

AWS 네트워크

AWS Cloud Club

DDWU ACC Crew

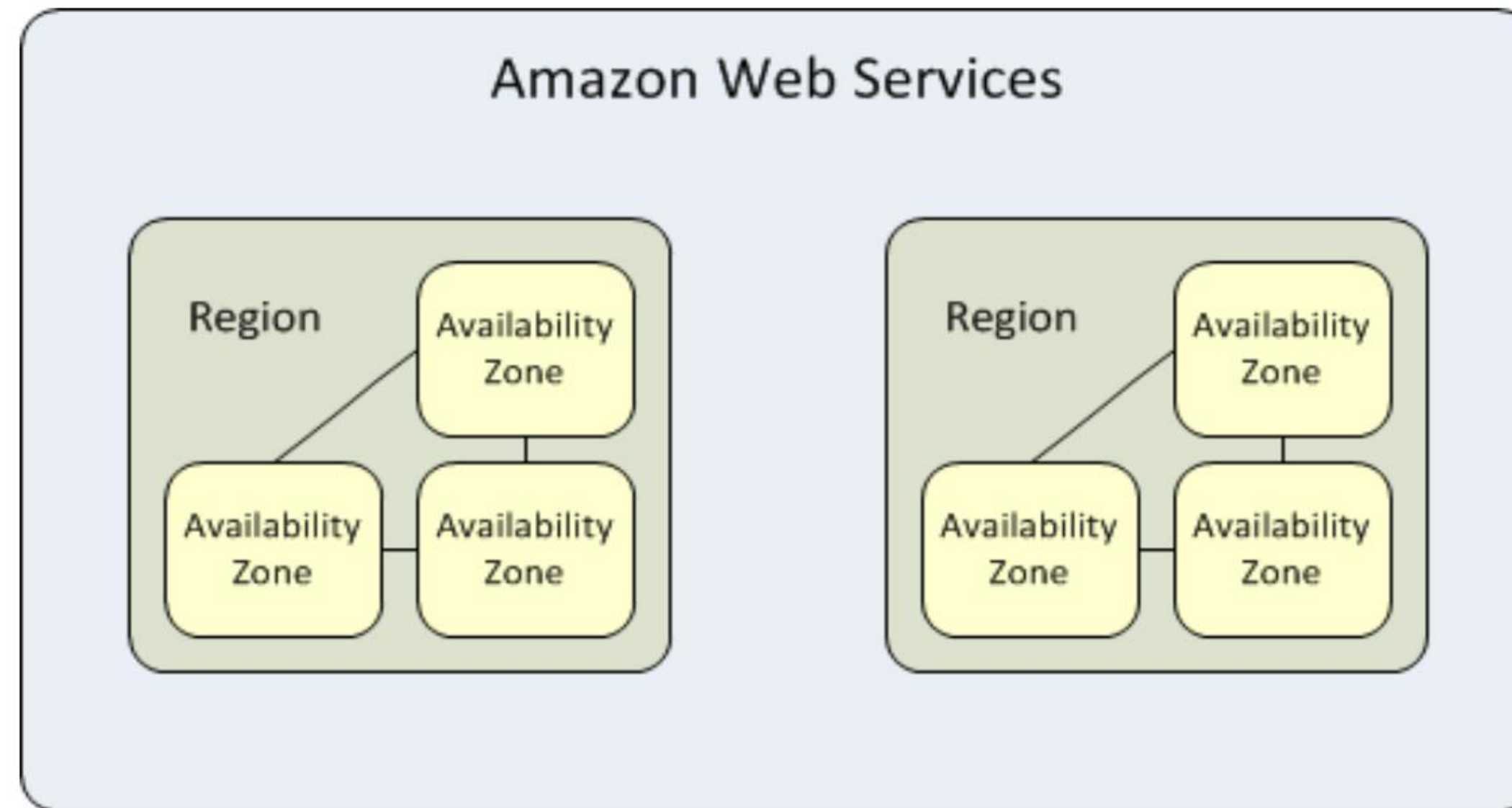
류혜수

VPC



ip대역의 일부를 할당해서 만드는 가상의 네트워크

리전(Region)과 AZ(가용영역)



