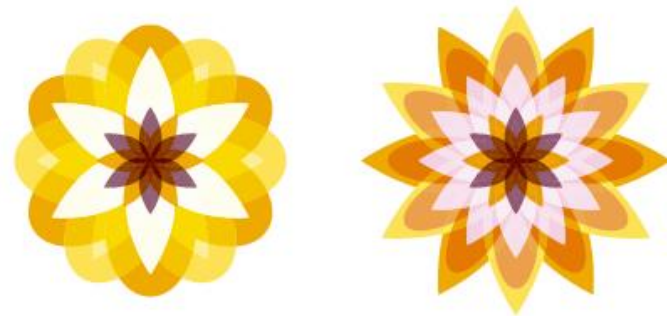


*Chapter 10*

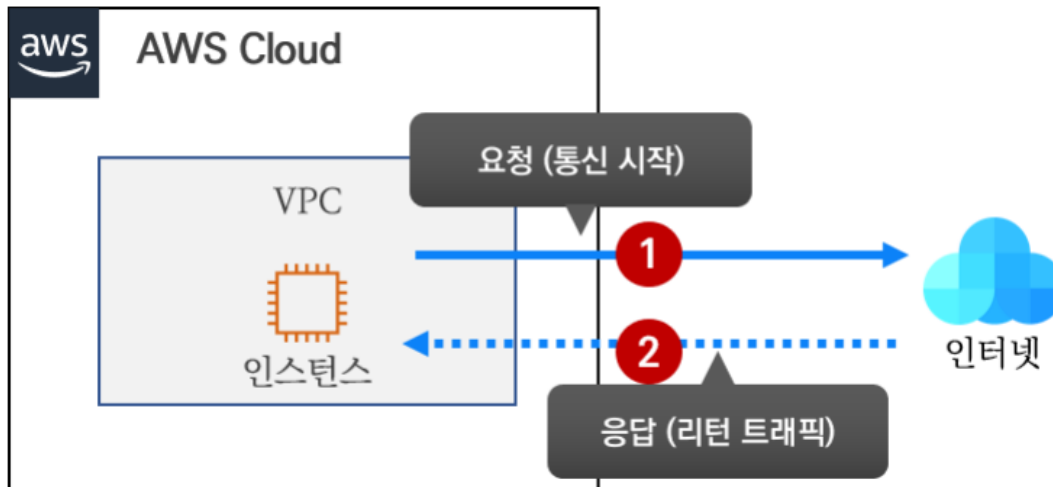
# 인터넷 연결



# 1. AWS의 인터넷 연결

## ■ AWS의 인터넷 연결 소개

- AWS에서 인터넷 연결 정의



# 1. AWS의 인터넷 연결

## ■ AWS의 인터넷 연결 소개

### ■ 인터넷 연결을 위한 4가지 조건

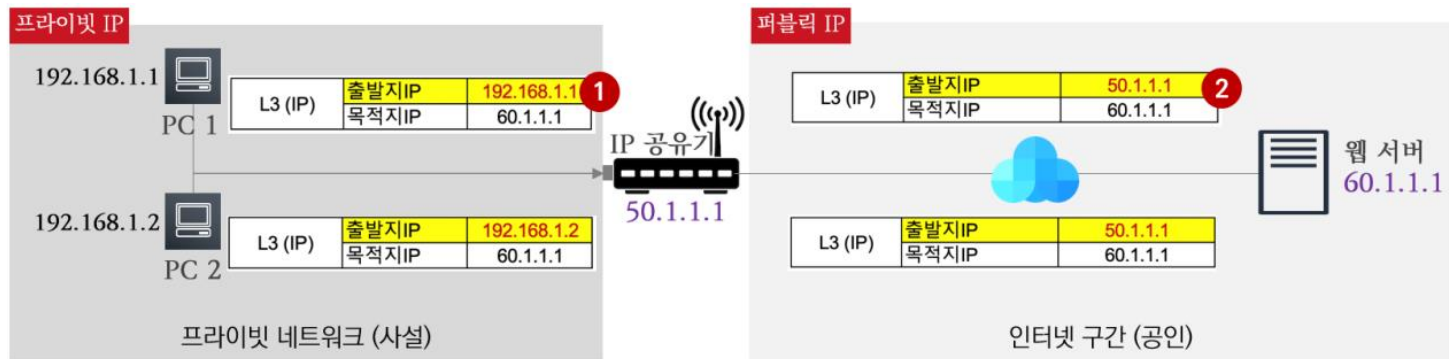
- 인터넷 게이트웨이
  - 외부 인터넷과 연결을 해주는 장비로 통신 트래픽들이 최종적으로 인터넷 게이트웨이를 통하여 통신하게 된다.
- 네트워크 라우팅 테이블 정보 (외부와 네트워크 통신을 위한)
  - 일종의 목적지를 가기 위한 지도 정보로, 모든 네트워크 대역 (0.0.0.0/0) 통신은 인터넷 게이트웨이로 전달하기 위해 경로를 지정한다.
- 공인 IP
  - AWS에 사용 가능한 공인 IP는 퍼블릭 IP나 탄력적 IP(Elastic IP)가 있다.
  - 현재 IPv4 주소 개수가 부족하기 때문에 프라이빗 IP를 가진 대상이 인터넷 사용을 위해서 공인 IP로 변환(NAT: Network Address Translation)이 필요하다.
- 보안 그룹과 네트워크 ACL
  - 보안 그룹과 네트워크 ACL 에 의해서 외부 네트워크와 통신이 허용되어야 한다.

# 1. AWS의 인터넷 연결

## ■ AWS의 인터넷 연결 소개

### ■ NAT 동작

- IP 를 변환하는 것을 NAT(Network Address Translation)라고 부르며, IP와 포트 번호를 동시에 변화하는 것을 PAT (Port Address Translation)라고 부른다.

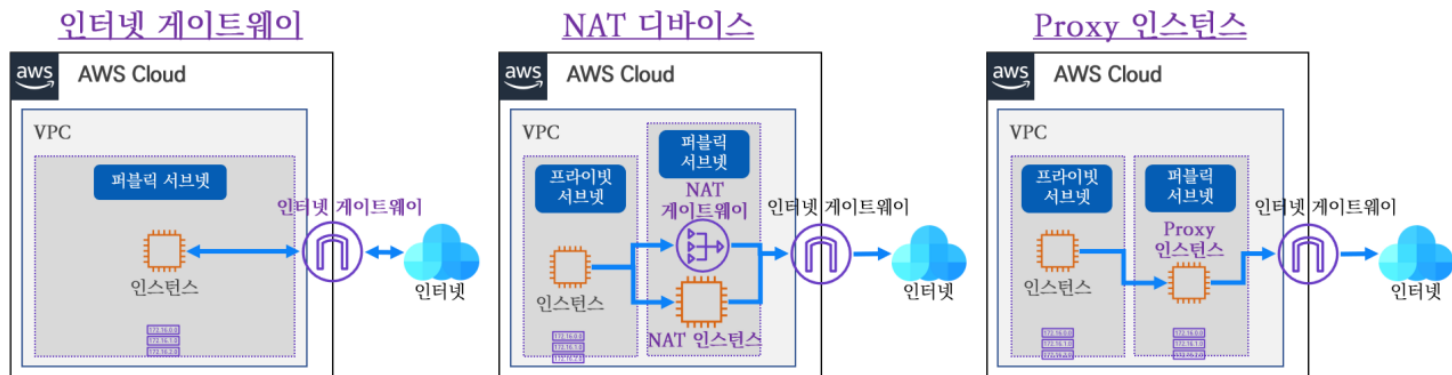


# 1. AWS의 인터넷 연결

## ■ AWS의 인터넷 연결 소개

### ■ 인터넷 연결을 위한 3가지 방안 비교

| 특징   | 인터넷 게이트웨이                            | NAT 다바이스                       | Proxy 인스턴스                 |
|------|--------------------------------------|--------------------------------|----------------------------|
| 동작   | Layer3 계층 동작                         | Layer4 계층 동작                   | Layer7 계층 동작               |
| 주소변환 | 프라이빗 IP를 퍼블릭 IP 혹은 탄력적 IP로 1:1 주소 변환 | IP 주소와 포트 번호 변환                | IP 주소와 포트 번호 변환(TCP 신규 연결) |
| 특징   | 1개의 프라이빗 IP 마다 1개의 공인 IP 매칭          | 여러 개의 프라이빗 IP가 1개의 공인 IP 사용 가능 | 어플리케이션 수준 제어(통제) 가능        |



