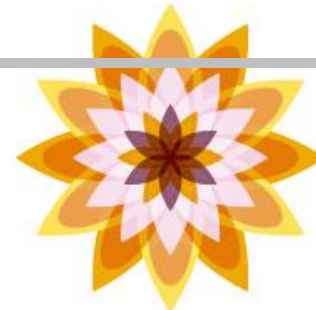
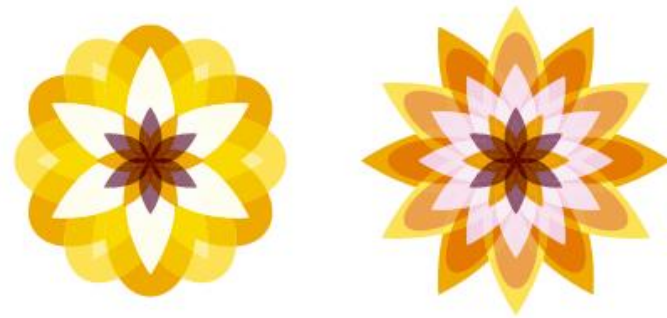


Chapter 06

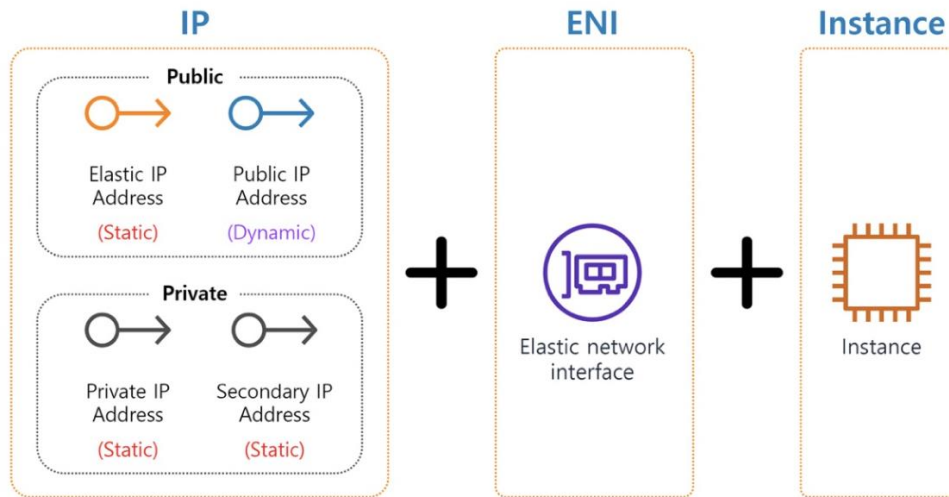
컴퓨팅 서비스 활용



1. 인스턴스의 네트워킹 패턴

■ 인스턴스 기본 통신 요건

- 인스턴스가 VPC상에서 통신하려면 컴퓨팅 기본 3요소가 결합돼야 한다.
- 그림은 인스턴스가 VPC 상에서 통신하기 위한 최소 결합 요건을 나타낸다.



- IP에서 정적 퍼블릭 IP를 탄력적 IP(Elastic IP), 동적Dynamic 퍼블릭 IP는 퍼블릭 IP(Public IP)라 한다.
- 프라이빗 IP(Private IP)는 정적 IP만 존재하며 기본 프라이빗 IP와 보조 프라이빗 IP 두 종류가 있다.

1. 인스턴스의 네트워킹 패턴

■ 인스턴스 기본 통신 요건

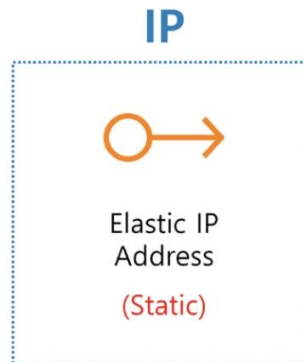
- ENI는 기본 프라이빗 IP 1개가 반드시 연결돼 있고 1개 이상의 보조 프라이빗 IP를 추가 할당할 수 있다.
- 탄력적 IP와 퍼블릭 IP도 필요할 때만 사용한다.
- IP와ENI, 그리고 인스턴스가 결합하면 VPC 위에서 트래픽 전송을 위한 준비가 완료된 것이다.
- 인스턴스 이외 다른 VPC 서비스를 사용한다면 해당 서비스를 인스턴스 자리로 대체하면 된다.
- 인스턴스는 생성 완료 시점에 이미 3가지 요건을 모두 갖추고 있다.
- 그러므로 인스턴스 아이콘만 있어도 ENI와 IP가 연결된 상태로 봐야 한다.

1. 인스턴스의 네트워킹 패턴

■ 컴퓨팅 기본 3요소의 독립 형태

■ IP

- 4가지 IP(퍼블릭 IP, 탄력적 IP, 기본 프라이빗 IP, 보조 프라이빗 IP) 중 탄력적 IP만 그 무엇과도 연결되지 않은 독립 상태로 존재할 수 있다.



- 반면 퍼블릭 IP와 프라이빗 IP는 ENI를 반드시 동반해야 한다.
- 프라이빗 IP의 생성과 소멸은 ENI의 수명 주기와 함께 한다.
- ENI가 소멸되면 프라이빗 IP도 함께 사라진다.
- 퍼블릭 IP는 ENI뿐만 아니라 인스턴스와 같은 컴퓨팅 서비스가 반드시 필요하다.
- 퍼블릭 IP는 탄력적 IP처럼 Amazon IPv4 Pool에서 할당하지만 계정이 마음대로 보유할 수 없고 인터페이스 작업과 형태에 따라 기존 IP를 유지하기도 하고 다른 IP로 변경되기도 한다.

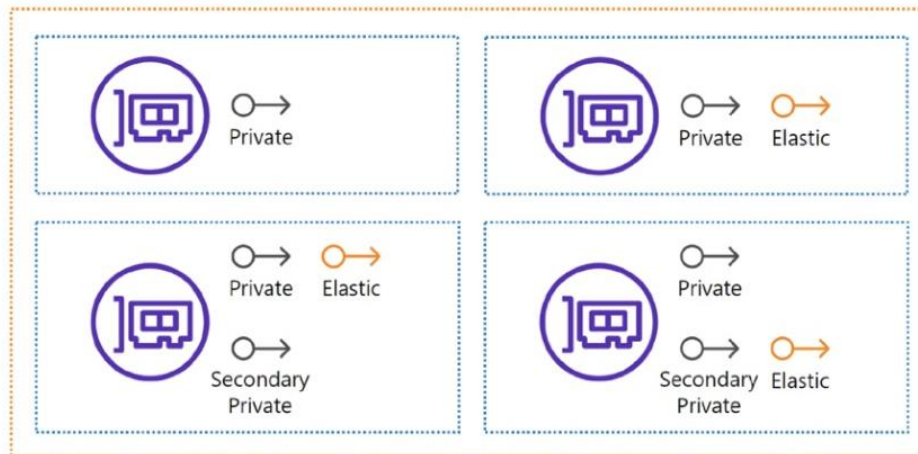
1. 인스턴스의 네트워킹 패턴

■ 컴퓨팅 기본 3요소의 독립 형태

■ ENI

- ENI는 그림처럼 기본 프라이빗 IP가 반드시 설정돼 있어야 한다.
- ENI와 기본 프라이빗 IP는 1 : 1 관계를 유지한다.

ENI



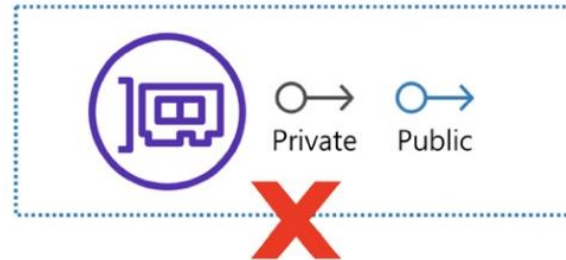
- 탄력적 IP는 프라이빗 IP와 쌍을 이룬다.
- 탄력적 IP를 연결하는 대상은 사실 ENI가 아닌 ENI에 할당된 프라이빗 IP다.
- 프라이빗 IP 종류(기본, 보조)와 무관하게 탄력적 IP를 연결할 수 있다.

