Architecting with AWS (실습편)

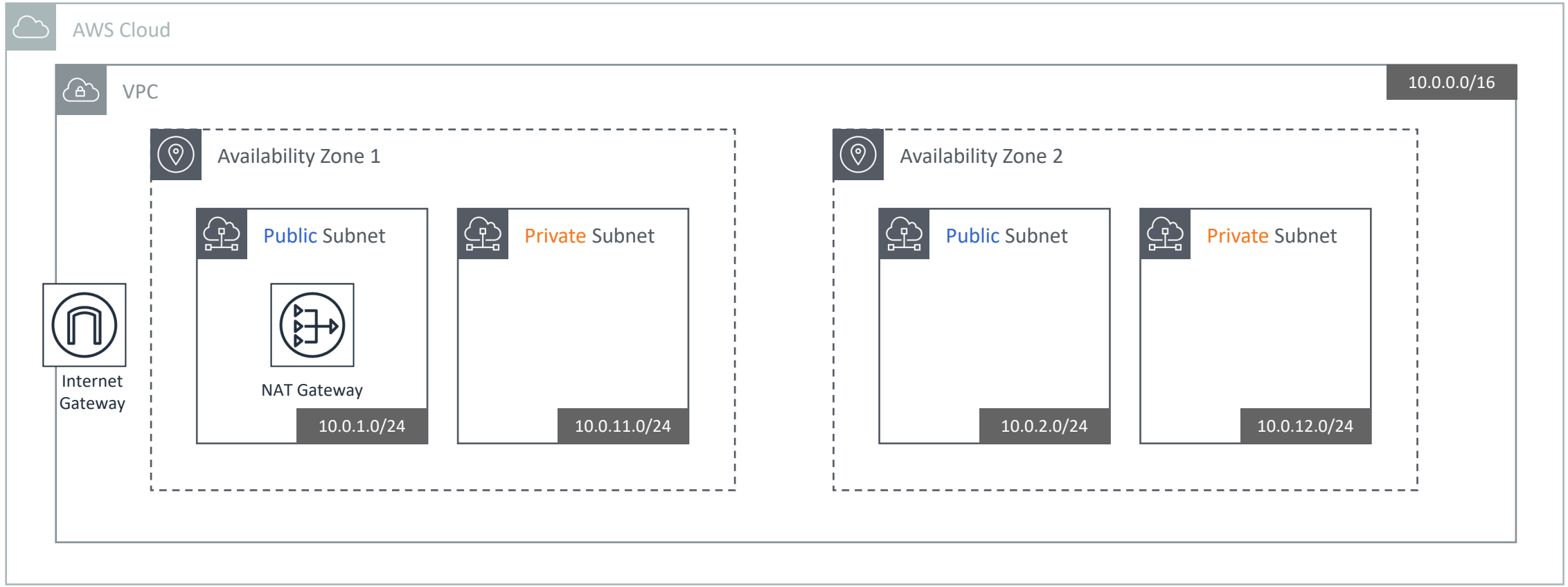
GSNeotek

COPYRIGHT 2021 GS NEOTEK ALL RIGHTS RESERVED

01

기본 네트워크 구성

STEP 1. 기본 네트워크 구성



Public Subnet's Route table

172.16.0.0
172.16.1.0
172.16.2.0

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-xxxxxxxx

Private Subnet's Route table

172.16.0.0
172.16.1.0
172.16.2.0

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	nat-xxxxxxxx

GS Neotek

STEP 1. 기본 네트워크 구성

1-1. VPC 생성

1-2. VPC Subnet 생성 x 4EA

1-3. Route Table 생성 x 2EA

1-4. Internet G/W 생성 + Attach to VPC

1-5. NAT G/W 생성

1-6. Route Table 규칙 수정 x 2EA

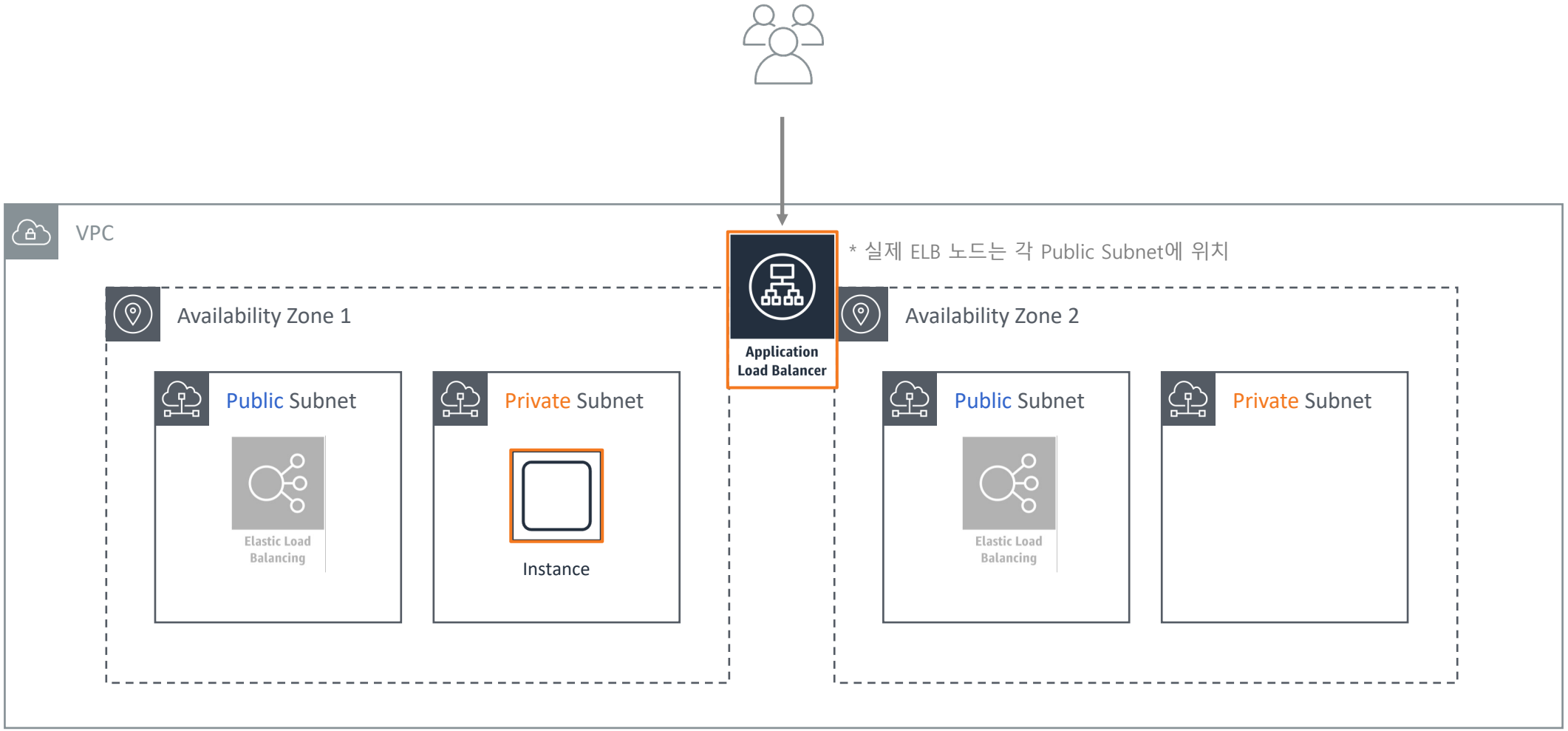
1-7. VPC Subnet에 Route Table 연결

GS Neotek

02

단일 EC2 인스턴스 + LB 구성

STEP 2. 단일 EC2 인스턴스 + Load Balancer 구성



GS Neotek

STEP 2. 단일 EC2 인스턴스 + Load Balancer 구성

2-1. EC2 인스턴스 생성

2-2. EC2 인스턴스 상태 확인

2-3. ELB(Application LB) 생성

