Virtual Private Cloud(VPC)

- Starter 계정의 경우 네트워크 설정 이후의 실습 진행을 위해서 리전을 버지니아 북부, 오하이오, 오레곤으로 설정하여 진행하십시오.

VPC 설정

VPC 만들기

VPC는 AWS 클라우드의 격리된 부분으로서, Amazon EC2 인스턴스와 같은 AWS 객체로 채워집니다. VPC에 대한 IPv4 주소 범위를 지정해야 합니다. IPv4 주소 범위를 CIDR(Classless Inter-Domain Routing) 블록으로 지정합니다(예: 10.0.0.0/16). /16보다 큰 IPv4 CIDR 블록은 지정할 수 없습니다. 또는 Amazon 제공 IPv6 CIDR 블록을 VPC에 연결할 수 있습니다.

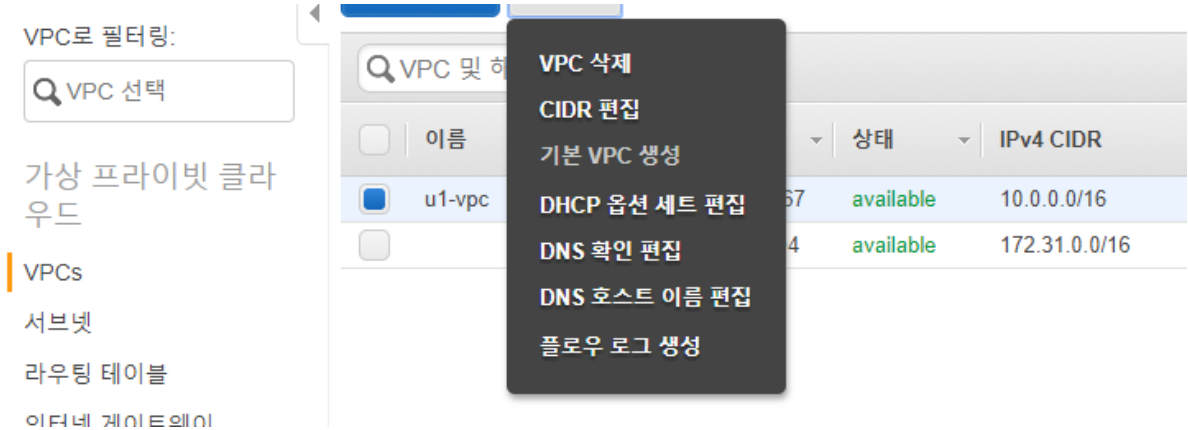
Name 태그 u1-vpc

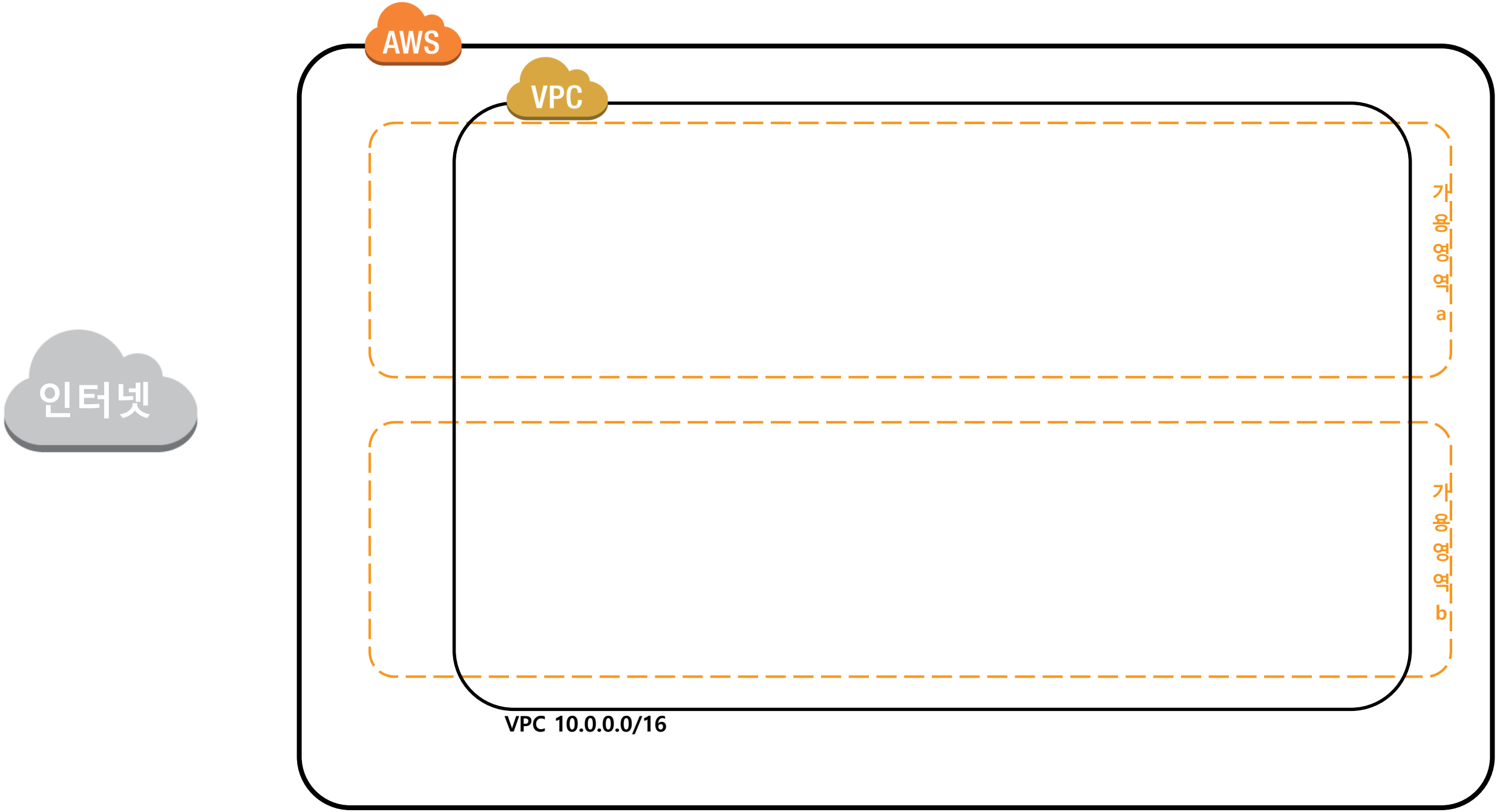
IPv4 CIDR 블록* 10.0.0.0/16

IPv6 CIDR 블록* ◉ IPv6 CIDR 블록 없음
○ Amazon에서 IPv6 CIDR 블록 제공

테넌시 기본값

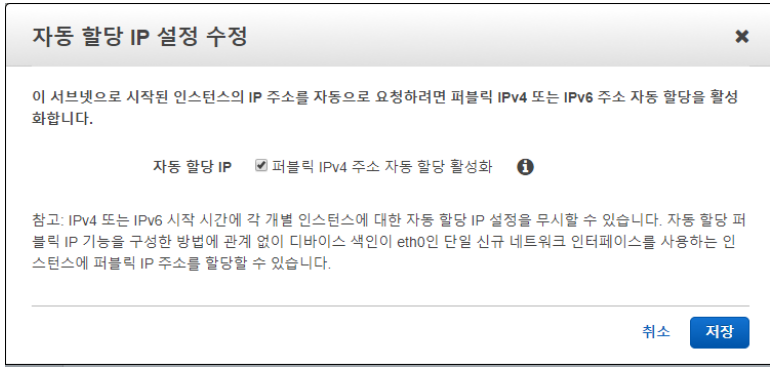
취소 | 예, 생성




AWS
VPC
가용영역 a
가용영역 b
인터넷
VPC 10.0.0.0/16
오레곤 리전

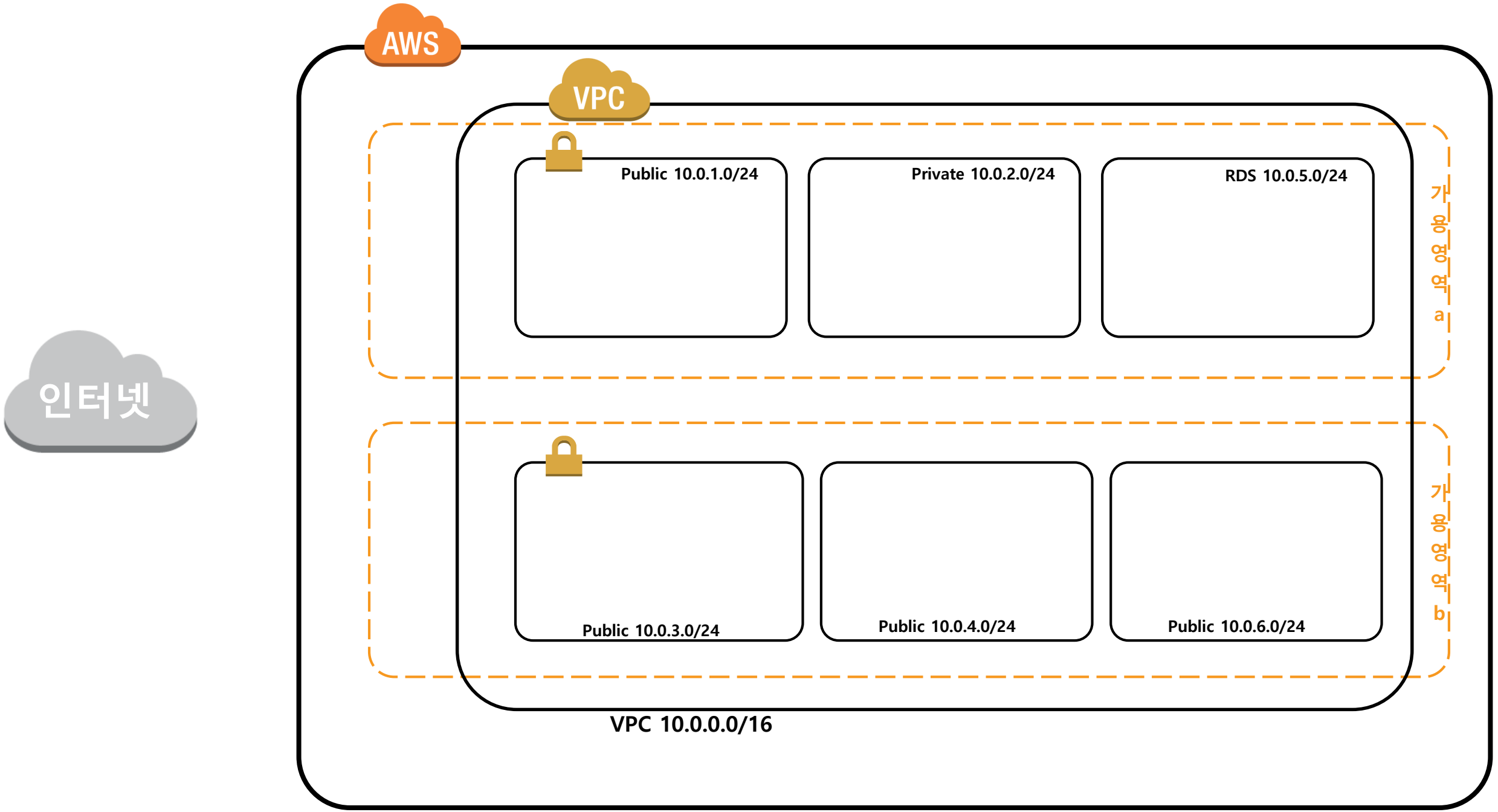
서브넷 설정

서브넷 내의 리소스에 IP를 자동 할당하려면 해당 서브넷을 체크하고 서브넷 작업에서 “자동 할당 IP 설정 수정“-



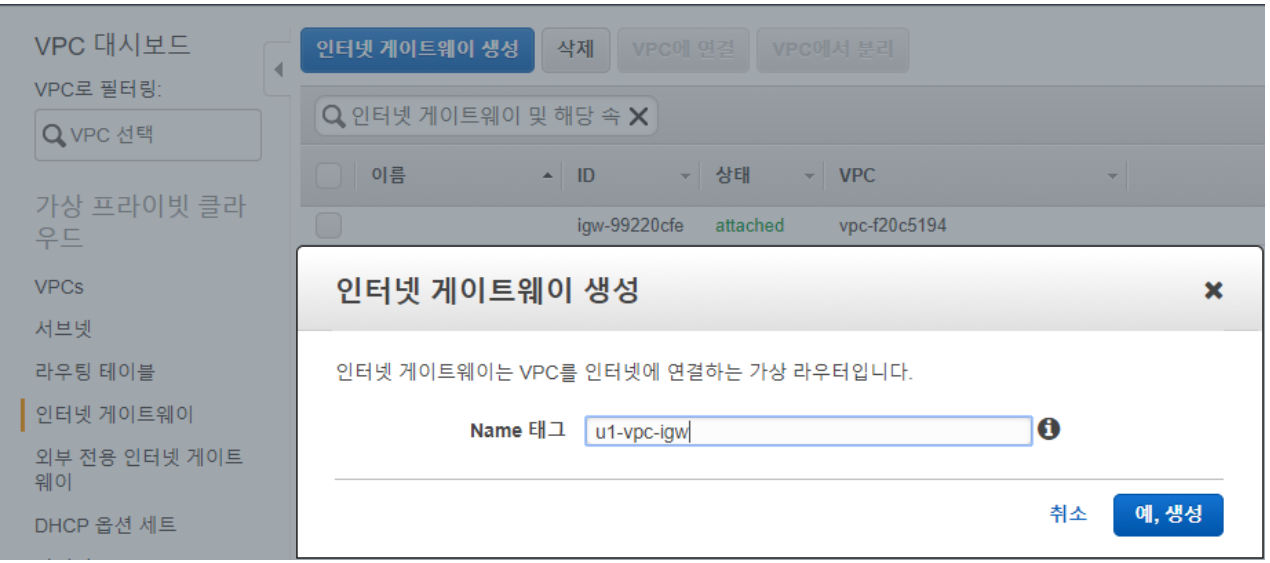
가용영역2a에 퍼블릭 서브넷: u1-subnet-uw2a-public 10.0.1.0/24
가용영역2a에 프라이빗 서브넷: u1-subnet-uw2a-public 10.0.2.0/24
가용영역2b에 퍼블릭 서브넷: u1-subnet-uw2b-public 10.0.3.0/24
가용영역2b에 프라이빗 서브넷: u1-subnet-uw2b-public 10.0.4.0/24
가용영역2a에 RDS 서브넷: u1-subnet-uw2a-rds 10.0.5.0/24
가용영역2b에 RDS 서브넷: u1-subnet-uw2b-rds 10.0.6.0/24

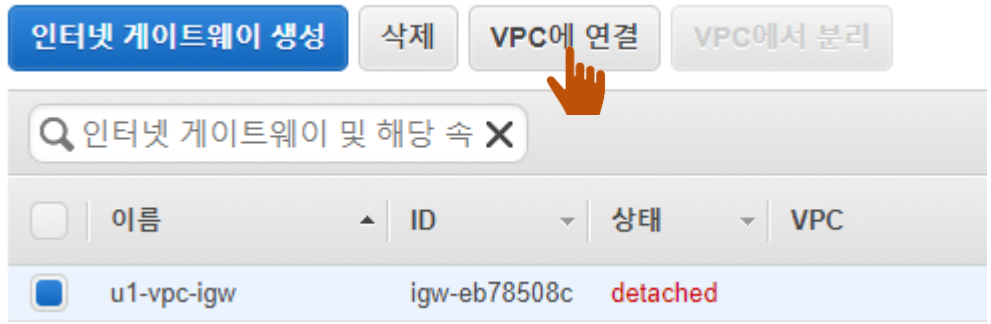
이름	서브넷 ID	상태	VPC	IPv4 CIDR	사용 가능한 IPv4	IPv6 CIDR	가용 영역	라우팅 테이블	네트워크 ACL	기본 서브넷	퍼블릭 IP 자동 할당	자동 할당 IPv6 주소
u1-subnet-uw2b-rds	subnet-fe63e3b6	available	vpc-0191cd67 | u1-vpc	10.0.6.0/24	251		us-west-2b	rtb-b123adc8	acl-33ee114a	아니요	예	아니요
u1-subnet-uw2b-public	subnet-d2eb6b9a	available	vpc-0191cd67 | u1-vpc	10.0.3.0/24	251		us-west-2b	rtb-7f6ae306 | u1-subnet-public-rtb	acl-33ee114a	아니요	예	아니요
u1-subnet-uw2b-private	subnet-cce76784	available	vpc-0191cd67 | u1-vpc	10.0.4.0/24	251		us-west-2b	rtb-706ae309 | u1-subnet-private-rtb	acl-33ee114a	아니요	예	아니요
u1-subnet-uw2a-rds	subnet-9c6c0ffa	available	vpc-0191cd67 | u1-vpc	10.0.5.0/24	251		us-west-2a	rtb-b123adc8	acl-33ee114a	아니요	예	아니요
u1-subnet-uw2a-public	subnet-c5f797a3	available	vpc-0191cd67 | u1-vpc	10.0.1.0/24	249		us-west-2a	rtb-7f6ae306 | u1-subnet-public-rtb	acl-33ee114a	아니요	예	아니요
u1-subnet-uw2a-private	subnet-60fb9b06	available	vpc-0191cd67 | u1-vpc	10.0.2.0/24	251		us-west-2a	rtb-706ae309 | u1-subnet-private-rtb	acl-33ee114a	아니요	예	아니요


AWS
VPC
Public 10.0.1.0/24
Private 10.0.2.0/24
RDS 10.0.5.0/24
가용영역 a
인터넷
Public 10.0.3.0/24
Public 10.0.4.0/24
Public 10.0.6.0/24
가용영역 b
VPC 10.0.0.0/16

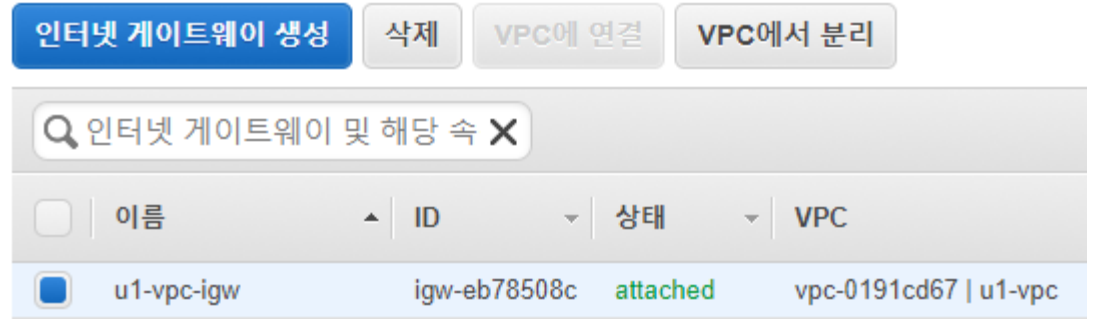
오레곤 리전

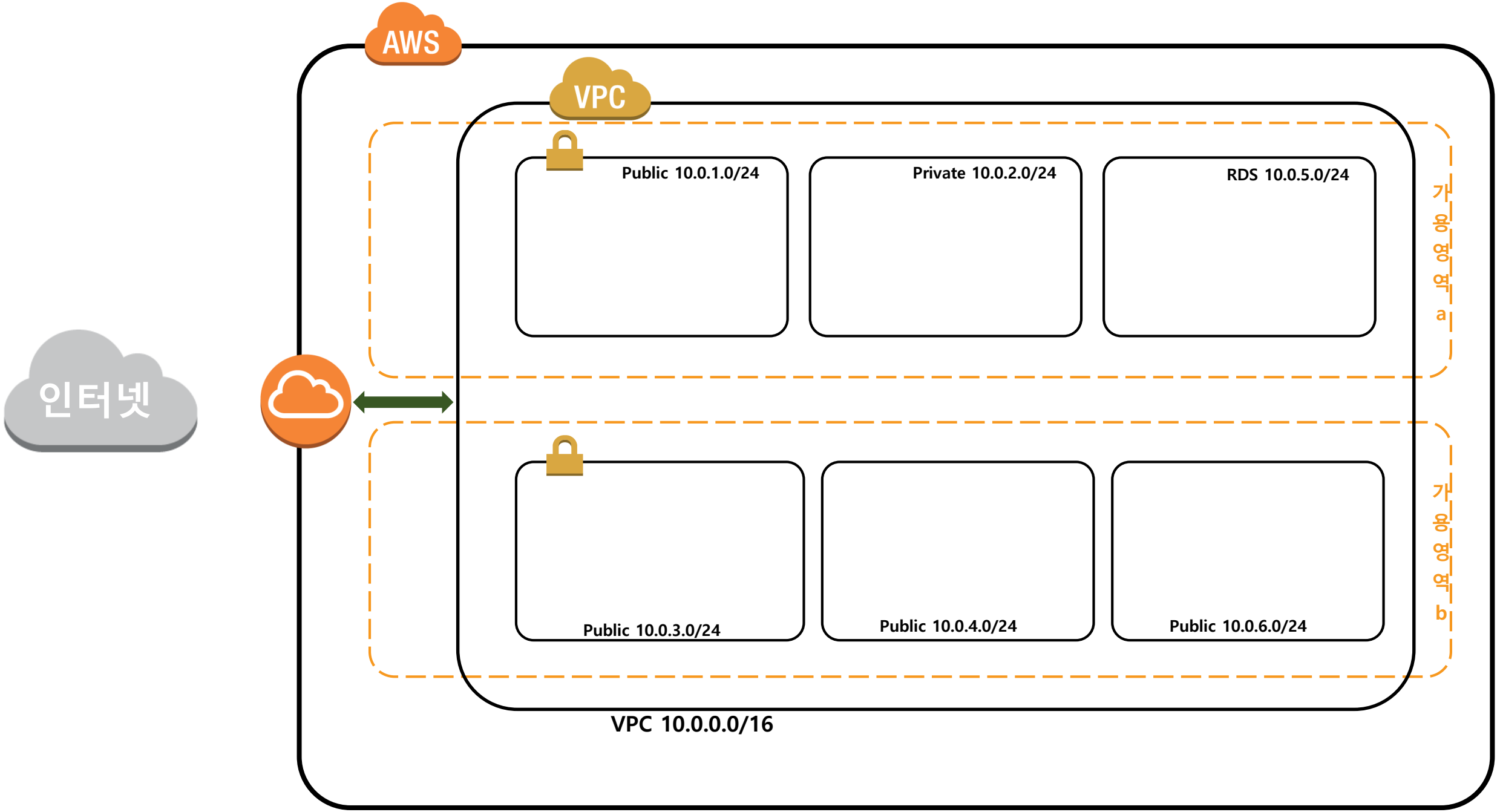
인터넷 게이트웨이 설정


VPC 대시보드
VPC로 필터링:
VPC 선택
가상 프라이빗 클라우드
VPCs
서브넷
라우팅 테이블
인터넷 게이트웨이
외부 전용 인터넷 게이트웨이
DHCP 옵션 세트
인터넷 게이트웨이 생성
삭제
VPC에 연결
VPC에서 분리
인터넷 게이트웨이 및 해당 속
이름
ID
상태
VPC
igw-99220cfe
attached
vpc-f20c5194
인터넷 게이트웨이 생성
인터넷 게이트웨이는 VPC를 인터넷에 연결하는 가상 라우터입니다.
Name 태그
u1-vpc-igw
취소
예, 생성


인터넷 게이트웨이 생성
삭제
VPC에 연결
VPC에서 분리
인터넷 게이트웨이 및 해당 속
이름
ID
상태
VPC
u1-vpc-igw
igw-eb78508c
detached


VPC에 연결
인터넷 게이트웨이를 VPC에 연결하여 인터넷과의 통신을 활성화합니다.
VPC
vpc-0191cd67 | u1-vpc
취소
예, 연결


인터넷 게이트웨이 생성
삭제
VPC에 연결
VPC에서 분리
인터넷 게이트웨이 및 해당 속
이름
ID
상태
VPC
u1-vpc-igw
igw-eb78508c
attached
vpc-0191cd67 | u1-vpc


AWS
VPC
Public 10.0.1.0/24
Private 10.0.2.0/24
RDS 10.0.5.0/24
가용영역 a
인터넷
Public 10.0.3.0/24
Public 10.0.4.0/24
Public 10.0.6.0/24
가용영역 b
VPC 10.0.0.0/16

오레곤 리전

NAT 게이트웨이 설정

NAT 게이트웨이 생성

NAT 게이트웨이를 생성하고 탄력적 IP 주소를 할당합니다. 자세히 알아보기

서브넷* ID, 이름 또는 VPC로 검색(예: "subnet-1a2b3c4d")

탄력적 IP 할당 ID* 할당 ID를 입력하거나 EIP를 선택합니다.

새 EIP 생성

* 필수 취소 NAT 게이트웨이 생성

NAT 게이트웨이 생성

NAT 게이트웨이를 생성하고 탄력적 IP 주소를 할당합니다. 자세히 알아보기

서브넷* subnet-c5f797a3

탄력적 IP 할당 ID*

속성별 필터

서브넷 ID	서브넷 이름	VPC
subnet-c5f797a3	u1-subnet-uw2a-public	vpc-0191cd67 | u1-vpc
subnet-cce76784	u1-subnet-uw2b-private	vpc-0191cd67 | u1-vpc
subnet-725a3b14	-	vpc-f20c5194
subnet-d2eb6b9a	u1-subnet-uw2b-public	vpc-0191cd67 | u1-vpc
subnet-60fb9b06	u1-subnet-uw2a-private	vpc-0191cd67 | u1-vpc
subnet-9c6c0ffa	u1-subnet-uw2a-rds	vpc-0191cd67 | u1-vpc
subnet-4503850d	-	vpc-f20c5194

* 필수

NAT 게이트웨이 생성

NAT 게이트웨이를 생성하고 탄력적 IP 주소를 할당합니다. 자세히 알아보기

서브넷* subnet-c5f797a3

탄력적 IP 할당 ID* eipalloc-c41e8ff9

새 EIP 생성

새 EIP(52.38.89.213)를 성공적으로 생성했습니다.

