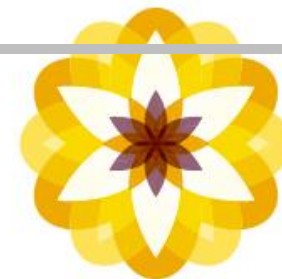
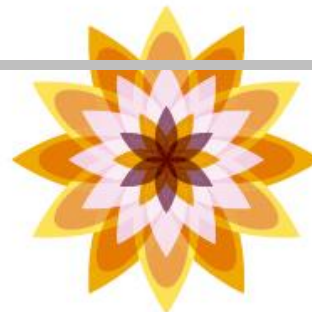


Chapter 04

독립적인 나만의 가상
네트워크 공간 만들기



1. Network

- Network는 Net(촘촘하게 연결되어 있는) + Work(일)의 합성어로 연결해서 서로가 가지고 있는 정보를 결합하여 생산적인 가치 만드는 일을 말합니다.
- 간략하게 말해서 '네트워킹을 한다 = 서로 통신(Communication)을 한다'고 할 수 있습니다.
- 서로 통신을 하기 위해서는 반드시 지켜야 하는 약속들이 있습니다.
- 예를 들어, 회사와 회사가 거래를 할 때 서로 간의 지켜야 할 조항 및 합의에 대한 내용을 담은 계약서를 작성하여 양쪽에서 교환하고 거래를 성립하는 것처럼 서로 간의 통신을 하기 위해 지켜야 하는 약속들을 준수하고, 교환함으로써 통신이 성립됩니다.
- 이렇게 통신을 위해 지켜야 하는 약속들을 프로토콜(Protocol)이라고 합니다.



2. VPN(Virtual Private Network)

- VPN은 Virtual Private Network의 약자로 큰 규모의 조직이 여러 곳에 분산되어 있는 컴퓨터들을 연결하는 보안성이 높은 사설 네트워크(Private Network)를 만들거나, 인터넷을 활용하여 원격지 간에 네트워크를 서로 연결하고 암호화 기술을 적용하여 보다 안정적이며, 보안성 높은 통신 서비스를 제공하는 서비스를 말합니다.

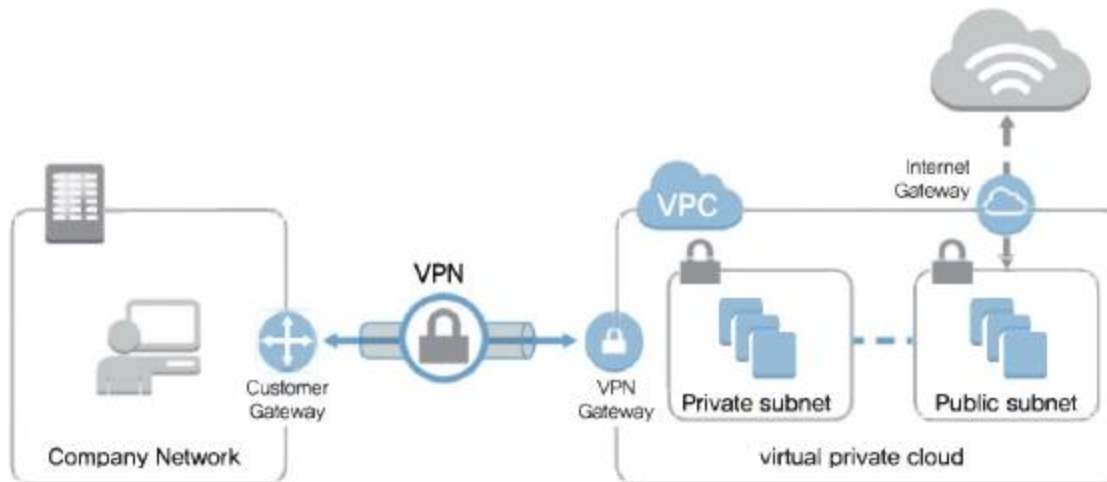


2. VPN(Virtual Private Network)

- 기존 IDC(Internet Data Center)에서 서비스하던 모든 시스템을 클라우드로 이전하는 것은 매우 어려운 일입니다.
- 이러한 경우 IDC - 클라우드 간의 네트워크 연결을 통해 기존 시스템과 클라우드 시스템 간의 데이터 통신이 필요하게 됩니다.
- Amazon Web Services는 VPC(Virtual Private Cloud)와 VPC Gateway를 통해 On-Premise의 VPN 장비와 Amazon Web Services 간의 VPN을 연결할 수 있으며, 이를 통해 보안성 높은 하이브리드 클라우드(Hybrid Cloud) 환경을 구현하여, 원활한 클라우드 컴퓨팅 서비스를 지원할 수 있습니다.

3. VPC(Virtual Private Cloud)

- Amazon VPC는 Virtual Private Cloud의 약자로 AWS 클라우드에서 논리적으로 격리된 네트워크 공간을 할당하여 가상 네트워크에서 AWS 리소스를 이용할 수 있는 서비스를 제공합니다.
- Amazon VPC 자체 IP 주소 범위, 서브넷(Subnet) 생성, 라우팅 테이블(Routing Table) 및 네트워크 게이트웨이 구성 선택 등 가상 네트워킹 환경을 완벽하게 제어할 수 있으며, VPC에서 IPv4와 IPv6를 모두 사용하여 리소스와 애플리케이션에 안전하고 쉽게 액세스할 수 있습니다.



3. VPC(Virtual Private Cloud)

- 이러한 네트워크의 구성을 손쉽게 정의할 수 있으며, 보안 그룹(Security Group) 및 네트워크 제어 목록 (Network Access Control List)을 포함한 다중 보안 계층을 활용하여 각 서브넷(Subnet)에서 EC2 인스턴스에 대한 액세스를 제어할 수 있습니다.
- 또한 기업의 데이터 센터와 VPC 사이에 하드웨어 가상 사설 네트워크 연결을 생성하여, AWS 클라우드를 기업의 데이터 센터를 확장할 것처럼 사용할 수 있습니다.

3. VPC(Virtual Private Cloud)

구분	내용
서비스명	Amazon VPC(Virtual Private Cloud)
설명	직접 정의 가능한 가상 네트워크(Private Network)에서 AWS 리소스를 구동할 수 있는 논리적으로 격리된 네트워크 제공
주요 특징	<ul style="list-style-type: none">- AWS에 사설 네트워크 구축- 회사와 AWS 간 VPN을 연결하거나 가상 네트워킹 구현- 기존 데이터 센터와의 연결을 통해 하이브리드(Hybrid) 환경 구성- AWSB 회사 인프라의 일부처럼 사용할 수 있으며, 내부 시스템 소프트웨어의 연동이 매우 쉬움(예: 메일, 그룹웨어와 같은 업무 시스템, 파일 서버 등)- 세심한 네트워크 설정 가능- 모든 리전(Region)에서 이용 가능
프리티어 (Free Tier)	VPC 자체는 비용이 발생하지 않지만, VPN 연결 시 네트워크 송/수신에 따른 종량제 비용 발생

4. VPC의 구성 요소

■ 프라이빗 IP(Private IP) 주소, 퍼블릭 IP(Public IP) 주소, 탄성 IP(Elastic IP) 주소

- 프라이빗 IP 주소는, 인터넷을 통해 연결할 수 없는, VPC 내부에서만 사용할 수 있는 IP 주소입니다.
- 프라이빗 IP는 VPC에서 시작된 인스턴스 서브넷의 범위에서 자동으로 할당되며, 동일 네트워크에서 인스턴스 간 통신에 사용할 수 있습니다.
- 기본 프라이빗 주소와 별도로 보조 프라이빗 IP 주소라는 추가 프라이빗 주소를 할당할 수 있습니다.
- 퍼블릭 IP 주소는, 인터넷을 통해 연결할 수 있는 IP 주소로, 인스턴스와 인터넷 간의 통신을 위해 사용할 수 있습니다.
- EC2 생성 시 옵션으로 퍼블릭 IP 주소의 사용 여부를 선택할 수 있으며, 인스턴스에서 퍼블릭 IP 주소를 수동으로 연결하거나 해제할 수 없습니다.
- 또한 인스턴스가 재부팅되면 새로운 퍼블릭 IP 주소가 할당됩니다.
- 탄성 IP 주소는, 동적 컴퓨팅을 위해 고안된 고정 퍼블릭 IP 주소입니다.
- VPC의 모든 인스턴스와 네트워크 인터페이스에 탄성 IP를 할당할 수 있으며, 다른 인스턴스에 주소를 신속하게 다시 매칭하여 인스턴스 장애 조치를 수행할 수도 있습니다.
- 탄력적 IP 주소의 효율적인 활용을 위해 탄력적 IP 주소가 실행 중인 인스턴스와 연결되어 있지 않거나, 중지된 인스턴스 또는 분리된 네트워크 인터페이스와 연결되어 있는 경우 시간당 요금이 부과됩니다.
- 사용 가능한 탄력적 IP 주소는 5개로 제한되며, 이를 절약하기 위해 NAT 디바이스를 사용할 수 있습니다.

4. VPC의 구성 요소

■ VPC와 서브넷 (Subnet)

- VPC는 사용자의 AWS 계정을 위한 전용의 가상 네트워크를 말합니다.
- 이러한 VPC는 AWS 클라우드에서 다른 가상 네트워크와 논리적으로 분리되어 있으며, Amazon EC2 인스턴스와 같은 AWS 리소스를 VPC에서 실행할 수 있습니다.
- VPC 내부의 네트워크에서도 서비스 목적에 따라 IP Block으로 나누어 구분할 수 있습니다.
- 우리는 이렇게 분리된 IP Block의 모음을 서브넷(Subnet)이라고 합니다.
- 우리가 흔히 알고 있는 네트워크상 서브넷과 동일한 개념입니다.
- VPC는 리전(Region)의 모든 가용 영역(Availability Zone)에 적용되며, 각 가용 영역에 하나 이상의 서브넷을 추가할 수 있습니다.
- 하지만 서브넷은 단일 가용 영역에서만 생성할 수 있으며, 여러 가용 영역으로 확장할 수 없습니다.

