

# AWS 운영 기초

유정현

# 목차

1. VPC, Public Subnet, Private Subnet 생성
2. Public IP 자동할당 설정
3. IGW 생성 및 연결
4. Route Table 생성, Subnet 추가, IGW 연결
5. Bastion Host 생성
6. Private Instance 생성
7. NAT gateway 생성 및 연결

# 1. VPC, Subnet

10.0.0.0/16 IPv4 CIDR 블록을 가지는 VPC를 생성

가용영역 A와 B에 각각 VPC의 IPv4 CIDR 블록에 포함되는 Private, Public Subnet을 생성

Name ▼	VPC ID ▼	State ▼	IPv4 CIDR
testVPC	vpc-05b3b4b1fac40a9a2	✔ Available	10.0.0.0/16

Name ▼	Subnet ID ▼	State ▼	VPC ▼	IPv4 CIDR ▼
PrivateSubnetA	subnet-098037c1b09d22408	✔ Available	vpc-05b3b4b1fac40a9a2   test...	10.0.16.0/20
PublicSubnetA	subnet-0cfd01ed817c74da9	✔ Available	vpc-05b3b4b1fac40a9a2   test...	10.0.0.0/24
PrivateSubnetB	subnet-069e7afe931689ccc	✔ Available	vpc-05b3b4b1fac40a9a2   test...	10.0.32.0/20
PublicSubnetB	subnet-0a8d53401b07bd4db	✔ Available	vpc-05b3b4b1fac40a9a2   test...	10.0.1.0/24

## 2. Public IP 자동할당

현재는 instance 생성 시 Public IP를 할당하지 않는다

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of lower prices, or request Reserved Instances for a lower price over a long-term commitment.

Number of instances ⓘ

1

[Launch into Auto Scaling Group ⓘ](#)

Purchasing option ⓘ

☐ Request Spot instances

Network ⓘ

vpc-05b3b4b1fac40a9a2 | testVPC



[Create new VPC](#)

Subnet ⓘ

subnet-0cfd01ed817c74da9 | PublicSubnetA | ap-northeast-1

251 IP Addresses available

[Create new subnet](#)

Auto-assign Public IP ⓘ

Use subnet setting (Disable)

## 2. Public IP 자동할당

외부 연결이 필요한 Public Subnet의 설정을 수정해 IPv4 자동할당을 활성화

Subnets (1/8) [Info](#)

Filter subnets

	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6	
<input type="checkbox"/>	-	subnet-2908f666	Available	vpc-fa891191   default	172.31.32.0/20	-	
<input type="checkbox"/>	PrivateSubnetA	subnet-098037c1b09d22408	Available	vpc-05b3b4b1fac40a9a2   test...	10.0.16.0/20	-	
<input type="checkbox"/>	-	subnet-a9a368f6	Available	vpc-fa891191   default	172.31.48.0/20	-	
<input type="checkbox"/>	-	subnet-ac7d3ad7	Available	vpc-fa891191   default	172.31.16.0/20	-	
<input type="checkbox"/>	-	subnet-ef70fa84	Available	vpc-fa891191   default	172.31.0.0/20	-	
<input checked="" type="checkbox"/>	PublicSubnetA	subnet-0cfd01ed817c74da9	Available	vpc-05b3b4b1fac40a9a2   test...	10.0.0.0/24	-	

Actions

View details

Create flow log

Edit subnet settings

Edit IPv6 CIDRs

Edit network ACL associ

Edit route table associa

Edit CIDR reservations

Share subnet

Manage tags

### Auto-assign IP settings [Info](#)

Enable the auto-assign IP settings to automatically request a public IPv4 or IPv6 address for a new network interface in this subnet.

☒ Enable auto-assign public IPv4 address [Info](#)

☐ Enable auto-assign customer-owned IPv4 address [Info](#)  
Option disabled because no customer owned pools found.