1. 인스턴스의 네트워킹 패턴

■ 컴퓨팅 기본 3요소의 독립 형태

■ ENI

- 퍼블릭 IP는 ENI뿐만 아니라 인스턴스와 같은 컴퓨팅 서비스가 반드시 필요하다.
- 그러므로 그림처럼 독립 ENI에 할당할 수 없다.



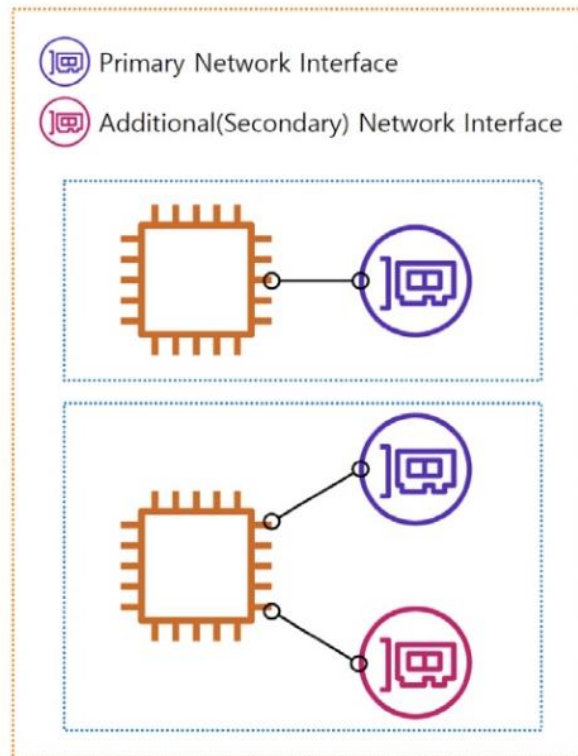
1. 인스턴스의 네트워킹 패턴

■ 컴퓨팅 기본 3요소의 독립 형태

■ 인스턴스

- 인스턴스는 그림처럼 단 1개의 기본 ENI가 연결됐거나 그 외 추가 ENI가 다수 연결된 형태일 수 있다.
- 기본ENI는 인스턴스 생성 즉시 연결되며 오직 1개만 존재한다.
- 사용자가 추가한 ENI는 분리할 수 있다.

Instance



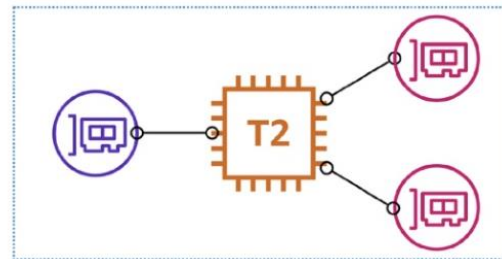
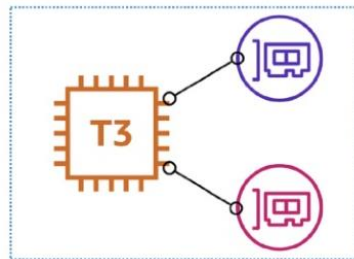
1. 인스턴스의 네트워킹 패턴

■ 인스턴스 유형별 ENI와 프라이빗 IP 최대 개수

- 다음 표는 인스턴스 유형별 연결 가능한 최대 ENI 수와 ENI당 프라이빗 IP 수가 정리된 표의 일부다.

인스턴스 유형	최대 네트워크 인터페이스 수	인터페이스당 프라이빗 IPv4 주소 수	인터페이스당 IPv6 주소 수
t2.micro	2	2	2
t2.small	3	4	4
t2.medium	3	6	6
t2.large	3	12	12
t2.xlarge	3	15	15
t2.2xlarge	3	15	15
t3.nano	2	2	2

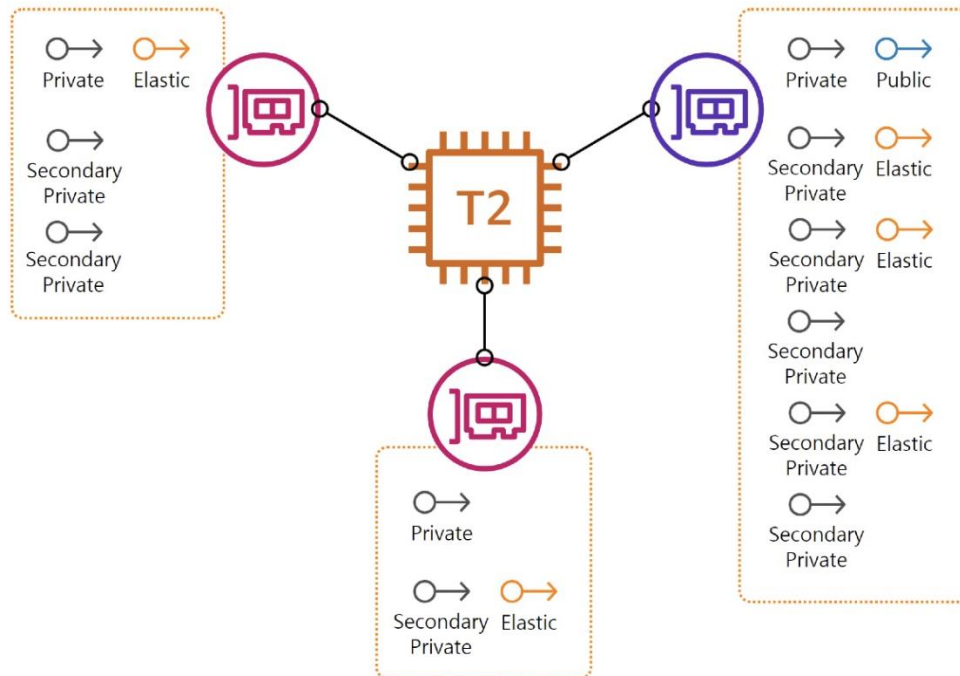
- t3.nano 유형을 사용하면 최대 2개의 ENI를 연결할 수 있으므로 왼쪽 그림처럼 기본 ENI에 추가 ENI 하나만 더 연결할 수 있다.



1. 인스턴스의 네트워킹 패턴

■ 인스턴스 유형별 ENI와 프라이빗 IP 최대 개수

- 그림은 t2.medium 유형 인스턴스에 최대 3개 ENI를 연결한 모습이다.
- 특히 기본 ENI(보라색)는 추가 ENI(자주색)가 절대 소유할 수 없는 퍼블릭 IP가 할당돼 있다.
- ENI마다 프라이빗 IP를 6개까지 할당할 수 있으므로, 기본 프라이빗 IP 1개를 제외하면 ENI마다 최대 5개 보조 프라이빗 IP를 할당할 수 있다.
- 또한 탄력 적 IP는 프라이빗 IP와 한 쌍을 이룬다.
- 따라서 ENI에 2개 이상의 탄력적 IP도 연결할 수 있다.