## ■ 인터넷 게이트웨이

### ■ 인터넷 게이트웨이(Internet Gateway) 소개

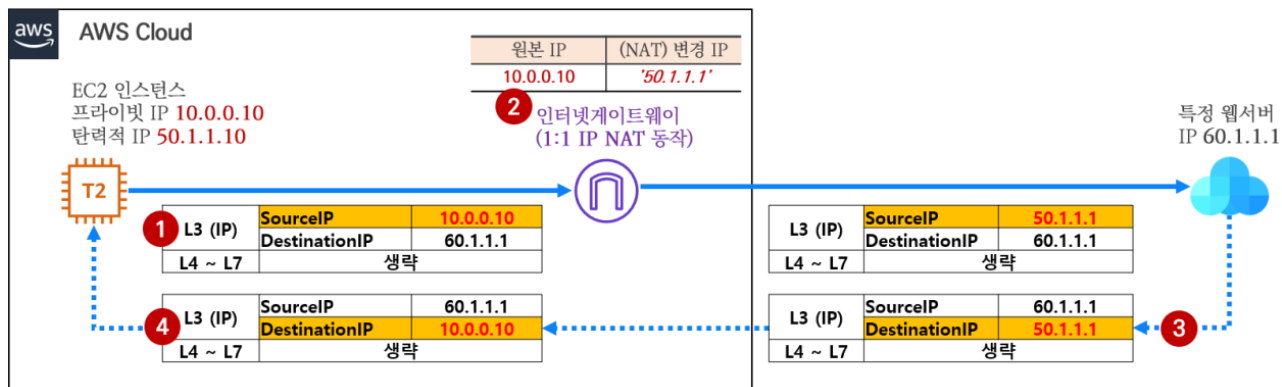
- 인터넷 게이트웨이는 확장성과 가용성이 있는 VPC 구성 요소로 VPC와 인터넷 간에 통신할 수 있게 해준다.
- 인터넷 게이트웨이는 퍼블릭 IPv4 주소가 할당된 인스턴스에 대해 1:1 IPv4 주소 변환을 수행한다.
- 참고로 인터넷 게이트웨이는 IPv4 및 IPv6 트래픽을 지원한다.

# 1. AWS의 인터넷 연결

## ■ 인터넷 게이트웨이

### ■ 인터넷 게이트웨이를 통한 외부 접속

- 인터넷 게이트웨이는 퍼블릭 IP 혹은 탄력적 IP에 대해서 1:1 IP NAT를 수행한다.
- 예를 들면 내부 인스턴스에 퍼블릭 IP 혹은 탄력적 IP가 연결되어 있으면, 외부 접속 시 프라이빗 IP를 퍼블릭 IP 혹은 탄력적 IP로 변환을 하게 된다.
- 요청 이후 되돌아오는 트래픽에서도 목적지 IP를 퍼블릭 IP 혹은 탄력적 IP에서 프라이빗 IP로 NAT를 수행한다.



## ■ 인터넷 게이트웨이

### ■ 인터넷 게이트웨이 제약 사항

- 하나의 VPC 에는 한 개의 인터넷 게이트웨이만 사용할 수 있다.
- VPC와 인터넷 게이트웨이의 최대 할당량은 동일하게 적용된다.
- 리전 당 VPC(인터넷 게이트웨이도 동일)의 기본 할당량은 5개이며, 그 이상 필요 시 AWS 케이스 오픈을 통해 요청 하여 리전 당 최대 100개까지 증가할 수 있다.

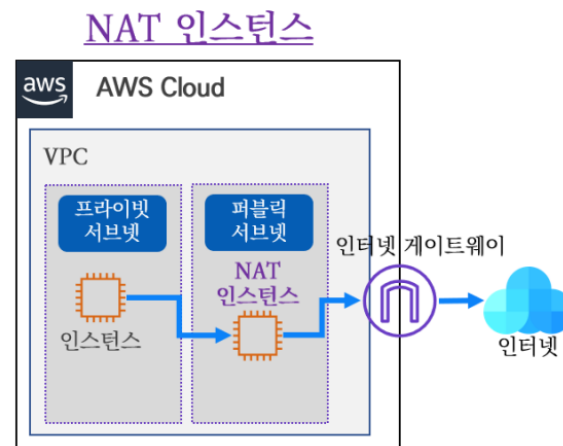
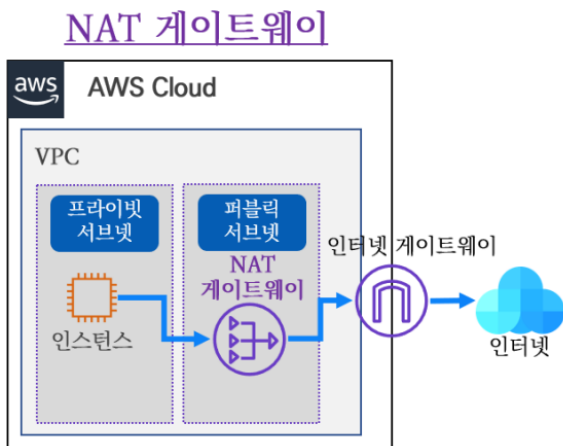


# 1. AWS의 인터넷 연결

## ■ NAT 디바이스 (NAT 인스턴스 & NAT 게이트웨이)

### ■ NAT 디바이스 소개

- NAT 인스턴스와 NAT 게이트웨이를 통칭하여 NAT 디바이스라고 말한다.
- 프라이빗 서브넷의 배치된 인스턴스는 공인 IP(퍼블릭 IP 혹은 탄력적 IP)를 연결할 수 없어서 직접 인터넷 연결이 불가능하며, 이때 NAT 디바이스를 사용하여 프라이빗 서브넷에 배치된 인스턴스가 인터넷 또는 기타 AWS 퍼블릭 서비스(S3 등)에 연결할 수 있다.
- 기본적으로는 내부(AWS 인스턴스)에서 외부 인터넷으로 통신만 가능하며, 인터넷 게이트웨이와는 다르게 외부 인터넷에서 내부 AWS 구간으로 직접 통신은 불가능하다.



# 1. AWS의 인터넷 연결

## ■ NAT 디바이스 (NAT 인스턴스 & NAT 게이트웨이)

### ■ NAT 게이트웨이와 NAT 인스턴스의 비교

- 소규모의 트래픽만 발생하고 서비스 중요도가 낮은 경우 저렴한 비용의 NAT 인스턴스로 구성을 권장한다.
- 그 이외의 경우에는 더 나은 가용성과 향상된 대역폭을 제공하면서도 관리 작업은 간소화하는 관리형 NAT 서비스인 NAT 게이트웨이 사용을 권장한다.

| 속성       | NAT 게이트웨이   | NAT 인스턴스  |
|----------|---|---|
| 유지 관리    | AWS에서 관리한다. 유지 관리 작업을 수행할 필요가 없다.                               | 사용자가 직접 관리한다. (예: 인스턴스에 소프트웨어 업데이트 또는 운영체제 패치 설치) |
| 가용성      | 가용 영역에 각기 NAT 게이트웨이를 만들어 고가용성 제공한다.                             | 직접 별도의 스크립트를 사용하여 인스턴스 간의 장애 조치를 관리한다.            |
| 네트워크 대역폭 | 최대 45Gbps까지 확장할 수 있다.   | 인스턴스 유형의 대역폭에 따라 다르다.                             |
| 비용       | 사용하는 NAT 게이트웨이 수, 사용 기간, NAT 게이트웨이를 통해 보내는 데이터의 양에 따라 요금이 청구된다. | 사용하는 NAT 인스턴스 수, 사용 기간, 인스턴스 유형과 크기에 따라 요금이 청구된다. |
| 유형 및 크기  | 균일하게 제공되므로 유형 또는 크기를 결정할 필요가 없다.                                | 예상 워크로드에 따라 적합한 인스턴스 유형과 크기를 선택한다.                |

# 1. AWS의 인터넷 연결

## ■ NAT 디바이스 (NAT 인스턴스 & NAT 게이트웨이)

### ■ NAT 게이트웨이와 NAT 인스턴스의 비교

- 소규모의 트래픽만 발생하고 서비스 중요도가 낮은 경우 저렴한 비용의 NAT 인스턴스로 구성을 권장한다.
- 그 이외의 경우에는 더 나은 가용성과 향상된 대역폭을 제공하면서도 관리 작업은 간소화하는 관리형 NAT 서비스인 NAT 게이트웨이 사용을 권장한다.

