용어통일

[평생] 멀티미디어 촬영 교안형

[스토리보드] 클라우드 보안 구축

08회차 : 계정보안 : VPC2

내용전문가	최민	교수설계(한기대)	한기대
협력업체	위지런	교수설계(협력업체)	김은혜

업무	작성자	버전	작성일	특이사항
SB 작성	위지런	V1.0	2023. 10.23	1차안 작성

과정명	클라우드 보안 구축	회차명	계정보안 : VPC2	화면번호	01_01

▶ Intro
- 학습열기
- 학습목표

▶ 본학습
- VPC 생성 실습
- Gateway / Subnet 설정 실습
- 웹서버 인스턴스 실행 실습

▶ 정리하기
- 문제풀기
- Outro

인트로

계정보안 : VPC2

화면설명

인트로

이미지 번호

내레이션

Simple Storage Service(S3)보안2

학습목표

STEP

학습 목표

#1

- VPC 개념과 주요 구성요소에 대해 설명할 수 있다.
- VPC에서 다루는 Peering, Router, NAT, IG, Endpoint 등 개념을 설명할 수 있다.

#2

학습 내용

- VPC 생성 실습
- Gateway / Subnet 설정 실습
- 웹서버 인스턴스 실행 실습

화면설명

학습목표는
성우 음성 진행

이미지 번호

내레이션

성우: #1 #2이번 학습을 통해 여러분은 VPC 개념과 주요 구성요소, 그리고 VPC에서 다루는 Peering, Router, NAT, IG, Endpoint 등 개념을 설명할 수 있습니다.

