

AWS Basic Networking Design HoL

실습 순서

- 워크샵 시작 전 준비 사항
- Amazon VPC
 - VPC 생성하기
 - 추가 서브넷 생성하기
 - 라우팅 테이블 편집하기
 - 보안 그룹 생성하기
- VPC 엔드포인트
 - Gateway 엔드포인트 생성하기
- VPC 피어링
 - 피어링 요청 생성하기
 - 피어링 요청 수락하기
 - 피어링 라우팅 테이블 편집하기
- 실습 리소스 정리

워크샵 시작 전 준비 사항

AWS 계정 생성하기

이미 AWS 계정을 가지고 있다면 바로 이 실습의 가이드를 따라 진행할 수 있으나 계정이 없다면 먼저 AWS 계정을 만들어야 합니다.

관리자 권한이 있는 **AWS 계정**이 아직 **없**는 경우, 여기를 클릭하여 계정을 생성합니다.

IAM 사용자

AWS 계정을 생성했거나 이미 있는 경우, AWS 계정에 접근할 수 있는 **IAM 사용자**를 생성합니다. 계정에 로그인한 후, IAM 콘솔을 사용하여 IAM 사용자를 생성할 수 있습니다. 아래의 순서에 따라 Administrator(관리자) 권한을 가진 사용자를 생성합니다. 이미 관리자 권한을 가진 IAM 사용자가 있다면, 다음 작업을 건너뛰니다.

1. 로그인 페이지에서 AWS 계정 이메일 주소와 비밀번호를 사용하여 **AWS 계정의 루트 사용자**로 IAM 콘솔에 로그인 합니다.
2. IAM 콘솔 화면 왼쪽 사이드 바에서 **Users**(사용자)를 클릭한 다음, **Add user**(사용자 추가) 버튼을 클릭합니다.
3. **User name**(사용자 이름)은 **Administrator** 로 입력합니다.
4. Access type(엑세스 유형)에서 **AWS Management Console access** 체크 박스를 선택하고, **Custom password**를 선택한 다음 비밀번호를 입력합니다.
5. **Next: Permissions**(다음: 권한)을 클릭합니다.

Add user



Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[+ Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type* ☐ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☒ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* ☐ Autogenerated password
☒ Custom password

☐ Show password

Require password reset ☐ User must create a new password at next sign-in
Users automatically get the `IAMUserChangePassword` policy to allow them to change their own password.

* Required

[Cancel](#)


[Next: Permissions](#)


6. **Attach existing policies directly** (기존 정책 직접 연결)를 선택하고, **AdministratorAccess** 정책에 체크박스를 선택한 후, **Next: Tags** (다음: 태그)를 클릭합니다.


Add user

1 2 3 4 5

Set permissions

 Add user to group

 Copy permissions from existing user

 Attach existing policies directly

Create policy

Filter policies Showing 577 results

	Policy name	Type	Used as
<input checked="" type="checkbox"/>	AdministratorAccess	Job function	Permissions policy (10)
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessFullAccess	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None
<input type="checkbox"/>	AlexaForBusinessReadOnlyAccess	AWS managed	None
<input type="checkbox"/>	AllowStorageGatewayAssumeBucketAccessRole6ecb5bc6-f551-466...	Customer managed	Permissions policy (1)
<input type="checkbox"/>	AmazonAPIGatewayAdministrator	AWS managed	None

Set permissions boundary

Cancel

Previous

Next: Tags

7. 태그 추가(선택 사항) 단계에서 **Next: Review** (다음: 검토)를 클릭합니다.
8. Administrator 사용자에게 AdministratorAccess 관리형 정책이 추가된 것을 확인하고 **Create user** (사용자 만들기)를 클릭합니다.
9. 사용자가 추가되면 **로그인 URL**을 복사합니다. 해당 URL은 아래의 형식을 가집니다. `https://<your_aws_account_id>.signin.aws.amazon.com/console`

<your_aws_account_id>는 본인 AWS 계정의 고유 ID가 들어가는 자리입니다. 루트 사용자로 해당 실습을 진행하는 것은 권고드리지 않는 사항입니다. 반드시 Administrator 사용자로 로그인하여 실습을 진행하세요.

Add user



Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://signin.aws.amazon.com/console>

Download .csv

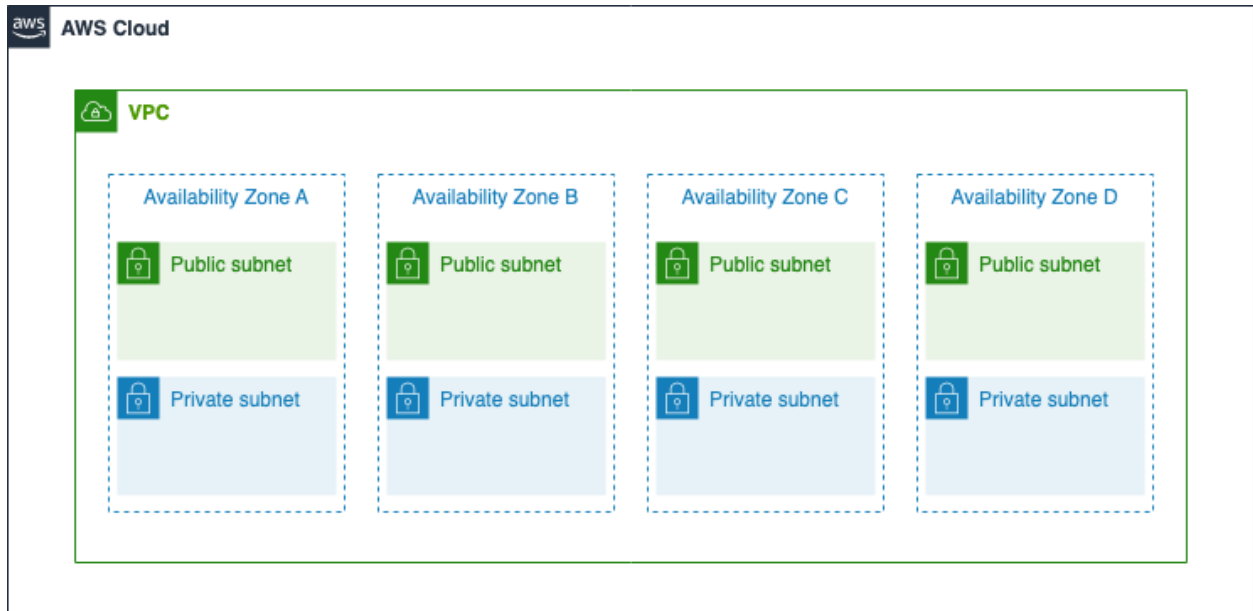
	User	Email login instructions
▶	✓ Administrator	Send email

10. 이제 루트 사용자에서 로그아웃하고, 방금 복사한 URL로 접속해서 **새로 생성한 Administrator 사용자**로 로그인 합니다.

Amazon VPC

Amazon Virtual Private Cloud(Amazon VPC) 를 이용하면 사용자가 정의한 가상 네트워크로 AWS 리소스를 시작할 수 있습니다. 이 가상 네트워크는 AWS의 확장 가능한 인프라를 사용한 다는 이점과 함께 고객의 자체 데이터 센터에서 운영하는 기존 네트워크와 매우 유사합니다.

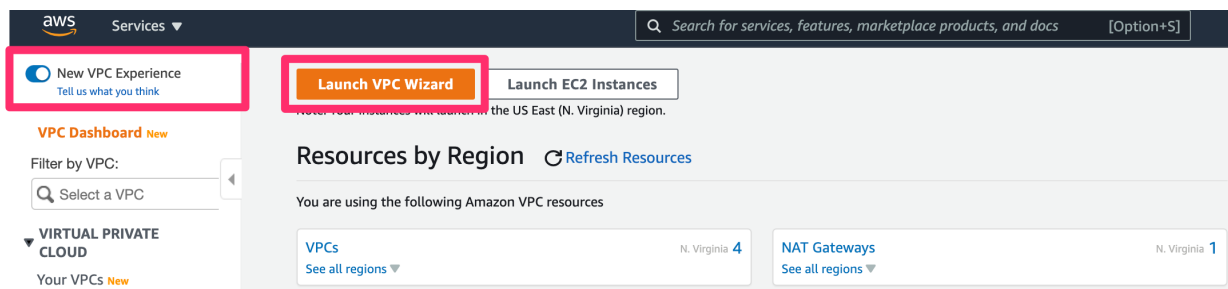
Amazon VPC를 사용하면 사용자가 정의하는 논리적으로 격리된 가상 네트워크에서 AWS 리소스를 시작할 수 있습니다. IP 주소 범위 선택, 서브넷 생성, 라우팅 테이블 및 네트워크 게이트웨이 구성 등 가상 네트워킹 환경을 완벽하게 제어할 수 있습니다. 리소스 및 애플리케이션에 대한 안전하고 쉬운 액세스를 보장하도록 지원하기 위해 IPv4 및 IPv6를 가상 사설 클라우드 내 대개의 리소스에 대해 사용할 수 있습니다.