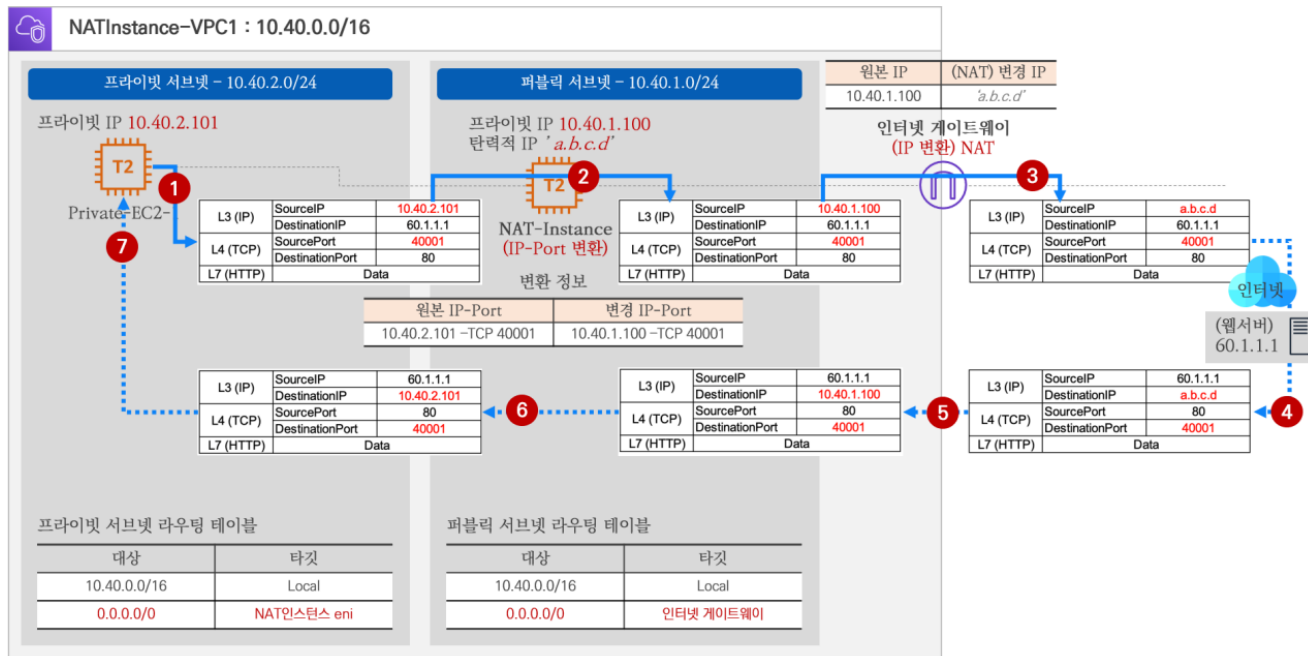
| 속성         | NAT 게이트웨이   | NAT 인스턴스   |
|------------|---|--|
| 퍼블릭 IP 주소  | 생성할 때 NAT 게이트웨이와 연결할 탄력적 IP 주소를 선택한다. 할당된 탄력적 IP 주소는 변경이 불가능하다. | 탄력적 IP 주소 또는 퍼블릭 IP 주소를 NAT 인스턴스와 함께 사용한다. 새 탄력적 IP 주소를 인스턴스와 연결하여 언제든지 퍼블릭 IP 주소를 변경할 수 있다. |
| 프라이빗 IP 주소 | 게이트웨이를 만들 때 서브넷 IP 주소 범위에서 자동으로 선택된다.                           | 인스턴스를 시작할 때 서브넷의 IP 주소 범위에서 특정 프라이빗 IP 주소를 할당한다.   |
| 보안 그룹      | 보안그룹을 NAT 게이트웨이와 연결할 수 없다.                                      | 보안그룹을 NAT 인스턴스와 연결하여 인바운드 및 아웃바운드 트래픽을 제어한다.   |
| 플로우 로그     | 플로우 로그를 사용하여 트래픽을 캡처한다.   | 플로우 로그를 사용하여 트래픽을 캡처한다.  |
| 접속 서버      | NAT 게이트웨이로 접속(예: SSH)을 지원하지 않는다.                                | NAT 게이트웨이로 접속(예: SSH)하여 SSH 접속 서버로 사용 가능하다.  |

# 1. AWS의 인터넷 연결

## ■ NAT 디바이스 (NAT 인스턴스 & NAT 게이트웨이)

### ■ NAT 인스턴스를 통한 외부 접속

- 프라이빗 서브넷에 연결된 내부 인스턴스에서 외부 인터넷과 통신 시 퍼블릭 서브넷의 NAT 인스턴스로 트래픽을 전송한다.
- NAT 인스턴스는 IP masquerading 기능을 통하여 내부 인스턴스의 IP와 포트를 NAT 인스턴스의 IP와 포트로 변환된다.
- 변환된 후 NAT 인스턴스는 인터넷 게이트웨이로 트래픽을 전송한다.
- 인터넷 게이트웨이는 NAT 인스턴스의 프라이빗 IP를 미리 맵핑된 탄력적 IP로 1:1 IP NAT하여 외부 인터넷으로 전송한다.
- 결과적으로 IP 변환이 두 번 이루어지게 된다.

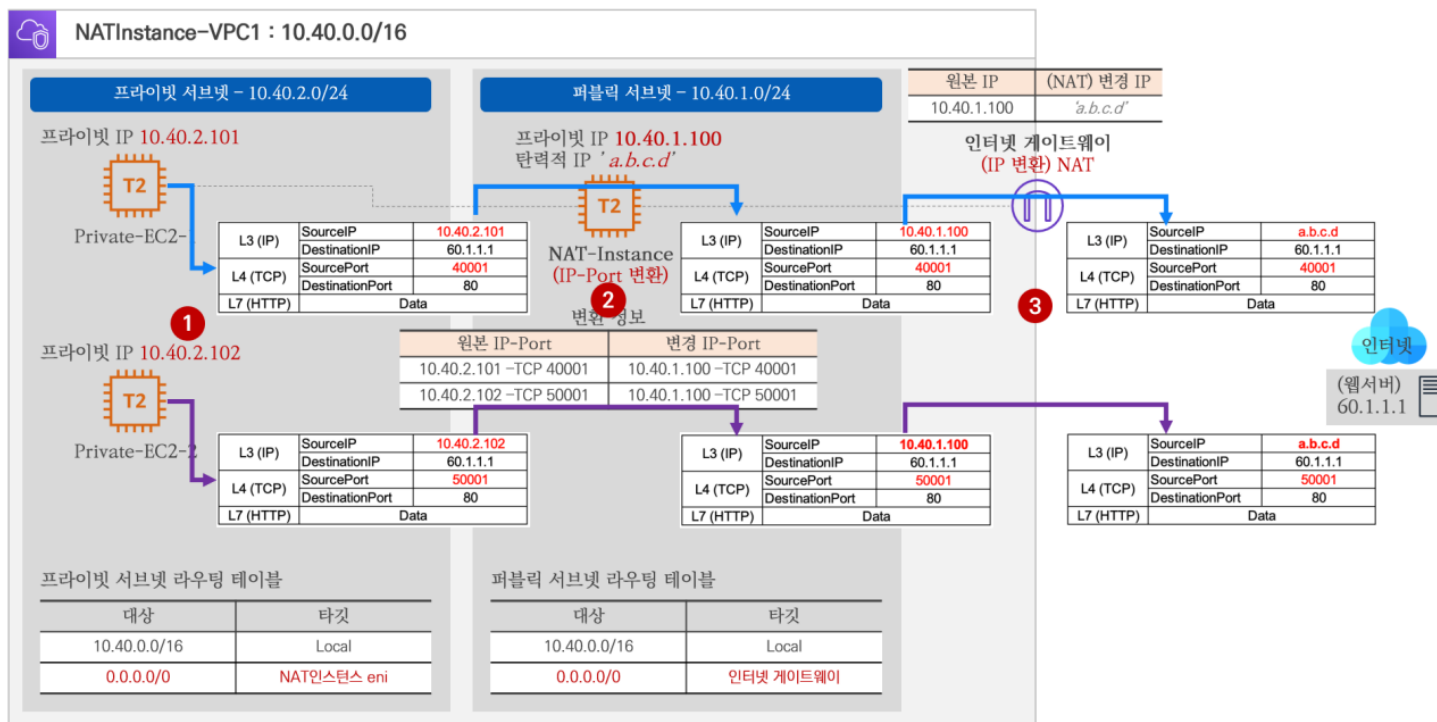


# 1. AWS의 인터넷 연결

## ■ NAT 디바이스 (NAT 인스턴스 & NAT 게이트웨이)

### ■ NAT 인스턴스를 통한 외부 접속

- 다수의 인스턴스가 외부 인터넷으로 접속 시 NAT 인스턴스에 연결된 탄력적 IP를 사용한다.
- 결과적으로 다수의 인스턴스의 출발지 IP가 1개의 탄력적 IP를 공유하여 사용하기 때문에 포트 번호 정보를 기준으로 하여 내부 인스턴스의 트래픽을 구별할 수 있다.
- 이러한 동작을 PAT(Port Address Translation)라고 한다.



## ■ NAT 디바이스 (NAT 인스턴스 & NAT 게이트웨이)

### ■ NAT 게이트웨이 제약 사항

- NAT 게이트웨이는 5Gbps의 대역폭을 지원하며, 최대 45Gbps까지 자동 확장한다.
- NAT 게이트웨이는 단일 대상(예: 외부 웹서버 1대의 IP)에 대해 분당 최대 55,000개의 동시 연결을 지원할 수 있다.
- NAT 게이트웨이 가용 영역당 기본 할당량은 5개이며, 그 이상 필요할 경우 AWS 케이스 오픈을 통해 증가 요청이 가능하다.