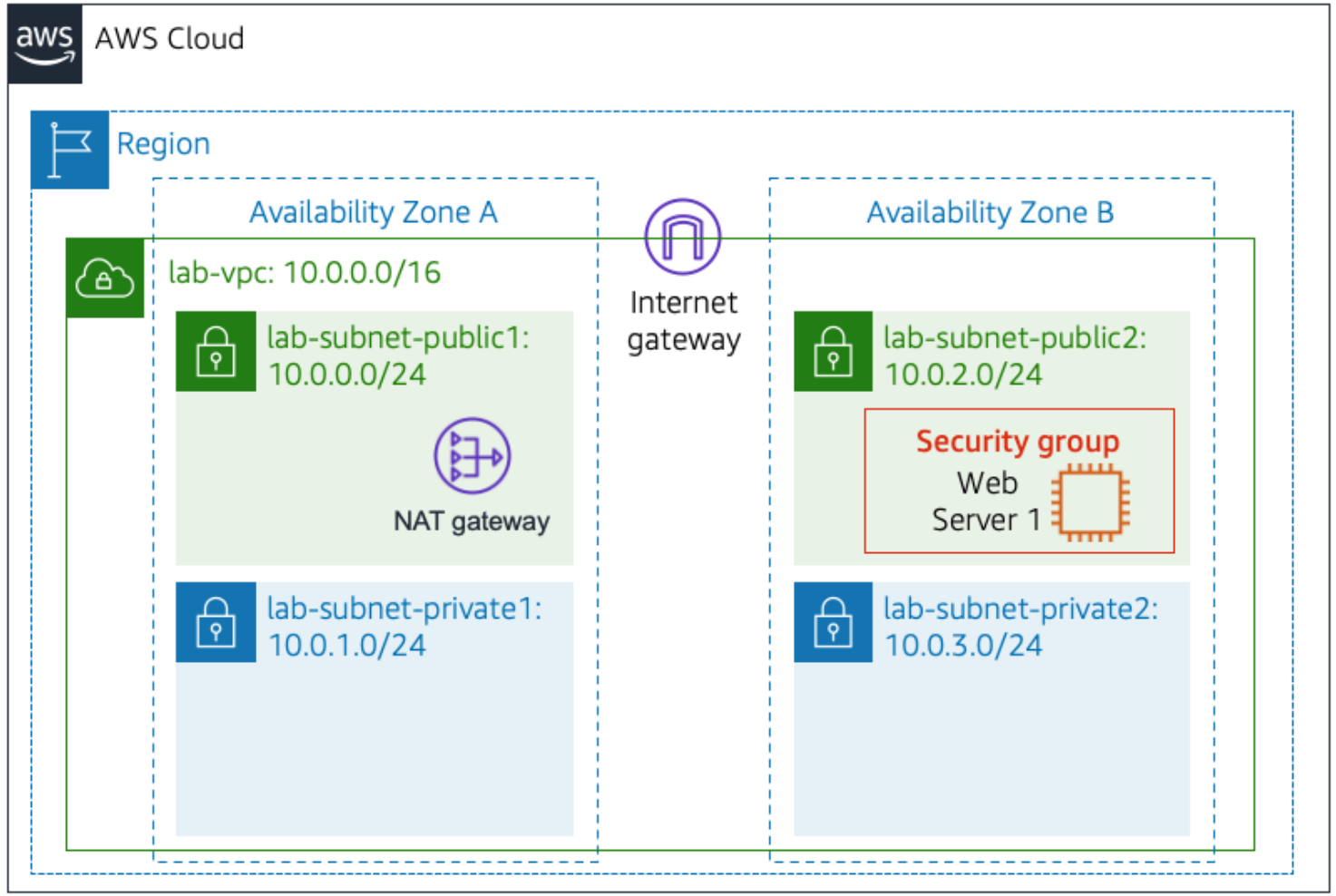
VPC 생성 실습

- VPC 아키텍쳐
- VPC 생성
- VPC 생성 결과

화면설명

이미지 번호

내레이션



Public Route Table

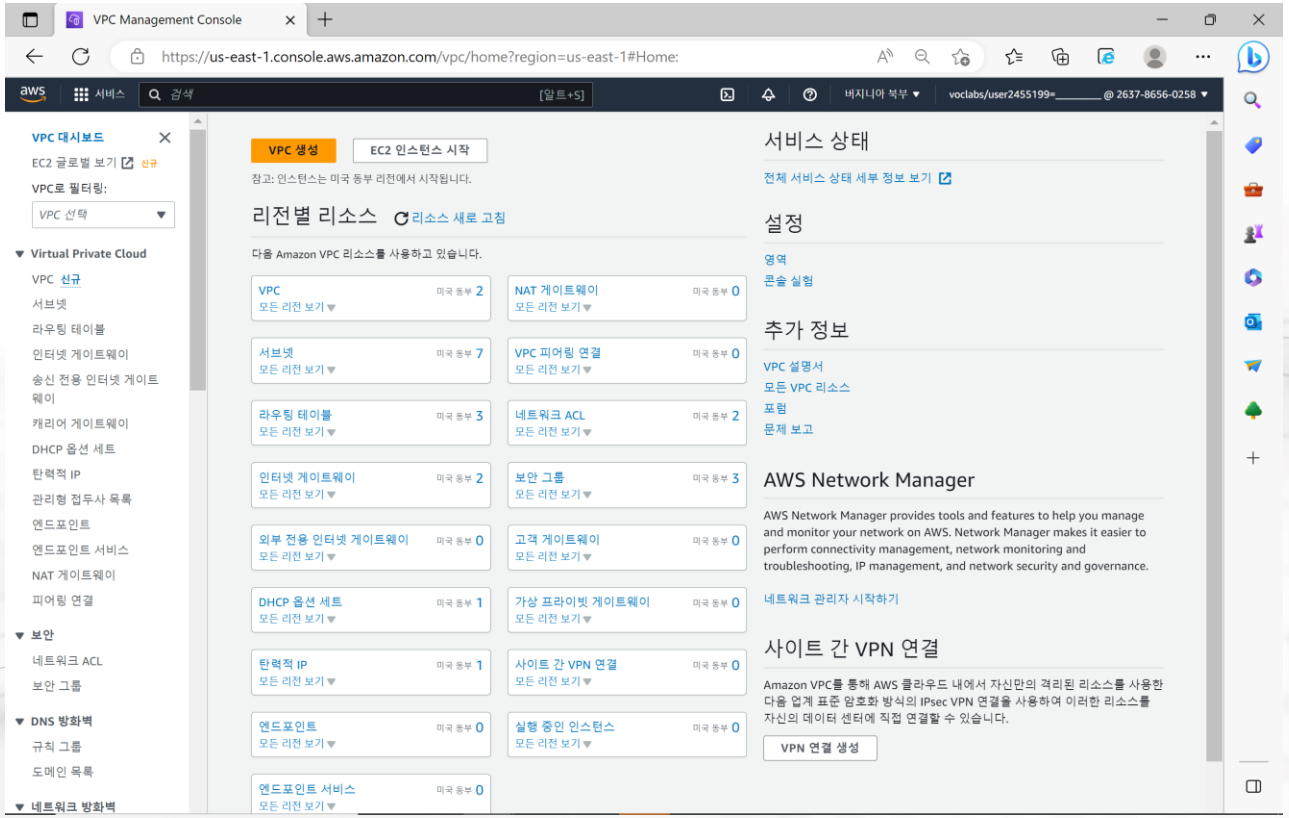
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	Internet gateway

Private Route Tables

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	NAT gateway

VPC 대쉬보드

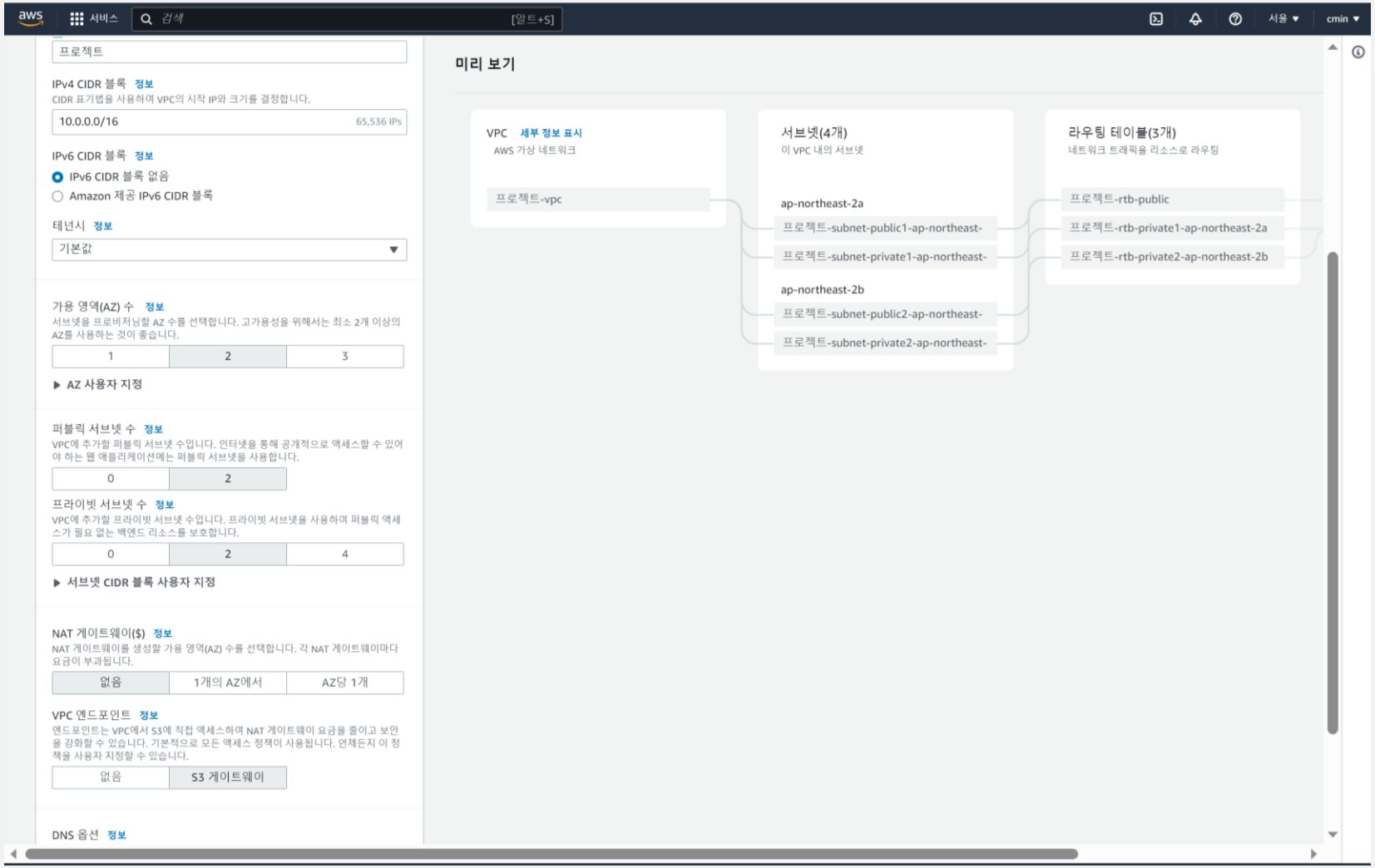
VPC 생성, 옵션 설정을 통한 리소스 생성



사용 리소스

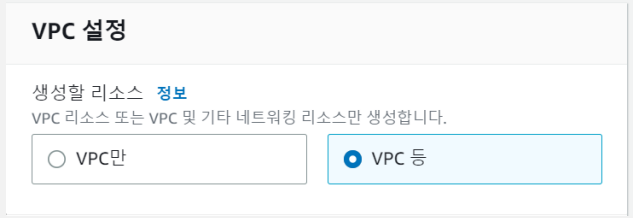
- VPC 1개
- 인터넷 게이트웨이 (IG) 1개
- 퍼블릭 서브넷 1개
- 프라이빗 서브넷 1개
- 가용구역 (AZ) 1개
- 라우팅 테이블 2개
- NAT 게이트웨이 1개