* 필수 취소 NAT 게이트웨이 생성

NAT 게이트웨이 생성

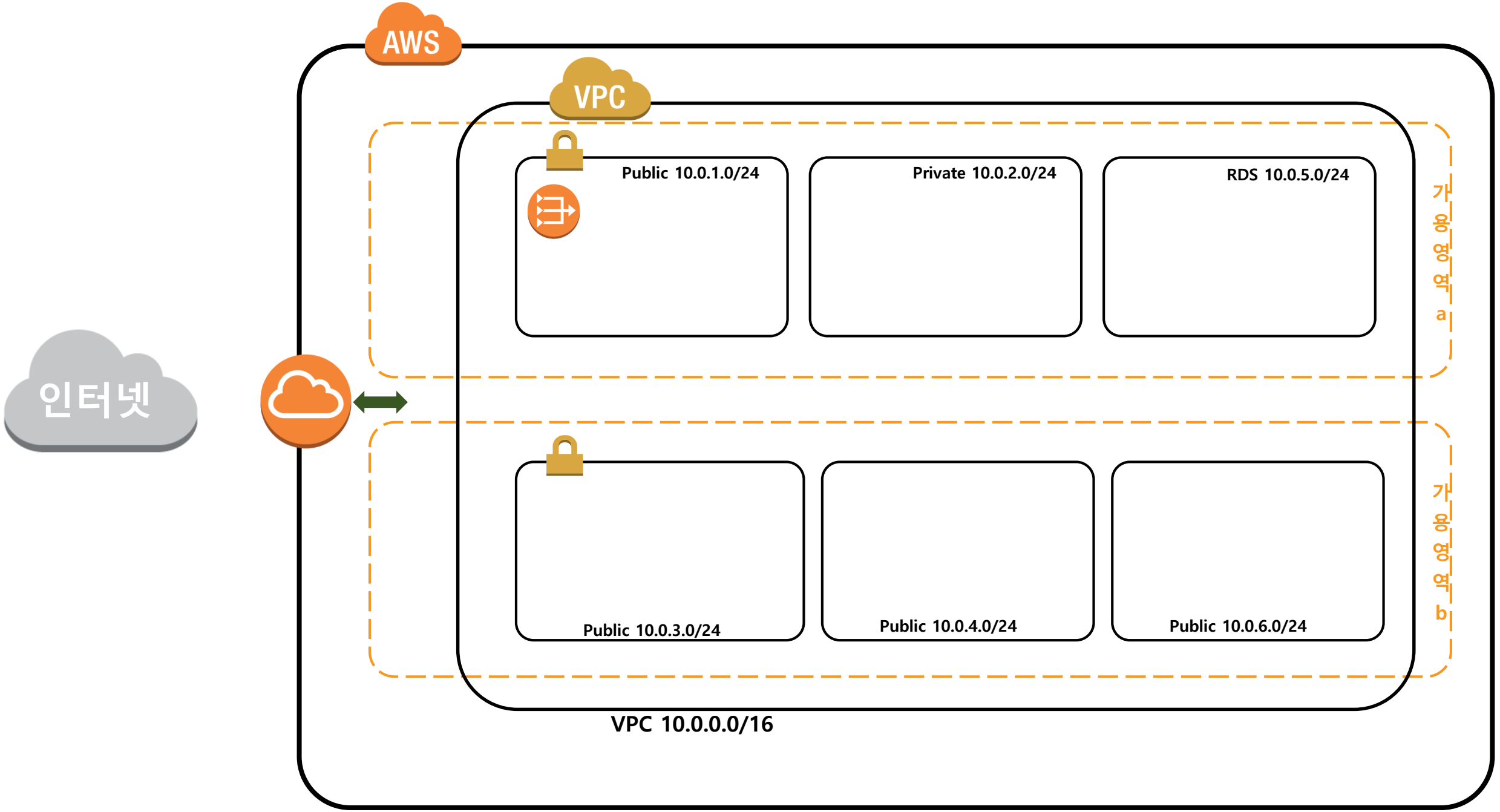
NAT 게이트웨이가 생성되었습니다.

참고: NAT 게이트웨이를 사용하려면, 다음 NAT 게이트웨이와 함께 라우팅을 포함하도록 라우팅 테이블을 편집 해야 합니다.

자세히 알아보기

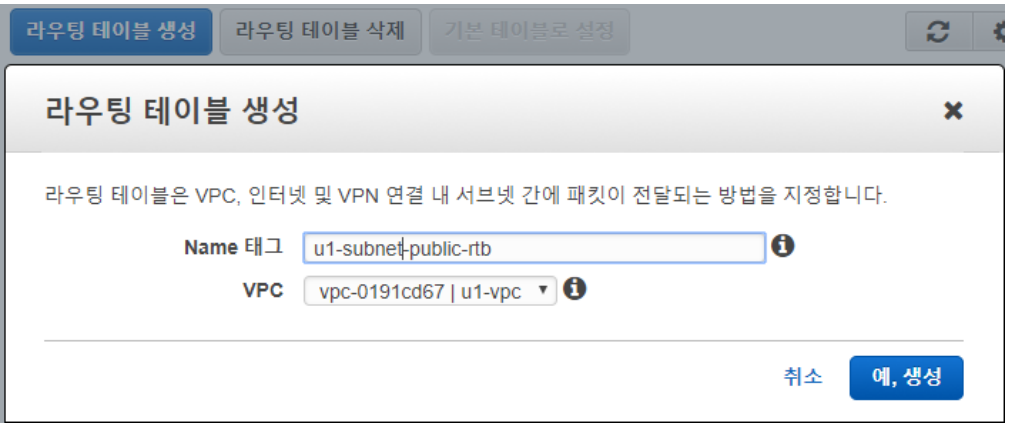
NAT 게이트웨이 ID nat-09ed0c44922189083

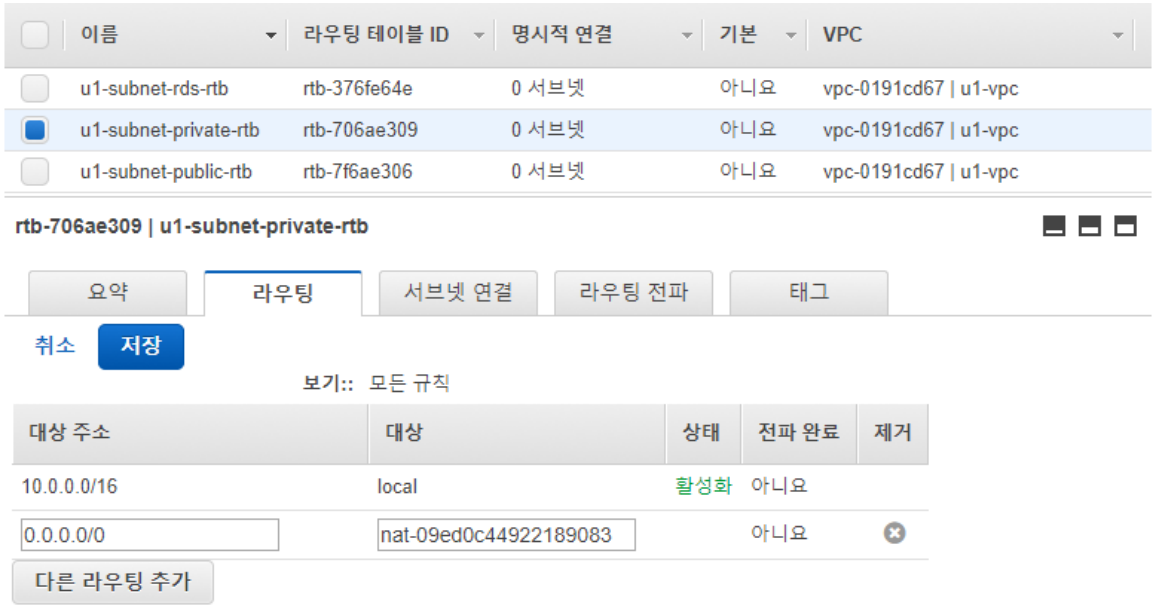
라우팅 테이블 편집 닫기


AWS
VPC
Public 10.0.1.0/24
Private 10.0.2.0/24
RDS 10.0.5.0/24
가용영역 a
인터넷
Public 10.0.3.0/24
Public 10.0.4.0/24
Public 10.0.6.0/24
가용영역 b
VPC 10.0.0.0/16

오레곤 리전

라우팅테이블 생성 및 설정





u1-subnet-public-rtb: 내부 외부 인바운드/아웃바운드 통신 가능
u1-subnet-private-rtb: 내부 외부 아웃바운드 통신 가능
U1-subnet-rds-rtb: 내부 통신만 가능

라우팅테이블 매핑(public)

라우팅 테이블 및 해당 속성 검

라우팅 테이블 1~5/5

이름	라우팅 테이블 ID	명시적 연결	기본	VPC
u1-subnet-rds-rtb	rtb-376fe64e	0 서브넷	아니요	vpc-0191cd67 | u1-vpc
u1-subnet-private-rtb	rtb-706ae309	0 서브넷	아니요	vpc-0191cd67 | u1-vpc
u1-subnet-public-rtb	rtb-7f6ae306	0 서브넷	아니요	vpc-0191cd67 | u1-vpc

rtb-7f6ae306 | u1-subnet-public-rtb

요약 | 라우팅 | 서브넷 연결 | 라우팅 전파 | 태그

취소 **저장**

연결	서브넷	IPv4 CIDR	IPv6 CIDR	현재 라우팅 테이블
☑	subnet-c5f797a3 | u1-subnet-uw2a-public	10.0.1.0/24	-	기본
☐	subnet-60fb9b06 | u1-subnet-uw2a-private	10.0.2.0/24	-	기본
☑	subnet-d2eb6b9a | u1-subnet-uw2b-public	10.0.3.0/24	-	기본
☐	subnet-cce76784 | u1-subnet-uw2b-private	10.0.4.0/24	-	기본
☐	subnet-9c6c0ffa | u1-subnet-uw2a-rds	10.0.5.0/24	-	기본
☐	subnet-fe63e3b6 | u1-subnet-uw2b-rds	10.0.6.0/24	-	기본

이름	라우팅 테이블 ID	명시적 연결	기본	VPC
u1-subnet-rds-rtb	rtb-376fe64e	0 서브넷	아니요	vpc-0191cd67 | u1-vpc
u1-subnet-public-rtb	rtb-7f6ae306	2 서브넷	아니요	vpc-0191cd67 | u1-vpc
u1-subnet-private-rtb	rtb-706ae309	0 서브넷	아니요	vpc-0191cd67 | u1-vpc

요약 | 라우팅 | 서브넷 연결 | 라우팅 전파 | 태그

편집

서브넷	IPv4 CIDR	IPv6 CIDR
subnet-c5f797a3 | u1-subnet-uw2a-public	10.0.1.0/24	-
subnet-d2eb6b9a | u1-subnet-uw2b-public	10.0.3.0/24	-

다음 서브넷은 어떤 라우팅 테이블과도 명시적으로 연결되어 있지 않고 기본 라우팅 테이블에 연결되어 있는 상태:

서브넷	IPv4 CIDR	IPv6 CIDR
subnet-60fb9b06 | u1-subnet-uw2a-private	10.0.2.0/24	-
subnet-cce76784 | u1-subnet-uw2b-private	10.0.4.0/24	-
subnet-9c6c0ffa | u1-subnet-uw2a-rds	10.0.5.0/24	-
subnet-fe63e3b6 | u1-subnet-uw2b-rds	10.0.6.0/24	-

라우팅테이블 매핑(private)

이름	라우팅 테이블 ID	명시적 연결	기본	VPC
u1-subnet-rds-rtb	rtb-376fe64e	0 서브넷	아니요	vpc-0191cd67 | u1-vpc
u1-subnet-public-rtb	rtb-7f6ae306	2 서브넷	아니요	vpc-0191cd67 | u1-vpc
u1-subnet-private-rtb	rtb-706ae309	0 서브넷	아니요	vpc-0191cd67 | u1-vpc

rtb-706ae309 | u1-subnet-private-rtb

요약 | 라우팅 | 서브넷 연결 | 라우팅 전파 | 태그

취소 **저장**

연결	서브넷	IPv4 CIDR	IPv6 CIDR	현재 라우팅 테이블
☐	subnet-c5f797a3 | u1-subnet-uw2a-public	10.0.1.0/24	-	rtb-7f6ae306 | u1-subnet-public-rtb
☑	subnet-60fb9b06 | u1-subnet-uw2a-private	10.0.2.0/24	-	기본
☐	subnet-d2eb6b9a | u1-subnet-uw2b-public	10.0.3.0/24	-	rtb-7f6ae306 | u1-subnet-public-rtb
☑	subnet-cce76784 | u1-subnet-uw2b-private	10.0.4.0/24	-	기본
☐	subnet-9c6c0ffa | u1-subnet-uw2a-rds	10.0.5.0/24	-	기본
☐	subnet-fe63e3b6 | u1-subnet-uw2b-rds	10.0.6.0/24	-	기본

이름	라우팅 테이블 ID	명시적 연결	기본	VPC
u1-subnet-private-rtb	rtb-706ae309	2 서브넷	아니요	vpc-0191cd67 | u1-vpc
	rtb-b123adc8	0 서브넷	예	vpc-0191cd67 | u1-vpc
	rtb-c8ff70b1	0 서브넷	예	vpc-f20c5194

rtb-706ae309 | u1-subnet-private-rtb

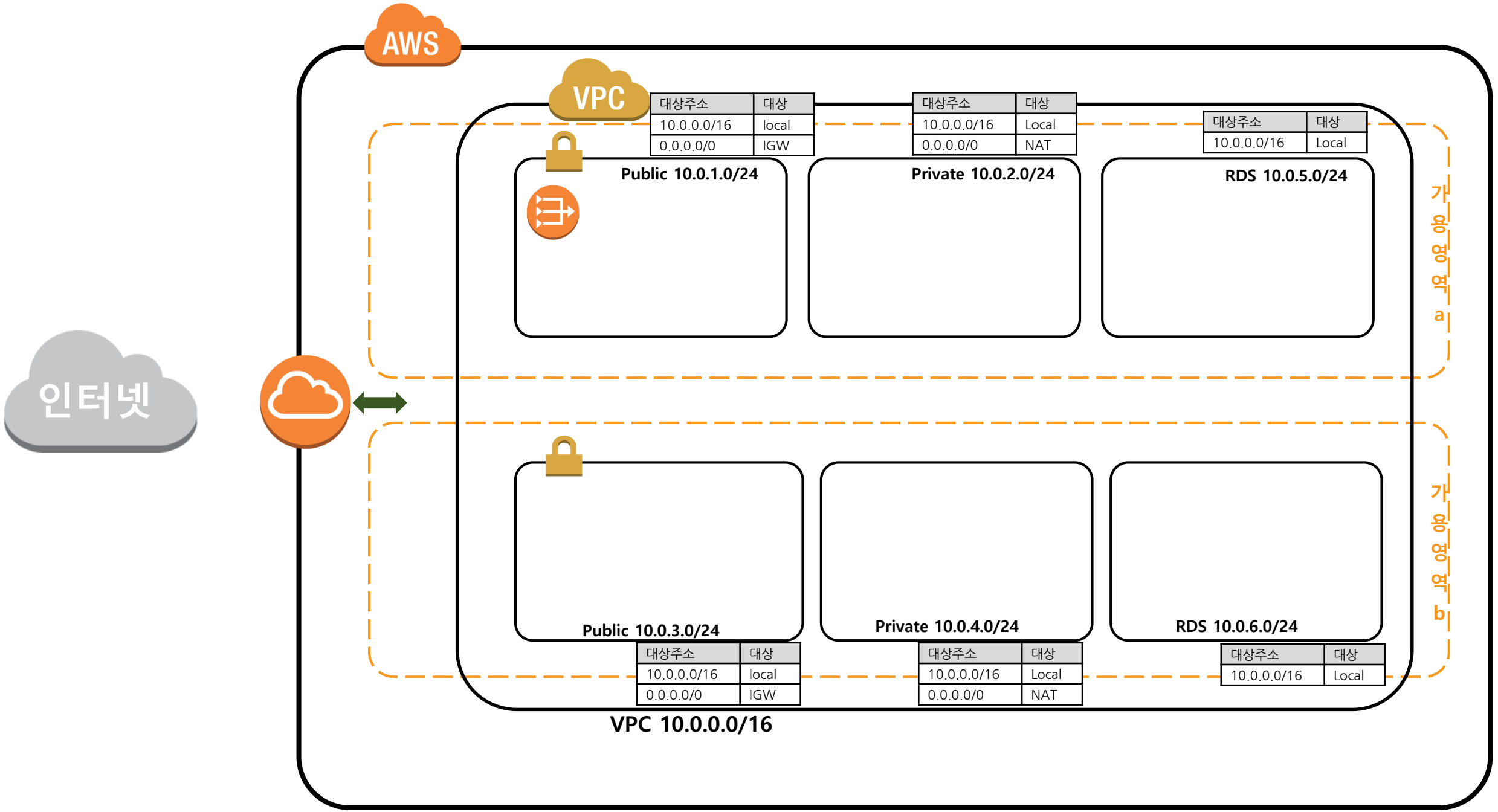
요약 | 라우팅 | 서브넷 연결 | 라우팅 전파 | 태그

편집

서브넷	IPv4 CIDR	IPv6 CIDR
subnet-60fb9b06 | u1-subnet-uw2a-private	10.0.2.0/24	-
subnet-cce76784 | u1-subnet-uw2b-private	10.0.4.0/24	-

다음 서브넷은 어떤 라우팅 테이블과도 명시적으로 연결되어 있지 않고 기본 라우팅 테이블에 연결되어 있는 상태:

서브넷	IPv4 CIDR	IPv6 CIDR
subnet-9c6c0ffa | u1-subnet-uw2a-rds	10.0.5.0/24	-
subnet-fe63e3b6 | u1-subnet-uw2b-rds	10.0.6.0/24	-

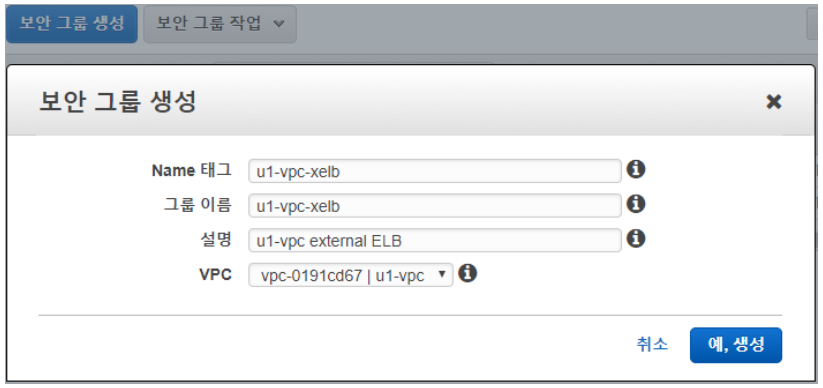

AWS
VPC
인터넷
대상주소 | 대상
10.0.0.0/16 | local
0.0.0.0/0 | IGW
대상주소 | 대상
10.0.0.0/16 | Local
0.0.0.0/0 | NAT
대상주소 | 대상
10.0.0.0/16 | Local
Public 10.0.1.0/24
Private 10.0.2.0/24
RDS 10.0.5.0/24
가용영역 a
Public 10.0.3.0/24
Private 10.0.4.0/24
RDS 10.0.6.0/24
가용영역 b
대상주소 | 대상
10.0.0.0/16 | local
0.0.0.0/0 | IGW
대상주소 | 대상
10.0.0.0/16 | Local
0.0.0.0/0 | NAT
대상주소 | 대상
10.0.0.0/16 | Local
VPC 10.0.0.0/16

오레곤 리전

네트워크 ACL 정책 설정

Default로 인바운드 규칙과 아웃바운드 규칙이 모든 트래픽을 허용하도록 되어 있음
규칙#의 숫자가 낮을 수록 우선 순위가 높음
주로 특정 구간의 IP(범위)에 대해서 거부를 하고자 할 경우 사용
여기에선 bypass

보안그룹 정책 설정



왼 쪽과 같이, 4개의 보안그룹을 설정합니다.

External Load Balancer : u1-vpc-xelb

Bastion Host : u1-vpc-bastion

Web Tier: u1-vpc-webtier

RDS Tier: u1-vpc-rdstier

보안 그룹 생성 | 보안 그룹 작업

필터 모든 보안 그룹 | 보안 그룹 및 해당 속성 검색... | 보안 그룹 1~7/7

Name 태그	그룹 ID	그룹 이름	VPC	설명
u1-vpc-xelb	sg-0a532677	u1-vpc-xelb	vpc-0191cd67 | u1-vpc	u1-vpc external ELB
u1-vpc-webtier	sg-6056231d	u1-vpc-webtier	vpc-0191cd67 | u1-vpc	u1-vpc Web Tier
u1-vpc-rdstier	sg-fd502580	u1-vpc-rdstier	vpc-0191cd67 | u1-vpc	u1-vpc RDS tier
u1-vpc-bastion	sg-fb532686	u1-vpc-bastion	vpc-0191cd67 | u1-vpc	u1-vpc bastion host

보안그룹 정책 설정(External ELB)

외부에서 들어오는 HTTP / HTTPS 요청을 허용

Name 태그	그룹 ID	그룹 이름	VPC	설명
u1-vpc-xelb	sg-0a532677	u1-vpc-xelb	vpc-0191cd67 | u1-vpc	u1-vpc external ELB
u1-vpc-webtier	sg-6056231d	u1-vpc-webtier	vpc-0191cd67 | u1-vpc	u1-vpc Web Tier
u1-vpc-rdstier	sg-fd502580	u1-vpc-rdstier	vpc-0191cd67 | u1-vpc	u1-vpc RDS tier
u1-vpc-bastion	sg-fb532686	u1-vpc-bastion	vpc-0191cd67 | u1-vpc	u1-vpc bastion host

sg-0a532677 | u1-vpc-xelb

요약 | 인바운드 규칙 | 아웃바운드 규칙 | 태그

취소 | 저장

유형	프로토콜	포트 범위	소스	설명	제거
HTTP (80)	TCP (6)	80	0.0.0.0/0		
HTTPS (443)	TCP (6)	443	0.0.0.0/0		

다른 규칙 추가

보안그룹 정책 설정(Bastion 호스트)

특정 IP범위(CIDR)을 지정하여 접근이 가능하도록 함.
주로 사무실이나 전산센터의 관리 PC
여기에서는 실습 목적상 0.0.0.0/0으로 하였으나, 실제 이렇게 하면 보안상 무의미함

Name 태그	그룹 ID	그룹 이름	VPC	설명
u1-vpc-xelb	sg-0a532677	u1-vpc-xelb	vpc-0191cd67	u1-vpc external ELB
u1-vpc-webtier	sg-6056231d	u1-vpc-webtier	vpc-0191cd67 | u1-vpc	u1-vpc Web Tier
u1-vpc-rdstier	sg-fd502580	u1-vpc-rdstier	vpc-0191cd67 | u1-vpc	u1-vpc RDS tier
u1-vpc-bastion	sg-fb532686	u1-vpc-bastion	vpc-0191cd67 | u1-vpc	u1-vpc bastion host

sg-fb532686 | u1-vpc-bastion

요약 | 인바운드 규칙 | 아웃바운드 규칙 | 태그

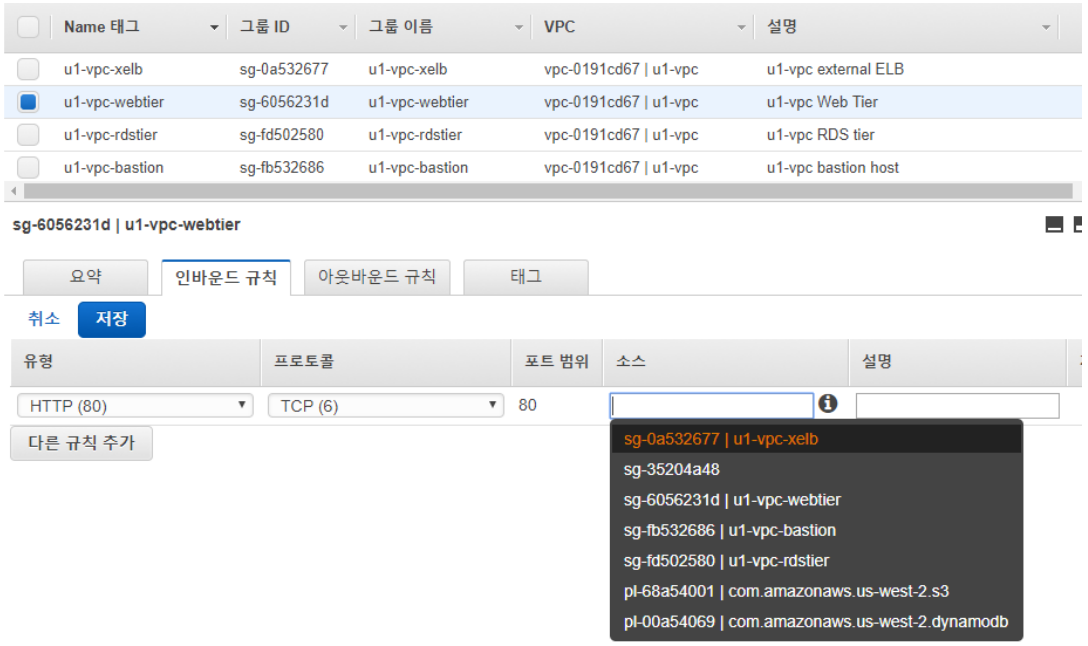
취소 **저장**

유형	프로토콜	포트 범위	소스	설명	제거
모든 트래픽	모두	모두	0.0.0.0/0		

다른 규칙 추가

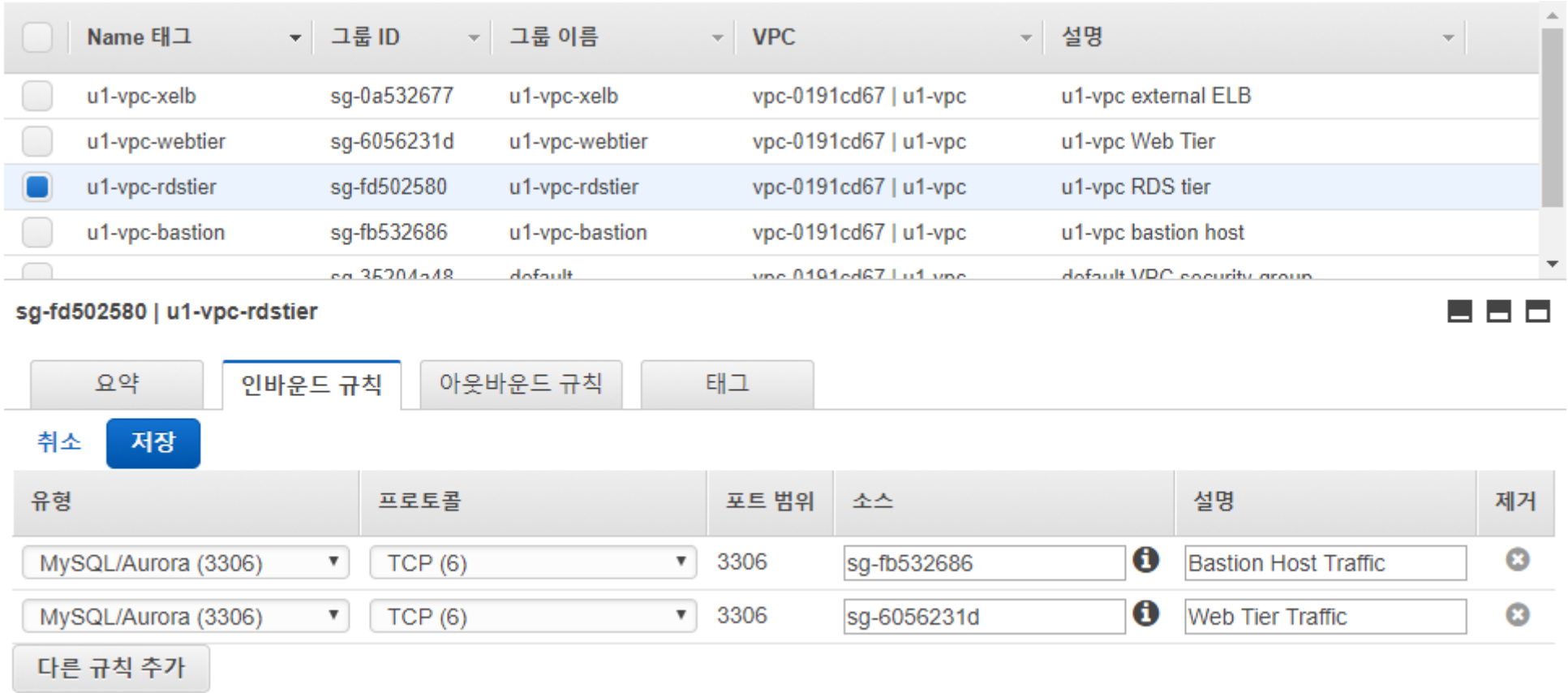
보안그룹 정책 설정(Web tier)

Web Tier의 경우 External ELB 그리고 Bastion 호스트의 리소스와 통신이 필요함.
ELB와는 HTTP/HTTPS를 오픈하고, Bastion 호스트와도 연결함.
보안그룹의 소스에는 IP범위와 보안그룹에 등록된 리소스(ENI)들과 통신도 허용함.
따라서 잦은 IP변경에 따른 관리 부담을 줄이기 위해 보안그룹 ID 바인딩을 통한 인바운드 룰 구성을 권장함.