1. 인스턴스의 네트워킹 패턴

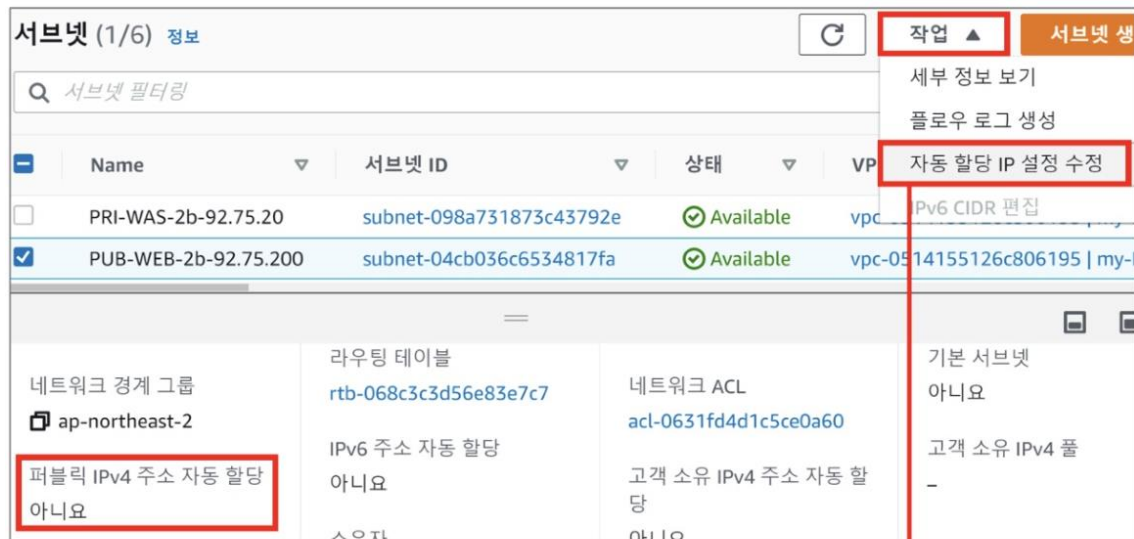
■ 퍼블릭 IP 자동 할당

- 인스턴스 생성 시점에 퍼블릭 IP를 동시에 소유하는 방법은 동적 퍼블릭 IP를 할당하는 방법뿐이다.
- 탄력적 IP는 인스턴스가 생성된 이후에만 연결할 수 있다.
- 퍼블릭 IP 자동 할당 옵션의 기능은 다음과 같다.
 - 활성화(able)는 인스턴스의 기본 ENI에 퍼블릭 IP를 할당한다.
 - 비활성화(disable)는 퍼블릭 IP를 할당하지 않는다.
 - 서브넷 사용 설정(Use subnet setting)은 서브넷 설정값에 따라 퍼블릭 IP 할당 여부를 결정한다.

1. 인스턴스의 네트워킹 패턴

■ 퍼블릭 IP 자동 할당

- 서브넷에는 그림에 보이는 퍼블릭 IPv4 주소 자동 할당 옵션이 있다.



서브넷 (1/6) 정보

서브넷 필터링

Name	서브넷 ID	상태	VP
PRI-WAS-2b-92.75.20	subnet-098a731873c43792e	Available	vpc-
PUB-WEB-2b-92.75.200	subnet-04cb036c6534817fa	Available	vpc-0514155126c806195 my-

네트워크 경계 그룹
ap-northeast-2

라우팅 테이블
rtb-068c3c3d56e83e7c7

네트워크 ACL
acl-0631fd4d1c5ce0a60

기본 서브넷
아니요

고객 소유 IPv4 풀
-

퍼블릭 IPv4 주소 자동 할당
아니요

IPv6 주소 자동 할당
아니요

고객 소유 IPv4 주소 자동 할당
아니요



퍼블릭 IP 자동 할당

서브넷 사용 설정(활성화)

서브넷 사용 설정(활성화)

배치 그룹

활성화

비활성화



설정

서브넷 ID
subnet-04cb036c6534817fa

자동 할당 IPv4 정보

☒ 퍼블릭 IPv4 주소 자동 할당 활성화

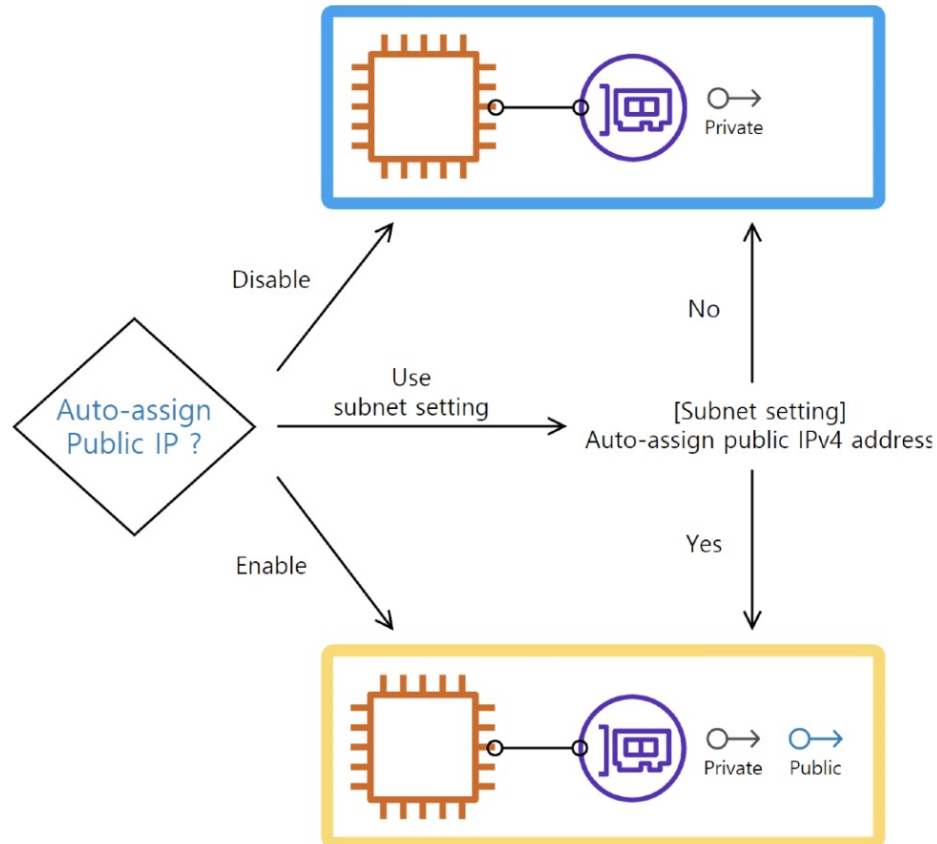
고객 소유 IPv4 주소 자동 할당 정보

☐ 고객 소유 IPv4 주소 자동 할당 활성화
고객 소유 풀을 찾을 수 없어 옵션이 비활성화되었습니다.

1. 인스턴스의 네트워킹 패턴

■ 퍼블릭 IP 자동 할당

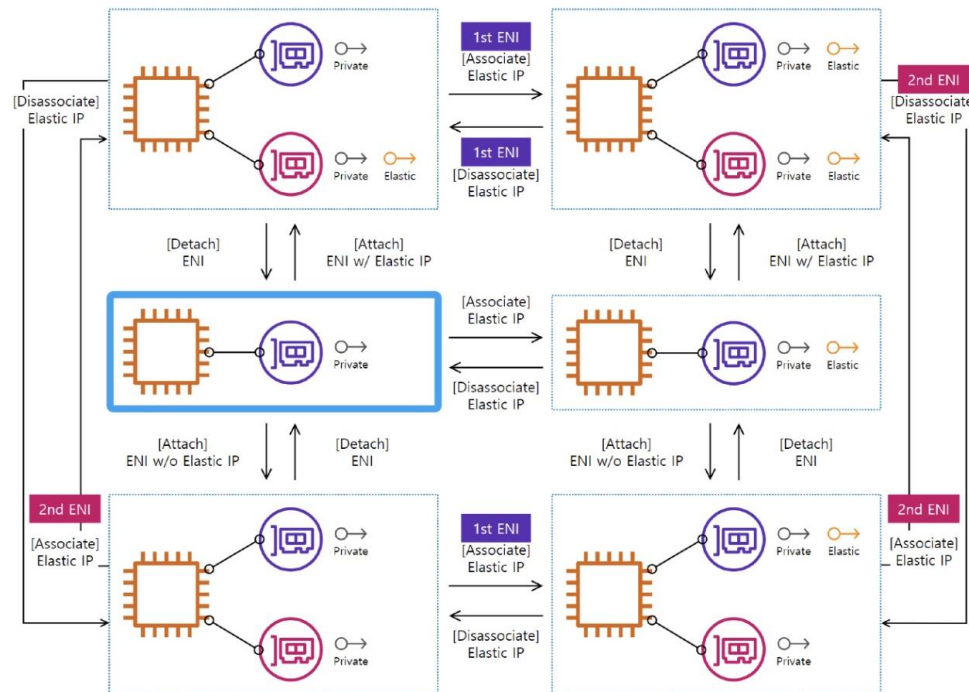
- 퍼블릭 서브넷은 인터넷 접속용으로 사용할 것이다.
- 그러나 퍼블릭 서브넷의 모든 인스턴스가 반드시 퍼블릭 IP를 사용할 의무는 없으므로, 퍼블릭 IPv4 주소자동 할당 옵션은 사용하지 않는 게 바람직하다.
- 위 과정을 그림처럼 순서도로 표현했다.