사용 리소스

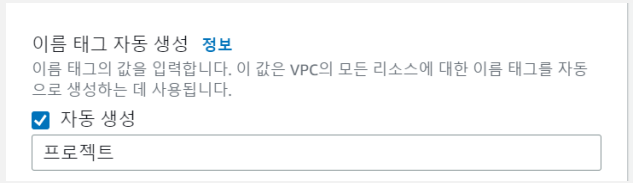

aws
서비스
검색
[알트+S]
서울
cmin
프로젝트
IPv4 CIDR 블록 정보
CIDR 표기법을 사용하여 VPC의 시작 IP와 크기를 결정합니다.
10.0.0.0/16
65,536 IPs
IPv6 CIDR 블록 정보
IPv6 CIDR 블록 없음
Amazon 제공 IPv6 CIDR 블록
테넌시 정보
기본값
가용 영역(AZ) 수 정보
서브넷을 프로비저닝할 AZ 수를 선택합니다. 고가용성을 위해서는 최소 2개 이상의 AZ를 사용하는 것이 좋습니다.
1
2
3
AZ 사용자 지정
퍼블릭 서브넷 수 정보
VPC에 추가할 퍼블릭 서브넷 수입니다. 인터넷을 통해 공개적으로 액세스할 수 있어야 하는 웹 애플리케이션에는 퍼블릭 서브넷을 사용합니다.
0
2
프라이빗 서브넷 수 정보
VPC에 추가할 프라이빗 서브넷 수입니다. 프라이빗 서브넷을 사용하여 퍼블릭 액세스가 필요 없는 백엔드 리소스를 보호합니다.
0
2
4
서브넷 CIDR 블록 사용자 지정
NAT 게이트웨이($) 정보
NAT 게이트웨이를 생성할 가용 영역(AZ) 수를 선택합니다. 각 NAT 게이트웨이마다 요금이 부과됩니다.
없음
1개의 AZ에서
AZ당 1개
VPC 엔드포인트 정보
엔드포인트는 VPC에서 S3에 직접 액세스하여 NAT 게이트웨이 요금을 줄이고 보안을 강화할 수 있습니다. 기본적으로 모든 액세스 정책이 사용됩니다. 언제든지 이 정책을 사용자 지정할 수 있습니다.
없음
S3 게이트웨이
DNS 옵션 정보
미리 보기
VPC 세부 정보 표시
AWS 가상 네트워크
프로젝트-vpc
서브넷(4개)
이 VPC 내의 서브넷
ap-northeast-2a
프로젝트-subnet-public1-ap-northeast-
프로젝트-subnet-private1-ap-northeast-
ap-northeast-2b
프로젝트-subnet-public2-ap-northeast-
프로젝트-subnet-private2-ap-northeast-
라우팅 테이블(3개)
네트워크 트래픽을 리소스로 라우팅
프로젝트-rtb-public
프로젝트-rtb-private1-ap-northeast-2a
프로젝트-rtb-private2-ap-northeast-2b

VPC 설정 패널에서 VPC 세부 정보 구성하기

생성할 리소스: VPC 등 선택

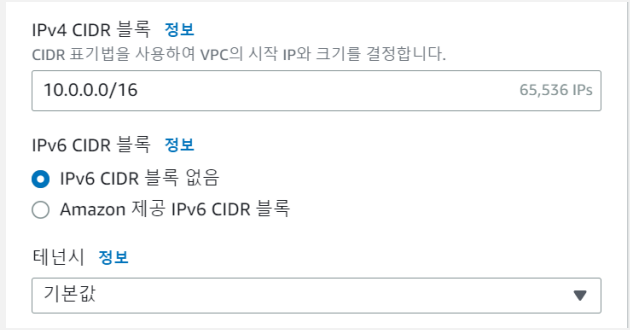


이름 태그 자동 생성, 이름 변경 가능

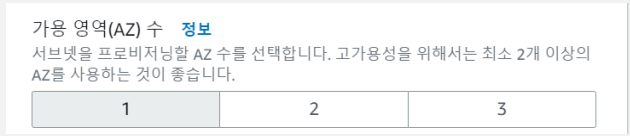


VPC 설정 패널에서 VPC 세부 정보 구성하기

IPv4 CIDR 블록: 10.0.0.0/16 설정

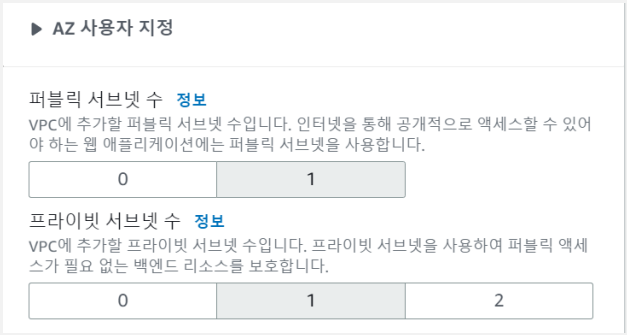


가용 영역 수: 1

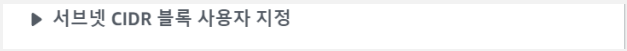


VPC 설정 패널에서 VPC 세부 정보 구성하기

- 퍼블릭 서브넷 수: 1
- 프라이빗 서브넷 수: 1



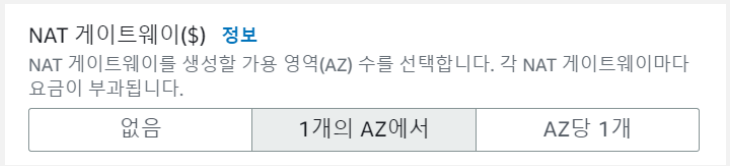
- 서브넷 CIDR 블록 사용자 지정 섹션 확장



서브넷 CIDR 블록 사용자 지정 섹션 설정사항

- us-east-1a의 퍼블릭 서브넷 CIDR 블록: 10.0.0.0/24
- us-east-1a의 프라이빗 서브넷 CIDR 블록: 10.0.1.0/24

- NAT 게이트웨이 : "1개의 AZ에서"



서브넷 CIDR 블록 사용자 지정 섹션 설정사항

VPC 엔드포인트 : "없음"

VPC 엔드포인트 정보

엔드포인트는 VPC에서 S3에 직접 액세스하여 NAT 게이트웨이 요금을 줄이고 보안을 강화할 수 있습니다. 기본적으로 모든 액세스 정책이 사용됩니다. 언제든지 이 정책을 사용자 지정할 수 있습니다.