2-4. Target Group 생성 + EC2 인스턴스 등록

2-5. Target Group에서 EC2 Status 확인

2-6. 웹브라우저에서 ELB 주소로 요청/테스트

2-7. (페이지가 뜨지 않을 경우) 원인 찾기

GS Neotek

STEP 2. 단일 EC2 인스턴스 + Load Balancer 구성

하단 예시의 스크립트(**웹 서버 구축**) 를 복사 후 user-data 항목에 붙여넣기

User Data 예시

```
#!/bin/sh
yum -y install httpd php php-mysql
chkconfig httpd on
systemctl start httpd
cd /var/www/html
wget dbxh6vyykosu3.cloudfront.net/web-php-v1.tar.gz
tar xvfz web-php-v1.tar.gz
yum -y update
amazon-linux-extras install -y epel
yum –y install stress
```

부하테스트(CPU) 시나리오

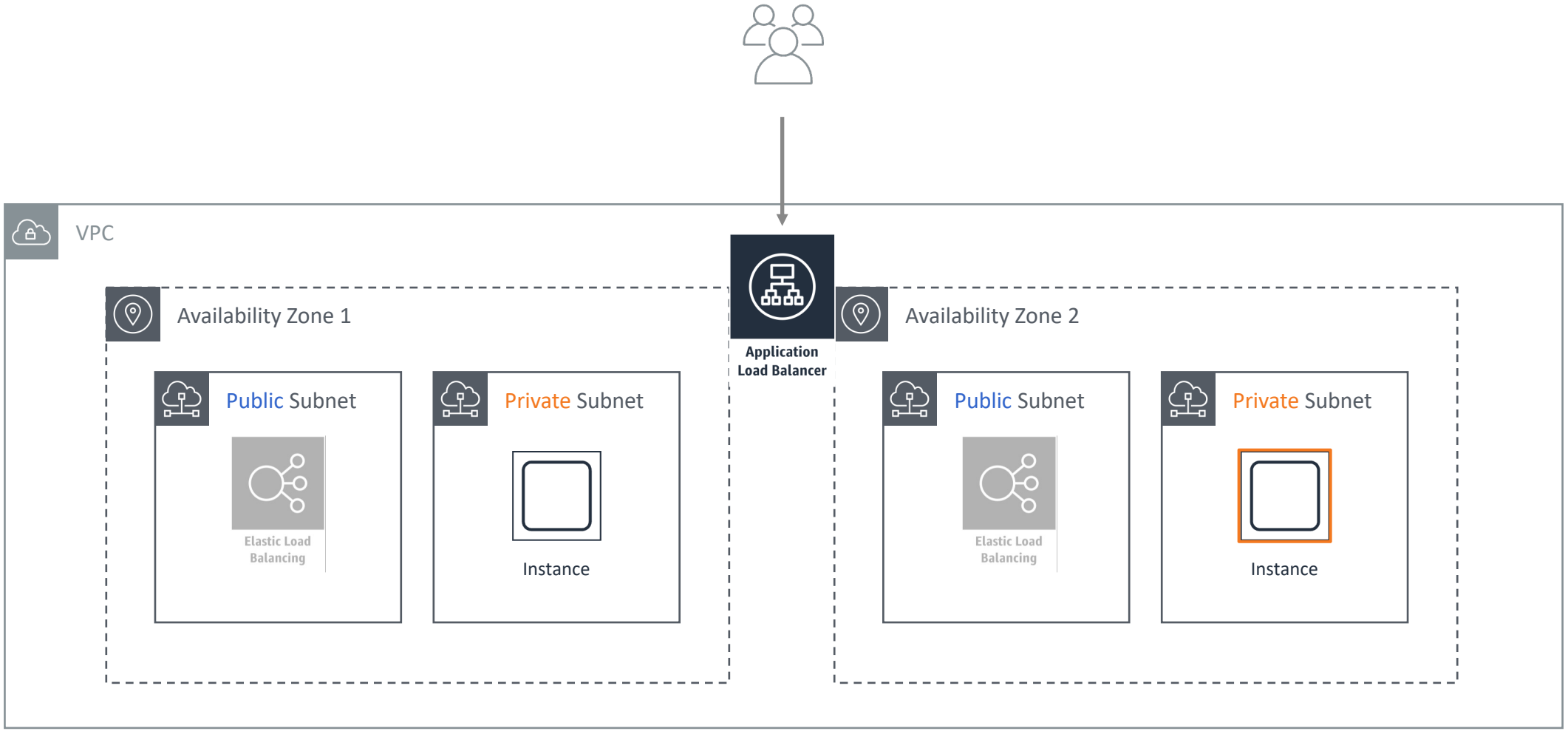
```
stress --cpu 1 --timeout 300s
```

GS Neotek

03

고가용성 구성

STEP 3. 고가용성 구성



GS Neotek

STEP 3. 고가용성 구성

3-1. AMI(Amazon Machine Image) 생성

3-2. 추가 EC2 인스턴스 생성

3-3. 추가 EC2 인스턴스를 Target Group에 추가

3-4. Target Group에 추가 인스턴스 Status 확인

3-5. 웹브라우저에서 ELB 주소로 요청/테스트

3-6. 특정 EC2 인스턴스 중지 (시뮬레이션)