4. VPC의 구성 요소

■ VPC(Virtual Private Cloud)와 서브넷(Subnet)의 사이즈

- VPC를 생성할 때 VPC에서 사용하게 될 IP 주소의 범위(예: 10.0.0.0/16)를 지정하게 되는 데 범위를 CIDR(Classless Inter-Domain Routing) 블록 형태로 지정해야 합니다.
- 이때 사용하게 될 CIDR 표기법에 대해 처음 접하는 경우 어려울 수 있습니다.
- VPC를 생성하는 경우 10.0.0.0/24로 VPC를 생성하게 되면 256개의 IP 주소를 지원하게 되며, CIDR 블록을 각각 128개의 IP 주소를 지원하는 2개의 서브넷으로 나눌 수 있습니다.
- 한 서브넷은 10.0.0.0/25 CIDR(10.0.0.0-10.0.0.127)과 다른 서브넷은 10.0.0.128/25 CIDR 블록(10.0.0.128~ 10.0.0.255)을 사용하도록 구성할 수 있습니다.
- 보다 자세한 CIDR 블록 계산 방법은 네이버(Naver)나 구글(Google)을 통해 검색 및 확인할 수 있습니다.

4. VPC 의 구성 요소

■ 퍼블릭 서브넷(Public Subnet)과 프라이빗 서브넷(Private Subnet)

- 서브넷 네트워크 트래픽이 인터넷 게이트웨이(Internet Gateway, IGW)로 라우팅되는 서브넷을 퍼블릭 서브넷(Public Subnet)이라 하고, 인터넷 게이트웨이로 라우팅 되지 않는 서브넷을 프라이빗 서브넷 (Private Subnet) 이라 합니다.
- EC2 인스턴스가 IP를 통해 인터넷과 통신을 할 수 있게 하려면, 퍼블릭 IP(Public IP) 주소나 탄력적 IP(Elastic IP) 주소가 있어야 합니다.
- 일반적으로 인터넷망을 통해 서비스를 수행하는 웹 서버(Web Server)는 퍼블릭 서브넷에 생성하며, 인터넷에 직접적으로 연결할 필요가 없고, 보다 높은 보안성을 필요로 하는 DB 서버는 프라이빗 서브넷에 생성합니다.

4. VPC 의 구성 요소

■ 라우팅 테이블(Routing Table)

- 각 서브넷은 서브넷 외부로 나가는 아웃바운드(Outbound) 트래픽에 대해 허용된 경로를 지정하는 라우팅 테이블(Routing Table)이 연결되어 있어야 합니다.
- 생성된 서브넷은 자동으로 VPC의 기본 라우팅 테이블과 연결되며, 테이블의 내용을 변경할 수 있습니다.
- 이러한 라우팅 테이블은 VPC의 서브넷 내에서 생성된 네트워크 패킷이 목적지 주소로 이용하기 위해 어떤 경로로 이동되어야 하는지를 알려주는 나침반과 비슷한 개념으로 이해하면 됩니다.
- 그래서 서브넷 간의 통신이나 VPC 간의 원활한 통신을 위해 라우팅 테이블을 이용합니다.

5. VPC의 주요 서비스

■ 보안 그룹(Security Group)과 네트워크 액세스 제어 목록(Network ACL)

- VPC는 네트워크 통신과 트래픽에 대해 IP와 Port를 기준으로 통신을 허용하거나 차단하기 위한 기능을 제공합니다.
- 이러한 서비스를 보안 그룹(Security Group)과 네트워크 ACL(Network ACL)이라 합니다.
- VPC의 보안 그룹과 네트워크 ACL을 통해 AWS 상에서 방화벽과 동일한 기능을 사용할 수 있습니다.
- 보안 그룹과 네트워크 ACL의 서비스에 대한 비교는 다음과 같습니다.

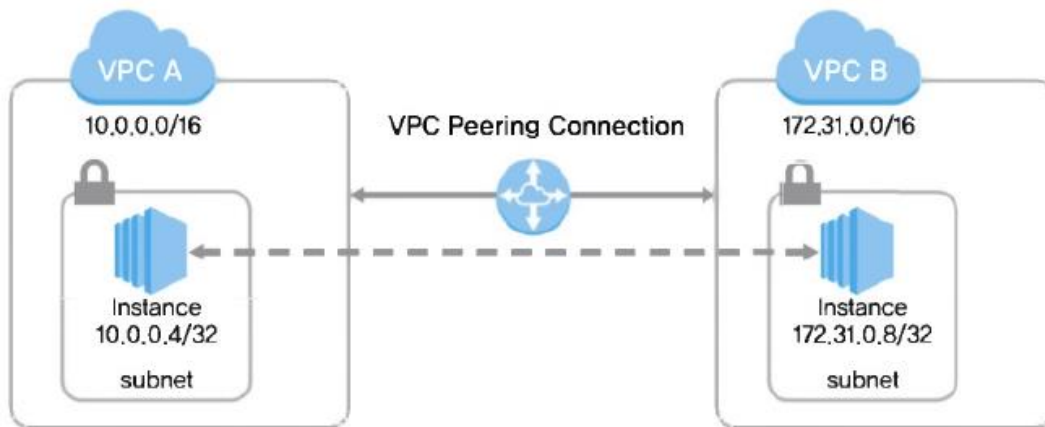
구분	보안 그룹 (Security Group)	네트워크 ACL (Network Access Control List)
서비스 범위	인스턴스 레벨(Instance Level)에 적용	서브넷 레벨(Subnet Level)에 적용
적용 정책	허용(Allow) 규칙만 적용	허용(Allow) 및 거부(Deny) 규칙 적용
구동 방식	규칙에 상관없이 반환 트래픽 허용	반환 트래픽이 별도로 허용되어야 함
룰(Rule) 검토/적용	해당 객체 내 모든 룰(Rule) 검토	해당 객체 내 룰(Rule)을 번호 순으로 처리
적용 방법	인스턴스에 보안 그룹 추가 필요	연결된 서브넷에 모든 인스턴스 자동 적용됨

- 이와 같이 보안 그룹과 네트워크 ACL은 차이가 있으므로 필요에 따라 선택적으로 적용하여 사용하는 것을 권장합니다.

5. VPC의 주요 서비스

■ VPC 피어링 연결(VPC Peering Connection)

- 피어링 연결은 비공개적으로 두 VPC 간에 트래픽을 라우팅할 수 있게 하기 위한 서로 다른 VPC 간의 네트워크 연결을 제공합니다.
- VPC Peering을 통해 동일한 네트워크에 속한 것과 같이 서로 다른 VPC의 인스턴스 간에 통신이 가능합니다.



- 일반적으로 엔터프라이즈(Enterprise) 규모의 글로벌 기업에서 전세계 임직원을 대상으로 이메일 서비스를 제공하는 경우에는 보다 빠른 메일 서비스 제공을 위해 주요 거점별로 메일 서버를 별도로 구축하고, 안전한 메일 송수신을 위해 고가의 글로벌 전용회선 서비스를 이용합니다.
- Amazon Web Services는 2017년 11월 다른 리전(Region) 간 VPC Peering 지원을 발표하였으며, 2018년 7월부터는 서울 리전을 비롯한 대부분의 리전에서 '리전 간 VPC Peering'을 제공함으로써, Amazon의 글로벌 Back Bone망을 활용하여 빠르고 보안성 높은 데이터 통신을 지원하게 되었습니다.
- 이를 통해 엔터프라이즈 기업의 글로벌 시스템을 구축하는 경우에도 저렴한 비용으로 안정성과 보안성 높은 네트워크 인프라를 활용할 수 있습니다.

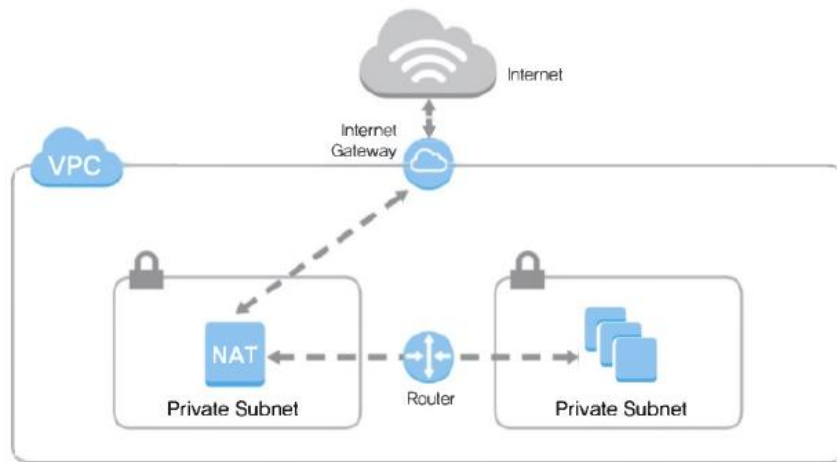
■ NAT(Network Address Translation) 게이트웨이

- NAT는 Network Address Translation의 약자로, 외부 네트워크에 알려진 것과 다른 IP 주소를 사용하는 내부 네트워크에서, 내부 IP 주소를 외부 IP 주소로 변환하는 작업을 수행하는 서비스입니다.
- NAT 게이트웨이는 프라이빗 서브넷(Private Subnet) 내에 있는 인스턴스를 인터넷(예: 소프트웨어 업데이트용) 또는 다른 AWS 서비스에 연결하고, 외부망 또는 인터넷에서 해당 인스턴스에 연결하지 못하도록 구성하는 데 사용합니다.
- 외부에 공개될 필요가 없거나, 보안상 중요한 서비스이지만 윈도우 패치나 보안 업데이트, 소프트웨어 업데이트를 인터넷을 통해 받아야 하는 경우 NAT 게이트웨이나 NAT 인스턴스(NAT Instance)를 사용하게 됩니다.

5. VPC의 주요 서비스

■ NAT(Network Address Translation) 게이트웨이

- NAT 게이트웨이를 구성하기 위해 다음 세 가지 조건을 만족해야 합니다.
 - NAT 게이트를 생성하기 위해 퍼블릭 서브넷(Public Subnet)을 지정
 - NAT 게이트웨이와 연결할 탄력적 IP(Elastic IP) 주소 필요
 - NAT 게이트웨이를 만든 후 인터넷 트래픽이 NAT 게이트웨이로 통신이 가능하도록 프라이빗 서브넷(Private Subnet)과 연결된 라우팅 테이블(Routing Table) 업데이트

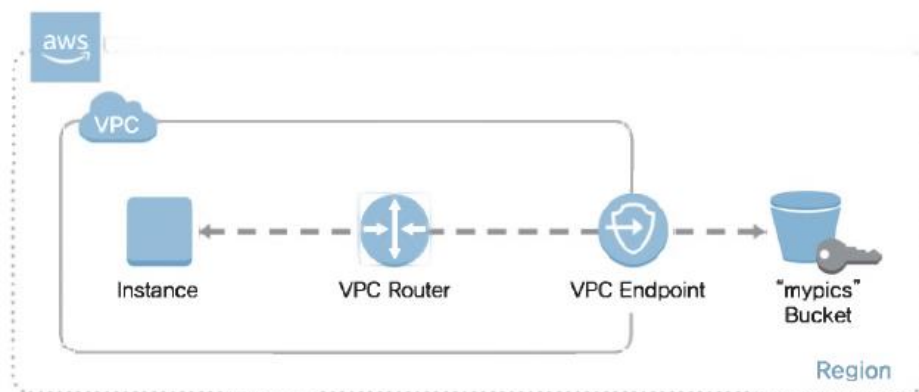


- 이와 같이 NAT 게이트웨이를 구성하면 프라이빗 서브넷(Private Subnet)의 인스턴스가 인터넷과 통신할 수 있습니다.