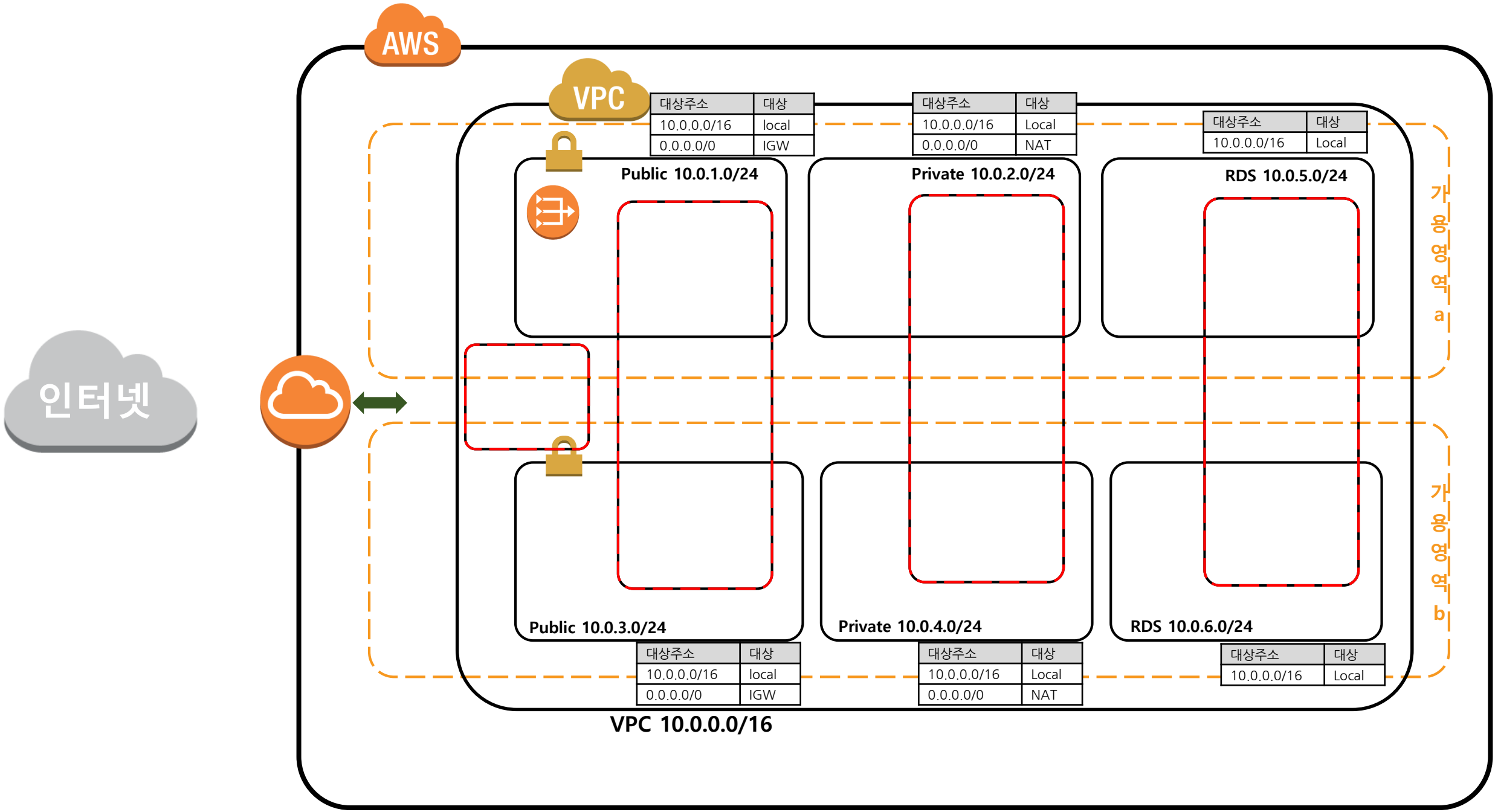


보안그룹 정책 설정(RDS Tier)

데이터베이스는 Bastion 호스트의 관리자와 Web Tier에서 접근이 가능해야 함.
실습에서 데이터베이스는 MySQL을 사용함.
보안 그룹은 기본적으로 상태 저장이므로, 아웃바운드를 설정하지 않더라도 쌍방향 트래픽이 이루어짐.



Name 태그	그룹 ID	그룹 이름	VPC	설명
u1-vpc-xelb	sg-0a532677	u1-vpc-xelb	vpc-0191cd67 | u1-vpc	u1-vpc external ELB
u1-vpc-webtier	sg-6056231d	u1-vpc-webtier	vpc-0191cd67 | u1-vpc	u1-vpc Web Tier
u1-vpc-rdstier	sg-fd502580	u1-vpc-rdstier	vpc-0191cd67 | u1-vpc	u1-vpc RDS tier
u1-vpc-bastion	sg-fb532686	u1-vpc-bastion	vpc-0191cd67 | u1-vpc	u1-vpc bastion host


AWS
VPC
인터넷
대상주소 | 대상
10.0.0.0/16 | local
0.0.0.0/0 | IGW
대상주소 | 대상
10.0.0.0/16 | Local
0.0.0.0/0 | NAT
대상주소 | 대상
10.0.0.0/16 | Local
Public 10.0.1.0/24
Private 10.0.2.0/24
RDS 10.0.5.0/24
가용영역 a
Public 10.0.3.0/24
Private 10.0.4.0/24
RDS 10.0.6.0/24
가용영역 b
대상주소 | 대상
10.0.0.0/16 | local
0.0.0.0/0 | IGW
대상주소 | 대상
10.0.0.0/16 | Local
0.0.0.0/0 | NAT
대상주소 | 대상
10.0.0.0/16 | Local
VPC 10.0.0.0/16

오레곤 리전

VPC 실습의 비용 계산

VPC의 객체 대부분은 별도의 요금이 발생하지 않지만, NAT Gateway 나 VPN 구성은 비용이 발생함.
NAT Gateway의 경우 사용 시간과 NAT Gateway를 통해 처리한 데이터 양에 따라 과금됨.

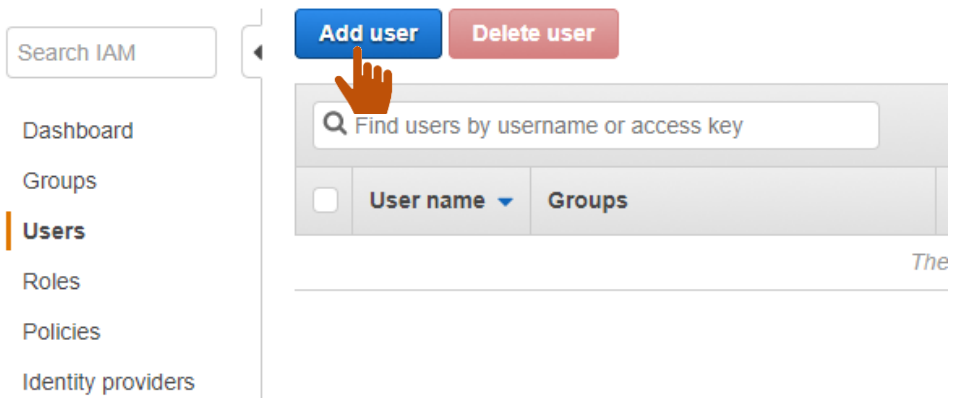
리전	NAT 게이트웨이당 요금(USD/시간)	처리된 데이터 GB당 요금(USD)
미국 동부(버지니아 북부)	0.045	0.045
미국 동부(오하이오)	0.045	0.045
미국 서부(오레곤)	0.045	0.045

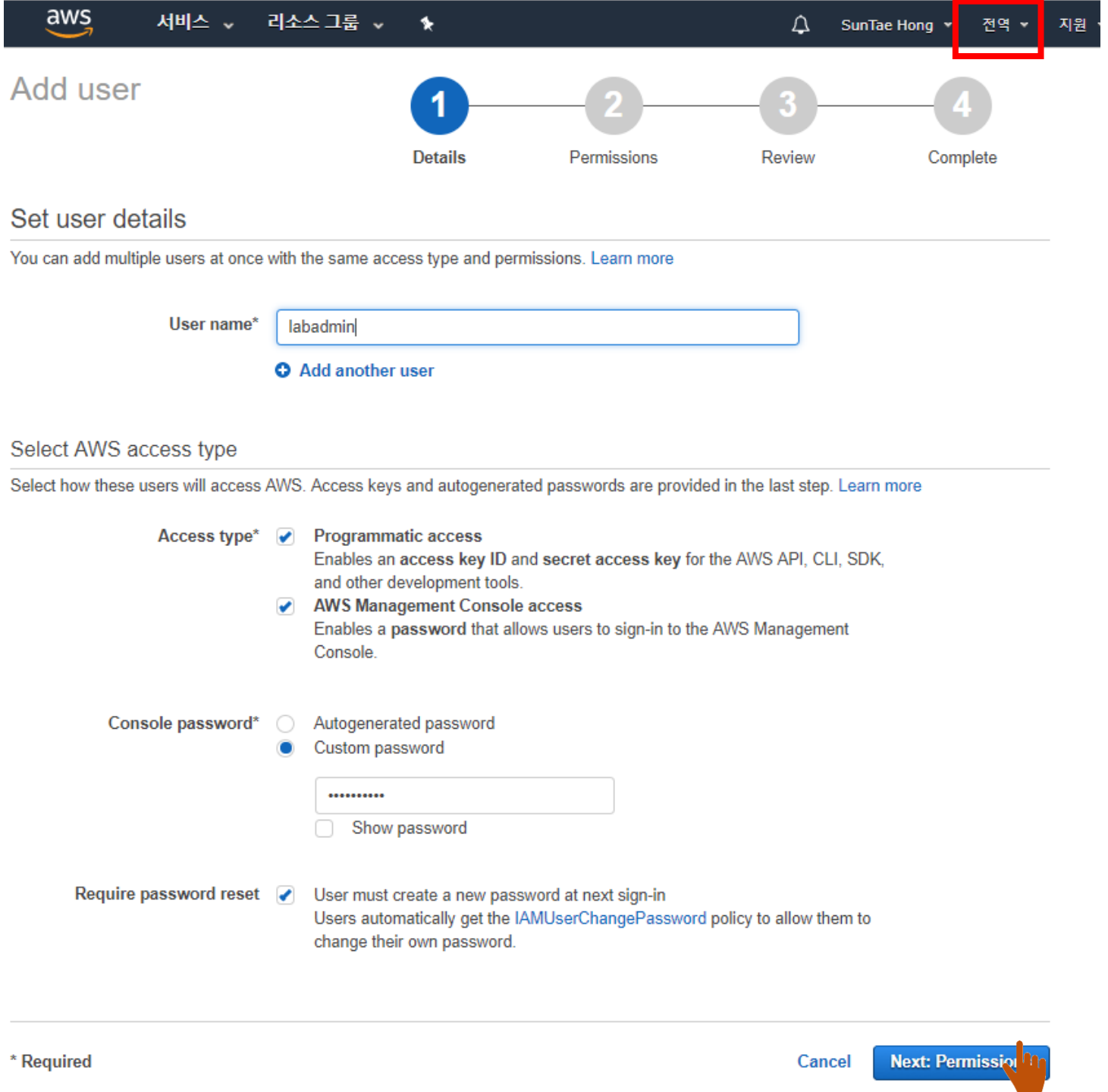
AWS Identity and Access Management (IAM)

이번 장은 Starter 계정으로 실습이 불가능합니다.

Starter 계정으로 실습하고자 할 경우, Qwiklabs의 Introduction to AWS Identity and Access Management (IAM)를 실습하기 바랍니다.

IAM user


Search IAM
Add user
Delete user
Dashboard
Groups
Users
Roles
Policies
Identity providers
Find users by username or access key
User name
Groups


aws
서비스
리소스 그룹
SunTae Hong
전역
지원
Add user
1 Details
2 Permissions
3 Review
4 Complete
Set user details
You can add multiple users at once with the same access type and permissions. Learn more
User name*
labadmin
Add another user
Select AWS access type
Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more
Access type*
Programmatic access
Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.
AWS Management Console access
Enables a password that allows users to sign-in to the AWS Management Console.
Console password*
Autogenerated password
Custom password
Show password
Require password reset
User must create a new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.
* Required
Cancel
Next: Permissio

IAM user

Set permissions for labadmin

Add user to group

Copy permissions from existing user

Attach existing policies directly

Attach one or more existing policies directly to the users or create a new policy. Learn more

Create policy | Refresh

Filter: Policy type | administratoraccess | Showing 1 result

	Policy name	Type	Attachments	Description
☑	AdministratorAccess	Job function	0	Provides full access to AWS services and re…

Cancel | Previous | Next: Review

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	labadmin
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	Yes

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	AdministratorAccess
Managed policy	IAMUserChangePassword

Cancel | Previous | Create user

Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://629491326515.signin.aws.amazon.com/console

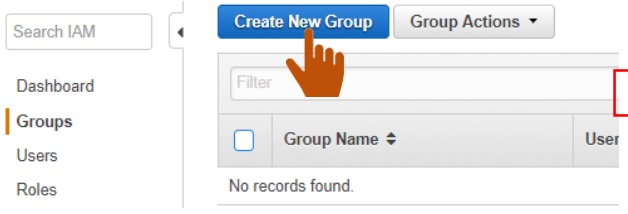
Download .csv

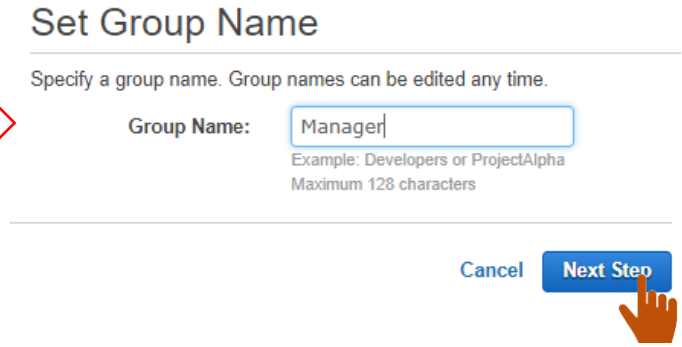
User	Access key ID	Secret access key	Email login instructions
labadmin	AK IGWSFZA	********** Show	Send email

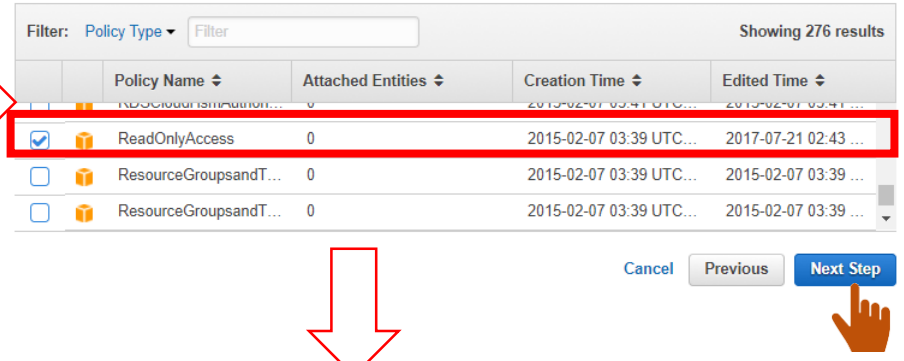
Close

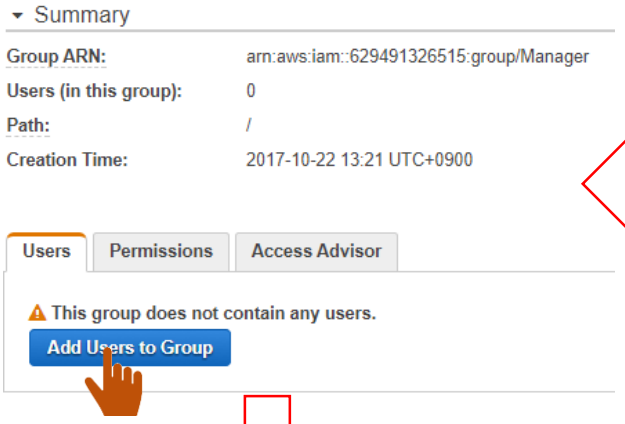
키를 잘 보관 할 것
메일로 보내서 정보 보관

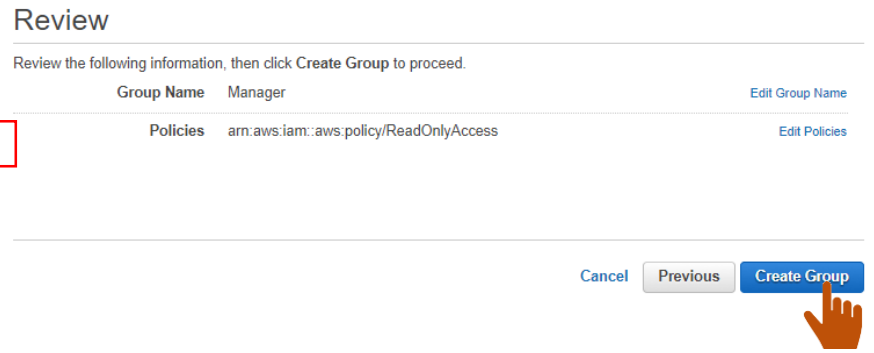
IAM Group

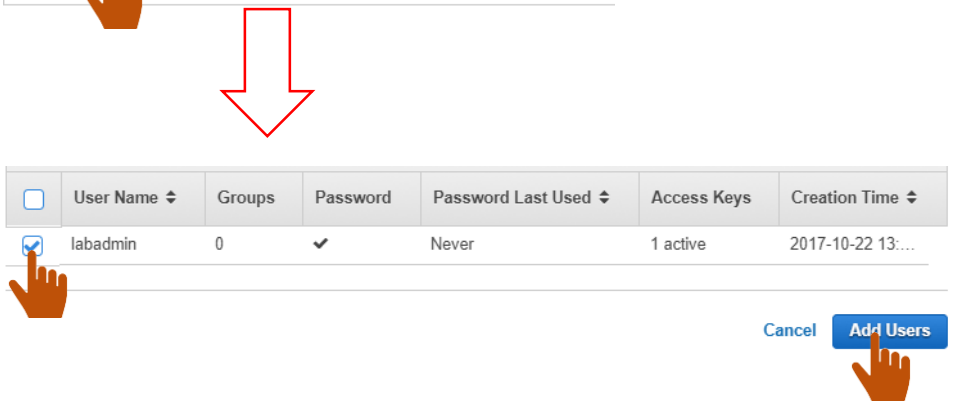


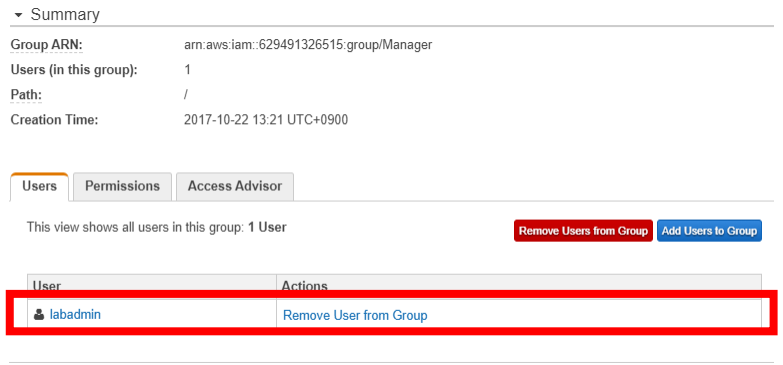












Group을 생성하고, 권한을 추가하고, Group에 User를 추가하는 과정임.

앞에서 labladmin에게 관리자 권한을 부여했기 때문에 그룹에 부여한 read-only권한은 사실상 무의미함.
단지 실습용 연습임.

IAM User

Summary

User ARN arn:aws:iam::629491326515:user/labadmin
Path /
Creation time 2017-10-22 13:00 UTC+0900

Permissions | Groups (1) | Security credentials | Access Advisor

Add permissions Attached policies: 3

Policy name	Policy type
Attached directly	
AdministratorAccess	AWS managed poli
IAMUserChangePassword	AWS managed poli
Attached from group	
ReadOnlyAccess	AWS managed poli

Summary

User ARN arn:aws:iam::629491326515:user/labadmin
Path /
Creation time 2017-10-22 13:00 UTC+0900

Permissions | Groups (1) | Security credentials | Access Advisor

Add user to groups

Group name	Attached permissions
Manager	ReadOnlyAccess

Summary

User ARN arn:aws:iam::629491326515:user/labadmin
Path /
Creation time 2017-10-22 13:00 UTC+0900

Permissions | Groups (1) | Security credentials | Access Advisor

Sign-in credentials

Console password Enabled Manage password
Console login link https://629491326515.signin.aws.amazon.com/console
Last login Never
Assigned MFA device No
Signing certificates None

Access keys

Use access keys to make secure REST or HTTP Query protocol requests to AWS service APIs. For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation. Learn more

Create access key

Access key ID	Created	Last used	Status
AKI 3FZA	2017-10-22 13:01 UTC+0900	N/A	Active | Make inactive

SSH keys for AWS CodeCommit

Use SSH public keys to authenticate access to AWS CodeCommit repositories. Learn more

Upload SSH public key

SSH key ID	Uploaded	Status
No results		

Summary

User ARN arn:aws:iam::629491326515:user/labadmin
Path /
Creation time 2017-10-22 13:00 UTC+0900

Permissions | Groups (1) | Security credentials | Access Advisor

Access advisor shows the service permissions granted to this user and when those services were last accessed. You can use this information to revise your policies. Learn more

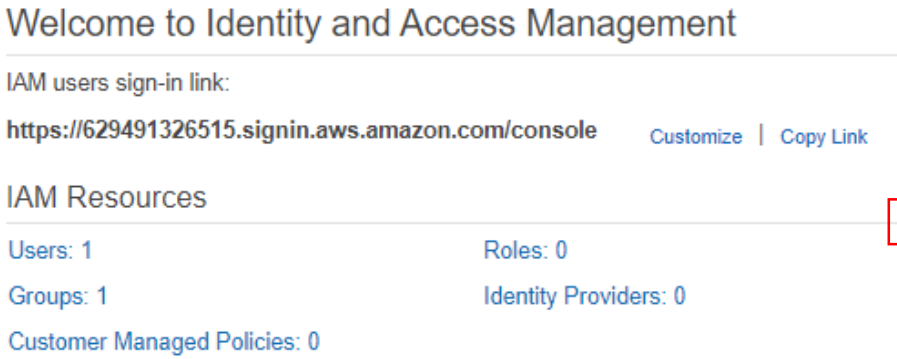
Note: recent activity usually appears within 4 hours. Access Advisor tracking began on Oct 1, 2015 Learn more

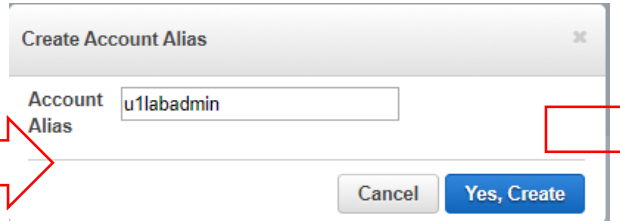
Filter: No filter Search Showing 73 results

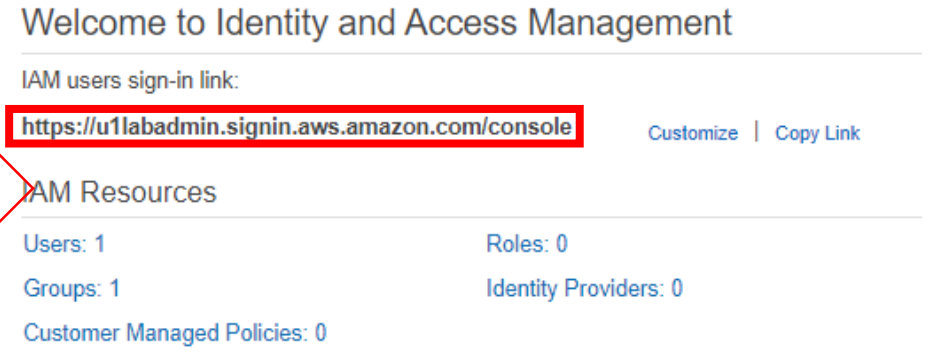
Service Name	Policies Granting Permissions	Last Accessed
Amazon RDS	ReadOnlyAccess and 1 more	Not accessed in the tracking period
AWS IoT	ReadOnlyAccess and 1 more	Not accessed in the tracking period
Amazon API Gateway	AdministratorAccess	Not accessed in the tracking period
Amazon SNS	ReadOnlyAccess and 1 more	Not accessed in the tracking period
AWS Database Migration Service	ReadOnlyAccess and 1 more	Not accessed in the tracking period
Amazon Storage Gateway	ReadOnlyAccess and 1 more	Not accessed in the tracking period

