**자격증명 및 엑세스 관리 AWS 스토리지**

IAM S3

EBS

**AWS 컴퓨팅기능** EFS

EC2 StorageGateWay

ECS

Lambda **네트워킹**

LightSail VPC

Direct Connect

**DB 밸런싱**

RDS LoadBalancing

DYNAMODB AutoScailing

RedShift

Elastic Cache

**컨텐츠전달, DNS 모니터링**

Route53 CloudWatch

CloudFront CloudTrail

**알람서비스 마이그레이션, 전송**

SNS DMS, SMS, Snowball

**클라우드 거버넌스, 보안**

GuardDuty, KMS, CloudHSM, Inspector, Config, ServiceCatalog

Waf&Shield, Artifact, TrustedAdvisor, Personal Health DashBoard

클라우드 6가지 이점

1. 가변비용의 축소

2. 대규모 경제로 인한 이점 -> 변동비용의 절감

3. 용량에 대한 추측x -> 자유로운 확장과 축소

4. 빠른 속도와 민첩성 -> 쉽고 빠르게 사용이 가능하다

5. 데이터센터의 운영 및 유지보수 필요x -> 비즈니스에 집중 가능

6. 짧은 시간에 가능한 글로벌화 -> 전 세계 여러 지역에 손쉽게 APP구축 가능

AWS 글로벌 인프라

Region - 2개 이상의 AZ로 구성, 다른 리전과 격리됨

AZ – 하나 이상의 PC, 물리적으로 분리되고 다른 AZ와 격리됨

엣지로케이션 – CloudFront별 사용자에게 기능을 제공할 컨텐츠 캐시가 있는 장소

Region edge cache – 서비스 및 edge의 위치에 대한 캐시

IAM

* IAM은 글로벌 서비스로 사용자 또는 서비스를 나타내는 개체이다.
* API, SDK, CLI, DEVTools에 대한 프로그래밍 방식 액세스를 위한 ID및 보안 액세스 할당
* 관리 콘솔에 엑세스 하기위해 비밀번호 할당이 가능하다.
* 디폴트 계정은 엑세스 할 수 없다.

루트계정

* 계정 및 암호를 생성하는데 사용되는 이메일
* 전체 관리에 대한 권한이 있으며 제한받지 않는다.
* 공유를 최소화하고 주로 사용을 최소화한다.

IAM GROUP

* IAM 그룹은 사용자들의 모임이며 정책들이 연결되어 있다.
* 그룹을 사용하여 사용자에게 권한을 할당한다.
* 권할을 할당할떄는 최소의 권한만 할당하는 것이 좋다
* 그룹내에서 그룹을 중첩할 수는 없다.

IAM Roles

* 신뢰 할 수 있는 엔티티가 역할을 만든다.
* 권한집합을 정의한다.
* 역할을 사용하면 영구적인 사용없이 사용자와 서비스의 리소스에 대한 사용권한을 관리
* 권한을 위임 할 수 있다.

IAM Policy

* 정책은 권한을 정의하고 사용자, 그룹, 역할에 적용될 수 있는 문서이다.
* JSON형식으로 작성한다
* 모든 권한은 디폴트에 의해 임시적으로 거부된다.
* 되도록이면 가장 제한적인 정책이 적용된다.
* 3가지 인증방법이 있다 (키, 콘솔, 서버인증서)

엑세스 키

* 엑세스 키 ID와 PASS 엑세스 키의 조합이다.
* API나 CLI를 사용하여 호출한다.
* 비밀 엑세스는 생성시에만 리턴된다.

콘솔비번

- AWS MANGE CONSOLE과 같은 대화형 세션에 로그인 할 떄 사용한다.

- 사용자가 자신의 비번 변경이 허가된다.

서버인증서

* 일부 서비스를 사용시 사용한다.
* MFA(다단계인증) 계정에 추가보안을 설정한다.
* STS토큰 제한된 임시권한을 요청할 수 있는 웹서비스 자격증명서이다.

IAM 관리의 정석

* 루트 사용자의 엑세스를 잠금
* 개별 IAM 사용자를 생성하고 관맇나다.
* AWS정책을 정의하여 사용권한을 할당한다,
* 최소권한만을 부여하도록 한다.
* 그룹을 사용하여 IAM사용자에게 권할을 할당한다.
* 엑세스 레벨을 검토하여 IAM권한을 검토한다.
* 암호정책을 강력하게 한다.
* MFA를 설정한다
* 정지적으로 자격정책을 수정한다
* 불필요한 정책은 제거한다
* 보안을 위한 정책을 설정하고 계정 모니터링을 설정한다.

IAM문제

1. 엑세스 키와 비밀 엑세스키가 연관된 IAM 개체는 IAM USer이다.

User에 엑세스 키 ID 및 보안 엑세스 키를 할당 할 수 있다.

2. 루트 사용자의 증명은 이메일 주소 형식이다.

3. ARN은 Amazone resources name의 약자이다.

4. 사용자와 그룹에 권한을 할당 시에는 최소권한을 할당하는 것이 좋다

5. 권한을 위임시에는 Roles

정책®은 역할을 사용하여 위임하고 정책(p)을 통해 역할에 대한 권한을 정의한다.

6. 디폴트 유저는 권한없이 생성이 가능하며 그 후 그룹, 정책에 의해 권한을 할당한다.

EC2

* Elastic Compute Cloud
* Aws의 대표컴퓨팅 기능
* 클라우드에서 안전하고 확장 가능한 컴퓨팅 용량을 제공한다.
* Elastic Web Scale은 몇 분안에 용량을 늘리거나 줄일 수 있다.
* 각 인스턴스에 대한 루트 엑세스를 포함하여 완전한 제어권한을 가지며 시작 중지를 할 수 있다.
* 여러 종류의 인스턴스 유형과 OS, 메모리, CPU, 스토리지 구성이 존재한다.
* APP요구사항에 따라 인스턴스의 CPU, RAM, 디스크, 네트워크처리량등을 선택한다.

AMI

* 인스턴스를 시작하는데 필요한 정보를 제공한다.
* 하나 이상의 EBS 스냅샷, 인스턴스 저장소 지원, 인스턴스의 루트볼륨에 대한 템플릿(OS< APP, APP SERVER), 시작권한, 볼륨을 지정하는 매핑 시스템이 필요하다.
* 3가지의 AMI가 있다. (Community, marketplace, My)
* Community AMI는 무료로 사용할 수 있으며 일반적으로 원하는 OS사용이 가능하다.
* Market은 비용을 지불하여 라이선스가 부여된 추가 SW패키지를 제공한다.
* MYAMI는 내가 직접 생성한 AMI이다.

UserDate

* 스크립트 형식으로 인스턴스 실행 시 사용자가 제공하는 데이터
* 16KB로 제한된다.
* 암호화되지 않음

MetaData

* 실행중인 인스턴스에 대한 데이터
* 인스턴스 메타데이터 관리도구를 사용하면 전체 URI 또는 카테고리 이름을 입력하지 않고도 메타데이터를 사용한다.

ECS

* Elastic Container Service
* 확장성이 뛰어난 고성능 컨테이너 관리기능
* 도커 컨테이너를 지원한다.
* 자체 클러스터 관리, 인프라설치, 운영, 확장 등을 할 필요가 없다.
* 컨테이너는 가상 인스턴스와 유사하며 코드, 런타임, 툴, 라이브러리, 옵션들이 패키지화 된다. 한 컴퓨팅 환경에서 가른 컴퓨팅 환경으로 실행이 가능하다.
* ECS의 유형에 따라 EC2, Fargate옵션이 존재한다.
* ECS(EC2)는 인스턴스를 명백하게 공급하며 EC2풀의 업그레이드 패치 관리 담당하며 클러스터 최적화가 필요하다, 인프라를 보다 세부적으로 관리한다.
* -ECS(Far)는 제어플레인은 리소스 요청, 파게이트는 자동공급, 파게이트의 피료에 따라 프로비저닝을 담당한다, 파게이트가 클러스터 최적화 처리를 담당하며 자동화 기능에 따라 제어기능이 제한되어 있다.

Lambda

* 서버를 프로비저닝이나 관리없이 코드를 실행할 수 있는 서버리스 컴퓨팅 기술이다.
* 필요한 경우에만 코드를 실행하고 자동으로 확장이 가능하다.
* 사용한 컴퓨팅 시간에 대해서만 요금을 지불한다.
* 지속적인 확장이 가능하며 대부분의 AWS서비스와 통합, 초 단위를 측정이 가능하다.

LightSail

* 기술지식이 없는 사용자에게 적합하다.
* 매우 쉽게 컴퓨팅 서비스를 프로비저닝 한다.
* 개발자에게 클라우드에서 web,app,유를 배포하고 관리 할 수 있는 컴퓨팅 스토리지 네트워킹 용량과 기능을 제공
* 가상머신 SSD기반 스토리, 데이터전송, DNS, Static IP등 프로젝트를 시작하는데 필요한 것을 포함한다.
* DB구축 적용에 필요한 모든 것을 포함하는 가상 프라이빗서버 제공
* 인스턴스, DB를 생성하고 Static, DNS, LB, 스토리지, 스냅샷등을 구성한다.

COMPUTING문제

1. EC2의 이점은 용량을 탄력적으로 늘리거나 줄일 수 있다.

2. 메타데이터는 인스턴스에 대한 정보 인스턴스가 있는 AZ,IP등을 알 수 있다.

스냅샷은 백업으로 사용할 수 있는 EBS볼륨의 복사본이다.

사용자데이터를 사용하여 EC2 인스턴스 시작시 명령실행이 가능하다.

3. ECS – 컨테이너

함수 – 람다

가상하드드라이브 - EBS

4. EC2는 프로비저닝하는 인스턴스를 관리한다.

라이트세일은 프로비저닝 하는 인스턴스를 관리

ECS(Ec2)는 Ec2컨테이너 인스턴스를 관리

람다는 서버리스, 코드, 함수를 위한 서버이며 인스턴스 유형에 선택이 없다.

5. S3는 객체 기반 스토리지

EFS는 파일기반 스토리지

EBS는 루트볼륨기반 스토리지

STORAGE GATEWAY는 ONPREMISS와 AWS간의 HYBRID이다.

S3

* Simple Storage Service
* 웹 모바일 iot app등 모든 데이터를 저장하고 검색하도록 구축된 객체 스토리지
* 모든 파일을 저장하며 내구성이 훌룡하다.
* 백업 및 저장, APP호스팅, 미디어 호스팅, SoftWare Delivery, 정적 웹 사이트 구성 등
* 파일은 버킷에 저장된다.
* 0~5TB 까지 저장가능하며
* 파일수의 제한은 없다
* 이름은 전역적으로 고유해야 한다.
* 지연시간을 줄이기 위해서는 가장 가까운 리전에 버킷을 설치한다.
* 객체의 구성요소로는 키, 값, ID, 메타데이터로 구성된다.
* 6개의 클래스가 존재한다.
* Standard : 내구성 즉시사용 빈번한 엑세스에 사용한다
* Intelligent tier : 데이터를 가장 비용 효율적으로 저장한다.
* Standard IA : 내구성, 즉시사용, 간헐적 엑세스에 사용한다.
* One Zone IA : 내구성이 떯어지며 간헐적 엑세스에 사용하며 비용이 저렴하다.
* Glacier : 데이터 보존시 사용하며 비교적 짧은 서치
* Glacier deep Archive : 장기보존, 가장 저렴한 클래스이다.

S3의 기능

* Transfer Accelataion : CloudFront를 역으로 사용하여 데이터 업로드 속도를 향상
* Request Pay : 요청자가 요청 및 데이터 전송 비용을 지불한다.
* Tag : 비용, 청구, 보안 등에 사용할 객체에 태그
* 이벤트 : 버킷에서 특정 이벤트 발생 시 SNS, SQS, Lambde에 알림
* 정적 웹 호스팅 : 간단하고 확장성이 뛰어나다.
* Bit Torrent : .torrent 파일을 자동생성 공개적으로 사용가능한 개체검색 프로토콜

S3 버전관리

* 동일한 버킷에서 객체의 버전관리 유지
* 언제든지 활성화 가능
* 일시중지 가능
* 버킷에 있는 객체의 보존, 검색 및 복원하는데 사용한다.

S3 복제

* 다른 리전이나 동일한 리전에 객체를 복제 할 수 있다.
* CRR은 다른리전에 복사
* SRR은 동일한 리전에 복사
* 먼 거리에도 데이터 저장 가능
* 가까운 거리의 사용자는 시간을 최소화하며 백업에 대비한다.