5. VPC의 주요 서비스

■ VPC Endpoint

- Amazon S3는 인터넷망에 연결된 서비스로 인터넷 기반의 IP 주소와 연결 정보를 가지고 있습니다.
- 이러한 공용 리소스에 대해 퍼블릭 서브넷(Public Subnet)에 위치한 인스턴스는 인터넷을 통해 문제 없이 연결 가능합니다.
- 하지만 프라이빗 서브넷(Private Subnet)에 위치한 인스턴스는 인터넷과 연결되어 있는 S3와 같은 공용 리소스를 연결할 수 없습니다.

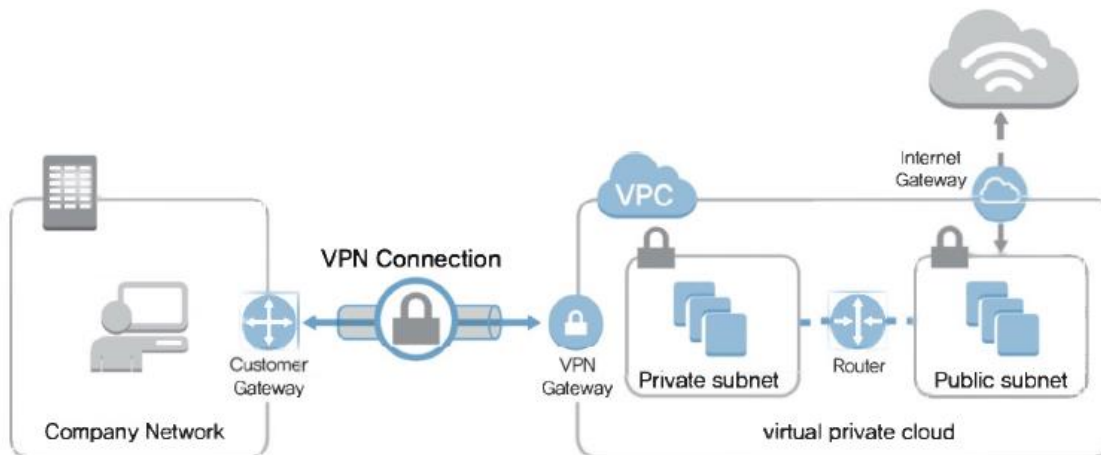


- 이러한 경우 S3에 연결하기 위해서는 NAT 게이트웨이나 NAT 인스턴스가 필요합니다.
- 하지만 VPC Endpoint# 이용하면 빠르고 손쉽게 S3, DynamoDB에 연결할 수 있습니다.

5. VPC의 주요 서비스

■ VPN(Virtual Private Network) 연결

- 기본적으로 Amazon VPC에서 서비스되는 인스턴스는 On-Premise에 있는 서버나 IDC 내의 시스템과 통신할 수 없습니다.
- 물론 인터넷을 통해 강제로 통신하도록 구성할 수 있으나, 보안을 필요로 하는 중요한 데이터를 송수신하기에는 보안적으로 매우 취약합니다.



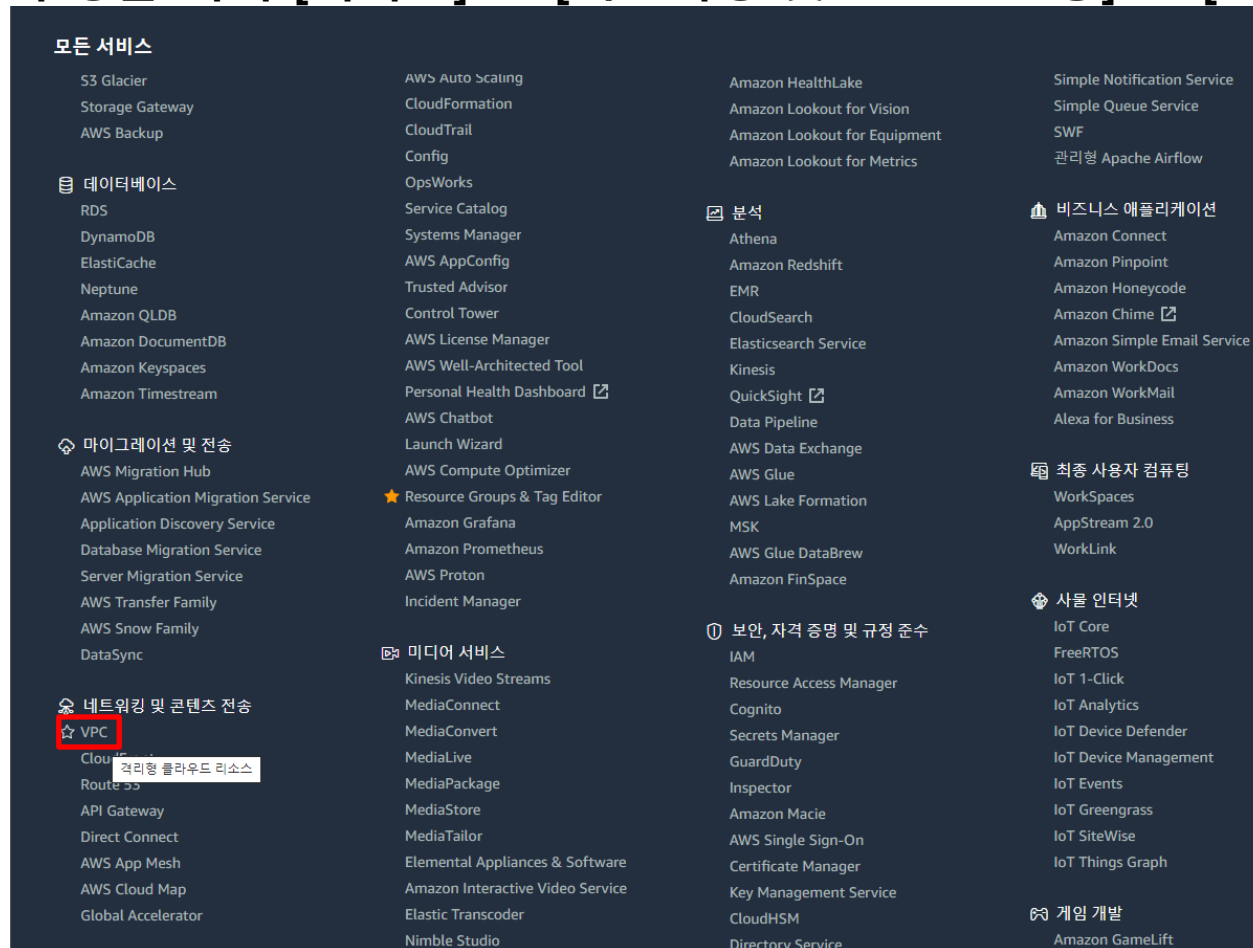
- 이렇게 AWS VPC 내 인스턴스와 IDC 내 시스템 간의 데이터 통신을 위해 VPC에 가상의 프라이빗 (Private) 게이트웨이를 연결하고 사용자 지정 라우팅 테이블을 생성하며, 보안 그룹의 규칙을 업데이트하고, AWS 관리형 VPN 연결을 생성하여 VPC에서 원격의 네트워크에 접속 가능하도록 하이브리드 클라우드(Hybrid Cloud) 환경을 구성할 수 있습니다.
- VPN 연결은 VPC와 자체 네트워크 사이의 연결을 의미합니다.

6. 실습 : VPC 마법사를 통해 퍼블릭 서브넷(Public Subnet)과 프라이빗 서브넷(Private Subnet) 만들기

- 마법사를 사용하여 Amazon VPC(Virtual Private Cloud)를 구성하고 퍼블릭 서브넷과 프라이빗 서브넷을 생성하여 NAT 게이트웨이를 통해 프라이빗 인스턴스가 인터넷에 연결되도록 실습을 진행합니다.
- Amazon VPC는 비용이 발생하지 않습니다.
- 다만 VPC 외부로 데이터를 송신하는 경우 사용량에 비례하여 Outbound 트래픽에 대한 비용이 발생하게 됩니다.

6. 실습 : VPC 마법사를 통해 퍼블릭 서브넷(Public Subnet)과 프라이빗 서브넷(Private Subnet) 만들기

- 웹 브라우저를 열고 <http://aws.amazon.com>에 접속 후 본인의 AWS 계정으로 로그인합니다.
- VPC 구성을 위해 [서비스] → [네트워킹 및 콘텐츠 전송] → [VPC]로 이동합니다



6. 실습 : VPC 마법사를 통해 퍼블릭 서브넷(Public Subnet)과 프라이빗 서브넷(Private Subnet) 만들기

- NAT 게이트웨이에 사용할 탄력적 IP 할당을 위해 [탄력적 IP]로 이동하여 [탄력적 IP 주소 할당] 버튼을 클릭합니다.

The screenshot shows the AWS Management Console interface. On the left sidebar, the '탄력적 IP' (Elastic IP) option is highlighted with a red box. The main content area displays the '탄력적 IP 주소' (Elastic IP address) console. At the top right of this console, the '탄력적 IP 주소 할당' (Allocate Elastic IP address) button is highlighted with a red box. The console shows a table with columns for Name, 할당된 IPv4 주소 (Allocated IPv4 address), 유형 (Type), 할당 ID (Allocation ID), 연결된 인스턴스 ID (Associated instance ID), 프라이빗 IP 주소 (Private IP address), 연결 ID (Association ID), and 네트워크 인터페이스 소유자 계정 ID (Network interface owner account ID). The table is currently empty, with a message below it stating '이 리전에서 탄력적 IP 주소를 찾을 수 없음' (No Elastic IP addresses found in this region).

6. 실습 : VPC 마법사를 통해 퍼블릭 서브넷(Public Subnet)과 프라이빗 서브넷(Private Subnet) 만들기

- [탄력적 IP 주소 할당] 페이지에서 [할당] 버튼을 클릭합니다.