1. 인스턴스의 네트워킹 패턴

■ ENI 연결과 탄력적 IP 할당

- 탄력적 IP는 다음 3가지 방법으로 인스턴스에 연결할 수 있다.
 - 인스턴스에 직접 연결 (Associate) 하는 방법
 - 인스턴스 ID와 인스턴스가 소유한 프라이빗 IP를 지정한다.
 - 인스턴스가 사용하는 ENI에 직접 연결 (Associate) 하는 방법
 - ENI와 ENI가 소유한 프라이빗 IP를 지정한다.
 - 탄력적 IP를 ENI에 할당한 뒤, 해당 ENI를 인스턴스에 연결(Attach)하는 방법
- 그림은 퍼블릭 IP가 없는 인스턴스의 여러 형태를 보여준다

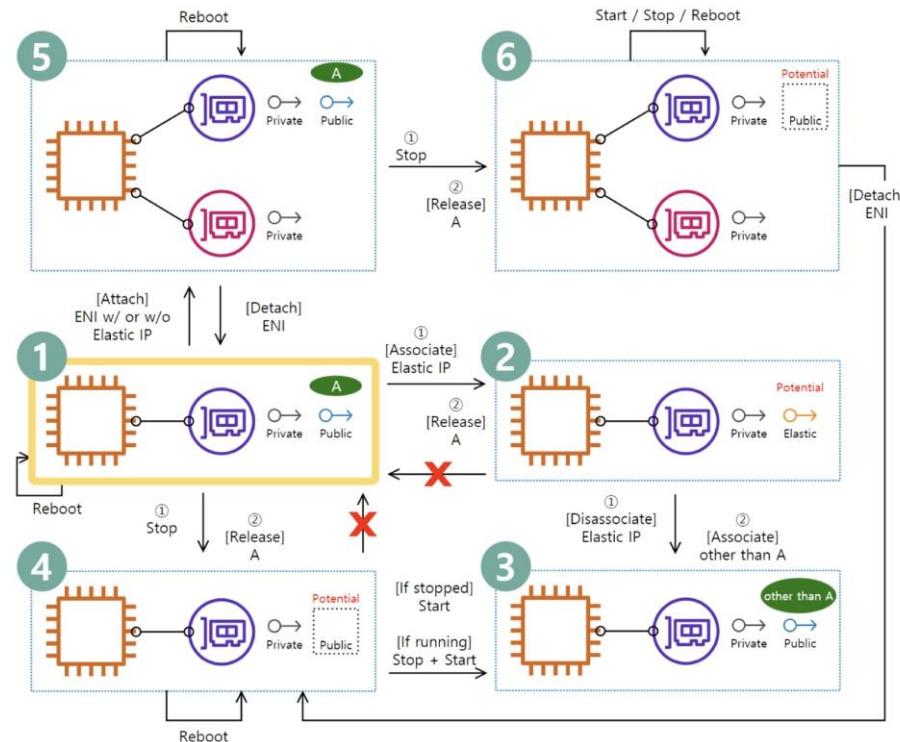


1. 인스턴스의 네트워킹 패턴

■ ENI 연결과 탄력적 IP 할당

■ 동적 퍼블릭 IP가 없는 인스턴스의 성질

- 생성 시점부터 동적 퍼블릭 IP가 없었던 인스턴스는, 탄력적 IP 작업(연결/해제)과 ENI 작업(연결/분리)이 자유롭다. 단, 기본 ENI 연결/분리는 불가능하다.
- 탄력적 IP는 프라이빗 IP와 쌍을 이루므로 모든 프라이빗 IP(기본, 보조)에 연결할 수 있다. 다시 말해 ENI에 기본 프라이빗 IP와 보조 프라이빗 IP가 다수 할당돼 있으면 하나의 ENI에 2개 이상의 탄력적 IP를 연결할 수 있다.
- 위 2개 규칙은 인스턴스 상태(Running, Stopped)와 무관하며, ENI가 3개 이상일 때도 똑같이 적용된다.



1. 인스턴스의 네트워킹 패턴

■ 결코 뗄 수 없는 꼬리표: 동적 퍼블릭 IP

■ 동적 퍼블릭 IP를 보유한 인스턴스의 성질

- 인스턴스를 재부팅(Reboot, ①~⑥ 각 상태에서)하면 퍼블릭 IP 보유 여부와 무관하게 기존 상태를 유지한다.
- 인스턴스를 중지(Stop, ①→④)하면 현재 보유한 퍼블릭 IP를 Amazon IPv4 Pool로 반환(Release)한다.
- 이미 반환된 IP는 다시 살릴(②→① 또는 ④→①) 수 없다.
- 퍼블릭 IP를 반환한 인스턴스(④)는 언제나 새로운 퍼블릭 IP를 할당받을 준비 태세(Potential)를 갖추고 있다. 그러므로 ENI에 퍼블릭 IP가 없다고 해서 모두 같은 상태로 볼 수 없다.



- 실행 중인 인스턴스에 ENI(탄력적 IP 연결 여부와 무관)를 추가 연결(①→⑤)해도 기존 퍼블릭 IP를 잃지 않는다. 재부팅 이후라도 현재 상태를 유지한다. ENI를 분리(⑤→①)해도 마찬가지다.
- 추가 ENI를 연결한 상태에서 인스턴스를 중지(Stop, ⑤→⑥)하면 ①→④ 과정처럼 퍼블릭 IP가 릴리스된다.
- 그러나 이 상태에서 어떤 작업(Start, Stop, Reboot)을 해도 새로운 퍼블릭 IP를 할당받지 못한다.
- 이유는 다음과 같다.
 - 인스턴스가 중지된(Stopped) 상태에서 부팅(Start, ④→③ 또는 ⑥→⑥)할 때 Amazon IPv4 Pool에서 새로운 IP를 할당받는다. 이 때 2가지를 확인한다.
 - 1) 인스턴스가 기본 ENI 이외 추가 연결된 ENI가 있는지 확인한다. 있다면(⑥) 퍼블릭 IP를 할당받지 않는다.
 - 2) 추가 연결된 ENI가 없다면(④) 기본 ENI에 탄력적 IP가 연결됐는지 확인한다. 연결되지 않았다면 새로운 퍼블릭 IP를 할당(③)받는다.

