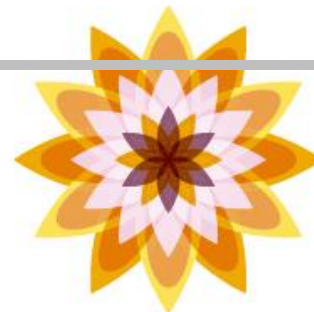
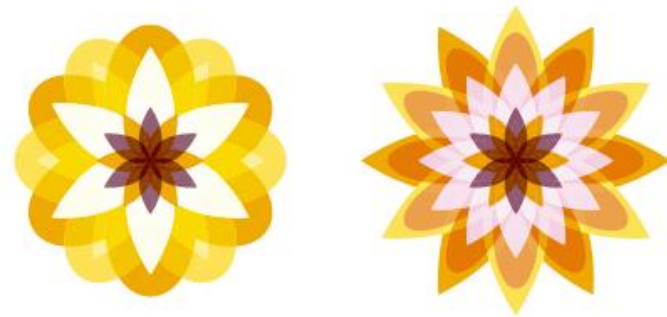


Chapter 09
VPC 고급

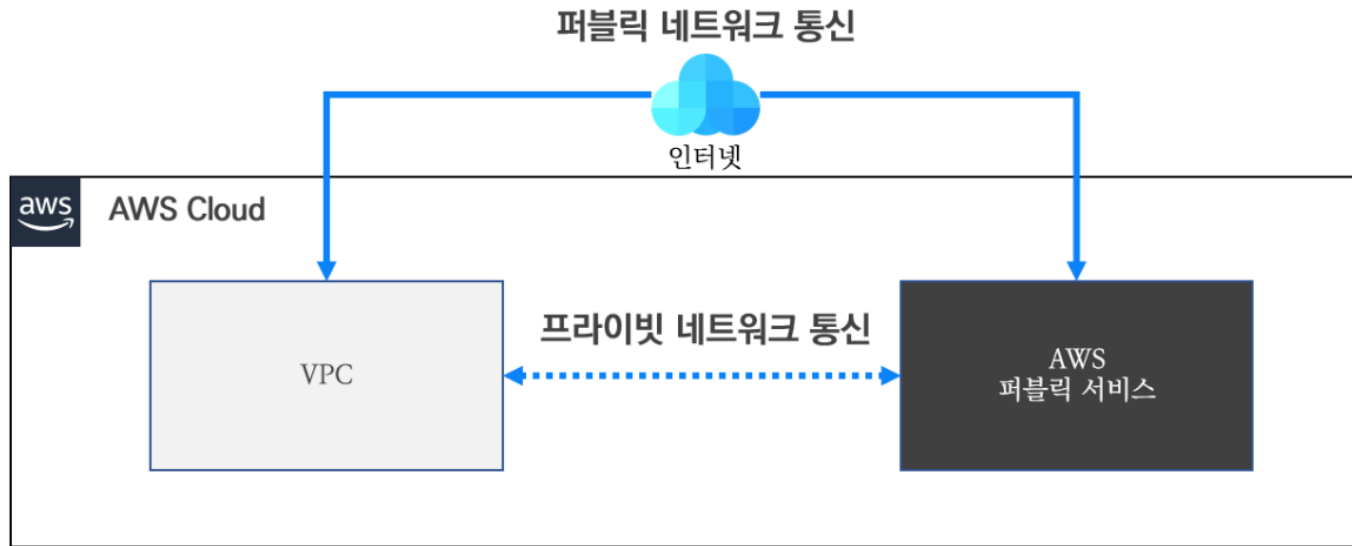


1. VPC 엔드포인트 (VPC Endpoint)

■ VPC 엔드포인트란?

■ VPC 엔드포인트 개요

- 사용자가 생성한 VPC에서 AWS 퍼블릭 서비스와 통신을 하거나 다른 VPC로 통신이 필요할 경우 일반적으로 외부 인터넷 구간인 퍼블릭 네트워크를 통해 통신이 이루어진다.



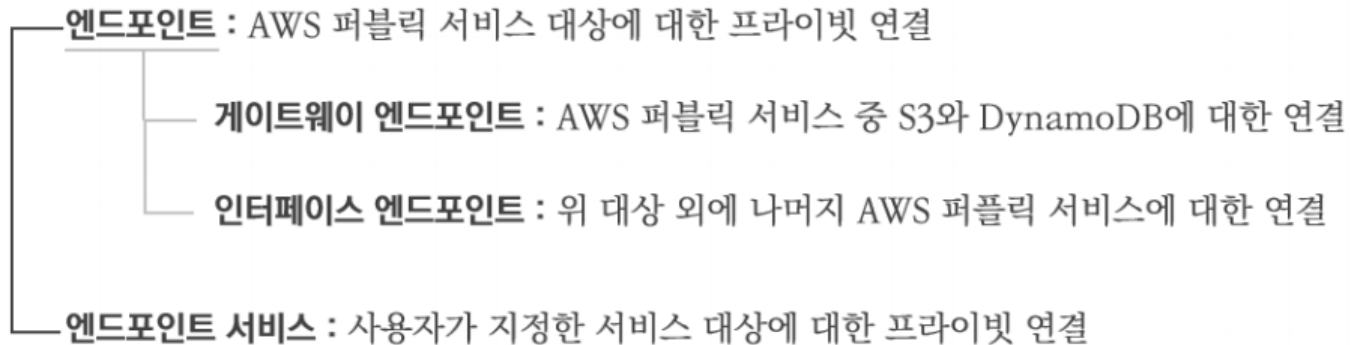
- VPC 엔드포인트(VPC Endpoint)는 AWS의 퍼블릭 서비스나 직접적으로 생성한 AWS 서비스에 대해 외부 인터넷 구간을 통한 접근이 아닌 직접적으로 접근할 수 있는 프라이빗 액세스 기능이다.

1. VPC 엔드포인트 (VPC Endpoint)

■ VPC 엔드포인트란?

■ VPC 엔드포인트 유형

- VPC 엔드포인트는 연결 대상 서비스에 따라 엔드포인트와 엔드포인트 서비스로 구분 지을 수 있다.
- 엔드포인트는 AWS 퍼블릭 서비스에 대상으로 연결을 하고, 엔드포인트 서비스는 사용자가 직접 생성한 서비스에 대해 연결을 한다는 차이이다.
- 이 중에 엔드포인트는 연결 대상 서비스 종류에 따라 게이트웨이 엔드포인트(Gateway Endpoint)와 인터페이스 엔드포인트(Interface Endpoint) 유형으로 나뉘어 진다.

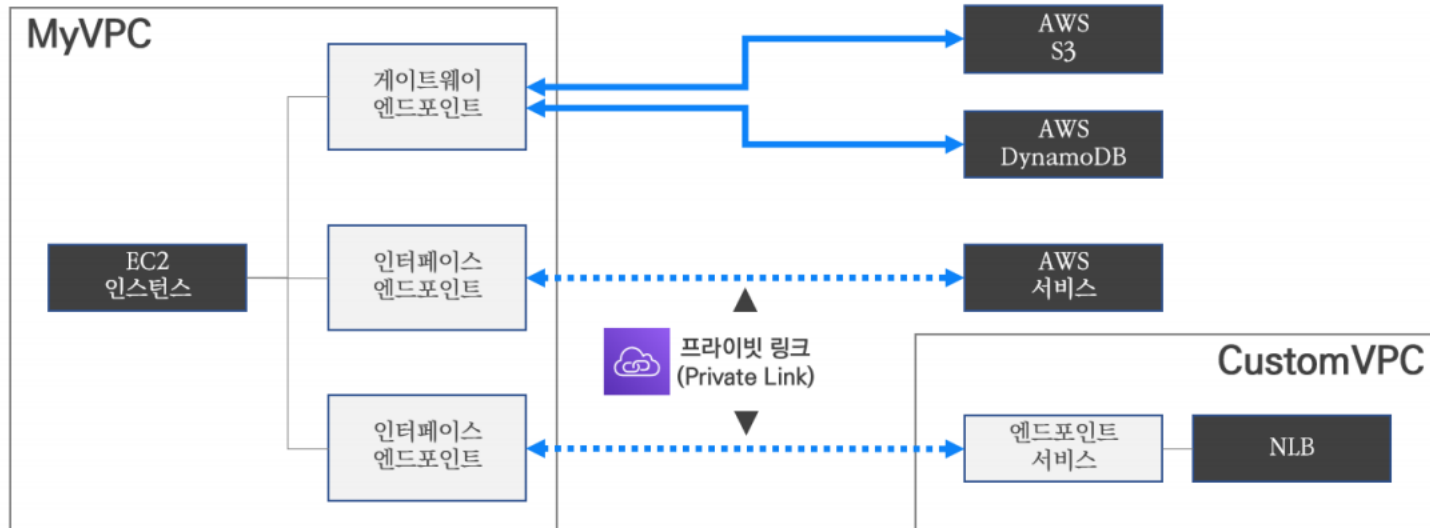


1. VPC 엔드포인트 (VPC Endpoint)

■ VPC 엔드포인트란?

■ VPC 엔드포인트 유형

- 다음 그림은 VPC 엔드포인트 종류별 차이를 보여준다.

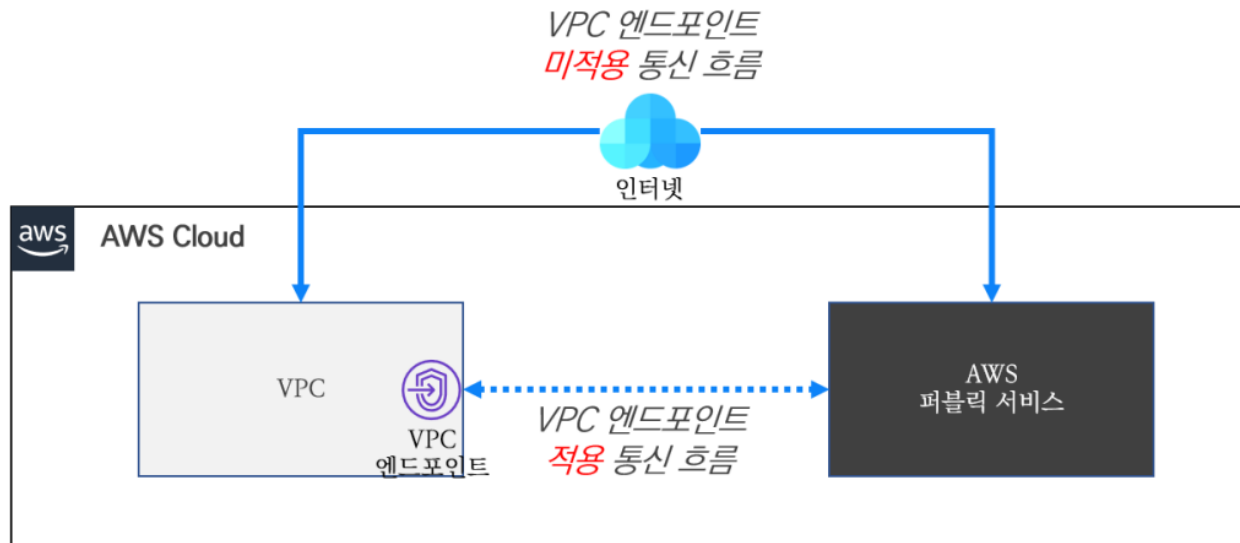


1. VPC 엔드포인트 (VPC Endpoint)

■ VPC 엔드포인트란?

■ VPC 엔드포인트 특징

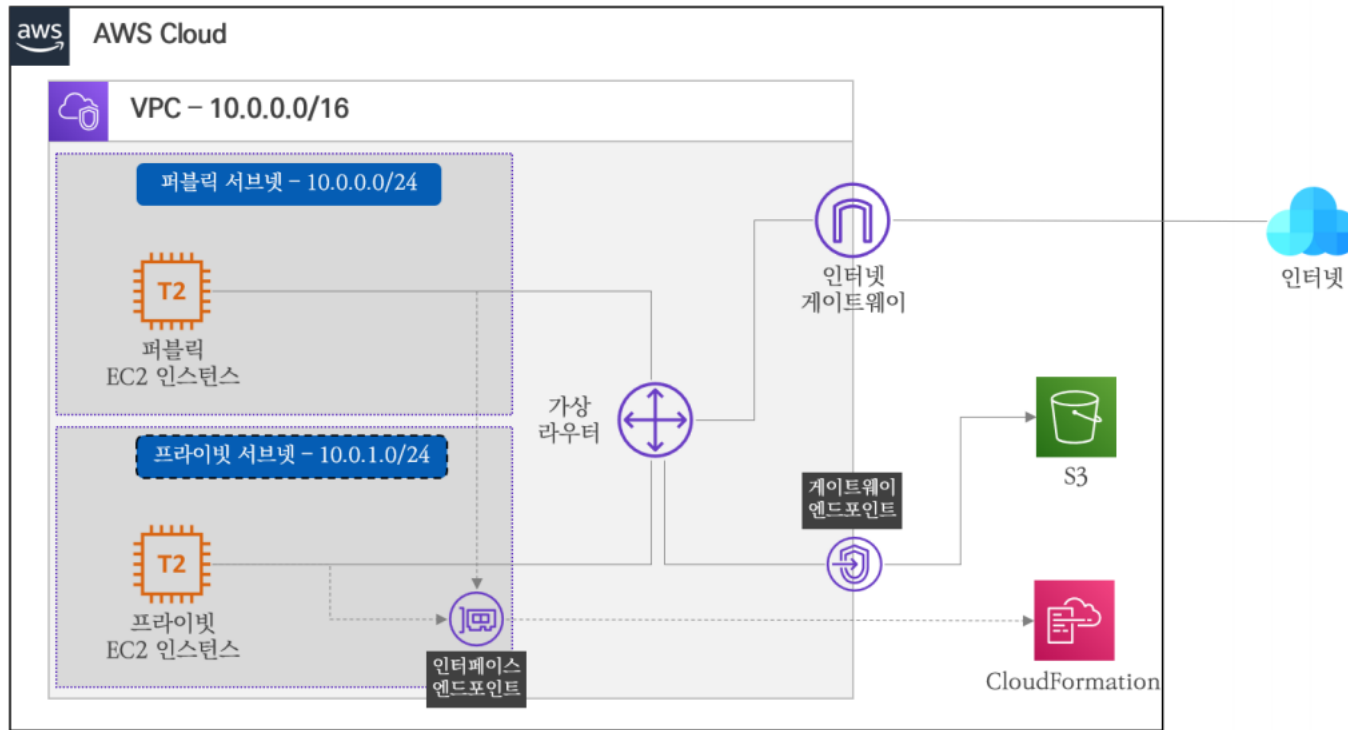
- 다음 그림은 VPC 엔드포인트 적용과 미적용에 따른 통신 흐름의 차이를 보여주고 있다.



- 대표적인 특징은 외부 인터넷 구간을 통한 퍼블릭 통신에서 프라이빗 링크를 통한 프라이빗 통신으로 볼 수 있다.
- 이에 따라 VPC 엔드포인트는 아래와 같은 특징을 가지고 있다.
 - 보안 측면 강화 : 프라이빗 연결을 통해 외부 구간으로 노출이 되지 않는다.
 - 서비스 제약 : 연결 대상 서비스는 동일 리전에 속한 서비스만 가능하다.
 - VPC 종속 : 오직 VPC 하나에만 연결할 수 있다. (다수의 VPC에 종속 불가)
 - 권한 제어 : AWS IAM 기능을 통해 정책을 수립하여 VPC 엔드포인트에 대한 권한 부여가 가능하다.

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

- 실습 후의 토폴로지는 다음 그림과 같다.

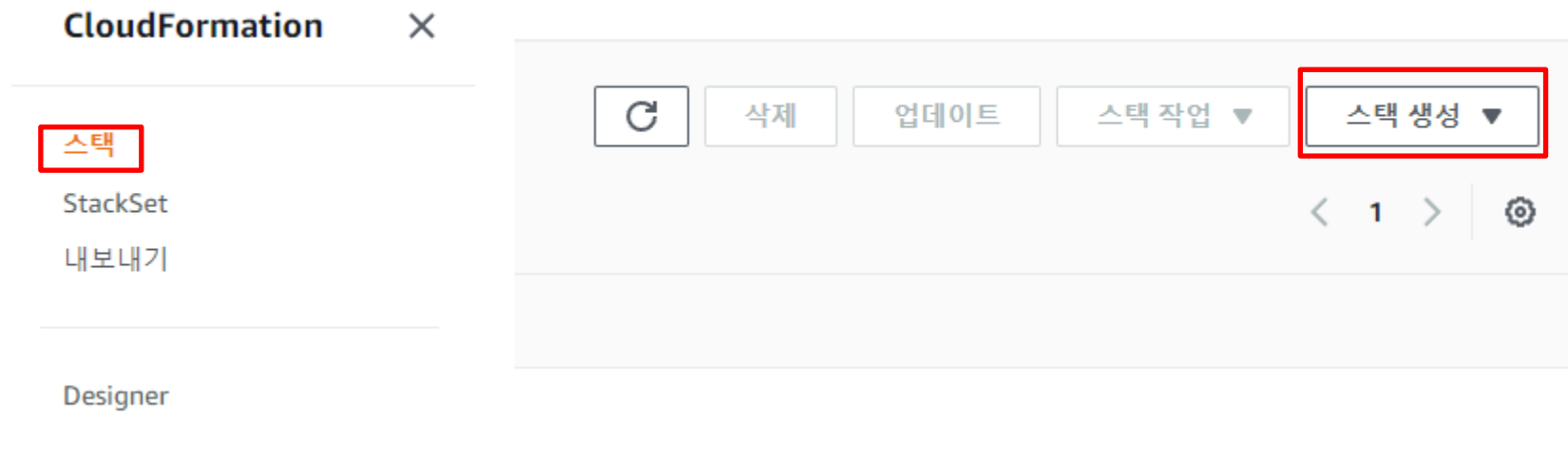


2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 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 lab09-1.yaml을 다운로드하고 스택 생성을 한다.



