

1 Lab. Creating Bastion Host
2
3 1. VPC 생성
4 1)[생성할 리소스] : VPC만
5 2)[이름 태그] : lab-vpc
6 3)[IPv4 CIDR 블록] : IPv4 CIDR 수동 입력
7 4)[IPv4 CIDR] : 10.0.0.0/16
8 5)[IPv6 CIDR 블록] : IPv6 CIDR 블록 없음
9 6)[태년시] : 기본값
10 7)[VPC 생성] 버튼 클릭
11
12
13 2. 인터넷 게이트웨이 생성
14 1)[이름 태그] : lab-igw
15 2)[인터넷 게이트웨이 생성] 버튼 클릭
16 3)[작업] > [VPC에 연결] 클릭
17 4)[VPC에 연결] 페이지에서,
18 -[사용 가능한 VPC] : lab-vpc
19 -[인터넷 게이트웨이 연결] 버튼 클릭
20
21 5)[상태]가 Attached 확인
22
23
24 3. 서브넷 생성하기
25 1)[서브넷 생성] 페이지에서,
26 -[VPC ID] : lab-vpc
27 -[서브넷 이름] : lab-public-subnet
28 -[가용 영역] : ap-northeast-2a
29 -[IPv4 VPCCIDR block] : 10.0.0.0/16
30 -[IPv4 subnet CIDR block] : 10.0.10.0/24
31 -[서브넷 생성] 버튼 클릭
32
33 2)[서브넷 생성] 페이지에서,
34 -[VPC ID] : lab-vpc
35 -[서브넷 이름] : lab-private-subnet
36 -[가용 영역] : ap-northeast-2c
37 -[IPv4 VPCCIDR block] : 10.0.0.0/16
38 -[IPv4 subnet CIDR block] : 10.0.20.0/24
39 -[서브넷 생성] 버튼 클릭
40
41 3)위와 같이 Private Subnet과 Public Subnet을 생성함.
42
43
44 4. 라우팅 테이블 생성하기
45 1)[라이팅 테이블 생성] 페이지에서,
46 -[이름] : lab-public-rt
47 -[VPC] : lab-vpc
48 -[라우팅 테이블 생성] 버튼 클릭
49 -[서브넷 연결] 탭 클릭
50 -[서브넷 연결 편집] 버튼 클릭
51 -[이용 가능한 서브넷] 페이지에서
52 --lab-public-subnet 체크
53 --[연결 저장] 버튼 클릭
54 -[라우팅] 탭에서
55 --[라우팅 편집] 버튼 클릭

```

56      --[라우팅 편집] 페이지에서,
57      ---[라우팅 추가] 버튼 클릭
58      ---[대상] : 0.0.0.0/0
59      ---[대상] : 인터넷 게이트웨이, lab-igw
60      ---[변경 사항 저장] 버튼 클릭
61
62  2)[라이팅 테이블 생성] 페이지에서,
63      -[이름] : lab-private-rt
64      -[VPC] : lab-vpc
65      -[라우팅 테이블 생성] 버튼 클릭
66      -[서브넷 연결] 탭 클릭
67      -[서브넷 연결 편집] 버튼 클릭
68      -[이용 가능한 서브넷] 페이지에서
69          --lab-private-subnet 체크
70          --[연결 저장] 버튼 클릭
71
72  3)위와 같이 Public Routing Table은 Public Subnet에 연결하고, Internet Gateway까지 연결하는
73  Routing Table을 생성하고, Private Routing Table은 Private Subnet에 연결하였다.
74
75  5. 보안 그룹 생성
76  1)[보안 그룹 생성] 페이지에서,
77      -[보안 그룹 이름] : lab-bastionhost-sg
78      -[설명] : Security Group for Bastion Host
79      -[VPC] : lab-vpc
80      -[인바운드 규칙] 섹션에서,
81          --[규칙 추가]
82              ---모든 ICMP-IPv4, 0.0.0.0/0
83              ---SSH, 22, 0.0.0.0/0
84      -[태그]
85          --[새로운 태그 추가] 버튼 클릭
86          --[키] : Name
87          --[값] : lab-bastionhost-sg
88
89  2)[보안 그룹 생성] 페이지에서,
90      -[보안 그룹 이름] : lab-private-sg
91      -[설명] : Security Group for Private EC2 Instance
92      -[VPC] : lab-vpc
93      -[인바운드 규칙] 섹션에서,
94          --[규칙 추가]
95              ---모든 ICMP-IPv4, 사용자 지정, lab-bastionhost-sg
96              ---SSH, 22, 사용자 지정, lab-bastionhost-sg
97      -[태그]
98          --[새로운 태그 추가] 버튼 클릭
99          --[키] : Name
100          --[값] : lab-bastionhost-sg
101
102
103  6. Public EC2 Instance(Bastion Host) 생성하기
104  1)[이름] : Bastion Host
105  2)[AMI] : Ubuntu 22.04 LTS, 64-bit
106  3)[인스턴스 유형] : t2.micro
107  4)[키 페어(로그인)] : 새 키 페어 생성 -> Bastion-Host-Key.pem
108  5)[네트워크 설정] > [편집] 클릭
109      -[VPC] : lab-vpc