EBS

* EC2 인스턴스와 함께 사용할 영구적인 블록스토리지, 볼륨을 제공한다.
* 볼륨은 AZ 내에서 자동으로 복제되어 장애로부터 보호되며 가용성과 내구성이 좋다.
* 볼륨데이터는 인스턴스 수명과 무관하게 유지된다.
* 볼륨은 인스턴스에 연결할 필요가 없다.
* 한 인스턴에 여러 볼륨을 연결할 수 있다.
* 볼륨을 여러 인스턴스에 연결은 불가능하다.
* 볼륨은 연결된 인스턴스와 동일한 AZ에 위치하여야 한다.
* Termianation보호는 기본으로 해제되어 있으며 수동으로 활성화가 필요하다.
* 루트EBS 볼륨은 기본적으로 종료시 삭제된다.
* Extra non-boot volume은 기본적으로 종료시 삭제되지 않는다.
* Delete Termination에서 속성을 변경가능하다.

인스턴스 볼륨

* ISV는 EC2가 실행되는 호스트시스템에 물리적으로 연결된 고성능 로컬디스크
* 인스턴스 스토어는 전원을 끄면 데이터가 손실된다.
* 인스턴스 스토어는 버퍼 캐시 스크래치 데이터와같이 자주 변경되는 정보를 저장하는데 좋다.
* ISV 루트장치는 S#에 저장된 AMI 탬플릿에서 생성
* 인스턴스 스토어는 재연결, 분리가 불가능하다.

EBS스냅샷

* 인스턴스의 특정 시점, 상태를 캡처
* S3에 저장된다.
* 세분화된 백업은 제공하지 않는다
* 볼륨은 AZ마다 다르고 스냅샷은 리전에 따라 다르다

EFS

* 파일스토리지를 쉽게 설정하고 확장 할 수 있는 완전관리형 서비스
* 파일시스템 인터페이스 제공, NFSv4.1 프로토콜 사용
* 빅데이터분석, 미디어처리, 워크플로우, 컨텐츠관리, 웹서비스 홈디렉터리에 사용
* EFS 데이터는 한 리전 내에 여러 AZ에 저장된다.
* Write 일관검사 후 Read
* 사용한 만큼 시불하며 사전 프로비저닝은 없다.
* 탄력적이며 여러 AZ에서 최대 1000개의 EC2 인스턴스와 동시 연결된다.
* 파일시스템은 해당 리전의 모든 AZ에 동시에 엑세스 된다.
* 디폴트 계정당 10개의 파일시스템 생성이 가능하다.
* Direct Connetct와 VPN을 통해 온프레미스 엑세스 가능
* 인스턴스는 ELB 뒤에 위치한다.
* Genera 모드는 대부분의 파일시스템에 사용
* MAX I/O는 여러 개의 EC2 인스턴스가 파일시스템에 액세스 하는 APP에 사용

Storage 문제

1. S3는 Object스토리지, EBS는 블록스토리지, EFS는 파일스토리지이다

2. S3의 루트수준 컨테이너는 버킷이다.

3. 볼륨은 가용영역과 함께 저장된다.

4. AWS Gate Storag는 클라우드 스토리지에 온프레미스 엑세스를 제공하는 하이브리드 클라우드 서비스이다.

5. 디폴트 설정에는 EC2 인스턴스가 종료된면 루트EBS볼륨은 삭제된다.

6. 리눅스 AMI만 EFS사용

VPC

* Virtual Private Cloud
* 자체 DC를 가진것과 비슷
* 다른 가상 네트워크와 논리적으로 격리된다.
* IP범위, 서브넷, 라우팅테이블, 게이트웨이 구성등 네트워킹 환경을 조정
* VPC 생성시 CIDR 블록 형태의 IPv4로 주소가 지정된다.
* VPC는 해당 리전의 모든 AZ에 걸쳐있다.
* 기본적으로 리전당 최대 5개의 VPC를 생성 가능
* 각 AZ에 서브넷이 잇는 리전에 기본 VPC가 존재한다.
* 안전옵션으로는
* AWS Managed vpn 빠른설정
* Aws direct connection 광대역, 짧은 지연시간, 설정 시 몇분
* Cloud Hub 여러사이트를 AWS에 연결
* Software VPN 타사 Sw사용

Direct Connect

* 인터넷을 사용하여 고객의 온프레미스 사이트를 aws에 연결하는 네트워크 서비스
* 하이브리드 클라우드 생성에 사용한다.
* 데이터 전송은 Aws와 고객의 데이터센터 또는 기업의 사설 네트워크 연결을 통해 전송됨
* 장점으로는 대량의 트래픽사용시 비용절감
* 신뢰성 향상, 대역폭증가, 예측가능한 상능, 지연감소, 1Gbps ~ 10Gbps사용
* 포트시간이나 데이터 전송에 따라 요금지불

보안그룹

* 인스턴스 레벨 방화벽
* 허용규칙
* 상태저장
* 그룹과 연결된 경우에만 인스턴스에 적용

Network ACL

* 서브넷 레벨 방화벽
* 허용 및 거부규칙
* 상태저장x
* 순서대로 처리
* 연결된 서브넷의 모든 인스턴스에 자동적용

NAT Instance

* 사용자가 관리
* 수동확장, 향상된 네트워킹
* HA불가, 여러 서브넷에서 스크립팅, 자동확장
* 보안그룹 필요
* Bastion 호스트 가능
* 탄력적IP, 공용IP 사용가능
* 수동으로 지정하여 포트포워딩 가능

NAT GateWay

* AWS가 관리
* 최대 45Gbps의 탄력적 확장성
* AZ내에서 HA제공, 여러 AZ에 배치가 가능
* 보안그룹 필요하지 않음
* SSH를 통한 액세스x
* 탄력적IP선택
* 포트포워딩 불가능

Network 문제

1. VPC의 범위는 리전이며 리전 내에서 여러 VPC생성이 가능하다. 리전에 기본 VPC가 있다.

2. 서브넷 수준의 방화벽 NACL(Network Access Control list), 인스턴스 수준의 방화벽은 보안그룹

3. Direct Connect는 AWS 클라우드에 대한 사설 네트워크간 연결이며 안정적인 성능, 높은 대역폭, 낮은 대기시간이 특징이다.

4. 탄력적 IP 주소는 인스턴스가 중지되어도 주소유지되며 비용도 지불한다.

공용IP는 인스턴스 중지 시 삭제된다

5. NAT 게이트웨이는 사설 서브넷의 EC2 인스턴스 연결 (AWS관리)

NAT 인스턴스는 내가 관리한다는 것이다.

6. peering은 두 VPC를 연결하는 방법이다.

Direct connect는 사설네트워크의 연결이며 예측가능한 성능을 제공한다.

DB

OLTP

* 온라인 트랙잭션 프로세싱
* 짧은 트랜잭션 처리
* 관계형 DB - RDS, Oracle, mysql
* 비관계형 DB – Mongodb, Kasandra

OLAp

* 온라인 분석처리, OLTP DB에서 소스를 생산
* 데이터 웨어하우스, 의사결정을 위한 데이터 추출
* 긴 트랜잭션 처리
* 관계형 : RedShift, Teradata
* 비관계형 : EMR, MapReduce

관게형 DB

* 행, 컬럼, 테이블로 구성
* 경직된 스키마
* 수직적 확장
* 복잡한 쿼리 및 조인을 지원한다
* RDS, Oracle

비관계형 DB

* 다양한 데이터 모델
* 유연한 스키마
* 수평적 확장
* 모든 종류의 스키마를 지원하며 구조화되지 않은 언어 사용
* DynamoDB, Mongo DB

DynamoDB

* 원할한 확장성과 빠르고 예측 가능한 성능을 제공하는 완전관리형 NoSQL DB서비스
* Push버튼 스케일링은 다운타임 없이 언제든지 DB를 스케일링 할 수 있다
* 데이터는 한 리전의 3개 AZ에 동기식으로 복제된다.
* 다이나모DB 글로벌 테이블은 다중리전, 다중 마스터 DB 배포를 위한 완전관리형 솔루션을 제공한다
* DAX(Accelator)는 최대 10배 성능 향상을 제공하는 완전관리형, HA 메모리 캐시이다.
* 서버리스 형태로 완전관리, 내결함성 서비스이다.
* HA, 99% 가동성의 서비스이다.
* 이름/값 구조를 가지는 Nosql 유형의 DB
* 유연한 스키마를 가진다.
* 수평확장, PUSH스케일링, 오토스케일링을 통해 원할한 확장가능
* Nosql DB, 완전관리형, 확장성, 비관계형, 수평적 확장, 비정형데이터, 유연한 스키마
* DAX를 통한 성능향상

RDS

* Relation Database Service
* 클라우드에서 관계형 DB를 쉽게 설정, 운영, 확장 할 수 있는 완전관리형 서비스
* EC2 인스턴스를 사용하며 인스턴스의 유형선택 가능하다.
* 관계형 DB, 수직적 확장
* 온라인 트랜잭션처리를 위한 DB, OLTP
* 설치가 쉬우며, 고가용성, 내결함성 및 확장이 가능하다
* 온라인 은행이나 상점등에 적합하다
* 암호화 기술로는 KMS(Key Management System) 사용
* 인스턴스의 크기를 늘려야 확장이 가능하다.
* 멀티 AZ옵션을 통해 내결함성, 에러복구, 자동장애 조치가 가능하다.
* OLTP, 관계형DB, 수직적확장, 운영오버헤드 감소, 다중AZ 사용으로 결함성 확보

RedShift

* 표준 SQL 및 비즈니스 인텔리전스를 사용하여 데이터를 간단하고 효율적으로 분석할 수 있는 완전관리형 데이터웨어하우스
* 분석 프로그램에 사용되는 SQL기반 데이터웨어하우스
* OLAP, 유스케이스에 사용되는 관계형 데이터베이스
* 비즈니스에 사용되어 많은 양의 데이터를 처리하는데 이상적이다
* EC2 인스턴스를 사용한다.
* 컬럼데이터 스토리지를 사용한다
* OLAP, DW, 관계형DB, 수직적확장

Elastic Cache

* Memcached와 redis 프로토콜 서버를 쉽게 실행하고 배포하는 웹 서비스
* EC2인스턴스를 사용하나.
* In-memory 캐싱으로 읽기 작업이 많은 App의 워크로드, 컴퓨팅에 집중적인 워크로드의 릴레이와 처리량을 향상한다.
* 웹 세션 저장소, DB캐싱, 리더보드, 스트리밍 데이터 대시보드에 사용한다.
* Memcached는 간단한 모델, 스레드로 대형 노드를 실행하며 db같은 개체를 캐싱할 수 있다.
* Redis는 복잡한 모델에 사용하며 암호화가 필요하다 자동장애 조치 및 백업이가능하며 클러스터링을 지원한다. 복잡한 데이터 유형에 사용한다.

APP LB

* 7계층에서 작동, 사용자 요청에 작동한다.
* 요청 내용에 따라 경로가 지정되며 경로기반, 호스트기반, 쿼리문자열기반, IP주소 기반 라우팅을 실시하며
* IP주소 람다 기능 및 컴테이너를 대상으로 지원한다.

Network LB

* 4계층에서 작동하며 IP프로토콜 데이터를 기반으로 연결한다.
* 빠른속도와 짧은 지연시간 규모에 맞는 TLS기능을 제공한다.

Classic LB

* 구닥다리 방식으로 4,7계층에서 라우팅된다, EC2의 클래식 기능에 사용한다.

ELB

* 수신되는 APP 트래픽을 EC2인스턴스, 컨테이너 및 IP주소와 같은 여러 대상에 자동으로 분산한다.
* 단일 AZ 또는 다중AZ에서 APP트래픽의 다양한 로드를 처리한다.
* 내결함성 유지를 위한 HA, 자동확장, 보안기능을 제공한다.
* ALB, NLB, CLB가 존재한다.

Auto Scailing

* 수평적 확장
* 탄력성과 확장성을 제공한다
* 트래픽의 수요에 따라 EC2 인스턴스의 추가 및 제거를 하는 프로세스를 자동화
* ALB 처리 시 사용하는 EC2인스턴스 수량 확보시 도움
* ASG(AutoScailing Group)라는 Ec2 인스턴스 모음을 생성한다.
* 각 ASG에서 최소 인스턴스 수 지정, 최대 인스턴스 수를 지정가능하다.
* 원하는 용량 구성, 인스턴스 맞춤확인이 가능하다.