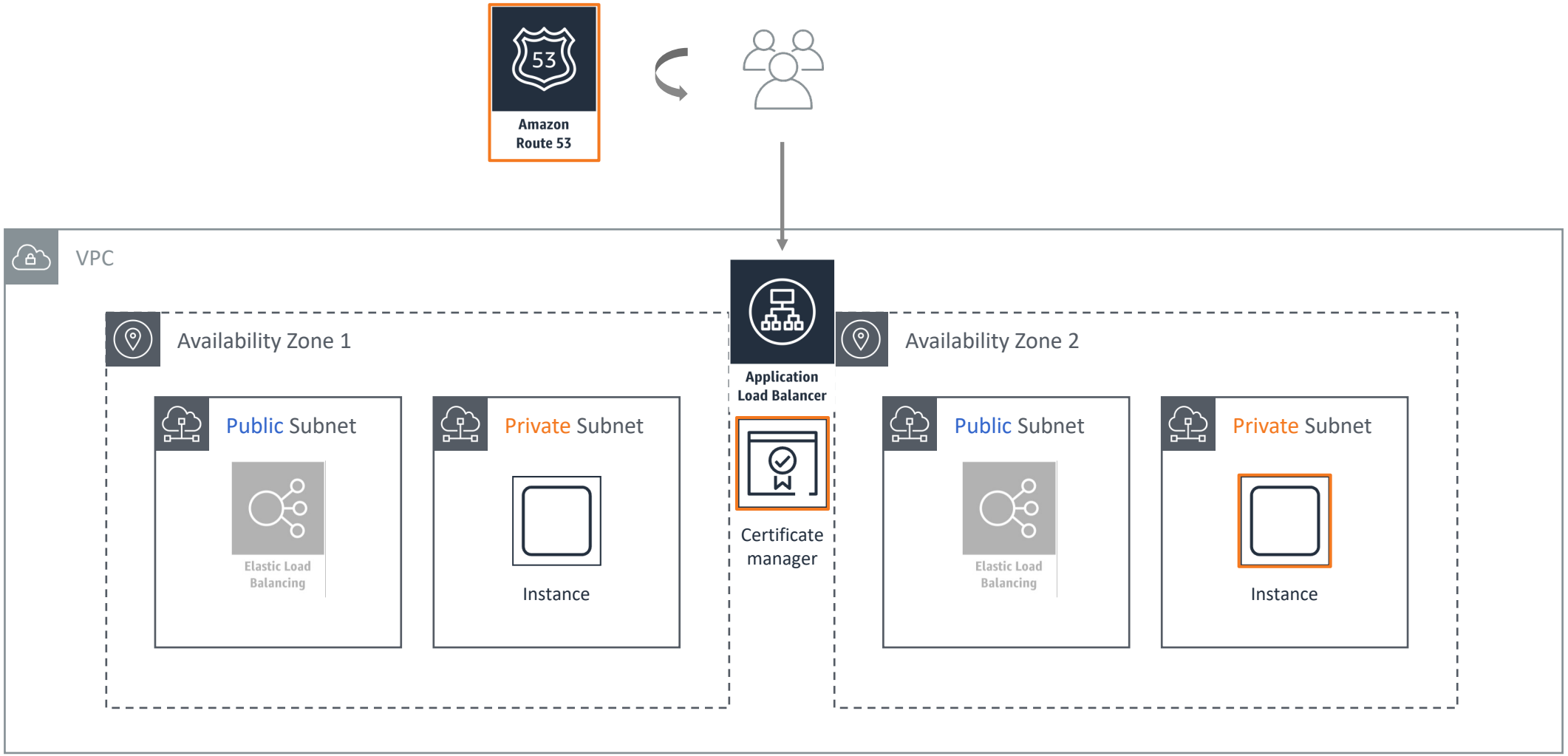
3-7. 웹브라우저에서 ELB 주소로 요청/테스트

GS Neotek

04

HTTPS 서비스 구성

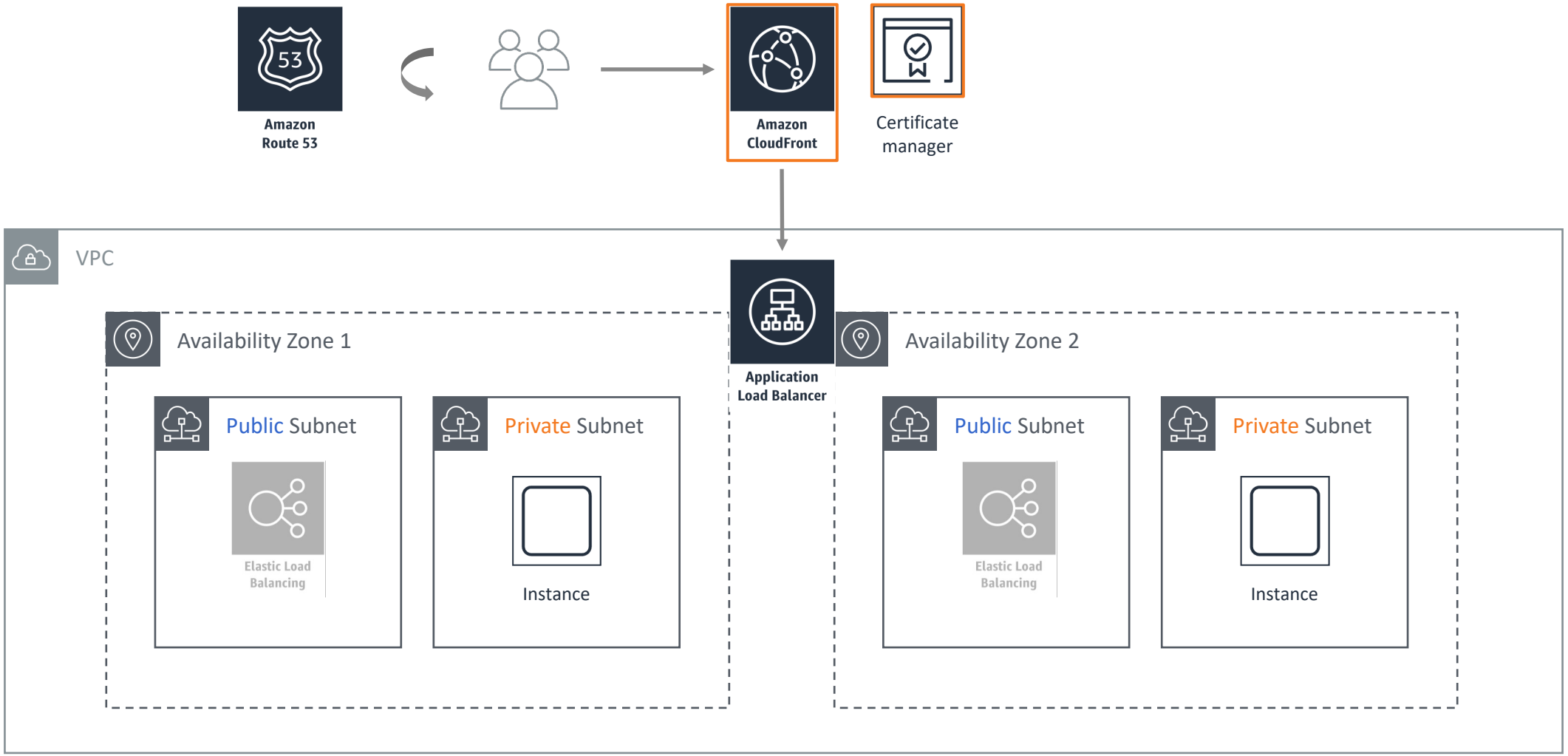
STEP 4. HTTPS 서비스 구성



05

CDN 계층 구성

STEP 5. CDN 계층 구성

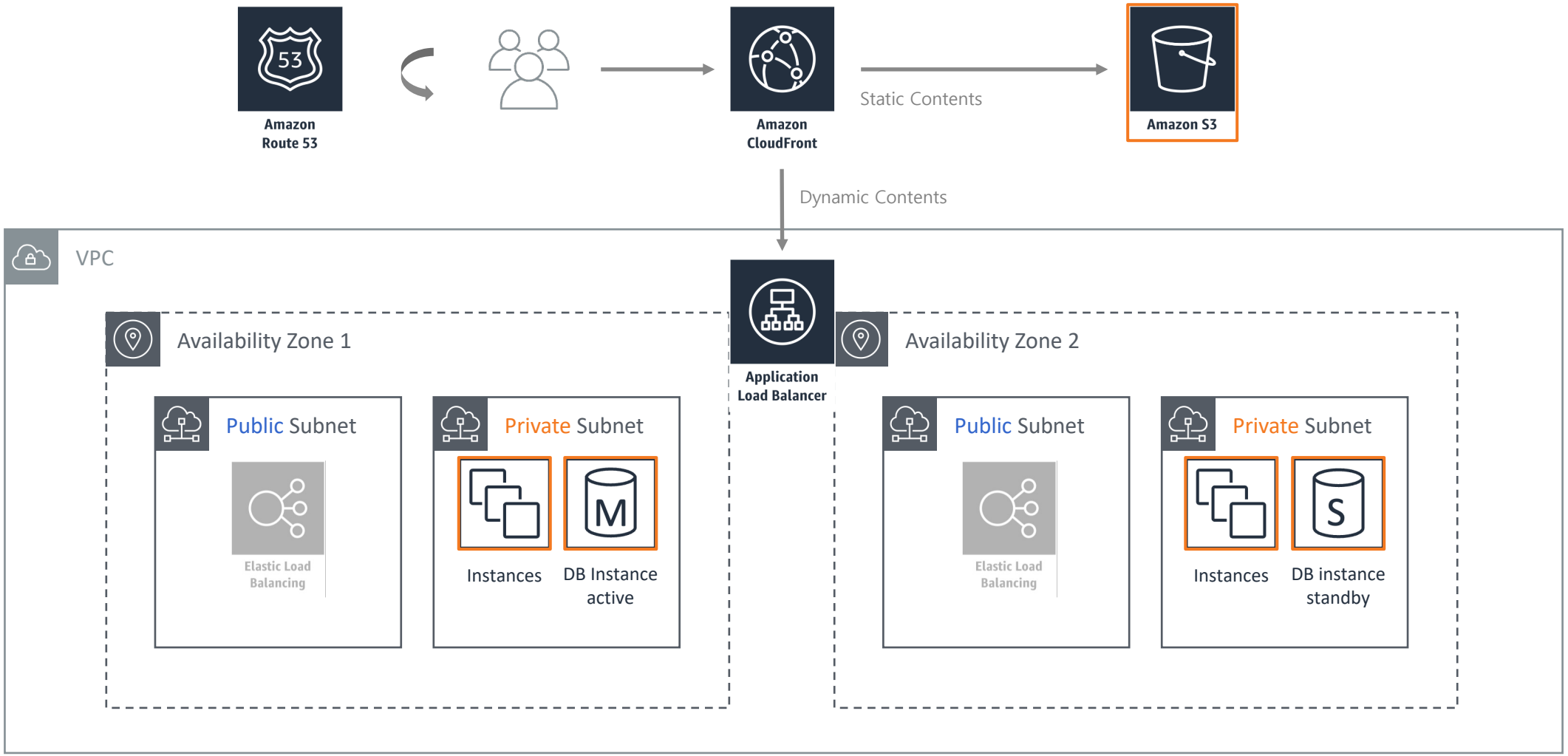


GS Neotek

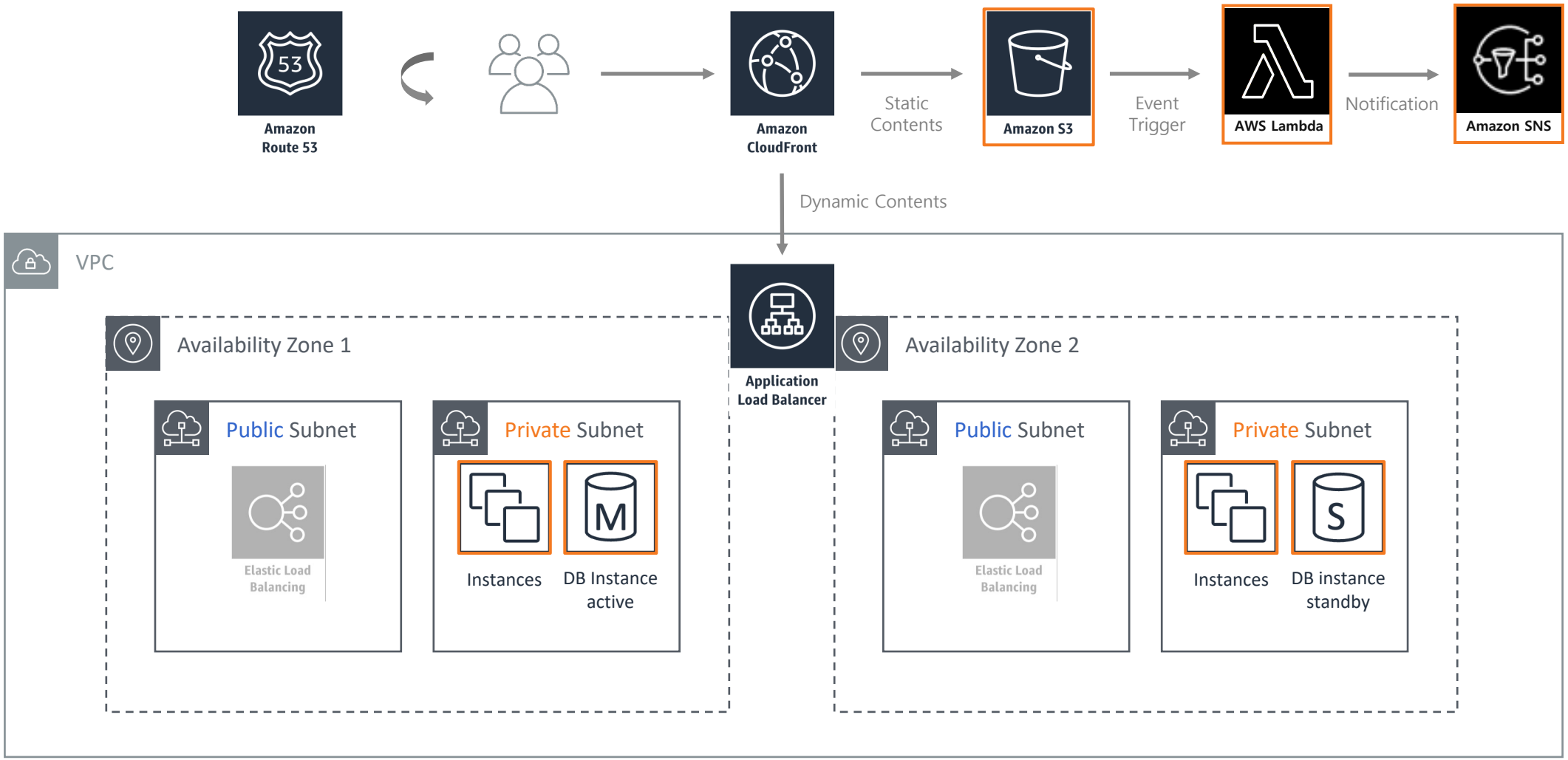
06

최종 표준 구성

STEP 6. 최종 표준 구성



(별첨). 이벤트 트리거 및 알람추가



GS Neotek

(별첨). 이벤트 트리거 및 알람추가

6-1. S3-bucket 생성