아래의 순서 대로 실습을 진행하면서 네트워크를 직접 구성합니다:

VPC 생성하기

1. VPC 콘솔에 로그인 합니다.
2. 아래의 화면에서 **VPC 마법사 시작**을 클릭하여 VPC 생성 마법사를 시작합니다. VPC 마법사를 사용하면 기본이 아닌 VPC 구성을 손쉽게 생성할 수 있습니다.



3. 단계 1: VPC 구성 선택에서 첫 번째 옵션인 **단일 퍼블릭 서브넷이 있는 VPC**를 선택합니다.

VPC with a Single Public Subnet

VPC with Public and Private Subnets

VPC with Public and Private Subnets and Hardware VPN Access

VPC with a Private Subnet Only and Hardware VPN Access

Your instances run in a private, isolated section of the AWS cloud with direct access to the Internet. Network access control lists and security groups can be used to provide strict control over inbound and outbound network traffic to your instances.

Creates:

A /16 network with a /24 subnet. Public subnet instances use Elastic IPs or Public IPs to access the Internet.

Important:

If you are using a Local Zone with your VPC [follow this link](#) to create your VPC.

Select

4. 서브넷을 만들 때 해당 서브넷에 대한 CIDR 블록을 지정합니다. 이는 VPC CIDR 블록의 부분 집합입니다. 각 서브넷은 단일 가용 영역 내에서만 존재해야 합니다. 단계 2: 단일 퍼블릭 서브넷이 있는 VPC에서 화면과 같이 값을 입력한 후, 우측 하단의 **VPC 생성** 버튼을 누릅니다.

aws Services ▾ Search for services, features, marketplace products, and docs [Option+S]

Step 2: VPC with a Single Public Subnet

IPv4 CIDR block:* 10.0.0.0/16 (65531 IP addresses available)

IPv6 CIDR block: ☒ No IPv6 CIDR Block
☐ Amazon provided IPv6 CIDR block

VPC name: VPC-Lab

Public subnet's IPv4 CIDR:* 10.0.10.0/24 (251 IP addresses available)

Availability Zone:* ap-northeast-2a ▾

Subnet name: public subnet A

You can add more subnets after AWS creates the VPC.

Service endpoints

Add Endpoint

Enable DNS hostnames:* ☒ Yes ☐ No

Hardware tenancy:* Default ▾

Aa 키

≡ 값

Aa 키	≡ 값
IPv4 CIDR 블록	10.0.0.0/16
VPC 이름	VPC-Lab
퍼블릭 서브넷의 IPv4 CIDR	10.0.10.0/24
가용 영역	ap-northeast-2a
서브넷 이름	public subnet A

VPC IPv4 CIDR 블록 값을 지정할 때에는 향후 직접 연결할 가능성이 있는 네트워크와 주소가 중복되지 않도록 할당하는 것이 중요합니다. 또한, 향후 확장을 고려하여 충분히 큰 주소를 할당합니다.

- 생성이 완료되면 화면과 같이 **VPC-Lab** 이름을 가진 VPC가 생성된 것을 확인할 수 있습니다.

The screenshot displays the AWS Management Console interface for VPCs. At the top, there's a section titled 'Your VPCs (1/2)' with a search bar and a 'Create VPC' button. Below this is a table listing VPCs. The table has columns for Name, VPC ID, State, IPv4 CIDR, IPv6 CIDR (Network border group), DHCP options set, and Main route table. Two VPCs are listed: one with ID 'vpc-eca62a87' and another named 'VPC-Lab' with ID 'vpc-0974345f87c196f41'. The 'VPC-Lab' VPC is selected, and its details are shown below the table. The details section includes tabs for 'Details', 'CIDRs', 'Flow logs', and 'Tags'. The 'Details' tab is active, showing various attributes of the VPC-Lab, such as its ID, state (Available), DHCP options set, main route table, and owner ID.

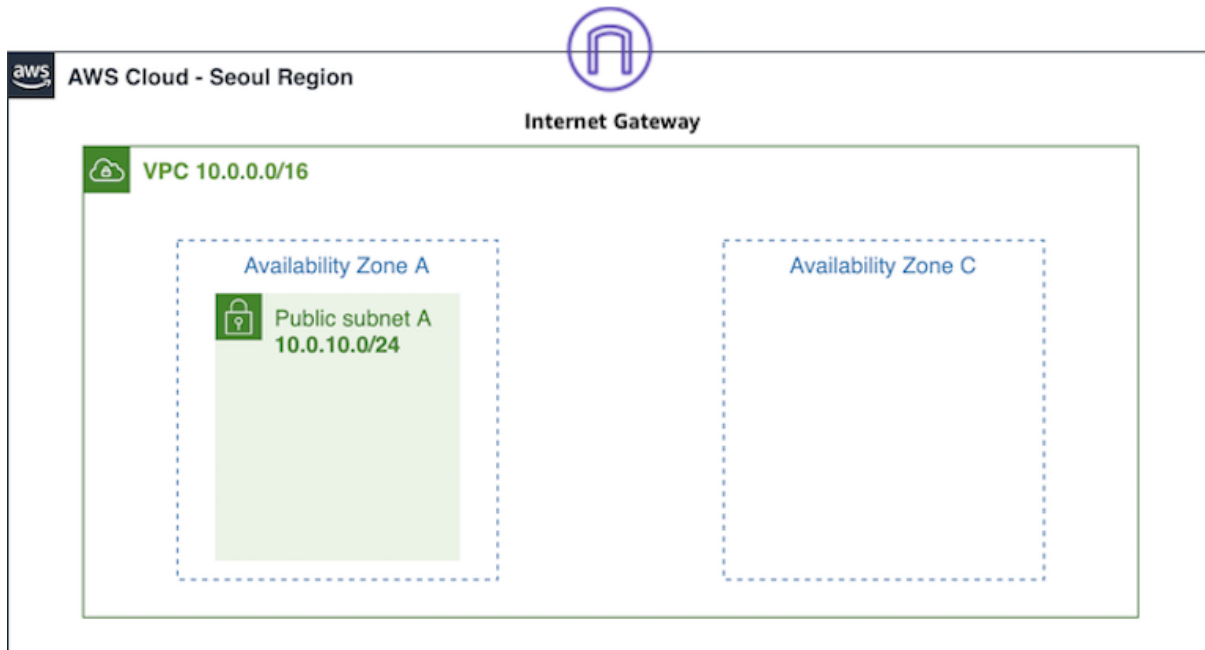
Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR (Network border group)	DHCP options set	Main route table
-	vpc-eca62a87	Available	172.31.0.0/16	-	dopt-79d5a412	rtb-e92c7982
VPC-Lab	vpc-0974345f87c196f41	Available	10.0.0.0/16	-	dopt-79d5a412	rtb-0147aed7

vpc-0974345f87c196f41 / VPC-Lab

Details

VPC ID vpc-0974345f87c196f41	State Available	DNS hostnames Enabled	DNS resolution Enabled
Tenancy Default	DHCP options set dopt-79d5a412	Main route table rtb-0147aed7d6f8bdf8	Main network ACL acl-05f2f240120dc9aa8
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 CIDR (Network border group) -	Route 53 Resolver DNS Firewall rule groups -
Owner ID 612544235551			

- 현재까지의 아키텍처 구성은 아래와 같습니다.



추가 서브넷 생성하기

고가용성을 확보하기 위해, 다중 가용 영역에 서비스를 배포하는 것이 중요합니다. 따라서 본 실습에서는 앞에서 생성한 서브넷이 위치한 가용 영역 A 외에 다른 가용 영역인 C에 서브넷을 생성합니다.

1. 왼쪽 사이드 바에서 **서브넷** 메뉴를 클릭한 후, **서브넷 생성** 버튼을 클릭합니다.