# 1. AWS의 인터넷 연결

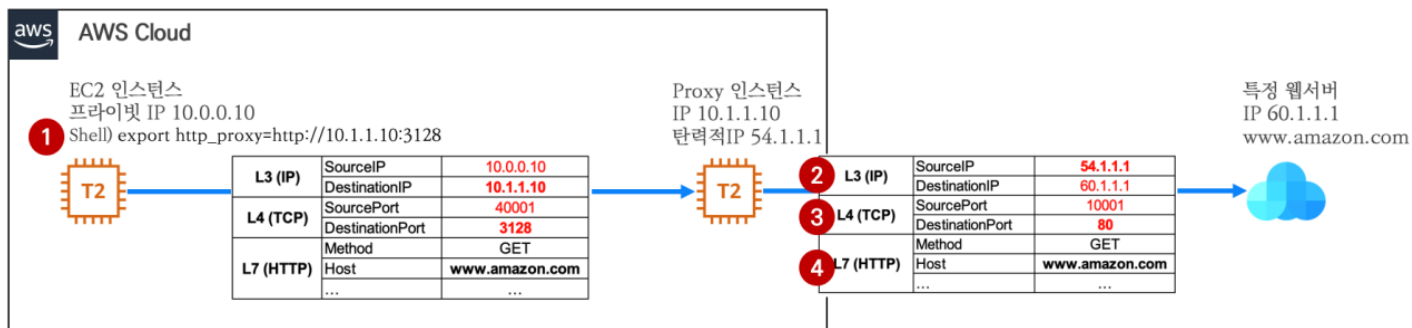
## ■ Proxy 인스턴스

### ■ Proxy 인스턴스 소개

- Proxy는 일종의 대리자로 클라이언트와 서버 중간에 통신을 대신 처리해주는 역할을 한다.
- Proxy가 클라이언트의 통신을 대신 처리하기 때문에 서버의 입장에서는 마치 Proxy와 통신을 하는 것으로 보인다.
- 클라이언트는 기존 애플리케이션 통신을 Proxy로 보내기 위한 설정이 필요하다.
  - 예) HTTP 통신을 Proxy로 보내는 설정

### ■ Proxy 인스턴스를 통한 외부 접속

- 프라이빗 서브넷 내부의 인스턴스는 HTTP 통신을 위해서 목적지 IP는 Proxy 인스턴스로 향하게 된다.
- 이후 Proxy 인스턴스는 대신 외부 구간과 통신을 하고 결과를 다시 내부 인스턴스로 보낸다.

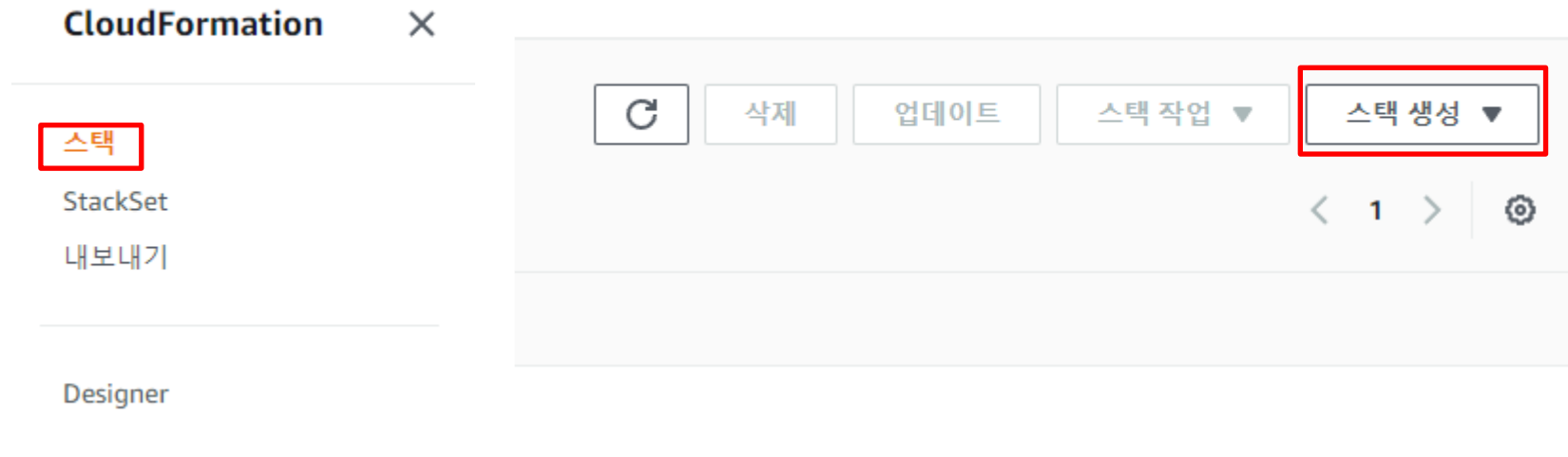


## 2. 실습 1. NAT 인스턴스를 통한 인터넷 연결

### ■ 기본 환경 적용

#### ■ CloudFormation 적용

- 본 실습을 위한 기본 실습 환경을 CloudFormation을 통해 자동으로 구성한다.
- 서비스 > CloudFormation > 스택 > 스택 생성
- 다운로드 링크 : <https://github.com/jjin300/cloud>
- CloudFormation 적용을 위해 상단의 링크를 통해 lab10-1.yaml을 다운로드하고 스택 생성을 한다.





## 2. 실습 1. NAT 인스턴스를 통한 인터넷 연결

### ■ 기본 환경 적용

#### ■ 생성 자원 확인

- 기본 환경 구성 자원 정보

| 자원           | 태그 이름                          | 정보   |
|--------------|--------------------------------|--|
| VPC          | NATInstance-VPC1               | IP CIDR: 10.40.0.0/16  |
| 인터넷 게이트웨이    | NATInstance-IGW1               | 연결: NATInstance-VPC1   |
| 퍼블릭 서브넷      | NATInstance-VPC1-Subnet1       | IP CIDR: 10.40.1.0/24, AZ: ap-northeast-2a   |
| 퍼블릭 라우팅 테이블  | NATInstance-PublicRouteTable1  | 연결: NATInstance-VPC1-Subnet1<br>라우팅 정보: 대상 0.0.0.0/0, 타겟: NATInstance-IGW1                             |
| 프라이빗 서브넷     | NATInstance-VPC1-Subnet2       | IP CIDR: 10.40.2.0/24, AZ: ap-northeast-2a   |
| 프라이빗 라우팅 테이블 | NATInstance-PrivateRouteTable1 | 연결: NATInstance-VPC1-Subnet2   |
| EC2 인스턴스     | NAT-Instance                   | 연결: NATInstance-VPC1-Subnet1<br>프라이빗 IP: 10.40.1.100 – 탄력적 IP 연결<br>AMI: 'amzn-ami-vpc-nat' 포함된 AMI 사용 |
|              | Private-EC2-1                  | 연결: NATInstance-VPC1-Subnet2<br>프라이빗 IP: 10.40.2.101 – SSH: Password 로그인 방식 활성화, root 로그인 활성화          |
|              | Private-EC2-2                  | 연결: NATInstance-VPC1-Subnet2<br>프라이빗 IP: 10.40.2.102 – SSH: Password 로그인 방식 활성화, root 로그인 활성화          |