VPC > 탄력적 IP 주소 > 탄력적 IP 주소 할당

탄력적 IP 주소 할당 Info

탄력적 IP 주소 설정 Info

퍼블릭 IPv4 주소 풀

- ☒ Amazon의 IPv4 주소 풀
- ☐ AWS 계정으로 가져오는 퍼블릭 IPv4 주소 (풀을 찾을 수 없으므로 옵션이 비활성화됨) [자세히 알아보기](#)
- ☐ IPv4 주소의 고객 소유 풀 (고객 소유 풀을 찾을 수 없기 때문에 옵션이 비활성화됨) [자세히 알아보기](#)

글로벌 정적 IP 주소

AWS Global Accelerator는 AWS 엣지 로케이션의 애니캐스트를 사용하여 전 세계에 배포된 글로벌 정적 IP 주소를 제공할 수 있습니다. 이를 통해 Amazon 글로벌 네트워크를 사용하여 사용자 트래픽의 가용성과 지연 시간을 개선할 수 있습니다. [자세히 알아보기](#)

[액셀러레이터 생성](#)

태그 - 선택 사항

태그는 사용자가 AWS 리소스에 할당하는 레이블입니다. 각 태그는 키와 값(선택 사항)으로 구성됩니다. 태그를 사용하여 리소스를 검색 및 필터링하거나 AWS 비용을 추적할 수 있습니다.

리소스에 연결된 태그가 없습니다.

[새로운 태그 추가](#)

최대 50개의 태그를 더 추가할 수 있습니다.

[취소](#) [할당](#)

6. 실습 : VPC 마법사를 통해 퍼블릭 서브넷(Public Subnet)과 프라이빗 서브넷(Private Subnet) 만들기

■ 상단 [VPC 대시보드]에서 [VPC 마법사 시작] 버튼을 클릭합니다.

The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with the AWS logo and a search bar. Below the navigation bar, there's a header section with two buttons: 'VPC 마법사 시작' (highlighted with a red box) and 'EC2 인스턴스 시작'. Below this, there's a section titled '리전별 리소스' (Resources by Region) with a sub-header '리소스 새로 고침' (Refresh Resources). Below this, there's a message: '다음 Amazon VPC 리소스를 사용하고 있습니다.' (Using the following Amazon VPC resources). Below this, there's a grid of resource cards showing the following resources and their counts:

Resource	Count
VPC	1
NAT 게이트웨이	0
서브넷	3
VPC 피어링 연결	0
라우팅 테이블	1
네트워크 ACL	1
인터넷 게이트웨이	1
보안 그룹	4
외부 전용 인터넷 게이트웨이	0
고객 게이트웨이	0

6. 실습 : VPC 마법사를 통해 퍼블릭 서브넷(Public Subnet)과 프라이빗 서브넷(Private Subnet) 만들기

- [1 단계 : VPC 구성 선택] 페이지에서 [퍼블릭 및 프라이빗 서브넷이 있는 VPC]의 [선택] 버튼을 클릭합니다.

 서비스 ▼

서비스, 가

1단계: VPC 구성 선택

단일 퍼블릭 서브넷이 있는 VPC

퍼블릭 및 프라이빗 서브넷이 있는 VPC

퍼블릭 및 프라이빗 서브넷이 있고 하드웨어 VPN 액세스를 제공하는 VPC

프라이빗 서브넷만 있고 하드웨어 VPN 액세스를 제공하는 VPC

이 구성은 퍼블릭 서브넷을 포함하는 이외에 인터넷에서 인스턴스의 주소를 지정할 수 없는 프라이빗 서브넷을 추가합니다. 프라이빗 서브넷의 인스턴스는 NAT(Network Address Translation)를 사용하는 퍼블릭 서브넷을 통해 인터넷과 아웃바운드 연결을 설정할 수 있습니다.

생성:

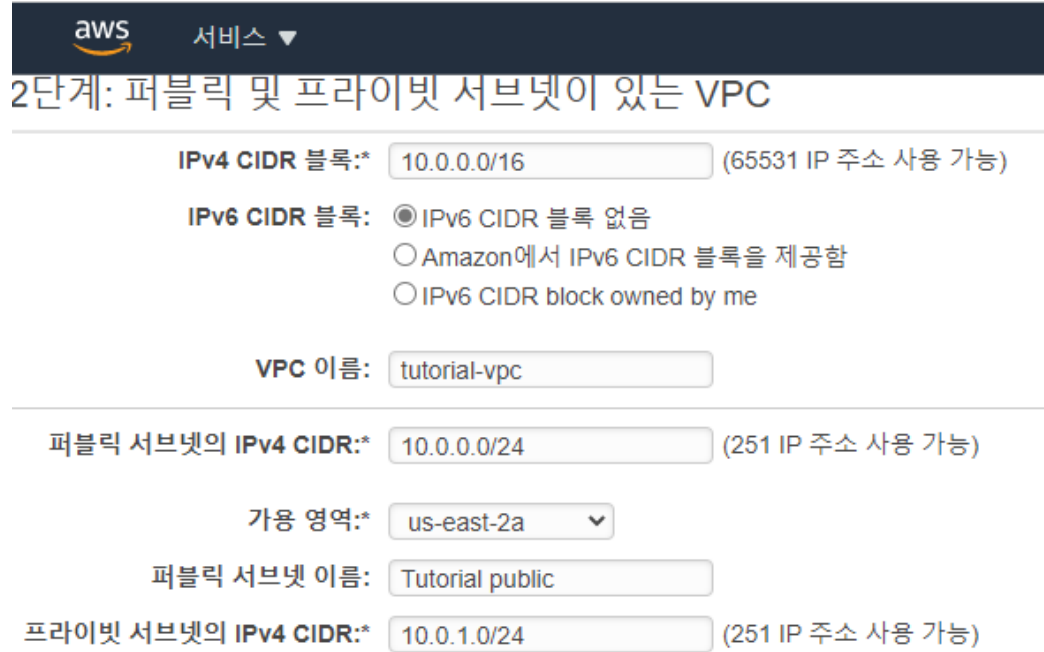
2개의 /24 서브넷이 있는 /16 네트워크입니다. 퍼블릭 서브넷 인스턴스는 인터넷을 액세스하기 위해 탄력적 IP를 사용합니다. 프라이빗 서브넷 인스턴스는 NAT(Network Address Translation)을 통해 인터넷을 액세스합니다. (NAT 디바이스에 대한 시간당 요금이 적용됩니다.)

선택



6. 실습 : VPC 마법사를 통해 퍼블릭 서브넷(Public Subnet)과 프라이빗 서브넷(Private Subnet) 만들기

- VPC 구성을 위해 다음과 같이 입력 후 [VPC 만들기] 버튼을 클릭해서 VPC를 생성합니다.



The image shows the AWS VPC creation wizard interface. At the top, there's a dark blue header with the AWS logo and a '서비스' (Services) dropdown. Below the header, the title '2단계: 퍼블릭 및 프라이빗 서브넷이 있는 VPC' (Step 2: VPC with public and private subnets) is displayed. The form contains several input fields and radio buttons. The 'IPv4 CIDR 블록' (IPv4 CIDR block) is set to '10.0.0.0/16' with a note '(65531 IP 주소 사용 가능)'. The 'IPv6 CIDR 블록' (IPv6 CIDR block) section has three options: 'IPv6 CIDR 블록 없음' (selected), 'Amazon에서 IPv6 CIDR 블록을 제공함', and 'IPv6 CIDR block owned by me'. The 'VPC 이름' (VPC name) is 'tutorial-vpc'. The '퍼블릭 서브넷의 IPv4 CIDR' (Public subnet IPv4 CIDR) is '10.0.0.0/24' with a note '(251 IP 주소 사용 가능)'. The '가용 영역' (Availability zone) is 'us-east-2a'. The '퍼블릭 서브넷 이름' (Public subnet name) is 'Tutorial public'. The '프라이빗 서브넷의 IPv4 CIDR' (Private subnet IPv4 CIDR) is '10.0.1.0/24' with a note '(251 IP 주소 사용 가능)'.

aws 서비스 ▼

2단계: 퍼블릭 및 프라이빗 서브넷이 있는 VPC

IPv4 CIDR 블록:* 10.0.0.0/16 (65531 IP 주소 사용 가능)

IPv6 CIDR 블록: ☒ IPv6 CIDR 블록 없음
☐ Amazon에서 IPv6 CIDR 블록을 제공함
☐ IPv6 CIDR block owned by me

VPC 이름: tutorial-vpc

퍼블릭 서브넷의 IPv4 CIDR:* 10.0.0.0/24 (251 IP 주소 사용 가능)

가용 영역:* us-east-2a ▼

퍼블릭 서브넷 이름: Tutorial public

프라이빗 서브넷의 IPv4 CIDR:* 10.0.1.0/24 (251 IP 주소 사용 가능)

- IPv4 CIDR 블록 : 10.0.0.0/16
- VPC 이름: tutorial-vpc
- 퍼블릭 서브넷의 IPv4 CIDR : 10.0.0.0/24
- 가용 영역 : us-east-2a
- 퍼블릭 서브넷 이름 : Tutorial public
- 프라이빗 서브넷의 IPv4 CIDR : 10.0.1.0/24

6. 실습 : VPC 마법사를 통해 퍼블릭 서브넷(Public Subnet)과 프라이빗 서브넷(Private Subnet) 만들기

- VPC 구성을 위해 다음과 같이 입력 후 [VPC 만들기] 버튼을 클릭해서 VPC를 생성합니다.

가용 영역:*

프라이빗 서브넷 이름:

AWS가 VPC를 생성한 후 더 많은 서브넷을 추가할 수 있습니다.

NAT 게이트웨이의 세부 정보를 지정합니다([NAT 게이트웨이 속도 적용](#)).

탄력적 IP 할당 ID:*

서비스 엔드포인트

DNS 호스트 이름 활성화:* ☒ 예 ☐ 아니요

하드웨어 테넌시:*

- 가용 영역 : us-east-2a
- 프라이빗 서브넷 이름: Tutorial Private 1
- NAT 게이트웨이의 세부 정보를 지정합니다 : 대신 NAT 게이트웨이 사용
- 탄력적 IP 할당 ID : 이전에 선택한 탄력적 IP 선택
- DNS 호스트 이름 활성화 : 예
- 하드웨어 테넌시 : 기본값

6. 실습 : VPC 마법사를 통해 퍼블릭 서브넷(Public Subnet)과 프라이빗 서브넷(Private Subnet) 만들기

- VPC 구성을 위해 다음과 같이 입력 후 [VPC 만들기] 버튼을 클릭해서 VPC를 생성합니다.