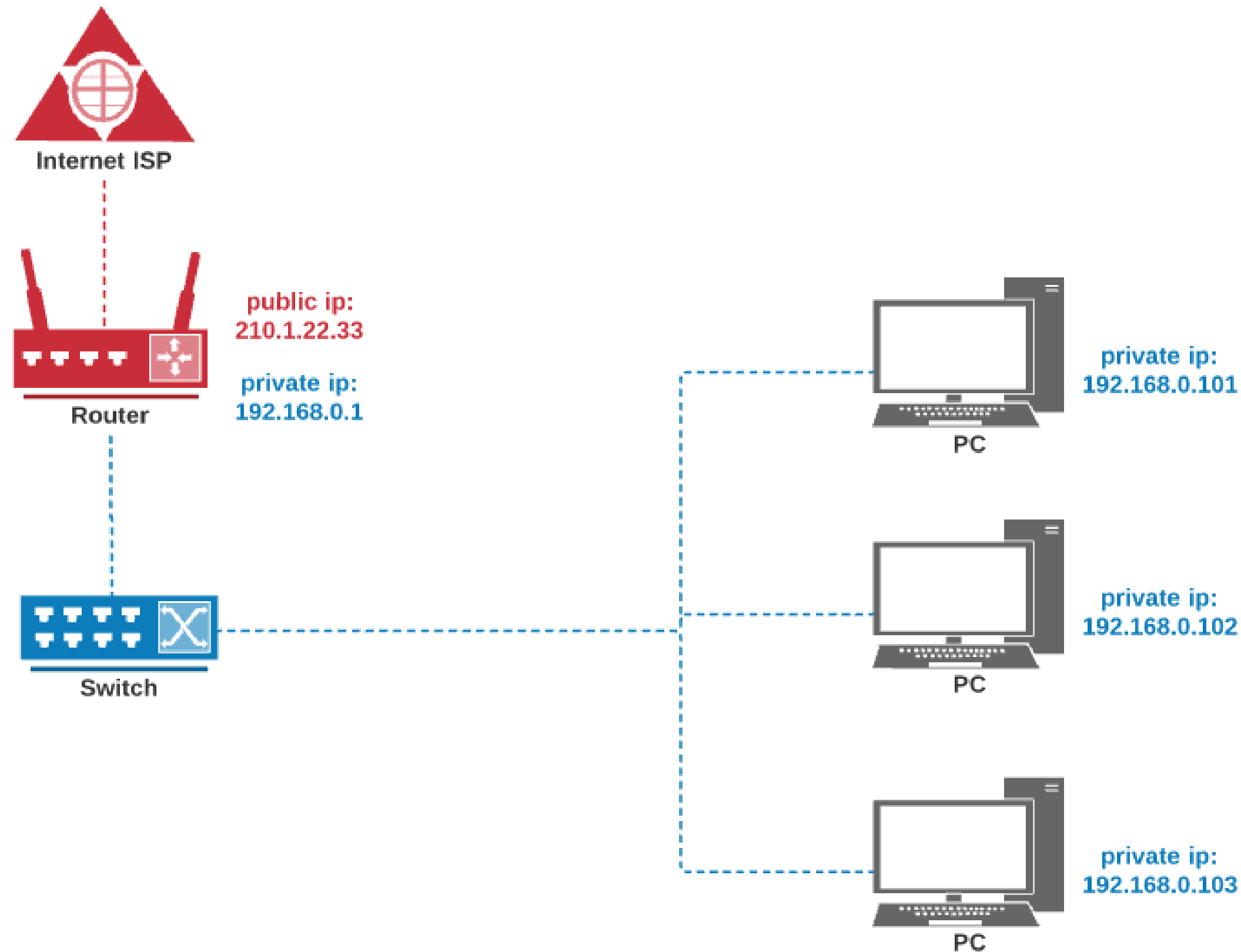
리전은 aws 서비스가 위치한 지리적 장소,
하나의 리전에는 다수의 AZ(가용영역)이 있음

Mult AZ를 통한 고가용성 확보

Multi 데이터센터는 지진같은 천재지변으로 인한 데이터센터 장애나 데이터센터 자체의 전력, 네트워크 장애에 대비하기 위한 이중화 구성이다.