1. 인스턴스의 네트워킹 패턴

■ 결코 뺄 수 없는 꼬리표: 동적 퍼블릭 IP

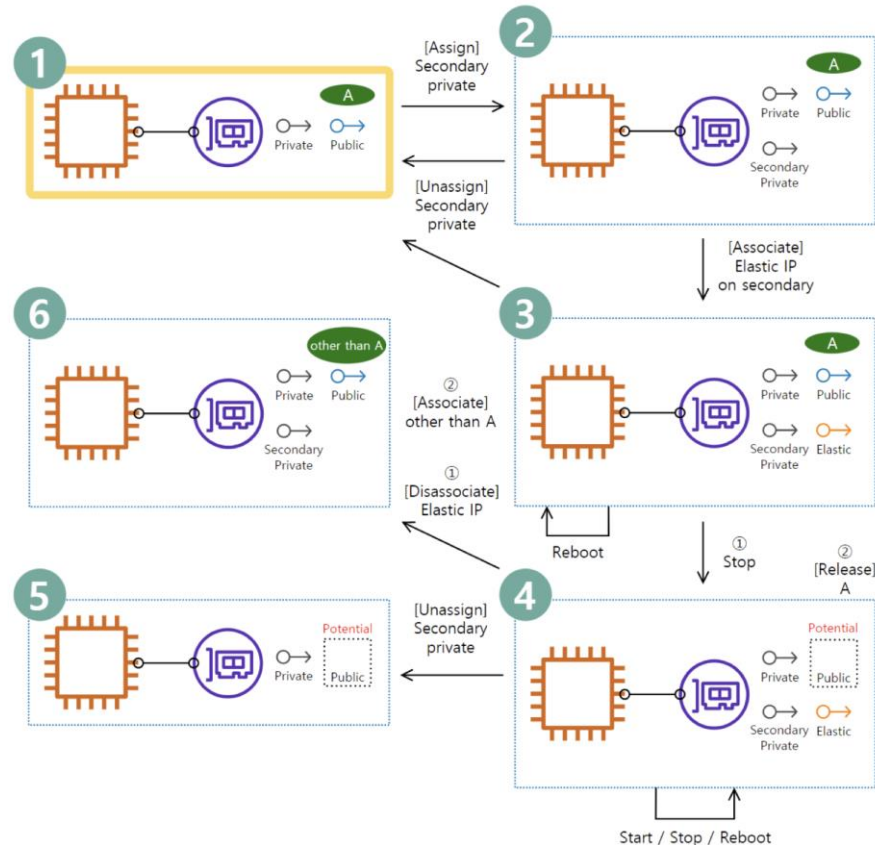
■ 동적 퍼블릭 IP를 보유한 인스턴스의 성질

- 인스턴스에서 ENI를 분리(⑥ → ④)한다고 해서 퍼블릭 IP를 바로 할당받진 못한다. 그러나 중지한후 부팅(Stop + Start, ④ → ③)하면 새로운 퍼블릭 IP를 할당받을 수 있다.
 - 퍼블릭 IP가 할당된 ENI에 탄력적 IP를 연결(① → ②)하면 기존 퍼블릭 IP(A)는 릴리스된다. 반대로 이 탄력적 IP를 해제(② → ③)하면 새로운 퍼블릭 IP(A 이외)를 할당받는다.
-
- 이처럼 인스턴스 생성 시 퍼블릭 IP를 할당받으면 그 꼬리표는 절대 뺄 수 없다.
 - 그러므로 인터넷 사용 여부가 확실치 않은 인스턴스는 생성 시 퍼블릭 IP를 할당하면 안된다.
 - 생성 시점엔 프라이빗 IP만 보유해야 하며, 인터넷 접속이 필요한 것으로 결정되면 NAT 게이트웨이 나 탄력적 IP를 사용하는 것이 바람직하다.

1. 인스턴스의 네트워킹 패턴

■ 보조 프라이빗 IP에 탄력적 IP 할당

- 보조 프라이빗 IP에도 탄력적 IP를 연결할 수 있다.
- 또 보조 프라이빗 IP에서 탄력적 IP만 다시 해제할 순 있지만, 탄력적 IP만유지한채 보조 프라이빗 IP만 해제할 수는 없다.
- 그림은 퍼블릭 IP를 보유한 인스턴스에 보조 프라이빗 IP 또는 탄력적 IP 관련 작업을 수행한 모습이 다.



1. 인스턴스의 네트워킹 패턴

■ 보조 프라이빗 IP에 탄력적 IP 할당

■ 보조 프라이빗 IP를 보유한 퍼블릭 인스턴스의 성질

- 보조 프라이빗 IP를 할당(①→②)하고 해제(②→①)하는 동안 퍼블릭 IP는 그대로 유지된다.
- 보조 프라이빗 IP에 탄력적 IP를 연결(②→③)한 뒤 중지(③→④)하지 않는 한 기존 퍼블릭 IP가 변경되거나 릴리스되지 않는다. 보조 프라이빗 IP를 해제(③→①)하면 홀로 설 수 없는 탄력적 IP는 보조 프라이빗 IP에서 분리와 동시에 해제된다.
- 잠재적 퍼블릭 인스턴스에 탄력적 IP가 있으면(④) 어떤 작업(Start, Stop, Reboot)을 가해도 퍼블릭 IP를 살릴 수 없다. 탄력적 IP와 쌍을 이루는 보조 프라이빗 IP 해제(④→⑤)작업은 인스턴스 입장에서 탄력적 IP 해제가 아닌 보조 프라이빗 IP 해제로 인식할 뿐이다.
- 보조 프라이빗 IP에 탄력적 IP를 해제(④→⑥)하면 새로운 퍼블릭 IP를 할당받는다.

1. 인스턴스의 네트워킹 패턴

■ 실습. 인스턴스에 ENI 연결/분리, 신규 퍼블릭 IP 확인

- 인스턴스생성 예제를 참고해 인스턴스를 생성한다.
- 생성된 인스턴스의 기본 ENI에 연결된 기본 프라이빗 IP와 퍼블릭 IP를 확인한다.
- 네트워킹 탭의 네트워크 인터페이스 항목을 선택하면 인스턴스에 연결된 기본 ENI의 정보가 나타난다.
- 인터페이스 ID를 클릭해 네트워크 인터페이스 메뉴로 바로 이동한다.

인스턴스 ID: i-0b379af0a6646baba

가용 영역: ap-northeast-2a

퍼블릭 IPv4 주소: 3.34.53.50

프라이빗 IP 주소: 92.75.100.15

보안 그룹 이름: launch-wizard-1

인스턴스: i-0b379af0a6646baba

세부 정보 | 보안 | **네트워킹** | 스토리지 | 상태 검사 | 모니터링 | 태그

▶ 네트워킹 세부 정보 정보

▶ **네트워크 인터페이스** 정보

▶ 탄력적 IP 주소 정보

인터페이스 ID	설명	퍼블릭 IPv4 주소	프라이빗 IPv4 주소
eni-0b8937b319865230e	Primary network interface	3.34.53.50	92.75.100.15

1. 인스턴스의 네트워킹 패턴

■ 실습. 인스턴스에 ENI 연결/분리, 신규 퍼블릭 IP 확인

- 인스턴스에 연결된 기본 ENI를 확인할 수 있다.
- 우측 상단의 네트워크 인터페이스 생성 버튼을 클릭한다.

네트워크 인터페이스 (1) 정보				
<div>네트워크 인터페이스 필터링</div>				
네트워크 인터페이스 ID ▼	가용 영역 ▼	인스턴스 ID ▼	퍼블릭 IPv4 주소 ▼	기본 프라이빗 IPv4 주소
eni-0b8937b319865230e	ap-northeast-2a	i-0b379af0a6646baba	3.34.53.50	92.75.100.15

1. 인스턴스의 네트워킹 패턴

■ 실습. 인스턴스에 ENI 연결/분리, 신규 퍼블릭 IP 확인

- 서브넷을 선택하고 프라이빗 IP 주소와 보안 그룹을 선택한 뒤, 우측 하단의 네트워크 인터페이스 생성 버튼을 클릭한다.

네트워크 인터페이스 생성

탄력적 네트워크 인터페이스는 가상 네트워크 카드를 나타내는 VPC의 논리적 네트워킹 구성 요소입니다.

세부 정보 [정보](#)

Description - [선택 사항](#)
네트워크 인터페이스를 설명하는 이름입니다.

Additional ENI

서브넷
생성한 네트워크 인터페이스가 위치할 서브넷입니다.

세부 정보 [정보](#)

subnet-04cb036c6534817fa PUB-WEB-2b-92.75.200 소유자: 671559022704	ap-northeast-2b
subnet-0b985a2d487fd363c PRI-WAS-2a-92.75.10 소유자: 671559022704	ap-northeast-2a
subnet-0765bc7c7bd1b3b09 PUB-WEB-2a-92.75.100 소유자: 671559022704	ap-northeast-2a
subnet-0a8f690278a26e95f PRI-DB-2a-92.75.1 소유자: 671559022704	ap-northeast-2a

1. 인스턴스의 네트워킹 패턴

■ 실습. 인스턴스에 ENI 연결/분리, 신규 퍼블릭 IP 확인

- 목록에 새로운 ENI가 나타난다.
- ENI를 선택한 후 우측 상단 작업 > 연결 메뉴를 클릭한다.
- 연결할 인스턴스를 선택하고 연결 버튼을 클릭하면 연결이 완료된다.