The screenshot shows the AWS Management Console interface. On the left sidebar, the 'Subnets' menu item is highlighted with a green checkmark and a callout '1) Click subnet menu'. The main content area displays the 'Subnets (5)' table. The table has columns for Name, Subnet ID, State, VPC, IPv4 CIDR, IPv6 CIDR, and Available IPv4 addresses. The table lists five subnets, including 'public subnet A'. The 'Create subnet' button is highlighted with a green checkmark and a callout '2) Click create subnet'.

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses
-	subnet-264cf24d	Available	vpc-eca62a87	172.31.0.0/20	-	4091
public subnet A	subnet-014aa4647ffa312b7	Available	vpc-0974345f87c196f41 VP...	10.0.10.0/24	-	251
-	subnet-b212f0fd	Available	vpc-eca62a87	172.31.32.0/20	-	4091
-	subnet-cf8de6b4	Available	vpc-eca62a87	172.31.16.0/20	-	4091
-	subnet-4bf10e14	Available	vpc-eca62a87	172.31.48.0/20	-	4091

2. VPC ID에는 방금 생성한 VPC를 선택합니다.

Create subnet [Info](#)

VPC

VPC ID

Create subnets in this VPC.

Select a VPC

Q |

vpc-eca62a87
172.31.0.0/16

(default)

vpc-0974345f87c196f41 (VPC-Lab)
10.0.0.0/16

Select a VPC first to create new subnets.

Add new subnet

Cancel

Create subnet

3. 아래의 **서브넷 설정**에서는 화면과 같이 값을 입력한 후, **서브넷 생성** 버튼을 클릭합니다.

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

public subnet C

The name can be up to 256 characters long.

Availability Zone [Info](#)

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

Asia Pacific (Seoul) / ap-northeast-2c

IPv4 CIDR block [Info](#)

10.0.20.0/24

▼ Tags - optional

Key

Name

Value - optional

public subnet C

Remove

Add new tag

You can add 49 more tags.

Remove

Add new subnet

Cancel

Create subnet

<u>Aa</u> 키	<u>≡</u> 값
서브넷 이름	public subnet C
가용 영역	ap-northeast-2c
IPv4 CIDR 블록	10.0.20.0/24
<u>Name</u>	public subnet C

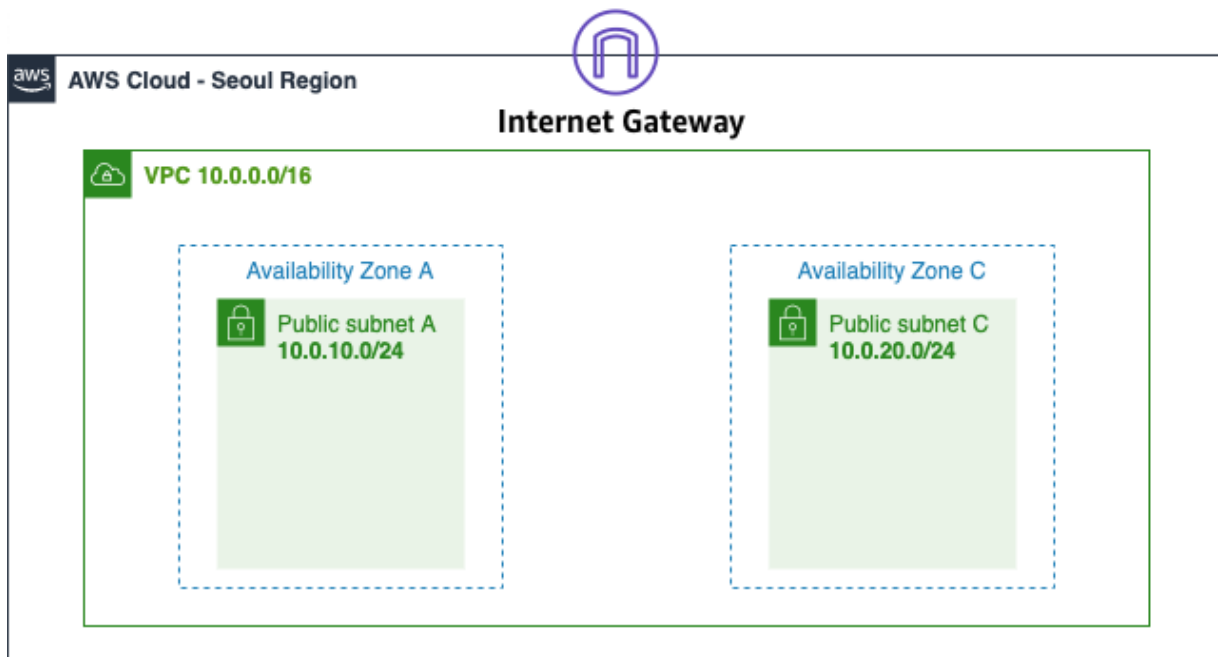
4. **public subnet A**와 **public subnet C**가 모두 생성된 것을 확인할 수 있습니다.

Subnets (1/6) Info							
Filter subnets							
	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses
<input checked="" type="checkbox"/>	public subnet C	subnet-0f9fa61bcf22173f4	Available	vpc-0974345f87c196f41 VP...	10.0.20.0/24	-	251
<input type="checkbox"/>	public subnet A	subnet-014aa4647ffa312b7	Available	vpc-0974345f87c196f41 VP...	10.0.10.0/24	-	251
<input type="checkbox"/>	-	subnet-264cf24d	Available	vpc-eca62a87	172.31.0.0/20	-	4091
<input type="checkbox"/>	-	subnet-b212f0fd	Available	vpc-eca62a87	172.31.32.0/20	-	4091
<input type="checkbox"/>	-	subnet-cf8de6b4	Available	vpc-eca62a87	172.31.16.0/20	-	4091
<input type="checkbox"/>	-	subnet-4bf10e14	Available	vpc-eca62a87	172.31.48.0/20	-	4091

Details	Flow logs	Route table	Network ACL	Sharing	Tags
---------	-----------	-------------	-------------	---------	------

Details			
Subnet ID subnet-0f9fa61bcf22173f4	State Available	VPC vpc-0974345f87c196f41 VPC-Lab	IPv4 CIDR 10.0.20.0/24
Available IPv4 addresses 251	IPv6 CIDR -	Availability Zone ap-northeast-2c	Availability Zone ID apne2-az3
Network border group ap-northeast-2	Route table rtb-0147aed7dd6f8bdf8	Network ACL acl-05f2f240120dc9aa8	Default subnet No

5. 현재까지의 아키텍처 구성은 아래와 같습니다.



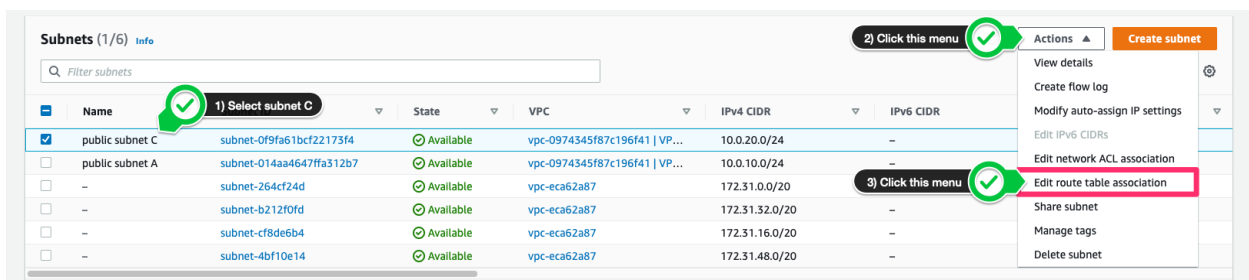
라우팅 테이블 편집하기

VPC 라우팅 테이블 개념

라우팅 테이블에는 서브넷 또는 게이트 웨이의 네트워크 트래픽이 전송되는 위치를 결정하는데 사용되는 라우팅이라는 규칙 집합이 포함되어 있습니다.

- 기본 라우팅 테이블은 VPC와 함께 자동으로 생성되는 라우팅 테이블입니다. 다른 라우팅 테이블과 명시적으로 연결되지 않은 모든 서브넷의 라우팅을 제어하는 역할을 합니다.
- 사용자 지정 라우팅 테이블은 기본 라우팅 테이블 외에 사용자가 생성한 라우팅 테이블입니다.