2단계: 퍼블릭 및 프라이빗 서브넷이 있는 VPC

IPv4 CIDR 블록:*

10.0.0.0/16

(65531 IP 주소 사용 가능)

IPv6 CIDR 블록:

☒ IPv6 CIDR 블록 없음

☐ Amazon에서 IPv6 CIDR 블록을 제공함

☐ IPv6 CIDR block owned by me

VPC 이름:

tutorial-vpc

퍼블릭 서브넷의 IPv4 CIDR:*

10.0.0.0/24

(251 IP 주소 사용 가능)

가용 영역:*

us-east-2a

퍼블릭 서브넷 이름:

Tutorial public

프라이빗 서브넷의 IPv4 CIDR:*

10.0.1.0/24

(251 IP 주소 사용 가능)

가용 영역:*

us-east-2a

프라이빗 서브넷 이름:

Tutorial Private 1

AWS가 VPC를 생성한 후 더 많은 서브넷을 추가할 수 있습니다.

NAT 게이트웨이의 세부 정보를 지정합니다(NAT 게이트웨이 속도 적용).

탄력적 IP 할당 ID:*

elipalloc-0015b93a79fbf9dda

서비스 엔드포인트

엔드포인트 추가

DNS 호스트 이름 활성화:*

☒ 예 ☐ 아니요

하드웨어 태넌시:*

기본값

취소 및 종료

뒤로

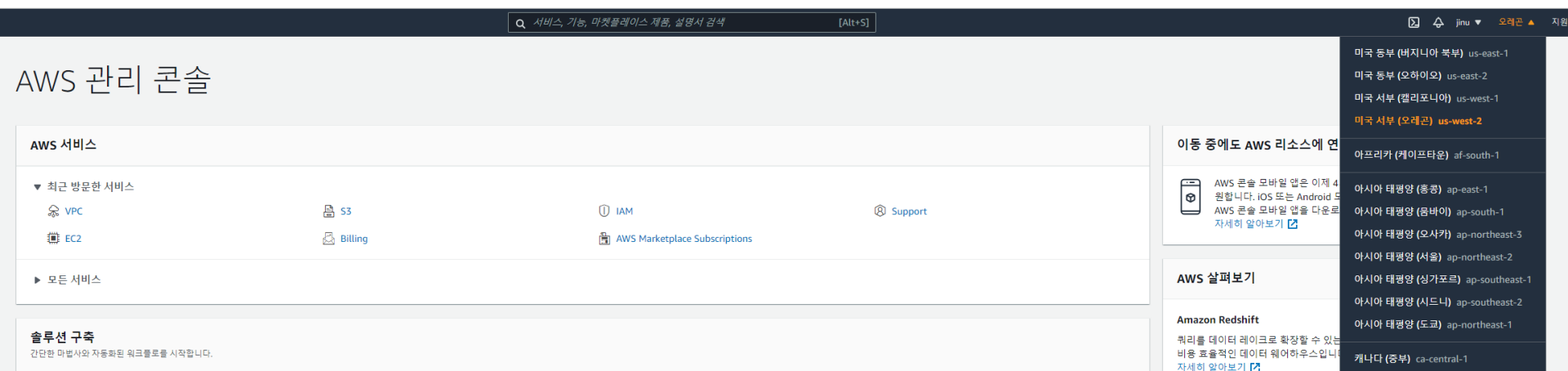
VPC 생성

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

- Inter-Region VPC Peering을 테스트하기 위해 오레곤 리전에 VPC를 만들고, 오아이오 리전과 오레곤 리전 간에 VPC Peering을 수행한 후 각 리전 간 네트워크가 정상적으로 연결되는지 확인합니다.
- 본 실습은 네트워크 테스트를 위해 각각의 리전에 EC2 인스턴스를 생성하게 됩니다.
- 실습 후 생성된 인스턴스를 삭제하면 프리티어(Free Tier) 범위 내에서 추가적인 비용이 발생하지 않을 것입니다.
- 각 리전에 생성된 EC2 인스턴스는 실습 이후 삭제하기 바랍니다.

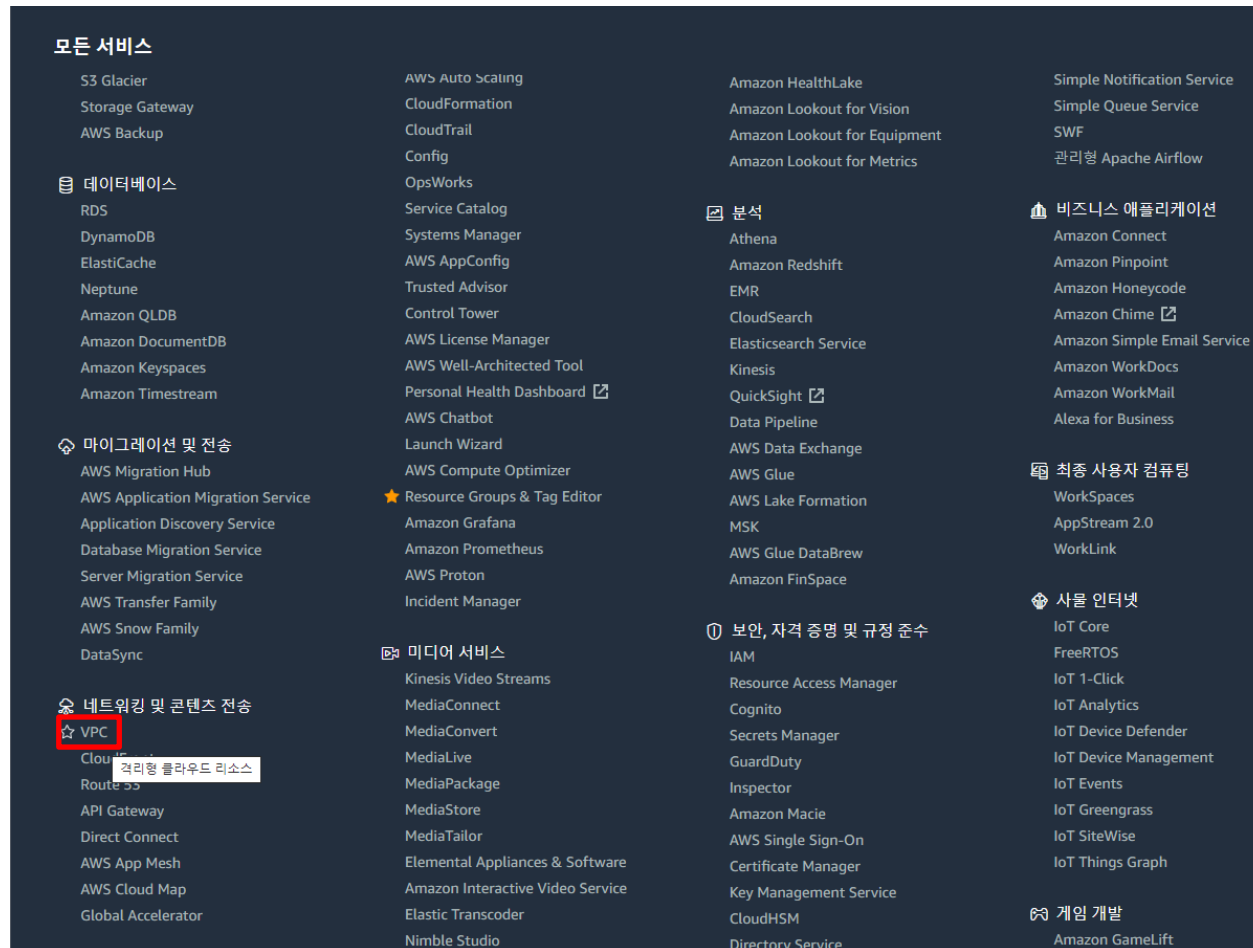
7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

- 웹 브라우저를 열고 <http://aws.amazon.com>에 접속 후 본인의 AWS 계정으로 로그인합니다.
- 오레곤 리전에 VPC 구성을 구성하기 위해 오른쪽 상단의 [리전 선택] 항목에서 “미국 서부(오레곤)” 리전을 클릭합니다.



7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

■ [서비스] → [네트워킹 및 콘텐츠 전송] → [VPC]를 클릭하여 VPC로 이동합니다.



7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기


- [VPC] 페이지에서 [VPC 만들기] 버튼을 눌러 [VPC 마법사 시작] 버튼을 클릭합니다.

The screenshot shows the AWS Management Console interface for the VPC service. On the left, there is a navigation pane with the 'VPC 대시보드' (VPC Dashboard) selected. The main content area displays two buttons at the top: 'VPC 마법사 시작' (Start VPC Wizard) and 'EC2 인스턴스 시작' (Start EC2 Instance). Below these buttons, a message states '참고: 인스턴스는 유럽(런던) 리전에서 시작됩니다.' (Note: Instances start in the Europe (London) region). The '리전별 리소스' (Resources by Region) section shows a table of resources. The 'VPC 마법사 시작' button is highlighted with a red box.

리전별 리소스	리소스 새로 고침
다음 Amazon VPC 리소스를 사용하고 있습니다.	
VPC 모든 리전 보기 ▼	런던 1
서브넷 모든 리전 보기 ▼	런던 3
라우팅 테이블 모든 리전 보기 ▼	런던 1
인터넷 게이트웨이 모든 리전 보기 ▼	런던 1

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

- [VPC 구성 선택] 페이지에서 “단일 퍼블릭 서브넷이 있는 VPC”를 선택 후 [선택] 버튼을 클릭합니다.

 서비스 ▼

1단계: VPC 구성 선택

단일 퍼블릭 서브넷이 있는 VPC

퍼블릭 및 프라이빗 서브넷이 있는 VPC

퍼블릭 및 프라이빗 서브넷이 있고 하드웨어 VPN 액세스를 제공하는 VPC

프라이빗 서브넷만 있고 하드웨어 VPN 액세스를 제공하는 VPC

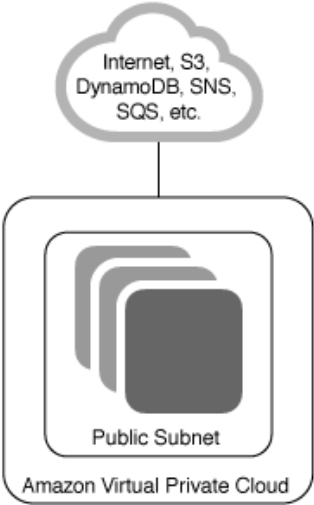
고객의 인스턴스는 AWS 클라우드의 프라이빗 격리 섹션에서 실행되며 인터넷에 직접 액세스합니다. 네트워크 액세스 제어 목록 및 보안 그룹을 사용하여 인스턴스를 드나드는 인바운드 및 아웃바운드 네트워크 트래픽을 엄격히 제어할 수 있습니다.