2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 기본 환경 적용

■ CloudFormation 적용

- 다운로드 링크 : <https://github.com/jjin300/cloud>
- CloudFormation 적용을 위해 상단의 링크를 통해 lab09-1.yaml을 다운로드하고 스택 생성을 한다.

스택 생성

사전 조건 - 템플릿 준비

템플릿 준비
모든 스택은 템플릿을 기반으로 합니다. 템플릿은 JSON 또는 YAML 텍스트 파일로, 스택에 포함하려는 AWS 리소스에 대한 구성 정보가 들어 있습니다.

☒ 준비된 템플릿 ☐ 샘플 템플릿 사용 ☐ Designer에서 템플릿 생성

템플릿 지정
템플릿은 스택의 리소스와 속성을 설명하는 JSON 또는 YAML 파일입니다.

템플릿 소스
템플릿을 선택하면 템플릿이 저장될 Amazon S3 URL이 생성됩니다.

☐ Amazon S3 URL ☒ 템플릿 파일 업로드

템플릿 파일 업로드

lab09-1.yaml

JSON 또는 YAML 형식 파일

S3 URL: <https://s3.ap-northeast-2.amazonaws.com/cf-templates-wala0sr1keps-ap-northeast-2/2022204E8Z-lab09-1.yaml>

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 기본 환경 적용

■ CloudFormation 적용

- 스택 이름을 입력하고, 리전에서 생성한 키페어를 선택하고 [다음]을 클릭

스택 세부 정보 지정

스택 이름

스택 이름

CloudNeta-Lab9-1

스택 이름은 문자(A-Z 및 a-z), 숫자(0-9) 및 대시(-)를 포함할 수 있습니다.

파라미터

파라미터는 템플릿에서 정의되며, 이를 통해 스택을 생성하거나 업데이트할 때 사용자 지정 값을 입력할 수 있습니다.

KeyName
Name of an existing EC2 KeyPair to enable SSH access to the instances. Linked to AWS Parameter

aws_study_key

LatestAmild
(DO NOT CHANGE)

/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2

취소 이전 다음

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 기본 환경 적용

■ CloudFormation 적용

- 이번 페이지에서는 별도의 선택없이 [다음]을 클릭

고급 옵션

스택에 알림 옵션 및 스택 정책 등과 같은 추가 옵션을 설정할 수 있습니다. [자세히 알아보기](#)

▶ 스택 정책

스택 업데이트 중 의도치 않게 업데이트되지 않도록 하려는 리소스를 정의합니다.

▶ 롤백 구성

CloudFormation이 스택을 생성 및 업데이트할 때 모니터링할 경보를 지정합니다. 작업이 경보 임계값을 위반할 경우 CloudFormation이 작업을 롤백합니다. [자세히 알아보기](#)

▶ 알림 옵션

▶ 스택 생성 옵션

취소

이전

다음

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 기본 환경 적용

■ CloudFormation 적용

- 이번 페이지에서는 별도의 선택없이 [스택 생성]을 클릭

알림 옵션

알림 옵션 없음
정의된 알림 옵션이 없습니다

스택 생성 옵션

제한 시간
-

종료 방지
비활성

▶ 빠른 생성 링크

취소

이전

변경 세트 만들기

스택 생성

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 기본 환경 적용

■ 생성 자원 확인

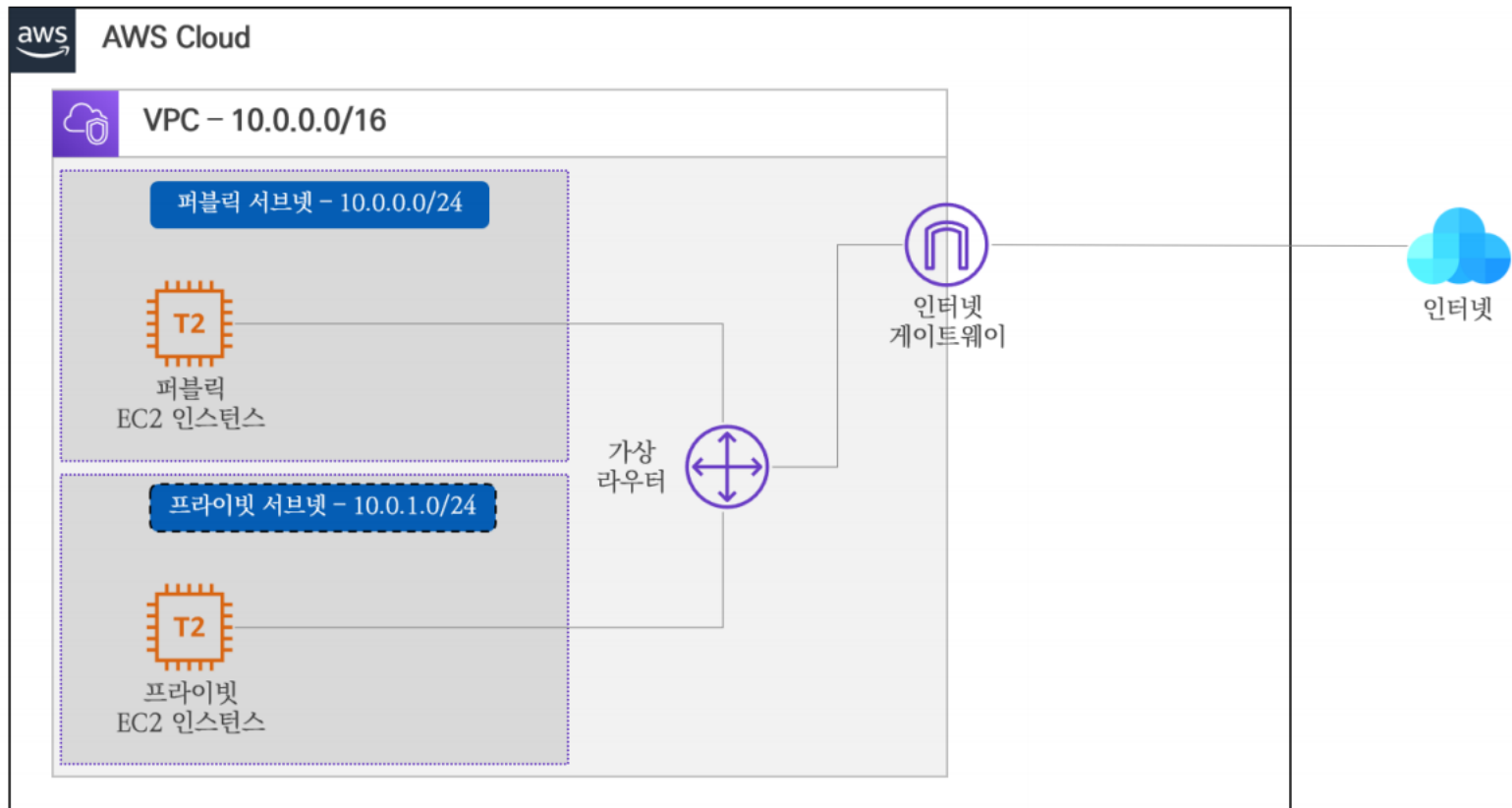
- 기본 환경 구성 자원 정보

자원	태그 이름	정보
VPC	CloudNeta-VPC	IP CIDR: 10.0.0.0/16
퍼블릭 서브넷	CloudNeta-Public-SN	IP CIDR: 10.0.0.0/24, AZ: ap-northeast-2a
프라이빗 서브넷	CloudNeta-Private-SN	IP CIDR: 10.0.1.0/24, AZ: ap-northeast-2c
퍼블릭 라우팅 테이블	CloudNeta-Public-RT	연결: 퍼블릭 서브넷, 라우팅 0.0.0.0/0 → IGW
프라이빗 라우팅 테이블	CloudNeta-Private-RT	연결: 프라이빗 서브넷
인터넷 게이트웨이	CloudNeta-IGW	연결: CloudNeta-VPC
퍼블릭 EC2 인스턴스	CloudNeta-Public-EC2	연결: 퍼블릭 서브넷, 퍼블릭 IP 할당: 활성화
프라이빗 EC2 인스턴스	CloudNeta-Private-EC2	연결: 프라이빗 서브넷, 계정: root, 비밀번호: qwe123

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 기본 환경 적용

- 생성 자원 확인
 - 기본 환경 토폴로지



2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 기본 환경 적용

■ 기본 환경 검증

- 퍼블릭 EC2 인스턴스

```
Microsoft Windows [Version 10.0.22000.795]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Wjin>ping s3.ap-northeast-2.amazonaws.com

Ping s3.ap-northeast-2.amazonaws.com [52.219.144.69] 32바이트 데이터 사용:
52.219.144.69의 응답: 바이트=32 시간=4ms TTL=49
52.219.144.69의 응답: 바이트=32 시간=4ms TTL=49
52.219.144.69의 응답: 바이트=32 시간=6ms TTL=49
52.219.144.69의 응답: 바이트=32 시간=5ms TTL=49

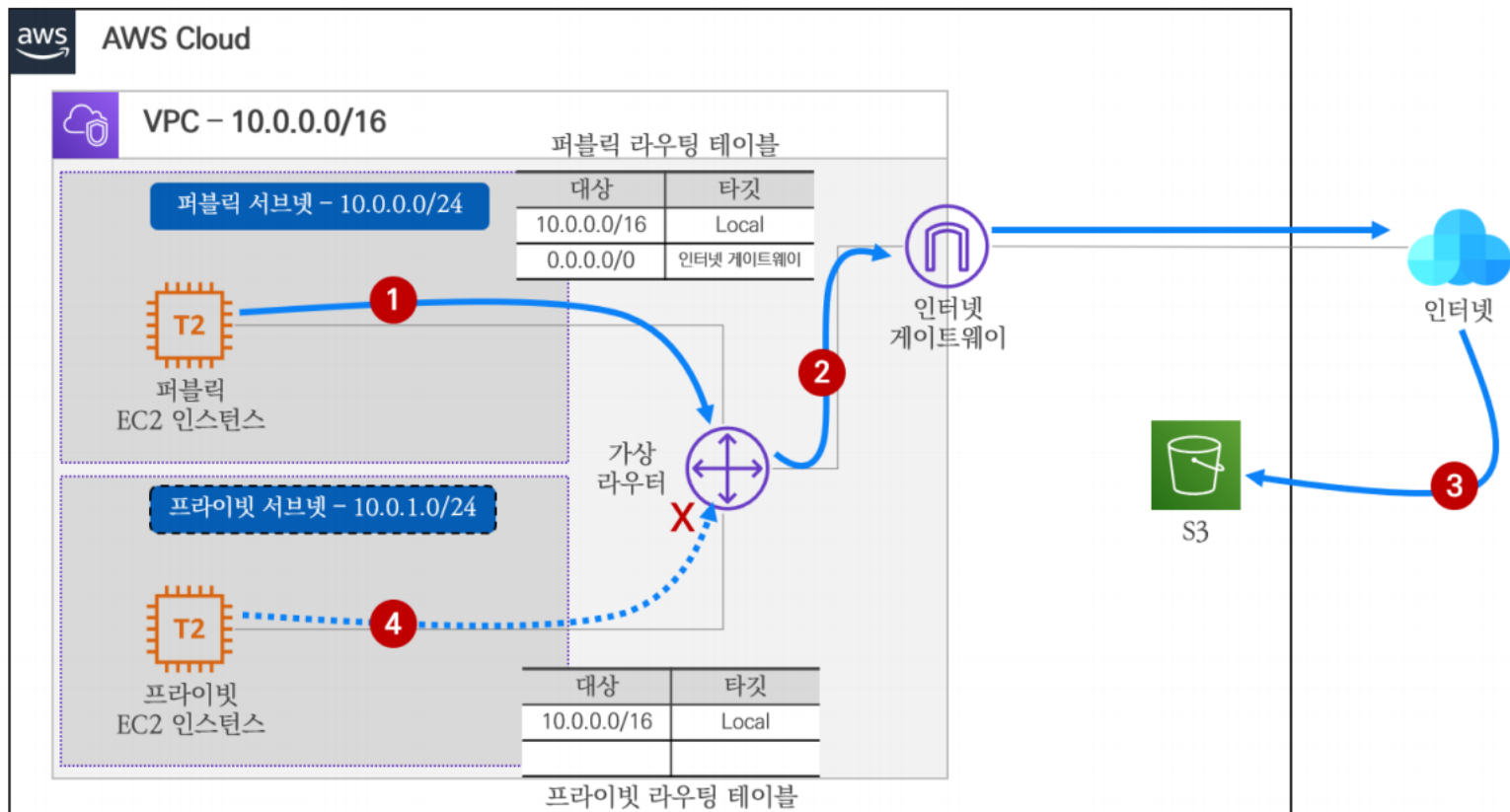
52.219.144.69에 대한 Ping 통계:
    패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
    왕복 시간(밀리초):
        최소 = 4ms, 최대 = 6ms, 평균 = 4ms
```

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 기본 환경 적용

■ 기본 환경 검증

- 기본 환경에서의 통신 흐름



2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 게이트웨이 엔드포인트 생성 및 검증

■ 게이트웨이 엔드포인트 생성

- 서비스 > VPC > Virtual Private Cloud > 엔드포인트 > 엔드포인트 생성

▼ Virtual Private Cloud

VPC

서브넷

라우팅 테이블

인터넷 게이트웨이

송신 전용 인터넷 게이트
웨이

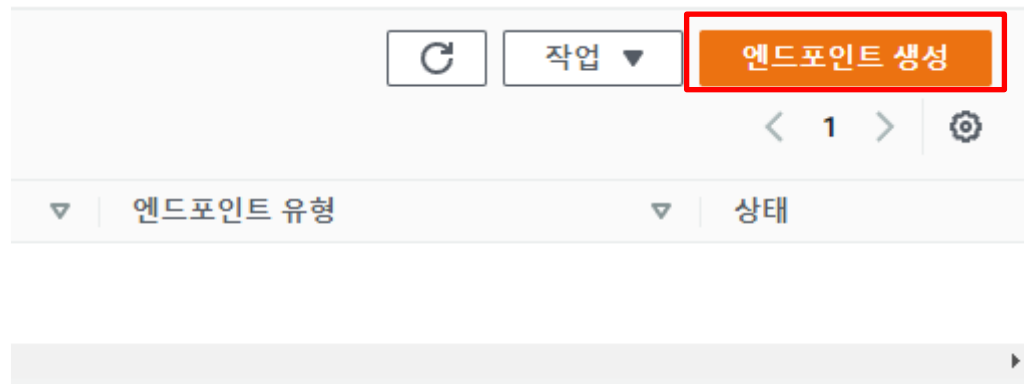
캐리어 게이트웨이

DHCP 옵션 세트

탄력적 IP

관리형 접두사 목록

엔드포인트



2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 게이트웨이 엔드포인트 생성 및 검증

■ 게이트웨이 엔드포인트 생성

- 서비스 필터에 "S3"을 입력 후 엔터
- S3 서비스 지정, VPC 엔드포인트 타입은 게이트웨이

서비스 (1/4)

서비스 필터링

search: s3 ✕ 필터 지우기

	서비스 이름	소유자	유형
<input checked="" type="radio"/>	com.amazonaws.ap-northeast-2.s3	amazon	Gateway
<input type="radio"/>	com.amazonaws.ap-northeast-2.s3	amazon	Interface
<input type="radio"/>	com.amazonaws.ap-northeast-2.s3-out...	amazon	Interface
<input type="radio"/>	com.amazonaws.s3-global.accesspoint	amazon	Interface

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 게이트웨이 엔드포인트 생성 및 검증

■ 게이트웨이 엔드포인트 생성

- VPC 엔드포인트의 VPC와 라우팅 테이블에서 퍼블릭/프라이빗 라우팅 테이블을 지정

VPC

엔드포인트를 생성할 VPC를 선택

VPC
엔드포인트를 생성할 VPC입니다.

vpc-07de255d3a7c9c317 (CloudNeta-VPC)

라우팅 테이블 (2/3) 정보

라우팅 테이블 필터링

< 1 > ⚙

<input type="checkbox"/>	이름	라우팅 테이블 ID	기본
<input checked="" type="checkbox"/>	CloudNeta-Public-RT	rtb-0e4f3fae187fe258e (CloudNeta-Pu...	아니요
<input checked="" type="checkbox"/>	CloudNeta-Private-RT	rtb-0c19f738ede52a299 (CloudNeta-Pr...	아니요
<input type="checkbox"/>	-	rtb-0b1aa7e8e9ac62b35	예