Access Advisor는 사용하고 있는
권한과 접속 통계를 제공하여,
효율적인 계정 권한 관리에 사용

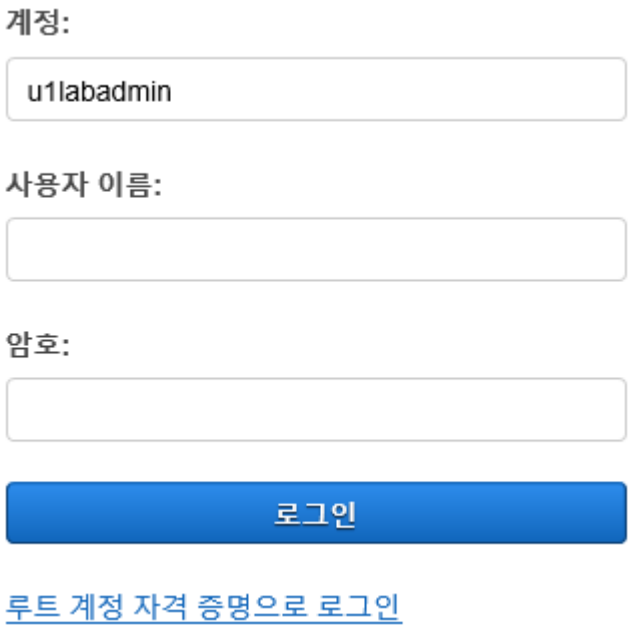
IAM custom URL 설정(custom sign-in link)

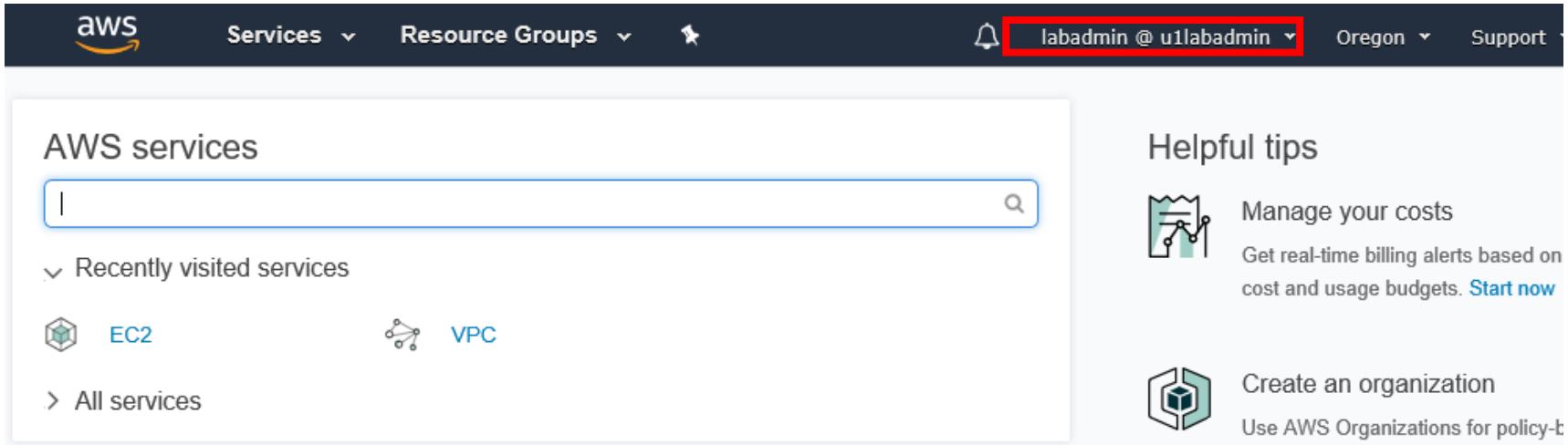




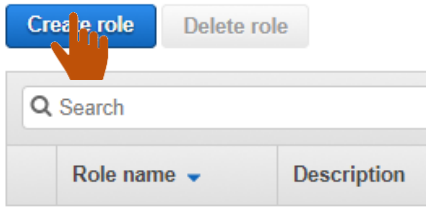


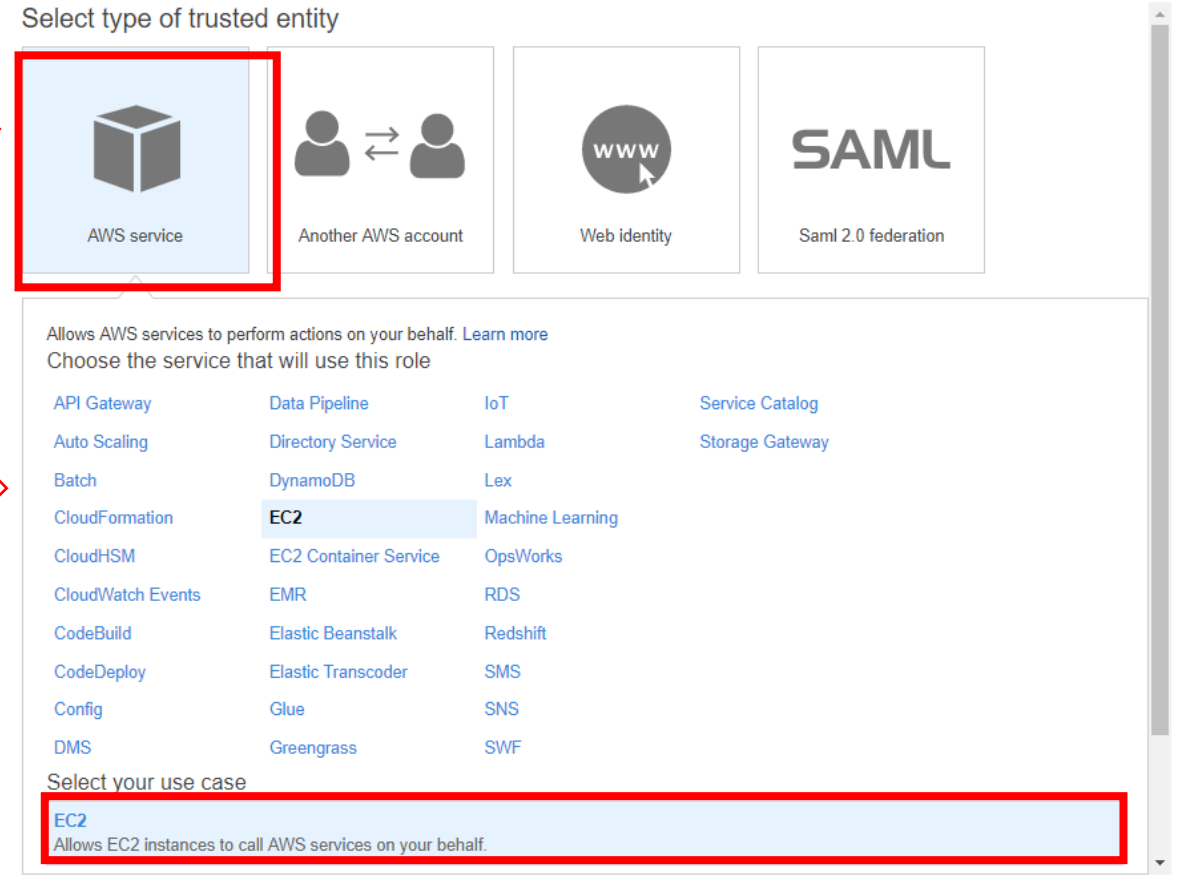
URL을 복사하여 새창에서 접속



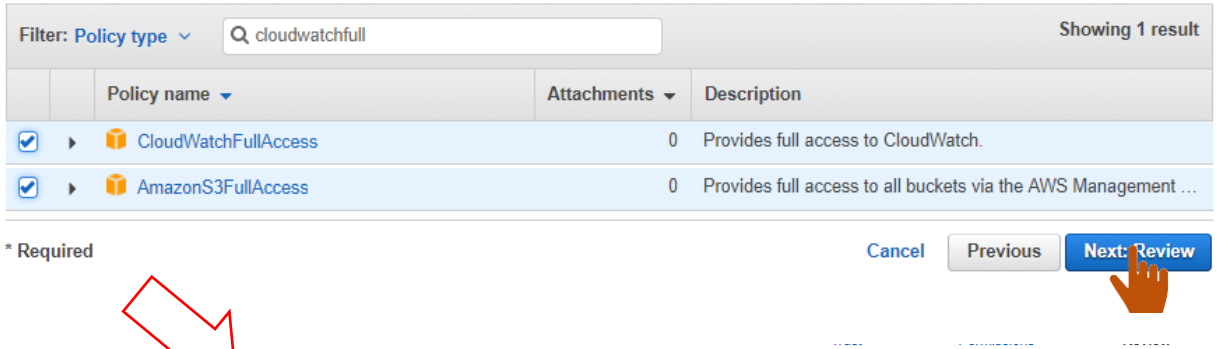


IAM Role

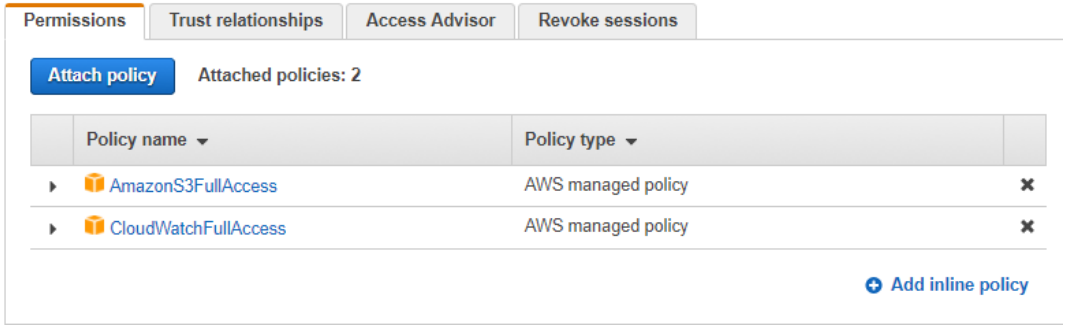




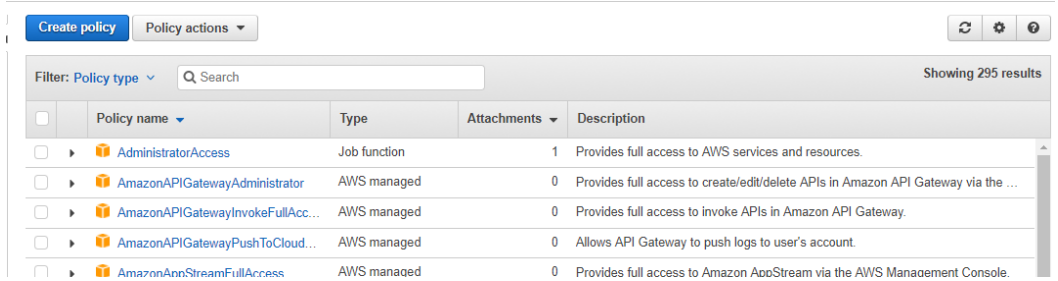
S3FullAccess 와 CloudWatchFullAccess 선택

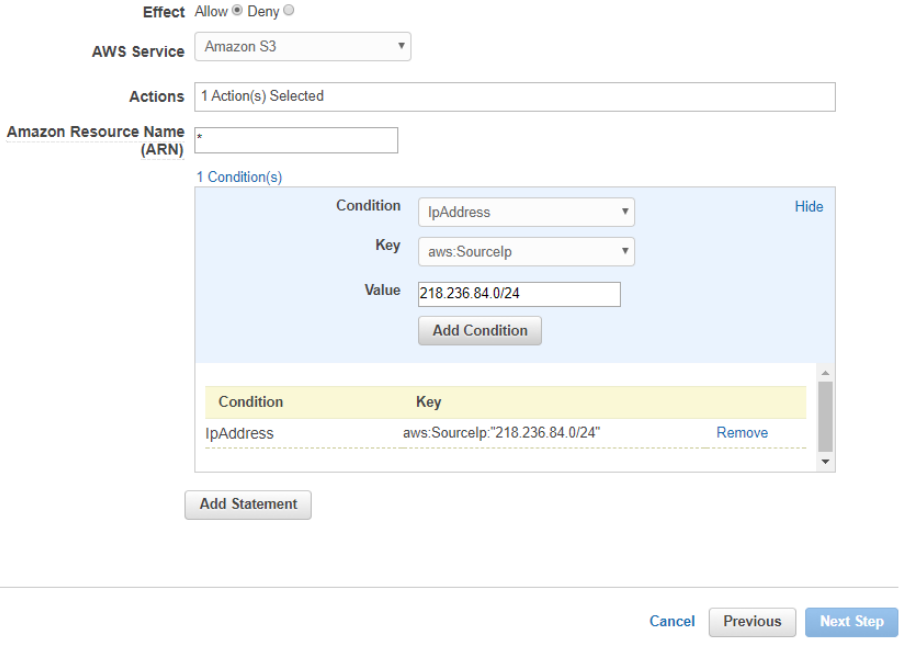


생성된 IAM-Role을 클릭하면

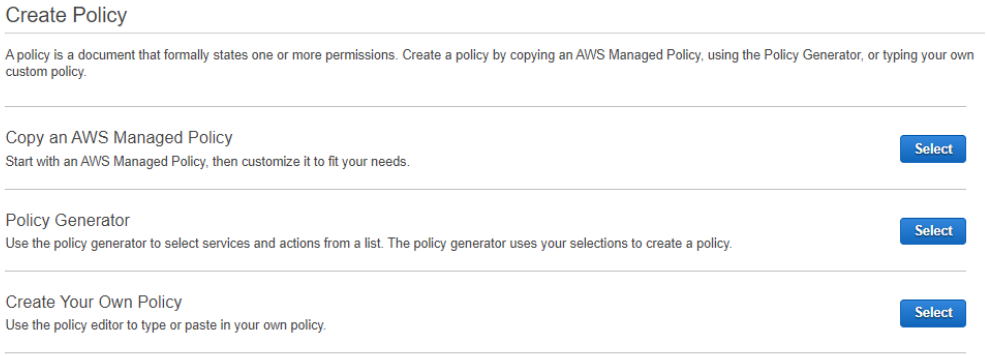


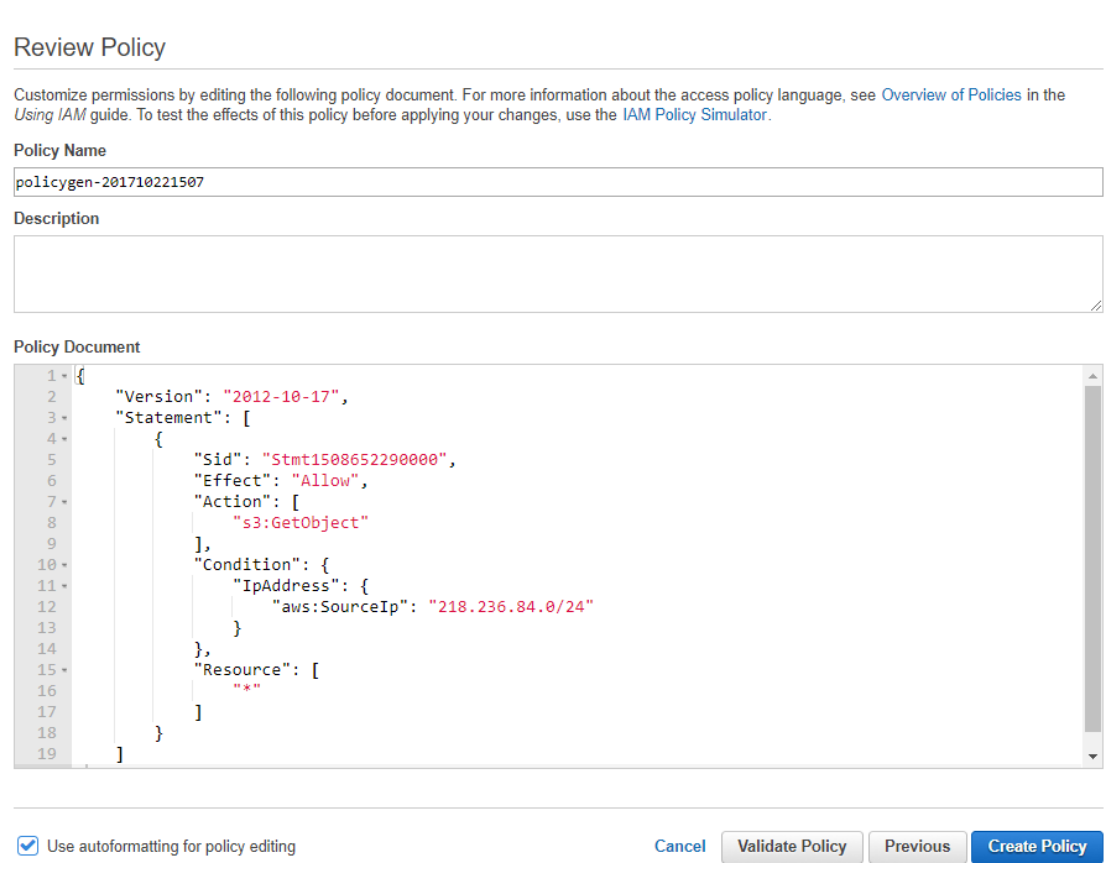
IAM Policy


Create policy
Policy actions
Filter: Policy type
Search
Showing 295 results
Policy name
Type
Attachments
Description
AdministratorAccess
Job function
1
Provides full access to AWS services and resources.
AmazonAPIGatewayAdministrator
AWS managed
0
Provides full access to create/edit/delete APIs in Amazon API Gateway via the ...
AmazonAPIGatewayInvokeFullAcc...
AWS managed
0
Provides full access to invoke APIs in Amazon API Gateway.
AmazonAPIGatewayPushToCloud...
AWS managed
0
Allows API Gateway to push logs to user's account.
AmazonAppStreamFullAccess
AWS managed
0
Provides full access to Amazon AppStream via the AWS Management Console.


Effect
Allow
Deny
AWS Service
Amazon S3
Actions
1 Action(s) Selected
Amazon Resource Name (ARN)
*
1 Condition(s)
Condition
IpAddress
Hide
Key
aws:SourceIp
Value
218.236.84.0/24
Add Condition
Condition
Key
IpAddress
aws:SourceIp:"218.236.84.0/24"
Remove
Add Statement
Cancel
Previous
Next Step


Effect
Action
Resource
Allow
s3:GetObject
*
Remove
Show Conditions

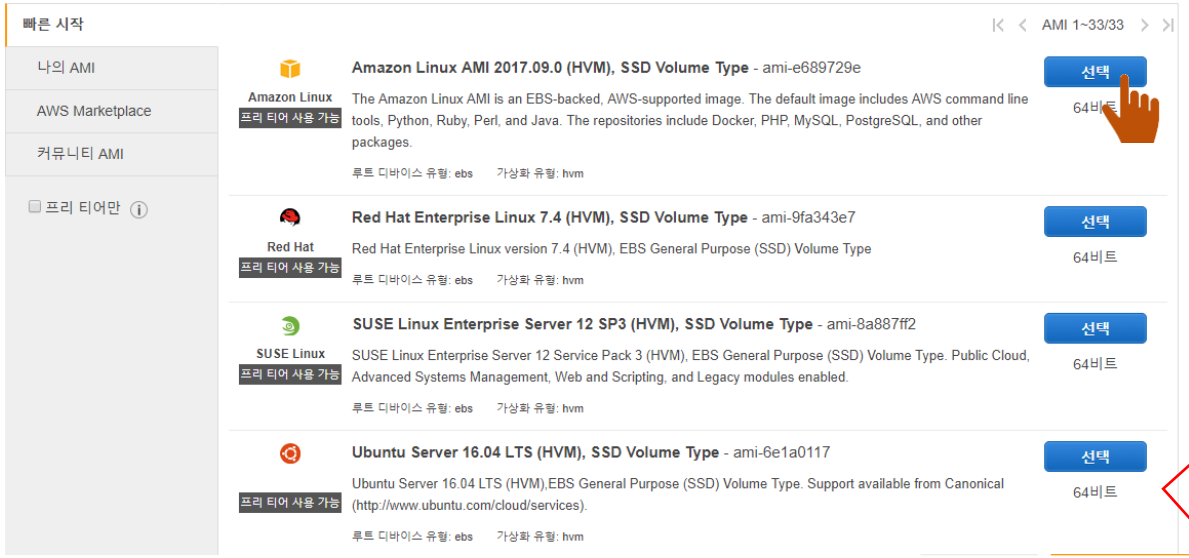

Create Policy
A policy is a document that formally states one or more permissions. Create a policy by copying an AWS Managed Policy, using the Policy Generator, or typing your own custom policy.
Copy an AWS Managed Policy
Start with an AWS Managed Policy, then customize it to fit your needs.
Select
Policy Generator
Use the policy generator to select services and actions from a list. The policy generator uses your selections to create a policy.
Select
Create Your Own Policy
Use the policy editor to type or paste in your own policy.
Select


Review Policy
Customize permissions by editing the following policy document. For more information about the access policy language, see Overview of Policies in the Using IAM guide. To test the effects of this policy before applying your changes, use the IAM Policy Simulator.
Policy Name
policygen-201710221507
Description
Policy Document
{
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Stmt1508652290000",
"Effect": "Allow",
"Action": [
"s3:GetObject"
],
"Condition": {
"IpAddress": {
"aws:SourceIp": "218.236.84.0/24"
}
},
"Resource": [
"*"
]
}
]
Use autoformatting for policy editing
Cancel
Validate Policy
Previous
Create Policy

Amazon EC2

- 이번 장에서 일부 설정(IAM)은 Starter 계정으로는 작동하지 않습니다.
- 버지니아 북부, 오하이오, 오레곤 리전에서는 Starter 계정으로도 IAM 설정없이 인스턴스 생성이 가능하므로, 리전 설정에 유의하여 실습하시기 바랍니다.

EC2



단계 2: 인스턴스 유형 선택

Amazon EC2는 각 사용 사례에 맞게 최적화된 다양한 인스턴스 유형을 제공합니다. 인스턴스는 애플리케이션을 실행할 수 있는 가상 서버입니다. 이러한 인스턴스에는 CPU, 메모리, 스토리지 및 네트워킹 용량이 다양하게 조합되어 있으며, 애플리케이션에 사용할 적절한 리소스 조합을 유연하게 선택할 수 있습니다. 인스턴스 유형과 이러한 인스턴스 유형이 컴퓨팅 요건을 충족하는 방식에 대해 자세히 알아보기

필터링 기준: 모든 인스턴스 유형 현재 세대 열 표시/숨기기

현재 선택된 항목: t2.micro (Variable ECU, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB 메모리, EBS 전용)

	패밀리	유형	vCPUs	메모리 (GiB)	인스턴스 스토리지 (GB)	EBS 최적화 사용 가능	네트워크 성능	IPv6 지원
☐	General purpose	t2.nano	1	0.5	EBS 전용	-	낮음에서 중간	예
☑	General purpose	t2.micro 프리 티어 사용 가능	1	1	EBS 전용	-	낮음에서 중간	예
☐	General purpose	t2.small	1	2	EBS 전용	-	낮음에서 중간	예
☐	General purpose	t2.medium	2	4	EBS 전용	-	낮음에서 중간	예
☐	General purpose	t2.large	2	8	EBS 전용	-	낮음에서 중간	예

취소 이전 검토 및 시작 다음: 인스턴스 세부 정보 구성

EC2

단계 3: 인스턴스 세부 정보 구성

요구 사항에 적합하게 인스턴스를 구성합니다. 동일한 AMI의 여러 인스턴스를 시작하고 스팟 인스턴스를 요청하여 보다 저렴한 요금을 활용하며 인스턴스에 액세스 관리 역할을 할당하는 등 다양한 기능을 사용할 수 있습니다.

인스턴스 개수 (i) 1 Auto Scaling 그룹 시작 (i)

구매 옵션 (i) ☐ 스팟 인스턴스 요청

네트워크 (i) vpc-0191cd67 | u1-vpc ▼ 새 VPC 생성

서브넷 (i) subnet-c5f797a3 | u1-subnet-uw2a-public | us-west- ▼ 새 서브넷 생성
250개 IP 주소 사용 가능

퍼블릭 IP 자동 할당 (i) 서브넷 사용 설정(비활성화) ▼

IAM 역할 (i) U1-EC2 ▼ 새 IAM 역할 생성

종료 방식 (i) 중지 ▼

종료 방지 기능 활성화 (i) ☐ 의도하지 않은 종료로부터 보호

모니터링 (i) ☐ CloudWatch 세부 모니터링 활성화
추가 요금이 적용됩니다.

테넌시 (i) 공유됨 - 공유된 하드웨어 인스턴스 실행 ▼
전용 테넌시에는 추가 요금이 적용됩니다.

VPC 실습에서 만든 VPC와 서브넷: 가용영역a의 퍼블릭 서브넷에 생성

퍼블릭 IP 자동 할당: 서브넷 사용 설정(비활성화)를 (활성화)로 바꾸려면 서브넷 구성 시 “자동 할당 IP 설정 수정 " 을 활성화 해야 함.

IAM 실습에서 만든 IAM 역할 추가, Starter 계정의 경우 생략

▼ 네트워크 인터페이스 (i)

디	네트워크 인터페이스	서브넷	기본 IP	보조 IP 주소	IPv6 IP
eth0	새 네트워크 인터페이 ▼	subnet-c5f797a3 ▼	자동 할당	IP 추가	

디바이스 추가

▼ 고급 세부 정보

사용자 데이터 (i) ◉ 텍스트 ○ 파일 ☐ 입력이 이미 base64로 인코딩됨

```
#!/bin/bash
yum -y update
yum -y install httpd24 php56 mysql55-server php56-mysqlnd
service httpd start
chkconfig httpd on
```

시작 시 설치 프로그램 설정 스크립트, Apache, php, mysql

취소 이전 검토 및 시작 다음: 스토리지 추가

EC2

단계 4: 스토리지 추가

인스턴스가 다음 스토리지 디바이스 설정으로 시작됩니다. 추가 EBS 볼륨 및 인스턴스 스토어 볼륨을 인스턴스에 연결하거나 루트 볼륨의 설정을 편집할 수 있습니다. 인스턴스를 시작한 후 추가 EBS 볼륨을 연결할 수도 있지만, 인스턴스 스토어 볼륨은 연결할 수 없습니다. Amazon EC2의 스토리지 옵션에 대해 자세히 알아보십시오.