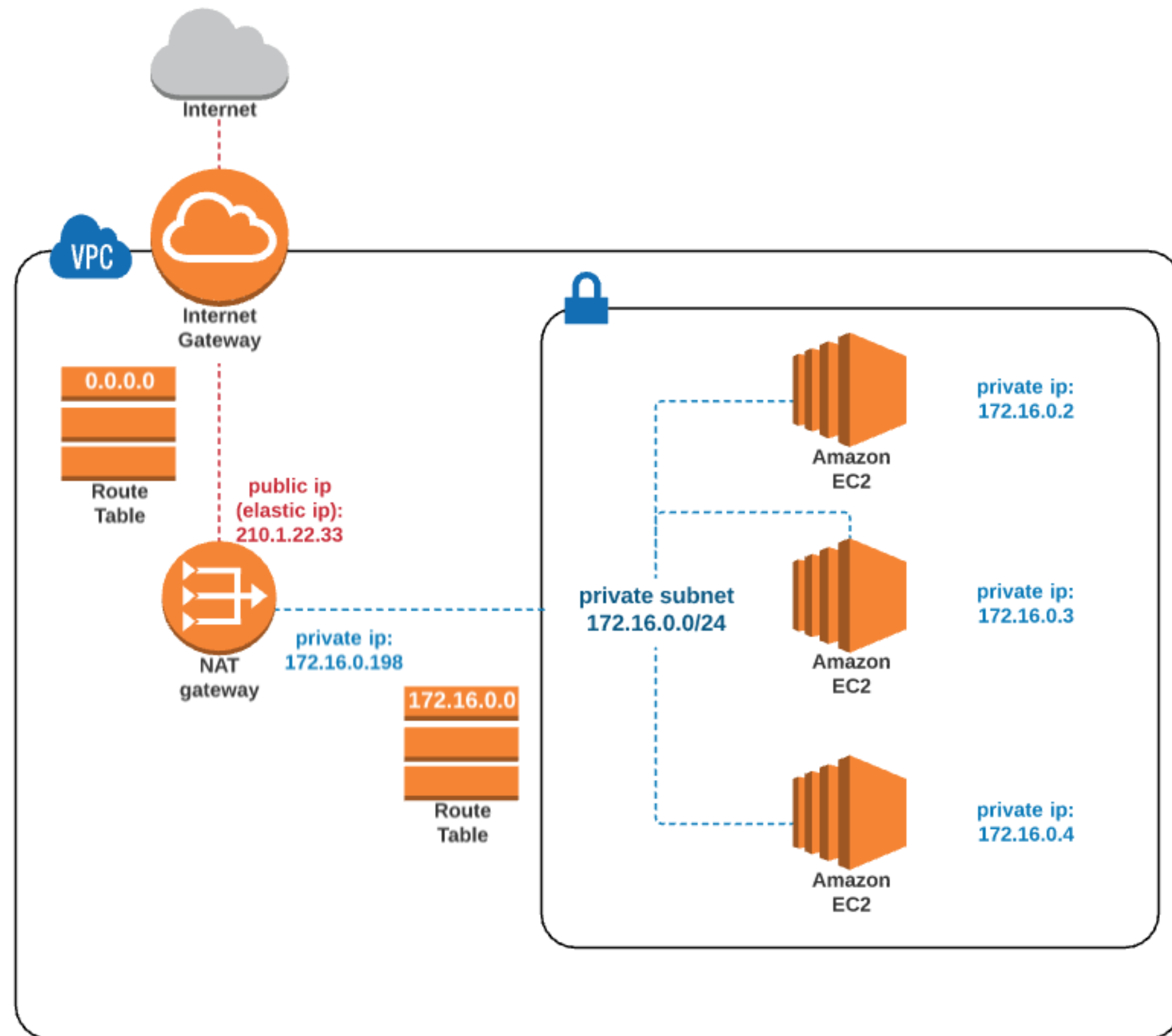
VPC 를 디자인 할때 Multi AZ를 기반으로 구성한다면, 사용자는 물리적으로 다수의 데이터센터를 이용하는 것과 같은 효과를 볼 수 있다

물리 네트워크 vs VPC



- 라우터 : 서로 다른 네트워크(subnet mask가 다른) 간의 통신 중계
- 스위치 : 각 포트에 연결된 MAC 주소를 기억하여 요청에 대해 destination MAC 주소를 읽어 해당 port로 데이터를 전송함
- NAT : 공유기 내부 장치(PC)는 private IP만 할당되어 있으므로 공유기의 NAT 기능을 이용하여 외부로 나가는 요청을 public IP로 전환하거나, 요청에 대한 응답이 오면 내부 IP로 전달함
- DHCP : 공유기에 연결된 새로운 장비에 동적으로 IP 주소를 할당함
- 방화벽 : 내/외부로 오가는 IP/Port를 특정 규칙으로 통제함