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 게이트웨이 엔드포인트 생성 및 검증

■ 게이트웨이 엔드포인트 생성

- [엔드포인트 생성]을 클릭한 후, 게이트웨이 엔드포인트 생성 확인

엔드포인트 (1/1) 정보

Q 엔드포인트 필터링

VPC 엔드포인트 ID: vpce-0ee6a8ee6dfbe3218 X 필터 지우기

<input checked="" type="checkbox"/>	Name	VPC 엔드포인트 ID	VPC ID	서비스 이름	엔드포인트 유형
<input checked="" type="checkbox"/>	-	vpce-0ee6a8ee6dfbe3218	vpc-07de255d3a7c9c317 CloudNeta-...	com.amazonaws.ap-northeast-2.s3	Gateway

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 게이트웨이 엔드포인트 생성 및 검증

■ 게이트웨이 엔드포인트 생성

- 프라이빗 라우팅 테이블의 경로 확인

라우팅 테이블 (1/5) 정보

Q 라우팅 테이블 필터링

	Name ▾	라우팅 테이블 ID ▾	명시적 서브넷 연결	엣지 연결	기본 ▾	VPC ▾	소유자 ID
<input type="checkbox"/>	route-table-01	rtb-06803ddd6f0e7d347	-	-	아니요	vpc-09a4345ed931a86cc my...	262663767358
<input type="checkbox"/>	CloudNeta-Public-RT	rtb-0e4f3fae187fe258e	subnet-09b299c06521d...	-	아니요	vpc-07de255d3a7c9c317 Clo...	262663767358
<input checked="" type="checkbox"/>	CloudNeta-Private-RT	rtb-0c19f738ede52a299	subnet-0395bde2bd100...	-	아니요	vpc-07de255d3a7c9c317 Clo...	262663767358
<input type="checkbox"/>	-	rtb-0679e4924f94f85df	-	-	예	vpc-09a4345ed931a86cc my...	262663767358
<input type="checkbox"/>	-	rtb-0b1aa7e8e9ac62b35	-	-	예	vpc-07de255d3a7c9c317 Clo...	262663767358

rtb-0c19f738ede52a299 / CloudNeta-Private-RT

세부 정보 라우팅 서브넷 연결 엣지 연결 라우팅 전파 태그

라우팅 (2)

Q 라우팅 필터링

모두 ▾

대상 ▾	대상 ▾	상태
pl-78a54011	vpce-0ee6a8ee6dfbe3218	✓ 활성화
10.0.0.0/16	local	✓ 활성화

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 게이트웨이 엔드포인트 생성 및 검증

■ 게이트웨이 엔드포인트 생성

- 퍼블릭 라우팅 테이블의 경로 확인

라우팅 테이블 (1/5) 정보

Q 라우팅 테이블 필터링

	Name ▾	라우팅 테이블 ID ▾	명시적 서브넷 연결	엣지 연결	기본 ▾	VPC ▾
<input type="checkbox"/>	route-table-01	rtb-06803ddd6f0e7d347	-	-	아니요	vpc-09a4345ed931a86cc my...
<input checked="" type="checkbox"/>	CloudNeta-Public-RT	rtb-0e4f3fae187fe258e	subnet-09b299c06521d...	-	아니요	vpc-07de255d3a7c9c317 Clo...
<input type="checkbox"/>	CloudNeta-Private-RT	rtb-0c19f738ede52a299	subnet-0395bde2bd100...	-	아니요	vpc-07de255d3a7c9c317 Clo...
<input type="checkbox"/>	-	rtb-0679e4924f94f85df	-	-	예	vpc-09a4345ed931a86cc my...
<input type="checkbox"/>	-	rtb-0b1aa7e8e9ac62b35	-	-	예	vpc-07de255d3a7c9c317 Clo...

rtb-0e4f3fae187fe258e / CloudNeta-Public-RT

세부 정보 | 라우팅 | 서브넷 연결 | 엣지 연결 | 라우팅 전파 | 태그

라우팅 (3)

Q 라우팅 필터링

모두 ▾

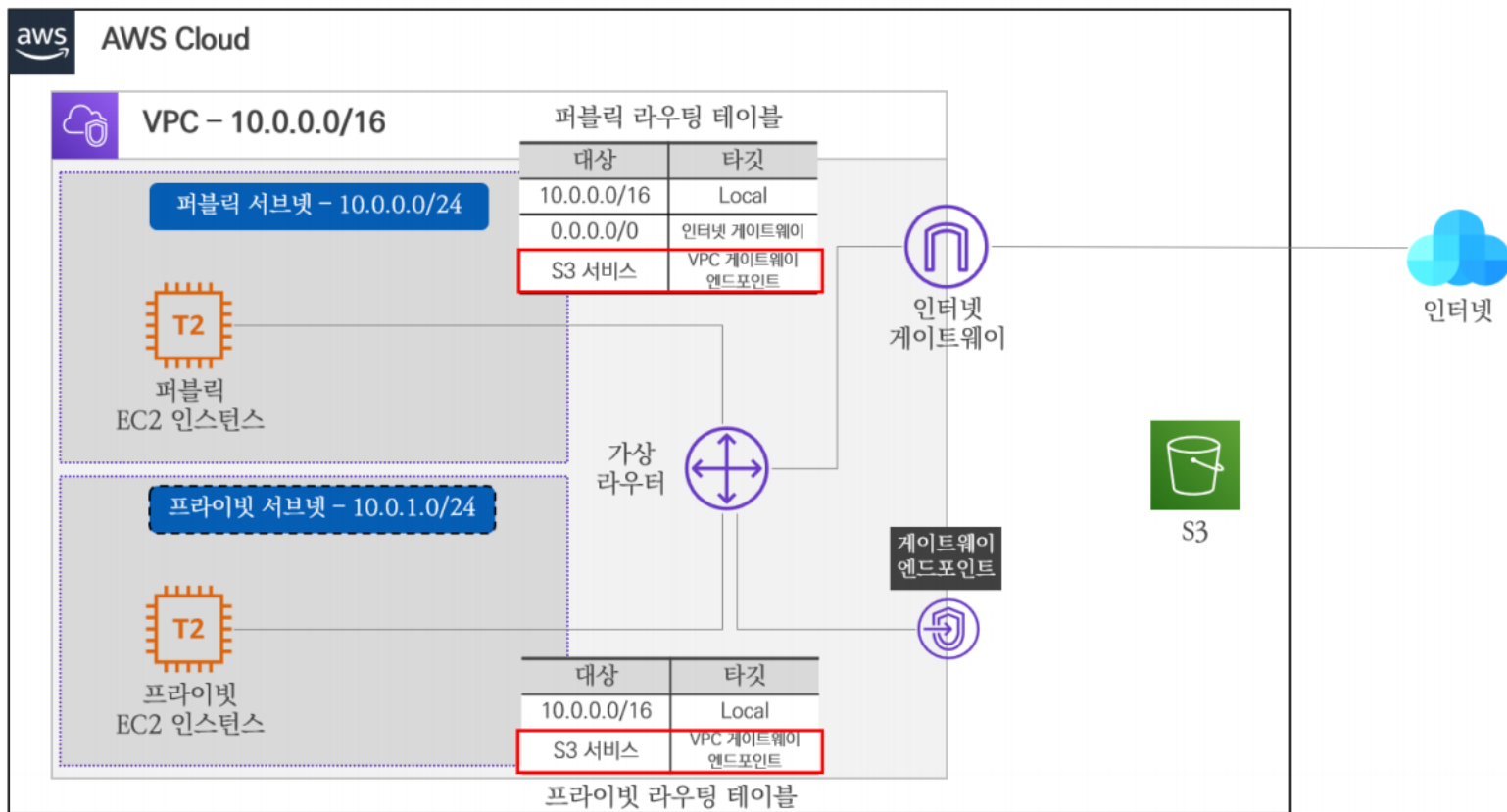
대상 ▾	대상 ▾	상태
pl-78a54011	vpce-0ee6a8ee6dfbe3218	✓ 활성화
0.0.0.0/0	igw-00cd24f62457b50ce	✓ 활성화
10.0.0.0/16	local	✓ 활성화

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 게이트웨이 엔드포인트 생성 및 검증

■ 게이트웨이 엔드포인트 생성

- 게이트웨이 엔드포인트 생성 도식화



2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 게이트웨이 엔드포인트 생성 및 검증

■ 게이트웨이 엔드포인트 검증

- 퍼블릭 EC2를 선택 후, 연결 버튼을 클릭

인스턴스 (1/2) 정보 🔄 연결

🔍 검색

인스턴스 상태 = running ✕ 필터 지우기

<input type="checkbox"/>	Name	인스턴스 ID	인스턴스 상태	인스턴스 유형	상태 검사	경보 상태	가용 영역	퍼블릭 IP
<input checked="" type="checkbox"/>	CloudNeta-Pu...	i-033fa1bc9a9817db2	🟢 실행 중 🔍	t2.micro	🟢 2/2개 검사 통과...	경보 없음	+	ap-northeast-2a
<input type="checkbox"/>	CloudNeta-Pri...	i-06620845270d412ac	🟢 실행 중 🔍	t2.micro	🟢 2/2개 검사 통과...	경보 없음	+	ap-northeast-2c

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 게이트웨이 엔드포인트 생성 및 검증

■ 게이트웨이 엔드포인트 검증

- [인스턴스에 연결] 화면에서 [연결] 버튼을 클릭

EC2 > 인스턴스 > i-033fa1bc9a9817db2 > 인스턴스에 연결

인스턴스에 연결 정보

다음 옵션 중 하나를 사용하여 인스턴스 i-033fa1bc9a9817db2 (CloudNeta-Public-EC2)에 연결

EC2 인스턴스 연결

Session Manager

SSH 클라이언트

EC2 직렬 콘솔

인스턴스 ID
i-033fa1bc9a9817db2 (CloudNeta-Public-EC2)

퍼블릭 IP 주소
3.34.49.218

사용자 이름

사용자 지정 사용자 이름을 사용하여 연결하거나 인스턴스 시작에 사용한 AMI의 기본 사용자 이름 ec2-user를(를) 사용합니다.

❗ 참고: 대부분의 경우 추정된 사용자 이름은 정확합니다. 하지만 AMI 사용 지침을 읽고 AMI 소유자가 기본 AMI 사용자 이름을 변경했는지 확인하십시오.

취소

연결

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 게이트웨이 엔드포인트 생성 및 검증

■ 게이트웨이 엔드포인트 검증

- ping s3.ap-northeast-2.amazonaws.com

```
aws  서비스  Q 서비스, 기능, 블로그, 설명서 등을 검색합니다. [Alt+S]
Last login: Sat Jul 23 13:35:33 2022 from 59.16.139.7

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

https://aws.amazon.com/amazon-linux-2/
12 package(s) needed for security, out of 22 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-0-29 ~]$ ping s3.ap-northeast-2.amazonaws.com
PING s3.ap-northeast-2.amazonaws.com (52.219.146.89) 56(84) bytes of data.
64 bytes from s3.ap-northeast-2.amazonaws.com (52.219.146.89): icmp_seq=1 ttl=57 time=0.598 ms
64 bytes from s3.ap-northeast-2.amazonaws.com (52.219.146.89): icmp_seq=2 ttl=57 time=0.650 ms
64 bytes from s3.ap-northeast-2.amazonaws.com (52.219.146.89): icmp_seq=3 ttl=57 time=0.623 ms
64 bytes from s3.ap-northeast-2.amazonaws.com (52.219.146.89): icmp_seq=4 ttl=57 time=0.683 ms
64 bytes from s3.ap-northeast-2.amazonaws.com (52.219.146.89): icmp_seq=5 ttl=57 time=0.632 ms
64 bytes from s3.ap-northeast-2.amazonaws.com (52.219.146.89): icmp_seq=6 ttl=57 time=0.601 ms
64 bytes from s3.ap-northeast-2.amazonaws.com (52.219.146.89): icmp_seq=7 ttl=57 time=0.609 ms
64 bytes from s3.ap-northeast-2.amazonaws.com (52.219.146.89): icmp_seq=8 ttl=57 time=0.611 ms
^Z
[1]+  Stopped                  ping s3.ap-northeast-2.amazonaws.com
[ec2-user@ip-10-0-0-29 ~]$
```

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 게이트웨이 엔드포인트 생성 및 검증

■ 게이트웨이 엔드포인트 검증

- 프라이빗 인스턴스를 선택 후, 프라이빗 IP 주소를 복사

인스턴스 (1/2) 정보

검색

	Name	인스턴스 ID	인스턴스 상태	인스턴스 유형	상태 검사	경보 상태	가용 영역	퍼블릭 IPv4
<input type="checkbox"/>	CloudNeta-Pu...	i-033fa1bc9a9817db2	실행 중	t2.micro	2/2개 검사 통과...	경보 없음	ap-northeast-2a	-
<input checked="" type="checkbox"/>	CloudNeta-Pri...	i-06620845270d412ac	실행 중	t2.micro	2/2개 검사 통과...	경보 없음	ap-northeast-2c	-

세부 정보

보안

네트워킹

스토리지

상태 검사

모니터링

태그

인스턴스 요약 정보

인스턴스 ID
i-06620845270d412ac (CloudNeta-Private-EC2)

IPv6 주소
-

호스트 이름 유형
IP 이름: ip-10-0-1-29.ap-northeast-2.compute.internal

프라이빗 리소스 DNS 이름 응답
-

퍼블릭 IPv4 주소
-

인스턴스 상태
실행 중

프라이빗 IP DNS 이름(IPv4만 해당)
ip-10-0-1-29.ap-northeast-2.compute.internal

인스턴스 유형
t2.micro

프라이빗 IPv4 주소
10.0.1.29

퍼블릭 IPv4 DNS
-

탄력적 IP 주소
-

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 게이트웨이 엔드포인트 생성 및 검증

■ 게이트웨이 엔드포인트 검증

- 퍼블릭 EC2 인스턴스 SSH 터미널에서 프라이빗 EC2 인스턴스에 접속(계정: root, 암호: qwe123)
- ssh root@프라이빗 EC2 IP 주소

```
aws | 서비스 | Q 서비스, 기능, 블로그, 설명서 등을 검색합니다. [Alt+S]
Last login: Sat Jul 23 13:39:53 2022 from ec2-13-209-1-61.ap-northeast-2.compute.amazonaws.com

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

https://aws.amazon.com/amazon-linux-2/
12 package(s) needed for security, out of 22 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-0-29 ~]$ ssh root@10.0.1.29
The authenticity of host '10.0.1.29 (10.0.1.29)' can't be established.
ECDSA key fingerprint is SHA256:iakYhrufxxgTCD6hDA2DGrP2yzubjoVHuOCi/SMcG4k.
ECDSA key fingerprint is MD5:c8:cd:c7:1e:55:57:97:7b:49:90:f1:19:e6:fb:c5:6a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.1.29' (ECDSA) to the list of known hosts.
root@10.0.1.29's password:

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

https://aws.amazon.com/amazon-linux-2/
[root@ip-10-0-1-29 ~]#
```