1. 서브넷 메뉴에서 작업 버튼을 클릭한 후, 라우팅 테이블 연결 편집을 선택합니다.




2. 라우팅 테이블 ID에서 기본 라우팅 테이블이 아닌 다른 라우팅 테이블을 선택한 후, 저장합니다. 이때, 선택한 라우팅 테이블에 인터넷으로 향하는 경로가 있는지 확인합니다.

Edit route table association [Info](#)

Subnet route table settings


Subnet ID
subnet-0f9fa61bcf22173f4

Route table ID
rtb-0c21eaa1ec6cd668e 

rtb-0c21eaa1ec6cd668e

rtb-0147aed7dd6f8bdf8
Main route table

Filter routes

< 1 > 

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-069c6c48857df4966

Cancel

Save

3. **public subnet C**를 선택한 후, 세부 정보 탭에서 변경된 라우팅 테이블 하이퍼 링크를 클릭하면 라우팅 정보를 확인할 수 있습니다.

Subnets (1/6) Info

Filter subnets

1) Select subnet C

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses
<input checked="" type="checkbox"/> public subnet C	subnet-0f9fa61bcf22173f4	Available	vpc-0974345f87c196f41 VP...	10.0.20.0/24	-	251
<input type="checkbox"/> public subnet A	subnet-014aa4647ffa312b7	Available	vpc-0974345f87c196f41 VP...	10.0.10.0/24	-	251
<input type="checkbox"/> -	subnet-264cf24d	Available	vpc-eca62a87	172.31.0.0/20	-	4091
<input type="checkbox"/> -	subnet-b212f0fd	Available	vpc-eca62a87	172.31.32.0/20	-	4091
<input type="checkbox"/> -	subnet-cf8de6b4	Available	vpc-eca62a87	172.31.16.0/20	-	4091
<input type="checkbox"/> -	subnet-4bf10e14	Available	vpc-eca62a87	172.31.48.0/20	-	4091

Details | Flow logs | Route table | Network ACL | Sharing | Tags

2) Click Details tab

Details

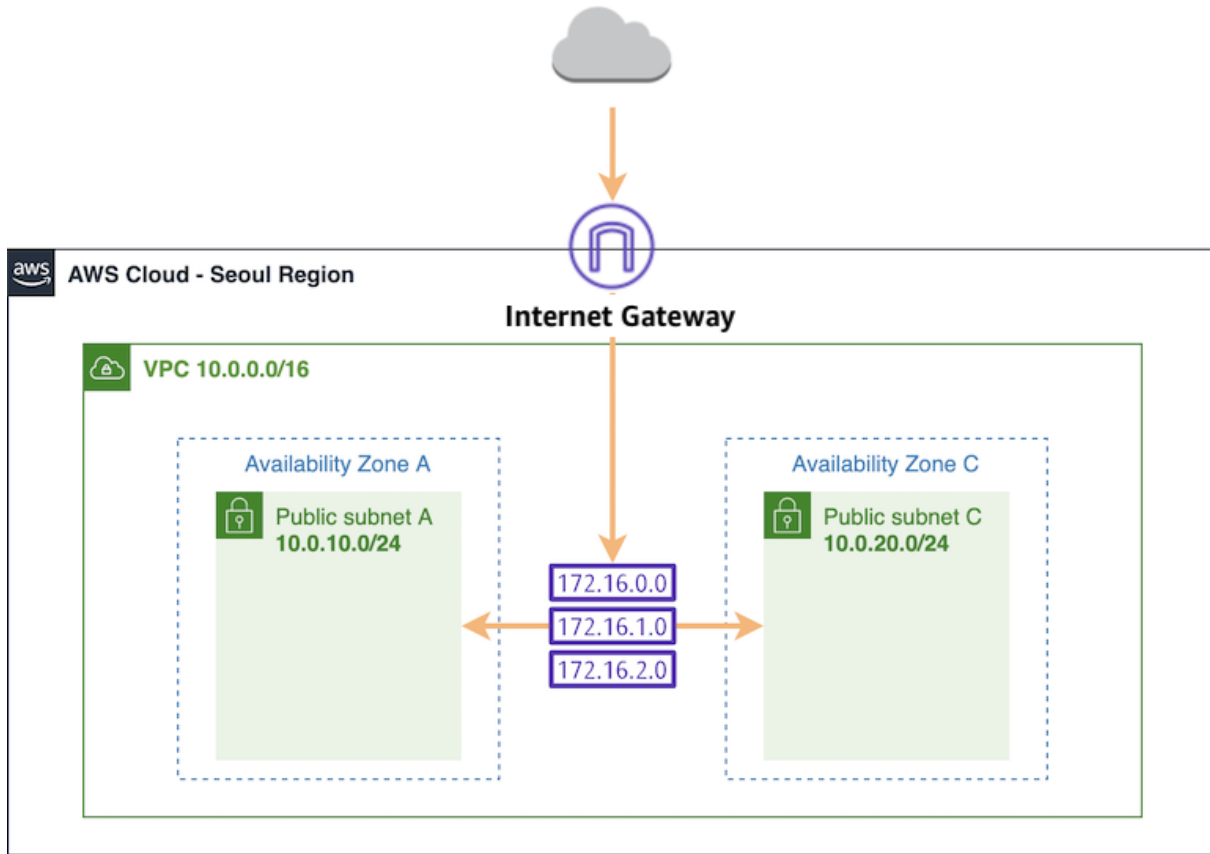
Subnet ID subnet-0f9fa61bcf22173f4	State Available	VPC vpc-0974345f87c196f41 VPC-Lab	IPv4 CIDR 10.0.20.0/24
Available IPv4 addresses 251	IPv6 CIDR -	Availability Zone ap-northeast-2c	Availability Zone ID apne2-az3
Network border group ap-northeast-2	Route table rtb-0c21eaa1ec6cd668e	Network ACL acl-05f2f240120dc9aa8	Default subnet No

3) Check routing info

라우팅 테이블을 클릭 후, **라우트** 탭에서 확인할 수 있는 결과는 아래와 같습니다. 이를 통해, public subnet C도 인터넷으로 향하는 경로가 생성되었음을 확인할 수 있습니다.

Destination	Target
<u>10.0.0.0/16</u>	local
<u>0.0.0.0/0</u>	igw-OOO

4. 현재까지의 아키텍처 구성은 아래와 같습니다.



보안 그룹 생성하기

보안 그룹은 인스턴스에 대한 인바운드 및 아웃바운드 트래픽을 제어하는 가상 방화벽 역할을 합니다.

1. 왼쪽 사이드 바에서 **보안 그룹** 메뉴를 클릭한 뒤, **보안 그룹 생성** 버튼을 클릭합니다.

Security Groups (2) Info									
<input type="text" value="Filter security groups"/> Actions Create security group									
<input type="checkbox"/>	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	Outbound rules count	
<input type="checkbox"/>	-	sg-0071c8cbaec74ae68	default	vpc-0974345f87c196f41	default VPC security group	612544235351	1 Permission entry	1 Permission entry	
<input type="checkbox"/>	-	sg-4a329f37	default	vpc-eca62a87	default VPC security group	612544235351	1 Permission entry	1 Permission entry	

- 화면과 같이 보안 그룹 및 설명을 입력한 후, 본 실습에서 생성한 VPC를 선택합니다.

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)

webserver-sg

Name cannot be edited after creation.

Description [Info](#)

security group for web servers

VPC [Info](#)

vpc-0974345f87c196f41 (VPC-Lab)

Q |

vpc-eca62a87

172.31.0.0/16

(default)

vpc-0974345f87c196f41 (VPC-Lab)

10.0.0.0/16

This security group has no inbound rules.

Aa 키	≡ 값
보안 그룹 이름	webserver-sg
설명	security group for web servers
VPC	VPC-Lab

- 인바운드 규칙에서 아래와 같이 규칙을 부여한 후, 오른쪽 하단의 보안 그룹 생성 버튼을 클릭합니다.

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
HTTP	TCP	80	Anywhere-IPv4		Delete
SSH	TCP	22	Anywhere-IPv4		Delete

[Add rule](#)

Aa 유형	소스
HTTP	Anywhere-IPv4
SSH	Anywhere-IPv4

4. 아래와 같이 인바운드 규칙이 생성된 것을 확인합니다.