생성:

/24 서브넷이 있는 /16 네트워크입니다. 퍼블릭 서브넷 인스턴스는 인터넷을 액세스하기 위해 탄력적 IP 또는 퍼블릭 IP를 사용합니다.

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

선택



Internet, S3, DynamoDB, SNS, SQS, etc.

Public Subnet

Amazon Virtual Private Cloud

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

■ VPC 구성을 위해 다음과 같이 입력합니다.

- IPv4 CIDR 블록 : 20.0.0.0/16
- VPC 이름 : tutorial-VPC-Oregon
- 퍼블릭 서브넷의 IPv4 CIDR : 20.0.0.0/24
- 가용 영역 : us-west-2a
- 서브넷 이름 : Tutorial public Oregon

aws 서비스 ▼

2단계: 단일 퍼블릭 서브넷이 있는 VPC

IPv4 CIDR 블록:* 20.0.0.0/16 (65531 IP 주소 사용 가능)

IPv6 CIDR 블록: ☒ IPv6 CIDR 블록 없음
☐ Amazon에서 IPv6 CIDR 블록을 제공함
☐ IPv6 CIDR block owned by me

VPC 이름: tutorial-VPC-Oregon

퍼블릭 서브넷의 IPv4 CIDR:* 20.0.0.0/24 (251 IP 주소 사용 가능)

가용 영역:* us-west-2a ▼

서브넷 이름: Tutorial public Oregon

AWS가 VPC를 생성한 후 더 많은 서브넷을 추가할 수 있습니다.

서비스 엔드포인트

엔드포인트 추가

DNS 호스트 이름 활성화:* ☒ 예 ☐ 아니요

하드웨어 테넌시:* 기본값 ▼

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

- 피어링 구성을 위해 리전을 다시 “미국 동부(오하이오)”로 전환 후 VPC로 이동합니다.

서비스 상태

현재 상태	세부 정보
Amazon EC2 - 미국 동부(오하이오)	서비스가 정상적으로 작동 중입니다.

전체 서비스 상태 세부 정보 보기

설정

영역
콘솔 실험

추가 정보

VPC 설명서
모든 VPC 리소스
포럼
문제 보고

Transit Gateway 네트워크 관리자

네트워크 관리자를 사용하면 AWS와 온프레미스의 전체 네트워크를 중앙에서 관리할 수 있습니다. 자세히 보기
네트워크 관리자 시작하기

사이트 간 VPN 연결

Amazon VPC를 통해 AWS 클라우드 내에서 자신만의 격리된 리소스를 사용한 다음 업계 표준 암호화 방식의 데이터 센터에 직접 연결할 수 있습니다.

미국 동부 (버지니아 북부) us-east-1

미국 동부 (오하이오) **us-east-2**

미국 서부 (캘리포니아) us-west-1

미국 서부 (오레곤) us-west-2

아프리카 (케이프타운) af-south-1

아시아 태평양 (홍콩) ap-east-1

아시아 태평양 (뮌헨) ap-south-1

아시아 태평양 (오사카) ap-northeast-3

아시아 태평양 (서울) ap-northeast-2

아시아 태평양 (싱가포르) ap-southeast-1

아시아 태평양 (시드니) ap-southeast-2

아시아 태평양 (도쿄) ap-northeast-1

캐나다 (중부) ca-central-1

유럽 (프랑크푸르트) eu-central-1

유럽 (아일랜드) eu-west-1

유럽 (런던) eu-west-2

유럽 (밀라노) eu-south-1

유럽 (파리) eu-west-3

유럽 (스톡홀름) eu-north-1

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

IT COOKBOOK

- [피어링 연결] 메뉴를 눌러 피어링 페이지로 이동 후 [피어링 연결 생성] 버튼을 클릭합니다.

The screenshot displays the AWS Management Console interface. On the left-hand navigation pane, the '가상 프라이빗 클라우드' (Virtual Private Cloud) section is expanded, and the '피어링 연결' (Peering connection) option is highlighted with a red rectangular box. The main content area shows a message indicating that no peering connections exist for the current region. Below this message, the '피어링 연결 생성' (Create VPC Peering Connection) button is highlighted with a red rectangular box. The top of the console shows the AWS logo, the '서비스' (Services) dropdown, and a search bar.

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

■ [피어링 연결 생성] 페이지에서 다음과 같이 구성을 진행 후 [피어링 연결 생성] 버튼을 클릭합니다.

- 피어링 연결 이름 태그 : Oaio-Oregon VPC Peering
- 피어링할 로컬 VPC 선택 - VPC (요청자) : tutorial-vpc
- 피어링할 다른 VPC 선택 - 계정 : 내 계정
- 피어링할 다른 VPC 선택 - 리전 : 다른 리전 - 오레곤(us-west-2)
- 피어링할 다른 VPC 선택 - VPC(수락자): 신규로 생성한 VPC ID

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통

합

aws 서비스 ▾

🔍 서비스, 기능, 마켓플레이스 제품, 설명서 검색

IT COOKBOOK

피어링 연결 > 피어링 연결 생성

피어링 연결 생성

결 생성]

피어링 연결 Name 태그 Oaio-Oregon VPC Peering ⓘ

피어링할 로컬 VPC 선택

VPC(요청자)* vpc-07bcb655120ee59aa ▾ C

CIDR	CIDR	상태	상태 사유
	10.0.0.0/16	● associated	

피어링할 다른 VPC 선택

계정 ☒ 내 계정
☐ 다른 계정

리전 ☐ 현재 리전 (us-east-2)
☒ 다른 리전

미국 서부(오레곤) (us-west-2) ▾ C

VPC ID(수락자)* vpc-0c1d9215afacd259f

Tags

키 (최대 127자)

값 (최대 255자)

이 리소스에는 현재 태그가 없습니다.

태그 추가 50개 남음 (최대 50개 태그)

* 필수 사항

취소 **피어링 연결 생성**

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

IT COOKBOOK

- VPC 연결이 정상적으로 생성되었습니다.
- 이후 피어링 연결 승인을 위해 오레곤 리전으로 이동합니다.

aws 서비스 ▼



피어링 연결 > 피어링 연결 생성

피어링 연결 생성



성공

VPC 피어링 연결(pcx-0b961221198715565)이 요청되었습니다.
피어링 연결을 수락하려면 리전을 **us-west-2**(으)로 변경해야 합니다.

요청자 VPC 소유자	262663767358 (현재 계정)
요청자 VPC ID	vpc-07bcb655120ee59aa
요청자 VPC 리전	us-east-2
요청자 VPC CIDR	10.0.0.0/16

수락자 VPC 소유자	262663767358 (현재 계정)
수락자 VPC ID	vpc-0c1d9215afacd259f
수락자 VPC 리전	us-west-2
수락자 VPC CIDR	-

확인

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

- 오레곤 리전으로 이동 후 [피어링 연결] 버튼을 눌러 수락 대기 중인 피어링 연결 요청을 확인합니다.

aws

서비스 ▼

새 서비스, 기능, 마켓플레이스 제품, 설명서 검색

[Alt+S]

New VPC Experience

Tell us what you think

VPC 대시보드

VPC로 필터링:

VPC 선택

가상 프라이빗 클라우드

VPC

서브넷

라우팅 테이블 New

인터넷 게이트웨이

외부 전용 인터넷 게이트웨이

캐리어 게이트웨이

DHCP 옵션 세트

탄력적 IP

관리형 접두사 목록

엔드포인트

엔드포인트 서비스 New

NAT 게이트웨이

피어링 연결

피어링 연결 생성

작업 ▼

태그 및 속성별 필터 또는 키워드별 검색

Name	피어링 연결	상태	요청자 VPC	수락자 VPC	요청자 CIDR	수락자 CIDR	요청자 소유자	수락자 소유자
pcx-0fbc8c883a86...		수락 대기 중	vpc-07bcb655120...	vpc-0ce0ce41628...	10.0.0.0/16	-	262663767358	262663767358

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

- [피어링 연결] 페이지에서 [작업]의 [요청 수락]을 클릭합니다.

The screenshot shows the AWS Management Console interface for VPC Peering Connections. The left sidebar contains navigation links for 'VPC 대시보드' and 'VPC로 필터링: VPC 선택'. The main content area has tabs for '피어링 연결 생성' and '작업'. A dropdown menu is open under the '작업' tab, showing options: '요청 수락' (highlighted), '요청 거부', 'VPC 피어링 연결 삭제', 'DNS 설정 편집', and '태그 추가/편집'. Below the menu is a table of VPC Peering Connections. The table has columns for 'Name', '상태' (Status), and '요청자 VPC' (Requesting VPC). One connection is listed with the status '수락 대기 중' (Pending Acceptance) and ID 'vpc-07bcb655120...'.

Name	상태	요청자 VPC
	수락 대기 중	vpc-07bcb655120...

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

- [VPC 피어링 연결 요청 수락] 페이지에서 [예, 수락] 버튼을 클릭합니다.
- 이후 VPC간의 연결 후 Network 통신을 위해 양쪽 VPC간에 라우팅 처리가 필요합니다.
- 이를 위해 기존 "라우팅 테이블"을 수정해 주어야 합니다.
- 이를 위해 다음의 작업을 수행합니다.

VPC 피어링 연결 요청 수락



이 VPC 피어링 연결 요청(pcx-0fbc8c883a86e052e)을(를) 수락하시겠습니까?

요청자 계정 ID	262663767358 (현재 계정)
요청자 VPC ID	vpc-07bcb655120ee59aa
요청자 VPC 리전	us-east-2
요청자 VPC CIDR	10.0.0.0/16

수락자 계정 ID	262663767358 (현재 계정)
수락자 VPC ID	vpc-0ce0ce41628d7ff6c
수락자 VPC 리전	eu-west-2
수락자 VPC CIDR	-

취소

예, 수락

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

- VPC 간 트래픽 통신을 수행하기 위해 [지금 내 라우팅 테이블 수정]을 클릭합니다.

VPC 피어링 연결 요청 수락



VPC 피어링 연결이 설정되었습니다.

이 VPC 피어링 연결을 통해 트래픽을 송수신하려면 하나 이상의 VPC 라우팅 테이블에 피어링된 VPC에 대한 라우팅을 추가해야 합니다. [자세히 알아보기](#)

[지금 내 라우팅 테이블 수정](#)

닫기

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

- 오레곤 리전의 [라우팅 테이블] 페이지에서 바로 전에 생성된 라우팅 테이블을 다음과 같이 선택하고 “라우팅” 탭 클릭 후 [라우팅 편집] 버튼을 클릭합니다.