네트워크 인터페이스 ID ▾	가용 영역 ▾	인스턴스 ID ▾	퍼블릭 IPv4 주소 ▾	기본 프라이빗 IPv4 주소
eni-0ecf29ad76350adae	ap-northeast-2a	-	-	92.75.10.245
eni-0b8937b319865230e	ap-northeast-2a	i-0b379af0a6646baba	3.34.53.50	92.75.100.15

네트워크 인터페이스 (1/2) 정보

작업 ▲

연결

분리

삭제

네트워크 인터페이스 ID ▾

eni-0ecf29ad76350adae

네트워크 인터페이스 연결

네트워크 인터페이스
eni-0ecf29ad76350adae



인스턴스
i-0b379af0a6646baba

취소 연결

1. 인스턴스의 네트워킹 패턴

■ 실습. 인스턴스에 ENI 연결/분리, 신규 퍼블릭 IP 확인

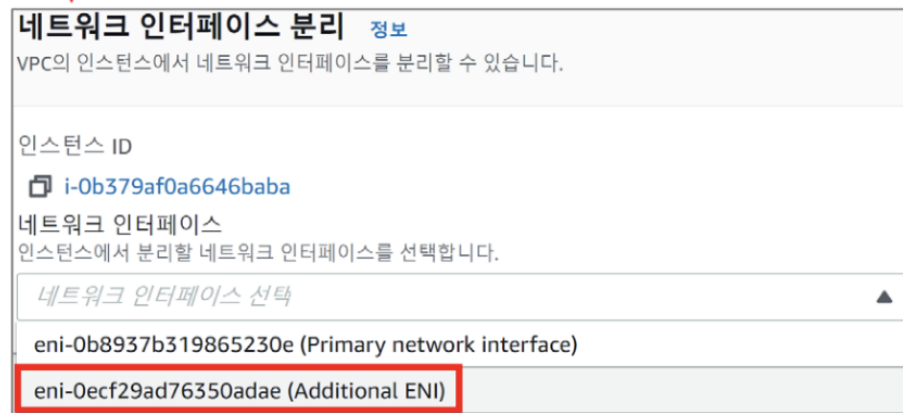
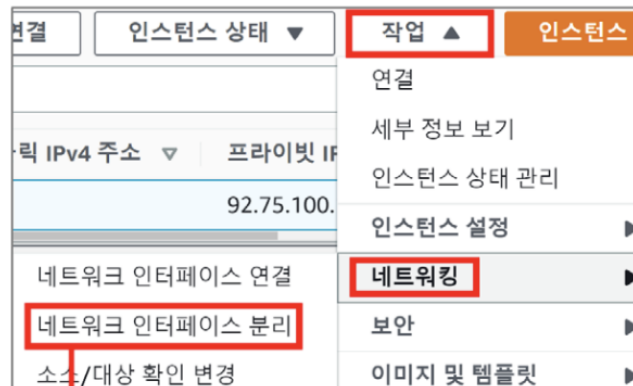
- 인스턴스를 중지하고 퍼블릭 IP를 확인한다.
- 퍼블릭 IP가 릴리스됐다.
- 인스턴스를 다시 시작해 퍼블릭 IP를 확인한다.
- 퍼블릭 IP를 여전히 할당받지 못하고 있다.

인스턴스 ID	가용 영역 ▼	퍼블릭 IPv4 주소 ▼	프라이빗 IP 주소 ▼	보안 그룹
i-0b379af0a6646baba	ap-northeast-2a	-	92.75.100.15	launch-
=				
인터페이스 ID	설명	퍼블릭 IPv4 주소	프라이빗 IPv4 주소	
 eni-0b8937b319865230e	Primary network interface	-	92.75.100.15	
 eni-0ecf29ad76350adae	Additional ENI	-	92.75.10.245	

1. 인스턴스의 네트워킹 패턴

■ 실습. 인스턴스에 ENI 연결/분리, 신규 퍼블릭 IP 확인

- 인스턴스 선택 > 작업 > 네트워킹 > 네트워크 인터페이스 분리를 선택해서 연결한 ENI를 다시 분리한다.
- 메뉴에서 네트워크 인터페이스를 선택하고 분리 버튼을 클릭한다.
- 이 상태에서도 퍼블릭 IP를 할당받지 못한다.



1. 인스턴스의 네트워킹 패턴

■ 실습. 인스턴스에 ENI 연결/분리, 신규 퍼블릭 IP 확인

- 인스턴스를 중지한 뒤 다시 시작한다.
- 기존 퍼블릭 IP와 다른 새로운 IP가 할당된 것을 확인할 수 있다.

인스턴스 ID	인스턴스 상태 ▼	퍼블릭 IPv4 주소 ▼	프라이빗 IP 주소 ▼	보안 그룹
i-0b379af0a6646baba	실행 중	3.35.231.51	92.75.100.15	launch-v
=				
인터페이스 ID	설명	퍼블릭 IPv4 주소	프라이빗 IPv4 주소	
eni-0b8937b319865230e	Primary network interface	3.35.231.51	92.75.100.15	

2. 컴퓨팅 서비스 응용 : RDS

■ VPC를 사용하는 데이터베이스의 종류

- 2022년 1월 현재, AWS는 9개 데이터베이스 서비스를 제공한다.

특징 DB 서비스	VPC 기반	RDS용 ENI	퍼블릭 액세스
· RDS	O	O	O
· Neptune · Amazon DocumentDB			X
· ElastiCache · Redis용 Amazon MemoryDB			
· DynamoDB · Amazon QLDB · Amazon Keyspaces · Amazon Timestream	X		

- 표를 보면 VPC 네트워킹을 사용하는 서비스는 5개(RDS, Neptune, DocumentDB, ElastiCache, Redis용 Amazon MemoryDB)임을 알 수 있다.
- 따라서 이들은 VPC 보안 통제 영역에 있다.
- 또한 이 중 3가지는 RDS용 ENI를 사용한다.

2. 컴퓨팅 서비스 응용 : RDS

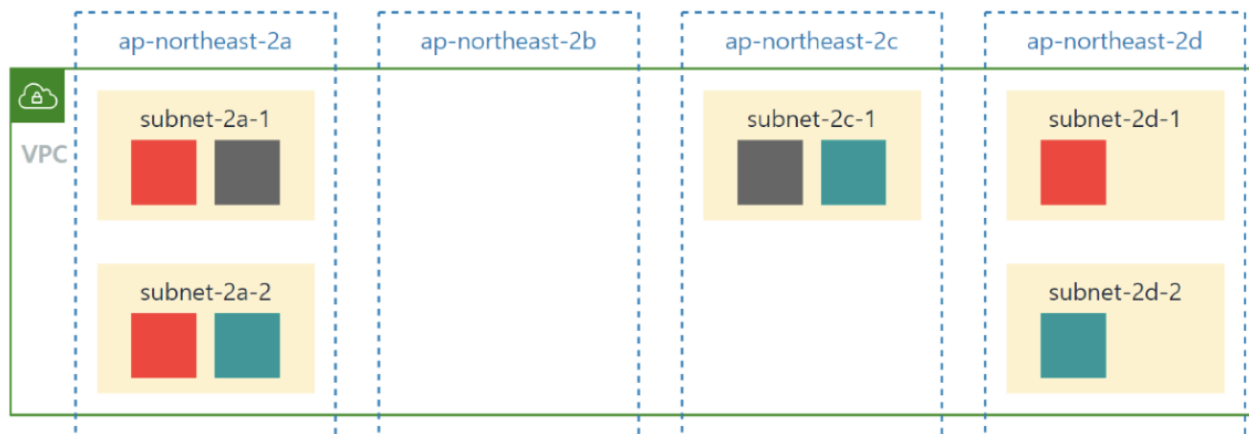
■ VPC를 사용하는 데이터베이스의 종류

- 인터넷에서 접속 가능한 퍼블릭 액세스 기능은 RDS에만 있다.
- 또 이 기능은 인스턴스 생성 이후라도 언제든지 켜고 끌 수 있으므로, 외부에서 RDS 인스턴스에 접속이 불필요하다면 반드시 프라이빗 서브넷에 생성해야 한다.
- 퍼블릭 액세스 옵션을 켜놔도 어차피 하나의 포트로만 접속할 수 있기 때문에 RDS가 사용하는 보안 그룹이나 네트워크 ACL을 광범위하게 허용해도 의미는 없다.
- 그러나 해당보안 그룹과 네트워크 ACL이 다른 서비스에 연결돼 있을 수도 있으므로 반드시 필요한 규칙만 등록해서 사용해야 한다.

2. 컴퓨팅 서비스 응용 : RDS

■ RDS 서브넷 그룹의 특징

- 서브넷 그룹은 말 그대로 서브넷의 모음이다.
- RDS를 생성하려면 서브넷 그룹 1개를 반드시 지정해야 한다.
- 서브넷 그룹은 RDS 인스턴스가 놓일 서브넷들의 집합이다.
- RDS 인스턴스가 한 가용 영역에서 서비스를 지속할 수 없으면 서브넷 그룹에 속한 다른 가용 영역에서 서비스를 지속한다.
- 그림은 RDS의 서브넷 그룹을 나타낸다.