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 게이트웨이 엔드포인트 생성 및 검증

■ 게이트웨이 엔드포인트 검증

- ping s3.ap-northeast-2.amazonaws.com

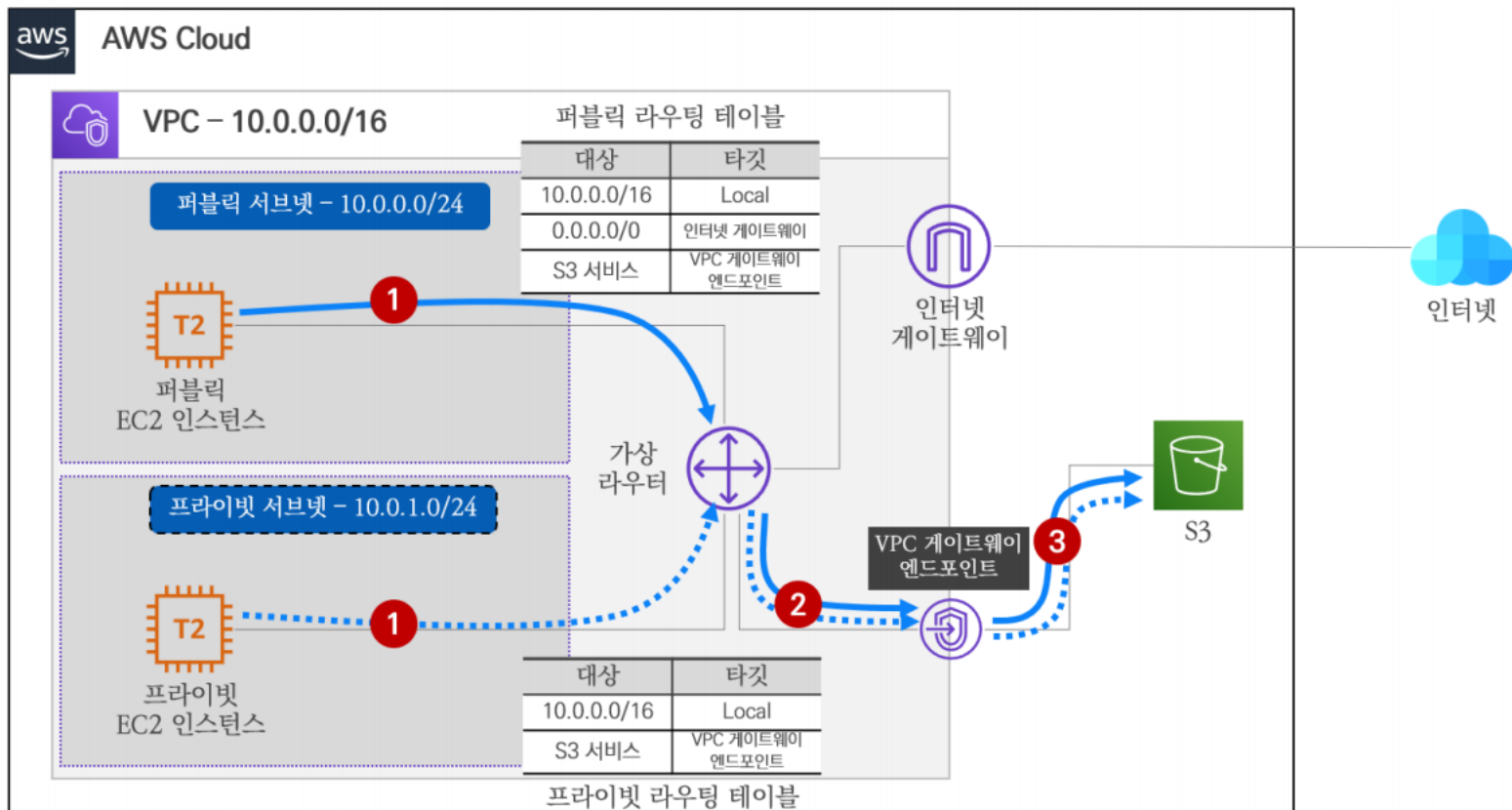
```
https://aws.amazon.com/amazon-linux-2/
[root@ip-10-0-1-29 ~]# ping s3.ap-northeast-2.amazonaws.com
PING s3.ap-northeast-2.amazonaws.com (52.219.144.73) 56(84) bytes of data.
64 bytes from s3.ap-northeast-2.amazonaws.com (52.219.144.73): icmp_seq=1 ttl=57 time=0.898 ms
64 bytes from s3.ap-northeast-2.amazonaws.com (52.219.144.73): icmp_seq=2 ttl=57 time=0.874 ms
64 bytes from s3.ap-northeast-2.amazonaws.com (52.219.144.73): icmp_seq=3 ttl=57 time=0.936 ms
64 bytes from s3.ap-northeast-2.amazonaws.com (52.219.144.73): icmp_seq=4 ttl=57 time=0.888 ms
64 bytes from s3.ap-northeast-2.amazonaws.com (52.219.144.73): icmp_seq=5 ttl=57 time=0.932 ms
64 bytes from s3.ap-northeast-2.amazonaws.com (52.219.144.73): icmp_seq=6 ttl=57 time=0.893 ms
^Z
[1]+  Stopped                  ping s3.ap-northeast-2.amazonaws.com
[root@ip-10-0-1-29 ~]#
```

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 게이트웨이 엔드포인트 생성 및 검증

■ 게이트웨이 엔드포인트 검증

- VPC 게이트웨이 엔드포인트 생성 후 S3 통신 흐름



2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 인터페이스 엔드포인트 생성 및 검증

■ 인터페이스 엔드포인트 생성

- 이번 실습에서는 통신 대상을 CloudFormation 서비스로 변경하여 실습해보자.
- 실습을 진행하기에 앞서 기본 환경에서 동작을 우선 확인한다.
- `dig +short cloudformation.ap-northeast-2.amazonaws.com`

```
[1]+  Stopped                  ping s3.ap-northeast-2.amazonaws.com
[root@ip-10-0-1-29 ~]# dig +short cloudformation.ap-northeast-2.amazonaws.com
52.95.193.132
[root@ip-10-0-1-29 ~]#
```

- 퍼블릭 EC2 인스턴스는 인터넷 구간을 통해 통신이 가능하나 프라이빗 EC2 인스턴스는 통신이 불가능하다.
- 이러한 통신 제약을 해소하기 위해 VPC 엔드포인트를 활용하여 해결할 수 있으며, 연결 대상 AWS 서비스가 S3나 DynamoDB가 아니기 때문에 인터페이스 엔드포인트를 통해 실습을 진행한다.

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 인터페이스 엔드포인트 생성 및 검증

■ 인터페이스 엔드포인트 생성

- 기본적으로 AWS 서비스는 리전별로 기본 DNS 호스트 주소를 가지고 있다.
- 여기에 VPC 인터페이스 엔드포인트를 생성하면, 엔드포인트 전용 DNS 호스트가 생성된다.
- 이 DNS 주소들은 인터페이스 엔드포인트의 설정값 중에 '프라이빗 DNS 활성화' 설정 여부에 따라 통신 흐름이 달라진다.

설정	통신 흐름	
프라이빗 DNS 비활성화	기본 DNS 호스트	인터넷 구간을 통한 퍼블릭 통신
	엔드포인트 전용 DNS 호스트	인터페이스 엔드포인트를 통한 프라이빗 통신
프라이빗 DNS 활성화	기본 DNS 호스트	인터페이스 엔드포인트를 통한 프라이빗 통신
	엔드포인트 전용 DNS 호스트	인터페이스 엔드포인트를 통한 프라이빗 통신

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 인터페이스 엔드포인트 생성 및 검증

■ 인터페이스 엔드포인트 생성

- 이번 실습에서는 프라이빗 DNS 활성화를 설정하여 모든 DNS 호스트가 인터페이스 엔드포인트를 통해 프라이빗 통신을 하도록 한다.
- 인터페이스 엔드포인트에서 프라이빗 DNS 활성화를 설정하려면, 생성한 VPC에서 'DNS 호스트 이름을 활성화해야 한다.'
- 서비스 > VPC > Virtual Private Cloud > VPC > 작업 > DNS 호스트 이름 편집

▼ Virtual Private Cloud

VPC

서브넷

라우팅 테이블

인터넷 게이트웨이

송신 전용 인터넷 게이트웨이

The screenshot shows the AWS VPC console interface. On the left, the 'Virtual Private Cloud' section is expanded, and 'VPC' is selected. The main area displays a table of VPCs. The '작업' (Actions) dropdown menu is open, and 'DNS 호스트 이름 편집' (Edit DNS hostnames) is highlighted. The table has columns for IPv4 CIDR, IPv6 CIDR, and DHCP 옵션 세트 (DHCP Options Set).

IPv4 CIDR	IPv6 CIDR	DHCP 옵션 세트
37.120.0.0/16	-	dopt-f6296e9d
10.0.0.0/16	-	dopt-f6296e9d

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 인터페이스 엔드포인트 생성 및 검증

■ 인터페이스 엔드포인트 생성

- DNS 호스트 이름 편집 메뉴에서 활성화를 선택 후, [변경 사항 저장] 버튼을 클릭

VPC > VPC > vpc-07de255d3a7c9c317 > DNS 호스트 이름 편집

DNS 호스트 이름 편집 정보

DNS 호스트 이름

퍼블릭 IP 주소가 있는 인스턴스가 이에 해당하는 퍼블릭 DNS 호스트 이름을 가질지 여부를 나타냅니다.

VPC ID	DNS 호스트 이름
 vpc-07de255d3a7c9c317	<input checked="" type="checkbox"/> 활성화

[취소](#)[변경 사항 저장](#)

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 인터페이스 엔드포인트 생성 및 검증

■ 인터페이스 엔드포인트 생성

- 위 작업이 완료 후 본격적인 인터페이스 엔드포인트를 생성한다.
- 서비스 > VPC > Virtual Private Cloud > 엔드포인트 > 엔드포인트 생성

▼ Virtual Private Cloud

VPC

서브넷

라우팅 테이블

인터넷 게이트웨이

송신 전용 인터넷 게이트웨이

캐리어 게이트웨이



DHCP 옵션 세트

탄력적 IP

관리형 접두사 목록

엔드포인트

엔드포인트 서비스

				작업 ▼	엔드포인트 생성
			< 1 > 		
서비스 이름	엔드포인트 유형	상태			
com.amazonaws.ap-northeast-2.s3	Gateway	🟢 사용 가능			

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 인터페이스 엔드포인트 생성 및 검증

■ 인터페이스 엔드포인트 생성

- VPC 엔드포인트 서비스 지정
- 필터에 cloudformation을 입력

서비스 (126)			
<div><input type="text" value="cloudformation"/></div>			
<div>< 1 2 3 4 5 6 7 ... 13 ></div>			
	서비스 이름	소유자	유형
<input type="radio"/>	aws.sagemaker.ap-northeast-2.notebook	amazon	Interface
<input type="radio"/>	aws.sagemaker.ap-northeast-2.studio	amazon	Interface
<input type="radio"/>	com.amazonaws.ap-northeast-2.access-...	amazon	Interface
<input type="radio"/>	com.amazonaws.ap-northeast-2.acm-pca	amazon	Interface
<input type="radio"/>	com.amazonaws.ap-northeast-2.airflow...	amazon	Interface
<input type="radio"/>	com.amazonaws.ap-northeast-2.airflow...	amazon	Interface
<input type="radio"/>	com.amazonaws.ap-northeast-2.airflow...	amazon	Interface
<input type="radio"/>	com.amazonaws.ap-northeast-2.applica...	amazon	Interface
<input type="radio"/>	com.amazonaws.ap-northeast-2.appme...	amazon	Interface
<input type="radio"/>	com.amazonaws.ap-northeast-2.appstr...	amazon	Interface

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 인터페이스 엔드포인트 생성 및 검증

■ 인터페이스 엔드포인트 생성

- VPC 엔드포인트의 VPC 대상과 서브넷 지정
- 필터에 cloudformation을 입력

서비스 (1/1)

서비스 필터링

search: cloudformation X 필터 지우기

서비스 이름	소유자	유형
com.amazonaws.ap-northeast-2.cloudf...	amazon	Interface

VPC

엔드포인트를 생성할 VPC를 선택

VPC

엔드포인트를 생성할 vpc입니다.

vpc-07de255d3a7c9c317 (CloudNeta-VPC)

추가 설정

서브넷 (2/4) 정보

가용 영역	서브넷 ID
<input checked="" type="checkbox"/> ap-northeast-2a (apne2-az1)	subnet-09b299c06521dd460
<input type="checkbox"/> ap-northeast-2b (apne2-az2)	사용 가능한 서브넷 없음
<input checked="" type="checkbox"/> ap-northeast-2c (apne2-az3)	subnet-0395bde2bd100a705
<input type="checkbox"/> ap-northeast-2d (apne2-az4)	사용 가능한 서브넷 없음

subnet-09b299c06521dd460 X CloudNeta-Public-SN

subnet-0395bde2bd100a705 X CloudNeta-Private-SN

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 인터페이스 엔드포인트 생성 및 검증

■ 인터페이스 엔드포인트 생성

- [엔드포인트 생성] 버튼 클릭

태그

이 리소스에 연결된 태그가 없습니다.

새 태그 추가

50을(를) 태그 개 더 추가할 수 있습니다.

[취소](#)[엔드포인트 생성](#)

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 인터페이스 엔드포인트 생성 및 검증

■ 인터페이스 엔드포인트 생성

- 인터페이스 엔드포인트를 생성하면 약 2분의 대기 후 사용 가능 상태로 전환된다.
- 해당 엔드포인트의 상세 정보를 보면, DNS 주소를 확인해 볼 수 있다.
- 기본 DNS 호스트는 동일한 형태이지만 엔드포인트 전용 DNS 호스트는 개별적으로 다른 형태이니 각자의 주소를 복사해 둔다.

엔드포인트 (1/1) 정보

Q 엔드포인트 필터링

VPC 엔드포인트 ID: vpce-093517d1686ace06d X 필터 지우기

<input checked="" type="checkbox"/>	Name	VPC 엔드포인트 ID	VPC ID	서비스 이름
<input checked="" type="checkbox"/>	-	vpce-093517d1686ace06d	vpc-07de255d3a7c9c317 CloudNeta-...	com.amazonaws.ap-northeast-2.cloudformation

세부 정보

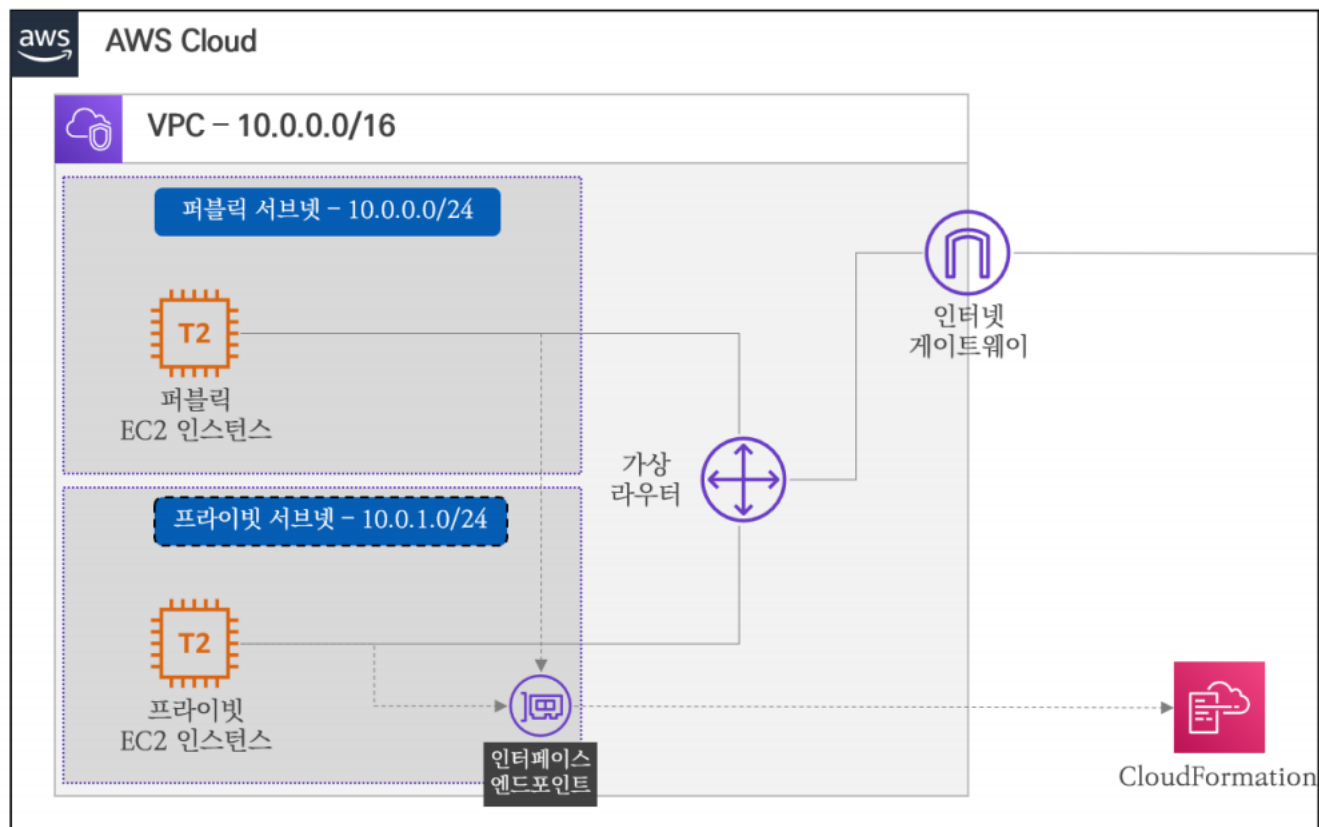
엔드포인트 ID vpce-093517d1686ace06d	상태 대기 중	생성 시간 2022년 7월 23일 토요일 23시 26분 10초 GMT+9
VPC ID vpc-07de255d3a7c9c317 (CloudNeta-VPC)	상태 메시지 -	서비스 이름 com.amazonaws.ap-northeast-2.cloudformation
DNS 레코드 IP 유형 ipv4	IP 주소 유형 ipv4	DNS 이름 vpce-093517d1686ace06d-txsku1pk.cloudformation.ap-northeast-2.vpce.amazonaws.com - (Z27UANNTOPRK1T) vpce-093517d1686ace06d-txsku1pk-ap-northeast-2c.cloudformation.ap-northeast-2.vpce.amazonaws.com - (Z27UANNTOPRK1T) vpce-093517d1686ace06d-txsku1pk-ap-northeast-

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 인터페이스 엔드포인트 생성 및 검증

■ 인터페이스 엔드포인트 생성

- 그림과 같이 인터페이스 엔드포인트는 가상 네트워크 인터페이스 형식으로 프라이빗 서브넷 내에 배치되어 있으며, CloudFormation과 연결되어 있다.