라우팅 테이블 (1/3) 정보

Q 라우팅 테이블 필터링

< 1 > ⚙

	Name	라우팅 테이블 ID	명시적 서브넷 연결	엣지 연결	기본	VPC	소유자 ID
<input checked="" type="checkbox"/>	-	rtb-03bcb62c7493fe51	subnet-0e793264baeb...	-	아니요	vpc-0c1d9215afacd259f tuto...	262663767358

rtb-03bcb62c7493fe51

세부 정보 라우팅 서브넷 연결 엣지 연결 라우팅 전파 태그

라우팅 (2)

Q 라우팅 필터링 모두

< 1 > ⚙

대상	대상	상태	전파됨
20.0.0.0/16	local	⊙ 활성	아니요
0.0.0.0/0	igw-0f1fd4dc1f92e5382	⊙ 활성	아니요

라우팅 편집

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

- 라우팅 편집 페이지에서 [라우팅 추가] 버튼을 클릭하고 좌측의 “대상”에서 오아시오 리전의 VPC 대역인 “10.0.0.0/16” 입력 후 대상 항목에서 “피어링 연결”을 선택합니다.
- 현재 구성된 “VPC Peering 연결”을 선택 후 [라우팅 저장] 버튼을 클릭합니다.

VPC > 라우팅 테이블 > rtb-0f3182862ef48f670 > 라우팅 편집

라우팅 편집

대상	대상	상태	전파됨
20.0.0.0/16	<input type="text" value="local"/>	🟢 활성	아니요
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="igw-0202af880094daace"/>	🟢 활성	아니요 <button>제거</button>
<input type="text" value="10.0.0.0/16"/>	<input type="text" value=""/>	-	아니요 <button>제거</button>

캐리어 게이트웨이
외부 전용 인터넷 게이트웨이
게이트웨이 로드 밸런서 엔드포인트
인스턴스
인터넷 게이트웨이
로컬
NAT 게이트웨이
네트워크 인터페이스
Outpost 로컬 게이트웨이
피어링 연결
Transit Gateway 피어링 연결
가상 프라이빗 게이트웨이

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

- 오아이오 리전의 [라우팅 테이블] 페이지에서 바로 전에 생성된 라우팅 테이블을 다음과 같이 선택하고, “라우팅” 탭 클릭 후 [라우팅 편집] 버튼을 클릭합니다.

The screenshot shows the AWS Management Console interface for the '라우팅 테이블 (1/3) 정보' page. The left sidebar contains navigation links for VPC, VPC Peering, and various VPC-related services. The main content area displays a table of routing tables. The table has columns for Name, 라우팅 테이블 ID, 명시적 서브넷 연결, 엣지 연결, 기본, VPC, and 소유자 ID. The row with ID 'rtb-066da4a6f910aa15c' is highlighted, and its '라우팅' tab is selected. The '라우팅 편집' button is visible in the bottom right corner.

Name	라우팅 테이블 ID	명시적 서브넷 연결	엣지 연결	기본	VPC	소유자 ID
-	rtb-0117396a	-	-	예	vpc-a23e5fc9	262663767358
-	rtb-08429141c506f64e9	-	-	예	vpc-07bcb655120ee59aa tut...	262663767358
-	rtb-066da4a6f910aa15c	subnet-0cabcb4908fa74...	-	아니오	vpc-07bcb655120ee59aa tut...	262663767358

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

- 라우팅 편집 페이지에서 [라우팅 추가] 버튼 클릭 후 좌측의 “대상”에서 런던 리전의 VPC 대역인 “20.0.0.0/16” 입력 후 대상 항목에서 “피어링 연결”를 선택합니다.
- 현재 구성된 “VPC Peering 연결” 선택 후 [변경사항 저장] 버튼을 클릭합니다.

라우팅 편집

대상	대상	상태	전파됨
10.0.0.0/16	<input type="text" value="local"/>	🟢 활성	아니요
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="igw-006f753234470e789"/>	🟢 활성	아니요 <button>제거</button>
<input type="text" value="20.0.0.0/16"/>	<input type="text" value=""/>	-	아니요 <button>제거</button>

라우팅 추가

외부 전용 인터넷 게이트웨이

게이트웨이 로드 밸런서 엔드포인트

인스턴스

인터넷 게이트웨이

로컬

NAT 게이트웨이

네트워킹 인터페이스

peer-0b961221198715565 (Oaio-Oregon VPC Peering)

피어링 연결

Transit Gateway

가상 프라이빗 게이트웨이

취소

미리 보기

변경 사항 저장

VPC > 라우팅 테이블 > rtb-066da4a6f910aa15c > 라우팅 편집

라우팅 편집

대상	대상	상태	전파됨
10.0.0.0/16	<input type="text" value="local"/>	🟢 활성	아니요
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="igw-006f753234470e789"/>	🟢 활성	아니요 <button>제거</button>
<input type="text" value="20.0.0.0/16"/>	<input type="text" value="pcx-0b961221198715565 (Oaio-Oregon VPC Peering)"/>	-	아니요 <button>제거</button>

라우팅 추가

pcx-0b961221198715565 (Oaio-Oregon VPC Peering)

취소

미리 보기

변경 사항 저장

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

- 다시 오레곤 리전의 EC2 생성 페이지로 이동 후 “Amazon Linux 2 AMI (HVM)”를 선택하여 t2.micro(Free-Tier) 선택 후 인스턴스 세부 정보 구성 페이지에서 VPC 선택 시 이전에 생성했던 VPC를 선택합니다.
- “퍼블릭 IP 자동 할당”을 “활성화”로 선택 후 [검토 및 시작] 버튼을 클릭해 인스턴스를 생성합니다.

단계 3: 인스턴스 세부 정보 구성

요구 사항에 적합하게 인스턴스를 구성합니다. 동일한 AMI의 여러 인스턴스를 시작하고 스팟 인스턴스를 요청하여 보다 저렴한 요금을 활용하며 인

인스턴스 개수	1	Auto Scaling 그룹 시작
구매 옵션	<input type="checkbox"/> 스팟 인스턴스 요청	
네트워크	vpc-0c1d9215afacd259f tutorial-VPC-Oregon	
서브넷	vpc-0c1d9215afacd259f tutorial-VPC-Oregon vpc-f8090c80 (기본값) 251개 IP 주소 자동 할당 가능	
퍼블릭 IP 자동 할당	활성화	
배치 그룹	<input type="checkbox"/> 배치 그룹에 인스턴스 추가	
용량 예약	열기	
도메인 조인 디렉터리	디렉터리 없음	
IAM 역할	없음	
종료 방식	중지	
최대 절전 중지 동작	<input type="checkbox"/> 추가 종료 동작으로 최대 절전 모드를 활성화	
종료 방지 기능 활성화	<input type="checkbox"/> 우발적인 종료로부터 보호	
모니터링	<input type="checkbox"/> CloudWatch 세부 모니터링 활성화 추가 요금이 발생합니다.	
테넌시	공유됨 - 공유된 하드웨어 인스턴스 실행 전용 테넌시에는 추가 요금이 적용됩니다.	
Elastic Inference	<input type="checkbox"/> Elastic Inference 액셀러레이터 추가 추가 요금이 발생합니다.	

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

- 오레곤 리전에서 인스턴스 생성 완료 후 세부 항목 페이지에서 등록된 “보안 그룹”을 확인하고 수정을 위해 “보안 그룹 링크”를 클릭합니다.

The screenshot displays the AWS Management Console interface for an EC2 instance. At the top, the instance details are shown in a table with columns: Name, 인스턴스 ID, 인스턴스 상태, 인스턴스 유형, 상태 검사, 경보 상태, 가용 영역, and 퍼블릭 IPv4 DNS. The instance 'i-04808e661a79532a0' is listed with status '대기 중' and type 't2.micro'. Below this, the '인스턴스: i-04808e661a79532a0' details page is open, with the '보안' (Security) tab selected. Under '보안 세부 정보' (Security details), the 'IAM 역할' (IAM role) is shown as '-', and the '소유자 ID' (Owner ID) is '262663767358'. The '보안 그룹' (Security groups) section shows 'sg-08d02292e428dc3cd (launch-wizard-1)' highlighted with a red box. The '인바운드 규칙' (Inbound rules) section is partially visible at the bottom.

Name	인스턴스 ID	인스턴스 상태	인스턴스 유형	상태 검사	경보 상태	가용 영역	퍼블릭 IPv4 DNS
-	i-04808e661a79532a0	대기 중	t2.micro	-	경보 없음	us-west-2a	ec2-34-219-124-1

인스턴스: i-04808e661a79532a0

세부 정보 | **보안** | 네트워킹 | 스토리지 | 상태 검사 | 모니터링 | 태그

▼ 보안 세부 정보

IAM 역할
-

소유자 ID
262663767358

보안 그룹
sg-08d02292e428dc3cd (launch-wizard-1)

▼ 인바운드 규칙

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

- 보안 그룹 페이지 하단의 “인바운드 규칙” 탭에서 [인바운드 규칙 편집] 버튼을 클릭하여 인바운드 규칙 편집 페이지로 이동합니다.

EC2 > 보안 그룹 > sg-08d02292e428dc3cd - launch-wizard-1

sg-08d02292e428dc3cd - launch-wizard-1 작업 ▼

세부 정보

보안 그룹 이름

launch-wizard-1

보안 그룹 ID

sg-08d02292e428dc3cd

설명

launch-wizard-1 created 2021-07-17T20:37:33.579+09:00

VPC ID

vpc-0c1d9215afacd259f

소유자

262663767358

인바운드 규칙 수

1 권한 항목

아웃바운드 규칙 수

1 권한 항목

인바운드 규칙

아웃바운드 규칙

태그

Inbound rules (1/1)

Filter security group rules

Manage tags

Edit inbound rules

< 1 > ⚙

<input checked="" type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
<input checked="" type="checkbox"/>	-	sgr-0282449b6b99edffd	IPv4	SSH	TCP	22	0.0.0.0/0	-

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

- 인바운드 규칙 편집 페이지로 이동 후 [규칙 추가] 버튼을 클릭하여 “유형 : 모든 트래픽, 소스 : 10.0.0.0/16(서울 리전 VPC대역)” 등록 후 [규칙 저장] 버튼을 클릭합니다.

인바운드 규칙 편집 정보

인바운드 규칙은 인스턴스에 도달하도록 허용된 수신 트래픽을 제어합니다.

인바운드 규칙 정보

Security group rule ID	유형 정보	프로토콜 정보	포트 범위 정보	소스 정보	설명 - 선택 사항 정보
sgr-0282449b6b99edffd	SSH	TCP	22	사용자 지정	
-	모든 트래픽	전체	전체	사용자 지정	

규칙 추가

취소

변경 사항 미리 보기

규칙 저장

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

- 오아이오 리전에도 오레곤 리전과 동일한 방식으로 신규로 생성한 VPC의 Public Subnet을 선택하여 EC2 인스턴스를 생성하고, 보안 그룹으로 이동합니다.

