

VPC - practice

Sung-Dong Kim,
School of Computer Engineering,
Hansung University

Contents

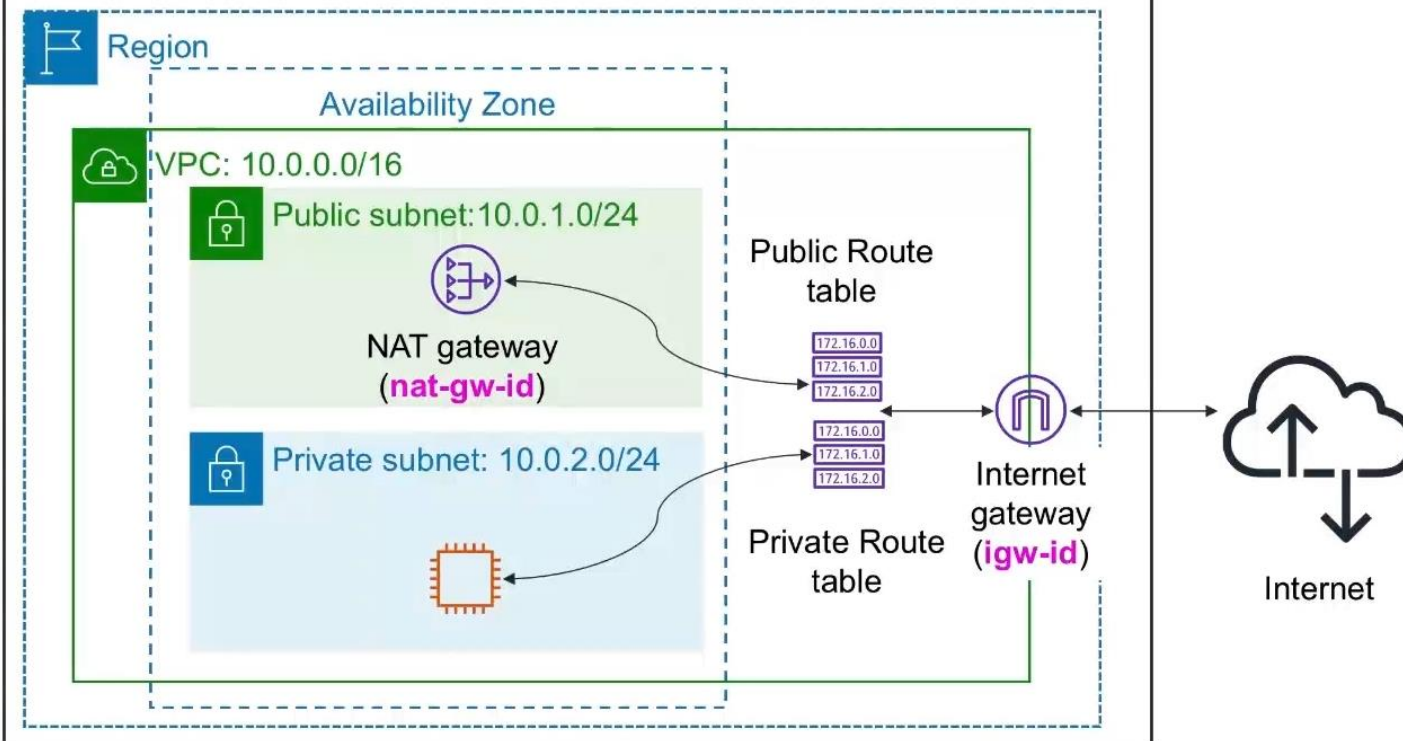
- ▶ VPC 및 VPC 관련 요소 검토
- ▶ VPC 생성 실습
 - ▶ Internet gateway 연결
 - ▶ Subnet 추가
 - ▶ Routing Table 정의: IG와 subnet간 traffic flow

NAT Gateway

- ▶ VPC 마법사 → NAT gateway를 시작함
 - ▶ private subnet에 구축되는 private resource에 대한 internet access 제공
 - ▶ 공용 인터넷 (public internet)에 접속함
 - ▶ EIP가 할당됨

Amazon VPC Demo

aws AWS Cloud



Public subnet route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id

Private subnet route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	nat-gw-id

Step 2: VPC with Public and Private Subnets

IPv4 CIDR block: (65531 IP addresses available)

IPv6 CIDR block: ☒ No IPv6 CIDR Block
☐ Amazon provided IPv6 CIDR block
☐ IPv6 CIDR block owned by me

VPC name:

Public subnet's IPv4 CIDR: (251 IP addresses available)

Availability Zone:

Public subnet name:

Private subnet's IPv4 CIDR: (251 IP addresses available)

Availability Zone:

Private subnet name:

You can add more subnets after AWS creates the VPC.

Specify the details of your NAT gateway ([NAT gateway rates apply](#)).

Elastic IP Allocation ID:

Service endpoints

Enable DNS hostnames: ☒ Yes ☐ No

Hardware tenancy:

Steps

- ▶ Step 1: EIP 생성 (고정 IP) → NAT gateway에 할당됨
- ▶ Step 2: VPC 생성 (VPC 마법사)
 - ▶ VPC 대시보드 → VPC 생성 → VPC등 = **my-vpc**

VPC 설정

생성할 리소스 정보

VPC 리소스 또는 VPC 및 기타 네트워킹 리소스만 생성합니다.