로드밸런싱 문제

1. ELB는 여러 인스턴스에 배포하는데 사용하며 오토스케일링은 수요 변화에 따라 인스턴스를 조절한다.

2. 도메인기반은 로드밸런싱은 ALB

3. ELB는 인스턴스간 부하를 균등하게 분산하며 오토스케일링은 수요에 따라 인스턴스를 처리한다.. 처리하는 인스턴스만 요금을 지불한다.

4. ELB는 여러 백엔드 인스턴스에 연결을 분산,

오토스케일링은 적절한 수의 인스턴스 사용으로 내결함성 유지

5. ELB는 AZ에 배포하며 인터넷 연결, HA, 내결함성 유지가 있다

6. ELB HealthCheck는 인스턴스가 사용가능하고 정상인지 확인한다.

7. 4계층 로드밸런싱은 NLB

8. ASG는 EC2인스턴스의 모임이다.

Router53 DNS record types

Simple

* 이름과 관련된 IP주소를 제공하는 Simple DNS 응답 서비스

Failover : 기본이 다운된 경우 보조대상으로 라우팅

Geolocation : 현재있는 지리적 위치를 사용하여 가장 가까운 리전으로 경로안내

Latency : 지연시간이 가장 짧은 리소스 경로를 기반으로 안내

Multivalue answer : 로드밸런서로 여러 IP 주소 및 기능을 리턴한다

Weighted : 자원 할당된 상대적 가중치를 사용하여 라우팅한다.

Router 53

* Aws의 DNS 서비스이다.
* 글로벌 서비스
* 3가지 주요기능으로는 도메인등록, DNS(주소를 IP로), 핼스체크등이 있다.
* DNS 패일오버는 시스템 장애 시 도메인 엔드포인트를 자동변경한다
* 라우팅 정책은 Router53 DNS가 쿼리에 응답하는 방식을 결정한다.
* 지역간에 트래픽을 전달한다.

CloudFront

* 전 세계 위치한 엣지로케이션에 컨텐츠를 저장(캐시) 할 수 있는 컨텐츠 전송 네트워크(CDN)
* 고객은 컨텐츠에 더 빠르게 엑세스하고 DDOS에 보호
* 데이터 비디오 APP API등에 사용한다.
* 고객에게 빠른 배포를 위해 엣지로케이션에서 컨텐츠를 캐시한다.
* S3, EC2, ELB, ROUTER53 LAMBDE와 통합가능
* 엣지로케이션은 CloudFront와 Router53의 캐시서버이다.

DNS 문제

1. CloudFront를 사용하여 전 세계 엑세스 하며 사용자들의 성능을 향상시킨다.

2. 리전엣지캐시는 CloudFront와 엣지로케이션 사이에 존재한다.

3. CloudFront의 지원유형은 S3버킷, Ec2인스턴스, 라우터53이 있다

4. IAM, CloudFront, Router53은 글로벌 서비스이다.

5. Router53의 기능은 상태확인, DNS, 도메인등록 등이 있으며 Route53 레코드의 모음을 hosted zone이라고 한다.

6. CloudFront는 DDOS를 보호해준다.

7. CloudFrontEdgeLocation은 사용자에게 더 가까운 데이터를 제공하기 위해 데이터를 캐시하는데 사용한다.

CloudWatch

* 클라우드 리소스, 실행중인 APP에 대한 모니터링 서비스이다.
* 성능모니터링을 담당한다.
* 메트릭스를 수집, 추적하고 로그파일 수집, 모니터링, 경보설정에 사용한다.
* 리전 서비스이다.
* 알람은 리소스의 변경에 대응하여 설정한다.
* CloudWatchEvent는 리소스 상태가 변경될 떄 이벤트를 생서하고 대상에게 제공한다.
* 로그는 리소스에서 가져오며 중앙집중형이다.
* 자원활용에 대한 시스템 전반의 가시성을 확보한다.
* 모니터링에서 app성능이 포함된다.
* Ec2 인스턴스 비정상 사용에 대한 경고가 가능하며 대부분의 AWS서비스와 통합된다.

CloudTrail

* 계정에서 이루어진 활동을 기록하고 S3버킷에 로그파일을 전송하는 웹 서비스이다.
* 감사를 위한 서비스이다
* 로깅에 관한 서비스이며 API호출 기록을 저장한다.
* 계정에서 수행한 작업을 기록하여 사용자 활동에 대한 가시성을 제공한다
* API기록을 통해 보안분석, 리소스변경, 추적 및 규정준수에 대한 감사를 실행한다
* API호출 기록수단으로 관리콘솔, SDK, 커맨드라인툴, CloudFormation이 있다.
* API활동 정보기록을 감사한다.
* 기본적으로 90일 동안의 레코드만 보고나되며 영구적으로 유지하기 위해서는 Tracer를 생서하고 S3버킷에 이벤트를 기록하여야 한다.

CloudFormaion

* 클라우드 환경의 모든 인프라 리소스를 설명하고 프로비저닝 할 수 있는 공통언어를 제공한다.
* 광범위한 AWS리소스를 프로비저닝 하는데 사용가능
* 인프라 스트럭처를 코드로 구축한다
* 코드를 사용하여 인프라를 배포한다.
* 대부분의 AWS서비스를 배포하는데 사용한다
* JSON이나 YAML 템플릿 파일을 사용한다.
* 빈스톡 환경에 배포가능하다.

BeansTalk

* 웹 앱을 간편하게 사용하며
* Ec2(Paas)에 APP을 배포한다.
* JAVA, .NET, PHP, NodeJS, Python 및 도커를 기반으로 웹 App을 배포한다.
* Zip, Git, WAR파일 형식을 사용한다.
* 빈스톡은 CloudFormation을 사용하여 배포가 불가능하다.
* 빈스톡을 사용하면 AWS클라우드에서 APP을 빠르게 배포하고 관리할 수 있다.
* APP을 업로드하고 빈스톡으로 용량 프로비저닝, 로드밸런싱, 자동확장, 상태모니터링 배포정보등을 처리한다.
* Paas 솔루션이다

자동화 및 플랫폼 문제

1. 조직의 일관성을 위해서는 동일한 템플릿을 사용한 것이 좋으며 일관성 유지를 위해 CloudFormaion의 템플릿기반 프로비전닝을 추천

2. 빈스톡은 APP을 빠르게 배포하고 관리가 가능하다.

3. CloudForamtion은 코드를 사용하여 인프라를 배포하고 JSON이나 YAML 템플릿을 사용한다.

빈스톡은 Zip, Git, WAR파일의 형식을 사용

4. 빈스톡은 CloudFormation을 사용하여 서비스를 배포할 수 잇다.

5. 빈스톡은 Paas 솔루션이다.

6. CloudFormation은 VPC를 생성하고 다양한 리소슬 리반으로 하는 전체 프로세스 자동화가 가능

Migration

DMS

* Database Migragtion Service
* 온프레미스 환경에서 EC2, RDS에 DB를 마이그레이션하는데 사용한다.
* 같은 종류의 전송(Oracle – Oracle), 이기종(Oracle – Aurora) 전송을 지원한다.
* 데이터는 APP이 실행되는 동안 지속적으로 복제되어 다운타임이 최소화된다.
* 마이그레이션, 로그저장 중에 사용된 컴퓨팅 리소스를 기준으로 요금을 지불
* 완전관리 서비스이다.

SMS

* Server Migration Service
* 온프레미스나 클라우드 기반 VM을 AWS로 마이그레이션하기위한 서비스
* 에이전트가 필요없다
* VMware, Hyper-V, MsAzure 플랫폼 사용이 가능하다.
* 서버볼륨을 복제되고 AMI로 저장하며 EC2 인스턴스로 시작가능
* APP그룹을 사용가능

DataSync

* 온프레미스 NAS스토리지와 S3, EFS와 연결이 가능하다
* TLS암호화를 사용하는 데이터를 전송
* NFS와 SMB프로토콜을 사용한다
* 기존툴링보다 최대 10배 빠르게 데이터 전송성능을 향상
* 퍼미션과 메타데이터는 보존된다
* 이체된 GB당 요금을 지불한다.

Snowball

* 온프레미스 DC와 S3간에 수백 테라바이트, 페타바이트의 데이터 전송을 지원
* 물리적 운송을 위한 안전한 저장장치 사용
* 식별, 암호에 사용하는 SW는 Snowball Client이다.
* 256비트 암호화 방식(KMS), TPM 변조방식 암호화 사용
* SnowBall(80TB, 50TB)는 페타바이트 규모
* SnowMobile(100TB)는 엑사바이트 규모에 사용한다

SnowballEdge

* 페타바이트 규모에는 온보드 스토리지, 컴퓨팅 기능을 제공
* SnowBall Edge Stoage는 대규모 데이터 전송을 위하 S3호환 객체 스토리, 블록스토리지를 제공하며 옵티마이저가 제공된다.
* Snoball Edge Commpute는 옵티마이저가 제공되지 않으며 고급 머신러닝, 풀모션 비디오 분석, 머신러닝 처리를 위한 컴퓨팅기능을 제공한다.

마이그레이션 문제

1. AWS DMS를 사용하면 온프레미스 DB를 RDS로 마이그레이션 가능

2. SnowMobile(100PB) 엑사바이트 규모의 데이터를 AWS로 마이그레이션 가능

3. 인터넷 연결이 느린회사의 경우 50TB 데이터를 S3로 빠르게 저렴하게 마이그레이션 하기위햇는 SnowBall을 사용한다.

4. DMS는 다운타임 없이 온라인으로 데이터베이스를 마이그레이션 가능하며 다양한 소스, 오브젝트 옵션을 지원한다.

5. 데이터시으는 온프레미스 NAS스토리지에서 S3, EFS로 마이그레이션이 가능하다.

6. SMS는 서버 워크로드를 마이그레이션하며 에이전트가 필요없다

7. S3는 멀티파트업로드는 S3에 업로드하는 대용량 파일을 분할하는데 유용하다.

8. SnowBallEdge는 네트워크가 아닌 물리적 장치를 사용하여 데이터를 마이그레이션

AWS Pricing Model

On – Demand (주문형)

* 컴퓨팅 및 데이터베이스 용량에 사용한다.
* 장기약정 및 선결제가 없다.

Dedicated Instance (전용인스턴스)

* Ec2 인스턴스에 사용한다.
* HW는 단일고객 전용이다.

Spot Instance

* 약정없이 예비용량 구매에 사용
* 시간 단위의 요금에서 할인이 크다

Reservation

* 최대 75% 할인된 교환계약 기관이 있다.
* 1년 또는 3년 기간의 옵션이 있다.

지불옵셔 ( 선불, 후불, 부분선불)

* 사용가능 서비스

EC2 예약인스턴스, DynamoDB예약용량, 엘라스틱캐시 예약노드, RDS 예약인스턴스, Redshift 예약노드

FREE 모델

무료요금

* VPC
* 빈스톡 (생성된 리소스는 제외)
* CloudFormation(“”)
* ID 액세스 관리, IAM
* Auto Scailing(“”)
* 통합결제

EC2 요금구성

* 서버가동시간을 계산하는 시계
* 인스턴스의 구성, 유형, 수량
* Load Balancing
* 상세 모니터링
* Elastic IP주소 (할당 이후에는 계속 청구)
* OS 및 SW패키지

Ec2 요금모델

* On demand
* Reserved instance
* Spot instance
* Dedicate instance
* Savings plan

Ec2(On demand)

* 장기약정이나 선불결제 없이 컴퓨팅 또는 DB용량에 대한 비용지불
* 시간 단위 또는 초단위로 컴퓨팅 용량에 대해 지불한다. (Linux전용이며 ondemand, reserved, spot)
* 선불 또는 장기 약정없이 저렴한 비용과 유연성을 선호하는 사용자들에게 추천
* 중단이 불가피하거나 예측이 어렵거나 수요가 급증하는 워크로드에 적합하다.

Ec2(Reserved)

* 예약 인스턴스는 사전에 용량을 지불함으로써 최대 75의 할인을 해준다.
* 특정 AZ에 적용시 예약 용량을 제공한다.
* 예측가능한 사용량, 예약용량이 필요한 경우, 1~3년 약정이 가능한 고객에게 적합
* 예약옵션은 선불, 부분선불, 후불이 존재한다.

Spot Instnace

* 사전 약정없이 여분의 컴퓨팅 용량을 구입한다.
* 최대 온디멘드의 90%할인이 가능하다.
* 유연한 시작 및 종료시간이 있는 응용 애플리케이션, 매우저렴한 가격으로 구동이 필요한 APP, 많은 추가용량이 필요한 긴급한 컴퓨팅이 필요한 사용자에게 적합하다.