6-2. CloudFront의 Distribution 생성 및 버킷 연결 (OAI)

6-3. S3-bucket 파일 업로드

정적웹호스팅을 위한 파일 > 다운로드

https://github.com/jogilsang/cloudfront-s3

6-4. Cloudfront의 URL 경로로 index.html 접속

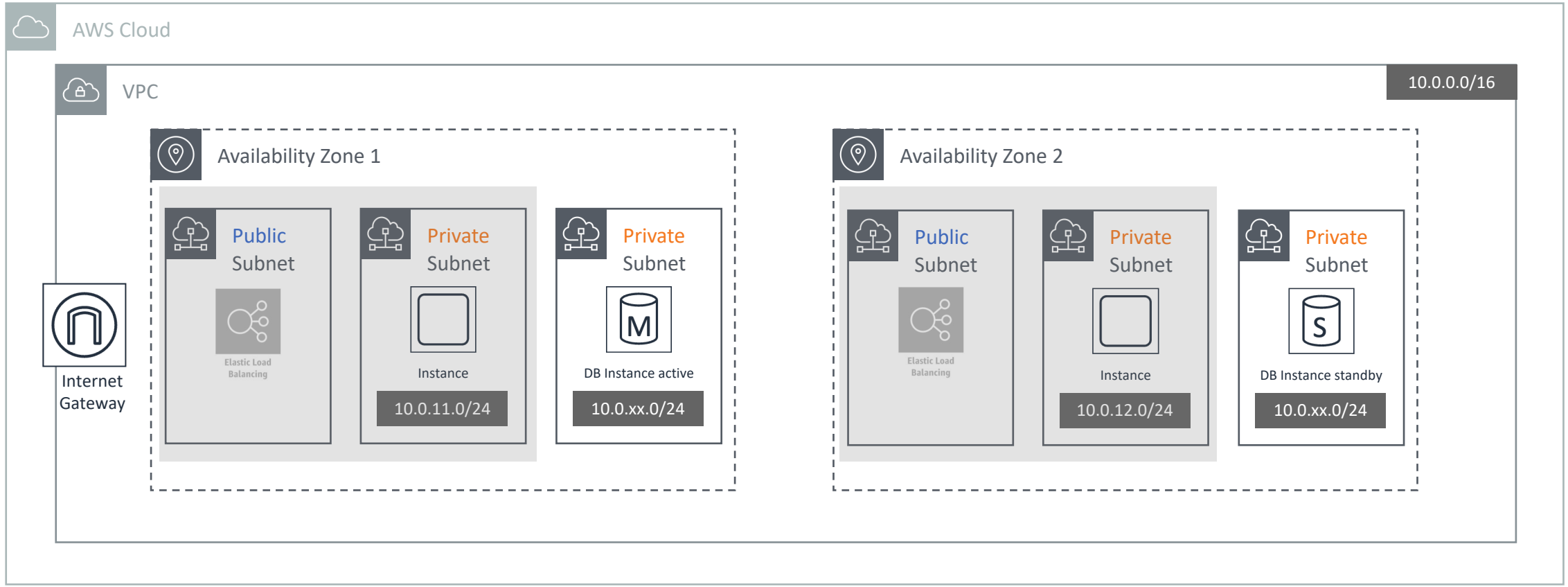
6-5. error.html을 이용한 에러페이지 설정

GS Neotek

07

(별첨) DB 인스턴스 구성

STEP 7. DB인스턴스 구성



Instance Security Group

Protocol	Port-Range	Source
TCP	80	LB-SG
TCP	443	LB-SG

RDS Security Group

Protocol	Port-Range	Source
TCP	3306	Instance-SG

GS Neotek

STEP 7. DB 인스턴스 구성

7-1. AWS RDS를 통해 DB인스턴스(MySQL) 생성

7-2. DB인스턴스에 대한 Security Group 수정

7-3. CLI를 이용한 DB Connection 확인

```
sudo yum install -y mysql
mysql -u admin -P 3306 -h [endpoint주소] -p [패스워드]
```

7-4. CLI를 이용한 TABLE 생성 및 SELECT 쿼리

```
-- DML
use mysql;
select user from user;
-- DDL
CREATE DATABASE test;
```