☐ VPC만

☒ VPC 등

이름 태그 자동 생성 정보

이름 태그의 값을 입력합니다. 이 값은 VPC의 모든 리소스에 대한 이름 태그를 자동으로 생성하는 데 사용됩니다.

☒ 자동 생성

my

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

1

프라이빗 서브넷 수 정보

VPC에 추가할 프라이빗 서브넷 수입니다. 프라이빗 서브넷을 사용하여 퍼블릭 액세스가 필요 없는 백엔드 리소스를 보호합니다.

0

1

2

▼ 서브넷 CIDR 블록 사용자 지정

ap-northeast-2a 퍼블릭 서브넷 CIDR 블록

10.0.1.0/24

256 IPs

ap-northeast-2a 프라이빗 서브넷 CIDR 블록

10.0.2.0/24

256 IPs

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

- ☒ DNS 호스트 이름 활성화
- ☒ DNS 확인 활성화

VPC 세부 정보 표시

AWS 가상 네트워크

my-vpc

서브넷(2개)

이 VPC 내의 서브넷

ap-northeast-2a

my-subnet-public1-ap-northeast-2a

my-subnet-private1-ap-northeast-2a

라우팅 테이블(2개)









네트워크 트래픽을 리소스로 라우팅

my-rtb-public

my-rtb-private1-ap-northeast-2a

✔ 성공

▼ 세부 정보

- ✔ VPC 생성: [vpc-0c698debd965bb9f6](#) 
- ✔ Enable DNS hostnames
- ✔ Enable DNS resolution
- ✔ Verifying VPC creation: [vpc-0c698debd965bb9f6](#) 
- ✔ Create subnet: [subnet-0460d2104499d951b](#) 
- ✔ Create subnet: [subnet-06fcfba83a3a1377e](#) 
- ✔ Create internet gateway: [igw-07111c1173792a411](#) 
- ✔ Attach internet gateway to the VPC
- ✔ Create route table: [rtb-06676e4de059b6370](#) 
- ✔ Create route
- ✔ Associate route table
- ✔ Allocate elastic IP: [eipalloc-0459e52fb494705aa](#) 
- ✔ Create NAT gateway: [nat-010f32ed804996b53](#) 
- ✔ Wait NAT Gateways to activate
- ✔ Create route table: [rtb-0a5a3b052b606ac2f](#) 
- ✔ Create route
- ✔ Associate route table
- ✔ Verifying route table creation

확인

- ▶ 인터넷 게이트웨이 = my-igw
- ▶ public/private 서브넷

<input checked="" type="checkbox"/>	Name ▾	서브... ▾	상태 ▾	VPC ▾	IPv4 CI... ▾
<input checked="" type="checkbox"/>	my-subnet-public1-a...	subnet...	✔ Available	vpc-0c698debd965bb9f6 my-vpc	10.0.1.0/24
<input checked="" type="checkbox"/>	my-subnet-private1-...	subnet...	✔ Available	vpc-0c698debd965bb9f6 my-vpc	10.0.2.0/24

확인

- ▶ 사용 가능한 주소: 250
- ▶ 라우팅 테이블
 - ▶ local: VPC 내부 다른 위치로 향하는 traffic
 - ▶ 공용 인터넷: 0.0.0.0/0 → IG
- ▶ why public: IG 경로가 포함된 routing table에 연결되어 있음
 - ▶ IG를 통해 외부와 연결됨

라우팅 테이블: [rtb-06676e4de059b6370 / my-rtb-public](#)

라우팅 (2)

🔍 라우팅 필터링

대상	대상
10.0.0.0/16	local
0.0.0.0/0	igw-07111c1173792a411

확인

- ▶ Network ACLs
 - ▶ subnet 안팎으로 전송되는 traffic을 제어하는 방화벽 역할을 하는 VPC에 대한 선택적 보안 계층
 - ▶ 기본: 모든 트래픽 허용 (wide open)
 - ▶ inbound / outbound rules
 - ▶ 보안그룹: resource에 대한 추가적인 방화벽 역할

확인

- ▶ private subnet
 - ▶ 사용 가능한 주소: 251
 - ▶ routing table
 - ▶ local: VPC 내부에서의 트래픽을 처리하는 local 경로
 - ▶ NAT
 - ▶ private에서 public internet으로의 단방향 연결 정의
 - ▶ private subnet 내의 resource에 대한 patch, update traffic 제공

라우팅 테이블: [rtb-0a5a3b052b606ac2f](#) / [my-rtb-private1-ap-northeast-2a](#)

라우팅 (2)

🔍 라우팅 필터링

대상	대상
10.0.0.0/16	local
0.0.0.0/0	nat-010f32ed804996b53

정리

- ▶ NAT 삭제
- ▶ EIP 릴리스
- ▶ 서브넷 삭제 (public, private)
- ▶ 인터넷게이트웨이 → 작업 → VPC에서 분리 → 삭제
- ▶ VPC 삭제
 - ▶ routing table 함께 자동 삭제됨