Dedicate instance

* 단일 고객 전용 HW의 VPC에서 실행되는 EC2 인스턴스 맞춤이다.
* 전용인스턴스는 다른 AWS 계정에 속한 인스턴스와 호스트 HW는 물리적으로 격리됨
* 전용 인스턴스는 전용 인스턴스가 아닌 동일한 AWS 계정의 다른 인스턴스와 HW를 공유할 수 있다.

ECS

* EC2 시작유형 사용시 클러스터의 컴퓨팅 인스턴스에 대한 비용을 지불한다.
* Fargate 유형시 컨테이너화된 APP이 요청한 vCPU 및 메모리 리소스에 대한 비용청구

Lambda

* 함수에 대한 요청 수와 코드를 실행하는데 걸리는 시간에 따라 사용한 만큼 지불
* Function에 할당된 메모리에 따라 가격이 다르다

S3

* 클래스 별 스토리지 가격이 다름 (Standard, IA)
* 저장 용량에 따라 다름 (GB기준, 버킷에 저장된 데이터 볼륨)

(50TB, 450TB, 500TB Over)

* 유청의 수량과 유형 (GET, PUT, POST, LIST, COPY)
* LIFE Cycle의 전환 요청 시 – 스토리지 클래스 간의 데이터 요청
* 데이터 전송 : S3 지역에서 전송된 데이터 요금 부하
* 전송가속 시 , 일부 추가 기능에 대한 스토리지 관리에 따른 추가

S3 Glacier

* 매우 저렴한 비용으로 선불 수수료 없이 필요한 만큼 지불
* Glacier 외부로 전송된 요청 및 데이터에 대한 비용청구
* Amazone glacier select 요금을 사용하면 아카이브를 검색하지 않고도 glacier에 저장된 데이터에서 쿼리사용이 가능하다.
* 스캔, 리턴데이터, 양 및 시작된 요청의 수에 따라 가격이 책정
* 아카이브 액세스를 위한 세 가지 옵션
* 신속( 1~5분의 데이터 액세스 시간, 비싼 데이터검색 비용)
* 표준(3~5 시간의 데이터 액세스 시간, 평범한 데이터검색비용)
* Bulk(5~12시간의 데이터 액세스 시간, 가장 저렴한 검색비용, 요청비용)

EBS

* Volume: 매월 프로비저닝된 GB의 양으로 청구된다
* 스냅샷 : S3에서 스냅샷이 사용하는 공간의 양을 기준으로 한다. 스냅샷 복사는 리전 간에 복사된 데이터 양에 따라 청구한다.
* 데이터 전송 : 인바운드 데이터는 무료이며 아웃바운드 데이터는 전송요금이 계층으로 나뉨

EFS

* Standard와 IA가 있다.
* 사용한 저장용량에 대해서 지불한다.
* IA를 사용하면 비용이 절감된다., 프로비저닝된 처리량에 대해서 지불

VPC

* VPC 자체는 무료이며 밑에 서비스는 유료이다.
* SITE TO SITE의 VPN
* AWS Private LINK
* VPC 트래픽 미러링
* NAT 게이트웨이

Direct Connect

* 포트의 사용시간 별로 청구한다
* 아웃바운드 데이터 전송시

수용량 1GB/10GB 포트타임 0.3/2.25

RDS

* 서버가동 계산 시계, DB인스턴스가 실행되는 시간에 따라
* DB엔진, 인스턴스 크기 및 메모리
* DB 구매 유형에는 온디맨드, 예약이 있다
* Request DB에 대한 입력 및 출력 요청의 수에 따라
* 배포유형에 따라 단일AZ or 멀티AZ
* 데이터 전송, 인바운드는 무료, 아웃바운드는 계층화

DynamoDB

* 프로비저닝된 처리량(read, write)
* 인덱싱된 데이터 저장
* 온디멘드 용량모드

App이 테이블에 작성한 read, write에 대해 청구

* 프로비저닝 용량모드

App에 필요한 초당 read, write수 지정, 자동조정을 위한 auto scailing과 함꼐 사용

* 데이터전송, 글로벌 테이블, 예약용량등에 따라 과금

CloudFront

* 트래픽 배포 : 데이터 전송 및 요청에 대한 지불, 지역에 따라 다르며 컨텐츠가 제공되는 엣지로케이션을 베이스로 한다.
* 요청의 수와 유형(HTTP/S) 및 요청이 이루어진 유형에 따라
* 무효화 요청, 필드수준 암호화 요청, 사용자지정 SSL은 추가비용이 들어간다.

Route53

* 호스팅 영역 관리에 대한 월별 요금 청구
* DNS 쿼리, 도메인 네임에 대해

COST TOOL

Cost Explorer

* 비용차트를 볼 수 있는 무료도구
* 지난 13개월 동안의 비용데이터를 보고 향후 3개월 동안 지출 할 가능성을 예측한다.
* 시간이 지남에 따라 AWS리소스에 대한 패턴을 발견, 문제 영역 실벽하는데 사용한다.
* 통계식별에 도움이 된다.(가장 많이 사용하는 서비스, AZ의 트랙픽이 가장많은 매트릭, 가장많이 사용하는 계정 식별)

월별계산기 (simple monthly circulator\_

* 고객과 잠재적인 고객들이 월별 AWS 청구액을 보다 효율적으로 추정하는데 도움이된다.
* 다른 리전에 서비스를 추가 할 수 있다.
* 대부분의 AWS 서비스에 대한 자원을 포함해서 데이터 수신,송신 요금, 데이터 젖ㅇ 요금 및 검색 요금과 같은 추가 내용이 포함된다.
* 다양한 가격 모델로 EC2 전용호스트 및 예약 인스턴스를 선택 가능

TCO (총 소유 비용 계산기)

* 무료도구 이며 클라우드 사용과 온프레미스 데이터센터 사용으로 인한 비용절감을 비교하여 효과적으로 한다.
* HW, 인프라에 대한 자본지출을 방지하여 총소유 비용을 줄인다.
* 비용절감에 대한 지침을 제공한다.
* 현재 예상되는 온프레미스 DC의 비용요소를 입력하고 해당 비용 요구 사항을 AWS에서 발생하는 비용과 비교가 가능하다.
* 원가 절감을 예측하기 위해 프로세스를 진행하면서 요소를 추가하거나 수정할 수 있다.

Plan

Aws 지원 plan

* Basic 청구 및 계정 전용
* 개발자 : 이메일을 통한 업무시간 지원
* 비즈니스 & 엔터프라이즈 : 연중무휴 이메일, 채팅 및 전화 지원
* 엔터프라이즈 지원은 기술계정 관리자(TAM)과 함께 제공
* 개발자는 한 사람이 제한 없이 케이스를 오픈 할 수 있다.

조직 및 통합결제

* AWS Oraganization을 사용하면 여러 AWS 계정을 생성하고 중아에서 관리하는 조직으로 통합가능
* 두 가지 기능세트를 제공한다,

통합결제, ALL Features

* 루트 계정 및 조직단위로 포함하며
* 정책은 루트계정 또는 OU에 적합하다
* 통합결제에는 다음이 포함된다.

Paying계정 : 독립적이며 다른 계정의 리소스에 엑세스가 불가

Connected계정 : 연결된 계정은 모두 독립적이다.

통합결제의 이점

* 여러 계정에 대해 하나의 청구서만 받는다
* 여러 계정에 대한 요금을 추적하고 결합된 비용 및 사용데이터를 다운로드 가능
* 조직의 모든 게정에 대한 사용량을 결합하여 볼륨가격 및 예약 인스턴스 할인등을 공유하며 부서나 회사에 대한 비용을 낮출 수 잇다.
* 추가 비용이 없다

TAG

* AWS 리소스에 연결 할 수 있는 키/값 쌍
* 메타데이터를 포함한다.
* 오토스케일링, 빈스톡, CloudFormation등 생성한 리소스에 대해서 상속된다.

리소스 그룹

* 할당된 태그를 사용하여 리소스를 쉽게 그룹화 한다.
* 하나 이상의 태그를 공유하는 리소스를 그룹화 할 수 있다.
* 리전, 이름, Health Check등과 같은 정보를 포함
* Public & Private IP주소(Ec2), 포트구성(ELB), DB엔진(RDS) 정보 포함

문제

1. 상당한 컴퓨팅 성능과 언제든지 중지 할 수 있는 배치 컴퓨팅워크로드에 적합한 모델은 스팟인스턴스

전용인스턴스는 단일 고객 전용 HW에서 워크로드를 실행 시

예약인스턴스는 1년이나 3년 기간으로 약정 할 수 있는 안정적인 장기 실행 워크로드에 적합하다.

2. EC2 오토스케일링, IAM, CloudFront는 무료 서비스이다.

3. S3의 청구목록으로는 버킷의 용량, 라이프사이클전환, 전송가속, 아웃바운드 전송이 포함된다.

4. 자주 액세스하지 않고 7년 동안 보존되며 24시간 이내에 검색이 가능해야하는 계층은 glacier Deep Archive가 적당하다

5. EFS 스토리지 클래스는 Standard, IA(infrequent access)가 있다.

6. VPC는 무료요금에는 인터넷 게이트웨이, 라우팅테이블, 보안그룹에는 무료이며 VPN은 유료이다.

7. 태그는 비용보고를 위해 AWS리소스에 메타데이터를 할당하는데 사용한다.

8. TCO는 AWS와 온프레미스 데이터센터 사용에 따른 비용절감을 추정시 사용한다.

Cost Explorer는 비용차트를 보는데 사용한다.

통합결제(Consolidated biling)는 여러 계정에서 대량 요금할인을 활용하는데 사용한다.

9. Trusted Advisor는 AWS 모범사례에 따라 리소스를 프로비전이 하는데 도움이 되는 지침을 제공한다.

10. 엔터프라이즈와 기업의 plan에는 기술 계정 관리자(TAM)이 제공된다.

11. TCO 분석 시 온프레밋 DB 운영비용과 aws가 비교될 수 있도록 온프레미스에 발생하는 모든 비용이 포함된다.

12. EC2 인스턴스 결제옵션은 선불 후불 부분선불이 있다.

13. AWS 조직을 사용하면 여러 AWS 계정을 생성하고 중앙에서 관리하며 조직으로 통합이 가능하다.

CloudWatch는 모니터링 도구이며 CostExploree는 비용차트를 보는데 사용하며 13개월 동안의 비용데이터를 보고 3개월 향후 지출가능을 예측한다.

Instegration

SNS

* Simplpe Notification Service
* 간단한 알림 서비스
* 클라우드에서 알림을 설정, 운영 및 전송한다
* CloudWatch 경보 트리거 시 이메일 알림 전송
* 느슨하게 결합된 분산 APP을 구축하고 통합하는데 사용한다.
* 간단한 API를 사용하고 즉각적인 푸시기반 전달을 제공한다.
* 선불비용없이 저렴한 종량제 모델로 제공한다.

SQS

* Simple Queue Service
* 단순 대기열 서비스
* 메시징 대기열, 패턴 저장 및 전달
* 분산된 app빌드에 사용
* 처리 대기중인 메시지를 저장하는 메시지 대기열에 대한 액세스를 제공
* 메시지 지향 API 사용, 풀(pull)기반 polling을 사용한다.

SWF

* Simple Workflow Service
* 외부 프로세스 또는 특수한 실행로직을 지원
* 주문이행 시스템 또는 절차요청과 같은 사람이 사용할 수 있는 워크플로에 사용
* 분산된 비동기 시스템을 워크플로우를 만든다.
* 순차처리와 병렬처리를 지원한다.
* Api를 통해 상호작용하고 업데이트하는 워크프롤의 상태를 추적한다.
* 미디어 처리, 웹 app 사이트 백엔드, 비즈니스 워크프로우, 분석 파이프라인 등 다양한 사용사례를 위한 설계

Step Function

* 시간적 워크플로를 사용하여 서비스들의 구성요소를 조정한다.
* State machine을 구축하고 실행하여 app 단계를 안정적이고 확장가능한 방식으로 실행가능
* 작동원리

JSON기반 STate언어로 워크플로 단계를 정의

앱의 단계와 의도한 대로 작동하는지 시각화, 확인, 각 단계를 실시간 상태로 강조하고 자세한 내역확인

기본 컴퓨팅 단계를 운영 확장하여 수요 증가에 따라 app이 안정적으로 실행되도록 한다.

문제

1. app의 제품업데이트를 알리기 위해 고객에게 SMS 문자메시지를 보내려한다 SNS를 사용한다.