서비스, 기능, 마켓플레이스 제품, 설명서 검색

[Alt+S]

jinu 오하이오 지원

인스턴스 (1/2) 정보

인스턴스 필터

< 1 >

	Name	인스턴스 ID	인스턴스 상태	인스턴스 유형	상태 검사	경보 상태	가용 영역	퍼블릭 IPv4 DNS	퍼블릭 IPv4 ...	탄력적 IP	IPv6 IP	모니터링	보안 그룹 이름	키 이름
<input type="checkbox"/>	-	i-0ae71771a7a94bd7a	중지됨	t2.micro	-	경보 없음	us-east-2a	-	-	-	-	disabled	launch-wizard-3	AWS_Study_Key
<input checked="" type="checkbox"/>	-	i-03e18e9de049fff22	실행 중	t2.micro	-	경보 없음	us-east-2a	ec2-3-17-154-52.us-eas...	3.17.154.52	-	-	disabled	launch-wizard-5	AWS_Study_Key

인스턴스: i-03e18e9de049fff22

세부 정보 보안 네트워킹 스토리지 상태 검사 모니터링 태그

▼ 보안 세부 정보

IAM 역할
-

소유자 ID
262663767358

시작 시간
Sat Jul 17 2021 20:51:52 GMT+0900 (대한민국 표준시)

보안 그룹
sg-05a91cedda76d0616 (launch-wizard-5)

▼ 인바운드 규칙

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

- 보안 그룹으로 이동 후 [규칙 추가] 버튼을 클릭하여 “유형: 모든 트래픽, 소스 : 20.0.0.0/16 (오레곤 리전 VPC대역)” 등록 후 [규칙 저장] 버튼을 클릭합니다.

인바운드 규칙 편집

정보

인바운드 규칙은 인스턴스에 도달하도록 허용된 수신 트래픽을 제어합니다.

인바운드 규칙

정보

Security group rule ID	유형 정보	프로토콜 정보	포트 범위 정보	소스 정보	설명 - 선택 사항	정보
sgr-02c3f7040106e0d37	SSH	TCP	22	사용자 지정	<input type="text"/>	<div>삭제</div>
-	모든 트래픽	전체	전체	사용자 지정	<div>0.0.0.0/0</div> <div>20.0.0.0/16</div>	<div>삭제</div>

규칙 추가

취소

변경 사항 미리 보기

규칙 저장

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

- Putty를 이용하여 오아이오 리전의 인스턴스에 접속 후 오레곤 리전에 생성된 인스턴스의 Private IP로 Ping 명령어를 실행하여, 정상적으로 통신이 가능함을 확인합니다.

7. 실습 : 리전(Region) 간 VPC Peering으로 글로벌 통합 네트워크 환경 구축하기

- Putty를 이용하여 런던 리전의 인스턴스에 접속 후 서울 리전에 생성된 인스턴스의 Private IP로 Ping 명령어를 실행하여, 정상적으로 통신이 가능함을 확인합니다.

```
ec2-user@ip-20-0-0-144:~  
login as: ec2-user  
Authenticating with public key "imported-openssh-key"  
Last login: Sat Jul 17 12:10:38 2021 from 220.85.203.55  
  
 _ _ | _ _ | _ )  
 _ | ( _ _ /   Amazon Linux 2 AMI  
 _ | \ _ _ | _ |  
  
https://aws.amazon.com/amazon-linux-2/  
6 package(s) needed for security, out of 18 available  
Run "sudo yum update" to apply all updates.  
ec2-user@ip-20-0-0-144 ~]$ ping 10.0.0.15  
PING 10.0.0.15 (10.0.0.15) 56(84) bytes of data.
```

8. EC2 삭제

- 본 실습과 이전 실습에서 사용된 EC2는 더 이상 사용되지 않습니다.
- 오아이오 리전에 생성된 인스턴스와 오레곤 리전에 생성된 EC2 인스턴스를 모두 삭제하는 절차는 다음과 같습니다.

8. EC2 삭제

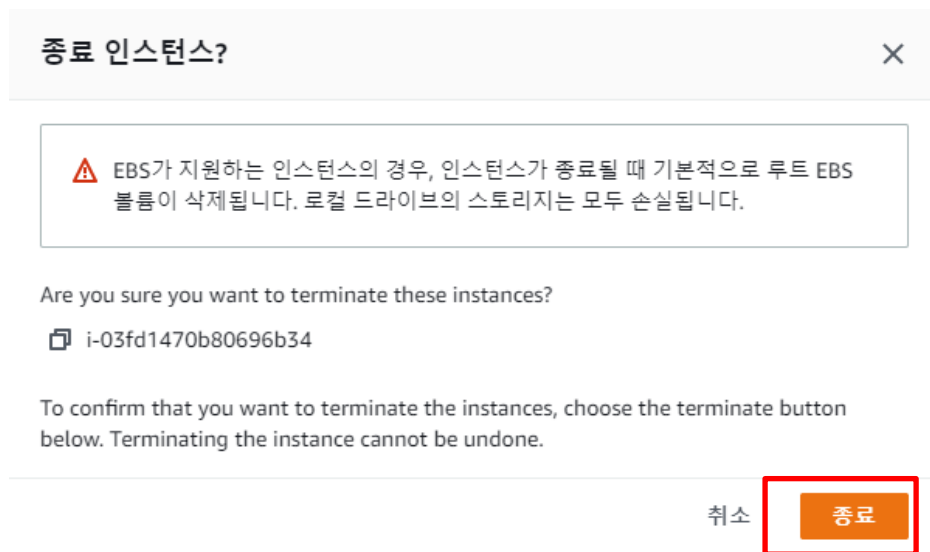
- 웹 브라우저를 열고 <http://aws.amazon.com>에 접속 후 본인의 AWS 계정으로 로그인합니다.
- 왼쪽 상단 메뉴의 [서비스] → [컴퓨팅] → [EC2]로 이동합니다.
- 메뉴의 [인스턴스]를 선택한 후 중지할 인스턴스를 클릭 후 [작업] → [인스턴스 상태] → [종료]를 클릭합니다.

The screenshot shows the AWS Management Console interface for EC2 instances. At the top, there's a search bar and filters. Below, a table lists instances. The first instance is selected, and its details are shown below the table. The '인스턴스 종료' (Terminate Instance) button is highlighted with a red box.

Name	인스턴스 ID	인스턴스 상태	인스턴스 유형	상태 검사	경보 상태	가용 영역	퍼블릭 IPv4 DNS	퍼블릭 IPv4 ...	탄력적 IP	IPv6 IP	모니
-	i-03fd1470b80696b34	실행 중	t2.micro	2/2개 검사 통과...	경보 없음	us-east-1a	ec2-54-173-35-101.co...	54.173.35.101	-	-	disa

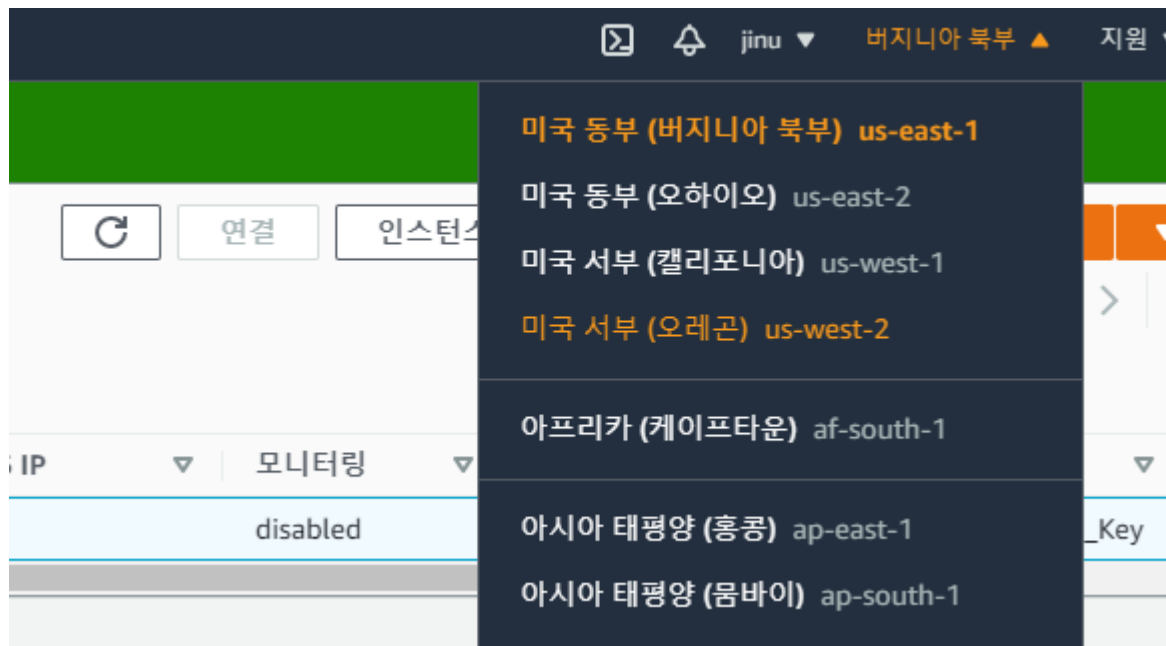
8. EC2 삭제

- 확인 창에서 [종료] 버튼을 클릭 후 인스턴스 상태가 “종료됨”으로 변경됨을 확인합니다.



8. EC2 삭제

- 오레곤 리전의 인스턴스 삭제를 위해 오른쪽 상단의 [리전] 항목을 선택 후 “미국 서부(오레곤)”을 클릭합니다.



8. EC2 삭제

- 미국 서부 (오레곤)으로 이동 후 [인스턴스] 항목에서 중지할 인스턴스를 선택 후 [작업] → [인스턴스 상태]의 [종료] 버튼을 클릭하여 인스턴스 종료 후 인스턴스 상태가 “종료됨”으로 변경됨을 확인합니다.

성공적으로 종료됨 i-017ae94cd09a6bb77

인스턴스 (1/1) 정보

인스턴스 필터링

인스턴스 상태: running X 필터 지우기

<input checked="" type="checkbox"/>	Name	인스턴스 ID	인스턴스 상태	인스턴스 유형	상태 검사	경보 상태	가용 영역	퍼블릭 IPv4 DNS	퍼블릭 IPv4 ...	탄력적 IP
<input checked="" type="checkbox"/>	-	i-017ae94cd09a6bb77	종료됨	t2.micro	2/2개 검사 통과...	경보 없음	us-west-2a	-	52.32.61.21	-



Thank You