## 2. 실습 1. NAT 인스턴스를 통한 인터넷 연결

### ■ 기본 환경 적용

#### ■ 생성 자원 확인

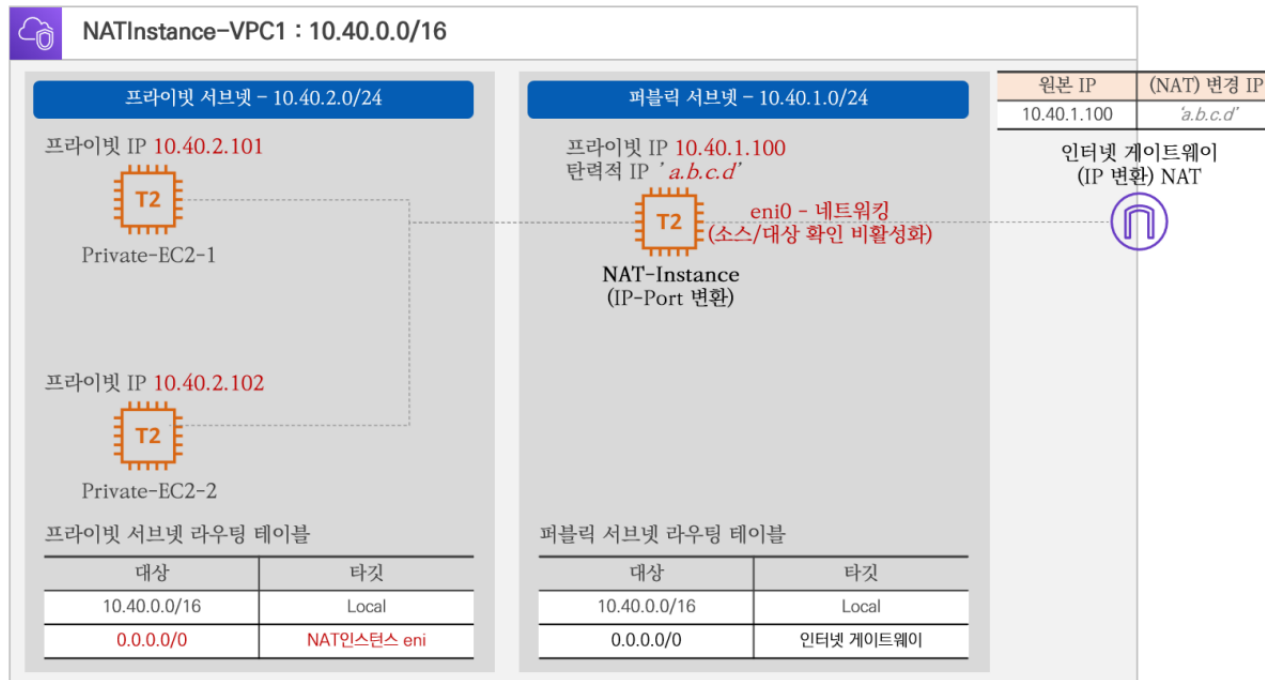
- 기본 환경 구성 자원 정보

| 자원    | 태그 이름                          | 정보   |
|-------|--------------------------------|--|
| 보안 그룹 | VPC1-NATInstance-SecurityGroup | 인바운드 규칙: SSH/ICMP - 0.0.0.0/0,<br>HTTP(S) - 10.40.0.0/16 |
|       | VPC1-PrivateEC2-SecurityGroup  | 인바운드 규칙: SSH/ICMP - 10.40.0.0/16,<br>ICMP - 0.0.0.0/0    |

## 2. 실습 1. NAT 인스턴스를 통한 인터넷 연결

### ■ 기본 환경 적용

- 생성 자원 확인
  - 기본 환경 구성 도식화

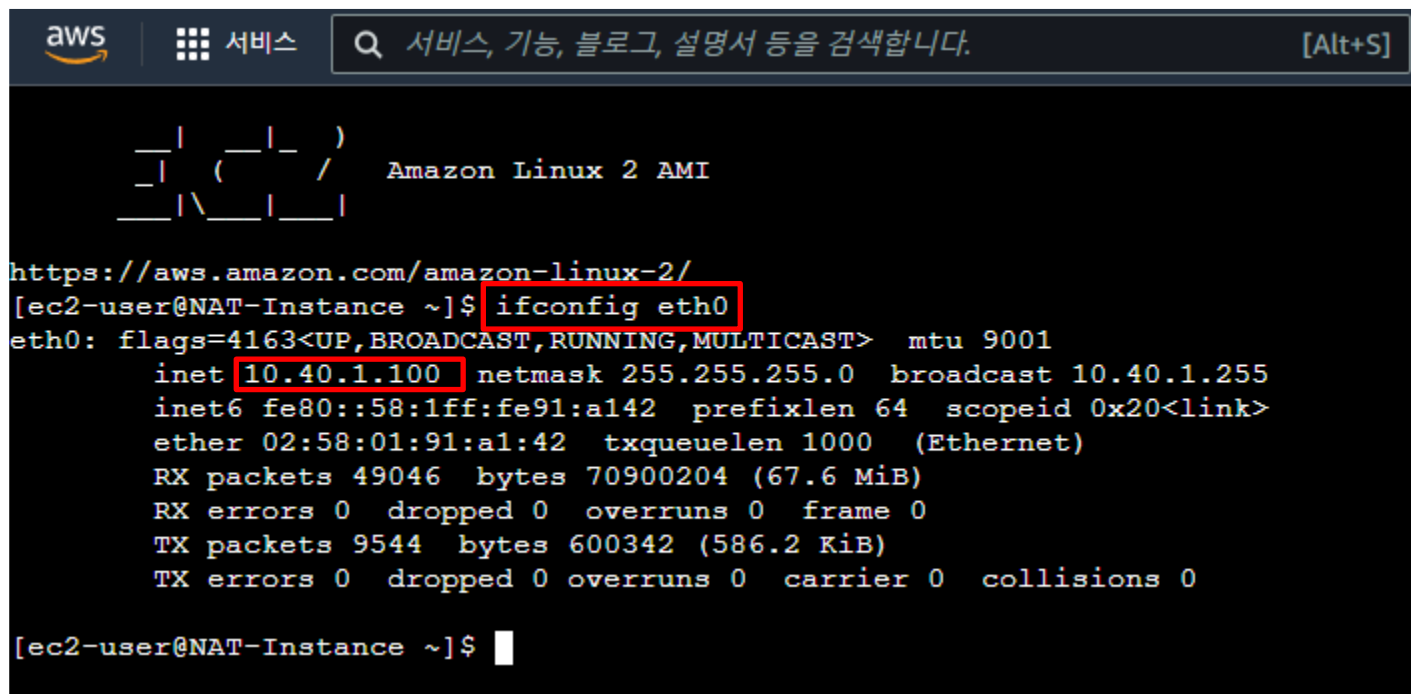


## 2. 실습 1. NAT 인스턴스를 통한 인터넷 연결

### ■ 기본 환경 적용

#### ■ 기본 환경 검증

- 프라이빗 서브넷에 위치한 인스턴스는 현재 외부에서 직접 SSH 접속이 불가능하다.
- 퍼블릭 서브넷에 위치한 NAT 인스턴스를 먼저 SSH로 접속 후 다시 프라이빗 서브넷에 있는 인스턴스로 접속을 해야 한다.
- 최종적으로 프라이빗 서브넷에 있는 인스턴스에 SSH 접속을 하였다면 외부 인터넷과 통신이 되는지 확인한다.
- NAT 인스턴스의 프라이빗 IP를 확인
  - `ifconfig eth0`



The screenshot shows the AWS Management Console interface. At the top, there's a search bar with the text "서비스, 기능, 블로그, 설명서 등을 검색합니다." and a button labeled "[Alt+S]". Below the search bar, there's a terminal window titled "Amazon Linux 2 AMI". The terminal shows the command `ifconfig eth0` being executed, and the output displays network configuration details for the `eth0` interface, including the IP address `10.40.1.100`. The terminal output is as follows:

```
https://aws.amazon.com/amazon-linux-2/
[ec2-user@NAT-Instance ~]$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
    inet 10.40.1.100 netmask 255.255.255.0  broadcast 10.40.1.255
    inet6 fe80::58:1ff:fe91:a142 prefixlen 64  scopeid 0x20<link>
    ether 02:58:01:91:a1:42  txqueuelen 1000  (Ethernet)
    RX packets 49046  bytes 70900204 (67.6 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 9544  bytes 600342 (586.2 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

[ec2-user@NAT-Instance ~]$
```

## 2. 실습 1. NAT 인스턴스를 통한 인터넷 연결

### ■ 기본 환경 적용

#### ■ 기본 환경 검증

- NAT 인스턴스의 탄력적 IP를 확인
  - curl <http://checkip.amazonaws.com/>

```
[ec2-user@NAT-Instance ~]$ curl http://checkip.amazonaws.com/  
3.37.78.100  
[ec2-user@NAT-Instance ~]$
```

- 프라이빗 서브넷의 Private-EC2-1 인스턴스에 SSH 접속 (암호: qwe123)
  - ssh root@10.40.2.101

```
[ec2-user@NAT-Instance ~]$ ssh root@10.40.2.101  
The authenticity of host '10.40.2.101 (10.40.2.101)' can't be established.  
ECDSA key fingerprint is SHA256:Ilc2FGQPw4ozRHgj9ktWVDjTA/90/jMZzozyYJpba/4.  
ECDSA key fingerprint is MD5:33:3f:ce:f5:a3:ea:e9:73:d8:67:a9:1d:44:83:7f:96.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '10.40.2.101' (ECDSA) to the list of known hosts.  
root@10.40.2.101's password:
```

```
  _ |  ( _ |  )  
  _ |  /  
  _ | \ _ |  |  
Amazon Linux 2 AMI
```

```
https://aws.amazon.com/amazon-linux-2/  
[root@Private-EC2-1 ~]#
```

## 2. 실습 1. NAT 인스턴스를 통한 인터넷 연결

### ■ 기본 환경 적용

#### ■ 기본 환경 검증

- Private-EC2-1 인스턴스가 외부 인터넷 통신이 되는지 확인
  - curl <http://checkip.amazonaws.com/> --connect-timeout 3

```
https://aws.amazon.com/amazon-linux-2/
[root@Private-EC2-1 ~]# curl http://checkip.amazonaws.com/ --connect-timeout 3
curl: (28) Failed to connect to checkip.amazonaws.com port 80 after 2988 ms: Connection timed out
[root@Private-EC2-1 ~]#
```