2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 인터페이스 엔드포인트 생성 및 검증

■ 인터페이스 엔드포인트 검증

- CloudFormation 서비스 연결을 위한 인터페이스 엔드포인트를 생성하였다.
- 실제 EC2 인스턴스에 접속하여 CloudFormation의 DNS 주소에 대한 매핑 정보를 검증하고, 최초 환경과 통신 흐름을 비교해보자.
- `dig +short cloudformation.ap-northeast-2.amazonaws.com`
- `dig +short vpce-093517d1686ace06d-txsku1pk.cloudformation.ap-northeast-2.vpce.amazonaws.com`
- 퍼블릭 EC2 인스턴스 터미널

```
aws | 서비스 | Q 서비스, 기능, 블로그, 설명서 등을 검색합니다. [Alt+S]
Last login: Sat Jul 23 13:47:17 2022 from ec2-13-209-1-60.ap-northeast-2.compute.amazonaws.com

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

https://aws.amazon.com/amazon-linux-2/
12 package(s) needed for security, out of 22 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-0-29 ~]$ dig +short cloudformation.ap-northeast-2.amazonaws.com
10.0.0.108
10.0.1.47
[ec2-user@ip-10-0-0-29 ~]$ dig +short vpce-093517d1686ace06d-txsku1pk.cloudforamtion.ap-northeast-2.amazonaws.com
[ec2-user@ip-10-0-0-29 ~]$ dig +short vpce-093517d1686ace06d-txsku1pk.cloudforamtion.ap-northeast-2.vpce.amazonaws.com
[ec2-user@ip-10-0-0-29 ~]$ dig +short vpce-093517d1686ace06d-txsku1pk-ap-northeast-2c.cloudformation.ap-northeast-2.vpce.amazonaws.com
10.0.0.108
10.0.1.47
[ec2-user@ip-10-0-0-29 ~]$ dig +short vpce-093517d1686ace06d-txsku1pk.cloudformation.ap-northeast-2.vpce.amazonaws.com
10.0.0.108
10.0.1.47
[ec2-user@ip-10-0-0-29 ~]$
```


2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 인터페이스 엔드포인트 생성 및 검증

■ 인터페이스 엔드포인트 검증

- CloudFormation 서비스 연결을 위한 인터페이스 엔드포인트를 생성하였다.
- 실제 EC2 인스턴스에 접속하여 CloudFormation의 DNS 주소에 대한 매핑 정보를 검증하고, 최초 환경과 통신 흐름을 비교해보자.
- `dig +short cloudformation.ap-northeast-2.amazonaws.com`
- `dig +short vpce-093517d1686ace06d-txsku1pk.cloudformation.ap-northeast-2.vpce.amazonaws.com`
- 프라이빗 EC2 인스턴스 터미널

```
[ec2-user@ip-10-0-0-29 ~]$ ssh root@10.0.1.29
root@10.0.1.29's password:
Last login: Sat Jul 23 13:52:47 2022 from 10.0.0.29

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

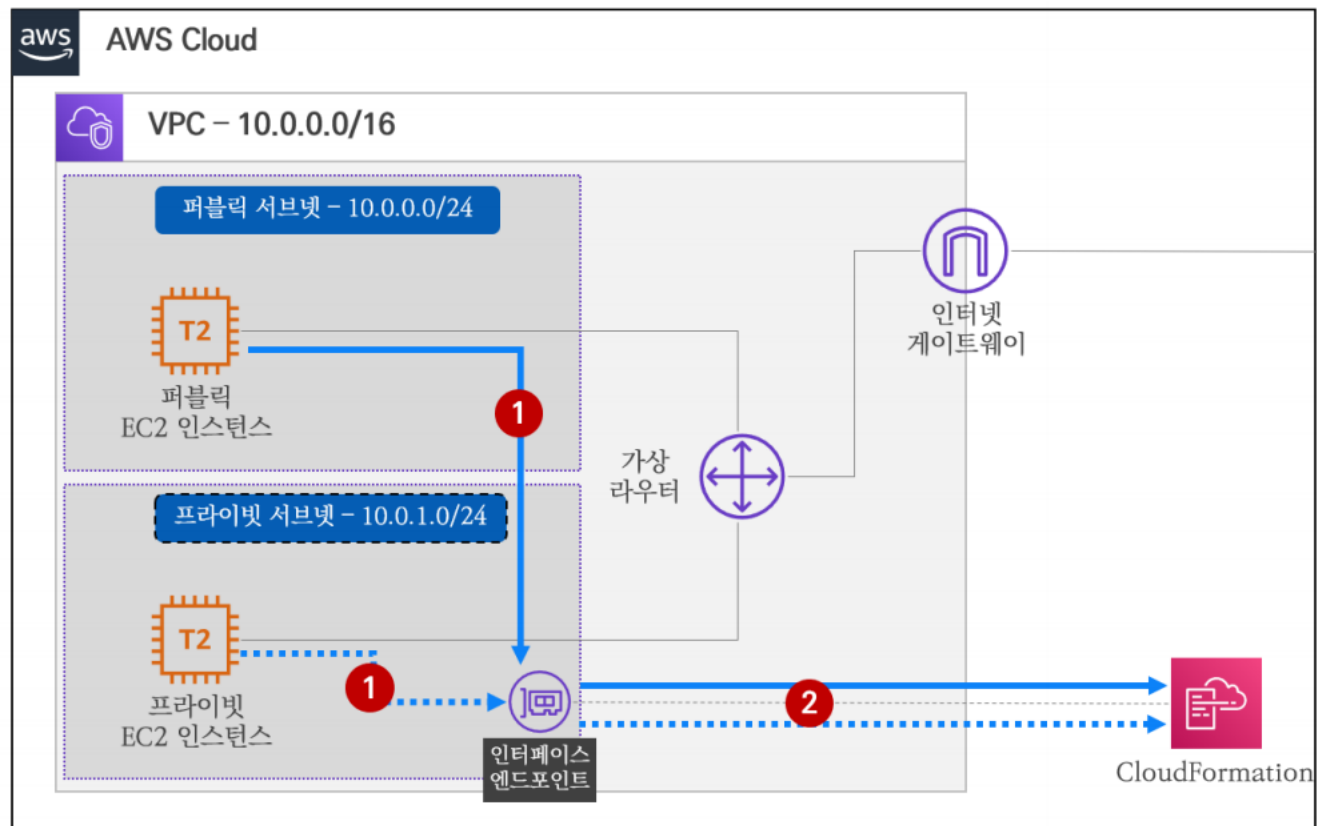
https://aws.amazon.com/amazon-linux-2/
13 package(s) needed for security, out of 23 available
Run "sudo yum update" to apply all updates.
[root@ip-10-0-1-29 ~]# dig +short cloudformation.ap-northeast-2.amazonaws.com
10.0.0.108
10.0.1.47
[root@ip-10-0-1-29 ~]# dig +short vpce-09351d168ace06d-txsku1pk.cloudformation.ap-northeast-2.vpce.amazonaws.com
[root@ip-10-0-1-29 ~]# dig +short vpce-09351d1686ace06d-txsku1pk.cloudformation.ap-northeast-2.vpce.amazonaws.com
[root@ip-10-0-1-29 ~]# dig +short vpce-093517d1686ace06d-txsku1pk.cloudformation.ap-northeast-2.vpce.amazonaws.com
10.0.1.47
10.0.0.108
[root@ip-10-0-1-29 ~]#
```

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 인터페이스 엔드포인트 생성 및 검증

■ 인터페이스 엔드포인트 검증

- 인터페이스 엔드포인트 생성 후 CloudFormation과 통신 흐름



2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 자원 삭제

■ 엔드포인트 삭제

- VPC > 엔드포인트 > 작업 > 엔드포인트 삭제

▼ Virtual Private Cloud

VPC

서브넷

라우팅 테이블

인터넷 게이트웨이

송신 전용 인터넷 게이트웨이

캐리어 게이트웨이

DHCP 옵션 세트

탄력적 IP

관리형 접두사 목록

엔드포인트

엔드포인트 (1/2) 정보

Q 엔드포인트 필터링

	Name	VPC 엔드포인트 ID	VPC ID	서비스 이름
<input type="checkbox"/>	-	vpce-0ee6a8ee6dfbe3218	vpc-07de255d3a7c9c317 CloudNeta...	com.amazonaws.ap-no
<input checked="" type="checkbox"/>	-	vpce-093517d1686ace06d	vpc-07de255d3a7c9c317 CloudNeta...	com.amazonaws.ap-no

작업 ▲ 엔드포인트 생성

- 세부 정보 보기
- 서브넷 관리
- 보안 그룹 관리
- 라우팅 테이블 관리
- 정책 관리
- 프라이빗 DNS 이름 수정
- 엔드포인트 설정 수정
- 태그 관리
- VPC 엔드포인트 삭제

엔드포인트 삭제

이(가) 삭제됩니다

다음 엔드포인트는 영구적으로 삭제되며 나중에 복구할 수 없습니다.

이름	VPC 엔드포인트 ID	서비스 이름
-	vpce-093517d1686ace06d	com.amazonaws.ap-northeast-2.cloudformation

삭제를 확인하려면 필드에 삭제를 입력하십시오.

삭제

취소

삭제

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 자원 삭제

■ 엔드포인트 삭제

- VPC > 엔드포인트 > 작업 > 엔드포인트 삭제

엔드포인트 (1/1) 정보

Q 엔드포인트 필터링

<input checked="" type="checkbox"/>	Name	VPC 엔드포인트 ID	VPC ID	서비스 이름
<input checked="" type="checkbox"/>	-	vpce-0ee6a8ee6dfbe3218	vpc-07de255d3a7c9c317 CloudNeta...	com.amazonaws.ap-northeast-2.s3

작업 ▲

- 세부 정보 보기
- 서브넷 관리
- 보안 그룹 관리
- 라우팅 테이블 관리
- 정책 관리
- 프라이빗 DNS 이름 수정
- 엔드포인트 설정 수정
- 태그 관리
- VPC 엔드포인트 삭제

엔드포인트 삭제

이(가) 삭제됩니다

다음 엔드포인트는 영구적으로 삭제되며 나중에 복구할 수 없습니다.

이름	VPC 엔드포인트 ID	서비스 이름
-	vpce-0ee6a8ee6dfbe3218	com.amazonaws.ap-northeast-2.s3

삭제를 확인하려면 필드에 삭제를 입력하십시오.

삭제

취소

삭제

2. 실습 1. 게이트웨이/인터페이스 엔드포인트 비교

■ 자원 삭제

■ CloudFormation 스택 삭제

- CloudFormation > 스택 > 삭제

CloudFormation > 스택

스택 (1)

🔄 삭제 업데이트 스택 작업 ▼ 스택 생성 ▼

🔍 스택 이름으로 필터링

🔵 뷰 중첩됨

활성 ▼

< 1 > ⚙️

스택 이름	상태	생성 시간	설명
CloudNeta-Lab9-1	✔️ CREATE_COMPLETE	2022-07-23 21:46:37 UTC+0900	-

CloudNeta-Lab9-1을(를) 삭제하시겠습니까?



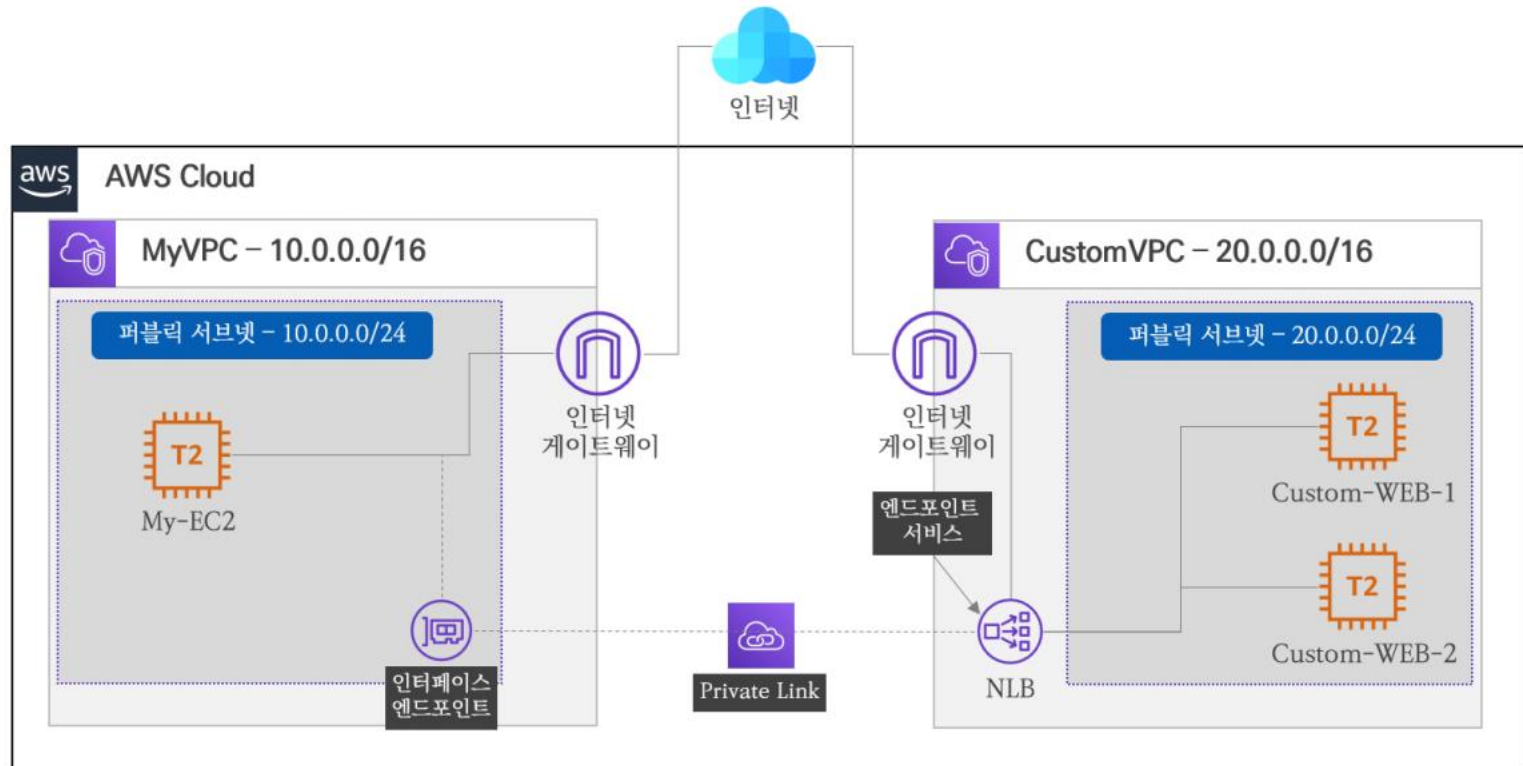
이 스택을 삭제하면 모든 스택 리소스가 삭제됩니다. 리소스는 해당하는 DeletionPolicy에 따라 삭제됩니다. [자세히 알아보기](#)

취소

스택 삭제

3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

- 엔드포인트 서비스 기능을 활용하여, 시용자가 생성한 VPC 와 프라이빗 연결을 확인하고 통신되는 과정을 살펴보자
- 이 실습을 완료하면 다음과 같은 토폴로지가 생성된다.



3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

■ 기본 환경 구성

■ CloudFormation 적용

- 본 실습을 위한 기본 실습 환경을 CloudFormation을 통해 자동으로 구성한다.
- 다운로드 링크 : <https://github.com/jjin300/cloud>
- CloudFormation 적용을 위해 상단의 링크를 통해 lab09-2.yaml을 다운로드하고 스택 생성을 한다.

스택 생성

사전 조건 - 템플릿 준비

템플릿 준비
모든 스택은 템플릿을 기반으로 합니다. 템플릿은 JSON 또는 YAML 텍스트 파일로, 스택에 포함하려는 AWS 리소스에 대한 구성 정보가 들어 있습니다.

☒ 준비된 템플릿 ☐ 샘플 템플릿 사용 ☐ Designer에서 템플릿 생성

템플릿 지정

템플릿은 스택의 리소스와 속성을 설명하는 JSON 또는 YAML 파일입니다.

템플릿 소스
템플릿을 선택하면 템플릿이 저장될 Amazon S3 URL이 생성됩니다.

☐ Amazon S3 URL ☒ 템플릿 파일 업로드

템플릿 파일 업로드

파일 선택  lab09-2.yaml

JSON 또는 YAML 형식 파일

S3 URL: <https://s3.ap-northeast-2.amazonaws.com/cf-templates-wala0sr1keps-ap-northeast-2/2022204Kgn-lab09-2.yaml> [Designer에서 보기](#)

취소 다음

3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

■ 기본 환경 구성

■ CloudFormation 적용

- 본 실습을 위한 기본 실습 환경을 CloudFormation을 통해 자동으로 구성한다.
- 다운로드 링크 : <https://github.com/jjin300/cloud>
- CloudFormation 적용을 위해 상단의 링크를 통해 lab09-2.yaml을 다운로드하고 스택 생성을 한다.

스택 세부 정보 지정

스택 이름

스택 이름

lab9-2

스택 이름은 문자(A-Z 및 a-z), 숫자(0-9) 및 대시(-)를 포함할 수 있습니다.

파라미터

파라미터는 템플릿에서 정의되며, 이를 통해 스택을 생성하거나 업데이트할 때 사용자 지정 값을 입력할 수 있습니다.