볼륨 유형	디바이스	스냅샷	크기(GiB)	볼륨 유형	IOPS	처리량(MB/초)	종료 시 삭제	암호화
루트	/dev/xvda	snap-0cfc1bfe4dc1b09e1	8	범용 SSD(GP2)	100/3000	해당 사항 없음	☑	암호화되지 않음

새 볼륨 추가

프리 티어 사용 가능 고객은 최대 30GB의 EBS 범용(SSD) 또는 마그네틱 스토리지를 사용할 수 있습니다. 프리 티어 자격 및 사용량 제한에 대해 자세히 알아보기

취소 | 이전 | 검토 및 시작 | 다음: 태그 추가

단계 5: 태그 추가

태그는 대소문자를 구별하는 키-값 페어로 이루어져 있습니다. 예를 들어 키가 Name이고 값이 Webserver인 태그를 정의할 수 있습니다.
태그 복사본은 볼륨, 인스턴스 또는 둘 다에 적용될 수 있습니다.
태그는 모든 인스턴스 및 볼륨에 적용됩니다. Amazon EC2 리소스 태그 지정에 대해 자세히 알아보기

키 (최대 127자)	값 (최대 255자)	인스턴스	볼륨	
Name	u1-subnet-uw2a-public-ec2	☑	☑	⊗
Team	Cloud Computing Lab	☑	☑	⊗
Owner	SunTae Hong	☑	☑	⊗
Purpose	Bastion SSH Tunneling	☑	☑	⊗

다른 태그 추가 (최대 50개 태그)

비용 관리용 태그 추가

취소 | 이전 | 검토 및 시작 | 다음: 보안 그룹 구성

EC2

단계 6: 보안 그룹 구성

보안 그룹은 인스턴스에 대한 트래픽을 제어하는 방화벽 규칙 세트입니다. 이 페이지에서는 특정 트래픽을 인스턴스에 도달하도록 허용할 규칙을 추가할 수 있습니다. 예를 들면 웹 서버를 설정하여 인터넷 트래픽을 인스턴스에 도달하도록 허용하려는 경우 HTTP 및 HTTPS 트래픽에 대한 무제한 액세스를 허용하는 규칙을 추가합니다. 새 보안 그룹을 생성하거나 아래에 나와 있는 기존 보안 그룹 중에서 선택할 수 있습니다. Amazon EC2 보안 그룹에 대해 자세히 알아보기

보안 그룹 할당: ○새 보안 그룹 생성
◉기존 보안 그룹 선택

	보안 그룹 ID	이름	설명	작업
☐	sg-35204a48	default	default VPC security group	새로 복사
☑	sg-fb532686	u1-vpc-bastion	u1-vpc bastion host	새로 복사
☐	sg-fd502580	u1-vpc-rdstier	u1-vpc RDS tier	새로 복사
☐	sg-6056231d	u1-vpc-webtier	u1-vpc Web Tier	새로 복사
☐	sg-0a532677	u1-vpc-xelb	u1-vpc external ELB	새로 복사

sg-fb532686에 대한 인바운드 규칙 (선택한 보안 그룹: sg-fb532686)

유형	프로토콜	포트 범위	소스	설명
모든 트래픽	모두	모두	0.0.0.0/0	

취소 이전 검토 및 시작

VPC 보안그룹 실습에서 만든 Bastion 호스트 보안그룹 선택
여기에서는, u1-vpc-bastion

단계 7: 인스턴스 시작 검토

인스턴스 시작 세부 정보를 검토하십시오. 이전으로 돌아가서 각 섹션에 대한 변경 내용을 편집할 수 있습니다. 키 페어를 인스턴스에 할당하고 시작 프로세스를 완료하려면 [시작]을 클릭합니다.

⚠ 인스턴스 보안을 개선하십시오. 보안 그룹 u1-vpc-bastion이(가) 세계에 개방되어 있습니다.
인스턴스를 모든 IP 주소에서 액세스할 수 있습니다. 보안 그룹 규칙을 업데이트하여 알려진 IP 주소에서만 액세스를 허용하는 것이 좋습니다.
실행 중인 애플리케이션이나 서비스에 쉽게 액세스할 수 있도록 보안 그룹에서 추가 포트를 열 수도 있습니다. 예를 들어 웹 서버용 HTTP(80)를 엽니다. 보안 그룹 편집

▾ AMI 세부 정보 AMI 편집

Amazon Linux AMI 2017.09.0 (HVM), SSD Volume Type - ami-e689729e

프리 티어 사용 가능

The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.

루트 디바이스 유형: ebs 가상화 유형: hvm

▾ 인스턴스 유형 인스턴스 유형 편집

인스턴스 유형	ECU	vCPUs	메모리 (GiB)	인스턴스 스토리지 (GB)	EBS 최적화 사용 가능	네트워크 성능
t2.micro	Variable	1	1	EBS 전용	-	Low to Moderate

▾ 보안 그룹 보안 그룹 편집

보안 그룹 ID	이름	설명
sg-fb532686	u1-vpc-bastion	u1-vpc bastion host

선택한 모든 보안 그룹 인바운드 규칙

유형	프로토콜	포트 범위	소스	설명
모든 트래픽	모두	모두	0.0.0.0/0	

▸ 인스턴스 세부 정보 인스턴스 세부 정보 편집

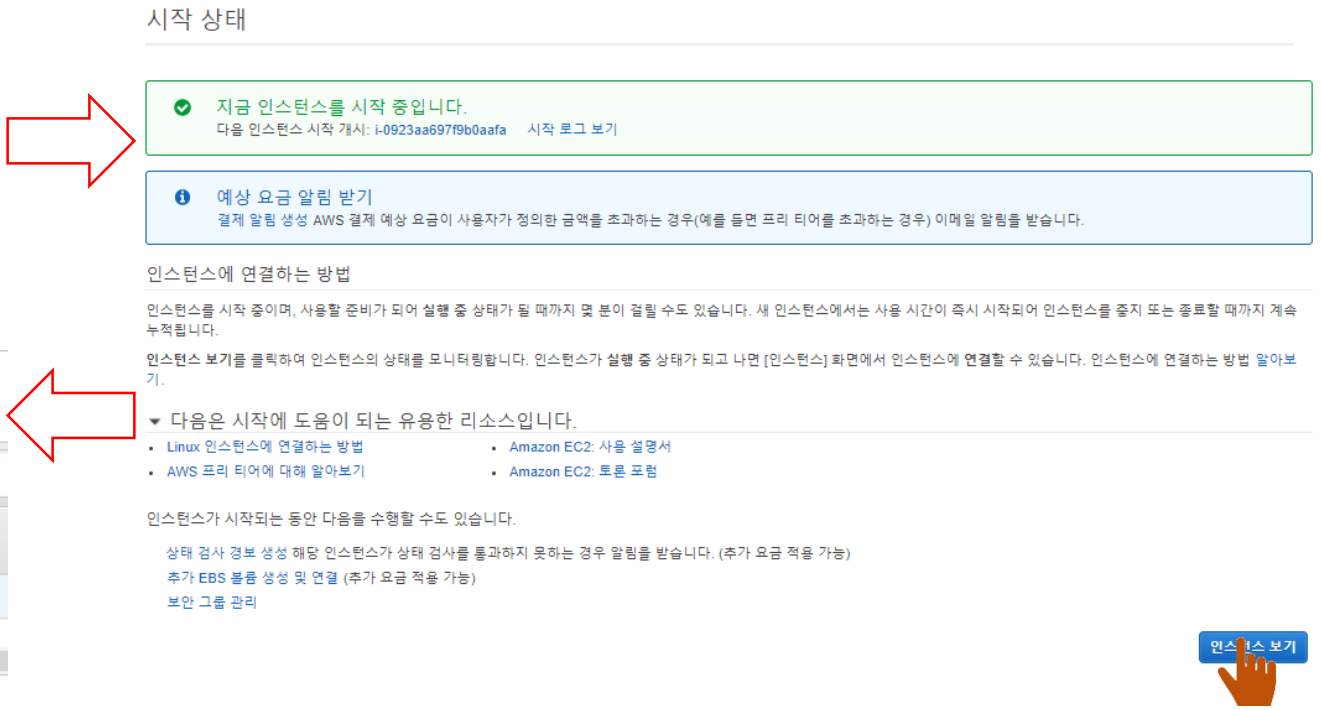
▸ 스토리지 스토리지 편집

▸ 태그 태그 편집

취소 이전 시

EC2

기존의 키 페어가 있으면 기존의 키 페어 선택,
키 페어가 없으면 새로 생성.
키 페어는 리전 당 발급되므로, 별도의 공간을 만들어 계정당/리전 당 별도 관리하는 것이 바람직함
재발급되지 않으므로 잘 보관해야 함.



EC2 (Bastion 호스트)

Name	인스턴스 ID	인스턴스 유형	가용 영역	인스턴스 상태	상태 검사	경보 상태	퍼블릭 DNS(IPv4)	IPv4 퍼블릭 IP	IPv6 IP	키 이름	모니터링	시작 시간	보안 그룹
u1-subnet-uw2a-public-ec2	i-0a5e0b47...	t2.micro	us-west-2a	running	2/2 검사 통과	없음		35.164.190.138	-	sthongu1ackr-oregon	disabled	2017년 1...	u1-vpc-bastion

인스턴스: i-0a5e0b47cc78600fe (u1-subnet-uw2a-public-ec2)

퍼블릭 IP: 35.164.190.138

탄력적 IP: 34.214.113.139

설명 | 상태 검사 | 모니터링 | 태그

인스턴스 ID	i-0a5e0b47cc78600fe	퍼블릭 DNS(IPv4)	-
인스턴스 상태	running	IPv4 퍼블릭 IP	35.164.190.138
인스턴스 유형	t2.micro	IPv6 IP	-
탄력적 IP		프라이빗 DNS	ip-10-0-1-65.us-west-2.compute.internal
가용 영역	us-west-2a	프라이빗 IP	10.0.1.65
보안 그룹	u1-vpc-bastion. 인바운드 규칙 보기	보조 프라이빗 IP	
예약된 이벤트	예약된 이벤트 없음	VPC ID	vpc-0191cd67
AMI ID	amzn-ami-hvm-2017.09.0.20170930-x86_64-gp2 (ami-e689729e)	서브넷 ID	subnet-c5f797a3
플랫폼	-	네트워크 인터페이스	eth0
IAM 역할	U1-EC2	소스/대상 확인	예
키 페어 이름	sthongu1ackr-oregon		
		EBS 최적	아니요
		루트 디바이스 유형	ebs
		루트 디바이스	/dev/xvda
		블록 디바이스	/dev/xvda

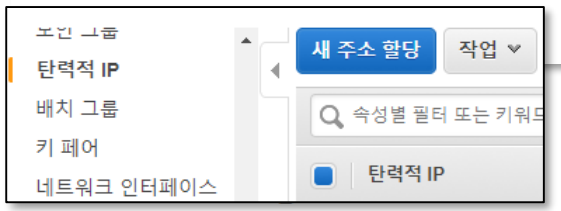
인스턴스와 관련한 정보를 확인할 수 있음.

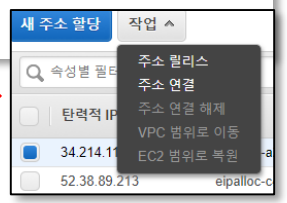
기본적으로 EC2인스턴스에는 퍼블릭, 프라이빗 IP/DNS가 각각 하나씩 할당됨.

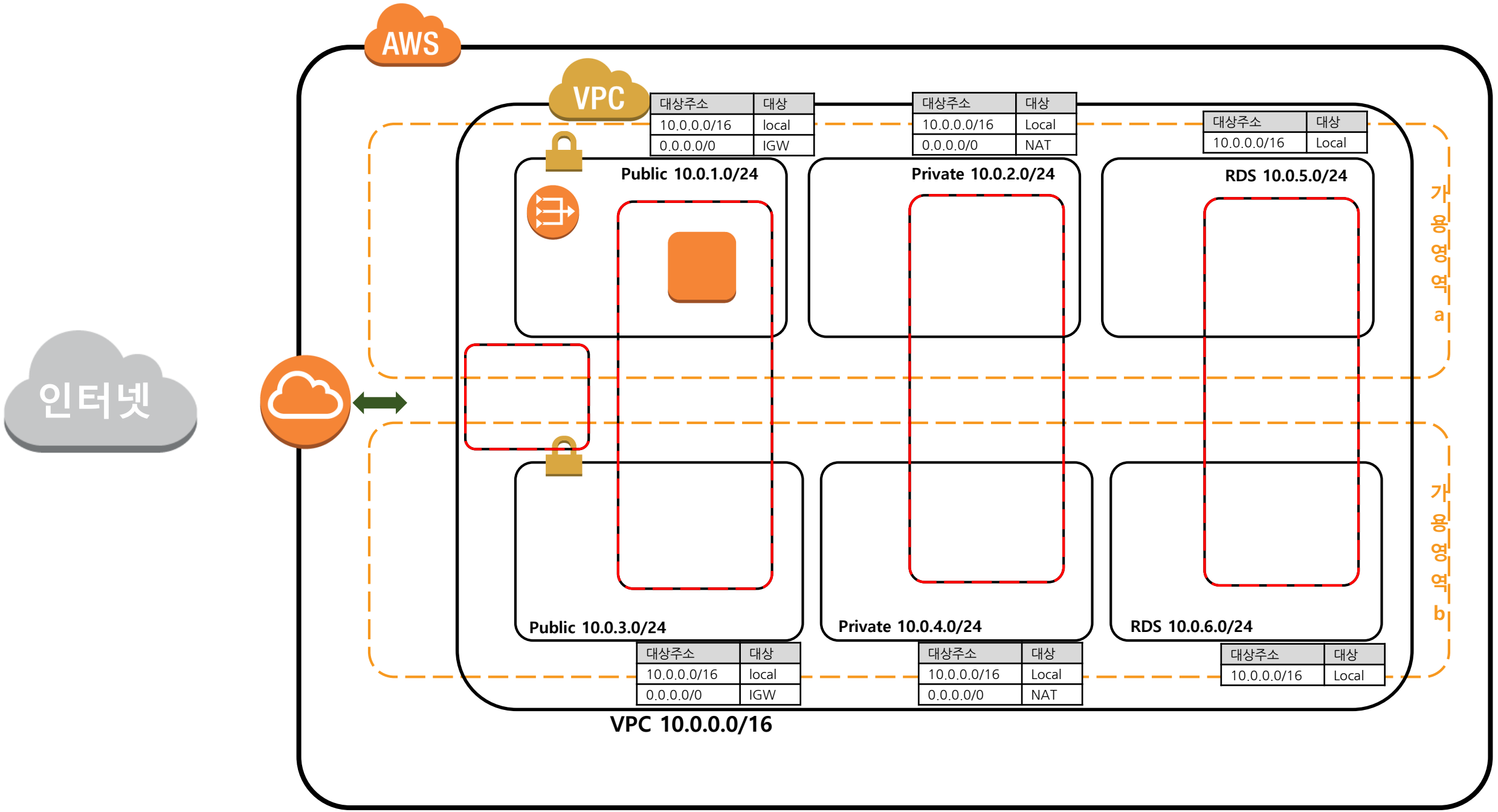
이 주소는 정시/시작의 작업에 따라 변경될 수 있음.

Bastion 호스트는 고정 IP가 필요하므로, EIP 설정으로 고정 IP를 확보함.

EIP가 할당되면 기존 퍼블릭 IP는 해제됨






AWS
VPC
인터넷
대상주소 | 대상
10.0.0.0/16 | local
0.0.0.0/0 | IGW
대상주소 | 대상
10.0.0.0/16 | Local
0.0.0.0/0 | NAT
대상주소 | 대상
10.0.0.0/16 | Local
Public 10.0.1.0/24
Private 10.0.2.0/24
RDS 10.0.5.0/24
가용영역 a
Public 10.0.3.0/24
Private 10.0.4.0/24
RDS 10.0.6.0/24
가용영역 b
대상주소 | 대상
10.0.0.0/16 | local
0.0.0.0/0 | IGW
대상주소 | 대상
10.0.0.0/16 | Local
0.0.0.0/0 | NAT
대상주소 | 대상
10.0.0.0/16 | Local
VPC 10.0.0.0/16

오레곤 리전

EC2 (Web Server)

AMI 세부 정보

AMI 편집

Amazon Linux AMI 2017.09.0 (HVM), SSD Volume Type - ami-e689729e

프리 티어 사용 가능

The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.

루트 디바이스 유형: ebs 가상화 유형: hvm

인스턴스 유형

인스턴스 유형 편집

인스턴스 유형	ECU	vCPUs	메모리 (GiB)	인스턴스 스토리지 (GB)	EBS 최적화 사용 가능	네트워크 성능
t2.micro	Variable	1	1	EBS 전용	-	Low to Moderate

보안 그룹

보안 그룹 편집

보안 그룹 ID	이름	설명
sg-6056231d	u1-vpc-webtier	u1-vpc Web Tier

선택한 모든 보안 그룹 인바운드 규칙

유형	프로토콜	포트 범위	소스	설명
이 보안 그룹에 규칙이 없습니다.				

인스턴스 세부 정보 편집

인스턴스 개수	1
네트워크	vpc-0191cd67
서브넷	subnet-60fb9b06
EBS 최적	아니요
모니터링	아니요
종료 방지	아니요
종료 방식	중지
IAM 역할	U1-EC2
테넌시	default
호스트 ID	
선호도	해제
커널 ID	기본값 사용
RAM 디스크 ID	기본값 사용
사용자 데이터	lyEvYmluL2Jhc2gKeXVtIC15IHVwZGF0ZQp5dW0gLXkgaW5zdGFsbCBodHRwZDI0IHBocDU2IG15c3FsNTUtc2VydmVyIHBocDU2LW15c3FsbmQKc2Vydm
퍼블릭 IP 할당	서브넷 사용 설정(활성화)
IPv6 IP 할당	서브넷 사용 설정(활성화)

네트워크 인터페이스

디바이스	네트워크 인터페이스	서브넷	기본 IP	보조 IP 주소
eth0	새 네트워크 인터페이스	subnet-60fb9b06	Auto-assign	

스토리지

스토리지 편집

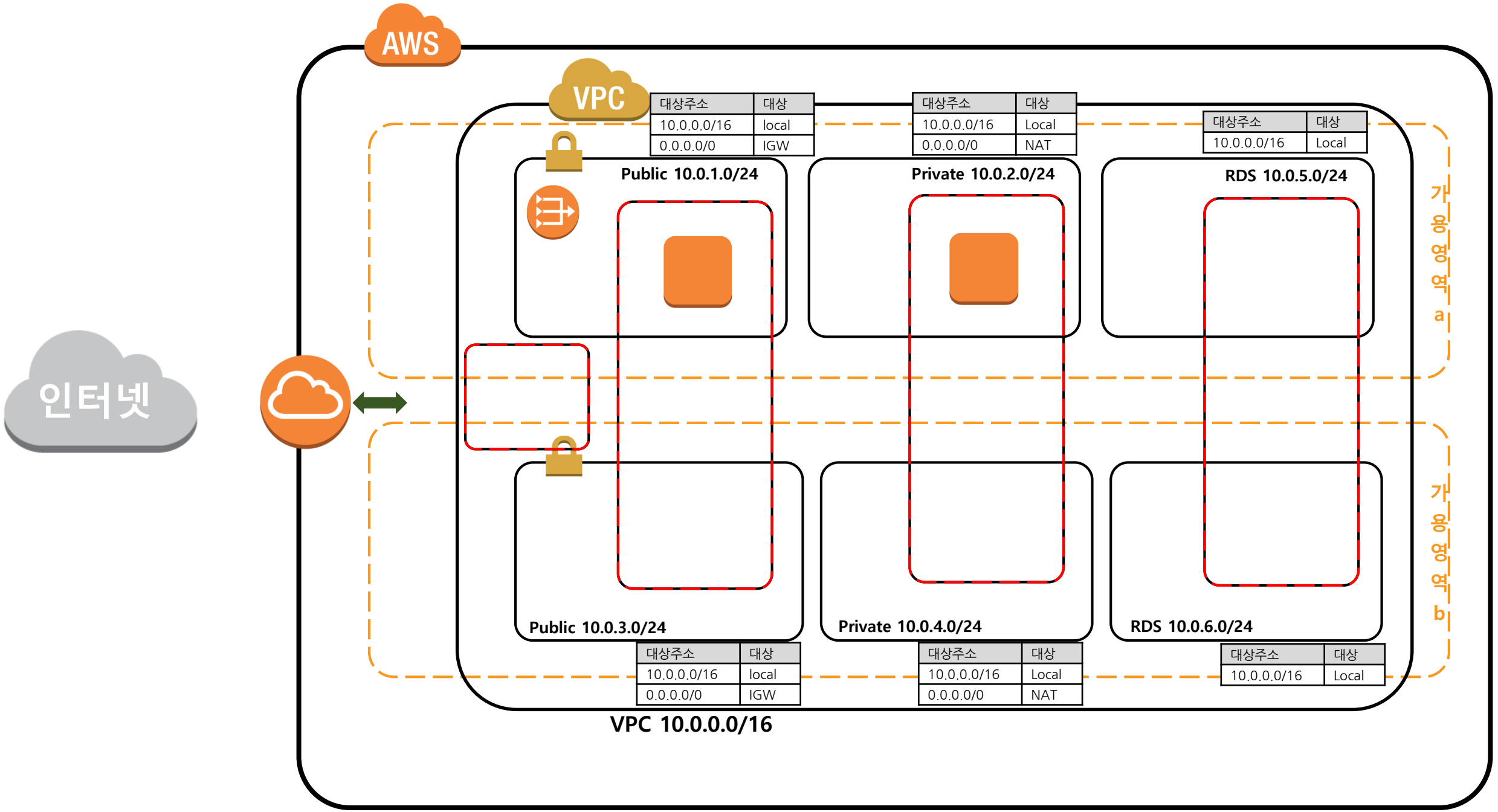
볼륨 유형	디바이스	스냅샷	크기(GiB)	볼륨 유형	IOPS	처리량(MB/초)	종료 시 삭제	암호화
루트	/dev/xvda	snap-0cfc1bfe4dc1b09e1	8	gp2	100/3000	해당 사항 없음	예	암호화되...

태그

태그 편집

키	값	인스턴스	볼륨
Name	u1-subnet-uw2a-private-ec2	✔	✔
Team	Cloud Computing Lab	✔	✔
Owner	SunTae Hong	✔	✔
Purpose	Web Server	✔	✔

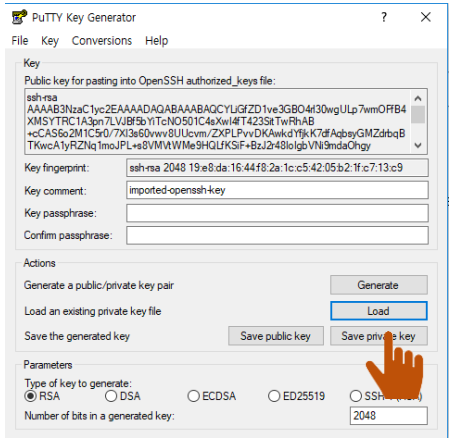
Name	인스턴스 ID	인스턴스 유형	가용 영역	인스턴스 상태	상태 검사	경보 상태	퍼블릭 DNS(IPv4)	IPv4 퍼블릭 IP	IPv6 IP	키 이름	모니터링	시작 시간	보안 그룹
u1-subnet-uw2a-private-ec2	i-0100beff4...	t2.micro	us-west-2a	running	초기화	없음		34.213.167.99	-	sthongu1ackr-oregon	disabled	2017년 1...	u1-vpc-webtier
u1-subnet-uw2a-public-ec2	i-0a5e0b47...	t2.micro	us-west-2a	running	2/2 검사 통과	없음		34.214.113.139	-	sthongu1ackr-oregon	disabled	2017년 1...	u1-vpc-bastion


AWS
VPC
인터넷
대상주소 | 대상
10.0.0.0/16 | local
0.0.0.0/0 | IGW
대상주소 | 대상
10.0.0.0/16 | Local
0.0.0.0/0 | NAT
대상주소 | 대상
10.0.0.0/16 | Local
Public 10.0.1.0/24
Private 10.0.2.0/24
RDS 10.0.5.0/24
가용영역 a
Public 10.0.3.0/24
Private 10.0.4.0/24
RDS 10.0.6.0/24
가용영역 b
대상주소 | 대상
10.0.0.0/16 | local
0.0.0.0/0 | IGW
대상주소 | 대상
10.0.0.0/16 | Local
0.0.0.0/0 | NAT
대상주소 | 대상
10.0.0.0/16 | Local
VPC 10.0.0.0/16