## 2. Public IP 자동할당

instance 생성 시 Public IP를 할당하는 것을 확인 가능

1. Choose AMI   2. Choose Instance Type   **3. Configure Instance**   4. Add Storage   5. Add Tags   6. Configure Security Group   7. Review

### Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of lower prices, or launch instances into an Auto Scaling Group.

Number of instances ⓘ

1

[Launch into Auto Scaling Group ⓘ](#)

Purchasing option ⓘ

☐ Request Spot instances

Network ⓘ

vpc-05b3b4b1fac40a9a2 | testVPC



[Create new VPC](#)

Subnet ⓘ

subnet-0cfd01ed817c74da9 | PublicSubnetA | ap-northeast-1

251 IP Addresses available

[Create new subnet](#)

Auto-assign Public IP ⓘ

Use subnet setting (Enable)

# 3. Internet Gateway

Internet Gateway를 생성 후 VPC에 연결

Name ▾	Internet gateway ID ▾	State ▾
testIGW	<a href="#">igw-0eefad139f037d885</a>	⊖ Detached

[VPC](#) > [Internet gateways](#) > [igw-0eefad139f037d885](#)

igw-0eefad139f037d885 / testIGW

Actions ▲

Attach to VPC

Name ▾	Internet gateway ID ▾	State ▾	VPC ID
testIGW	<a href="#">igw-0eefad139f037d885</a>	✔ Attached	<a href="#">vpc-00a58e0c6b61b107b</a>   testVPC

# 4. Route Table

VPC에 이미 존재하는 Route Table은 Private으로 변경, Public Route Table은 생성  
Private에는 Private Subnet, Public에는 Public Subnet을 명시적으로 연결

Name ▼	Route table ID ▼
PublicRT	<a href="#">rtb-0a34491e57835b985</a>
PrivateRT	<a href="#">rtb-0de0db1c39e9f46d2</a>

## Edit subnet associations

Change which subnets are associated with this route table.

### Available subnets (2/4)

🔍 Filter subnet associations

< 1 > ⚙️

<input checked="" type="checkbox"/>	Name ▼	Subnet ID ▼	IPv4 CIDR ▼	IPv6 CIDR ▼	Route table ID ▼
<input checked="" type="checkbox"/>	PrivateSubnetA	subnet-098037c1b09d22408	10.0.16.0/20	–	Main (rtb-0de0db1c39e9f46d2 / PrivateRT)
<input type="checkbox"/>	PublicSubnetA	subnet-0cfd01ed817c74da9	10.0.0.0/24	–	Main (rtb-0de0db1c39e9f46d2 / PrivateRT)
<input checked="" type="checkbox"/>	PrivateSubnetB	subnet-069e7afe931689ccc	10.0.32.0/20	–	Main (rtb-0de0db1c39e9f46d2 / PrivateRT)
<input type="checkbox"/>	PublicSubnetB	subnet-0a8d53401b07bd4db	10.0.1.0/24	–	Main (rtb-0de0db1c39e9f46d2 / PrivateRT)

### Selected subnets

[subnet-069e7afe931689ccc / PrivateSubnetB](#) ✕ [subnet-098037c1b09d22408 / PrivateSubnetA](#) ✕

Cancel

Save associations



# 4. Route Table

외부 연결이 필요한 Public Route Table에 Internet Gateway를 연결

### Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	<input type="text" value="local"/>	Active	No
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="igw-0685f6392b4e14d30"/>	-	No

### Routes (2)

Both

< 1 >

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-0685f6392b4e14d30	Active	No

# 5. Public Instance

외부 연결이 가능하도록 Public Subnet A에 Bastion Instance를 생성

AMI : Linux / Instance Type : t2.micro / Security Group : SSH, HTTP 허용

Name ▾	Instance ID	Instance state ▾	Instance type ▾	Status check	Alarm status	Availability Zone ▾
Bastion	i-0935a9c82b3bf3ac7	✓ Running 🔍	t2.micro	✓ 2/2 checks passed	No alarms +	ap-northeast-2a