물리 네트워크 vs VPC



- 라우터 : Internet Gateway + Route Table
- 스위치 : aws는 스위치를 별도로 구분하지 않고, Subnet이 (가상)스위치 기능을 대신함, 가상 라우터와 가상 인스턴스의 가상 NIC를 연결하는 접점이 되며, 하나의 가상 스위치는 하나의 서브넷이 할당됨.
- NAT : Nat instance 혹은 Nat gateway
- 방화벽 : NACL(network ACL)과 Security Group

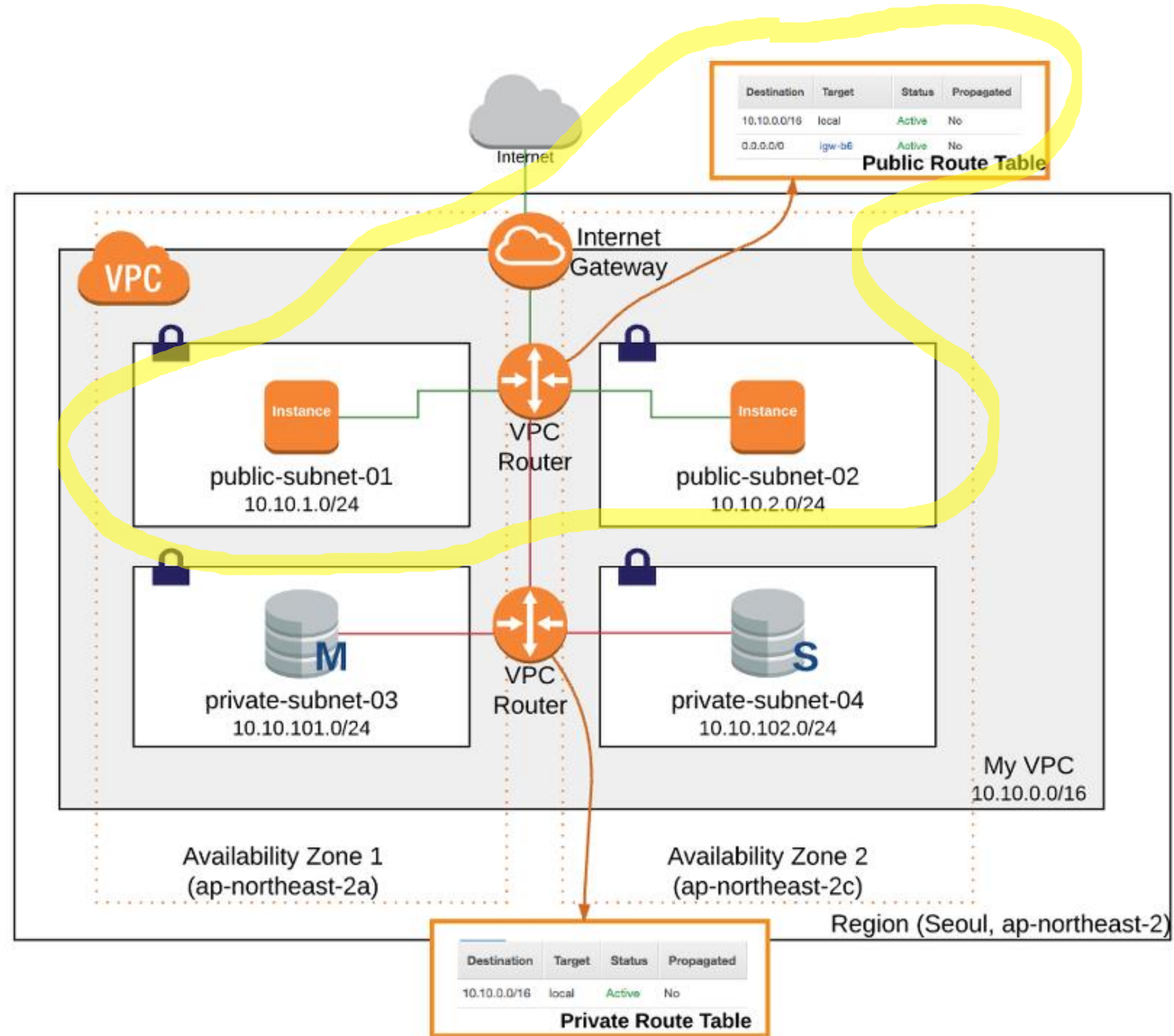
VPC의 리소스들

- Your VPCs
- Subnet
- Route tables
- Internet Gateways
- Egress Only Internet Gateways
- DHCP Options Sets
- Elastic IPs
- NAT Gateways
- Peering Connections

VPC의 리소스들

- Network ACLs
- Security Groups
- Customer Gateways
- Virtual Private Gateways
- VPN Connections

실습



CLI을 허용하는 IAM 계정 생성

[최신 버전의 AWS CLI설치 또는 업데이트 - AWS Command Line Interface \(amazon.com\)](#)

↗ AWS CLI 설치 및 업데이트 지침

설치 지침은 해당 운영 체제에 대한 섹션을 참조하세요.