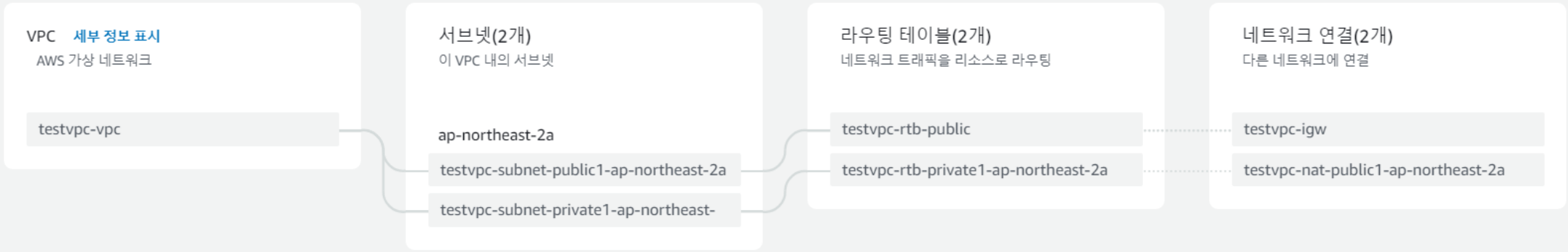
없음	S3 게이트웨이

DNS 호스트 이름과 DNS 확인을 모두 활성화 상태로 유지

DNS 옵션 정보

- [x] DNS 호스트 이름 활성화
- [x] DNS 확인 활성화

VPC설정 내역 확인


VPC 세부 정보 표시
AWS 가상 네트워크
testvpc-vpc
서브넷(2개)
이 VPC 내의 서브넷
ap-northeast-2a
testvpc-subnet-public1-ap-northeast-2a
testvpc-subnet-private1-ap-northeast-
라우팅 테이블(2개)
네트워크 트래픽을 리소스로 라우팅
testvpc-rtb-public
testvpc-rtb-private1-ap-northeast-2a
네트워크 연결(2개)
다른 네트워크에 연결
testvpc-igw
testvpc-nat-public1-ap-northeast-2a