KeyName

Name of an existing EC2 KeyPair to enable SSH access to the instances. Linked to AWS Parameter

aws_study_key

LatestAmild

(DO NOT CHANGE)

/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2

취소

이전

다음

3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

■ 기본 환경 구성

■ 생성 자원 확인

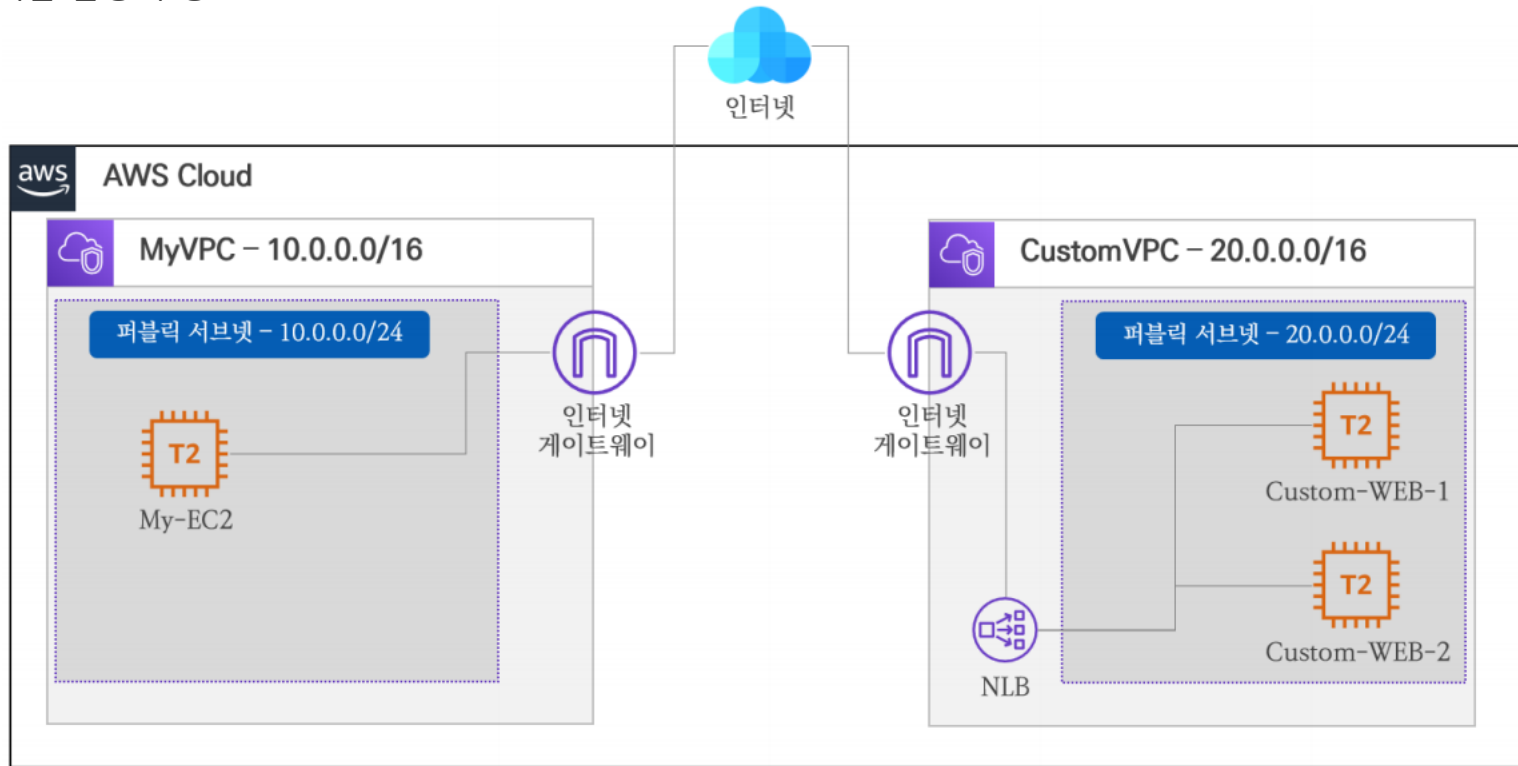
- 기본 환경 구성 자원 정보

자원	태그 이름	정보
VPC	MyVPC	IP CIDR: 10.0.0.0/16
	CustomVPC	IP CIDR: 200.0.0/16
퍼블릭 서브넷	My-Public-SN	IP CIDR: 10.0.0.0/24, AZ: ap-northeast-2a
	Custom-Public-SN	IP CIDR: 20.0.0.0/24, AZ: ap-northeast-2a
퍼블릭 라우팅 테이블	My-Public-RT	연결: My-Public-SN
	Custom-Public-RT	연결: Custom-Public-SN
인터넷 게이트웨이	My-IGW	연결: My-VPC
	Custom-IGW	연결: Custom-VPC
퍼블릭 EC2 인스턴스	My-EC2	연결: My-Public-SN, 퍼블릭 IP 할당: 활성화
	CIIslo I1I-WEB-1	연결: Custom-Public-SN, 퍼블릭 IP 할당: 활성화
	CIIslo m-WEB-2	연결: Custom-Public-SN, 퍼블릭 IP 할당: 활성화
네트워크 로드밸런서(NLB)	Custom-NLB	타겟 그룹: Custom-WEB-1, Custom-WEB-2

3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

■ 기본 환경 구성

- 생성 자원 확인
 - 기본 환경 구성



3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

■ 기본 환경 구성

■ 기본 환경 검증

- MyVPC에 존재하는 EC2 인스턴스에서 CustomVPC에 존재하는 웹 서버 인스턴스로 통신을 확인하고 통신 흐름에 대해 살펴보자.
- CloudFormation을 통해 생성된 자원 중 NLB는 정상적인 서비스까지 약간의 대기 시간이 필요하다.
- 정상적인 상태를 확인 후 검증을 진행한다.
- 서비스 > EC2 > 로드밸런싱 > 대상 그룹 > 대상 그룹 선택

▼ 네트워크 및 보안

보안 그룹

탄력적 IP

배치 그룹

키 페어

네트워크 인터페이스

▼ 로드 밸런싱

로드밸런서

대상 그룹 New

The image displays two screenshots from the AWS Management Console. The top screenshot shows the 'Target groups (1/1)' page with a table listing one target group: 'Custom-NLB-TG'. The bottom screenshot shows the 'Registered targets (2)' page for the 'Custom-NLB-TG' target group, with a table listing two EC2 instances, both of which are 'healthy'.

Target groups (1/1)

<input checked="" type="checkbox"/>	Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
<input checked="" type="checkbox"/>	Custom-NLB-TG	arn:aws:elasticloadbalancing...	80	TCP	Instance	lab9-Custo-1C1O2OWX9WGL9	vpc-03884a93

Target group: Custom-NLB-TG

Details | **Targets** | Monitoring | Health checks | Attributes | Tags

Registered targets (2)

<input type="checkbox"/>	Instance ID	Name	Port	Zone	Health status	Health status details
<input type="checkbox"/>	i-0060f59f5c3b14a40	Custom-WEB-1	80	ap-northeast-2a	healthy	
<input type="checkbox"/>	i-08ce439b83a2f51ef	Custom-WEB-2	80	ap-northeast-2a	healthy	

3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

■ 기본 환경 구성

■ 기본 환경 검증

- 먼저 실습을 위해 Custom-NLB의 DNS 주소를 확인한다.
- 서비스 > EC2 > 로드밸런싱 > 로드밸런서

▼ 네트워크 및 보안

보안 그룹

탄력적 IP

배치 그룹

키 페어

네트워크 인터페이스

▼ 로드 밸런싱

로드밸런서

대상 그룹 New

로드 밸런서 생성

작업 ▼

태그 및 속성별 필터 또는 키워드별 검색

<input type="checkbox"/>	이름	DNS 이름	상태	VPC ID	가용 영역	유형
<input checked="" type="checkbox"/>	lab9-Custo-1C1O2OWX9W...	lab9-Custo-1C1O2OWX9W...	활성	vpc-03884a93119c91cd3	ap-northeast-2a	network

로드 밸런서: lab9-Custo-1C1O2OWX9WGL9

설명

리스너

모니터링

통합 서비스

태그

기본 구성

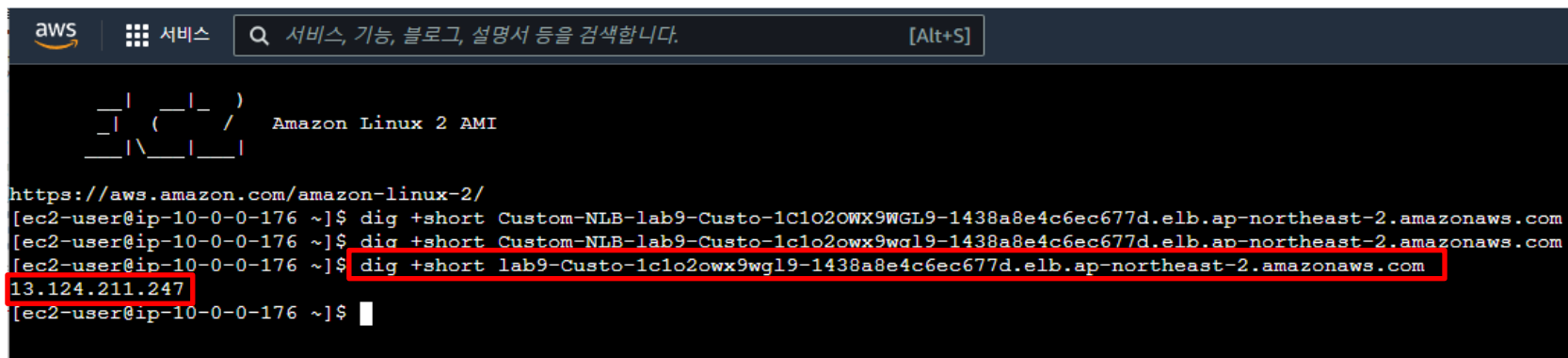
이름	lab9-Custo-1C1O2OWX9WGL9
ARN	arn:aws:elasticloadbalancing:ap-northeast-2::loadbalancer/net/lab9-Custo-1C1O2OWX9WGL9/1438a8e4c6ec677d
DNS 이름	lab9-Custo-1C1O2OWX9WGL9-1438a8e4c6ec677d.elb.ap-northeast-2.amazonaws.com
상태	활성
유형	network
체계	internet-facing

3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

■ 기본 환경 구성

■ 기본 환경 검증

- Custom-NLB의 DNS 이름을 복사하고 [My-EC2] EC2 인스턴스 터미널에서 IP 주소 확인
- `dig +short lab9-Custo-1C1O2OWX9WGL9-1438a8e4c6ec677d.elb.ap-northeast-2.amazonaws.com`



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

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-0-176 ~]$ dig +short Custom-NLB-lab9-Custo-1C1O2OWX9WGL9-1438a8e4c6ec677d.elb.ap-northeast-2.amazonaws.com
[ec2-user@ip-10-0-0-176 ~]$ dig +short Custom-NLB-lab9-Custo-1c1o2owx9wgl9-1438a8e4c6ec677d.elb.ap-northeast-2.amazonaws.com
[ec2-user@ip-10-0-0-176 ~]$ dig +short lab9-Custo-1c1o2owx9wgl9-1438a8e4c6ec677d.elb.ap-northeast-2.amazonaws.com
13.124.211.247
[ec2-user@ip-10-0-0-176 ~]$
```

3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

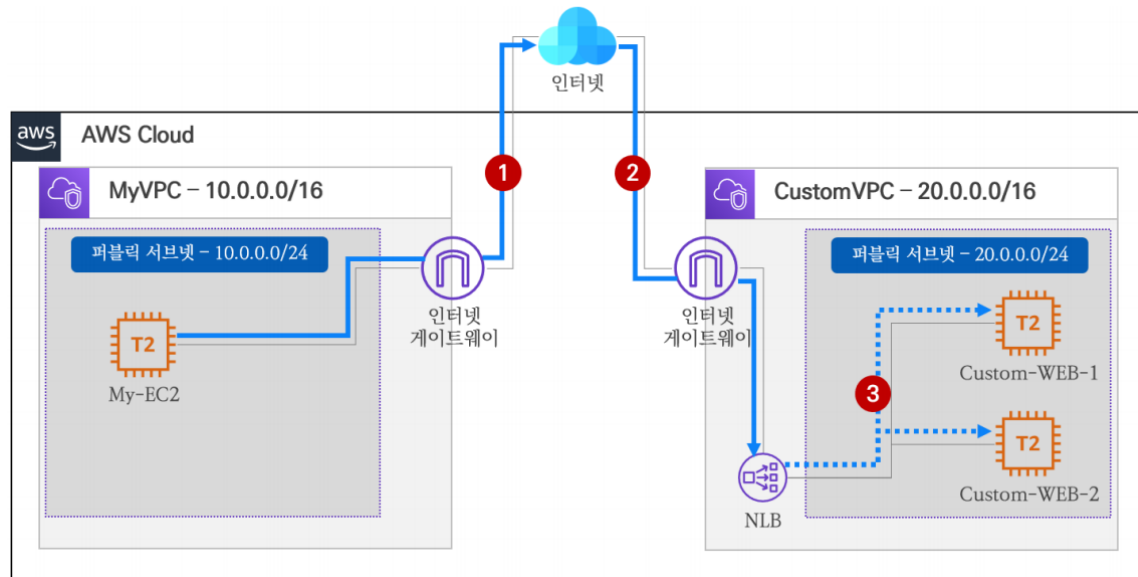
■ 기본 환경 구성

■ 기본 환경 검증

- curl 이라는 명령어를 통해 해당 웹 서버의 HTML 코드를 출력하며, 정상적인 웹 접근을 확인해 볼 수 있다.
- curl lab9-Custo-1C1O2OWX9WGL9-1438a8e4c6ec677d.elb.ap-northeast-2.amazonaws.com