VPC > Security Groups > sg-0d1e6fe025b1c4a05 - webserver-sg

sg-0d1e6fe025b1c4a05 - webserver-sg Actions ▼

Details

Security group name webserver-sg	Security group ID sg-0d1e6fe025b1c4a05	Description security group for web servers	VPC ID vpc-0974345f87c196f41
Owner [icon]	Inbound rules count 4 Permission entries	Outbound rules count 1 Permission entry	

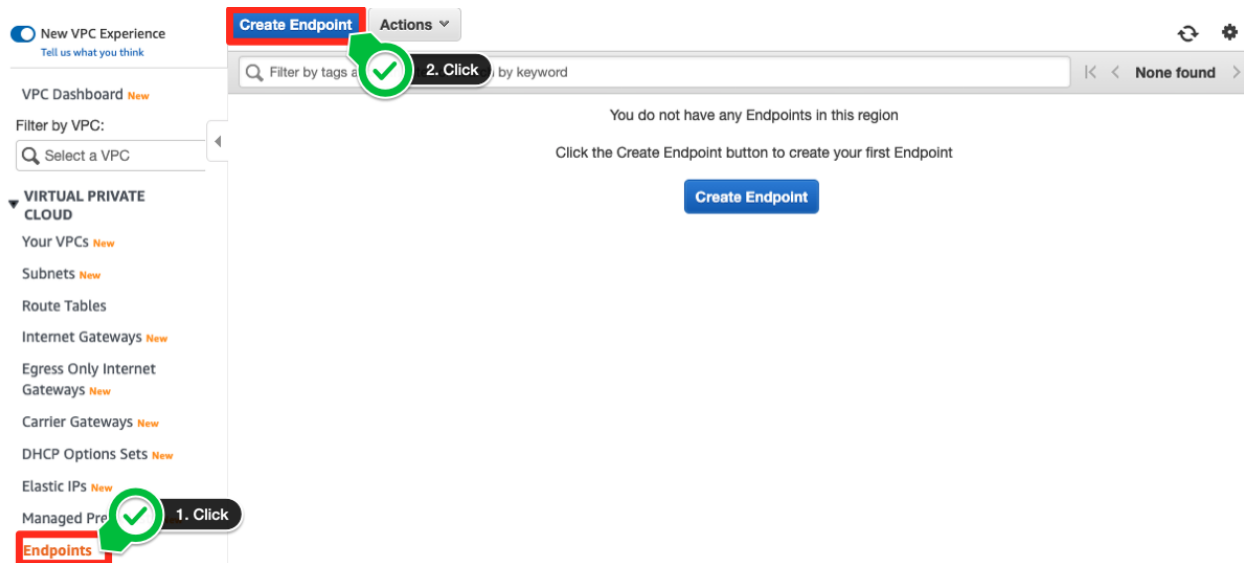
Inbound rules | Outbound rules | Tags

Inbound rules (4) Edit inbound rules

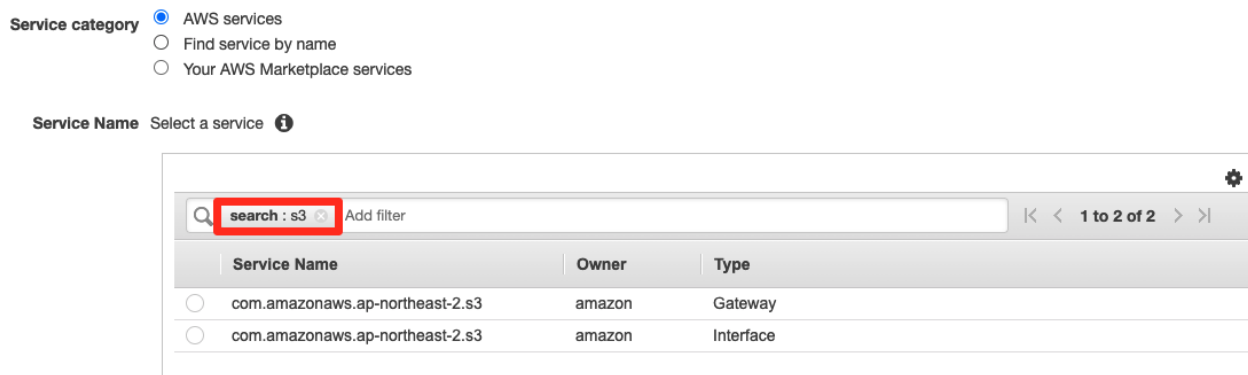
Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	0.0.0.0/0	-
HTTP	TCP	80	:::0	-
SSH	TCP	22	0.0.0.0/0	-
SSH	TCP	22	:::0	-

VPC 엔드포인트

1. VPC 대시보드에서 엔드포인트를 선택하십시오. 엔드포인트 생성을 클릭합니다.



2. 사용하고자 하는 엔드포인트의 서비스를 검색할 수 있습니다. 이번 실습에서는 S3를 검색하여 선택하고, 연결할 VPC를 선택하겠습니다. 아래 그림과 같이, S3는 게이트웨이 VPC 엔드포인트만 지원했으나, 인터페이스 엔드포인트도 추가로 지원하게 되었음을 확인할 수 있습니다. 이번 실습에서는 게이트웨이 엔드포인트 타입만 생성해 보겠습니다.



S3의 인터페이스 타입과 게이트웨이 타입을 각각 선택해 보면서 어떤 설정들이 다른지 비교해보세요.

3. 엔드포인트를 반영할 VPC를 선택하고 라우팅 테이블을 선택합니다. 선택된 라우팅 테이블에는 엔드포인트를 사용하기 위한 별도의 라우팅 정보가 자동으로 추가됩니다.

[Endpoints](#) > Create Endpoint

Create Endpoint

A VPC endpoint enables you to securely connect your VPC to another service.

There are three types of [VPC endpoints](#) – Interface endpoints, Gateway Load Balancer endpoints, and gateway endpoints.

Interface endpoints and Gateway Load Balancer endpoints are powered by [AWS PrivateLink](#), and use an elastic network interface (ENI) as an entry point for traffic destined to the service.

Interface endpoints are typically accessed using the public or private DNS name associated with the service, while gateway endpoints and Gateway Load Balancer endpoints serve as a target for a route in your route table for traffic destined for the service.

Service category ☒ AWS services
☐ Find service by name
☐ Your AWS Marketplace services

Service Name **com.amazonaws.ap-northeast-2.s3** ⓘ

search : s3	Add filter	< < 1 to 2 of 2 > >
Service Name	Owner	Type
<input checked="" type="radio"/> com.amazonaws.ap-northeast-2.s3	amazon	Gateway
<input type="radio"/> com.amazonaws.ap-northeast-2.s3	amazon	Interface

VPC* vpc-0371126043544b5b4 ⓘ

Configure route tables

Filter by attributes

<input checked="" type="checkbox"/> vpc-0371126043544b5b4	10.0.0.0/16	available	VPC-Lab
<input type="checkbox"/> vpc-a934bac2	172.31.0.0/16	available	

a target with this endpoints' ID (e.g. vpce-12345678) will be added to

VPC* vpc-0371126043544b5b4 ⓘ

Configure route tables

A rule with destination **pl-78a54011 (com.amazonaws.ap-northeast-2.s3)** and a target with this endpoints' ID (e.g. vpce-12345678) will be added to the route tables you select below.

Subnets associated with selected route tables will be able to access this endpoint.

rtb-0f35ec6439ba41a04 ⓘ

Route Table ID	Main	Subnets
<input type="checkbox"/> rtb-03467649fc6610ab2	No	2 subnets
<input checked="" type="checkbox"/> rtb-0f35ec6439ba41a04	Yes	2 subnets

Private subnet

subnet-074329abaec8eded8 | Private subnet C

subnet-03f74d9dc418ca6d6 | Private subnet A

4. 아래와 같이 엔드포인트에 대한 접근 통제를 위한 정책을 구성할 수도 있습니다.

VPC 엔드 포인트 정책을 이용해 AWS 서비스에 대해 전체 액세스를 허용하거나 사용자 지정(Custom) 정책을 만들 수 있습니다. VPC 엔드 포

인트 정책에 대해 자세히 알아보세요.

- Policy*** ☒ Full Access - Allow access by any user or service within the VPC using credentials from any AWS accounts to any resources in this AWS service. All policies — IAM user policies, VPC endpoint policies, and AWS service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed. ⓘ
- ☐ Custom

Use the [policy creation tool](#) to generate a policy, then paste the generated policy below.