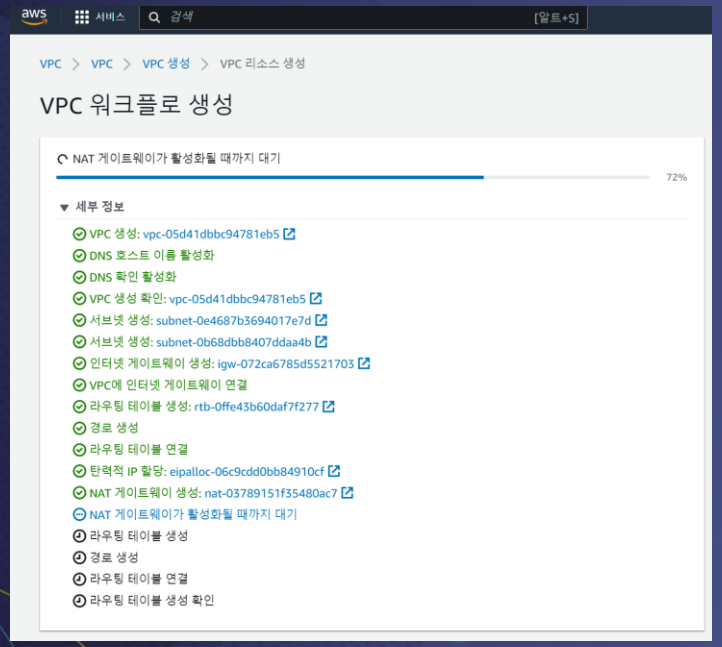
VPC 생성

VPC 생성 버튼 클릭

실행과정

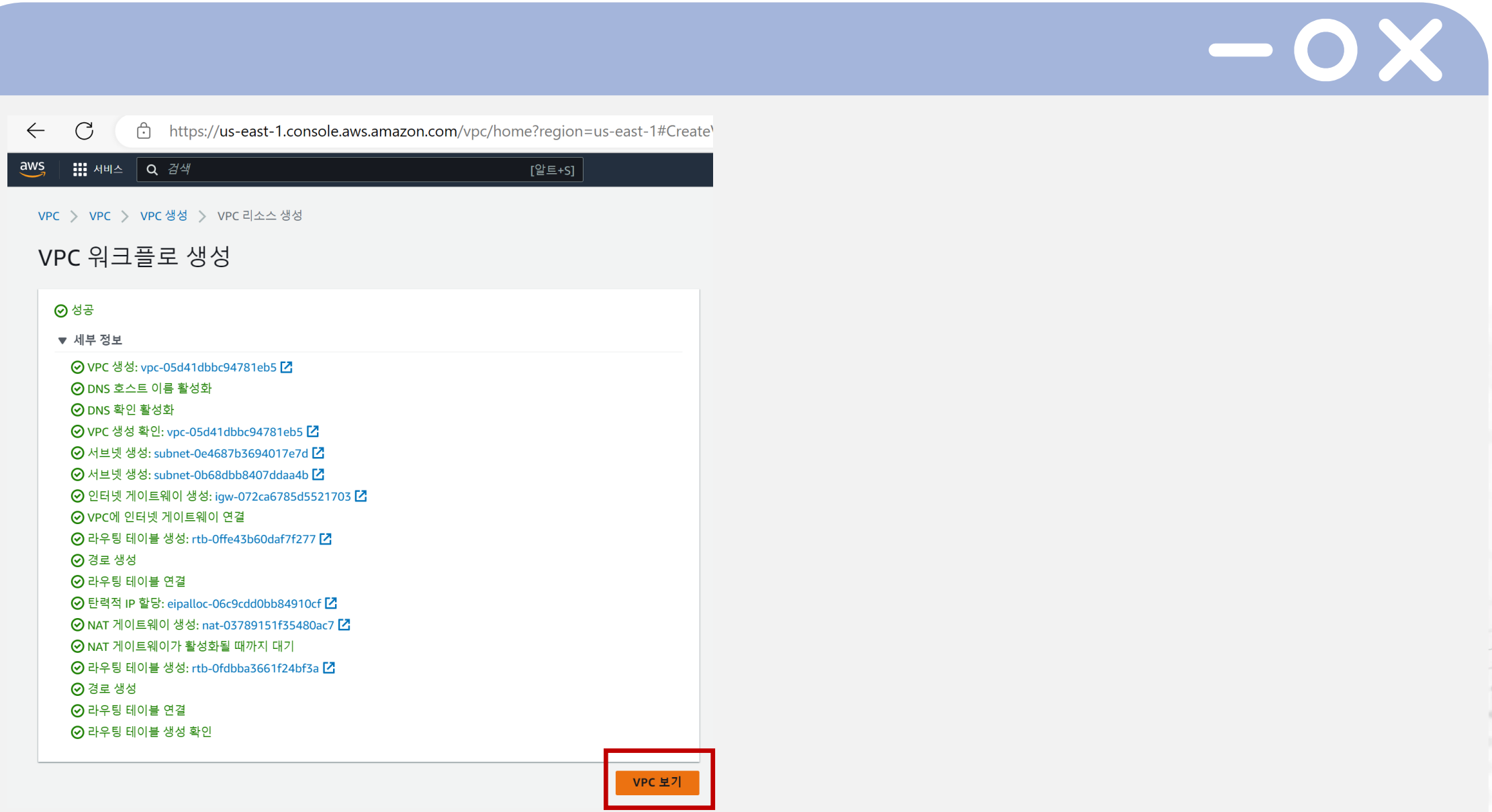
NAT gateway를 활성화하는 과정에서 시간소요

"모든 리소스가 생성되었다"는 메시지 확인 후 다음 단계로 진행



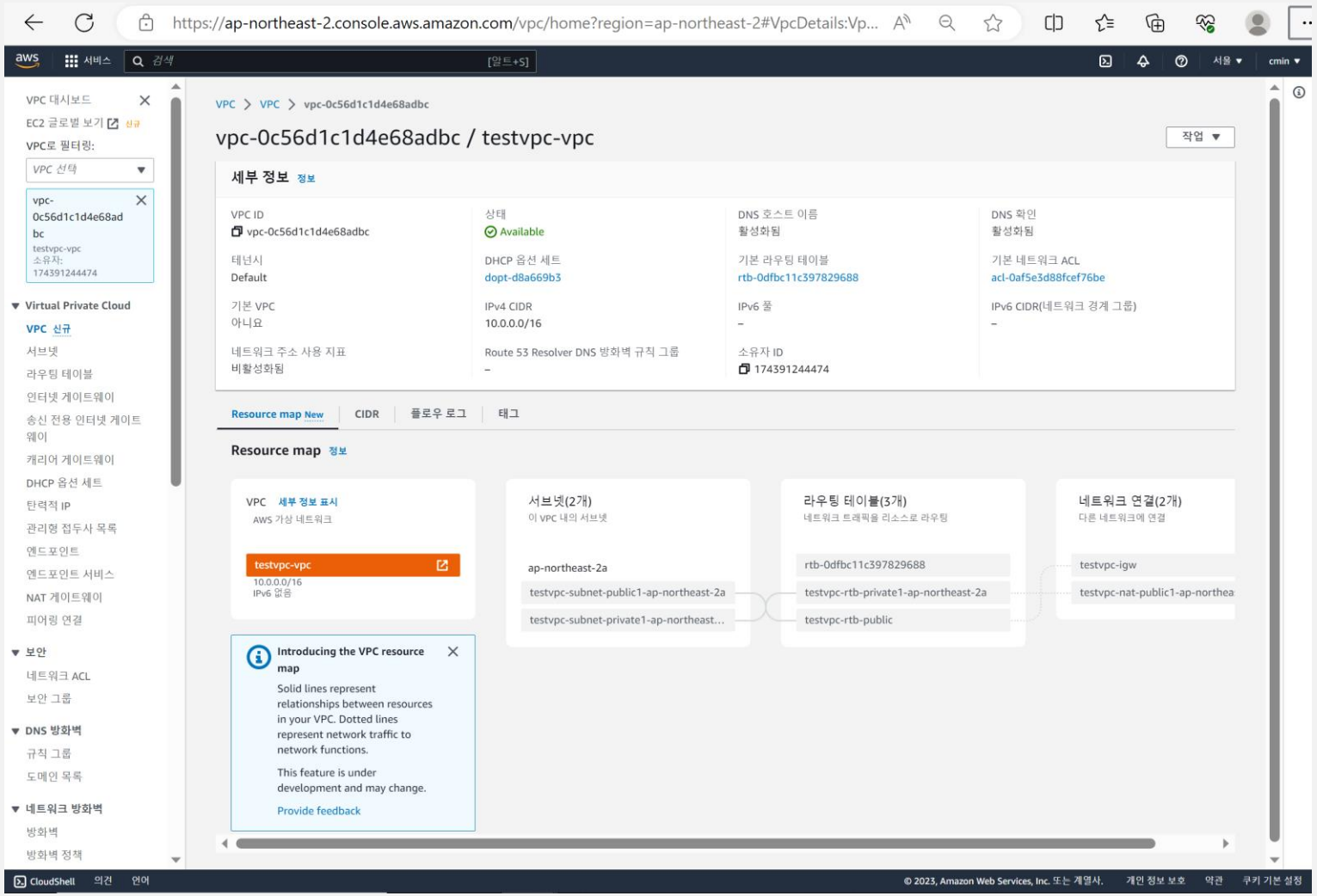
계정보안 : VPC2

VPC 생성

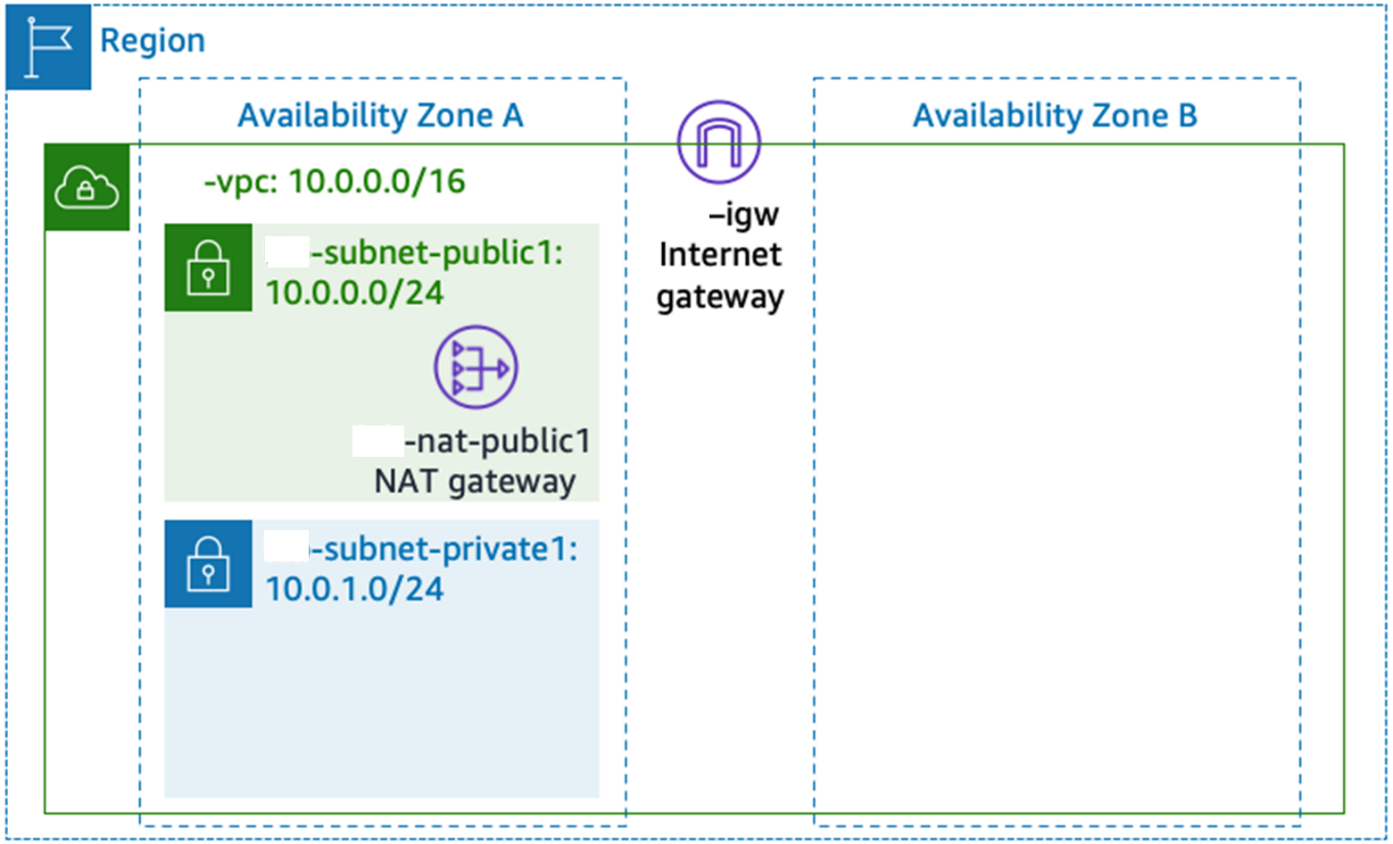


계정보안 : VPC2

VPC 생성



VPC 생성 결과



Public Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	Internet gateway

Private Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	NAT gateway

Gateway / Subnet 설정 실습

- Gateway / Subnet 설정

화면설명

이미지 번호

내레이션

인터넷 게이트웨이

인터넷 게이트웨이	VPC의 EC2 인스턴스와 인터넷 간의 통신을 허용하는 VPC 리소스

퍼블릭 서브넷
(Testvpc-subnet-public1-ap-northeast-2a)

10.0.0.0/24의 CIDR을 가지며,
10.0.0.x로 시작하는 모든 IP 주소를 포함함을 의미