- 프라이빗 서브넷의 Private-EC2-2 인스턴스에 SSH 접속 (암호 qwe123)

```
[root@Private-EC2-1 ~]# ssh root@10.40.2.102
The authenticity of host '10.40.2.102 (10.40.2.102)' can't be established.
ECDSA key fingerprint is SHA256:IUL9HlZuBFcbTlcAO4DvHs+ZRFGmXfs+Gm7RexjHuUs.
ECDSA key fingerprint is MD5:93:fe:7b:cb:c0:b5:ed:c2:e3:d0:a2:b9:42:37:05:97.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.40.2.102' (ECDSA) to the list of known hosts.
root@10.40.2.102's password:
_ _ | _ _ | _ )
_ | ( _ _ /   Amazon Linux 2 AMI
_ _ | \ _ _ | _ |

https://aws.amazon.com/amazon-linux-2/
[root@Private-EC2-2 ~]#
```

## 2. 실습 1. NAT 인스턴스를 통한 인터넷 연결

### ■ 기본 환경 적용

#### ■ 기본 환경 검증

- Private-EC2-2 인스턴스가 외부 인터넷 통신이 되는지 확인
  - curl <http://checkip.amazonaws.com/> --connect-timeout 3

```
https://aws.amazon.com/amazon-linux-2/  
[root@Private-EC2-2 ~]# curl http://checkip.amazonaws.com/ --connect-timeout 3  
curl: (28) Failed to connect to checkip.amazonaws.com port 80 after 2989 ms: Connection timed out  
[root@Private-EC2-2 ~]#
```

## 2. 실습 1. NAT 인스턴스를 통한 인터넷 연결

### ■ NAT 인스턴스 실습

#### ■ NAT 인스턴스 동작을 위한 스크립트 확인

- NAT 인스턴스 동작을 위해서 IPv4 라우팅 처리를 확인한다.
  - `cat /proc/sys/net/ipv4/ip_forward`

```
Last login: Thu Jul 28 06:30:04 2022 from ec2-13-209-1-60.ap-northeast-2.compute.amazonaws.com

  _ | _ | _ )
  _ | ( _ | /   Amazon Linux 2 AMI
  _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
[ec2-user@NAT-Instance ~]$ cat /proc/sys/net/ipv4/ip_forward
1
[ec2-user@NAT-Instance ~]$
```

- NAT 인스턴스 동작을 위해서 IP masquerade 동작을 확인한다.
  - `sudo iptables -nL POSTROUTING -t nat -v`

```
[ec2-user@NAT-Instance ~]$ sudo iptables -nL POSTROUTING -t nat -v
Chain POSTROUTING (policy ACCEPT 1 packets, 60 bytes)
  pkts bytes target     prot opt in     out     source               destination
   259 19093 MASQUERADE all  --  *      eth0    0.0.0.0/0            0.0.0.0/0
[ec2-user@NAT-Instance ~]$
```



## 2. 실습 1. NAT 인스턴스를 통한 인터넷 연결

### ■ NAT 인스턴스 실습

#### ■ NAT 인스턴스 동작을 위한 설정

- 프라이빗 서브넷에 라우팅 정보 추가
  - 현재 프라이빗 서브넷에 외부 인터넷과 통신하기 위한 라우팅 정보가 없기 때문에 해당 정보를 추가해야 한다.
  - 서비스 > VPC > Virtual Private Cloud > 라우팅 테이블 > NATInstance-PrivateRouteTable 1 선택 > 라우팅 탭 선택 > 라우팅 편집

새로운 VPC 환경  
의견을 알려주세요

VPC 대시보드

EC2 글로벌 보기 신규

VPC로 필터링:

VPC 선택

Virtual Private Cloud

VPC

서브넷

라우팅 테이블

인터넷 게이트웨이

송신 전용 인터넷 게이트웨이

라우팅 테이블 (1/9) 정보

Q 라우팅 테이블 필터링

|                                     | Name                            | 라우팅 테이블 ID            | 명시적 서브넷 연결              | 엣지 연결 | 기본  |
|-------------------------------------|---------------------------------|-----------------------|-------------------------|-------|-----|
| <input type="checkbox"/>            | 프로젝트-rtb-private2-ap-northea... | rtb-0deae5f364d77e49b | subnet-0b1c28fd5b411... | -     | 아니요 |
| <input type="checkbox"/>            | NATInstance-PublicRouteTable1   | rtb-02560509345602d30 | subnet-03ce34255468f... | -     | 아니요 |
| <input type="checkbox"/>            | route-table-01                  | rtb-06803ddd6f0e7d347 | -                       | -     | 아니요 |
| <input type="checkbox"/>            | -                               | rtb-0e3e6d88c7dd503b8 | -                       | -     | 예   |
| <input checked="" type="checkbox"/> | NATInstance-PrivateRouteTable1  | rtb-02b67a6ab59b103a9 | subnet-0a0e0dba4a58d... | -     | 아니요 |
| <input type="checkbox"/>            | 프로젝트-rtb-private1-ap-northea... | rtb-0d85571d88b3b70c1 | subnet-07a8afad54ab8... | -     | 아니요 |
| <input type="checkbox"/>            | -                               | rtb-0fdd6a829ad74551f | -                       | -     | 예   |
| <input type="checkbox"/>            | 프로젝트-rtb-public                 | rtb-0c53efa5e4d893205 | 2 서브넷                   | -     | 아니요 |
| <input type="checkbox"/>            | -                               | rtb-0679e4924f94f85df | -                       | -     | 예   |

세부 정보 라우팅 서브넷 연결 엣지 연결 라우팅 전파 태그

라우팅 (1)

Q 라우팅 필터링

모두

라우팅 편집

| 대상           | 대상    | 상태 | 전파됨 |
|--------------|-------|----|-----|
| 10.40.0.0/16 | local | 활성 | 아니요 |

## 2. 실습 1. NAT 인스턴스를 통한 인터넷 연결

### ■ NAT 인스턴스 실습

#### ■ NAT 인스턴스 동작을 위한 설정

- 프라이빗 서브넷에 라우팅 정보 추가
  - 외부 통신을 위한 라우팅 정보를 추가
  - 대상: 0.0.0.0/0, 대상 타겟: Network 인터페이스 선택 > NAT 인스턴스의 eth0 선택

| 대상           | 대상                                   | 상태                | 전파됨 |
|--------------|--------------------------------------|-------------------|-----|
| 10.40.0.0/16 | <input type="text" value="Q local"/> | <span>🟢 활성</span> | 아니요 |

| 대상                                       | 대상                                   | 상태                |
|--|--------------------------------------|-------------------|
| 10.40.0.0/16                             | <input type="text" value="Q local"/> | <span>🟢 활성</span> |
| <input type="text" value="Q 0.0.0.0/0"/> | <input type="text" value="Q  "/>     | -                 |

캐리어 게이트웨이  
외부 전용 인터넷 게이트웨이  
Gateway Load Balancer 엔드포인트  
인스턴스  
인터넷 게이트웨이  
로컬  
NAT 게이트웨이  
**네트워크 인터페이스**  
Outpost 로컬 게이트웨이

## 2. 실습 1. NAT 인스턴스를 통한 인터넷 연결

### ■ NAT 인스턴스 실습

#### ■ NAT 인스턴스 동작을 위한 설정

- 프라이빗 서브넷에 라우팅 정보 추가
  - 외부 통신을 위한 라우팅 정보를 추가
  - 대상: 0.0.0.0/0, 대상 타겟: Network 인터페이스 선택 > NAT 인스턴스의 eth0 선택

| 대상                                       | 대상   | 상태    | 전파됨 |
|--|--|-------|-----|
| 10.40.0.0/16                             | <input type="text" value="Q local"/>   | 🟢 활성화 | 아니요 |
| <input type="text" value="Q 0.0.0.0/0"/> | <input type="text" value="Q eni-"/><br>eni-0604249e4daf6dc08<br>eni-02a2f20fbf9e6cf1a<br>eni-008a92a05b7deee86 (NAT-Instance eth0) | -     | 아니요 |

## 2. 실습 1. NAT 인스턴스를 통한 인터넷 연결

### ■ NAT 인스턴스 실습

#### ■ NAT 인스턴스 동작을 위한 설정

- 소스/대상 확인 비활성화 (중지)
  - 기본적으로 인스턴스로 인입되는 트래픽이 자신이 목적지가 아닌 IP 트래픽이 들어올 경우 폐기한다.
  - 또한 인스턴스에서 나가는 트래픽의 출발지 IP가 자신이 아닐 경우 역시 폐기한다.
  - 이 기능은 소스/대상 확인 (Source/Destination Check)이며 기본적으로 VPC 의 네트워크 인터페이스(ENI)는 활성화 상태이다.
  - 그런데 NAT 인스턴스 경우에는 소스/대상 확인을 비활성화(중지)해야 한다.
  - 이유는 자신이 목적지가 아닌 트래픽이 NAT 인스턴스를 경유해서 외부로 나가기 때문이다.