7-5. SNS 생성 및 DB인스턴스 FAIL OVER 이벤트 구독

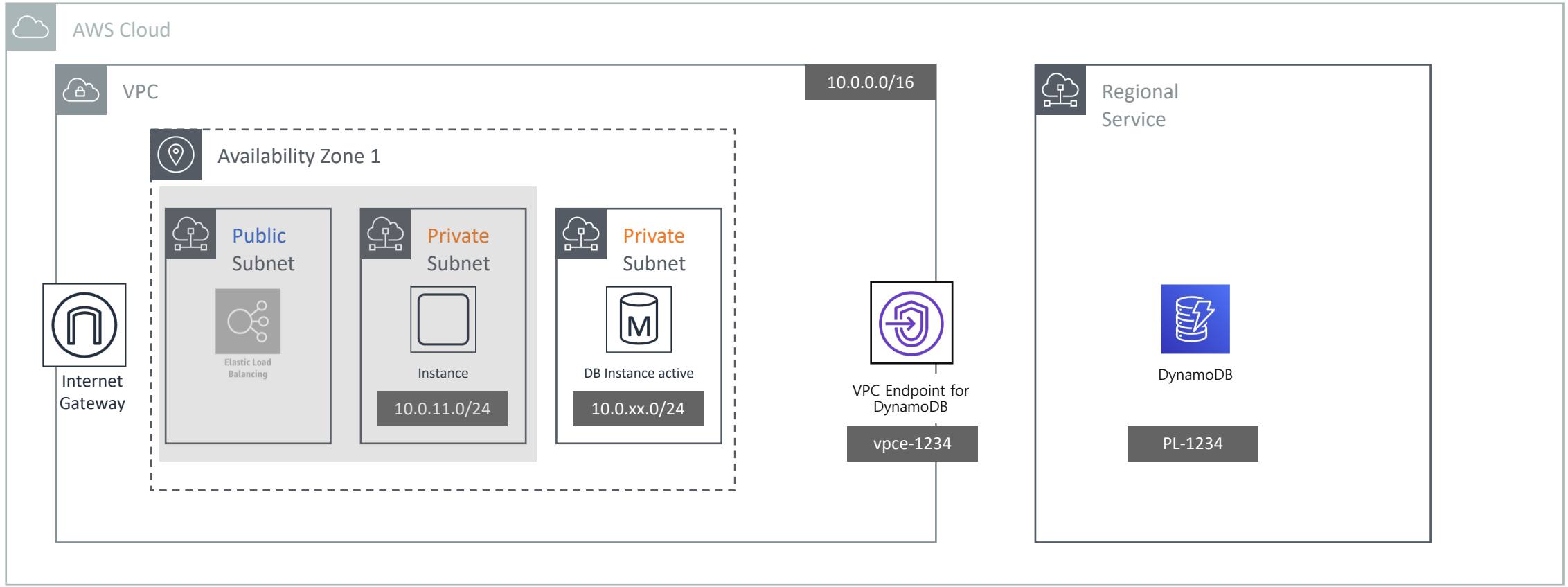
7-6. DB인스턴스 FAILOVER 알람 확인

GS Neotek

08

(별첨) DynamoDB 구성

STEP 8. DynamoDB 구성



Private Subnet's Route table

172.16.0.0
172.16.1.0
172.16.2.0

Destination	Target
PL-1234	vpce-1234
0.0.0.0/0	nat-xxxxxxxx
10.0.0.0/16	local

GS Neotek

STEP *8*. DynamoDB 구성

8-1. AWS DynamoDB 콘솔화면 둘러보기

8-2. 테이블 생성하기

8-3. 데이터 WRITE, READ 및 쿼리 진행

8-4. Global Secondary INDEX 생성 및 쿼리

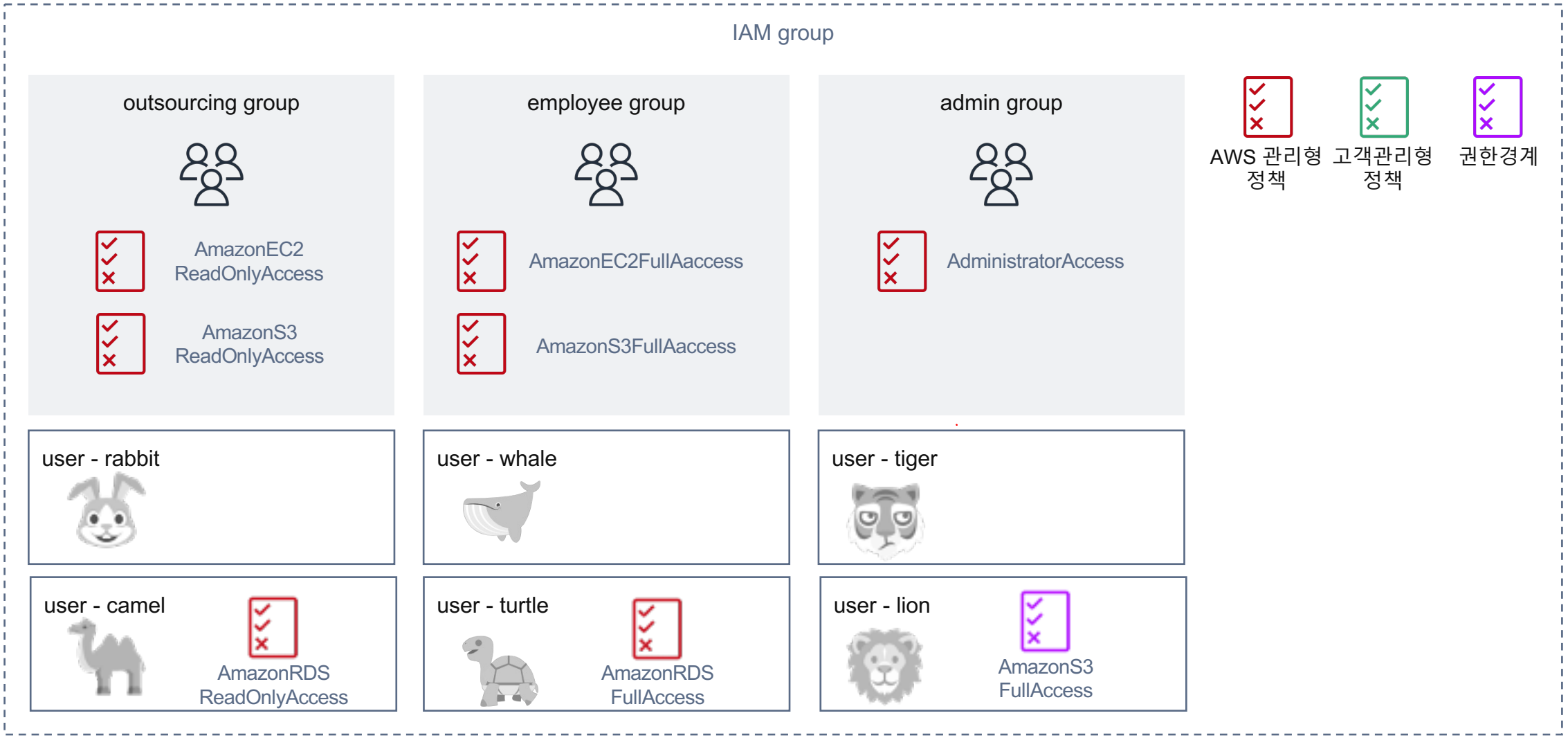
8-5. VPC Endpoint Gateway 생성 및 확인

GS Neotek

09

(별첨) IAM 구성

STEP 9. IAM 구성



GS Neotek

STEP 9. IAM 구성

하단 예시중에 1개 선택 후 진행

STEP 9-1. Role – 신뢰정책(Trust Entity)

```
{
        "Version": "2012-10-17",
        "Statement": [
                {
                        "Effect": "Allow",
                        "Principal": {
                                "AWS": "arn:aws:iam::[account-id]:root"
                },
                        "Action": "sts:AssumeRole",
                        "Condition": {}
                }
        ]
}
```

STEP 9-2. Role – 정책부여(Policy)