퍼블릭 서브넷과 연결된 라우팅 테이블은 0.0.0.0/0 네트워크 트래픽을
해당 인터넷 게이트웨이로 라우팅하므로 퍼블릭 서브넷임

계정보안 : VPC2

Gateway / Subnet 설정

Resource map New | CIDR | 플로우 로그 | 태그

Resource map 정보

VPC 세부 정보 표시
AWS 가상 네트워크

testvpc-vpc

Introducing the VPC resource map

Solid lines represent relationships between resources in your VPC. Dotted lines represent network traffic to network functions.

This feature is under development and may change.

서브넷(2개)
이 VPC 내의 서브넷

ap-northeast-2a

testvpc-subnet-public1-ap-northe...
10.0.0.0/24
IPv6 없음

testvpc-subnet-private1-ap-northeast...

라우팅 테이블(3개)
네트워크 트래픽을 리소스로 라우팅

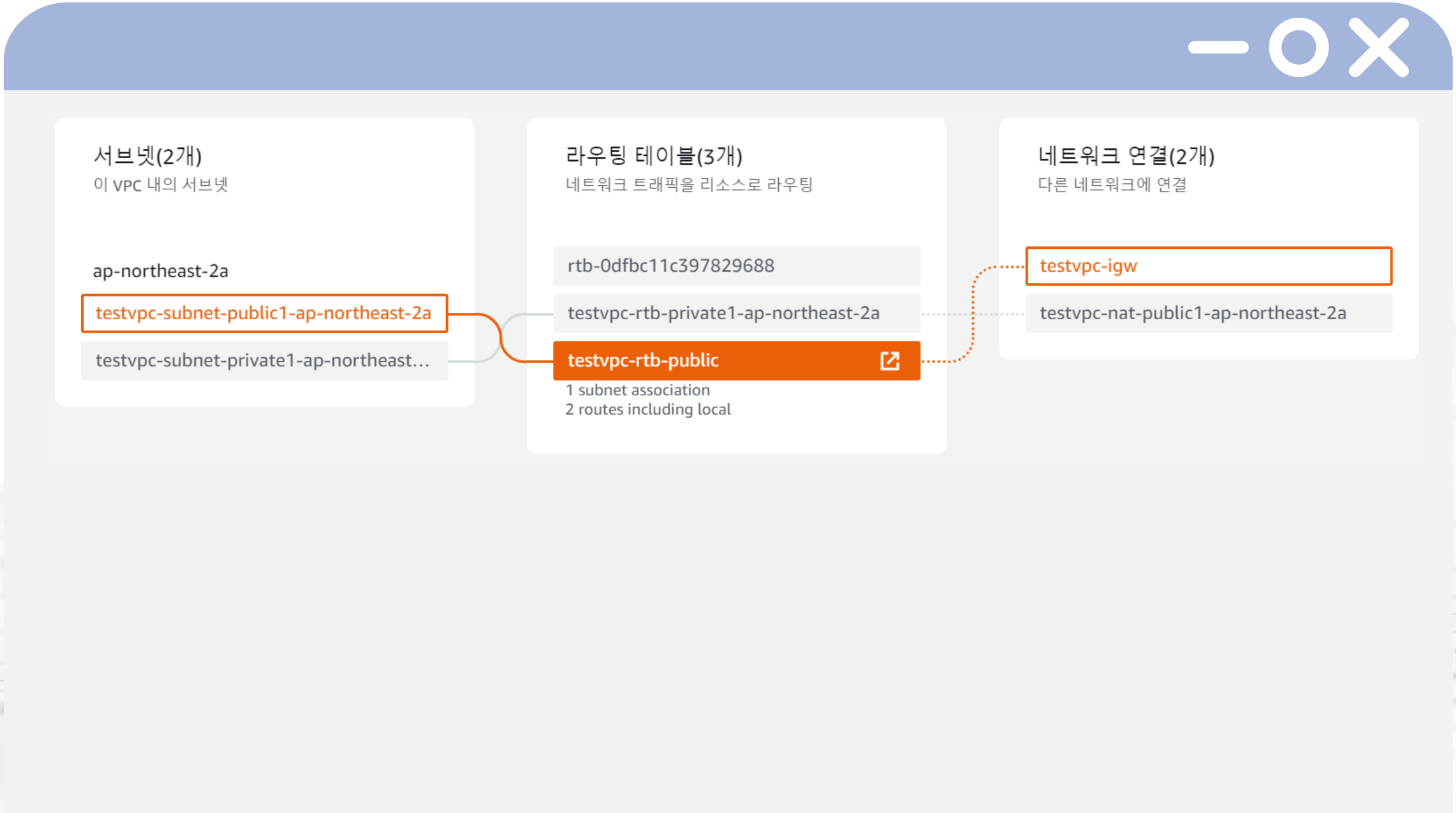
rtb-0dfbc11c397829688
testvpc-rtb-private1-ap-northeast-2a
testvpc-rtb-public