외부 연결이 가능한 것 확인

```

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

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-0-68 ~]$ ping google.com
PING google.com (172.217.175.46) 56(84) bytes of data.
64 bytes from nrt20s19-in-f14.1e100.net (172.217.175.46): icmp_seq=1 ttl=105 time=31.5 ms
64 bytes from nrt20s19-in-f14.1e100.net (172.217.175.46): icmp_seq=2 ttl=105 time=31.6 ms
64 bytes from nrt20s19-in-f14.1e100.net (172.217.175.46): icmp_seq=3 ttl=105 time=31.6 ms
```

## 6. Private Instance

외부 연결이 불가능하도록 Private Subnet A에 Web Instance를 생성  
AMI : Linux / Instance Type : t2.micro / Security Group : SSH, HTTP 허용

Name ▼	Instance ID	Instance state ▼	Instance type ▼	Status check	Alarm status	Availability Zone ▼
web	i-0d64d4fd331449cb5	Running	t2.micro	2/2 checks passed	No alarms +	ap-northeast-2a

Bastion에는 IPv4 할당, Web에는 IPv4 할당되지 않은 것 확인 가능

<b>Instance summary for i-0182d943bfad9e1b2 (Bastion)</b> <a href="#">Info</a>				<a href="#">Connect</a>	<a href="#">I</a>
Updated less than a minute ago					
Instance ID	Public IPv4 address		Private IPv4 addresses		
i-0182d943bfad9e1b2 (Bastion)	13.209.73.1   <a href="#">open address</a>		10.0.1.183		
<b>Instance summary for i-0f9d51fd1d4777da9 (web)</b> <a href="#">Info</a>				<a href="#">Connect</a>	
Updated less than a minute ago					
Instance ID	Public IPv4 address		Private IPv4 addresses		
i-0f9d51fd1d4777da9 (web)	-		10.0.43.188		

## 6. Private Instance

Bastion Instance를 통해서 내부 IP로 접속이 가능

```
[ec2-user@ip-10-0-1-183 ~]$ sudo ssh -i aws.pem ec2-user@10.0.43.188  
  
  _ |  _ |  _ )  
  _ | ( _ | /  Amazon Linux 2 AMI  
  _ |\ _ | _ |  
  
https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-10-0-43-188 ~]$
```

그러나 외부 인터넷과는 연결이 불가능

```
[ec2-user@ip-10-0-43-188 ~]$ ping google.com  
PING google.com (142.251.42.142) 56(84) bytes of data.  
^C  
--- google.com ping statistics ---  
2 packets transmitted, 0 received, 100% packet loss, time 1015ms
```

# 7. NAT Gateway

Web Instance에서도 외부 인터넷 연결이 가능하도록 Public Subnet에 NAT Gateway를 생성

## Create NAT gateway [Info](#)

A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.

### NAT gateway settings

#### Name - *optional*

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

The name can be up to 256 characters long.

#### Subnet

Select a subnet in which to create the NAT gateway.

할당 받은 Elastic IP를 연결

#### Elastic IP allocation ID [Info](#)

Assign an Elastic IP address to the NAT gateway.

# 7. NAT Gateway

Private Route Table에 추가해줘야 Private Subnet에서도 외부 인터넷 연결이 가능

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	nat-05bc151ee4a0b7136	-	No

Add route

Cancel Preview Save changes

이제 Web Instance에서도 외부 인터넷 접속 가능

```
[ec2-user@ip-10-0-43-188 ~]$ ping google.com
PING google.com (142.251.42.142) 56(84) bytes of data:
64 bytes from nrt12s45-in-f14.1e100.net (142.251.42.142): icmp_seq=1 ttl=100 time=34.8 ms
64 bytes from nrt12s45-in-f14.1e100.net (142.251.42.142): icmp_seq=2 ttl=100 time=34.5 ms
64 bytes from nrt12s45-in-f14.1e100.net (142.251.42.142): icmp_seq=3 ttl=100 time=34.4 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 34.471/34.607/34.838/0.270 ms
```