## 2. 실습 1. NAT 인스턴스를 통한 인터넷 연결

### ■ NAT 인스턴스 실습

#### ■ NAT 인스턴스 동작을 위한 설정

- 소스/대상 확인 비활성화 (중지)
  - 서비스 > EC2 > 인스턴스 > 인스턴스 > NAT -Instance 선택 > 작업 > 네트워킹 > 소스/대상 확인 변경 선택

The screenshot shows the AWS Management Console interface for EC2 instances. On the left, the '인스턴스' (Instances) link is highlighted in the navigation menu. The main area displays a list of instances. The instance named 'NAT-Instance' with ID 'i-0cb9bdfd35a7eddd1' is selected, and its row is highlighted in blue. The '작업' (Actions) dropdown menu is open, showing various options. The '네트워킹' (Networking) option is highlighted, and the '소스/대상 확인 변경' (Change source/destination check) option is also visible. The table below shows the details of the instances.

| Name            | 인스턴스 ID             | 인스턴스 상태 | 인스턴스 유형  | 상태 검사         | 경보 상태 | 가용 영역           |
|-----------------|---------------------|---------|----------|---------------|-------|-----------------|
| ProxyLAB-Squid  | i-0d10c67511f90c89b | 종료됨     | t2.micro | -             | 경보 없음 | ap-northeast-2a |
| Private-EC2-1   | i-0ac5c405e261aee2  | 종료됨     | t2.micro | -             | 경보 없음 | ap-northeast-2a |
| Private-EC2-2   | i-0d151e7216d3d2f58 | 실행 중    | t2.micro | 2/2개 검사 통과... | 경보 없음 | ap-northeast-2a |
| NAT-Instance    | i-0cb9bdfd35a7eddd1 | 실행 중    | t2.micro | 2/2개 검사 통과... | 경보 없음 | ap-northeast-2a |
| Private-EC2-1   | i-09159f2e622330c4a | 실행 중    | t2.micro | 2/2개 검사 통과... | 경보 없음 | ap-northeast-2a |
| Private-EC2-2   | i-0b04b6d5419c8ea77 | 종료됨     | t2.micro | -             | 경보 없음 | ap-northeast-2a |
| ProxyLAB-Client | i-0bb7e77f187dbb4e5 | 종료됨     | t2.micro | -             | 경보 없음 | ap-northeast-2a |
| NAT-Instance    | i-0718d898c1efa9da1 | 종료됨     | t2.micro | -             | 경보 없음 | ap-northeast-2a |

## 2. 실습 1. NAT 인스턴스를 통한 인터넷 연결

### ■ NAT 인스턴스 실습

#### ■ NAT 인스턴스 동작을 위한 설정

- 소스/대상 확인 비활성화 (중지)
  - 서비스 > EC2 > 인스턴스 > 인스턴스 > NAT -Instance 선택 > 작업 > 네트워킹 > 소스/대상 확인 변경 선택

### 소스/대상 확인 정보

각 EC2 인스턴스는 기본적으로 소스/대상 확인을 수행합니다. 인스턴스는 송수신되는 트래픽의 소스 또는 대상이어야 합니다.

인스턴스 ID  
i-0cb9bcfd35a7eddd1 (NAT-Instance)

네트워크 인터페이스 정보  
eni-008a92a05b7deee86(NAT-Instance eth0)

소스/대상 확인 정보  
☒ 중지

**i** NAT 인스턴스일 경우 소스/대상 확인을 중단해야 합니다. NAT 인스턴스는 소스 또는 대상이 그 자체가 아닐 때 트래픽을 송수신할 수 있어야 합니다.

▼ AWS CLI 명령

```
aws ec2 modify-instance-attribute --instance-id=i-0cb9bcfd35a7eddd1 --no-source-dest-check
```

복사

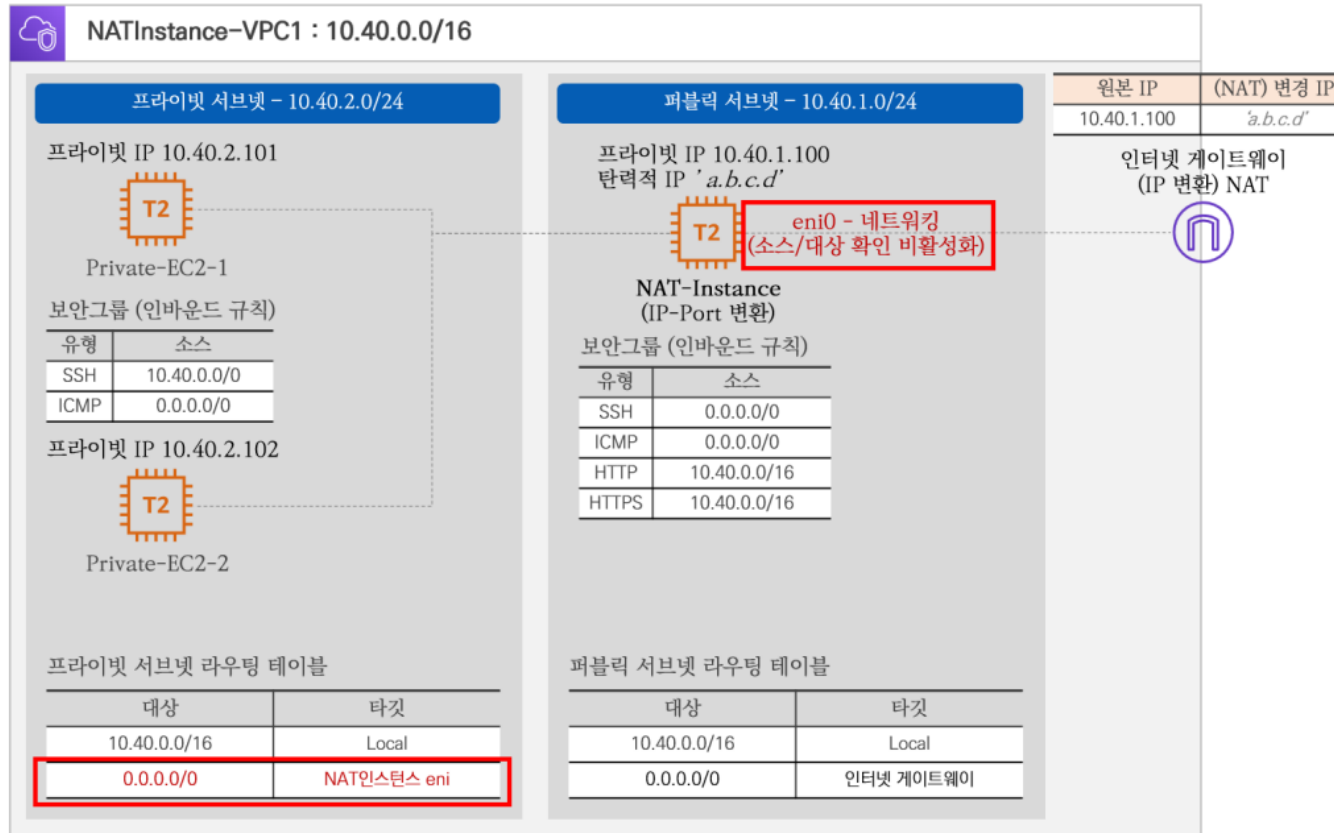
취소

저장

## 2. 실습 1. NAT 인스턴스를 통한 인터넷 연결

### ■ NAT 인스턴스 실습

- NAT 인스턴스 동작을 위한 설정
  - 소스/대상 확인 비활성화 (중지)
    - NAT 인스턴스 설정 완료 후 토폴로지



## 2. 실습 1. NAT 인스턴스를 통한 인터넷 연결

### ■ NAT 인스턴스 실습

#### ■ 프라이빗 서브넷에 위치한 인스턴스에서 외부로 통신 확인

- 우선 NAT 인스턴스의 퍼블릭 IP를 확인하고 SSH 접근을 하고 프라이빗 서브넷의 Private-EC2-1 인스턴스에 SSH 접속 (암호 qwe123)
  - ssh root@10.40.2.101

```
aws | 서비스 | Q 서비스, 기능, 블로그, 설명서 등을 검색합니다. [Alt+S]

Last login: Thu Jul 28 06:46:46 2022 from ec2-13-209-1-59.ap-northeast-2.compute.amazonaws.com

 _ | _ | _ )
 _ | ( _ | /   Amazon Linux 2 AMI
 _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
[ec2-user@NAT-Instance ~]$ ssh root@10.40.2.101
root@10.40.2.101's password:
Last login: Thu Jul 28 06:38:11 2022 from ip-10-40-1-100.ap-northeast-2.compute.internal

 _ | _ | _ )
 _ | ( _ | /   Amazon Linux 2 AMI
 _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
[root@Private-EC2-1 ~]#
```



## 2. 실습 1. NAT 인스턴스를 통한 인터넷 연결

### ■ NAT 인스턴스 실습

#### ■ 프라이빗 서브넷에 위치한 인스턴스에서 외부로 통신 확인

- Private-EC2-1 인스턴스가 외부 인터넷 통신이 되는지 확인
  - curl <http://checkip.amazonaws.com/> --connect-timeout 3

```
https://aws.amazon.com/amazon-linux-2/  
[root@Private-EC2-1 ~]# curl http://checkip.amazonaws.com/ --connect-timeout 3  
3.37.78.100  
[root@Private-EC2-1 ~]#
```