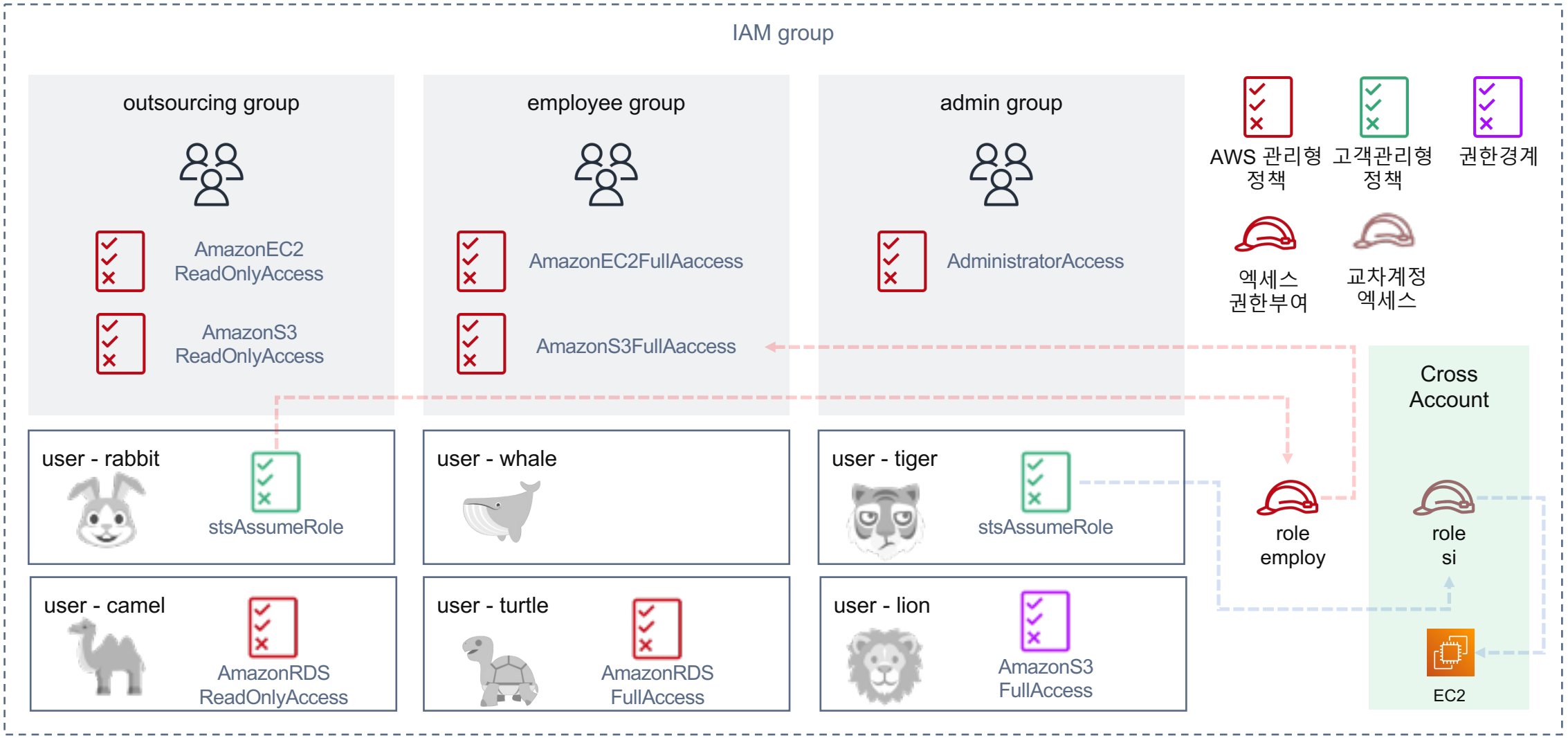
SupportUser

ReadOnlyAccess

AWSSupportAccess

GS Neotek

STEP 9. IAM 구성



GS Neotek

STEP 9. IAM구성

9-1. 사용자(User) 생성

9-2. 그룹(Group) 생성

9-3. 그룹에 정책(Policy) 추가

9-4. 그룹에 사용자 추가

9-5. 사용자 별 로그인 후 권한확인

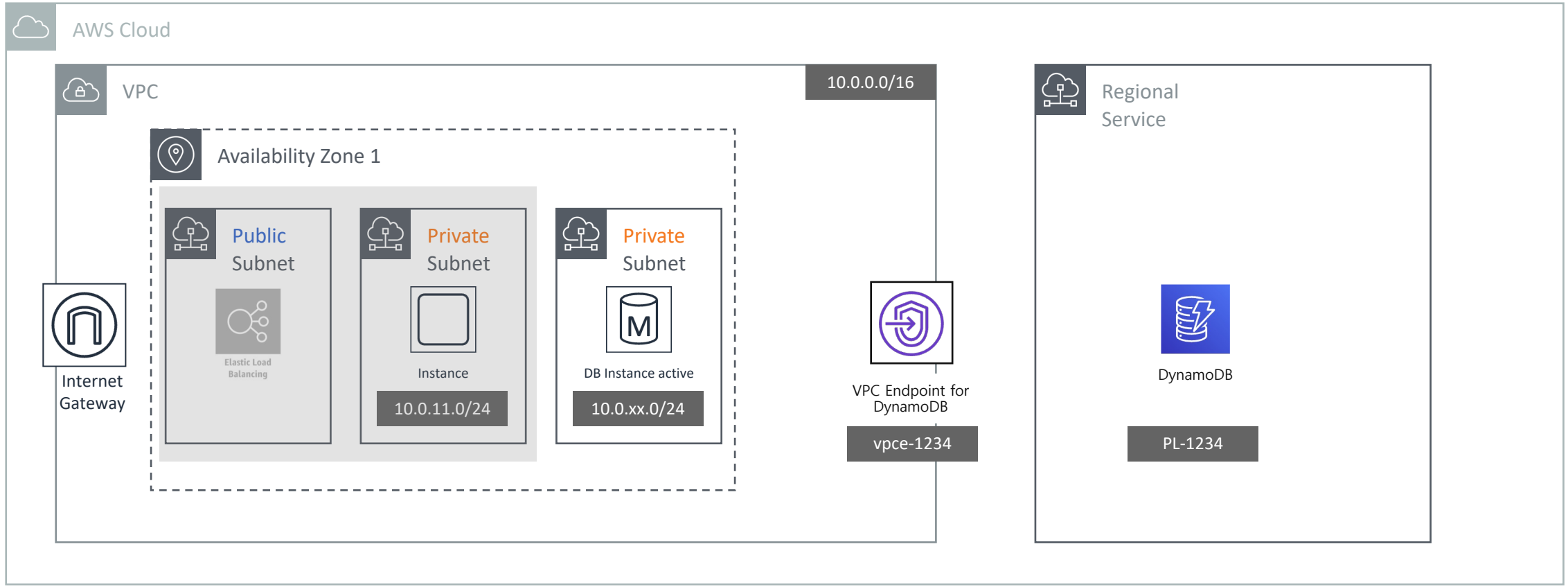
9-6. 역할전환(Role Switch) 이해

GS Neotek

09

(별첨) Auto Scaling Group 구성

STEP 8. DynamoDB 구성



Private Subnet's Route table

172.16.0.0
172.16.1.0
172.16.2.0

Destination	Target
PL-1234	vpce-1234
0.0.0.0/0	nat-xxxxxxxx
10.0.0.0/16	local

GS Neotek

STEP *8*. DynamoDB 구성

8-1. AWS DynamoDB 콘솔화면 둘러보기

8-2. 테이블 생성하기