네트워크 연결(2개)
다른 네트워크에 연결

testvpc-igw
testvpc-nat-public1-ap-northeast-2a

계정보안 : VPC2

Gateway / Subnet 설정



NAT 게이트웨이

NAT 게이트웨이	EC2 인스턴스가 인터넷 게이트웨이에 직접 연결되지 않더라도, VPC의 프라이빗 서브넷에서 실행되는 모든 EC2 인스턴스에 인터넷 연결을 제공하는 데 사용되는 VPC 리소스

프라이빗 서브넷
(testvpc-subnet-private1-ap-northeast-2a)

Private subnet의 CIDR은 10.0.1.0/24이며,
이는 10.0.1.x로 시작하는 모든 IP 주소를 포함함을 의미함

계정보안 : VPC2

Gateway / Subnet 설정

STEP

Resource map 정보

서브넷(2개)
이 VPC 내의 서브넷

us-east-1a

- lab-subnet-public1-us-east-1a
- lab-subnet-private1-us-east-1a

라우팅 테이블(3개)
네트워크 트래픽을 리소스로 라우팅

- rtb-071a1998875c10ec8
- lab-rtb-private1-us-east-1a
- lab-rtb-public

네트워크 연결(2개)
다른 네트워크에 연결

- lab-igw
- lab-nat-public1-us-east-1a

퍼블릭 NAT 게이트웨이
1개의 EIP가 있는 1개의 ENI

서브넷(2개)
이 VPC 내의 서브넷

ap-northeast-2a

- testvpc-subnet-public1-ap-northeast-2a
- testvpc-subnet-private1-ap-northeast...

라우팅 테이블(3개)
네트워크 트래픽을 리소스로 라우팅

- rtb-0dfbc11c397829688
- testvpc-rtb-private1-ap-northeast-2a
- testvpc-rtb-public

네트워크 연결(2개)
다른 네트워크에 연결

- testvpc-igw
- testvpc-nat-public1-ap-northeast-...