2. 회사는 AWS에서 여러 배치 프로세스를 오케스트레이션 (워크플로우 자동화) 해야한다. 서버리스를 사용해야 할 경우 사용하는 서비스는? Step Function 워크플로 오ㅔ스트레이션 서비스이며 서버리스이다.

3. SQS 대기열을 사용하여 APP 구성요소를 분리할 수 있다. 메시지지향 API를 사용한다.

4. 여러 SQS 대기열에 알림을 보내도록 APP을 구성하기 위해 SNS주제를 사용한다.

Manage and Governance

AWS Config

* 계정에 있는 AWS리소스를 세부적으로 관찰하여 리소스 간의 관계를 분석, 시간의 흐름에 따른 변화를 관찰한다.
* 보안 및 거버넌스를 활성화 하기 위해 AWS 리소스에 인벤토리, 구성기록 및 구성변경의 알림을 제공하는 완전관리형 서비스
* 기존 AWS 리소스를 검색하고 모든 구성의 세부정보와 함께 리소스가 어떻게 구성됫는지를 알 수 있다
* 리소스 구성, 평가,규정준수, 감사, 보안분석, 리소스 변경 추적 및 문제 해결이 가능하다
* ITIL 프로그램의 일부로 구성관리에 매우 유용하다.

CloudTrail

* 계정의 User API 활동을 기록하고 이 활동에 대한 정보에 엑세스 할 수 있도록 한다.
* 누가 이 리소스를 수정하기 위해 API를 호출했는가 알 수 있다.

Config와 차이점

* Config는 리소스에 대한 특정 시점의 세부구성 정보를 구성하여 기록, 리소스가 어떻게 구성됐는가를 알 수 있다.

Ops Works

* Chef 및 Puppet 의 관리형 인스턴스를 제공하는 구성관리 서비스
* 업데이트에는 패치, 업데이트, 백업, 구성 및 규정준수 관리가 포함된다.

Service Catalog

* 조직은 AWS에서 사용하도록 승인된 IT서비스 카탈로그를 생성하고 관리
* 가상머신 이미지, 서버, SW, DB에서 완전한 다계층 app 아키텍처를 포함
* 일반적으로 배포되는 IT서비스를 중앙에서 관리 할 수 있다.
* 일괄된 거버넌스를 달성하고 규정준수 요구사항을 충족하는데 도움이 된다.

Trustd Advisor

* Aws 환경을 최적화 하여 비용을 절감하고 성능을 높이며 보안에 도움이 되는 온라인 리소스
* 모범사례에 따라 리소스를 프로비전이 할 수 잇도록 실시간 지침을 제공한다
* 비용, 최적화, 성능, 보안 , 내결함성에 대해 조언을 해준다.

Health DashBoard

* AWS에서 영향을 줄 수 있는 이벤트 발생 시 경고 및 수정치짐을 제공한다.
* AWS 리소스에 기반을 둔 서비스이 성능과 가용성에 대한 개별화된 뷰를 제공한다
* 대시보드는 진행중인 이벤트를 관리하는데 도움이 되는 정보를 제공한다.
* 스케줄링된 활동을 계획하는데 도움이 되는 알림을 제공
* 알림은 리소스 상태변화에 따라 트리거되어 이벤트의 가시성과 문제를 신속하게 진단하고 해결하는데 도움이 되는 지침을 제공한다.
* AWS 서비스 상태를 개인별로 파악하여 영향을 주는 문제의 시기를 파악한다.

문제

1. Trusted Advisor는 비용최적화, 성능, 보안, 내결함성에 대한 조언을 해준다

2. Ops Works는 Chef또는 퍼펫의 관리 구현을 제공한다.

3. 서비스 카탈로그는 사용자가 시작할 수 있는 승인된 서비스 및 app ㅋ카탈로그를 제공하는데 사용

4. 서비스 상태 대시보드는 현재 상황만 표시하며 개인뷰를 제공하지 않는다

Personal Health DashBoard는 시스템에 영향을 미칠 수 있는 이벤트에 대한 개인적인 뷰를 제공한다.

보안

공유책임모델

* 상속된 제어 : 고객이 AWS로부터 완전히 상속받는 제어
* 공유 제어 : 인프라 계층과 고객 계층 모두에 적용되지만 완전히 별개의 컨텍스트가 제공
* 고객별 제어 : AWS 내에서 배포하는 APP을 기반으로 전적으로 고객의 책임인 제어

ComPliance (규정준수)

* 클라우드의 규정준수를 통해 AWS에서 강력한 제어 기능을 이해하고 클라우드에서 보안 및 데이터 보호를 유지할 수 있다.
* AWS 인프라를 기반으로 구축되며 규정준수 모델을 공유한다.
* 규정준수 프로그램 포함요소

인증/증명, 법률, 규정, 개인정보, 프레임워크

AWS Artifact

* 귀하에게 중요한 규정준수 관련 정보를 제공하는 핵심 리소스
* AWS의 보안 및 규정 준수 보고서에 대한 온디멘드 엑세스를 제공하고 온라인 계약을 체결
* 제공되는 리포트에는 AWS 보안제어의 구현 및 운영 효율성을 검증하는 SOC보고서, PCI보고, 전 세계의 인증기관의 인증이 포함된다.
* 제공되는 계약에는 BAA(Business Association ~) 및 NDA(비공개 계약) 포함

Instpector

* AWS에서 배포된 APP의 보안 및 규정준수를 개선하는데 도움이 되는 자동화 보안 평가 서비스
* 응용프로그램의 취약점과 모범사례로부터의 이탈을 자동으로 평가
* EC2인스턴스에 설치된 에이전트 사용, 인스턴스는 태그가 지정되어야 한다.

WAF

* 웹 app 방화벽
* App의 가용성을 저하시키고 보안을 손상시키거나 과도한 리소스를 소비 할 수 있는 공격에 대한 방화벽, 가장 기본적

AWS Shield

* AWS에서 관리는 DDOS 보호 서비스
* 상시감지 및 자동 인라인 완화 기능으로 AWS에서 실행되는 웹 APP을 보호한다.
* 다운타임 및 대기시간을 최소화
* CloudFormation과 통합된다.
* Standard 버전과 Advanced 버전이 있다.

AWS Macie

* 완전관리형 데이터 보안 및 데이터 개인 정보 보호 서비스이다.
* 머신러닝, 패턴 매칭을 사용하여 S3에서 민감한 데이터를 검색, 모니터링, 보호 한다.
* 보안준수사항, 보안예방, 데이터 보호 서비스

KMS

* Key management service
* 데이터 보호에 사용되는 암호화키를 중앙집중적으로 제어한다.
* 데이터 암호화에 사용되는 키를 생성 불러오기, route, 비활성화, 삭제 사용정책 정의 및 사용감사를 할 수 있다.
* KMS는 대부분의 다른 AWS서비스와 통합되어 사용자가 제어하는 암호화키를 사용하여 서비스에 저장된 이터를 쉽게 암호화한다

HSM

* Hardware Security Module
* 클라우드 기반 하드웨어 보안 모듈로 클라우드에서 자체 암호화키를 쉽게 생성하고 관리한다.
* FIPS 140-2 Level3 검증 HSm을 사용하여 자체 암호화키를 관리한다.
* JCE(JAVA). CNG(MS) 라이브러리와 같은 업계 표준 API를 사용하여 APP과 통합할 수 있는 유연성을 제공한다.

ACM

* 퍼블릭 SSL/TLS 인증서를 생성하고 관리하는데 사용
* ACM에서 제공하는 인증서, ACM으로 가져온 인증서 사용가능
* Certificate manage 사설인증 기관을 사용해서 사설CA에서 인증서 요청 가능
* 도메인 내의 여러 도메인으로부터 보호
* 하위 도메인을 보호 할 수 있는 와일드 카드 ssl인증서 생성가능

Secret Manger

* 코드를 배포 할 필요없이 암호를 안전하게 교체 할 수 있도록 하여 보안 및 규정준수 요구사항을 충족하는데 도움을 준다
* RDS, RedShift, DocumentDB에 대한 내장 통합을 제공하고 이러한 데이터 베이스 자격증명을 자동으로 교체한다.
* 람다함수 사용자를 지정하여 Secret Manage 교체를 API키 및 oa토큰과 같은 다른 보안유형으로 확장

Penetration

* 침투테스트, 공격을 시뮬레이션하여 취약점에 대한 자체 app의 보안을 테스트하는 방법
* Aws는 침투테스트를 허용하며 테스트 할 수 있는 자원이 한정되어있다.
* 다음 서비스에 대해서는 권한없이 침투테스트 가능 (ec2 ins, NAT Gateway, ELB, RDS, Aurora, CloudFront, API GateWay, Lambda, LightSail리소스, 빈스톡)
* 계정이 손상되거나 의심되는 경우 다음 단계를 수행한다.

루트계정 암호변경, 모든 IAM 사용자 비밀번호 변경, 모든 프로그램 API액세스 키 삭제 또는 전환, 계정에서 생성되지 않은 모든 리소스 삭제, aws 지원센터에 연락

Direct Service

AWS Managed

Microsoft AD

* 완전관리형 인프라 서비스
* 5000명 이상의 사용자가 있거나 신뢰관계를 설정시 중요하다
* 윈도우 서버에서 실행
* 온프레미스의 Active Directory에서 클라우드로 인증을 확장할 수 있도록 신뢰관계를 설정한다.
* 온프레미스 사용자들은 SSO를 사용하여 두 도메인의 리소스를 엑세스한다.
* VPN, Direct Connect 필요, 독립형 AD로 사용이 가능하다.
* 윈도우 서버 2012R2 에서 실행되는 AWS관리형 Microsoft AD
* MS AD호스팅을 원하ㅓ나 리눅스 APP용 LDAP가 필요한 기업

SimpleAD

* 일반적인 디렉터리 기능을 갖추 저렴한 AD 호환 서비스
* 독립형, 완전관리형 디렉터리
* 가장저렴한 옵션이있다. 5000명 미만이ㅡ 사용자를 위한 최상의 선택, 고급AD가 필요없다
* 삼바를 기반으로 한 저규모, 저비용 AD구현 EC2 인스턴스를 도메인에 조인한다.

AD Connector

* 디렉터리 요청을 온프레미스 AD로 리다이렉션 하기위한 디렉터리 게이트웨이
* 기존 온프레미스 AD를 AWS와 연결
* AWS 서비스와 함꼐 기존 AD사용하려는 경우
* EC2 인스턴스를 온프레미스 AD와 조인
* 인증을 통해 온프레미스 ADDC를 사용하면 AWS ManageConsle에 로그인 가능
* 기존의 자격증명을 사용하여 AWS서빗에 로그인 할 수 있도록 허용가능

보안문제

1. 공유책임모델에 따르면 Ec2 인스턴스에 대한 OS패치 담당은 고객에게 있다.

2. 공유책임모델에 따르면 S3에 대한 서버측 암호화 구성의 담당자는 고객에게 있다.

3. AWS 클라우드 플랫폼과 관련된 규정준수 정보를 가지는 툴은 Artifact이다

Inspector는 보안 및 규정준수를 개선하는데 도움이 되는 자동화된 평가서비스이다.

4. 침투테스트는 특정 서비스의 한해서 승인없이 실행이 가능하다

5. 일반적으로 웹 기반 공격으로부터 보호하는데 사용하는 서비스는 WAF이다. 보안손상, 과도한 리소스소비 방지등ㄷ 있다.

AWS Shield는 DDOSS로부터 보호해준다.

6. AWS 사용자에게 영향을 줄 수 있는 이벤트 발생 시 지침을 제공하는 기능은 Personal HealthDashBoard이다. 위 기능을 제공하며 성능 및 가용성에 대한 개인화된 뷰를 제공한다.

7. 계정이 손상된 경우 IAM암호 재설정, API교체 또는 삭제, 생성되지 않은 리소스 삭제, AWS지원ㄴ 서비스를 받아야한다.

8.공동책임모델에 의하면 DC의 보안담당은 AWS에게 있다.

9.암호화 키를 보호하기 위해 HW 보안 모듈을 사용하는 서비스는 HSM으로 자체 암호화 키를 생성한다.

KMS는 공유 서비스로 키 관리 서비스이다. 서비스 카탈로그는 일반적으로 배포되는 IT서비스를 중아에서 관리하고 규정준수 요구사항을 충족하는 일괄된 거버넌스를 충족하도록 도와준다

10. PCI, 규정준수에 대한 ㅂ고서를 찾는데 사용하는 서비스는 Artifact로 규정준수 정보를 포함

중요한 규정준수관련 정보를 제공하는 중앙 리소스로 AWS의 보안 및 규정 준수 보고서에 따른 온라인 계약을 체결한다.

