람 상태 지정 가능
- RDS 이벤트를 통해 DB 보안그룹에서 이벤트 작성 가능
    - RDS 이벤트 유형에는 인스턴스, 파라미터 그룹, 스냅샷, 보안그룹, DB 클러스터, 스냅샷이 있음
- Autoscaling 을 삭제하기 전에 최소 크기와 목표 용량을 0 으로 만들어 인스턴스를 지움
- 특정 사용자가 특정 리소스를 종료하지 못하게 하는 방법은 태그를 지정하여 해당 태그가 있는 경우 종료를 거부하도록 하는 것
- Cloudformation 의 스택은 단일 단위로 관리할 수 있는 AWS 리소스의 모임
- Cloudformation 에서 Ref 함수를 사용할 경우 인스턴스의 ID 를 전달하면 Ref 가 인스턴스 ID 를 반환함

* 추가 테스트 6
- EFS 는 파일 시스템 생성시 유휴 데이터 암호화 활성화 가능
- IAM 의 자격증명보고서를 통해 계정 내 모든 사용자의 자격 증명 상태 확인 가능
- Codepipeline 을 통해 CF 템플릿의 모든 변경사항의 사전/사후 검사를 실행할 수 있음
- Storage Gateway 를 KMS 와 통합하여 유휴 데이터를 암호화할 수 잇음
- AWS Config 는 퍼블릭 액세스 권한이 있는 S3 버킷이 생성된 경우 모니터링 / 경고 가능
- EC2 의 세부 모니터링이 인스턴스에 대한 통계를 집계할 수 있음
- Redshift Enhanced VPC Routing 을 사용할 경우 클러스터와 데이터 리포지토리 간의 모든 COPY, UNLOAD 트래픽이 VPC 를 통해 이루어짐
- EC2 에서 Redshift Cluster 로 연결하지 못할 경우, 클러스터 보안 그룹에서 수신규칙을 수정해야 함
- AWS 서비스에 권한을 전달하려면 사용자에게 서비스를 '전달할 권한(PassRole)'이 있어야하며, 서비스가 역할을 맡을 Trust Policy 필요
- 종료 방지 기능이 활성화된 상태에서, 시작 종료 동작을 종료로 바꾼 경우 종료함
- 인스턴스가 중지된 상태에서 재시작시 새 호스트로 마이그레이션됨
- 'DisableApiTermination'를 통해 실수로 종료되지 않도록 설정 가능
- 사용자정의 CloudWatch 지표!!!
- 5분 이내에 안정적으로 DB를 복원할 수 있는 방법은 'RDS 자동 백업'