2. 컴퓨팅 서비스 응용 : RDS

■ RDS 서브넷 그룹의 특징

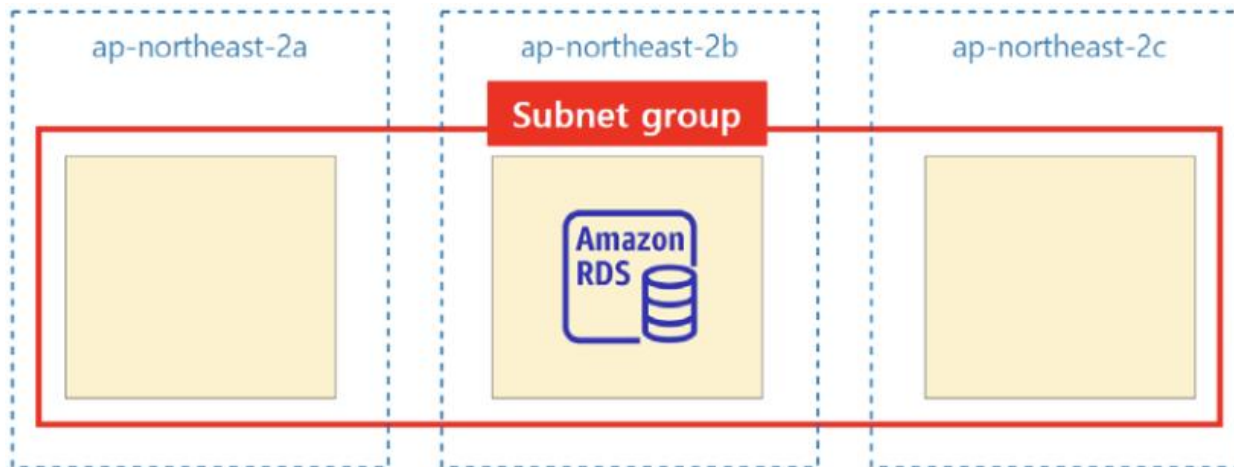
■ RDS 서브넷 그룹의 특징은 다음과 같다.

- 서브넷 그룹은 VPC에 종속되며, 최소 2개 이상의 가용 영역을 지정해야 한다.
- 모든 RDS는 생성 단계에서 서브넷 그룹을 지정해야 한다. 이는 엔진종류(Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, SQL Server)나 유형(프로비저닝 또는 서버리스)과 무관하다.
- 따라서 RDS 생성 전에 서브넷 그룹을 만들어 두어야 한다. 미리 준비한 서브넷 그룹이 없다면 RDS를 생성하면서 새 DB 서브넷 그룹 생성 옵션을 사용할 수도 있다.
- 그러나 선택한 VPC에 속한 서브넷이 1개 가용 영역 뿐이라면 RDS 생성에 실패한다. 다른 가용 영역에 서브넷을 새로 만들거나 새 VPC 생성과 새 DB 서브넷 그룹 생성 옵션을 사용해야 한다.
- 서브넷 그룹이 지정한 가용 영역의 모든 서브넷을 멤버로 지정할 수 있다.
- 리전의 모든 가용 영역을 포함하지 않아도 된다.
- A 서브넷 그룹이 포함하는 서브넷을 B 서브넷 그룹의 멤버로도 지정할 수 있다.
- 여러 RDS 인스턴스가 동일한 서브넷 그룹을 사용해도 된다.
- RDS 기본 인스턴스는 서브넷 그룹의 서브넷 멤버 중 한 곳에서 구동된다.
- 서브넷 그룹을 수정해 멤버 서브넷을 삭제 또는 추가할 수 있다. 그러나 RDS 사용 중에는 불가능하다.
- 서브넷 그룹의 멤버 서브넷을 서브넷 메뉴로도 삭제할 수 있다. 그러나 RDS 사용 중에는 불가능하다.

2. 컴퓨팅 서비스 응용 : RDS

■ RDS 서브넷 그룹의 역할

- RDS는 서브넷 그룹의 멤버(서브넷) 중 하나를 RDS 인스턴스 생성 위치로 선정한다.
- RDS 생성 단계에서 인스턴스를 구동할 특정 가용 영역을 선택했다면 그 가용 영역의 서브넷 중 한 곳에 인스턴스가 생성된다.
- 단, 해당 가용 영역에 서브넷이 2개 이상일 때 임의의 선택은 불가능하다.
- 반면 사용자가 가용 영역을 미지정하면 AWS는 서브넷 그룹이 포함하는 임의의 가용 영역을 선택하고 RDS 인스턴스를 생성한다.
- 그림은 3개 가용 영역의 서브넷을 멤버로 하는 서브넷 그룹을 나타낸다.



2. 컴퓨팅 서비스 응용 : RDS

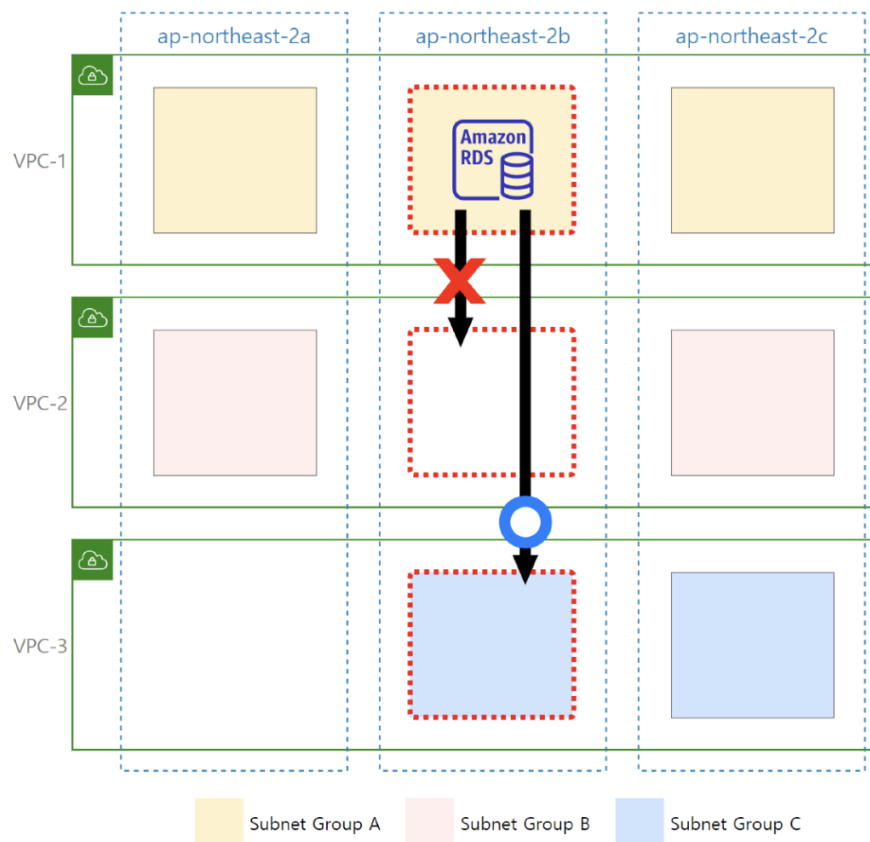
■ VPC 경계를 넘나드는 RDS : 서브넷 그룹 변경

- RDS는 가동 중에 서브넷 그룹을 변경할 수 있다.
- Amazon Aurora를 제외한 모든 엔진이 서브넷 그룹 변경을 지원한다.
- 서브넷 그룹의 변경 조건은 다음과 같다.
 - 단일 RDS 인스턴스만 서브넷 그룹 변경을 할 수 있다. 다중 AZ 인스턴스의 서브넷 그룹을 변경하려면 RDS를 단일화한 뒤 서브넷 그룹을 변경하고 다시 다중 AZ로 확장해야 한다.
 - 다른 VPC의 서브넷 그룹으로만 변경할 수 있다. 다시 말해 현재 RDS가 사용하는 VPC이 그 어떤 서브넷 그룹도 변경 대상으로 선택할 수 없다.
 - 현재 구동 중인 RDS 인스턴스의 가용 영역이, 변경 대상 서브넷 그룹에도 포함돼 있어야 한다.