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    }
  ]
}
```

5. **Create Endpoint**을 클릭하면, S3를 사용하기 위한 엔드포인트가 생성됩니다.

[Endpoints](#) > Create Endpoint

Create Endpoint

✓ The following VPC Endpoint was created:

VPC Endpoint ID [vpce-0ae4f949223e78d7b](#)

Close

6. 앞서 지정한 프라이빗 라우팅 테이블에 게이트웨이 엔드포인트를 통해 Amazon S3로 접근하기 위한 라우팅이 자동으로 추가되었음을 확인합니다.

Create route table Actions

Filter by tags and attributes or search by keyword

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
Public route	rtb-03467649fc6610ab2	2 subnets	-	No	vpc-0371126043544b5b4 ...
Private route	rtb-0f35ec6439ba41a04	2 subnets	-	Yes	vpc-0371126043544b5b4 ...
				Yes	vpc-a934bac2

Route Table: rtb-0f35ec6439ba41a04

Route Tables 1. Click Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
pl-78a54011 (com.amazonaws.ap-northeast-2.s3, 52.219.144.0/22, 3.5.144.0/23, 3.5.140.0/22, 52.219.148.0/23, 52.219.60.0/23, 52.219.56.0/22)	vpce-0a6501bf90e68de08	active	No
0.0.0.0/0	nat-037a35d9ef3f66829	active	No

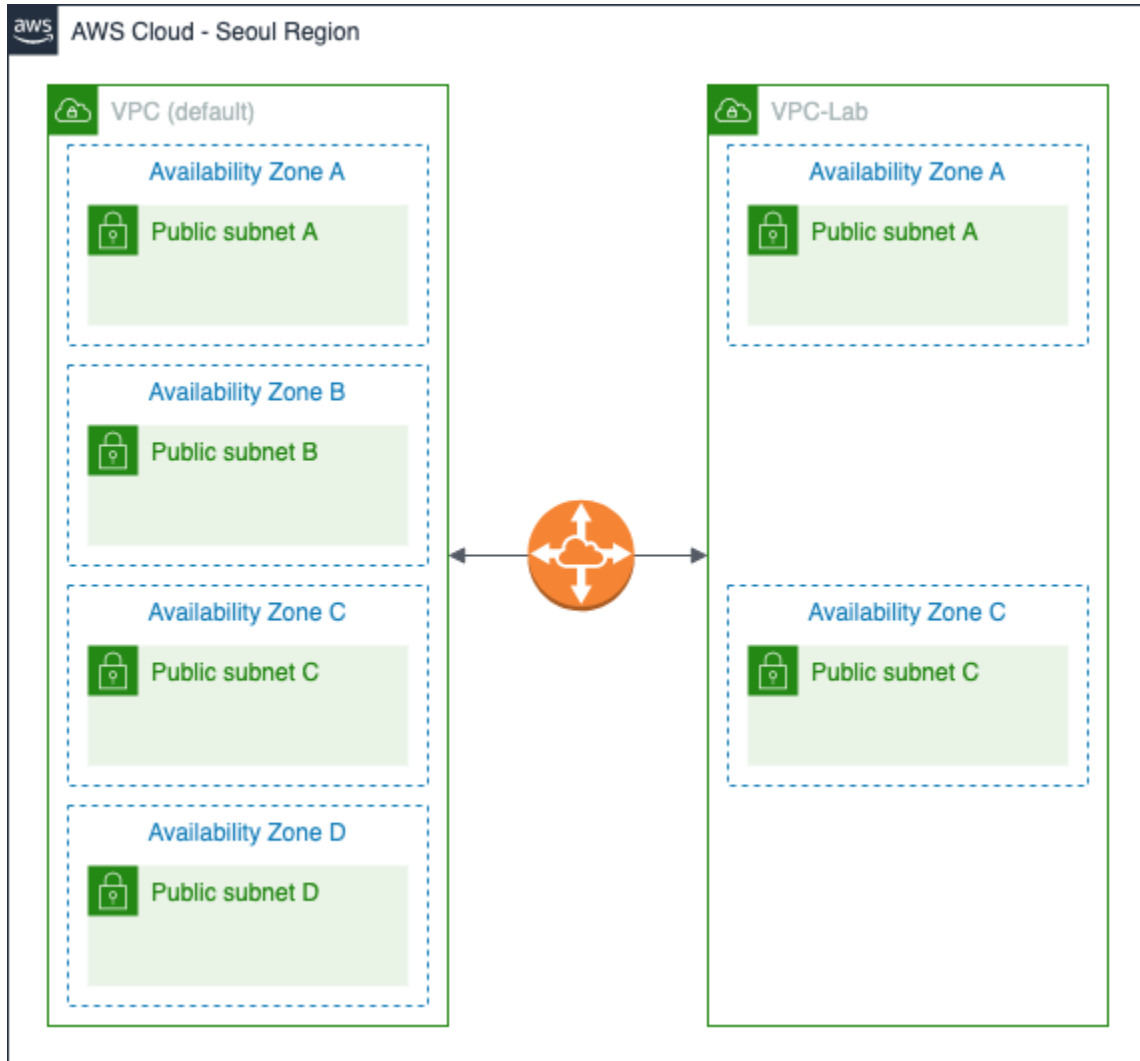
VPC 엔드포인트는 **AWS 네트워크 내부 통신**이며 엔드포인트를 통한 트래픽을 제어할 수 있다는 **보안 및 컴플라이언스**상 이점이 있습니다. 또한 NAT 게이트웨이가 아닌 VPC 엔드포인트를 통해 데이터를 전송할 경우 **데이터 처리 비용**을 최적화할 수 있습니다.

VPC Peering

Amazon Virtual Private Cloud(Amazon VPC)를 사용하면 정의한 가상 네트워크에서 AWS 리소스를 시작할 수 있습니다. VPC 피어링 연결은 프라이빗 IPv4 주소 또는 IPv6 주소를 사용하여 VPC 간에 트래픽을 라우팅할 수 있도록 하는 두 VPC 간의 네트워킹 연결입니다. 두 VPC의 인스턴스는 마치 동일한 네트워크 내에 있는 것처럼 서로 통신할 수 있습니다. 자체 VPC 간에 또는 다른 AWS 계정의 VPC와 VPC 피어링 연결을 생성할 수 있습니다. 또한 다른 리전에 있는 VPC도 연결을 생성할 수 있습니다.

주의 사항

1. 두 VPC의 CIDR에 겹치는 IP 주소 공간이 있을 수 없습니다.
2. VPC당 VPC 피어링 연결은 50개로 제한됩니다. 그러나 이 한도는 125까지 올릴 수 있습니다.



피어링 요청 생성하기

Default VPC에서 VPC 피어링 요청 생성

서비스 제공자는 NLB를 다른 VPC와 공유할 수 있도록 설정하려고 합니다. 새 엔드포인트 서비스의 이름을 명시적으로 알고 있는 경우 VPC에서 엔드포인트를 생성할 수 있는 AWS 계정을 화이트리스트에 추가할 수 있습니다. 화이트리스트를 사용하는 경우 PrivateLink가 활성화되기 전에 서비스 제공업체 측에서 명시적인 승인을 요구할 수도 있습니다.

1. **VPC 대시보드** 왼쪽 사이드바에서 **피어링 연결** 을 선택합니다 . 피어링 연결을 사용하면 다른 AWS 계정에서도 두 개의 VPC를 연결할 수 있습니다. 이번 실습에서는 로컬 리전에 초점을 맞출 것이지만 교차 리전 VPC 피어링을 생성할 수도 있습니다.
2. 기본 창에서 **피어링 연결 만들기** 버튼을 클릭합니다.
3. **피어링 연결 생성** 페이지 에서 : 연결에 **피어링 연결 이름 태그** 를 지정하고 **VPC(요청자)** 에 대해 default VPC를 선택하고 계정 및 지역을 기본값으로 유지하고 VPC-Lab을 선택합니다. **VPC(수락자)** .
4. 나열된 각각에 대한 CIDR 범위가 표시됩니다. 두 VPC 간에 겹치는 IP CIDR이 있으면 피어링이 성공하지 않습니다.

Peering connection settings

Name - *optional*

Create a tag with a key of 'Name' and a value that you specify.

DefaultToVPCLab

Select a local VPC to peer with

VPC ID (Requester)

vpc-cd23b2a6

VPC CIDRs for vpc-cd23b2a6

CIDR	Status	Status reason
172.31.0.0/16	✔ Associated	-

Select another VPC to peer with

Account

- ☒ My account
☐ Another account

Region

- ☒ This Region (ap-northeast-2)
☐ Another Region

VPC ID (Accepter)

vpc-083ad49b97c1d2bd8 (VPC-Lab)

VPC CIDRs for vpc-083ad49b97c1d2bd8 (VPC-Lab)

CIDR	Status	Status reason
10.0.0.0/16	✔ Associated	-

- 페이지 하단의 **피어링 연결 만들기** 버튼을 클릭합니다 .
- 성공 페이지가 표시되는 것을 확인합니다.

A VPC peering connection pcx-0888d8c5d1942ee7e / DefaultToVPCLab has been requested.

VPC > Peering connections > pcx-0888d8c5d1942ee7e

pcx-0888d8c5d1942ee7e / DefaultToVPCLab

Pending acceptance
You can accept or reject this peering connection request using the 'Actions' menu. You have until Thursday, March 31, 2022, 21:17:42 GMT+9 to accept or reject the request, otherwise it expires.

