AWS project2

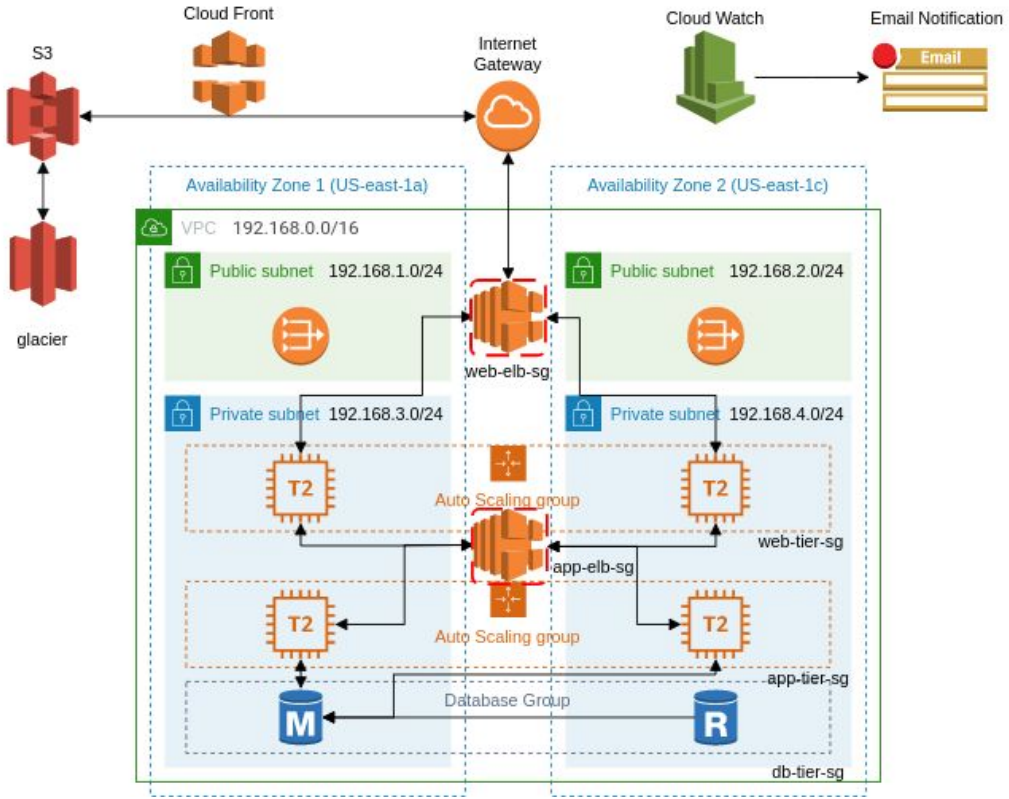
원혜진

Design - Network

VPC	Region	Purpose	Subnets	AZs
1	US-east-1	default	6	2
2	US-east-1	test	5	2

Subnet Name	VPC	Subnet Type(public/private)	AZ	Subnet Address
public1	2	public	a	192.168.1.0/24
public2	2	public	c	192.168.2.0/24
private1	2	private	a	192.168.3.0/24
private2	2	private	c	192.168.4.0/24
db-subnet	2	private	a	

Architecture Diagram



Design - Security

Security Group(SG)	SG Name	Rule	Source
ELB load balancer	web-elb-sg	80	0.0.0.0/0
Web Tier	web-tier-sg	80	web-elb-sg
App load balancer	app-elb-sg	80	web-tier-sg
App Tier	app-tier-sg	80	app-elb-sg
Database tier	db-tier-sg	3306	app-tier-sg

Design - Encryption

Requirement	Solution
Encryption option for data at rest	- RDS 암호화 - S3 서버 측 암호화 - AWS Key Management Service를 사용
Encryption option for data in transit	- SSL 인증서 사용

Design - Instance Details

Tier	AMI	Tag	Type	Size	Justification	# of instances
Web	Linux	Key : Name Value : web-tier	t2	micro	서버에서 75%이상의 메모리를 사용하면 인스턴스 개수를 늘리고, 5~60%일때는 인스턴스 개수를 줄인다.	4
App	Linux	Key : Name Value : app-tier	t2	micro	서버에서 90%이상의 메모리와 CPU를 사용하면 인스턴스 개수를 늘리고, 5~60%일때는 인스턴스 개수를 줄인다.	4
DB	SUSE Linux	N/A	t2	micro	RDS 인스턴스는 물리적 저장소로 필요에 따라 사이즈를 바꿀 수 있다.	2

Design - Recovery Point Objective

Q. 4시간 동안 복구 시점 목표(RPO)를 달성하려면 어떻게 해야 합니까?

A. 서버는 stateless하기 때문에, 스냅샷을 RDS DB에서만 매번 4시간 마다 구성해야 한다.
다른 옵션들은 비용이 많이 들기 때문에 사용하기 않는것이 좋다.

Design - Document Storage

Storage/Archive Option	Detail
S3 Bucket	드물게 문서에 접근하는 경우 저장한다. 3개월 이상 사용되지 않을 경우 glacier로 옮긴다. 6개월 이상 사용되지 않으면 삭제된다.
Amazon glacier	s3 Bucket에 문서가 더 이상 존재하지 않기 때문에 미리 정해진 시간이 지나면 문서가 완전히 삭제된다.

Design - Web Tier

Requirement	Solution
아키텍처는 유연해야 하며 트래픽이나 성능의 피크를 처리해야 합니다.	Elastic Load Balancers와 Auto-Scalers를 사용한다.
전체적으로 허용되는 수신 네트워크 대역폭은 300~750Mbps 입니다.	CloudWatch와 Auto-scalers를 통해 수신 대역폭이 750Mbps일때, 새로운 웹 서버를 생성하여 대역폭을 유지할 수 있다.
"400 HTTP 오류"가 분당 100건 이상 발생할 경우, 애플리케이션 관리자는 이메일로 통보를 받고자 합니다.	CloudWatch를 통해 웹서버의 웹로그를 '400 HTTP errors' 일때 알람을 보내도록 설정하고, 100번이 넘어가면 이메일로 통보하도록 한다.

Design - App Tier

Requirement	Solution
아키텍처는 유연해야 하며 트래픽이나 성능의 피크를 처리해야 합니다.	Auto-Scaling 그룹은 높은 트래픽이나 성능 피크를 잘 다룰수 있다.
전체 메모리 및 CPU 사용률은 각각 80% 및 75%를 초과해서는 안되며 각각 30% 미만이 되어서도 안됩니다.	CloudWatch는 메모리 사용량이 75%를 넘어서지 않게 하고, 30% 미만이 되지않도록 구성되었다.
서버를 노출시키지 않고 패치 및 업데이트를 위한 인터넷 액세스가 필요합니다.	VPC를 NAT Gateway로 설정하고 로컬이 아닌 트래픽만 라우팅하도록 한다.

Design - Database Tier

Requirement	Solution
데이터베이스는 21,000 IOPS의 일관된 스토리지 성능을 필요로 합니다.	프로비저닝 된 볼륨은 최대 30,000 IOPS를 허용하며,이 볼륨을 사용하여 데이터베이스를 설정하면 21,000 IOPS에 적합하다.
고가용성은 하나의 요구 사항에 속합니다.	한개의 az에 마스터 RDS DB를 두고, 두번째 RDS DB를 또다른 az에 위치하게 하여, 고가용성을 충족시킨다.
이때 데이터베이스 스키마를 변경할 수 없습니다.	5.7.22 MySQL 엔진은 클라우드로 원활하게 전환가능하다.