머신러닝, 분석

Rekognition

* 머신러닝, 지식없이 확장성이 뛰어난 딥러닝 기술을 사용하여 APP에서 이미지 및 비디오 분석을 한다.
* 물체, 사람, 텍스트, 장면 등을 식별하고 부적절한 컨텐츠를 감지한다.
* 신원확인, 공공안전 등 페이스 탐지 기능을 제공한다

Rekognition video

* S3 버킷에 저장된 비디오를 처리한다.
* 요청완료되면 SNS를 통해 전송
* 비디오 신에 대해 인원을 추적가능하며 얼굴을 검색하는 등 가능

Polly

* 텍스트를 음성을 바꾸는 서비스이다.
* TTS 기능으로 고급 딥러닝 기술을 사용하여 자연스러운 음성가능하다.

Transcribe

* App에 음성 – 텍스트 기능 추가
* 오디오 데이터는 응용프로그램에서 사용전 텍스트로 변환이 필요하다
* 자동음성인식(ASR)이라는 딥러닝 프로세스를 사용하여 음성을 텍스트로 변환한다.
* 자막자동화, 미디어리소스에 대해 메타데이터 생성, 완전히 검색 가능한 아카이브 생성
* 메디컬 기능도 있어 임상문서 처리가능

Translate

* 빠르고 고품질의 언어번역을 제공하는 머신러닝 번역 서비스
* 딥러닝을 사용 알고리즘이 뛰어나며 자연스럽다
* 해외 접속자들에 마제 현지화하며 많은 양의 텍스트를 효율적으로 쉽게 번역한다.

Athena

* 표준 SQL을 사용하여 S3 데이터를 쉽게 분석하는 대화형 쿼리 서비스
* 서버리스 이므로 관리할 인프라가 없으며 실행한 쿼리에만 요금을 지불한다.
* Glue를 사용하여 S3에 저장된 데이터 DB에 대한 정보화 스키마를 제공한다
* ETL 작업에 필요한 복잡한 과정이 필요없다
* SQL기술자는 누구나 대규모 데이터세트를 분석 가능하다

Glue

* 데이터 준비 단계를 자동화하며 완전관리형 종량제 ETL서비스이다.
* 데이터 카탈로그를 통해 데이터를 자동으로 검색 및 프로파일링 하고 ETL 코드를 생성하여 소스데이터를 대상 스키마로 변환한다.
* 저장된 데이터를 지정하면 Glue가 데이터를 검색하고 관련 메타데이터를 Glue데이터 카탈로그에 저장한다.
* 카탈로그가 작성되면 데이터를 즉시 검색하고 쿼리가 가능하며 ETL에 사용한다.
* S3데이터, RedShift, RDS와 함께 사용하면 좋다

Kinesis

* 실시간으로 데이터를 쉽게 수집, 처리, 분석 할 수 있으며 상시로 인사이트를 얻으며 새로운 정보에 신속하게 대응이 가능하다
* 다양한 데이터 스트림 처리를 위한 서비스가 있다

Date PipeLine

* 지정된 간격으로 서로 다른 AWS 컴퓨팅 및 스토리지 서비스와 온프레미스 데이터 원본 간에 데이터를 안정적으로 처리하고 이동 할 수 있도록 도와준다.
* 저장된 데이터에 정기적으로 엑세스하고 대규모로 변환, 처리하며 S3, RDS, DynamoDB 등 같은 서비스로 전송한다

Quick Sight

* 조직의 모든 사람에게 쉽게 인사이트를 제공할 수 있으며 클라우드 기반의 빠른 인텔리전스 서비스이다
* 완전관리형 서비스로 대화형 대시보드로 빠르게 접근간으하며 모든 장치에서 대시보드에 엑세스하고 APP 포털 및 웹사이트를 포함한다

아키텍트

기존방식과 클라우드의 차이점

IT리소스 (IT Assets as Provisined Resources)

* 프로비저닝된 리소스를 사용하며 필요에 따라 프로비저닝하며 필요에 따라 확장한다.

글로벌 (Global, Available, and scalable Capacity)

* 가용성 및 확장가능한 용량이며, 전 세계적으로 쉽게 비용효율적으로 빠르게 배포가 가능

고급관리서비스 (High Level Managed Service)

* 관리형 스토리지, DB분석, APP및 배포서비스를 활용하여 비용을 절감

보안

* 테스트를 단수화 하며 기본 보안 및 암호화 기능을 사용

비용설계

* 세분화된 청구, 투명한 비용, 예산알림도구
* Oss 전환을 위한 도구, 프로세스 모범사례가 존재한다

수직확장 ( vertically scailing)

* Ec2 인스턴스 RDS 인스턴스 등이 사용돈다.
* 수동조정이 가끔 필요하며, 불가피한 다운타임이 존재한다, 확장성에도 한계가 있따.

수평확장(Horozontal scailing)

* Ec2 오토스케일링, 다이나모 DB
* 다운타임 없이 원할한 확장이 가능하며 수직확장보다 확장성이 뛰어나다

모범 사례

고정서바가 아닌 경우의 모범사례

* 기존의 인프라는 초기비용과 읽기시간을 고려하여 고정리소스로 작업한다
* 클라우드 사용시 동적으로 프로비저닝된 리소스를 활용한다
* 동적 프로비저닝된 클라우드 컴퓨팅의 특성을 활용한다
* 서버 및 기타 구성 요소를 임시 리소스로 사용한다
* 필요한 만큼 실행하며 필요한 만큼 사용한다.
* 자동화 도구를 사용하여 시스템 안정성 및 조직효율성을 향상시킨다.

느슨한결합

* 상호의존성을 줄이기 위한 IT 시스템 설계
* 한 구성 요소의 변경 또는 오류가 다른 구성 요소에 영향을 미치지 않아야 한다
* 서버리스 검색, 비동기 통합

DB

* 각 워크로드에 적합한 DB기술을 사용한다
* 성능요구사항, 확장성, 내구성, 기능을 고려한다
* 관계형, NoSql, DW, 검색, 그래프등을 활용한다

Failure single point, 단일 실패 지점 제거

* Introduce Redundancy 구성요소가 손상시 다른 사용자가 인수 할 수 있는지 확인
* Detected Fail : 상태확인 및 경보를 사용하고 감지 및 대응 자동화
* 내구성 스토리지 : RPO(복구지점)과 RTO(복구시간)이 일치하는지
* 자동화된 데이터센터 복원력, 재난에 대한 복원력을 확보한다

비용최적화

* 적절한 사이즈를 조정한다. 비용효율성을 위해 최적합의 인스턴스 크기와 수를 관리
* 탄력성 : 변화하는 수요에 따라 필요에 따라 수평확장
* 다양한 구매옵션을 제공 : 예약 인스턴스, 스팟인스턴스

캐싱

* 성능과 비용 효율성을 향상시키는데 사용된다
* 캐싱방법 : APP데이터 캐싱, 엘라스틱 캐싱, 엣지캐시

보안

* 심층적인 방어를 위한 AWS기능 사용
* AWS 보안책임공유
* 권한 액세스 감소, 최소화한다.
* 실시간 검사(Trusted Advisor, Config, Instpector)
* Security as Code : CloudFront를 사용하여 보안환경을 구축

좋은 운영을 위한 5가지 요소

운영 우수성

* 시스템을 실행하고 모니터링하여 비즈니스 가치를 제공하고 지원 프로세스 및 절차를 지속적으로 개선하는 기능을 포함한다.

보안

* 정보시스템 및 자산을 보호하는 동시에 위험평가 및 완화전략을 통해 비즈니스 가치를 제공한다

신뢰성

* 인프라 또는 서비스의 중단으로부터 복구하고 수요를 충족하기 위해 동적으로 컴퓨팅 리소스를 제공하며 잘못된 접근이나 네트워크 문제와 같은 중단상태를 완화하는 시스템

성능효율성

* 리소스를 효율적으로 사용하여 시스템의 요구사항을 충족하고 수요변화와 기술발전함에 따라 효율성을 유지하는 능력

비용최적화

* 불필요한 비용또는 차선의 리소스를 방지하거나 제거하는 기능을 포함한다.

아키텍트 문제

1. 클라우드의 어떤 아키텍처 이점이 운영 비용 절감에 도움이 되는가?

하이레벨 메니지먼트 – 관리형 스토리지, 디비, 분석 등 서비스를 활용하여 운영비용으 낮춘다

느슨한결합 – 시스템 간의 상호 종속성을 줄이기위한 아키텍처 모범사례

Design of Failure – 설계자에게 APP이 실패 할 수 있는 방법을 고려하고 설계에 완화를 포함하도록 요청하는 설계 모범사례

2. 오토스케일링은 호리즌탈 유형

3. Amazone Read Replica에서 제공하는 유형은 호리즌탈 유형이다.

4. API 기반 서비스의 장점은? 프로그래밍 방식 및 동적으로 리소스를 시작할 수 있다.

5. 아키텍처 모범 사례로는 실패에 대비한 설계가 있다.

실패 할 수 있는 항목을 항상 고려하고 앱아키텍처가 실패의 영향을 완화할 수 있는지 확인

6. 모범사례 중 서버가 아닌 서비스란?

관리형 서비스 및 서버리스 서비스와 같은 더 많은 서비스를 사용하려고 하는 것

7. 다이나모 디비는 수평적으로 확장한다.

8. 상호의존성을 줄이기 위한 아키텍처 모범사례로는 느슨한 결합이 있다.

9. 수평관리 서비스는 다이나모DB, EC2 오토스케일링, S3가 있다.

10. 템플릿을 사용하는 클라우드포메이션이 보안환경 구축을 어떻게 지원할 수 있을까?

리소스를 잘 보호하는지 확인하기 위해서는 동일한 템플릿을 반복적 빌드하여 사용하면 템플릿에서 구축된 모든 환경이 안전한지 확인 할 수 있다.

11. AWS는 네트워킹, 컴퓨팅, 스토리지 하드웨어를 패치하고 보호 할 책임이 있다.

1. Cloud OverView

1. 리전은 하나 이상의 데이터 센터로 구성된 2개 이상의 AZ로 구성된다.

2. AWS 서비스 이용 정책은 AWS의 금지된 사용의 예를 설명합니다.

3. 가용영역(AZ)는 물리적으로 분리되어 있으며 서로 격리되어 있다. 하나 이상의 데이터센터를 보유하고 있다.

4. IAM 서비스는 사용자, 그룹, 역할 및 정책을 한곳에서 생성하고 관리하는 글로벌 서비스이다.

5. Aws 가격책정의 세 가지 기본사항은 컴퓨팅, 스토리지, 아웃바운드 데이터 전송이다.

6. 온디멘드는 유연성이 가장 필요한 경우 최상의 옵션이며 장기 약정이나 선불결제가 없다.

IAM 문제

1 . 엑세스 키 ID와 보안 액세스 키가 어떤 IAM 엔티티와 연결되어 있는가? User

액세스 키 ID 및 보안 액세스 키는 유저와 연결되며 CLI 또는 API를 사용하여 프로그래밍 방식 액세스 권한을 부여하는데 사용된다.

2. 루트계정은 계정을 만드는데 사용한 이메일주소로 자격을 증명한다.

3. ARN이란 Amazone Resource Name으로 유저 및 그룹과 같은 엔티티와 연결된다.

4. 권한을 할당 할 때는 항상 필요한 최소권한만을 부여하며 모범사례이다.

5. 권한을 위임하는데 사용할 수 있는 IAM엔티티는 역할(rule)로 영구 자격 증명을 사용하지 않고 사용자 및 서비스에 대한 리소스에 대한 권한을 제공하는 좋은 방법이다.

6. 루트 계정은 다단계 인증(MFA)를 추가하여 사용자 이름과 암호는 물론 로그인에 대한 보안 수준을 한층더 높여준다.

7. IAM의 모범사례로는 그룹을 사용하여 권한할당, 사용자를 위한 강력한 암호정책, 정지적으로 자격증명교체, 최소한의 권한부여가 있다.

8. 디폴트계정에는 권한없이 생성이 되며 그룹 및 정책을 사용하여 권한을 할당한다.

컴퓨팅 문제

1. 기존 서버와 비교하여 Amazone EC2의 이점은 빠른 시간내에 탄력적으로 확장이 가능하다는 점이다.

팔요할 때마다 인스턴스 유형을 변경하여 용량을 탄력적으로 늘리거나 줄일 수 있다.

2. 시작시 EC2인스턴스에서 명령을 내리는 방법은 유저데이터를 사용하는 방법이 있다.