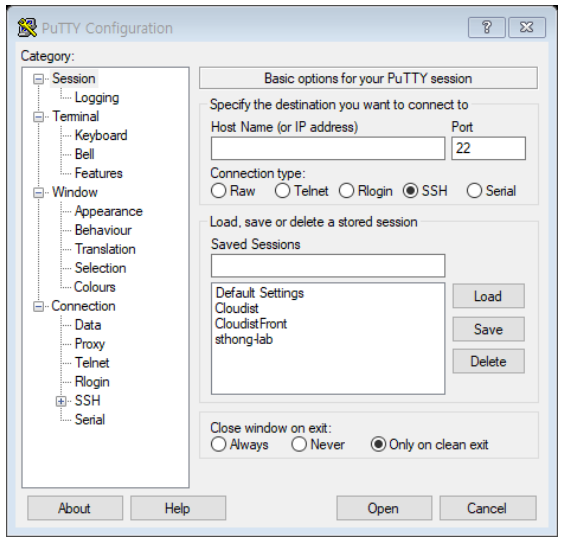
오레곤 리전

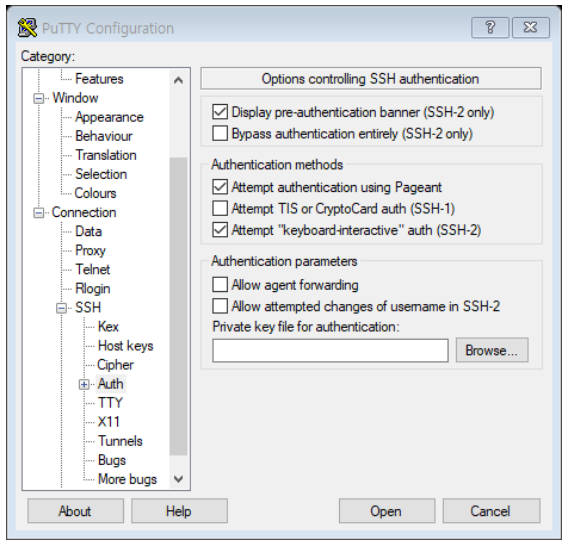
EC2 SSH Access

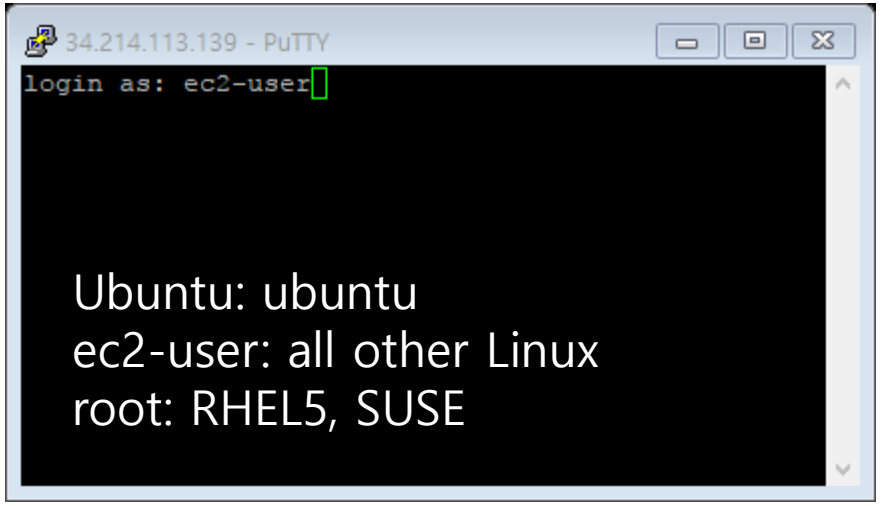
1. PuTTY 다운로드 (http://www.putty.org/)
2. PuTTYgen 실행-Load-확장자:모든파일-키페어 열기-Save Private Key

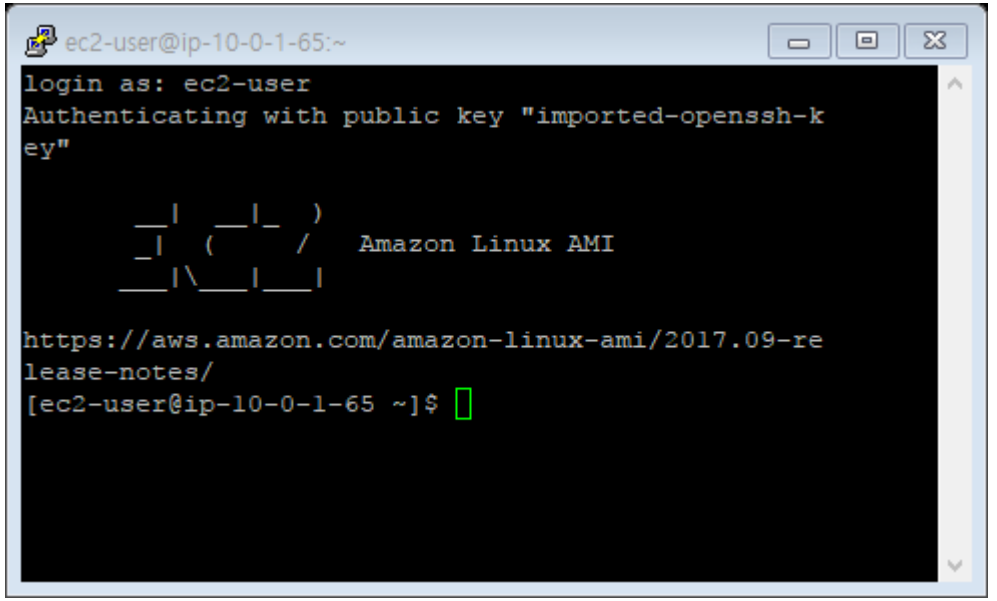


3. PuTTY 실행-Host Name: u1-subnet-uw2a-public-ec2의 EIP 입력
4. Connection/SSH/Auth에서 저장한 키페어 불러오기- Open



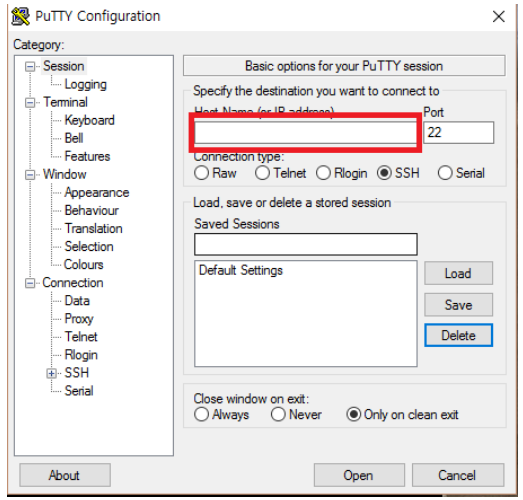




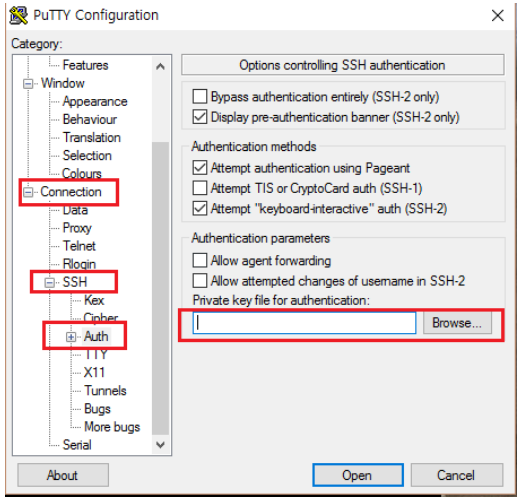


EC2 배스천을 통한 터널링 액세스

1. 배스천 서버의 IP 입력



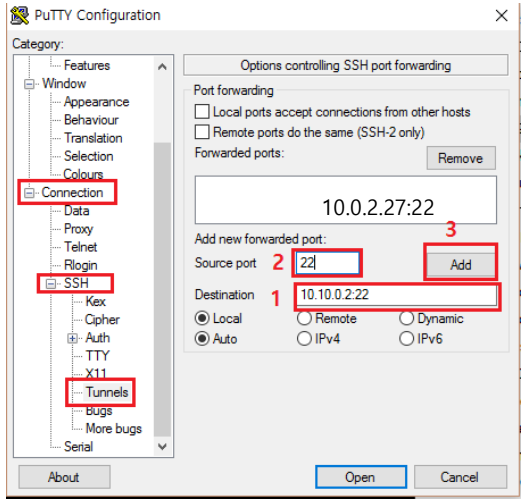
2. 키 페어 저장



3. 터널링 (connection-SSH-Tunnel)

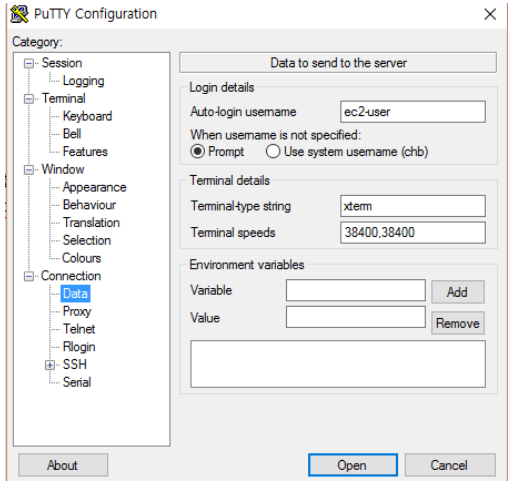
프라이빗 서버의 사설 IP, 포트 22

프라이빗 서버의 사설 IP, 포트 80

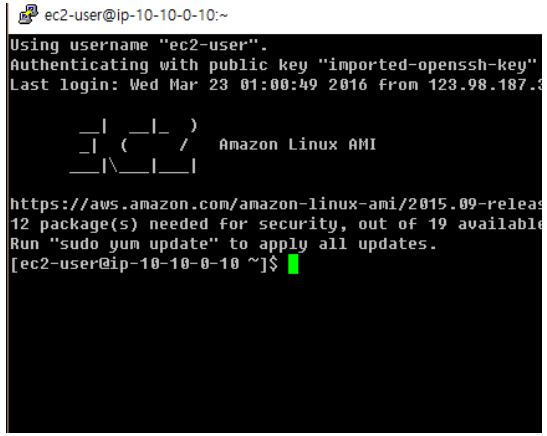


4. connection-data에서

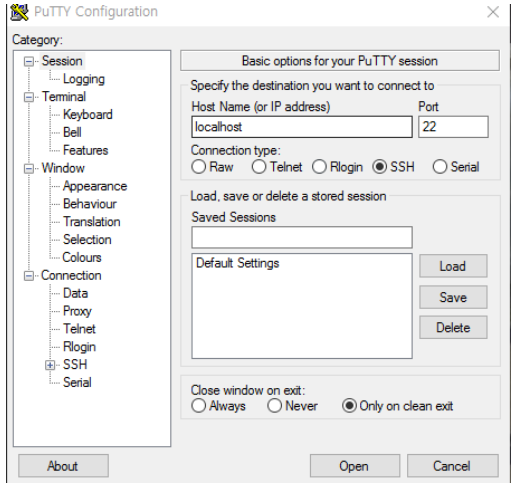
Auto-login username: ec2-user



5. Open 을 클릭, 창이 열리면, 그대로 두고 새 PuTTY창 열기.

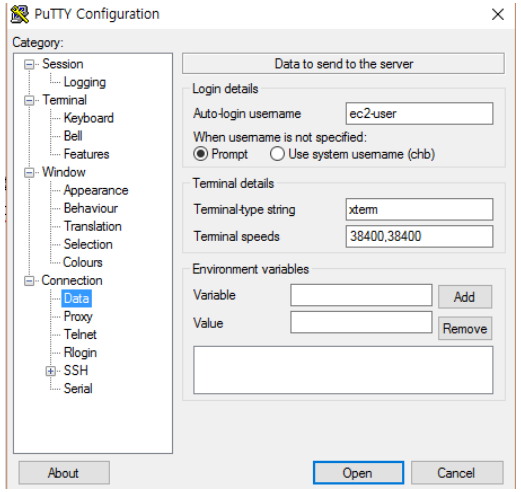


6. Host name: localhost, 포트:22

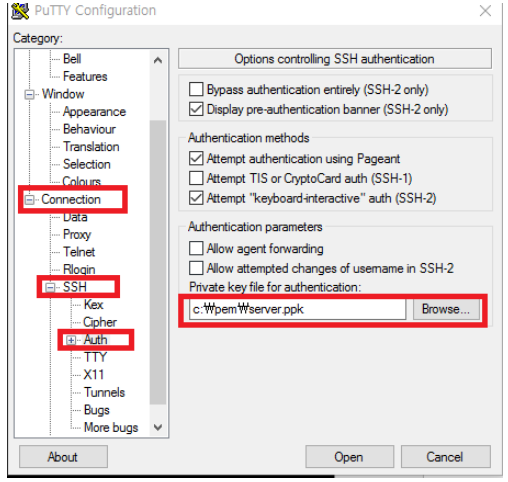


7. Connection-Data에서

Auto-login username: ec2-user



8. 키페어 저장, 그리고 Open



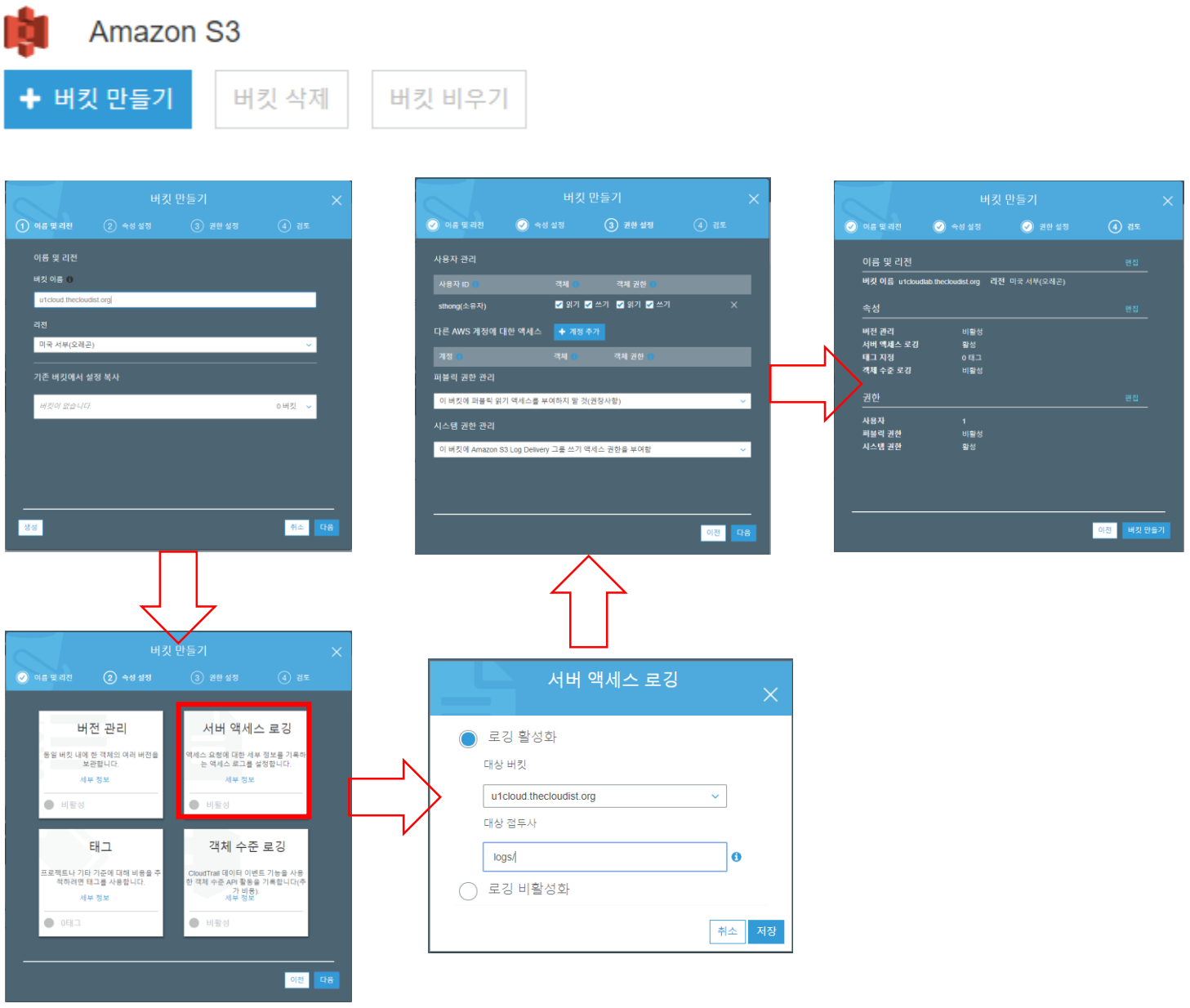
EC2 실습의 비용 계산

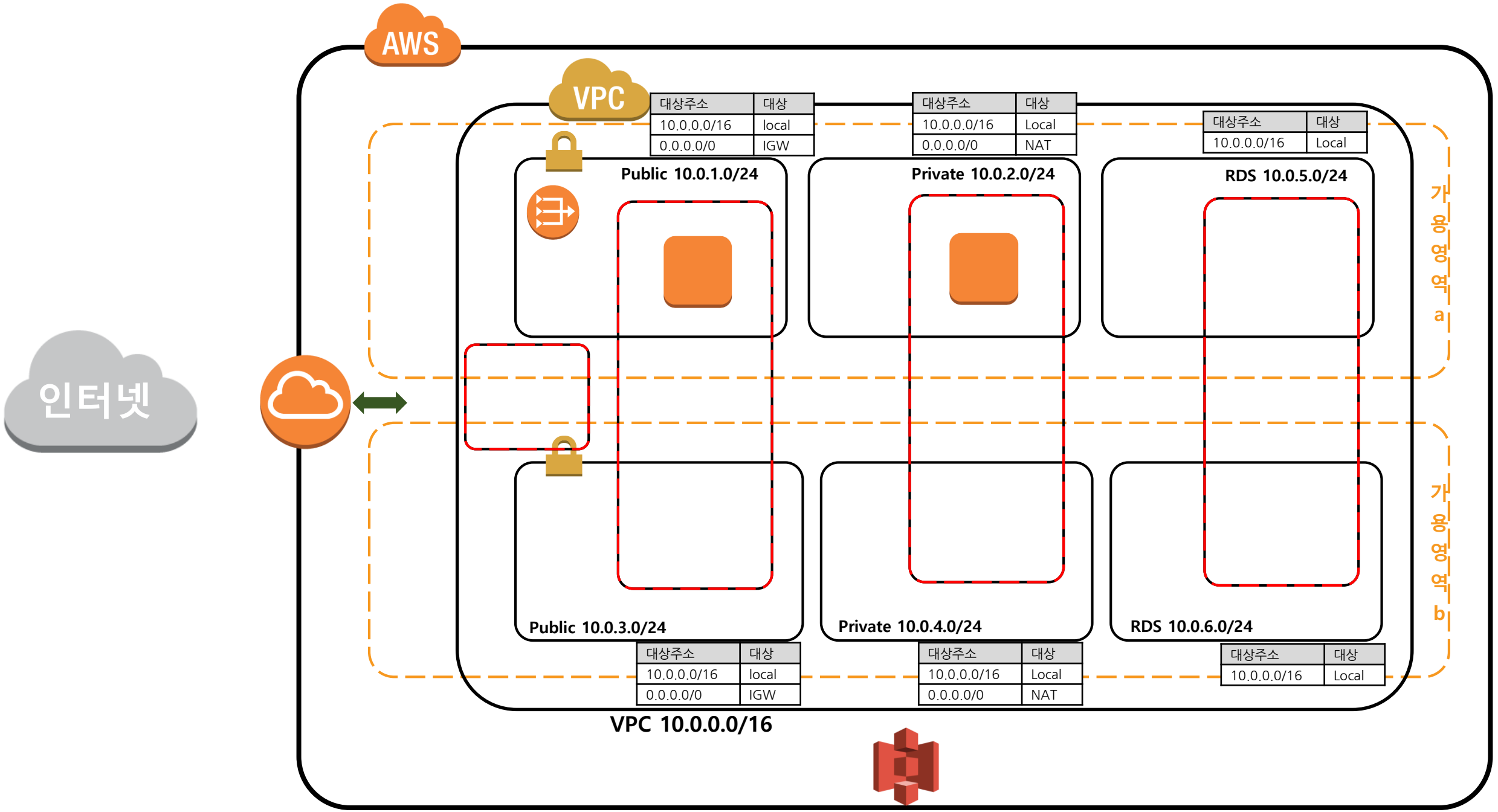
EC2는 EC2 인스턴스 사용 시간, Data Transfer(AZ단위, Region단위, 기타 구간에 따라 다름), 그리고 EBS 볼륨 크기와 타입. 이 세가지 요소로 과금된다.

인스턴스 사용시간은 인스턴스 타입, AMI 종류, 과금 모델에 따라 단가가 다름.

Amazon S3

- 이번 장은 Qwiklabs의 랩으로 대체합니다.

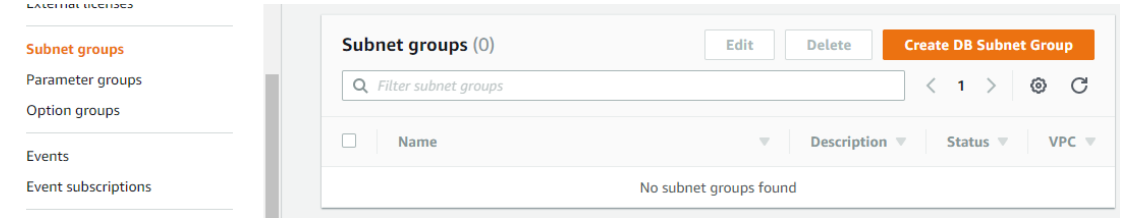

Amazon S3
+ 버킷 만들기
버킷 삭제
버킷 비우기
버킷 만들기
이름 및 리전
속성 설정
권한 설정
검토
버킷 이름
u1cloud.thecloudist.org
리전
미국 서부(오레곤)
기존 버킷에서 설정 복사
버킷이 없습니다
0 버킷
생성
취소
다음
사용자 관리
사용자 ID
객체
객체 권한
sthong(소유자)
읽기
쓰기
다른 AWS 계정에 대한 액세스
+ 계정 추가
계정
퍼블릭 권한 관리
이 버킷에 퍼블릭 읽기 액세스를 부여하지 말 것(권장사항)
시스템 권한 관리
이 버킷에 Amazon S3 Log Delivery 그룹 쓰기 액세스 권한을 부여함
이전
다음
이름 및 리전
편집
버킷 이름 u1cloudlab.thecloudist.org
리전 미국 서부(오레곤)
속성
버전 관리
비활성
서버 액세스 로깅
활성
태그 지정
0 태그
객체 수준 로깅
비활성
권한
사용자
1
퍼블릭 권한
비활성
시스템 권한
활성
이전
버킷 만들기
버전 관리
동일 버킷 내에 한 객체의 여러 버전을 보관합니다.
세부 정보
비활성
서버 액세스 로깅
액세스 요청에 대한 세부 정보를 기록하는 액세스 로그를 설정합니다.
세부 정보
비활성
태그
프로젝트나 기타 기준에 대해 비용을 추적하려면 태그를 사용합니다.
세부 정보
0태그
객체 수준 로깅
CloudTrail 데이터 이벤트 기능을 사용한 객체 수준 API 활동을 기록합니다(추가 비용).
세부 정보
비활성
이전
다음
서버 액세스 로깅
로깅 활성화
대상 버킷
u1cloud.thecloudist.org
대상 접두사
logs/
로깅 비활성화
취소
저장

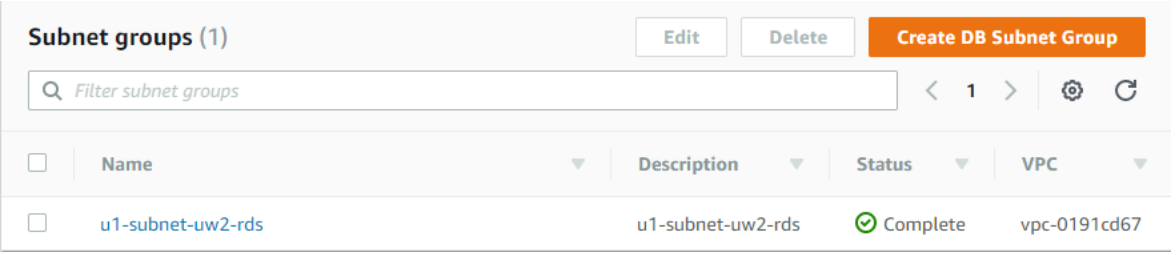

AWS
VPC
인터넷
대상주소 | 대상
10.0.0.0/16 | local
0.0.0.0/0 | IGW
대상주소 | 대상
10.0.0.0/16 | Local
0.0.0.0/0 | NAT
대상주소 | 대상
10.0.0.0/16 | Local
Public 10.0.1.0/24
Private 10.0.2.0/24
RDS 10.0.5.0/24
가용영역 a
Public 10.0.3.0/24
Private 10.0.4.0/24
RDS 10.0.6.0/24
가용영역 b
대상주소 | 대상
10.0.0.0/16 | local
0.0.0.0/0 | IGW
대상주소 | 대상
10.0.0.0/16 | Local
0.0.0.0/0 | NAT
대상주소 | 대상
10.0.0.0/16 | Local
VPC 10.0.0.0/16