Details Info

Requester owner ID 846732235403	Accepter owner ID 846732235403	Peering connection ID pcx-0888d8c5d1942ee7e
Requester VPC vpc-cd23b2a6	Accepter VPC vpc-083ad49b97c1d2bd8 / VPC-Lab	Status Pending Acceptance by 846732235403
Requester CIDRs 172.31.0.0/16	Accepter CIDRs -	Expiration time Thursday, March 31, 2022, 21:17:42 GMT+9
Requester Region Seoul (ap-northeast-2)	Accepter Region Seoul (ap-northeast-2)	

DNS Route tables Tags

DNS settings Edit DNS settings

피어링 요청 수락하기

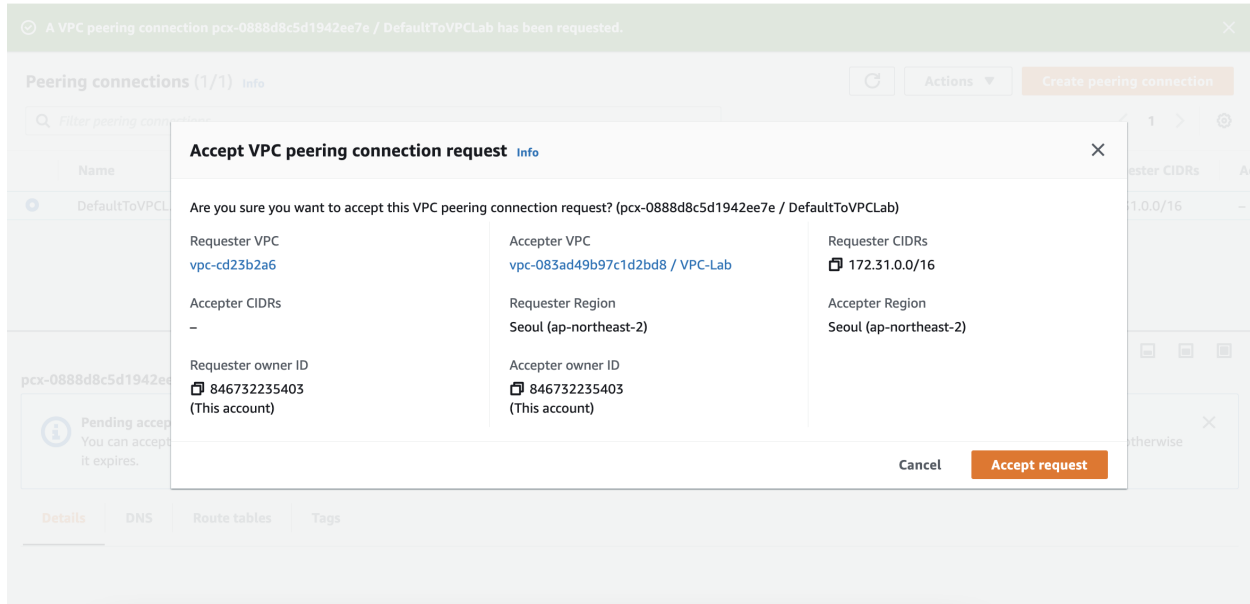
- 다시 왼쪽 사이드바에서 피어링 연결을 선택하여 생성된 요청을 확인합니다. 라인 항목 옆에 있는 상자가 선택되어 있는지 확인하고 **작업** 버튼에서 **요청 수락** 을 선택 합니다.

Peering connections (1/1) Info

Filter peering connections

Actions Create peering connection

Name	Peering connection ID	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs
DefaultToVPCLab	pcx-0888d8c5d1942ee7e	Pending acceptance	vpc-cd23b2a6	vpc-083ad49b97c1d2bd8 / VPC-Lab	172.31.0.0/16	-



2. 기본 창에서 이제 피어링 연결 라인 항목이 **상태 열에 활성** 으로 표시되어야 합니다.

Peering connections (1/1) Info							
<input type="text" value="Filter peering connections"/> 1							
Name	Peering connection ID	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs	Actions
DefaultToVPCLab	pcx-0888d8c5d1942ee7e	Active	vpc-cd23b2a6	vpc-083ad49b97c1d2bd8 / VPC-Lab	172.31.0.0/16		

피어링 라우팅 테이블 편집하기

Default VPC의 퍼블릭 서브넷에서 VPC 라우팅 구성

1. VPC 대시보드 왼쪽 사이드바에서 아래로 스크롤하여 **라우트 테이블**를 선택 합니다. 라우팅 테이블은 서브넷과 연결됩니다. 이 경우 우리는 defa 퍼블릭 서브넷과 연결된 라우팅 테이블을 수정해야 합니다.
2. 기본 창에서 이름이 지정되지 않은 default VPC와 연결된 라우트 테이블을 선택합니다.

Route tables (1/5) [Info](#)

Filter route tables

<1>

4. **작업** 버튼에서 **경로 편집** 을 선택 합니다. VPC Lab 대역인 10.0.0.0/16을 추가하도록 하겠습니다.

5. **경로 편집** 창에서 경로 추가 버튼을 클릭 하고 **다음** 항목을 추가합니다.

목적지: 10.0.0.0/16

대상: * **피어링 연결** 을 선택하고 드롭다운 목록에서 피어링 연결을 선택합니다(랩에 하나만 있어야 함)*

6. 오른쪽 하단에서 **경로 저장** 을 클릭 합니다.

VPC > Route tables > rtb-bba3fdd0 > Edit routes

Edit routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
0.0.0.0/0	igw-4630772e	Active	No Remove
10.0.0.0/16	pcx-0888d8c5d1942ee7e	-	No Remove

[Add route](#)

[Cancel](#) [Preview](#) [Save changes](#)

VPC Lab VPC의 퍼블릭 서브넷에서 VPC 라우팅 구성

default VPC에서 VPC-Lab VPC으로 향하는 라우트 경로를 추가했으니, 이제 VPC-Lab VPC 에서 default VPC로 향하는 경로를 추가할 순서입니다.

1. 왼쪽 사이드바에서 다시 **라우트 테이블**을 선택하고 VPC 열을 선택하여 VPC-Lab과 연결 된 라우트 테이블을 찾습니다. 이 중 Main이 Yes로 되어 있는 라우팅 테이블을 선택합니다.

Route tables (1/5) [Info](#)

Filter route tables

	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC
<input type="checkbox"/>	-	rtb-bba3fdd0	-	-	Yes	vpc-cd23b2a6
<input type="checkbox"/>	-	rtb-08887dc51ee321706	2 subnets	-	No	vpc-083ad49b97c1d2bd8 VPC-Lab
<input checked="" type="checkbox"/>	-	rtb-027dac6f1952c726b	-	-	Yes	vpc-083ad49b97c1d2bd8 VPC-Lab
<input type="checkbox"/>	-	rtb-0b226c509d41d79e2	-	-	Yes	vpc-07f6be73d806760f5 eksctl-eks-mlops-c...
<input type="checkbox"/>	-	rtb-05e4456dcf2a552b2	-	-	Yes	vpc-049fb57ca887240f1 eksctl-kubeflow-d...

rtb-027dac6f1952c726b

Details Routes Subnet associations Edge associations Route propagation Tags

Routes (1)

Filter routes

Both

Destination	Target	Status	Propagated
10.0.0/16	local	Active	No

3. 작업 버튼에서 **경로 편집** 을 선택 합니다. default VPC 대역인 172.31.0.0/16을 추가하도록 하겠습니다.

4. **경로 편집** 창에서 경로 추가 버튼을 클릭 하고 **다음** 항목을 추가합니다.

목적지: 172.31.0.0/16