▶ Linux

▶ macOS

▶ Windows

CLI을 허용하는 IAM 계정 생성

권한 설정

기존 그룹에 사용자를 추가하거나 새 그룹을 생성합니다. 직무별로 사용자의 권한을 관리하려면 그룹을 사용하는 것이 좋습니다. [자세히 알아보기](#)

권한 옵션

☐ 그룹에 사용자 추가
기존 그룹에 사용자를 추가하거나 새 그룹을 생성합니다. 그룹을 사용하여 직무별로 사용자 권한을 관리하는 것이 좋습니다.




☐ 권한 복사
기존 사용자의 모든 그룹 멤버십, 연결된 관리형 정책 및 인라인 정책을 복사합니다.

☒ 직접 정책 연결
관리형 정책을 사용자에게 직접 연결합니다. 사용자에게 연결하는 대신, 정책을 그룹에 연결한 후 사용자를 적절한 그룹에 추가하는 것이 좋습니다.

권한 정책 (1/1196)

새 사용자에게 연결할 정책을 하나 이상 선택합니다.

필터링 기준 유형
모든 유형

	정책 이름	유형	연결된 엔터티
<input type="checkbox"/>	 AccessAnalyzerServiceRolePolicy	AWS 관리형	0
<input checked="" type="checkbox"/>	 AdministratorAccess	AWS 관리형 - 직무	1
<input type="checkbox"/>	 AdministratorAccess-Amplify	AWS 관리형	0
...			

액세스 키 모범 사례 및 대안

보안 개선을 위해 액세스 키와 같은 장기 자격 증명을 사용하지 마세요. 다음과 같은 사용 사례와 대안을 고려하세요.

- 사용 사례

☒ Command Line Interface(CLI)
AWS CLI를 사용하여 AWS 계정에 액세스할 수 있도록 이 액세스 키를 사용할 것입니다.

☐ 로컬 코드
로컬 개발 환경의 애플리케이션 코드를 사용하여 AWS 계정에 액세스할 수 있도록 이 액세스 키를 사용할 것입니다.

☐ AWS 컴퓨팅 서비스에서 실행되는 애플리케이션
Amazon EC2, Amazon ECS 또는 AWS Lambda와 같은 AWS 컴퓨팅 서비스에서 실행되는 애플리케이션 코드를 사용하여 AWS 계정에 액세스할 수 있도록 이 액세스 키를 사용할 것입니다.

☐ 서드 파티 서비스
AWS 리소스를 모니터링 또는 관리하는 서드 파티 애플리케이션 또는 서비스에 액세스할 수 있도록 이 액세스 키를 사용할 것입니다.

☐ AWS 외부에서 실행되는 애플리케이션
이 액세스 키를 사용하여 AWS 리소스에 액세스해야 하는 AWS 외부의 데이터 센터 또는 기타 인프라에서 실행 중인 워크로드를 인증할 것입니다.

☐ 기타
귀하의 사용 사례가 여기에 나열되어 있지 않습니다.

계정 등록

액세스 키 검색 정보

액세스 키

분실하거나 잊어버린 비밀 액세스 키는 검색할 수 없습니다. 대신 새 액세스 키를 생성하고 이전 키를 비활성화합니다.