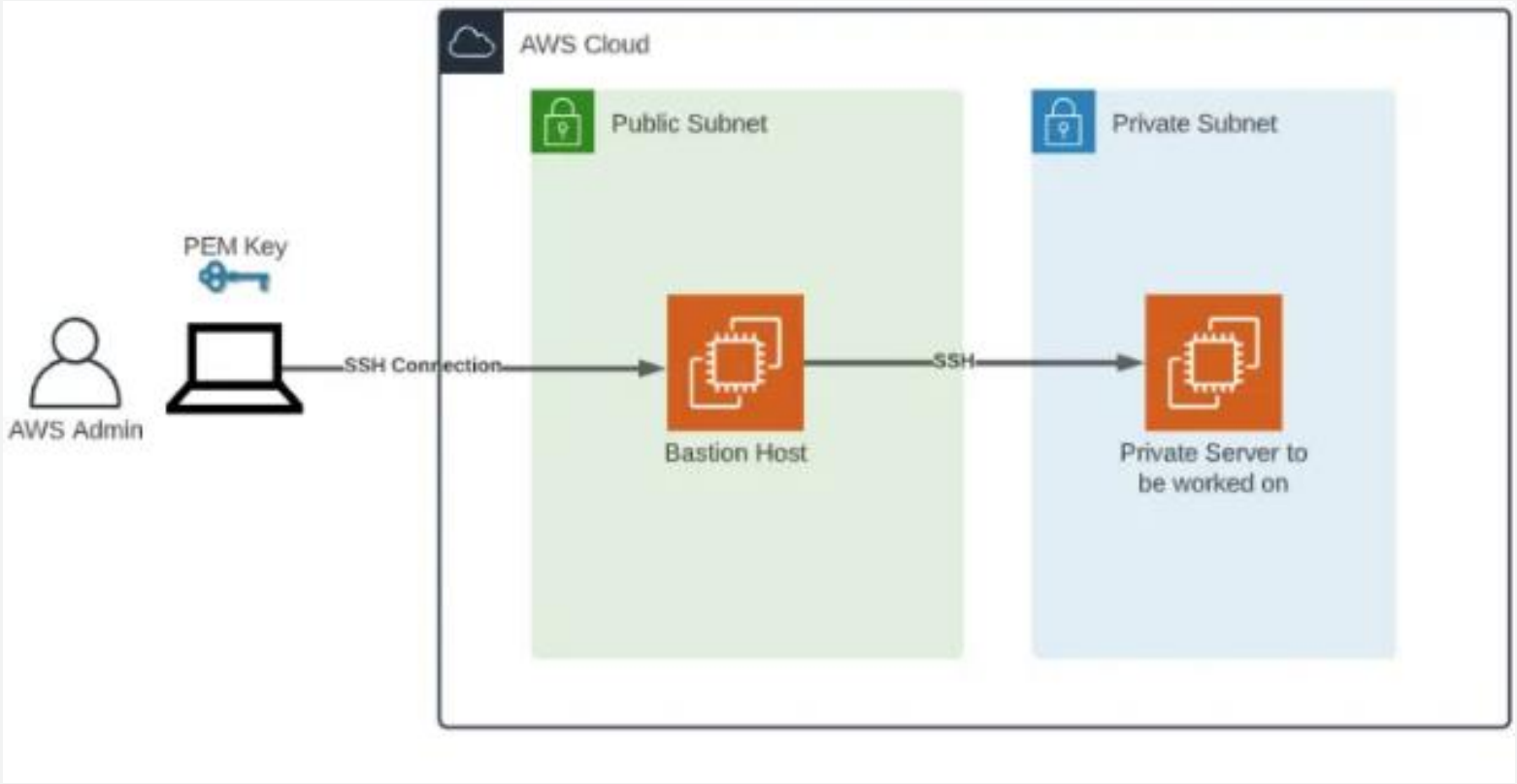
퍼블릭 NAT 게이트웨이
1개의 EIP가 있는 1개의 ENI

Private subnet 내부 인스턴스 접근 실습

- Private subnet은 외부에서 접근이 제한되므로, 내부 host에 접근이 어려움

ES2 인스턴스 시작

- private subnet 내부의 host(EC2 instance)에 대한 bastion host를 통한 접근



과정명	클라우드 보안 구축	회차명	계정보안 : VPC2	화면번호	06_05

▶ Intro
- 학습열기
- 학습목표

▶ 본학습
- VPC 생성 실습
- Gateway / Subnet 설정 실습
- 웹서버 인스턴스 실행 실습

▶ 정리하기
- 문제풀기
- Outro

QUIZ

학습한 내용을 바탕으로 문제를 풀어봅시다.

총 3문제가 제시되며,
문제를 풀 수 있는 기회는 1번입니다.

Start

화면설명

이미지 번호

내레이션

문제풀기

오늘 학습한 내용을 퀴즈를 통해 확인해 보세요.

Q1

1. 보안그룹(security group)에 대한 설명으로 적절하지 않은 것은?

① 범위는 인스턴스나 인터페이스 수준에서 설정한다.
② 사용가능한 규칙은 ALLOW와 DENY 규칙이다.
③ 상태유지(stateful) 특성을 가진다.
④ 규칙순서는 어떤 트래픽을 허용하는 결정을 내리기 전에 모든 규칙을 평가한다.

정답) 2

해설) 보안그룹(security group)의 범위는 인스턴스나 인터페이스 수준에서 설정한다. 보안구룹은 상태유지(stateful) 특성을 가집니다.

또한 보안그룹의 규칙순서는 어떤 트래픽을 허용하는 결정을 내리기 전에 모든 규칙을 평가합니다.

화면설명

[문제풀기]

- 4지선다 3문제
- '못한, 않는, 아닌'과 같은 부정표현에는 밑줄 긋기
- 확인버튼: 답을 선택하지 않고 클릭 시, '답을 선택해 주세요.' 팝업 나오기
- 답을 선택 후 처음 클릭 시, 답이 틀렸을 경우 '다시 생각해 보세요.' 팝업 나오기
- 답을 선택한 후 두 번째 클릭이거나, 맞은 답을 선택하고 클릭했을 때는 바로 정답 해설 페이지로 이동하기

이미지 번호

내레이션

퀴즈 3문항

번호	문제	보기	정답	해설
2	다음 보기의 내용이 맞으면 O, 틀리면 X를 선택하시오.	“AWS 외부에서 일반적인 사용자가 AWS 내 서버에 접근할 때, 외부 요청은 Network ACL을 정책을 먼저 적용된 후, Security Group 정책이 적용된다.”	O	AWS 외부에서 일반적인 사용자가 AWS내 서버에 접근할 때, 외부 요청은 Network ACL을 정책을 먼저 적용된 후, Security Group 정책이 적용됩니다.
3	다음 보기의 내용이 맞으면 O, 틀리면 X를 선택하시오.	“AWS 내부에 위치한 사용자(프로그램)이 동일 서브넷에 위치한 AWS 서버에 접속하는 경우, 요청은 Security Group 정책만 적용된다.”	O	AWS 내부에 위치한 사용자(프로그램)이 동일 서브넷에 위치한 AWS 서버에 접속하는 경우, 요청은 Security Group 정책만 적용됩니다.

과정명	클라우드 보안 구축	회차명	계정보안 : VPC2	화면번호	06_05

- ▶ Intro
  - 학습열기
  - 학습목표
- ▶ 본학습
  - VPC 생성 실습
  - Gateway / Subnet 설정 실습
  - 웹서버 인스턴스 실행 실습
- ▶ 정리하기
  - 문제풀기
  - Outro

화면설명

이미지 번호

내레이션

클라우드 보안 구축

계정보안 : VPC2

수고하셨습니다.

참고자료

- Neha Kewate, “A Review on AWS - Cloud Computing Technology”, International Journal for Research in Applied Science and Engineering Technology, 10.22214/ijraset.2022.39802, 2022, Vol 10(1)
- D. Stalin David, Mamoona Anam, Chandraprabha Kaliappan, S. Arun Mozhi Selvi, Dilip Kumar Sharm, “Cloud Security Service for Identifying Unauthorized User Behaviour”, Computers Materials & Continua, 10.32604/cmc.2022.020213, 2022, Vol 70(2)
- 임재덕, “클라우드 컴퓨팅 발전법 주요내용 및 정책방향”, 미래창조과학부
- 임철수, “클라우드 컴퓨팅 보안기술”, 정보보호학회지 정보보호 특집
- 앤서니 T, “미래코드 클라우드 컴퓨팅”, 전자신문사
- 편집부, “클라우드 컴퓨팅 차세대 컴퓨팅 기술”, 데이코 산업 연구소
- 임철수, “클라우드 컴퓨팅의 기초” 서경대학교
- 정인호, “클라우드 컴퓨팅”, 명지대학교

화면설명

이미지 번호

내레이션

8회차 메타데이터

- 주요학습내용 : 해당 회차 또는 레슨의 주요학습내용을 자세히 기입해 주세요.
- 검색 키워드 : 학습자가 검색창에 어떤 검색어를 입력하면 본 회차 또는 본 레슨이 검색될 수 있을지 검색 키워드를 5개 기입해 주세요.

제목	주요학습내용	검색 키워드1	검색 키워드2	검색 키워드3	검색 키워드4	검색 키워드5
계정보안 : VPC2	• VPC 생성 실습 • Gateway / Subnet 설정 실습 • 웹서버 인스턴스 실행 실습	클라우드 보안	VPC 생성	게이트웨이 설정	서브넷 설정	웹서버 인스턴스 실행