2. 컴퓨팅 서비스 응용 : RDS

■ VPC 경계를 넘나드는 RDS : 서브넷 그룹 변경

- 그림은 RDS가 서브넷 그룹 변경을 시도하고 있다.
- 서울 리전(ap-northeast-2) 에 3개의 VPC가 생성돼 있고, 각 VPC마다 서브넷 그룹(A,B,C)이 있다.
- VPC-1의 RDS를 VPC-2나 VPC-3의 서브넷 그룹(B 또는 C)으로 변경을 시도해본다



2. 컴퓨팅 서비스 응용 : RDS

■ VPC 경계를 넘나드는 RDS : 서브넷 그룹 변경

- 한편 기존 RDS 인스턴스에 퍼블릭 액세스 옵션이 켜진 상태라면 AWS는 서브넷 변경 전 다음 조건을 추가로 확인한다.
 - 변경 대상 VPC에도 인터넷 게이트웨이가 연결돼 있어야 한다. 단, 서브넷 라우팅 타킷에 인터넷 게이트웨이 지정 여부까지 검사하진 않는다.
 - DNS 확인(DNS resolution), DNS 호스트이름(DNS hostnames)이 활성화Enable돼 있는지 확인한다.
- 위 조건을 만족하면 서브넷 그룹을 변경할 수 있다.

2. 컴퓨팅 서비스 응용 : RDS

■ 다중 AZ 배포

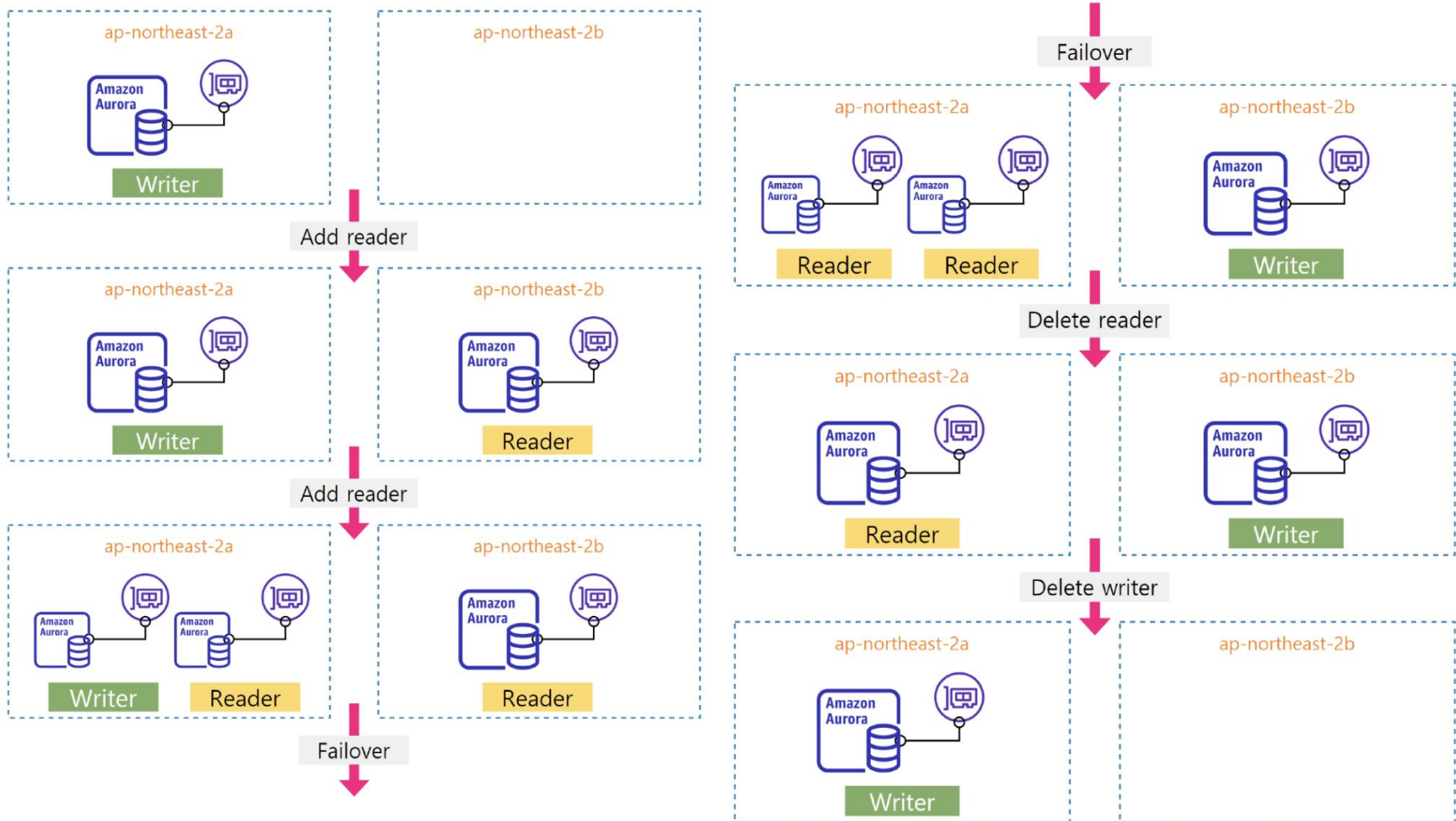
- RDS는 Aurora와 Aurora 이외의 엔진 유형(PostgreSQL, MySQL, MariaDB, Oracle Database, SQL Server)으로 구분한다.
- AWS가 제공하는 모든 RDS는 엔진 유형과 템플릿에 따라 방식의 차이는 있지만, 모두 다중 AZ를 사용해 서비스장애를 대비할 수 있다.
- 표는 RDS 인스턴스의 종류와 그 특징을 나타낸다.

인스턴스	접근성 (엔드포인트 여부)	RDS 엔진	
		Aurora	Aurora 이외
기본 인스턴스 (Primary db instance)	쓰기(W)+읽기(R) (엔드포인트 있음)	○	
읽기 노드 (Reader)	읽기(R) (엔드포인트 있음)	○	-
동기식 예비 복제본 (Standby replica)	접근 불가 (엔드포인트 없음)	-	○
읽기 추가		○	
읽기 노드(Reader)		○	-
읽기 전용 복제본(Read replica)		-	○

2. 컴퓨팅 서비스 응용 : RDS

■ Aurora RDS의 다중 AZ

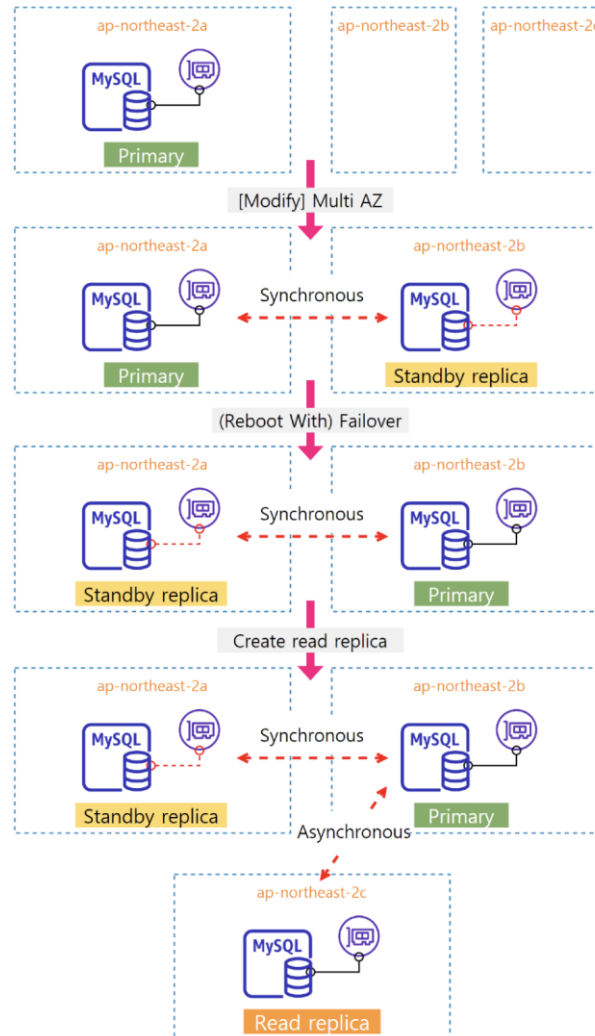
- 그림은 Aurora가 단일 AZ 상태에서 다중 AZ로 변하는 과정을 보여준다.



2. 컴퓨팅 서비스 응용 : RDS

■ Aurora 이외 RDS의 다중 AZ

- 그림은 Aurora 이외의 엔진 유형이 단일 AZ에서 다중 AZ 상태로 변하는 과정을 보여준다.





Thank You