```
[ec2-user@ip-10-0-0-176 ~]$ curl lab9-Custo-1c1o2owx9wql9-1438a8e4c6ec677d.elb.ap-northeast-2.amazonaws.com
<html><h1>Endpoint Service Lab - CloudNeta Web Server 1</h1></html>
[ec2-user@ip-10-0-0-176 ~]$
```

- 기본 환경에서 통신 흐름 (NLB를 통한 로드 밸런싱)



3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

■ 엔드포인트 서비스 생성 및 연결

■ 엔드포인트 서비스 생성

- 우선 엔드포인트 서비스를 생성하여 VPC 간 프라이빗 링크 연결을 위한 환경을 구성해야 한다.
- 엔드포인트 서비스 생성 시 CustomVPC에 존재하는 NLB를 연결해야 한다.
- 서비스 > VPC > Virtual Private Cloud > 엔드포인트 서비스

▼ Virtual Private Cloud

VPC

서브넷

라우팅 테이블

인터넷 게이트웨이

송신 전용 인터넷 게이트웨이

캐리어 게이트웨이

DHCP 옵션 세트

탄력적 IP

관리형 접두사 목록

엔드포인트

엔드포인트 서비스

NAT 게이트웨이

피어링 연결

🔄

작업 ▼

엔드포인트 서비스 생성

< 1 > ⚙️

▼	유형	▼	서비스 이름	▼	상태	▼	가용 영역	▼	수락
엔드포인트 서비스를 찾을 수 없음									

3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

■ 엔드포인트 서비스 생성 및 연결

■ 엔드포인트 서비스 생성

- 엔드포인트 서비스 생성 (NLB 선택)

VPC > 엔드포인트 서비스 > 엔드포인트 서비스 생성

엔드포인트 서비스 생성 정보

엔드포인트 서비스 설정

이름 - 선택 사항
"Name" 키와 사용자가 지정하는 값을 포함하는 태그를 생성합니다.

Custom-EPS

로드 밸런서 유형

☒ 네트워크
☐ 게이트웨이

사용 가능한 로드 밸런서 (1/1)

새 로드 밸런서 생성

서비스 소비자에서 애플리케이션 또는 서비스로 트래픽을 전송할 로드 밸런서를 선택합니다.

로드 밸런서 필터링

<input checked="" type="checkbox"/>	로드 밸런서 이름	가용 영역
<input checked="" type="checkbox"/>	lab9-Custo-1C1O2OWX9WGL9	ap-northeast-2a

3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

■ 엔드포인트 서비스 생성 및 연결

■ 엔드포인트 서비스 생성

- 엔드포인트 서비스 생성 (NLB 선택)

추가 설정

엔드포인트 수락 필수 정보

엔드포인트를 통한 서비스 소비자의 요청을 수락해야 하는지 여부를 지정합니다.

☒ 수락 필수

프라이빗 DNS 이름 활성화

이 옵션을 사용하면 엔드포인트 사용자가 지정된 프라이빗 DNS 이름을 사용하여 VPC에서 서비스에 액세스할 수 있습니다.

☐ 프라이빗 DNS 이름을 서비스에 연결

지원되는 IP 주소 유형

☐ IPv4

☐ IPv6

태그

태그는 AWS 리소스에 할당하는 레이블입니다. 각 태그는 키와 선택적 값으로 구성됩니다. 태그를 사용하여 리소스를 검색 및 필터링하거나 AWS 비용을 추적할 수 있습니다.

키

값 - 선택 사항

Q Name



Q Custom-EPS



제거

새 태그 추가

49을(를) 태그 개 더 추가할 수 있습니다.

취소

생성

3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

■ 엔드포인트 서비스 생성 및 연결

■ 엔드포인트 서비스 생성

- 엔드포인트 서비스 생성 확인
- 서비스 이름을 복사

엔드포인트 서비스 (1/1) 정보								엔드포인트 서비스 생성
Q 엔드포인트 서비스 필터링								< 1 > ⚙
<input checked="" type="checkbox"/>	Name ▾	서비스 ID ▾	유형 ▾	서비스 이름 ▾	상태 ▾	가용 영역 ▾	수	
<input checked="" type="checkbox"/>	Custom-EPS	vpce-svc-0f0f83cb8f81a64b0	Interface	com.amazonaws.vpce.ap-northeast-2...	✔ Available	ap-northeast-2a (a...	예	

vpce-svc-0f0f83cb8f81a64b0 / Custom-EPS

세부 정보

로드 밸런서

보안 주체 허용

엔드포인트 연결

알림

모니터링

태그

세부 정보

서비스 ID

vpce-svc-0f0f83cb8f81a64b0

Network Load Balancer ARNS

유형

Interface

Gateway Load Balancers ARNS

서비스 이름

com.amazonaws.vpce.ap-northeast-2.vpce-svc-0f0f83cb8f81a64b0

상태

Available

수락 필수

3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

■ 엔드포인트 서비스 생성 및 연결

■ 인터페이스 엔드포인트 생성 및 연결

- 엔드포인트 생성 (상단 설정)

VPC > 엔드포인트 > 엔드포인트 생성

엔드포인트 생성 정보

VPC 엔드포인트에는 인터페이스 엔드포인트, 게이트웨이 로드 밸런서 엔드포인트 및 게이트웨이 엔드포인트의 세 가지 유형이 있습니다. 인터페이스 엔드포인트와 게이트웨이 로드 밸런서 엔드포인트는 AWS PrivateLink에 의해 구축하며 ENI(탄력적 네트워크 인터페이스)를 서비스로 가는 트래픽의 진입점으로 사용합니다. 인터페이스 엔드포인트는 일반적으로 이러한 서비스에 연결된 퍼블릭 및 프라이빗 DNS 이름을 사용하여 액세스하며 게이트웨이 엔드포인트와 게이트웨이 로드 밸런서 엔드포인트는 서비스로 향하는 트래픽에 대한 라우팅 테이블의 경로에 대한 대상으로 사용됩니다.

엔드포인트 설정

이름 태그 - 선택 사항
'Name' 키와 귀하가 지정하는 값을 포함하는 태그를 생성합니다.

서비스 범주
서비스 범주 선택

☐ AWS 서비스
Amazon에서 제공하는 서비스

☐ PrivateLink Ready 파트너 서비스
AWS Service Ready 지정된 서비스

☐ AWS Marketplace 서비스
AWS Marketplace를 통해 구매한 서비스

☒ 다른 엔드포인트 서비스
서비스 이름별로 공유된 서비스 찾기

서비스 설정

서비스 이름

✓ 서비스 이름이 확인되었습니다.

3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

■ 엔드포인트 서비스 생성 및 연결

■ 인터페이스 엔드포인트 생성 및 연결

- 엔드포인트 생성 (하단 설정)

VPC

엔드포인트를 생성할 VPC를 선택

VPC
엔드포인트를 생성할 VPC입니다.

vpc-0e773e2b6de265f4f (MyVPC)

▶ 추가 설정

서브넷 (1/1) 정보

☒ 가용 영역

서브넷 ID

☒ ap-northeast-2a (apne2-az1)

subnet-091bfb956e278230a

subnet-091bfb956e278230a X
My-Public-SN

IP 주소 유형

☐ IPv4

☒ IPv6

☐ 듀얼 스택

보안 그룹 (1/2) 정보

Q 보안 그룹 필터링 < 1 > ⚙

<input type="checkbox"/>	그룹 ID	그룹 이름	VPC ID
<input type="checkbox"/>	sg-0cb369eeddfcb88e	default	vpc-0e773e2b6de26
<input checked="" type="checkbox"/>	sg-0f9ea707e9209b642	WebSG	vpc-0e773e2b6de2

sg-0f9ea707e9209b642 X

3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

■ 엔드포인트 서비스 생성 및 연결

- 인터페이스 엔드포인트 생성 및 연결
 - 엔드포인트 생성 확인 (수락 대기 중 상태)

엔드포인트 (1/1) [정보](#)

🔍 엔드포인트 필터링

VPC 엔드포인트 ID: vpce-0b40409379c428dd5 ✕ [필터 지우기](#)

<input checked="" type="checkbox"/>	Name	VPC 엔드포인트 ID	VPC ID	서비스 이름	엔드포인트 유형
<input checked="" type="checkbox"/>	-	vpce-0b40409379c428dd5	vpc-0e773e2b6de265f4f MyVPC	com.amazonaws.vpce.ap-northeast-2.vpce-svc-0f0f83c...	Interface

vpce-0b40409379c428dd5

[세부 정보](#) | [서브넷](#) | [보안 그룹](#) | [알림](#) | [태그](#)

세부 정보

엔드포인트 ID

vpce-0b40409379c428dd5

VPC ID

vpc-0e773e2b6de265f4f (MyVPC)

DNS 레코드 IP 유형

ipv4

상태

pendingAcceptance

상태 메시지

-

IP 주소 유형

ipv4

생성 시간

2022년 7월 24일 일요일 01시 0분 56초 GMT+9

서비스 이름

com.amazonaws.vpce.ap-northeast-2.vpce-svc-0f0f83cb8f81a64b0

DNS 이름

vpce-0b40409379c428dd5-

엔드포인트 유형

Interface

프라이빗 DNS 이름 활성화됨

아니요

3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

■ 엔드포인트 서비스 생성 및 연결

■ 인터페이스 엔드포인트 생성 및 연결

- 엔드포인트 서비스에서 엔드포인트 연결 요청 수락

▼ Virtual Private Cloud

VPC

서브넷

라우팅 테이블

인터넷 게이트웨이

송신 전용 인터넷 게이트웨이

캐리어 게이트웨이

DHCP 옵션 세트

탄력적 IP

관리형 접두사 목록

엔드포인트

엔드포인트 서비스

NAT 게이트웨이

피어링 연결

엔드포인트 서비스 (1/1) 정보

<input checked="" type="checkbox"/>	Name	서비스 ID	유형	서비스 이름	상태	가용 영역	수락
<input checked="" type="checkbox"/>	Custom-EPs	vpce-svc-0f0f83cb8f81a64b0	Interface	com.amazonaws.vpce.ap-northeast-2...	Available	ap-northeast-2a (a...	예

vpce-svc-0f0f83cb8f81a64b0 / Custom-EPs

세부 정보	로드 밸런서	보안 주체 허용	엔드포인트 연결	알림	모니터링	태그
-------	--------	----------	----------	----	------	----

엔드포인트 연결 (1/1) 정보

엔드포인트 ID	소유자	상태	생성됨
vpce-0b40409379c428dd5	262663767358	Pending acceptance	2022년 7월 24일 일요일 01시 0분 56초 GMT+9

3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

■ 엔드포인트 서비스 생성 및 연결

■ 인터페이스 엔드포인트 생성 및 연결

- 엔드포인트 서비스에서 엔드포인트 연결 요청 수락

엔드포인트 연결 요청 수락

×

이 엔드포인트 연결 요청을 수락하시겠습니까?

요약			
엔드포인트 ID vpce-0b40409379c428dd5	엔드포인트 서비스 ID vpce-svc-0f0f83cb8f81a64b0	엔드포인트 서비스 이름 태그 Custom-EPS	엔드포인트 서비스 이름 com.amazonaws.vpce.ap-northeast-2.vpce-svc-0f0f83cb8f81a64b0

수락을 확인하려면 필드에 수락 입력:

수락

취소

수락

3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

■ 엔드포인트 서비스 생성 및 연결

■ 인터페이스 엔드포인트 생성 및 연결

- 엔드포인트 서비스에서 엔드포인트 연결 요청 수락

vpce-svc-0f0f83cb8f81a64b0 / Custom-EPS

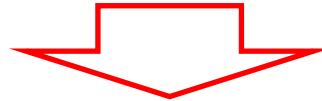
세부 정보 | 로드 밸런서 | 보안 주체 허용 | **엔드포인트 연결** | 알림 | 모니터링 | 태그

엔드포인트 연결 (1/1) 정보

Q 엔드포인트 연결을 기준으로 필터링

🔄 작업 ▼ VPC 엔드포인트 연결 생성

엔드포인트 ID	소유자	상태	생성됨
vpce-0b40409379c428dd5	262663767358	Pending	2022년 7월 24일 일요일 01시 0분 56초 GMT+9



vpce-svc-0f0f83cb8f81a64b0 / Custom-EPS

세부 정보 | 로드 밸런서 | 보안 주체 허용 | **엔드포인트 연결** | 알림 | 모니터링 | 태그

엔드포인트 연결 (1/1) 정보

Q 엔드포인트 연결을 기준으로 필터링

🔄 작업 ▼ VPC 엔드포인트 연결 생성

엔드포인트 ID	소유자	상태	생성됨
vpce-0b40409379c428dd5	262663767358	Available	2022년 7월 24일 일요일 01시 0분 56초 GMT+9

3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

■ 엔드포인트 서비스 검증

- MyVPC의 EC2 인스턴스에서 통신을 확인한다.
- 확인에 앞서 엔드포인트 DNS 이름을 알이 두어야 한다.

엔드포인트 (1/1) 정보

Q 엔드포인트 필터링

1

작업

엔드포인트 생성

Name	VPC 엔드포인트 ID	VPC ID	서비스 이름	엔드포인트 유형
-	vpce-0b40409379c428dd5	vpce-0e773e2b6de265f4f MyVPC	com.amazonaws.vpce.ap-northeast-2.vpce-svc-0f0f83c...	Interface

세부 정보

서브넷

보안 그룹

알림

모니터링

태그

세부 정보

엔드포인트 ID

vpce-0b40409379c428dd5

VPC ID

vpce-0e773e2b6de265f4f (MyVPC)

DNS 레코드 IP 유형

ipv4

상태

사용 가능

상태 메시지

-

IP 주소 유형

ipv4

생성 시간

2022년 7월 24일 일요일 01시 0분 56초 GMT+9

서비스 이름

com.amazonaws.vpce.ap-northeast-2.vpce-svc-0f0f83cb8f81a64b0

DNS 이름

vpce-0b40409379c428dd5-hxrsc9c7.vpce-svc-0f0f83cb8f81a64b0.ap-northeast-2.vpce.amazonaws.com - (Z27UANNT0PRK1T)

엔드포인트 유형

Interface

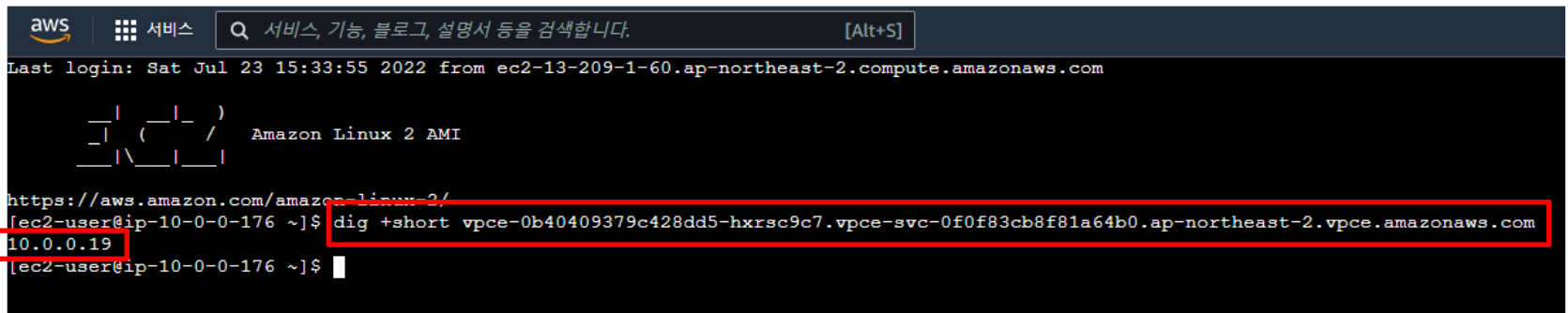
프라이빗 DNS 이름 활성화됨

아니요

3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

■ 엔드포인트 서비스 검증

- DNS 이름을 복사하고 [My-EC2] EC2 인스턴스 터미널에서 IP 주소 확인
 - `dig +short vpce-0b40409379c428dd5-hxrsc9c7.vpce-svc-0f0f83cb8f81a64b0.ap-northeast-2.vpce.amazonaws.com`



The screenshot shows an AWS EC2 terminal window. At the top, there's an AWS logo and a search bar. Below that, the terminal displays the last login information: "Last login: Sat Jul 23 15:33:55 2022 from ec2-13-209-1-60.ap-northeast-2.compute.amazonaws.com". The terminal then shows the Amazon Linux 2 AMI logo. Below the logo, the terminal displays the command: `dig +short vpce-0b40409379c428dd5-hxrsc9c7.vpce-svc-0f0f83cb8f81a64b0.ap-northeast-2.vpce.amazonaws.com`. The output of the command is `10.0.0.19`, which is highlighted with a red box. The terminal prompt is `[ec2-user@ip-10-0-0-176 ~]$`.

IT COOKBOOK

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

```
Last login: Sat Jul 23 15:33:55 2022 from ec2-13-209-1-60.ap-northeast-2.compute.amazonaws.com
```

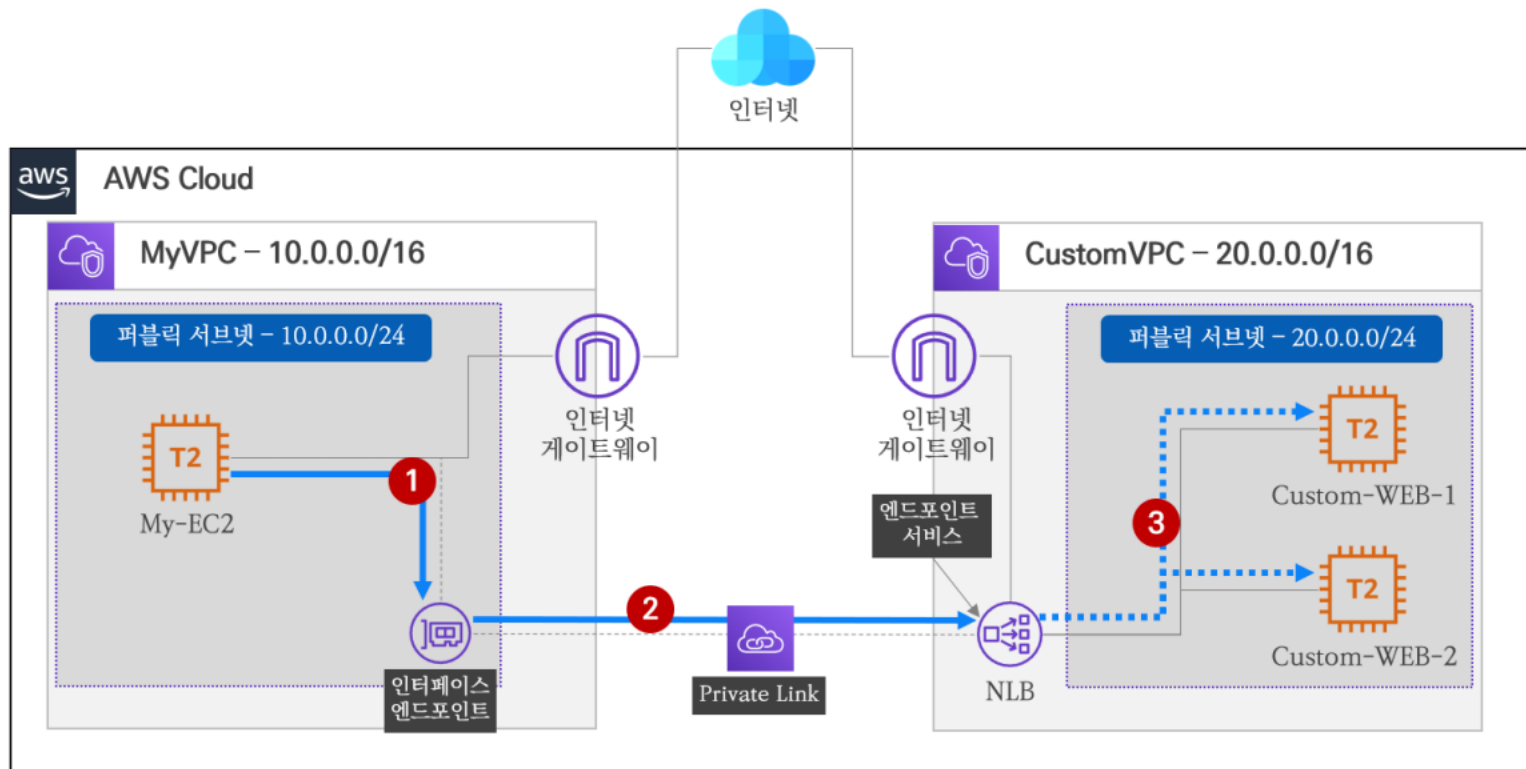
```
 _ | _ | )  
 _ | ( _ | /  Amazon Linux 2 AMI  
 _ | \ _ | _ |
```