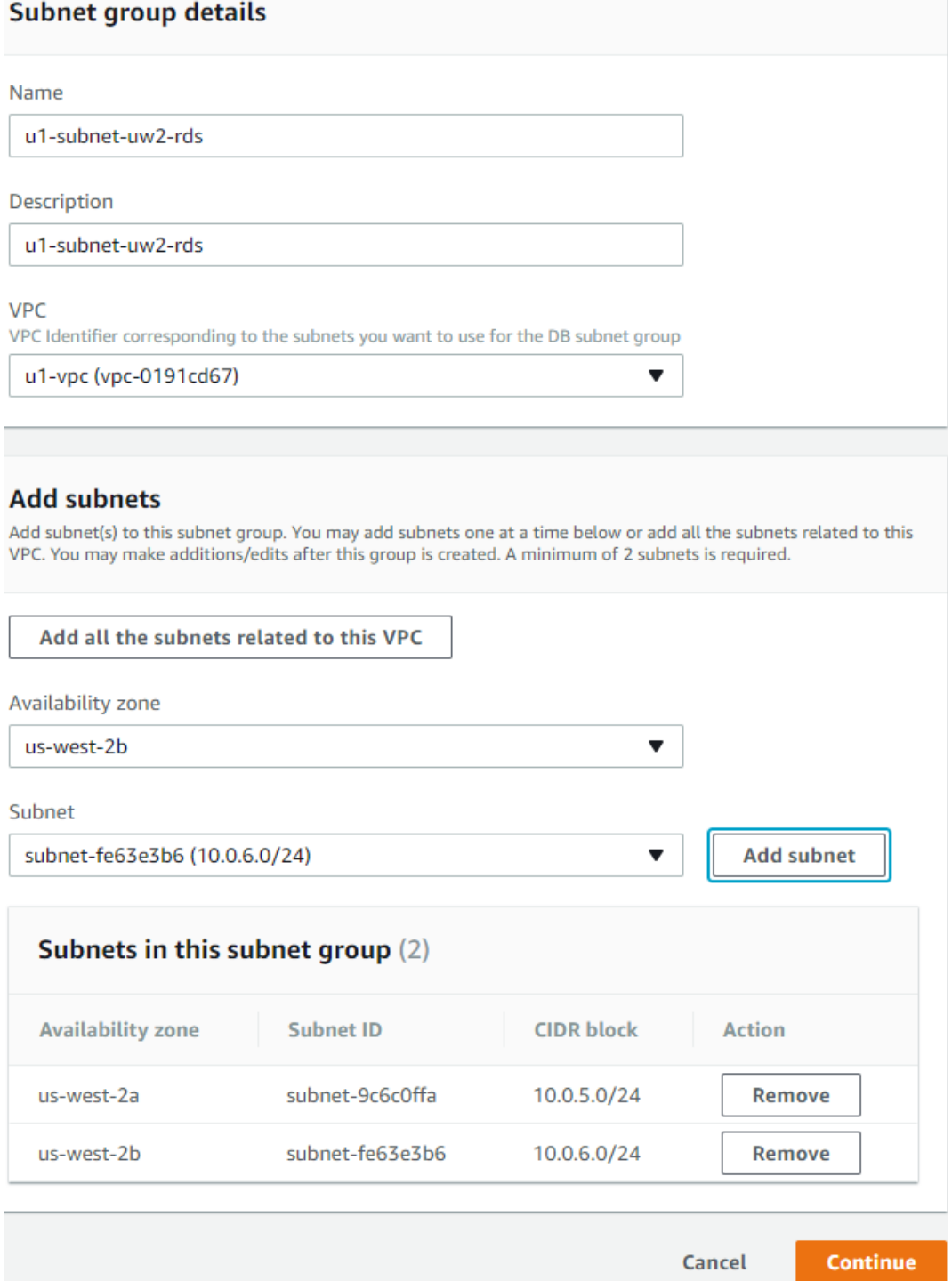
오레곤 리전

Amazon RDS

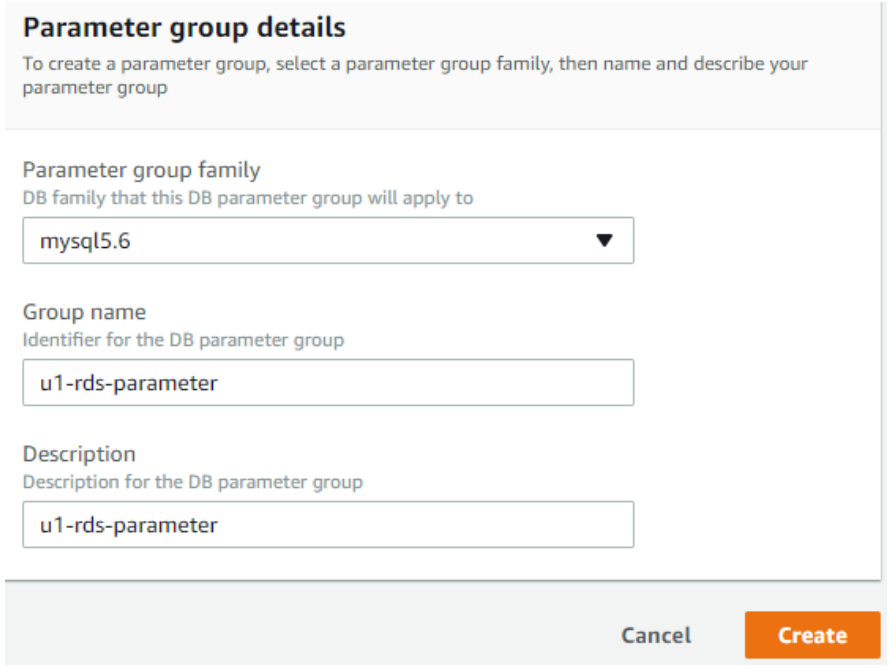
RDS subnet group

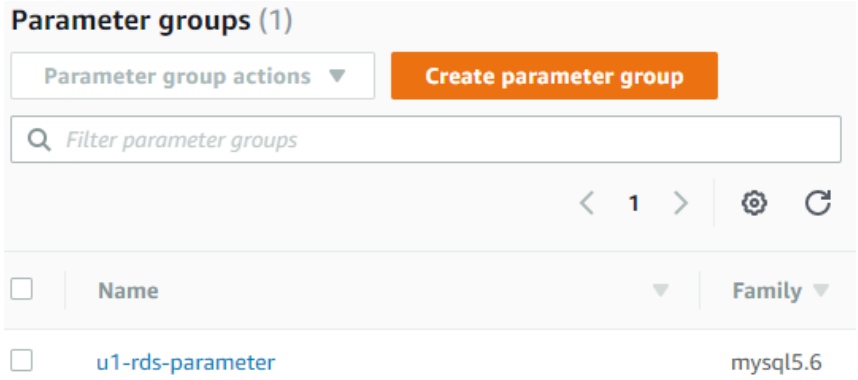


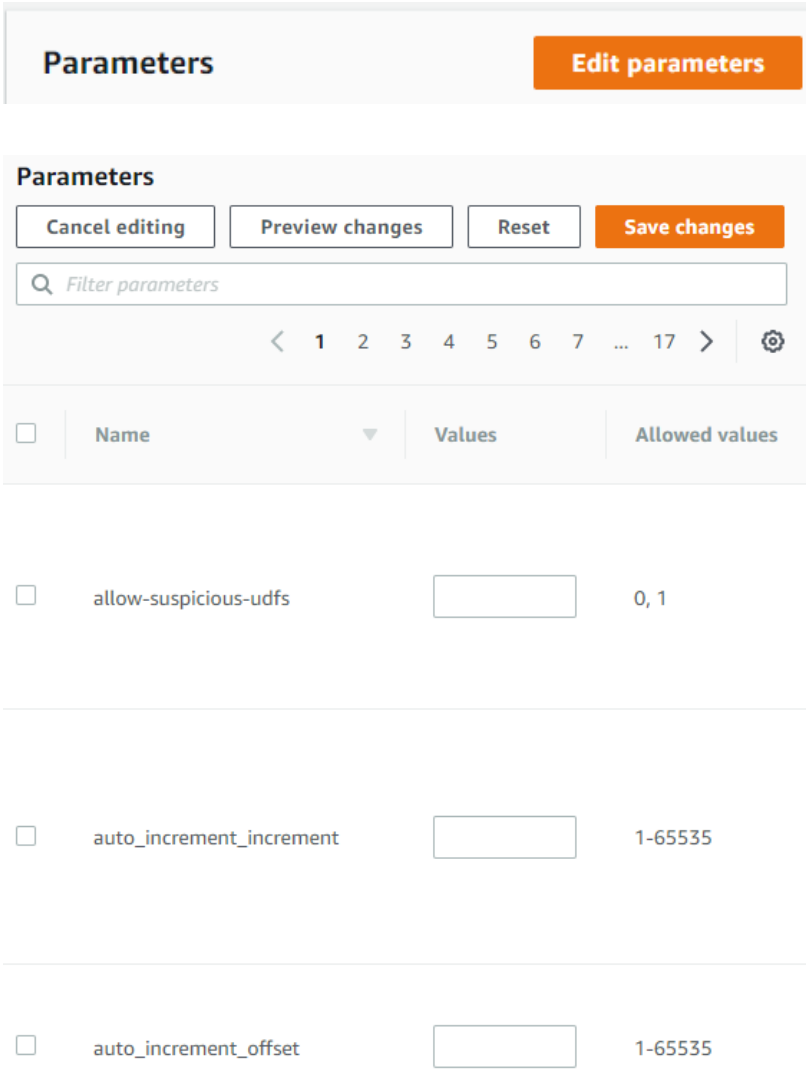




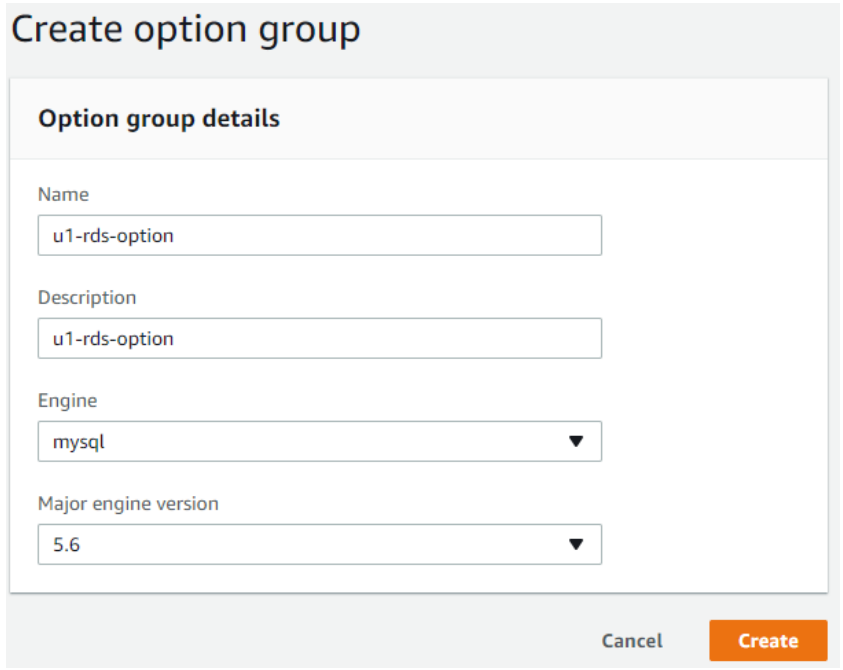
RDS Parameter group

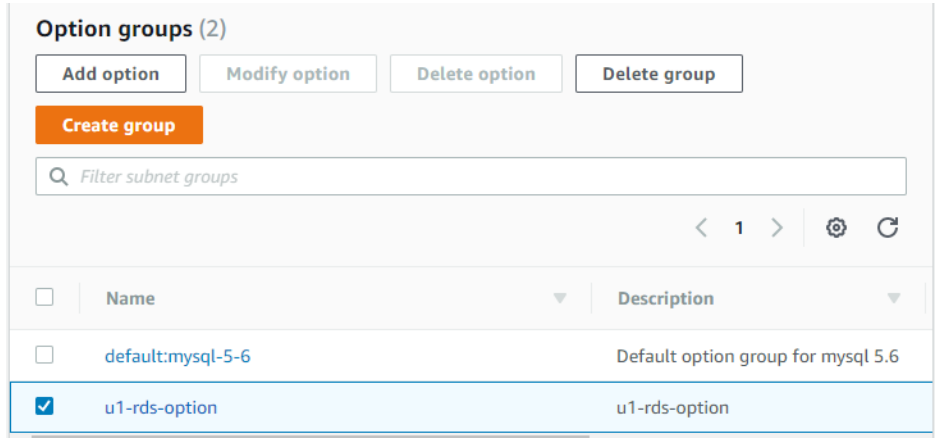


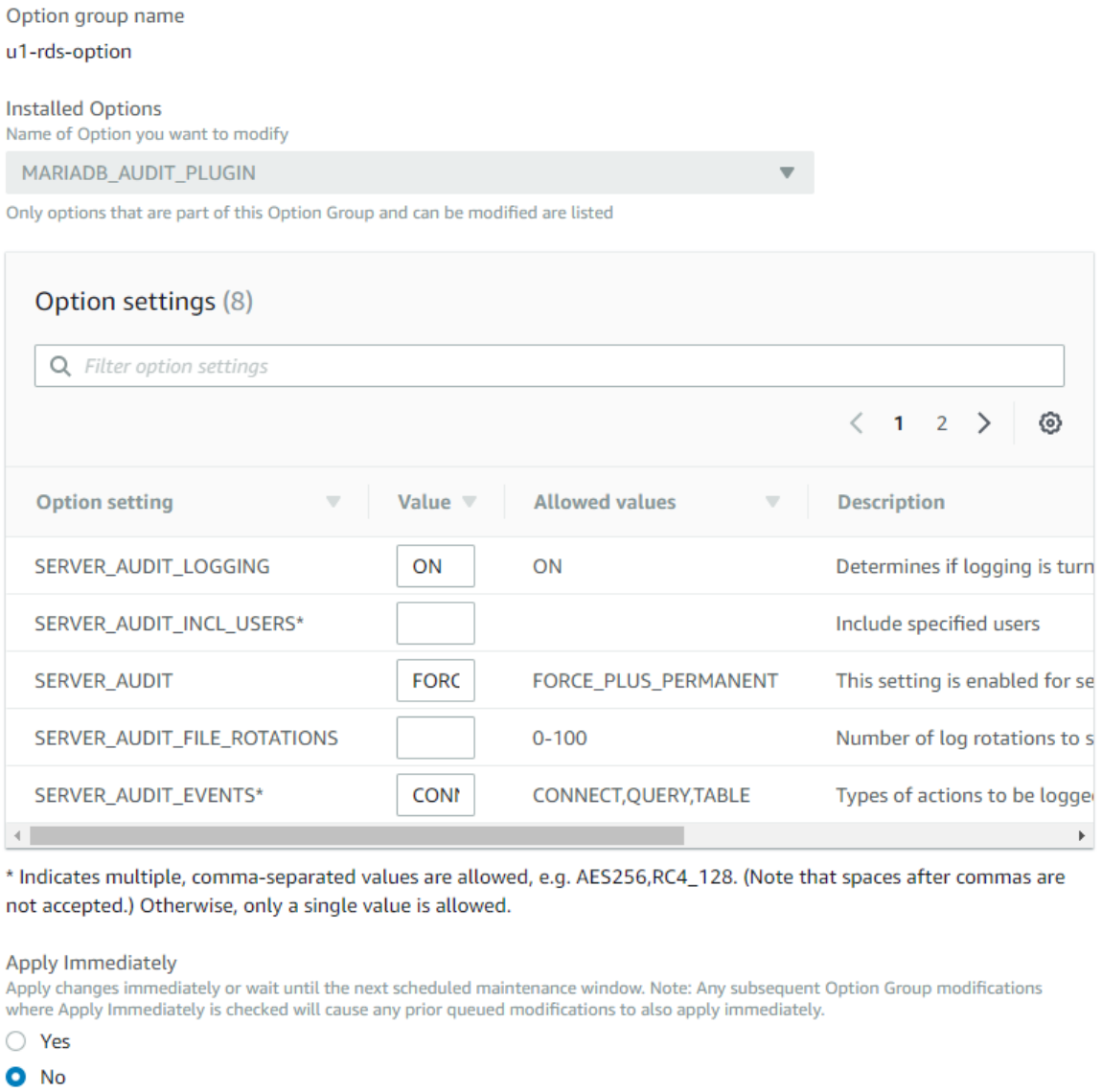




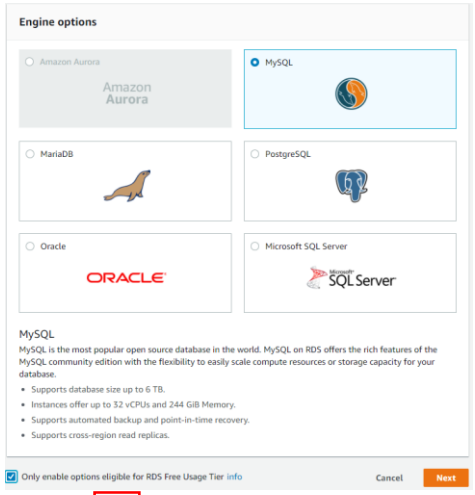
RDS Option group

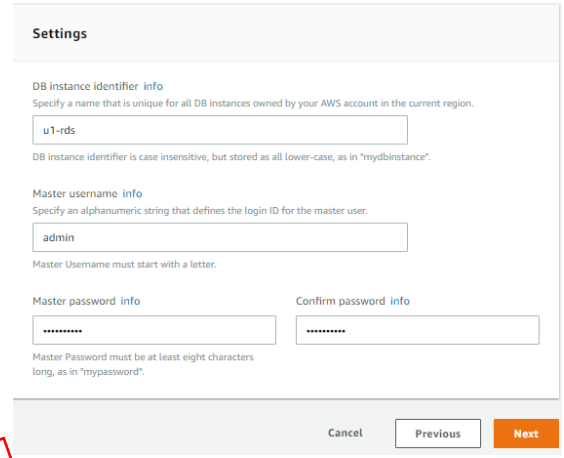


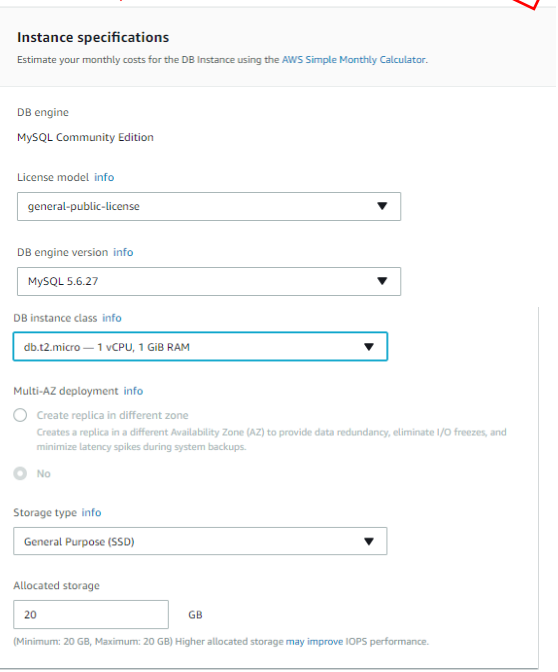


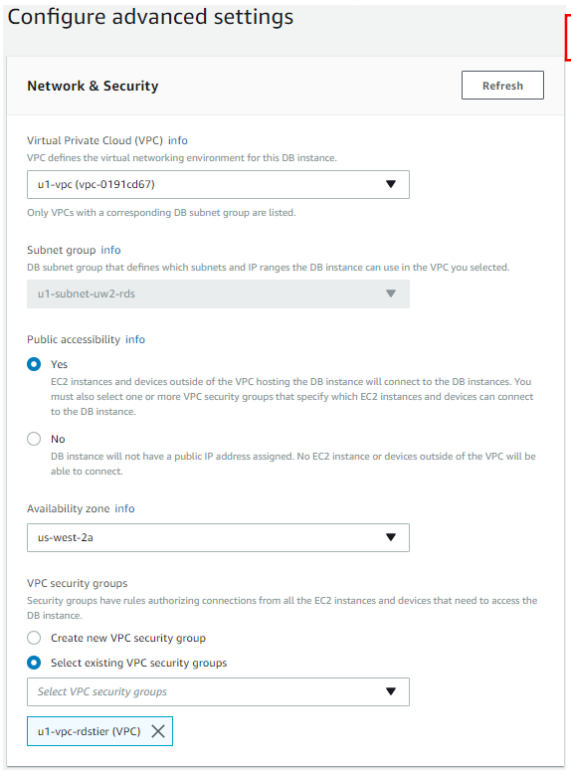


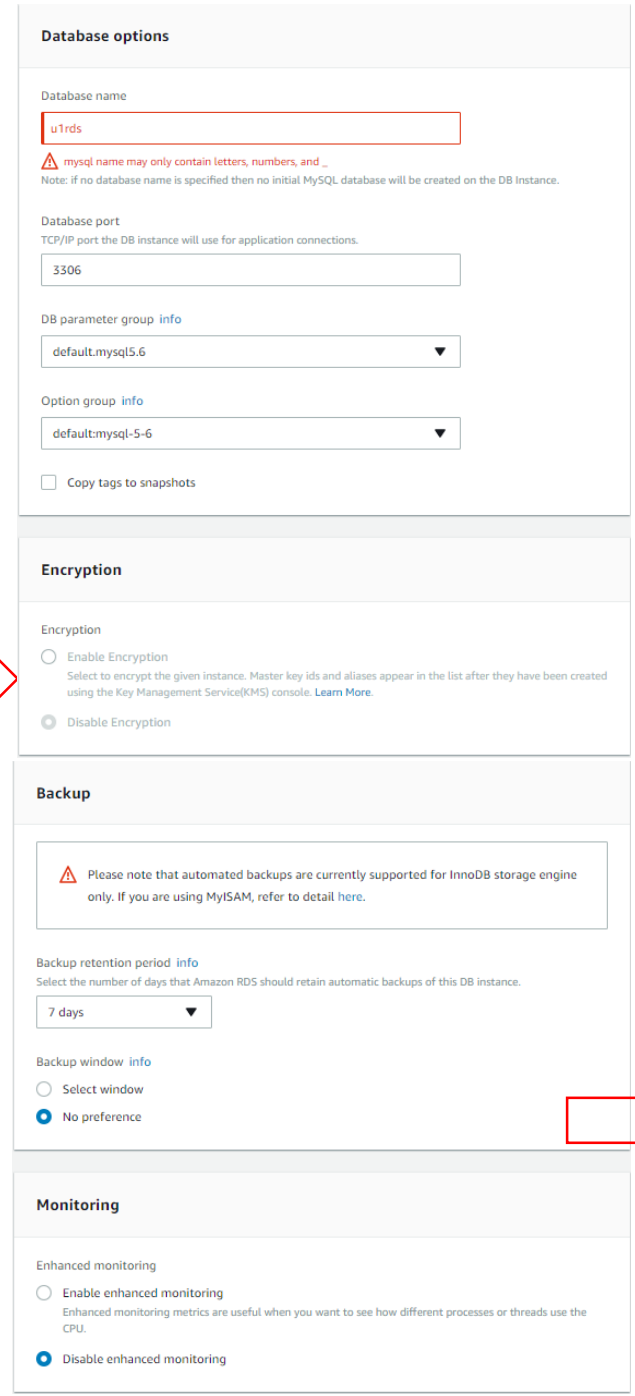
RDS 인스턴스 생성

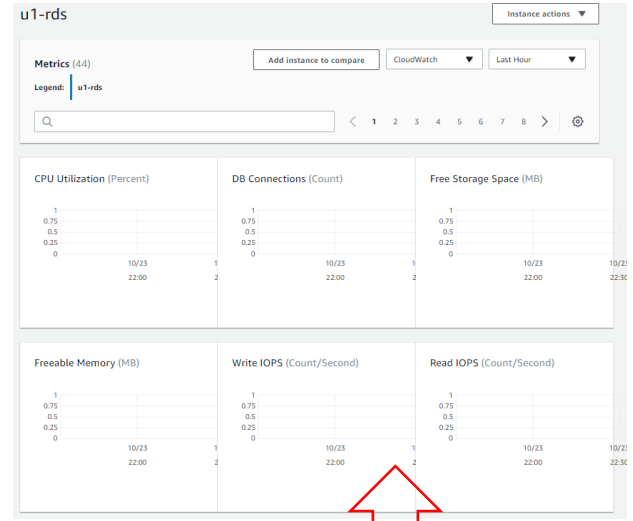

Engine options
Amazon Aurora
MySQL
MariaDB
PostgreSQL
Oracle
Microsoft SQL Server
MySQL
MySQL is the most popular open source database in the world. MySQL on RDS offers the rich features of the MySQL community edition with the flexibility to easily scale compute resources or storage capacity for your database.
Supports database size up to 6 TB.
Instances offer up to 32 vCPUs and 244 GiB Memory.
Supports automated backup and point-in-time recovery.
Supports cross-region read replicas.
Only enable options eligible for RDS Free Usage Tier info
Cancel
Next

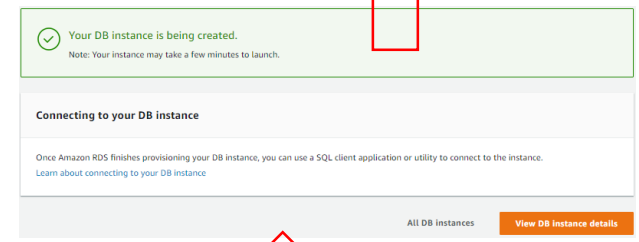

Settings
DB instance identifier info
Specify a name that is unique for all DB instances owned by your AWS account in the current region.
u1-rds
DB instance identifier is case insensitive, but stored as all lower-case, as in "mydbinstance".
Master username info
Specify an alphanumeric string that defines the login ID for the master user.
admin
Master Username must start with a letter.
Master password info
Confirm password info
Master Password must be at least eight characters long, as in "mypassword".
Cancel
Previous
Next

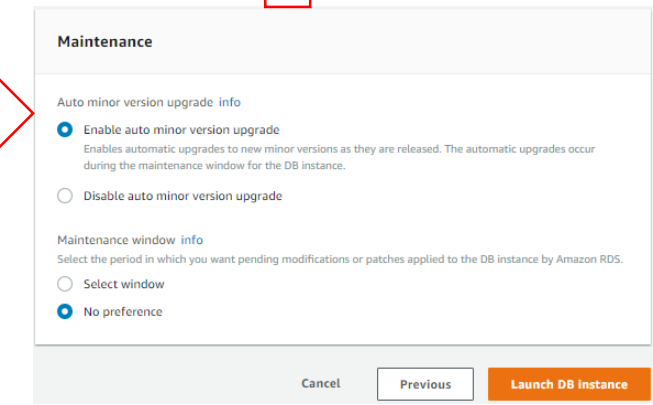

Instance specifications
Estimate your monthly costs for the DB Instance using the AWS Simple Monthly Calculator.
DB engine
MySQL Community Edition
License model info
general-public-license
DB engine version info
MySQL 5.6.27
DB instance class info
db.t2.micro — 1 vCPU, 1 GiB RAM
Multi-AZ deployment info
Create replica in different zone
Creates a replica in a different Availability Zone (AZ) to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups.
No
Storage type info
General Purpose (SSD)
Allocated storage
20
GB
(Minimum: 20 GB, Maximum: 20 GB) Higher allocated storage may improve IOPS performance.