- 외부로 ping(ICMP)도 정상 통신이 되는지 확인
  - ping [www.google.com](http://www.google.com)

```
[root@Private-EC2-1 ~]# ping www.google.com  
PING www.google.com (142.250.196.132) 56(84) bytes of data.  
64 bytes from nrt12s36-in-f4.1e100.net (142.250.196.132): icmp_seq=1 ttl=104 time=34.0 ms  
64 bytes from nrt12s36-in-f4.1e100.net (142.250.196.132): icmp_seq=2 ttl=104 time=34.2 ms  
64 bytes from nrt12s36-in-f4.1e100.net (142.250.196.132): icmp_seq=3 ttl=104 time=34.1 ms  
64 bytes from nrt12s36-in-f4.1e100.net (142.250.196.132): icmp_seq=4 ttl=104 time=34.2 ms  
^Z  
[1]+  Stopped                  ping www.google.com  
[root@Private-EC2-1 ~]#
```

## 2. 실습 1. NAT 인스턴스를 통한 인터넷 연결

### ■ NAT 인스턴스 실습

- 프라이빗 서브넷에 위치한 인스턴스에서 외부로 통신 확인
  - Private-EC2-2도 마찬가지로 외부 인터넷 구간과 정상적으로 통신된다.
  - 그러면 NAT 인스턴스에서 tcpdump 명령어로 트래픽이 경유하는지 확인한다.
  - tcpdump 실행한다.
    - `sudo tcpdump -nni eth0 tcp port 80`

```
Last login: Thu Jul 28 07:09:25 2022 from ec2-13-209-1-59.ap-northeast-2.compute.amazonaws.com
```

```
 _ | _ | _ )  
 _ | ( _ /   Amazon Linux 2 AMI  
__| \__|__|
```

```
https://aws.amazon.com/amazon-linux-2/
```

```
[ec2-user@NAT-Instance ~]$ sudo tcpdump -nni eth0 tcp port 80
```

```
sudo: tcpdump: command not found
```

```
[ec2-user@NAT-Instance ~]$ sudo tcpdump -nni eth0 tcp port 80
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
```

```
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

## 2. 실습 1. NAT 인스턴스를 통한 인터넷 연결

### ■ NAT 인스턴스 실습

#### ■ 프라이빗 서브넷에 위치한 인스턴스에서 외부로 통신 확인

- Private-EC2-2도 마찬가지로 외부 인터넷 구간과 정상적으로 통신된다.
- 그러면 NAT 인스턴스에서 tcpdump 명령어로 트래픽이 경유하는지 확인한다.
- tcpdump 실행 후 Private-EC2에서 외부로 웹 접속을 시도한다.
  - ssh [root@10.40.2.102](https://root@10.40.2.102)
  - ping [www.google.com](https://www.google.com)

```
Last login: Thu Jul 28 07:17:32 2022 from ec2-13-209-1-59.ap-northeast-2.compute.amazonaws.com

 _ | _ | _ |
 _ | ( _ | /
 _ | \ _ | _ |

Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/
[ec2-user@NAT-Instance ~]$ ssh root@10.40.2.102
The authenticity of host '10.40.2.102 (10.40.2.102)' can't be established.
ECDSA key fingerprint is SHA256:IUL9HlZuBFcbTlcAO4DvHs+ZRFgMxfs+Gm7RexjHuUs.
ECDSA key fingerprint is MD5:93:fe:7b:cb:c0:b5:ed:c2:e3:d0:a2:b9:42:37:05:97.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.40.2.102' (ECDSA) to the list of known hosts.
root@10.40.2.102's password:
Last login: Thu Jul 28 06:42:30 2022 from ip-10-40-2-101.ap-northeast-2.compute.internal

 _ | _ | _ |
 _ | ( _ | /
 _ | \ _ | _ |

Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/
[root@Private-EC2-2 ~]$ ping www.google.com
PING www.google.com (142.250.207.36) 56(84) bytes of data.
64 bytes from nrt13s55-in-f4.1e100.net (142.250.207.36): icmp_seq=1 ttl=104 time=32.6 ms
64 bytes from nrt13s55-in-f4.1e100.net (142.250.207.36): icmp_seq=2 ttl=104 time=32.8 ms
64 bytes from nrt13s55-in-f4.1e100.net (142.250.207.36): icmp_seq=3 ttl=104 time=32.9 ms
64 bytes from nrt13s55-in-f4.1e100.net (142.250.207.36): icmp_seq=4 ttl=104 time=32.7 ms
64 bytes from nrt13s55-in-f4.1e100.net (142.250.207.36): icmp_seq=5 ttl=104 time=32.7 ms
64 bytes from nrt13s55-in-f4.1e100.net (142.250.207.36): icmp_seq=6 ttl=104 time=32.7 ms
64 bytes from nrt13s55-in-f4.1e100.net (142.250.207.36): icmp_seq=7 ttl=104 time=32.7 ms
64 bytes from nrt13s55-in-f4.1e100.net (142.250.207.36): icmp_seq=8 ttl=104 time=32.8 ms
64 bytes from nrt13s55-in-f4.1e100.net (142.250.207.36): icmp_seq=9 ttl=104 time=32.8 ms
^Z
[1]+  Stopped                  ping www.google.com
[root@Private-EC2-2 ~]#
```

## 2. 실습 1. NAT 인스턴스를 통한 인터넷 연결

### ■ NAT 인스턴스 실습

#### ■ 프라이빗 서브넷에 위치한 인스턴스에서 외부로 통신 확인

- Private-EC2-2도 마찬가지로 외부 인터넷 구간과 정상적으로 통신된다.
- 그러면 NAT 인스턴스에서 tcpdump 명령어로 트래픽이 경유하는지 확인한다.
- tcpdump 실행 후 Private-EC2에서 외부로 웹 접속을 시도한다.

```
Last login: Thu Jul 28 07:09:25 2022 from ec2-13-209-1-59.ap-northeast-2.compute.amazonaws.com
```

```
 _ _ | _ _ | _ )  
 _ | ( _ | _ /  
 _ | \ _ | _ |  
 Amazon Linux 2 AMI
```

```
https://aws.amazon.com/amazon-linux-2/
```

```
[ec2-user@NAT-Instance ~]$ sudo tctdump -nni eth0 tcp port 80
```

```
sudo: tctdump: command not found
```

```
[ec2-user@NAT-Instance ~]$ sudo tcpdump -nni eth0 tcp port 80
```

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
```

```
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
07:19:51.390355 IP 10.40.1.100.58074 > 169.254.169.254.80: Flags [S], seq 2719265391, win 26883, options [mss 8961,sackOK,TS val 3000034898 ecr 0,nop,wscale 7], length 0  
07:19:51.390606 IP 169.254.169.254.80 > 10.40.1.100.58074: Flags [S.], seq 2437036431, ack 2719265392, win 26847, options [mss 8961,sackOK,TS val 2921686009 ecr 3000034898  
le 7], length 0  
07:19:51.390624 IP 10.40.1.100.58074 > 169.254.169.254.80: Flags [.] , ack 1, win 211, options [nop,nop,TS val 3000034898 ecr 2921686009], length 0  
07:19:51.390684 IP 10.40.1.100.58074 > 169.254.169.254.80: Flags [P.], seq 1:137, ack 1, win 211, options [nop,nop,TS val 3000034898 ecr 2921686009], length 136: HTTP: PUT  
api/token HTTP/1.1  
07:19:51.390911 IP 169.254.169.254.80 > 10.40.1.100.58074: Flags [.] , ack 137, win 219, options [nop,nop,TS val 2921686009 ecr 3000034898], length 0  
07:19:51.391853 IP 169.254.169.254.80 > 10.40.1.100.58074: Flags [P.], seq 1:234, ack 137, win 219, options [nop,nop,TS val 2921686009 ecr 3000034898], length 233: HTTP: 200 OK
```

## 2. 실습 1. NAT 인스턴스를 통한 인터넷 연결

### ■ 자원 삭제

- 모든 실습이 끝나면 자원 삭제를 반드시 수행해야 한다.
- 부득이하게 과금이 발생할 수 있으니, 아래 순서대로 진행해야 한다.
  - CloudFormation 스택 삭제 (CloudFormation > 스택 > 스택 삭제)
  - CloudFormation 스택 삭제까지 기다리고 생성 자원이 모두 삭제되었는지 확인한다.

CloudFormation 스택 삭제 화면

CloudFormation > 스택

스택 (1)

스택 이름으로 필터링

뷰 중첩됨

| 스택 이름   | 상태              | 생성 시간                        | 설명 |
|---------|-----------------|------------------------------|----|
| lab10-1 | CREATE_COMPLETE | 2022-07-28 15:25:13 UTC+0900 | -  |

lab10-1을(를) 삭제하시겠습니까?

이 스택을 삭제하면 모든 스택 리소스가 삭제됩니다. 리소스는 해당하는 DeletionPolicy에 따라 삭제됩니다. [자세히 알아보기](#)

취소 **스택 삭제**



**Thank You**

---