```

-[서브넷] : lab-public-subnet
-[퍼블릭 IP 자동 할당] : 활성화
-[방화벽] : 기존 보안 그룹 선택 -> lab-bastionhost-sg

6)[스토리지 구성] : 8GiB, gp2

7. Private EC2 Instance 생성하기

1)[이름] : lab-private-ec2
2)[AMI] : Ubuntu 22.04 LTS, 64-bit
3)[인스턴스 유형] : t2.micro
4)[키 페어(로그인)] : 새 키 페어 생성 -> lab-private-ec2-key.pem
5)[네트워크 설정] > [편집] 클릭
-[VPC] : lab-vpc
-[서브넷] : lab-private-subnet
-[퍼블릭 IP 자동 할당] : 비활성화
-[방화벽] : 기존 보안 그룹 선택 -> lab-private-sg

6)[스토리지 구성] : 8GiB, gp2

8. Bastion Host를 통한 Private EC2 Instance 접근하기

1)키 파일 복사 및 Bastion Host(Public EC2) 접속

-lab-private-ec2-key.pem 파일을 Bastion Host로 복사

```
$ scp -i Bastion-Host-Key.pem ./lab-private-ec2-key.pem  
ubuntu@52.79.145.199:/home/ubuntu
```

The authenticity of host '52.79.145.199 (52.79.145.199)' can't be established.

ECDSA key fingerprint is SHA256:5INwdm7RBhCkBDNfUWo3X/GwLqLFtqpmrRTK7U2vJw0.

Are you sure you want to continue connecting (yes/no/[fingerprint])?

Warning: Permanently added '52.79.145.199' (ECDSA) to the list of known hosts.

```
lab-private-ec2-key.pem                                100% 1678  
117.0KB/s   00:00.
```

-Bastion-Host-Key.pem 파일의 권한을 600으로 변경한다(현재 Linux or macOS의 경우)

```
$ chmod 600 Bastion-Host-Key.pem
```

-SSH Client Tool을 통해 Bastion Host 연결하기

-연결하면 위에서 복사한 private-ec2-key.pem 파일을 확인할 수 있다.

2)Bastion Host에서 Private EC2로 접속

-Bastion Host에서 lab-private-ec2-key.pem 파일의 권한을 600으로 변환

```
$ chmod 600 lab-private-ec2-key.pem
```

-lab-private-ec2-key.pem을 이용하여 Private EC2 Instance에 접속한다.

```
$ ssh -i lab-private-ec2-key.pem ubuntu@10.0.20.44
```

The authenticity of host '10.0.20.44 (10.0.20.44)' can't be established.

ED25519 key fingerprint is SHA256:IPewgzD2BrwUDCiXO7bsbtKb8y3R5A3COpQr5LrvlbQ.

This key is not known by any other names

Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Warning: Permanently added '10.0.20.44' (ED25519) to the list of known hosts.

Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.19.0-1025-aws x86_64)

3)Bastion Host에서 Private EC2 Instance에 성공적으로 연결하였다.