8-3. 데이터 WRITE, READ 및 쿼리 진행

8-4. Global Secondary INDEX 생성 및 쿼리

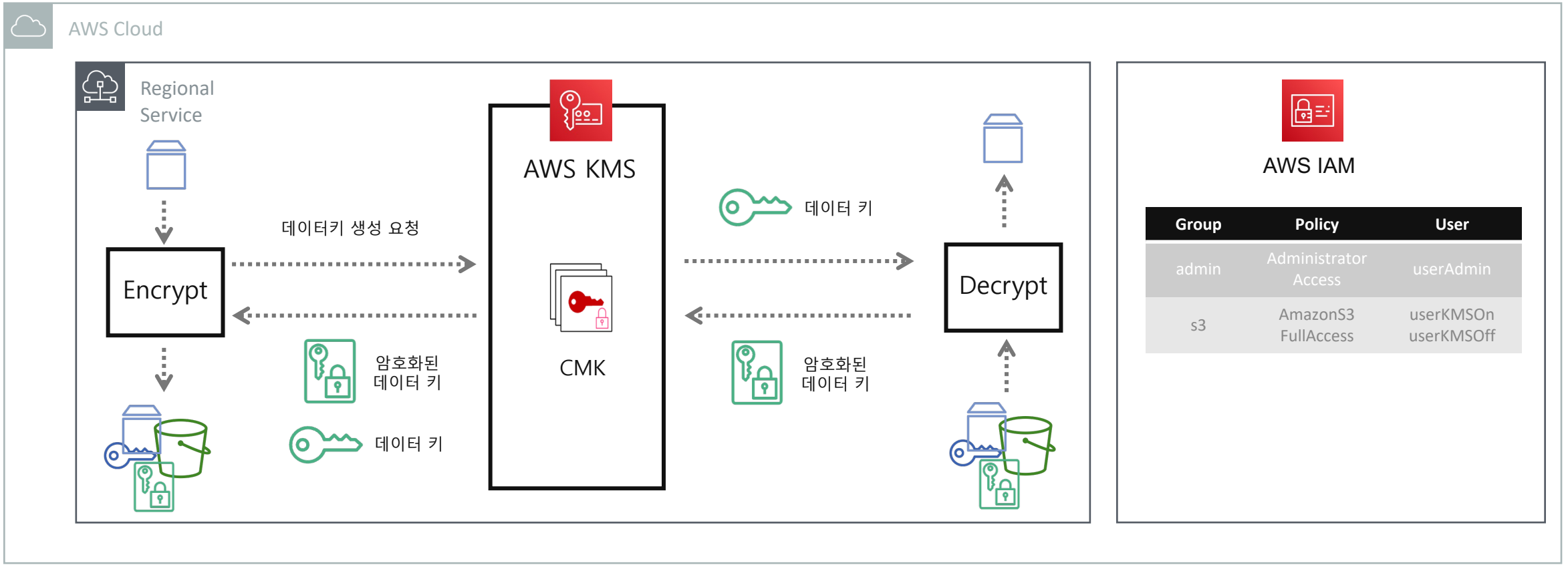
8-5. VPC Endpoint Gateway 생성 및 확인

GS Neotek

10

(별첨) KMS 실습

STEP 10. KMS 실습



GS Neotek

STEP *10*. KMS 실습

10-1. IAM 그룹 및 사용자 생성 (3)

10-2. KMS 접근 > 고객관리형 키 클릭

10-3. 키 생성 (대칭, 암호화 및 해독, KMS, 단일 리전)

10-4. 키 관리 및 사용 대상 확인 및 키 생성

10-5. S3 버킷 생성 후 SSE-KMS 설정

10-6. 파일 업로드 후 사용자 별 다운로드 진행

10-7. (과제) 파일 다운로드가 되지 않는 사용자 조치

Group

- Admin (AdministratorAccess)
  - userAdmin
- S3 (AmazonS3FullAccess)
  - userKMSOn
  - userKMSOff

KMS 관리 및 사용대상

- userKMSOn - 허용
- userKMSOff - 비 허용

GS Neotek

Thank you