Configure advanced settings
Network & Security
Refresh
Virtual Private Cloud (VPC) info
VPC defines the virtual networking environment for this DB instance.
u1-vpc (vpc-0191cd67)
Only VPCs with a corresponding DB subnet group are listed.
Subnet group info
DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.
u1-subnet-uw2-rds
Public accessibility info
Yes
EC2 instances and devices outside of the VPC hosting the DB instance will connect to the DB instances. You must also select one or more VPC security groups that specify which EC2 instances and devices can connect to the DB instance.
No
DB instance will not have a public IP address assigned. No EC2 instance or devices outside of the VPC will be able to connect.
Availability zone info
us-west-2a
VPC security groups
Security groups have rules authorizing connections from all the EC2 instances and devices that need to access the DB instance.
Create new VPC security group
Select existing VPC security groups
Select VPC security groups
u1-vpc-rdstier (VPC)


Database options
Database name
u1rds
mysql name may only contain letters, numbers, and _
Note: if no database name is specified then no initial MySQL database will be created on the DB Instance.
Database port
TCP/IP port the DB instance will use for application connections.
3306
DB parameter group info
default.mysql5.6
Option group info
default:mysql-5-6
Copy tags to snapshots
Encryption
Encryption
Enable Encryption
Select to encrypt the given instance. Master key ids and aliases appear in the list after they have been created using the Key Management Service(KMS) console. Learn More.
Disable Encryption
Backup
Please note that automated backups are currently supported for InnoDB storage engine only. If you are using MyISAM, refer to detail here.
Backup retention period info
Select the number of days that Amazon RDS should retain automatic backups of this DB instance.
7 days
Backup window info
Select window
No preference
Monitoring
Enhanced monitoring
Enable enhanced monitoring
Enhanced monitoring metrics are useful when you want to see how different processes or threads use the CPU.
Disable enhanced monitoring


u1-rds
Instance actions
Metrics (44)
Add instance to compare
CloudWatch
Last Hour
Legend:
u1-rds
CPU Utilization (Percent)
DB Connections (Count)
Free Storage Space (MB)
Freeable Memory (MB)
Write IOPS (Count/Second)
Read IOPS (Count/Second)


Your DB instance is being created.
Note: Your instance may take a few minutes to launch.
Connecting to your DB instance
Once Amazon RDS finishes provisioning your DB instance, you can use a SQL client application or utility to connect to the instance.
Learn about connecting to your DB instance
All DB instances
View DB instance details


Maintenance
Auto minor version upgrade info
Enable auto minor version upgrade
Enables automatic upgrades to new minor versions as they are released. The automatic upgrades occur during the maintenance window for the DB instance.
Disable auto minor version upgrade
Maintenance window info
Select the period in which you want pending modifications or patches applied to the DB instance by Amazon RDS.
Select window
No preference
Cancel
Previous
Launch DB instance

RDS Details

Details

Configurations

ARN
arn:aws:rds:us-west-2:629491326515:db:u1-rds

Engine
MySQL 5.6.27

License Model
General Public License

Created Time
Mon Oct 23 22:35:07 GMT+900 2017

DB Name
u1rds

Username
admin

Option Group
default:mysql-5-6

Parameter group
default.mysql5.6 (in-sync)

Copy tags to snapshots
false

Resource ID
db-MVFDCN4OJ3CXQDCWEFUCZTRALI

IAM DB Authentication Enabled
No

Security and network

Availability zone
us-west-2a

VPC
u1-vpc (vpc-0191cd67)

Subnet group
u1-subnet-uw2-rds

Subnets
subnet-9c6c0ffa
subnet-fe63e3b6

Security groups
sg-fd502580

Publicly accessible
No

Endpoint
u1-rds.c9i9apmmjzd2.us-west-2.rds.amazonaws.com

Certificate authority
rds-ca-2015 (Mar 5, 2020)

Instance and IOPS

Instance Class
db.t2.micro

Storage Type
General Purpose (SSD)

Storage
20 GB

Availability and durability

DB instance status
backing-up

Multi AZ
No

Automated backups
Enabled (7 Days)

Maintenance details

Auto minor version upgrade
Yes

Maintenance window
fri:10:56-fri:11:26

Backup window
12:38-13:08

Pending Modifications
None

Pending Maintenance
none

Encryption details

Encryption enabled
No

Endpoint는 RDS 접속 주소(DNS)

RDS

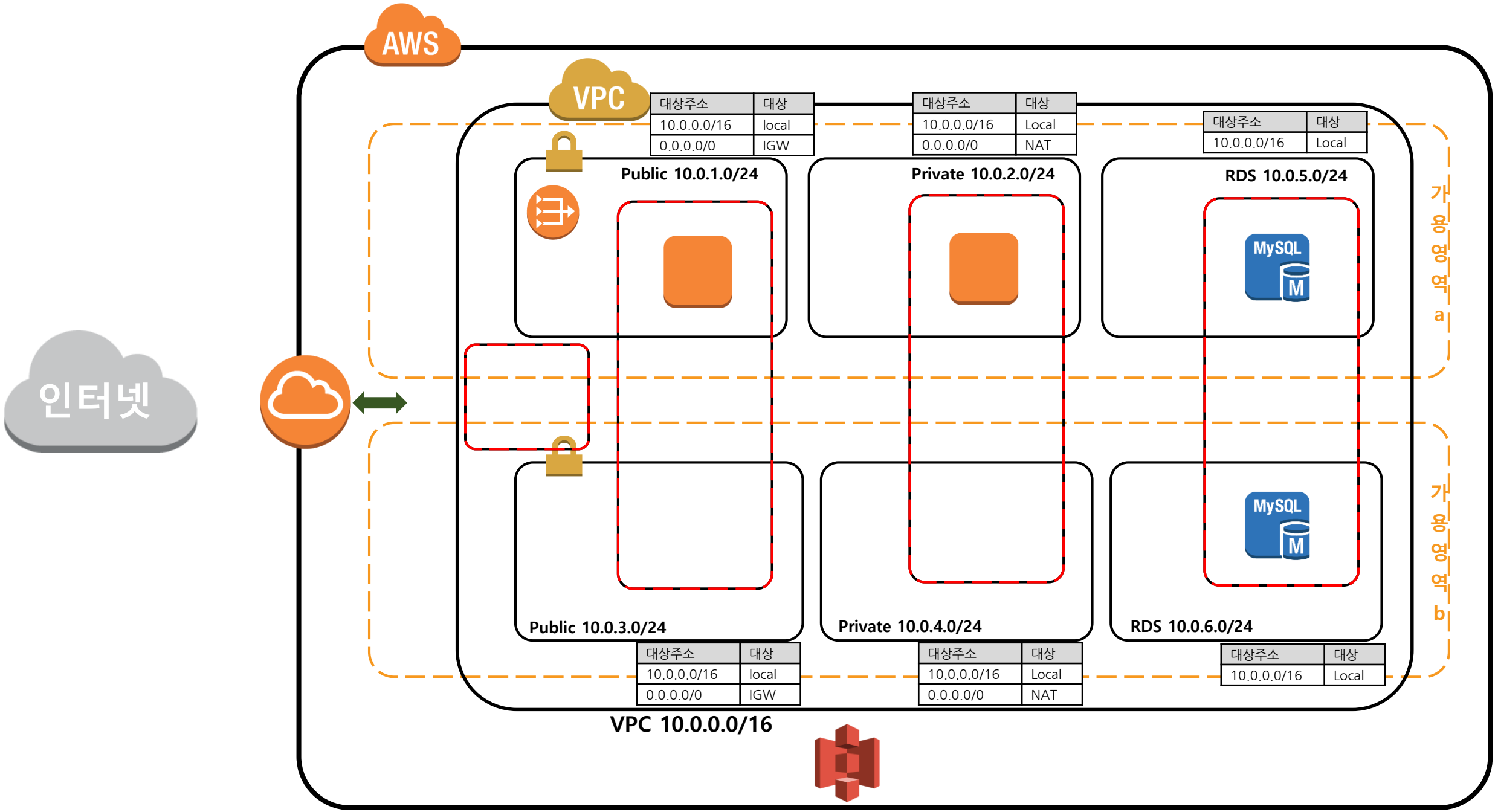
프라이빗 서브넷의 웹서버 EC2에 접속

mysql - u '계정명' -h 'RDS endpoint' -p

를 입력하고, 패스워드 입력

show databases;

로 테이블 확인


AWS
VPC
인터넷
대상주소 | 대상
10.0.0.0/16 | local
0.0.0.0/0 | IGW
대상주소 | 대상
10.0.0.0/16 | Local
0.0.0.0/0 | NAT
대상주소 | 대상
10.0.0.0/16 | Local
Public 10.0.1.0/24
Private 10.0.2.0/24
RDS 10.0.5.0/24
MySQL
가용영역 a
가용영역 b
Public 10.0.3.0/24
Private 10.0.4.0/24
RDS 10.0.6.0/24
대상주소 | 대상
10.0.0.0/16 | local
0.0.0.0/0 | IGW
대상주소 | 대상
10.0.0.0/16 | Local
0.0.0.0/0 | NAT
대상주소 | 대상
10.0.0.0/16 | Local
VPC 10.0.0.0/16

오레곤 리전

RDS 실습의 비용 계산

RDS 인스턴스 사용시간, EBS 사용량에 따라 비용 과금

Web Application: WordPress

WordPress

1. 퍼블릭 서브넷의 Bastion 서버에 SSH접속
2. 프라이빗 서브넷의 웹서버에 SSH 접속
3. sudo wget https://ko.wordpress.org/wordpress-4.8.2-ko_KR.tar.gz
4. sudo tar -zxvf wordpress-4.8.2-ko_KR.tar.gz
5. sudo cp -fr wordpress/* var/www/html
6. sudo cd /var/www/html
7. sudo cp wp-config-sample.php wp-config.php
8. sudo chown -R apache /var/www/html
9. sudo chmod 755 /var/www/html
10. sudo vi /var/www/html/wp-config.php

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'ulrds');

/** MySQL database username */
define('DB_USER', 'admin');

/** MySQL database password */
define('DB_PASSWORD', '    ****    ');

/** MySQL hostname */
define('DB_HOST', 'ul-rds.c9i9apmmjzd2.us-west-2.rds.amazonaws.com');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

생성한 RDS DB명

DB 관리자 ID

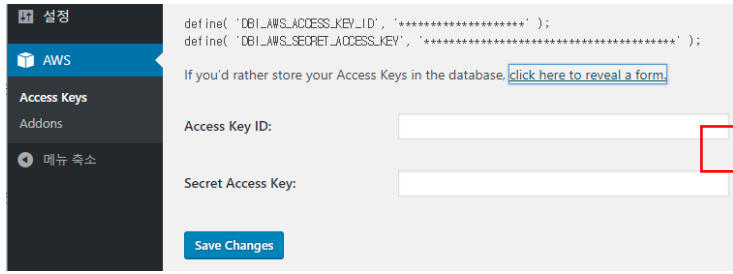
DB 관리자 패스워드

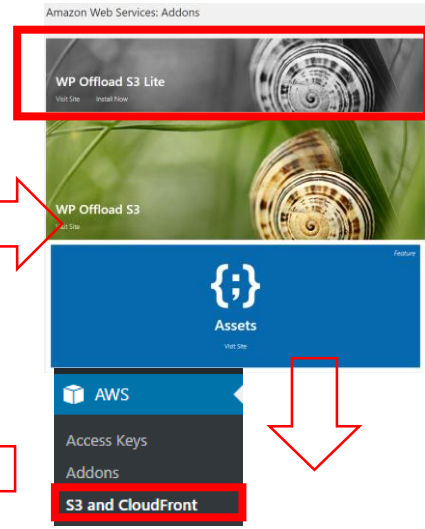
RDS 도메인 주소

1. 퍼블릭 서브넷의 Bastion 서버에 SSH 접속
2. 프라이빗 서브넷의 웹서버에 SSH 접속
3. 브라우저에서 http://localhost:80

WP Offload 설치/활성화

S3FullAccess 권한을 갖는 IAM user를 생성하고 키 입력





워드프레스에서 글과 그림을 upload하고 그 미디어 파일이 S3에 저장된 것을 확인한다.

생성한 S3 버킷이름 입력

Elastic Load Balancer

ELB 생성

로드 밸런서 유형 선택

탄력적 로드 밸런싱은 다음 세 유형의 로드 밸런서를 지원합니다 - 애플리케이션 로드 밸런서, 네트워크 로드 밸런서(신규) 및 클래식 로드 밸런서. 요구 사항을 충족하는 로드 밸런서 유형을 선택하십시오. 내게 적합한 로드 밸런서에 대해 자세히 알아보십시오.

애플리케이션 로드 밸런서

HTTP
HTTPS

생성

HTTP 및 HTTPS 트래픽을 사용하는 웹 애플리케이션에 대해 유연한 기능을 설정해야 할 경우 애플리케이션 로드 밸런서를 선택합니다. 요청 수준에서 작동하는 애플리케이션 로드 밸런서는 마이크로서비스 및 컨테이너를 비롯해 애플리케이션 아키텍처를 목표로 한 고급 라우팅, TLS 종료 및 표시 기능을 제공합니다.

자세히 알아보기 >

네트워크 로드 밸런서

TCP

생성

애플리케이션에 초고성능과 정적 IP 주소가 필요한 경우 네트워크 로드 밸런서를 선택합니다. 연결 수준에서 작동하는 네트워크 로드 밸런서는 초당 수백만 개의 요청을 처리하면서도 극히 낮은 지연 시간을 유지할 수 있습니다.

자세히 알아보기 >

클래식 로드 밸런서

이전 세대
HTTP, HTTPS 및 TCP용

생성

EC2-Classic 네트워크에서 구축된 기존 애플리케이션이 있는 경우 클래식 로드 밸런서를 선택합니다.

자세히 알아보기 >

단계 1: 로드 밸런서 정의

기본 구성

이 마법사는 새 로드 밸런서를 설정하는 방법을 안내합니다. 먼저 새 로드 밸런서를 다른 로드 밸런서와 구별할 수 있도록 고유한 이름을 지정하는 것부터 시작합니다. 또한 로드 밸런서에 포트 및 프로토콜도 구성해야 합니다. 클라이언트의 트래픽은 로드 밸런서 포트부터 EC2 인스턴스의 포트까지 라우팅됩니다. 기본적으로 로드 밸런서는 포트 80에서 표준 웹 서버로 구성되어 있습니다.

로드 밸런서 이름: u1-xelb
LB 내부 생성: vpc-0191cd67 (10.0.0.0/16) | u1-vpc
내부 로드 밸런서 생성: (자세히 알아보기)
고급 VPC 구성 활성화:
리스너 구성:

로드 밸런서 프로토콜	로드 밸런서 포트	인스턴스 프로토콜	인스턴스 포트	
HTTP	80	HTTP	80	⊗

추가

서브넷 선택

로드 밸런서가 트래픽을 라우팅할 각 가용 영역에 대한 서브넷을 선택해야 합니다. 인스턴스가 한 가용 영역에만 있는 경우, 서로 다른 가용 영역에 있는 서브넷을 2개 이상 선택하여 로드 밸런서의 가용성을 높이십시오.

VPC vpc-0191cd67 (10.0.0.0/16) | u1-vpc

사용 가능한 서브넷

작업	가용 영역	서브넷 ID	서브넷 CIDR	이름
⊕	us-west-2a	subnet-60fb9b06	10.0.2.0/24	u1-subnet-uw2a-private
⊕	us-west-2a	subnet-9c6c0ffa	10.0.5.0/24	u1-subnet-uw2a-rds
⊕	us-west-2b	subnet-cce76784	10.0.4.0/24	u1-subnet-uw2b-private
⊕	us-west-2b	subnet-fe63e3b6	10.0.6.0/24	u1-subnet-uw2b-rds

선택한 서브넷

작업	가용 영역	서브넷 ID	서브넷 CIDR	이름
⊖	us-west-2a	subnet-c5f797a3	10.0.1.0/24	u1-subnet-uw2a-public
⊖	us-west-2b	subnet-d2eb6b9a	10.0.3.0/24	u1-subnet-uw2b-public

취소 다음: 보안 그룹 할당

ELB 생성

단계 2: 보안 그룹 할당

VPC에서 탄력적 로드 밸런서를 사용하는 옵션을 선택하셨습니다. 그러므로 로드 밸런서에 보안 그룹을 할당할 수 있습니다. 이 로드 밸런서에 할당할 보안 그룹을 선택하십시오. 이 선택은 언제라도 변경할 수 있습니다.

보안 그룹 할당: ○ 새 보안 그룹 생성
● 기존 보안 그룹 선택

필터 VPC 보안 그룹

	보안 그룹 ID	이름	설명	작업
☐	sg-35204a48	default	default VPC security group	새로 복사
☐	sg-fb532686	u1-vpc-bastion	u1-vpc bastion host	새로 복사
☐	sg-fd502580	u1-vpc-rdstier	u1-vpc RDS tier	새로 복사
☐	sg-6056231d	u1-vpc-webtier	u1-vpc Web Tier	새로 복사
☑	sg-0a532677	u1-vpc-xelb	u1-vpc external ELB	새로 복사

취소 이전 다음: 보안 설정 구성

단계 6: 태그 추가

리소스에 태그를 추가하면 리소스를 정리하고 식별하는 데 도움이 됩니다.

태그는 대소문자를 구별하는 키-값 페어로 이루어져 있습니다. 예를 들어 키가 Name이고 값이 Webserver인 태그를 정의할 수 있습니다. Amazon EC2 리소스 태그 지정에 대하여 자세히 알아보기.

키	값	
Name	u1-xelb	⊗

태그 생성

취소 이전 검토 및 생성

단계 4: 상태 검사 구성

로드 밸런서는 자동으로 EC2 인스턴스에서 상태 검사를 수행하며 상태 검사를 통과하는 인스턴스로만 트래픽을 라우팅합니다. 상태 검사에 실패하는 인스턴스는 자동으로 로드 밸런서에서 제거됩니다. 요구 사항에 맞게 상태 검사를 사용자 지정하십시오.

Ping 프로토콜 TCP
Ping 포트 80

고급 세부 정보

응답 시간 초과 5 초
간격 30 초
비정상 임계값 2
정상 임계 값 10

취소 이전 다음: EC2 인스턴스 추가

단계 5: EC2 인스턴스 추가

아래 표에는 모든 실행 중인 EC2 인스턴스 목록이 있습니다. 현재 로드 밸런서에 인스턴스를 추가하려면 선택 열에서 확인란을 선택하십시오.

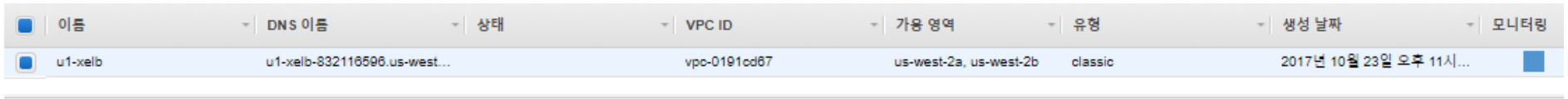
VPC vpc-0191cd67 (10.0.0.0/16) | u1-vpc

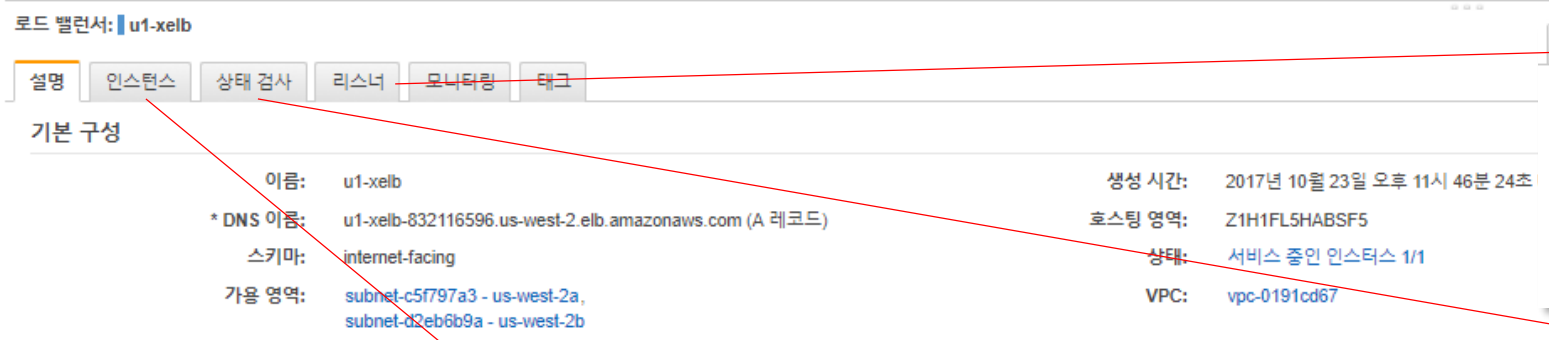
	인스턴스	이름	상태	보안 그룹	영역	서브넷 ID	서브넷 CIDR
☐	i-0a5e0b47cc78600fe	u1-subnet-uw2a-public-ec2	running	u1-vpc-bastion	us-west-2a	subnet-c5f797a3	10.0.1.0/24
☑	i-0100beff4d2a01c7e	u1-subnet-uw2a-private-ec2	running	u1-vpc-webtier	us-west-2a	subnet-60fb9b06	10.0.2.0/24

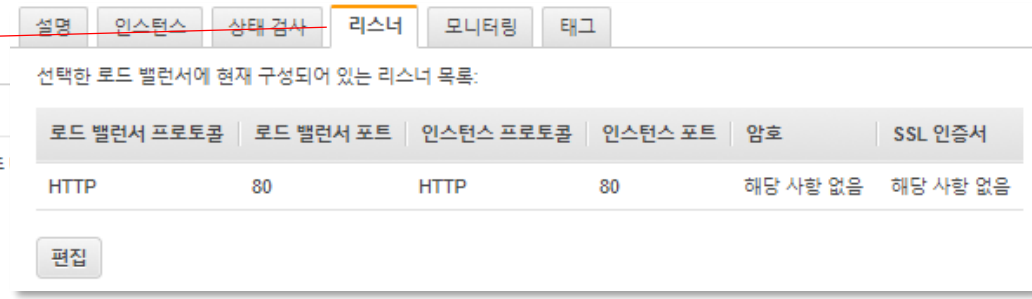
가용 영역 배포
us-west-2a 내 인스턴스 1개

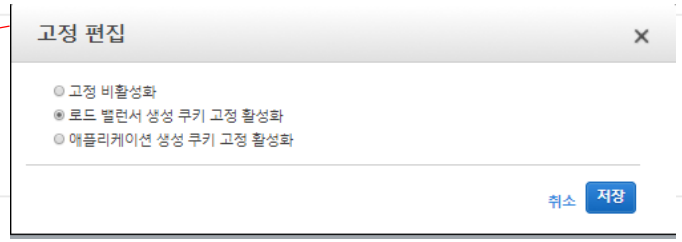
☑ 교차 영역 로드 밸런싱 활성화
☑ 연결 드레이닝 활성화 300 초

ELB









웹브라우저를 통해 ELB의 DNS 주소로 정상적 접근이 불가능함.

WordPress 설정에서 WordPress 주소와 사이트 주소를 localhost:8080에서 ELB DNS로 변경해야 함.

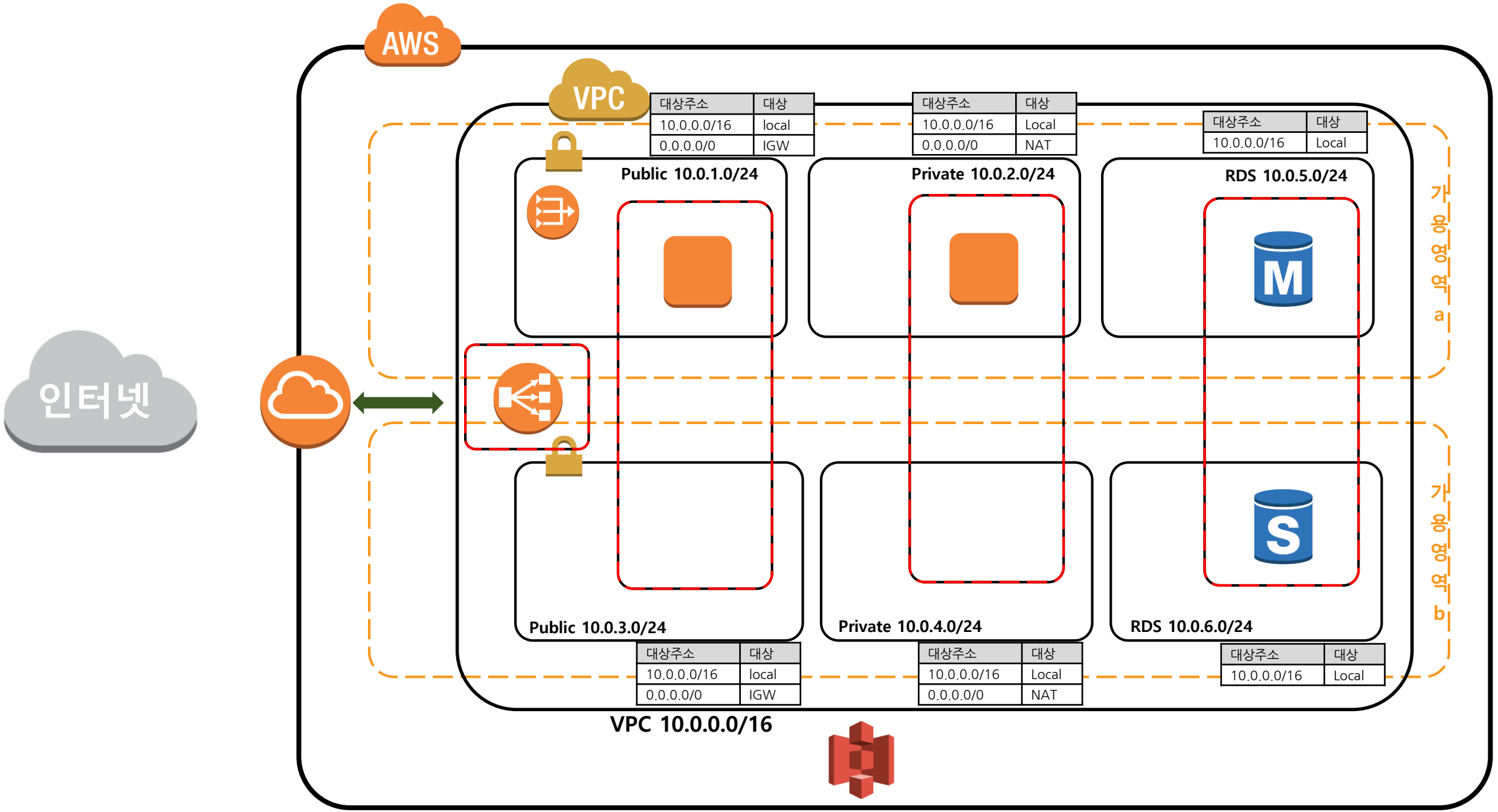
(뒤의 ELB 설정:Web)

이후에도 정상적으로 접근이 되지 않는다면

ELB 인스턴스탭에서 인스턴스 Status값이 In Service인지 확인,

만약 아니면, ELB와 EC2 구간의 방화벽 규칙확인

* LoadBalancer와 연결된 IP 주소 집합은 시간 경과에 따라 바뀔 수 있으므로 특정 IP 주소를 사용하여 "A" 레코드를 생성하면 안 됩니다. 탄력적 로드 밸런싱 서비스가 생성한 이름 대신 로드 밸런서에 대한 친숙한 DNS 이름을 사용하려면 LoadBalancer DNS 이름에 대한 CNAME 레코드를 생성하거나, Amazon Route 53를 사용하여 호스팅 영역을 생성해야 합니다. 자세한 내용은 탄력적 로드 밸런싱에서 도메인 이름 사용을 참조하십시오.


AWS
VPC
인터넷
대상주소 | 대상
10.0.0.0/16 | local
0.0.0.0/0 | IGW
대상주소 | 대상
10.0.0.0/16 | Local
0.0.0.0/0 | NAT
대상주소 | 대상
10.0.0.0/16 | Local
Public 10.0.1.0/24
Private 10.0.2.0/24
RDS 10.0.5.0/24
M
가용영역 a
Public 10.0.3.0/24
Private 10.0.4.0/24
RDS 10.0.6.0/24
S
가용영역 b
대상주소 | 대상
10.0.0.0/16 | local
0.0.0.0/0 | IGW
대상주소 | 대상
10.0.0.0/16 | Local
0.0.0.0/0 | NAT
대상주소 | 대상
10.0.0.0/16 | Local
VPC 10.0.0.0/16

오레곤 리전

ELB 실습의 비용 계산

ELB 가동 시간, ELB에서 처리한 데이터 량