3. AWS에서 Docker 컨테이너를 실행할 수 있는 서비스는 ECS(Elastic Container Service)이다.

4. 람다는 서버리스 서비스이며 코드나 함수를 실행하는 서비스이다.

5. 라이트세일은 기술 전문 지식이 없는 사람들도 컴퓨팅 워크로드를 실행하는데 적합한 서비스를 제공한다.

6. Amazone 머신 이미지(AMI)는 EC2 인스턴스를 시작하는데 필요한 정보를 제공한다.

7. 람다는 수요에 따라 탄력적으로 확장이 가능하며 서버리스 서비스이다.

서버리스 서비스이므로 인스턴스 유형을 선택할 수 없다.

8. 루트볼륨에 대해 EC2인스턴스에 사용하는 스토리지 서비스는? EBS이다.

스토리지 문제

1. Amazone S3는 오브젝트 스토리지이다. 객체기반 스토리지 시스템

2. 버킷은 S3의 루트 수준 컨테이너로 객체를 버킷에 업로드하는 방식이다.

3. EBS 볼륨은 가용영역(AZ)에 저장된다.

4. AWS Storage Gateway는 클라우드 스토리지에 온 프레미스 엑세스를 제공하는 하이브리드 클라우드 스토리지 서비스이다.

5. 디폴트 설정에 의하면 인스턴스가 종료될 때 EBS 루트 볼륨은 삭제된다.

6. Amazone Linux 2 AMI 만 EFS와 함께 사용이 가능하다.

7. 인스턴스 스토어 볼륨은 EC2 호스트 서버에 물리적으로 연결되어 있으며 전원이 꺼지면 데이터가 손실도ㅣ는 임시 스토어 이다.

8. S3 Glacier Deep Archive는 장기보존을 위한 가장 저렴한 스트로지 클래스이다.

VPC 문제

1. VPC는 리전 내에서 생성되며, 한 리전 내에서 여러 VPC를 생성 할 수 있으며 기본적으로 모든 리전에는 기본 VPC가 존재한다.

2. 서브넷 수준의 방화벽은 네트워크 엑세스 제어목록(NACL)이며 인스턴스 수준의 방화벽은 보안그룹이다.

NAT 게이트 웨이는 프라이빗 서브넷의 EC2 인스턴스에 대한 인터넷 액세스를 제공하는 서비스이다.

3. Direct Connect는 AWS 클라우드에 대한 사설 네트워크(온프레미스DC)와 연결하는 서비스이며 안정적이ㄴ 성능으로 높은 대역폭과 낮은 대기시간을 제공한다.

4. 탄력적 IP주소를 사용하면 인스턴스가 중지 될 때 주소가 유지된다. 사용하지 않은 Elastic IP 주소에 대해서도 지불을 해야한다.

5. NAT 게이트웨이는 사설 서브넷아 EC2 인스턴스에 대한 인터넷 연결을 활성화 하는데 사용하는 완전

관리형 네트워크 서비스이다.

NAT인스턴스는 사용자가 관리하는 EC2 인스턴스로, 개인 서브넷의 인스턴스가 인터넷에 액세스 할 수

있도록 하는데 사용한다..

6. 다이렉트 컨넥트는 사설 네트워크와의 연결이며 예측 가능한 성능을 제공한다.

DataBase 문제

1. RDS 데이터베이스의 용량을 늘리기 위해서는 인스턴스의 유형을 변경하여 수직확장 시킨다.

2. DynamoDB는 비정형 데이터, 유연한 스키마, 수평 확장에 적합한 NoSQL DB 서비스이다.

3. RDS는 온라인 트랜잭션 처리(OLTP) 워크로드에 사용되는 관계형 데이터베이스이다.

4. DynamoDB는 원할한 푸시버튼을 사용하여 수평확장을 제공한다.

5. RDS 데이터베이스는 다중 AZ 사용으로 내결함성을 더한다. 다중 AZ는 별도의 가용영역에 마스터 DB의 대기 복사본을 생성한다.

6. DynamoDB Accelator (DAX)는 DynamoDB 데이터베이스의 성능을 향상시키는 인 메모리 캐시이다.

7. RDS Aurora는 트랜잭션 워크로드에 적합한 관계형 데이터베이스이다.

8. RedShift는 데이터웨어 하우스 사용에 적합한 관계형 SQL데이터베이스이다.

9. 온프레미스 데이터베이스에서 RDS로 이동하는 결정적인 이유는 운영오버헤드를 줄이기 위해서이며 ㄲRDS를 사용하면 운영체제를 관리 할 필요가 없어 운영 오버헤드를 줄일 수 있다.

LB, Auto Scailing 문제

1. EC2에서 실행되는 앱의 탄력성을 활성화 시키기 위해서는 Auto Scailing을 사용하여 수요 변화에 따라

인스턴스를 조정하는 방법이 있다.

ELB는 트래픽을 여러 인스턴스에 배포하는데 사용하며 EC2 인스턴스의 탄력성 확장하지 않는다.

2. 애플리케이션로드 밸런서는 호스트 기반 라우팅을 수행 할 수 있으며 도메인 이름과 같은 호스트 헤ㅐ더의 정보를 기반으로 트래픽을 전달할 수 있다.

3. EC2 AutoScailing은 애플리케이션에 대한 수요가 변경되면 인스턴스를 시작하고 종료하므로 수요를

처리하는데 필요한 인스턴스에 대해서만 비용을 지불 할 수 있다.

4. ELB는 여러 백엔드 인스턴스에 트래픽을 배포하여 애플리케이션의 내결함성을 지원한다.

5. ELB는 가용성 영역에만 트래픽을 분산, 배포한다. 인터넷 연결이 가능하며 고가용성 및 내결함성을 가능하게 한다.

리전간의 트래픽을 전달하는 서비스는 route53이다.

6. ELB는 헬스체크를 사용하여 인스턴스가 사용 가능하고 정상적인지 확인한다.

7. 4계층 IP 프로토콜 데이터를 기반으로 연결하는 로드밸런서는 네트워크로드 밸런서이다.

ALB는 7계층, CLB는 4, 7계층에서 작동한다.

8. Auto Scailing Group(ASG)는 EC2인스턴스의 모음이다.

Scailing policy(확장정책)은 ASG가 확장 및 축소되는 시기와 방법을 결정한다.

Scailing Plan(확장계획)은 트리거 및 인스턴스 프로비저닝 on/off 시기를 정의한다.

9. Launch Configuration (런쳐구성)에는 EC2 오토스케일링에서 인스턴스 패밀리, AMI 키 페어 및 보안그룹을 정의하는데 사용하는 템플릿이다. EC2인스턴스를 생성하는데 사용되는 템플릿이다.

DNS, 컨텐츠 전송 문제

1. Amazome CloudFront를 사용하면 전 세계 사용자에게 더 가까운 컨텐츠를 캐시하여 성능을 향상 시킬 수 있다. 이 데이터를 캐시하는 장소를 엣지 로케이션이라고 한다.

2. (엣지 로케이션) -- (리전엣지 캐시) – (CloudFront)에 위치한다.

3. S3 버킷 및 EC2 인스턴스를 CloudFront 배포의 원본으로 사용할 수 있다. 또한 S3 정적 웹 사이트, Route53을 사용하는 다른 HTTP 서버, ELB 뒤의 인스턴스, MediaStore 컨테이너를 사용할 수 있다.

4. VPC는 리전서비스이다.

5. IAM, CloudFront, Route53은 글로벌 범위의 서비스이다.

6. Route53의 핵심기능은 상태확인, DNS서비스, 도메인 등록이 있다.

7. CloudFront에는 기본적으로 DDOS에 대한 보호기능이 있다.

8. 엣지로케이션은 AWS 글로벌 인프라를 위한 부분으로 전 세계에 있다. 성능향상을 위해 컨텐츠를 캐시하여 최종 사용자에게 더 가깝게 접근이 가능하다.

9. 라우팅 정책은 Route53이 쿼리에 응답하는 방식을 결정한다.

호스팅존은 도메인에 속한 레코드의 집합을 나타낸다.

모니터링 및 로깅 서비스 문제

1. CloudTrail은 성능감사에 대한 서비스이다.

CloudWatch는 성능 모니터링에 대한 서비스이며 EC2인스턴스에 과도하게 로드된 경우 경고 등을 할 수 있다.

2. CloudWatch는 대부분의 AWS서비스와 통합이 가능하다.

CloudWatch Log는 AWS리소스에서 로그를 수집하고 중앙집중화 하는 방식이다.

리소스 변경에 대응하도록 CloudWatch 알람을 설정 가능하다.

CloudWatch 모니터링에는 앱 성능이 포함 될 수 있따.

3. CloudTrail은 성능감사 서비스이며 계정의 모든 API활동 기록을 기록한다.

4. CloudTrail은 기본적으로 90일간의 레코드만 보간된다.

영구적으로 유지하기 위해서는 트레이서를 생성하고 S3버킷에 이벤트를 기록해야한다.

자동화 및 플랫폼 서비스

1. CloudFormation은 빈스톡에서 환경을 배포하는데 사용한다.

빈스톡은 CloudForamtion을 사용하여 환경에서 사용되는 서비스를 배포한다.

2. 빈스톡은 PaaS이다. 기본 인프라와 런타임 엔젠이 자동으로 관리되며 코드만 업로드하면 된다.

Saas(Sw)의 예시로는 Salesforce, Facebook, Gmail이 있다.

Iaas(Infrastructure)의 예시로는 EC2가 있따.

3. AWS관리 콘솔을 사용하면 수동으로 서비스를 사용할 수 있다.

4. Cloud Formation은 VPC를 생성하고 여기에 다양한 유형의 리소스를 시작하는 전체 프로세스를 자동화 할 수 있다. EC2인스턴스, 오토스케일링, ELB등을 사용할 수 있다.

마이그레이션 및 이전서비스

1. DMS(DataBase Migration Service)를 사용하면 온프레미스 데이터베이스를 Amazone RDS로 마이그레이션 할 수 있다.

2. AWS SnowBall은 페타바이트 규모의 데이터를 마이그레이션 한다. (50TB)

AWS Snowmobile은 엑사바이트 규모로 Snowmobile 당 최대 100PB의 마이그레이션이 가능하다

3. S3 Transfer Accelation은 빠른 업로드에 사용되지만 연결이 잘되어여하며 추가 비용이 든다.

4. S3 멀티파일 업로드는 S3에 업로드하기 위해 대용량 파일을 분할하는데 유용하다.

5. DMS는 다운타임 없이 데이터베이스를 온라인으로 마이그레이션 할 수 있으며 다양한 소스/대상 옵션을 지원한다. 다운타임 없이 EC2에서 RDS로 마이그레이션이 가능하다.

6. DataSync는 온프레미스 NAS 스토리지에서 S3, EFS, FSx로 마이그레이션 할 수 있다.

Pricing 문제

1. 예약 인스턴스는 1년 또는 3년 기간으로 약정되며 안정적인 장기 워크로드에 적합하다.

전용 인스턴스는 단일 고객 전용 HW에서 워크로드를 실행해야 하는 경우 적당하다.

스팟인스턴스는 상당한 컴퓨팅 성능이 필요하고 언제든지 중지할 수 있는 배치 컴퓨팅 워크로드에 적합하다. 집약적 워크로드에 상당한 비용 절감을 의미하는 할인을 받을 수 있다.

2. 오토스켕일링, CloudFormaion, IAM은 무료서비스이다. 단 생성한 리소스에 대해서는 지불해야함

3. 인바운드 데이터 전송에 대해서는 요금을 지불하지 않는다. 아웃바운드의 경우 전송 지불

4. S3 Glacier는 장기데이터 저장과 빠른 데이터 검색에 필요한 스토리지이다.

S3 Glacier Deep Archive는 자주 액세스 하지 않고 7년 동안 보존되며 24시간 내에 검색할 수 있어야하는 스토리지에 적합하며 가격이 저렴하다

5. 클라우드 이전시 필요한 것을 프로비저닝하고 필요에 따라 확장 할 수 있는점이 가장 큰 장점이다.

6. EFS에 사용할 수 잇는 스토리지 클래스에는 Standard, IA(Infrequent Access)가 있다.

7. VPC의 VPN은 요금을 지불해야한다. 보안그룹, 라우팅테이블, 인터넷 게이트웨이는 무료이다.

8. 태그 및 리소스 그룹은 메타데이터를 AWS리소스에 할당하고 하나 이상의 태그를 공유하는 리소스를 그룹화 할 수 있는 도구이다.