```
https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-10-0-0-176 ~]$ dig +short vpce-0b40409379c428dd5-hxrsc9c7.vpce-svc-0f0f83cb8f81a64b0.ap-northeast-2.vpce.amazonaws.com  
10.0.0.19  
[ec2-user@ip-10-0-0-176 ~]$ curl vpce-0b40409379c428dd5-hxrsc9c7.vpce-svc-0f0f83cb8f81a64b0.ap-northeast-2.vpce.amazonaws.com  
<html><h1>Endpoint Service Lab - CloudNeta Web Server 1</h1></html>  
[ec2-user@ip-10-0-0-176 ~]$
```

3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

■ 엔드포인트 서비스 검증

- DNS 이름을 복사하고 [My-EC2] EC2 인스턴스 터미널에서 IP 주소 확인
 - VPC 엔드포인트를 통한 프라이빗 링크 통신 흐름



3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

■ 자원 삭제

- 엔드포인트 삭제
- VPC > 엔드포인트 > 작업 > 엔드포인트 삭제

엔드포인트 (1/1) 정보

Q 엔드포인트 필터링

<input checked="" type="checkbox"/>	Name	VPC 엔드포인트 ID	VPC ID	서비스 이름
<input checked="" type="checkbox"/>	-	vpce-0b40409379c428dd5	vpce-0e773e2b6de265f4f MyVPC	com.amazonaws.vpce.ap-northeast-2.vp

작업 ▲

- 세부 정보 보기
- 서브넷 관리
- 보안 그룹 관리
- 라우팅 테이블 관리
- 정책 관리
- 프라이빗 DNS 이름 수정
- 엔드포인트 설정 수정
- 태그 관리
- VPC 엔드포인트 삭제

엔드포인트 삭제

이(가) 삭제됩니다

다음 엔드포인트는 영구적으로 삭제되며 나중에 복구할 수 없습니다.

이름	VPC 엔드포인트 ID	서비스 이름
-	vpce-0b40409379c428dd5	com.amazonaws.vpce.ap-northeast-2.vpce-svc-0f0f83cb8f81a64b0

삭제를 확인하려면 필드에 삭제를 입력하십시오.

삭제

취소

삭제

3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

■ 자원 삭제

- 엔드포인트 서비스 삭제
- VPC > 엔드포인트 서비스 > 작업 > 엔드포인트 서비스 삭제

엔드포인트 서비스 (1/1) 정보

Q 엔드포인트 서비스 필터링

<input checked="" type="checkbox"/>	Name	서비스 ID	유형	서비스 이름
<input checked="" type="checkbox"/>	Custom-EPS	vpce-svc-0f0f83cb8f81a64b0	Interface	com.amazonaws.vpce.ap-northeast-2a...

작업 ▲

세부 정보 보기
보안 주체 허용
로드 밸런서 연결 또는 연결 해제
엔드포인트 수정 수락 설정
프라이빗 DNS 이름 수정
프라이빗 DNS 이름에 대한 도메인 소유권 확인
지원되는 IP 주소 유형 수정
태그 관리
엔드포인트 서비스 삭제

엔드포인트 서비스 생성

< 1 > ⚙

가용 영역 ▼ 수락

ap-northeast-2a (a... 예

엔드포인트 서비스 삭제

다음 엔드포인트 서비스는 영구적으로 삭제되며 나중에 복구할 수 없습니다.

이름	서비스 ID	서비스 이름
Custom-EPS	vpce-svc-0f0f83cb8f81a64b0	com.amazonaws.vpce.ap-northeast-2.vpce-svc-0f0f83cb8f81a64b0

삭제를 확인하려면 필드에 삭제를 입력하십시오.

삭제

취소

삭제

3. 실습2. 엔드포인트 서비스로 프라이빗 링크 구성

■ 자원 삭제

- CloudFormation 스택 삭제
- CloudFormation > 스택 > 삭제

CloudFormation > 스택

스택 (1)

🔄 삭제 업데이트 스택 작업 ▼ 스택 생성 ▼

🔍 스택 이름으로 필터링 ☐ 뷰 중첩됨 활성 ▼ < 1 > ⚙️

스택 이름	상태	생성 시간	설명
lab9-2	✔️ CREATE_COMPLETE	2022-07-24 00:11:09 UTC+0900	-

lab9-2을(를) 삭제하시겠습니까?



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

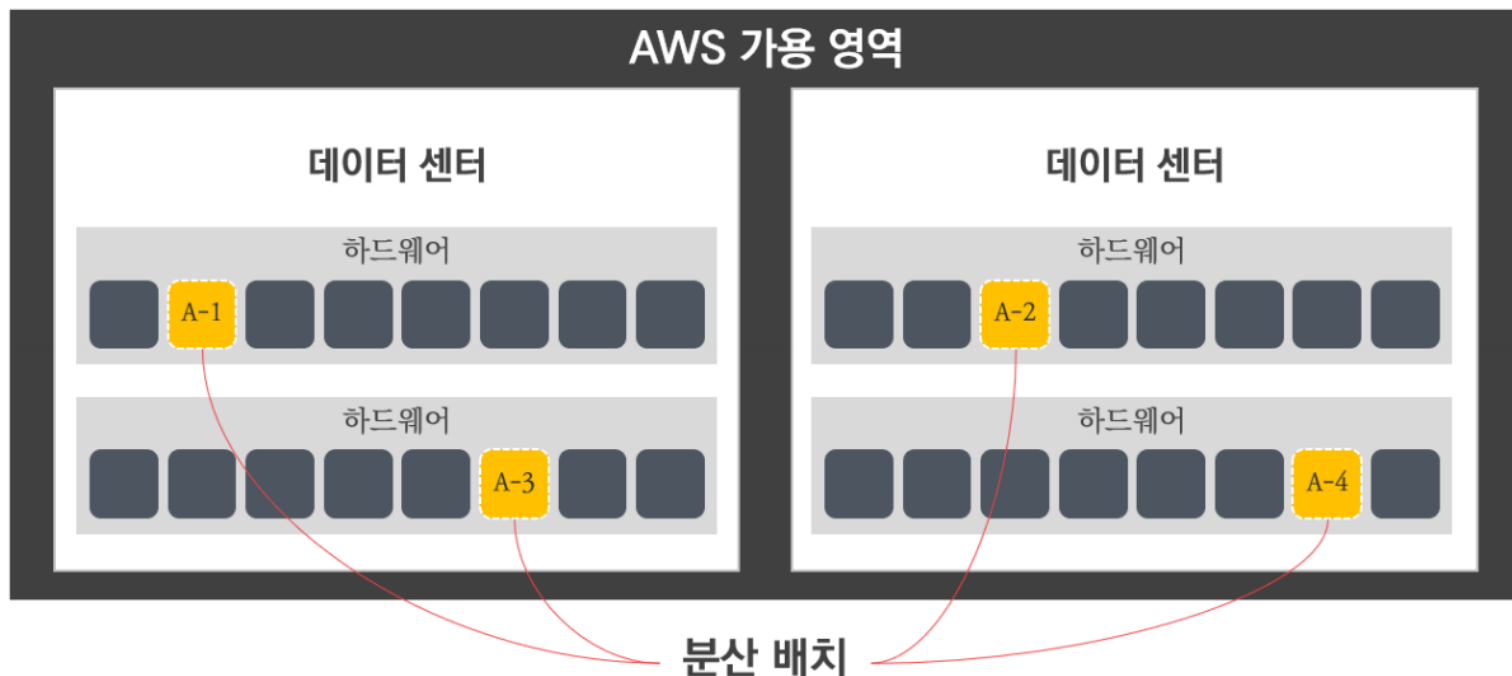
취소

스택 삭제

4. 배치 그룹 (Placement Group)

■ 배치 그룹이란?

- 새로운 인스턴스가 시작되면 AWS에서는 하드웨어에 최대한 분산하여 배치한다.
- 이유는 물리 호스트의 장애에 대해 상호 간 영향도를 최소화하고 장애를 줄이는 데 도움이 되기 때문이다.
- 물론 인스턴스의 배치가 분산되는 상황이 모두 좋은 것은 아니다.
- 워크로드(Workload)에 따라 인스턴스의 배치 위치를 조정하는 것이 유리한 경우가 있다.
- 이러한 필요에 따라 배치 그룹(Placement Group)은 그룹 내 인스턴스의 배치를 조정하는 기능이다.



4. 배치 그룹 (Placement Group)

■ 배치 그룹 종류

■ 클러스터 배치 그룹

- 클러스터 배치 그룹(Cluster Placement Group)은 인스턴스의 하드웨어 배치를 서로 근접하게 배치한다.
- 일반적으로 고성능 컴퓨팅 환경에서는 수많은 애플리케이션이 서로 긴밀한 통신을 요구하여 낮은 지연 시간과 높은 네트워크 성능이 필요하다.
- 이와 같은 환경에서 클러스터 배치 그룹으로 서로 인접하게 배치하여 지연과 성능을 보장한다.
- 클러스터 배치 그룹은 하나의 가용 영역에 종속되는 제약이 있으며, 그룹 내 인스턴스는 동일한 인스턴스 유형을 사용하는 것을 권고한다.



4. 배치 그룹 (Placement Group)

■ 배치 그룹 종류

■ 파티션 배치 그룹

- 파티션 배치 그룹(Partition Placement Group)은 인스턴스를 논리적인 세그먼트로 분산하며, 하나의 파티션에 존재하는 인스턴스는 다른 파티션의 인스턴스와 하드웨어를 공유하지 않아 상호 영향을 미치지 않는다.
- 파티션 배치 그룹은 가용 영역당 파티션을 최대 7개까지 가질 수 있으며, 파티션 배치 그룹에서 실행할 수 있는 인스턴스 숫자는 계정 제한의 적용을 받는다.

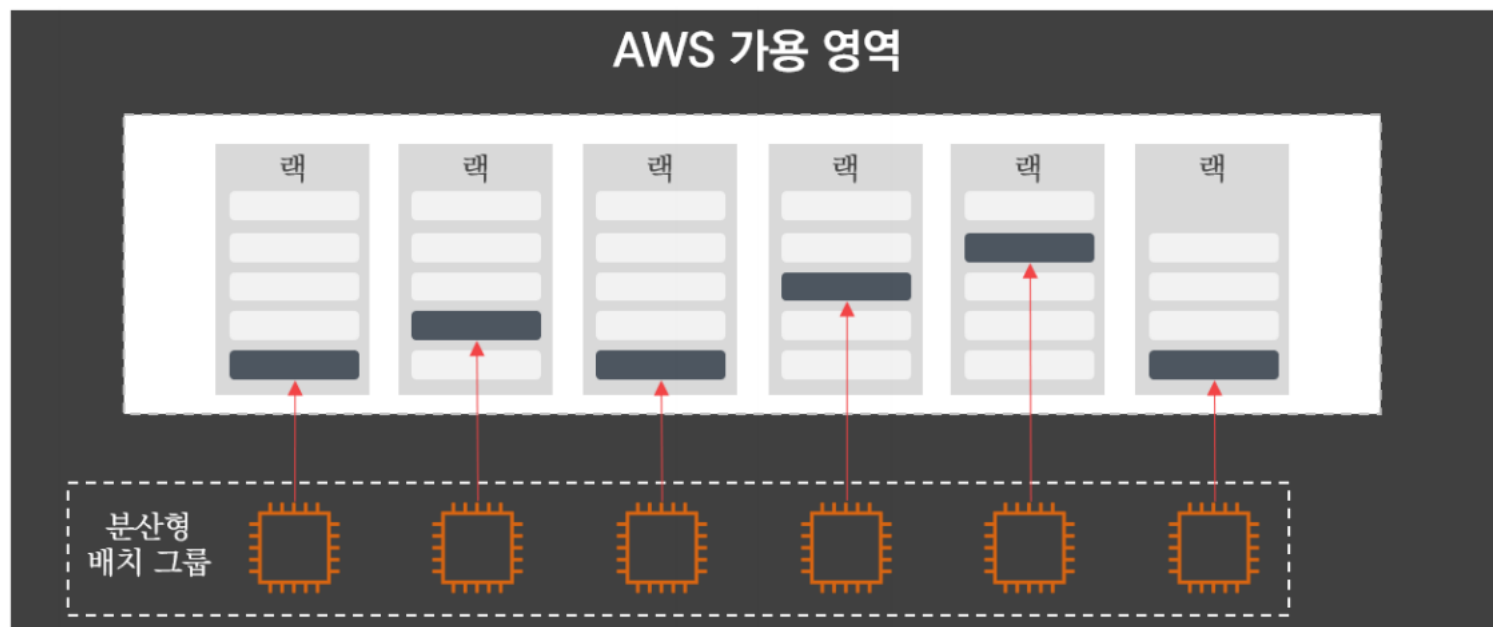


4. 배치 그룹 (Placement Group)

■ 배치 그룹 종류

■ 분산형 배치 그룹

- 분산형 인스턴스 그룹(Spread Placement Group)은 서로 다른 하드웨어로 분산하여 배치하여 인스턴스 간의 상호 장애 영향도를 최소화하는 방법이다.
- 보통 중요한 애플리케이션의고가용성을 보장받기 위해 사용한다.
- 분산형 배치 그룹은 각각 고유한 랙에 배치된 인스턴스 그룹이며 랙마다 자체 네트워크 및 전원이 있다.
- 분산형 배치 그룹은 가용 영역당 7개의 인스턴스로 제한된다.



5. 메타데이터 (Metadata)

■ 메타데이터란?

- 메타데이터(Metadata)는 객체에 대한 키와 값(Key&Value)에 대한 집합 데이터이다.
- 메타데이터에서 정의한 키에 대한 값을 가지고 있어 필요한 정보를 호출하여 정보를 파악할 수 있다.
- EC2 인스턴스 같은 경우에도 아래 표와 같이 인스턴스에 대한 메타데이터를 가지고 있다.

키	설명	키	설명
ami-id	AMI ID	placement/availability-zone	인스턴스의 가용 영역 정보
ami-launch-index	인스턴스 시작 순서	public-hostname	퍼블릭 IP의 DNS 호스트 이름
hostname	프라이빗 IP의 DNS 호스트 이름	public-ipv4	퍼블릭 IP 주소
instance-id	인스턴스 ID	public-keys/	퍼블릭 키 정보
instance-type	인스턴스 유형	security-groups	인스턴스에 적용된 보안 그룹
local-ipv4	프라이빗 IP 주소	services/domain	AWS 리소스 도메인 정보
mac	인스턴스의 MAC 주소	services/partition	리소스가 있는 파티션 정보
network/	네트워크 정보 (하위 메뉴 존재)		

IT COOKBOOK

- 실제 EC2 인스턴스를 생성하여 메타데이터 정보를 확인해 보자.
- 메타데이터를 호출하는 방법은 169.254.169.254라는 링크-로컬 주소를 가지고 HTTP 요청과 응답으로 확인할 수 있다.
- `http://169.254.169.254/latest/meta-data/` 주소로 `curl` 명령어를 통해 EC2 인스턴스에 대한 사용 가능한 키 또는 디렉터리를 확인할 수 있다.
- `curl http://169.254.169.254/latest/meta-data/`

```

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-45-24 ~]$ curl http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
identity-credentials/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
managed-ssh-keys/
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/[ec2-user@ip-172-31-45-24 ~]$
```

5. 메타데이터 (Metadata)

■ EC2 인스턴스 메타데이터 확인

- curl <http://169.254.169.254/latest/meta-data/ami-id>

```
services/[ec2-user@ip-172-31-45-24 ~]$ curl http://169.254.169.254/latest/meta-data/ami-id
ami-02d1e544b84bf7502[ec2-user@ip-172-31-45-24 ~]$ curl http://169.254.169.254/latest/meta-data/ami-id
ami-02d1e544b84bf7502[ec2-user@ip-172-31-45-24 ~]$
[ec2-user@ip-172-31-45-24 ~]$
[ec2-user@ip-172-31-45-24 ~]$ curl http://169.254.169.254/latest/meta-data/hostname
ip-172-31-45-24.us-east-2.compute.internal[ec2-user@ip-172-31-45-24 ~]$
[ec2-user@ip-172-31-45-24 ~]$ curl http://169.254.169.254/latest/meta-data/instance-id
i-0619258bf0c1714b2[ec2-user@ip-172-31-45-24 ~]$
[ec2-user@ip-172-31-45-24 ~]$ curl http://169.254.169.254/latest/meta-data/security-groups
launch-wizard-4[ec2-user@ip-172-31-45-24 ~]$
[ec2-user@ip-172-31-45-24 ~]$ █
```

- 위와 같이 `http://169.254.169.254/latest/meta-data/` 주소 뒤에 키를 추가하여 다양한 정보를 확인해 볼 수 있다.
- 이렇게 메타데이터를 통해 인스턴스의 설정 자동화 작업에 활용하거나 다수의 인스턴스를 일괄 관리하는 형태로 활용할 수 있다.



Thank You