대상: * **피어링 연결** 을 선택하고 드롭다운 목록에서 피어링 연결을 선택합니다(랩에 하나만 있어야 함)*

5. 오른쪽 하단에서 **경로 저장** 을 클릭 합니다.

VPC > Route tables > rtb-027dac6f1952c726b > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0/16	local	Active	No
172.31.0.0/16	pcx-0888d8c5d1942ee7e	-	No

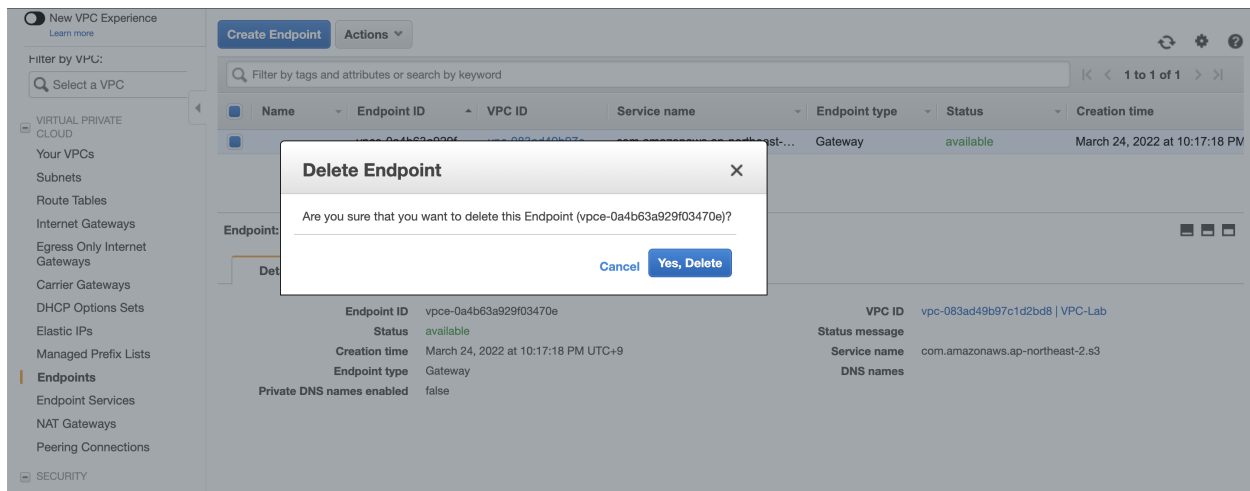
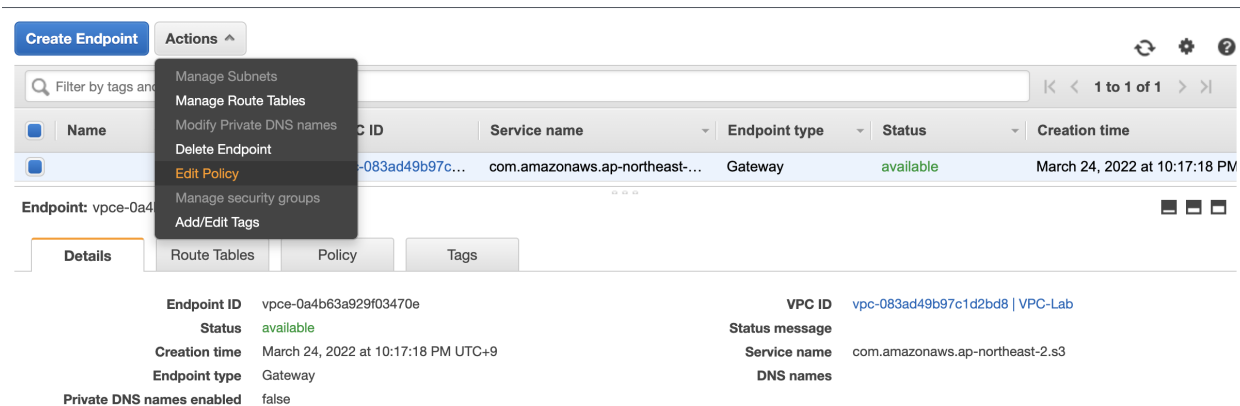
Add route

Cancel Preview Save changes

실습 리소스 정리

VPC 엔드포인트 삭제하기

1. VPC 콘솔 엔드포인트에서 오늘 생성한 엔드포인트를 선택한 후, 작업 메뉴에서 **피어링 연결 삭제**를 클릭합니다.



VPC 피어링 삭제하기

1. VPC 콘솔 피어링 연결에서 오늘 생성한 피어링 연결을 선택한 후, 작업 메뉴에서 **피어링 연결 삭제**를 클릭합니다.

Peering connections (1/1) [Info](#)

Filter peering connections

Name	Peering connection ID	Status	Requester VPC	Accepter VPC	Requester CIDRs	Accepter CIDRs
DefaultToVPCLab	pcx-0888d8c5d1942ee7e	Active	vpc-cd23b2a6	vpc-083ad49b97c1d2bd8	10.0.0.0/16	172.31.0.0/16

Actions: View details, Accept request, Reject request, Edit DNS settings, Manage tags, Delete peering connection

Create peering connection

- VPC 피어링 연결을 위한 라우트 경로를 먼저 삭제해야 하지만, 아래쪽 라우팅 테이블 항목에서 관련 라우팅 테이블 항목 삭제 옵션을 통해 라우트 경로를 삭제할 수 있습니다.

Delete peering connection

Are you sure that you want to delete this peering connection? (pcx-0888d8c5d1942ee7e / DefaultToVPCLab)

Requester VPC vpc-cd23b2a6	Accepter VPC vpc-083ad49b97c1d2bd8 / VPC-Lab
Requester Region Seoul (ap-northeast-2)	Accepter Region Seoul (ap-northeast-2)
Requester owner ID 846732235403 (This account)	Accepter owner ID 846732235403 (This account)

Routes targeting this peering connection

Route table ID	Destination
rtb-bba3fdd0	10.0.0.0/16
rtb-027dac6f1952c726b	172.31.0.0/16

Route table entries
Select whether or not to delete the entries that target this peering connection from the route tables.

☒ Delete related route table entries

☐ Do not delete route table entries

To confirm deletion, type *delete* in the field:

Cancel Delete

Peering connections (1/1) Info					
<input type="text" value="Filter peering connections"/> < 1 >					
Name	Peering connection ID	Status	Requester VPC	Accepter VPC	
DefaultToVPCL...	pcx-0888d8c5d1942ee7e	Deleted	vpc-cd23b2a6	vpc-083ad49b97c1d2bd8 / VP...	

VPC 삭제하기

VPC 콘솔 VPC 메뉴에서 오늘 생성한 VPC를 선택한 후, 작업 메뉴에서 VPC 삭제를 클릭하여 삭제합니다.

The screenshot shows the AWS VPC console interface. On the left sidebar, the 'Your VPCs' link is highlighted. The main panel displays a table of VPCs. The 'VPC-Lab' VPC is selected. The 'Actions' menu is open, and the 'Delete VPC' option is highlighted.

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR (Network border g
-	vpc-eca62a87	Available	172.31.0.0/16	-
VPC-Lab	vpc-0974345f87c196f41	Available	10.0.0.0/16	-

Delete VPC

✔ Will be deleted

This VPC will be deleted permanently and cannot be recovered later:

Name

VPC ID

State

VPC-Lab

vpc-0974345f87c196f41

✔ Available

✔ Will also be deleted

The following 6 resources will also be deleted permanently and cannot be recovered later:

Name	Resource ID	State
-	igw-069c6c48857df4966	✔ Available
-	rtb-0c21eaa1ec6cd668e	-
-	sg-02bcd4f1a9593216f	-
-	sg-0d1e6fe025b1c4a05	-
public subnet A	subnet-014aa4647ffa312b7	✔ Available
public subnet C	subnet-0f9fa61bcf22173f4	✔ Available

To confirm deletion, type *delete* in the field:

delete

Cancel

Delete

고생하셨습니다 😊

참고

- <https://kr-id-general.workshop.aws/ko/>
- <https://networking.aworkshop.io/>