액세스 키

비밀 액세스 키

 AKIAYWBDGSLNLQOHCZFY

 ****

[표시](#)

```
aws configure
AWS Access Key ID [None] : 액세스 키
AWS Secret Access Key [None] : 비밀 액세스 키
Default region name [None] : ap-northeast-2
Default output format [None] : json
```

실습 - vpc 생성

1. vpc 생성

```
aws ec2 create-vpc --cidr-block 192.168.0.0/16 --tag-specification  
"ResourceType=vpc,Tags=[{Key=Name,Value=vpc-test}]" --output text
```

```
C:\>aws ec2 create-vpc --cidr-block 192.168.0.0/16 --tag-specification "ResourceType=vpc,Tags=[{Key=Name,Value=vpc-test}]" --output text  
VPC      192.168.0.0/16  dopt-07658f5905c1a0599  default False  597074285399  pending vpc-062bda76521aa3c8a  
CIDRBLOCKASSOCIATIONSET vpc-cidr-assoc-00dd0699994f92c57  192.168.0.0/16  
CIDRBLOCKSTATE  associated  
TAGS      Name      vpc-test
```

1-1 vpc 확인

```
aws ec2 describe-vpcs
```

실습 - public subnet

2. 퍼블릭 서브넷 생성

(ap-northeast-2a와 ap-northeast-2c에 각각 퍼블릭 서브넷 생성)

```
aws ec2 create-subnet --vpc-id vpc-062bda76521aa3c8a --cidr-block  
192.168.0.0/20 --availability-zone ap-northeast-2a --tag-specification  
"ResourceType=subnet,Tags=[{Key=Name,Value=test-public-subnet-2a}]"
```

```
aws ec2 create-subnet --vpc-id vpc-062bda76521aa3c8a --cidr-block  
192.168.32.0/20 --availability-zone ap-northeast-2c --tag-specification  
"ResourceType=subnet,Tags=[{Key=Name,Value=test-public-subnet-2c}]"
```

실습 - public subnet-igw

2-1 인터넷 게이트 웨이 생성

```
aws ec2 create-internet-gateway --tag-specifications  
"ResourceType=internet-gateway,Tags=[{Key=Name,Value=test-igw}]"
```

2-2 인터넷 게이트웨이와 vpc 연결

```
aws ec2 attach-internet-gateway --vpc-id vpc-062bda76521aa3c8a --  
internet-gateway igw-059c90f322a4f710f
```

2-3 확인

```
aws ec2 describe-internet-gateways
```

실습 - public subnet-route-table

2-4 퍼블릭 라우팅 테이블 생성

```
aws ec2 create-route-table --vpc-id vpc-062bda76521aa3c8a --tag-specification "ResourceType=route-table,Tags=[{Key=Name,Value=test-public-route-table}]"
```

2-5 퍼블릭 라우팅 테이블에 igw 라우팅 정보 추가

```
aws ec2 create-route --route-table-id rtb-09aaf805564836532 --destination-cidr-block 0.0.0.0/0 --gateway-id igw-059c90f322a4f710f
```

2-6 확인

```
aws ec2 describe-route-tables --query "RouteTables[*].{Routes:Routes,Tags:Tags}"
```


실습 - public subnet-route-table

2-7 퍼블릭 라우팅 테이블을 퍼블릭 서브넷에 연결

```
aws ec2 associate-route-table --subnet-id subnet-0b2cd27778eedaa74 --  
route-table-id rtb-09aaf805564836532
```

```
aws ec2 associate-route-table --subnet-id subnet-0252aa7f87121cfd8 --  
route-table-id rtb-09aaf805564836532
```

실습 - public subnet

2-8 퍼블릭 IP주소 자동할당 (false -> true)

```
aws ec2 modify-subnet-attribute --subnet-id subnet-0252aa7f87121cfd8 --  
map-public-ip-on-launch
```

```
aws ec2 modify-subnet-attribute --subnet-id subnet-0b2cd27778eedaa74 --  
map-public-ip-on-launch
```

2-9 vpc dns 호스트 네임 활성화

```
aws ec2 modify-vpc-attribute --vpc-id vpc-062bda76521aa3c8a --enable-  
dns-hostnames
```

리소스 정리

1. 서브넷 삭제

```
aws ec2 delete-subnet --subnet-id subnet-0252aa7f87121cfd8
```

```
aws ec2 delete-subnet --subnet-id subnet-0b2cd27778eedaa74
```

2. igw와 vpc 분리

```
aws ec2 detach-internet-gateway --vpc-id vpc-062bda76521aa3c8a --  
internet-gateway-id igw-059c90f322a4f710f
```

리소스 정리

3. igw 삭제

```
aws ec2 delete-internet-gateway --internet-gateway-id igw-059c90f322a4f710f
```

4. 퍼블릭 라우트 테이블 삭제

```
aws ec2 delete-route-table --route-table-id rtb-09aaf805564836532
```

5. vpc 삭제

```
aws ec2 delete-vpc --vpc-id vpc-062bda76521aa3c8a
```