태그는 비용보고를 위해 AWS리소스에 메타 데이터를 할당하는데 사용한다.

9. Cost Explorer는 비용차트를 볼 수 있는 무료도구이다

TCO는 AWS에서 클라우드 사용과 온프레미스 데이터 센터 사용에 따른 비용절감 효과를 비교한다.

통합청구(Consolidated billing)은 조직의 모든 게정에서 사용량을 결합하여 볼륨 가격 할인 및 예약된 인스턴스 할인을 공유 할 수 있다. 개별 독립 실행형 게정보다 프로젝트, 부서에 대한 비용이 낮아진다.

Trusted Advisor는 AWS 모범사례에 따라 리소르르 프로비저닝 하는데 도움이 되는 실시간 지침을 제공하는 도구이다.

10. 엔터프라이즈 지원 플랜에 TAM이 제공된다.

11. TCO 분석에서 온프레미스 데이터센터의 운영비용을 고려해야한다.

12. EC2 예약 인스턴스에 대한 결제 옵션으로는 선불, 후불, 부분선불이 있다.

13. AWS 조직(Organization)을 사용하면 여러 AWS 계정을 생성하고 중앙에서 관리하는 조직으로 통합이 가능하다.

CostExplorer는 비용차트를 볼 수 잇는 도구이며 지난 13개월 동안의 비용 데이터를 보고 향후 3개월 동안 지출할 비용을 예측할 수 있다.

APP Integration 문제

1. SNS를 사용하면 고객에게 알림, SMS를 제공할 수 있으며 게시자/구독자 모델을 사용하는 알림서비스이다. 여러 전송 프로토콜을 통해 알림을 보내는데 사용할 수 있다.

2. Step Function은 워크플로 오케스트레이션 서비스이며 서버리스서비스이다.

3. SQS는 대기열을 사용하여 앱 구성요소를 분리할 수 있으며 메시지 지향 API를 사용한다.

4. 단일 SNS 주제에 여러 SQS 대기열을 구독할 수 있다.

관리 및 거버넌스 문제

1. AWS Trusted Advisor는 총 소유비용에 대한 조언을 제공하지 않는다.

비용최적화, 성능, 보안, 결함허용에 대해서만 조언한다.

2. AWS OpsWorks는 Chef 또는 퍼팻의 관리 인스턴스를 제공한다.

3. 서비스 상태 대시보드느 현재 상황을 표시해주는 대시보드이다.

Personal Health Dashboard는 시스템에 영향을 미칠 수 있는 이벤트에 대한 개인화된 뷰를 제공한다.

4. AWS 서비스 카탈로그는 사용자가 시작할 수 있는 승인된 서비스 및 애플리케이션 카탈로그를 제공하

는데 사용한다.

보안문제

1. AWS 공유책임모델에 의하면 EC2 인스턴스에 대한 OS 패치 담당을 하는 사람은 고객이다.

2. AWS 공유책임모델에 의하면 S3에 대한 서버 측 암호화 구성을 담당하는 사람은 고객이다.

3. Inspector는 AWS에 배포된 애플리케이션의 보안 및 규정 준수를 개선하는데 도움이 되는 자동화된

보안 평가 서비스이다.

Artifact는 중요한 규정 준수 관련 정보에 대한 중앙리소스로 규정 준수 정보를 찾는데 사용한다.

AWS 규정 준수 보고서에 대하여 온디멘드 액세스를 제공하고 온라인 계약을 선택한다.

4. 특정 서비스에 대해서는 승인없이 침투테스트가 가능하다.

5. WAF는 일반적인 웹 기반 공격으로부터 보호하는데 도움이 된다.

Route53은 DNS서비스이며 상태 확인 서비스 및 도메인 등록을 수행한다.

6. Personal Healt Dashboard는 AWS가 사용자에 영향을 줄 수 잇는 이벤트가 발생할 때 경고 및 교정 지침을 제공한다. AWS 리소스의 기반이 되는 AWS 서비스의 성능과 가용성에 대한 개별화 된 뷰를 제공한다.

7. KMS는 암호화 키 관리 서비스 이다.

8. 공유책임모델에 따르면 데이터 센터 보안을 담당하는 사람은 AWS이다.

9. AWS 서비스 카탈로그는 일반적으로 배포되는 IT서비스를 중앙에서 관리하고 규정준수 요구사항을 충족하는 일관된 거버넌스를 달성하는 동시에 사용자가 필요한 승인된 IT서비스를 빠르게 배포 할 수 있다.

10. Cloud HSM은 AWS 클라우드에서 자체 암호화 키를 쉽게 생성하고 사용할 수 있는 클라우드 기반

하드웨어 보안 모듈

11. AWS Artifact는 중요한 규정준수 관련 정보에 대한 중앙리소스로 규정 준수에 대한 보고서를 찾는데 사용할 수 있는 서비스이다.

머신러닝 & 분석 문제

1. Amazone Transcribe는 오디오를 텍스트로 추출 할 수 있다.

Polly는 텍스트를 음성으로 바꾸는 서비스이다.

2. AWS Rekognition을 사용하면 이미지에서 얼굴을 감지 할 수 있다.

3. Athena는 SQL 쿼리를 사용하여 S3의 데이터를 직접 분석 할 수 있는 서버리스 서비스이다.

Glue는 분석을 위해 데이터를 준비하고 로드하는데 사용되는 완전관리형 데이터 ETL 서비스이다.

Kinesis는 실시간 스트리밍 데이터를 쉽게 수집, 처리 및 분석할 수 있는 서비스이다. 센서가 있는 회사등에서 데이터를 수집하고 처리하는데 이상적이다.

4. Data PipeLine은 서비스간에 데이터를 처리하고 이동하는데 도움이 되는 서비스이다.

사내 데이터 소스뿐만 아니라 서로 다른 AWS 컴퓨팅 및 스토리지 서비스간에 데이터를 지정된 간격으로

안정적으로 처리하고 이동할 수 있도록 지원하는 웹 서비스이다.

5. Amazone QuickSight는 빠른 클라우드 기반 비즈니스 인텔리전스 서비스로 조직의 모든 사람에게 쉽게 통찰력을 제공 할 수 있다. 대화형 대시보드로도 사용한다.

아키텍트 문제

1. 아키텍트의 이점, 모범사례

Horizontal Scailing (수평확장)은 확장을 원할하게 하며 일반적으로 제한없이 확장이 가능하다.

Loose coupling (느슨한 결합)은 시스템 간의 상호 종속성을 줄이기 위한 아키텍처의 모범사례로 내결함성이 있는 안정적인 애플리케이션을 만드는데 사용한다.

Design for Failure (실패를 생각한 모델)은 설계자에게 응용프로그램이 어떻게 실패할 수 있는지 고려하고 설계에 대해 완화

Higher-level managed service (높은 수준의 관리서비스)는 관리형 스토리지, DB, 분석, APP 및 배포 서비스를 활용하여 운영비용을 낮출 수 있다.

2. EC2 Auto Scailing은 추가 Ec2 인스턴스를 시작 및 종료하여 수평적 확장을 제공한다.

3. Amazone Read Replica에서 제공하는 확장 유형은 수평적 확장이다.

수평확장 사용중인 다른 RDS 인스턴스를 READ한다

4. API 기반 서비스의 이점으로는 API기반 클라우드 서비스를 사용하면 프로그래밍 방식으로 동적으로 리소스를 시작할 수 있다.

5. “services, not servers”는 관리형 서비스 및 서버리스 서비스와 같은 서비스를 더 많이 사용해야 하는것을 추천한다.

6. 다이나모DB는 수평적 확장이다.

7. 수직확장의 한계점으로는 최대 인스턴스의 크기 제한, 수동개입의 필요성, 다운타임의 존재이다.

부하분산을 위해서는 ELB를 사용하면 된다.

8. 수평적 확장의 서비스로는 다이나모DB, EC2 AutoScailing, S3가 존재한다.

9. 작성이 잘된 템플릿을 사용하는 경우, CloudFormation의 보안환경을 구축하는데 도움을 줄 수 있는것은 반복적인 실행이다.

리소스를 안전하게 보호하고 잘 작성된 템플릿파일을 사용할 경우에는 템플릿에서 구축된 모든 환경의 보안을 유지하기 위해 반복적으로 동일한 템플릿을 사용한다.

추가로 필요한 것 들

AWS Batch

* 배치 작업의 코드를 패키징하고 종속성을 지정, CLI, SDK를 사용하여 배치작업을 제출하면 된다.

AWS Beanstalk

* 웹 앱을 시작하고 실행할 수 있는 가장 빠르고 간단한 방법
* 코드를 업로드하기마나면 서비스가 리소스를 프로비저닝, 로드밸런싱, 오토스케일링 및 모니터링 과 같은 모든 세부정보를 자동으로 처리

AWS Storage Gateway

* 기존 온프레미스 환경을 AWS 클라우드와 연결하는 하이브리드 클라우드 스토리지 서비스

Amazone Elasticache

* 완전관리형 Redis, Memcached를 제공하는 서비스
* 인기있는 오픈소스 호환 인메모리 데이터 저장소를 원할하게 배포, 실행 및 확장

AWS Migration Hub

* 여러 AWS 및 파트너 솔루션에서 앱 마이그레이션 진행 상황을 추적할 수 있는 위치를 제공한다.
* 마이그레이션 상태에 대한 가시성을 제공한다..

Amazone API Gateway

* 개발자가 모든 규모에서 API를 쉽게 생성, 게시, 유지관리, 모니터링, 보호 할 수 있는 완전관리형 서비스
* 애플리케이션이 백엔드 서비스의 데이터, 비즈니스 로직 또는 기능에 액세스 할 수 있는 프론터 백도어 역할을 하는 API를 생성

AWS CodeCommit

* Git기반 리파지토리를 호스팅하는 완전관리형 소스제어 서비스

AWS CodeDeploy

* EC2, 람다 및 온프레미스 서버와 같은 다양한 컴퓨팅 서비스에 대한 소프트웨어 배포를 자동화하는 완전관리형 배포 서비스

AWS CloudFormation

* 클라우드 환경의 모든 인프라 리소스를 설명하고 프로비저닝 할 수 있는 공통 언어를 제공

AWS Config

* AWS 리소스의 구성을 평가, 감사 할 수 있는 서비스
* 리소스 구성을 지속적으로 모니터링하고 기록하며 원하는 구성에 대해 기록된 구성 평가를 자동화 한다
* 감사 보안분석 변경관리 및 운영 문제를 해결을 단순화 한다.

AWS OpsWorks

* Chef 및 퍼팻의 관리형 인스턴스를 제공하는 관리 서비스
* Chef 및 Puppet은 코드를 사용하여 서버 구성을 자동화 할 수 있는 자동화 플랫폼이다

AWS Service Catalog

* 조직이 AWS에서 사용하도록 승인된 IT 서비스 카탈로그를 생성하고 관리할 수 있다
* 일반적으로 배포되는 IT서비스를 중앙에서 관리하고 일관된 거버넌스를 달성, 규정준수 요구사항을 충족하는 동시에 사용자가 필요한 승인된 IT 서비스만을 빠르게 배포할 수 있다.

AWS System Manager

* AWS에서 인프라에 대한 가시성과 제어를 제공한다.
* 통합된 사용자 인터페이스를 제공하므로 여러 AWS 서비스의 운영 데이터를 보고 AWS리소스 전체에서 운영작업을 자동화
* 리소스 및 앱 관리를 단순화하고 운영 문제를 감지 및 해결하는 시간을 단축하며 규모에 맞게 인프라를 쉽게 운영 및 관리

AWS Managed Services

* 애플리케이션에 집중할 수 있도록 AWS인프라를 지속적으로 관리한다
* 변경 요청, 모니터링, 패치관리, 보안 및 백업 서비스와 같은 일반적인 활동을 자동화하고 전체 라이프사이클 서비스를 제공하여 인프라를 프로비저닝, 실행등을 지원한다.

Amazone EMR

* 동적으로 확장가능한 EC2인스턴스에서 방대한 양의 데이터를 쉽고 빠르며 비용효율적으로 처리할 수 있는 관리형 하둡 프레임 워크를 제공하는 서비스이다

Amazone Cognito

* 웹 및 모바일 앱에 대한 사용자 등록, 로그인 액세스 제어를 빠르고 쉽게 추가할 수 있다.

Amazone Artifact

* 중요한 규정 준수 관련 정보에 대한 리소스

Amazone SWF

* 개발자가 병렬 또는 순차적 단계가 있는 백그라운드 작업을 빌드, 실행 및 확장하는데 도움이 된다