

Lab5. Create an Additional Security Group and NACL

목적

이번 실습에서는 기본 보안 그룹과 NACL외에 추가적으로 사용자 정의형 보안 그룹과 NACL을 생성한다. 또한 추가적으로 생성한 보안 그룹을 Lab3에서 생성한 lab-eni에 연결한다. 새로 생성한 NACL의 인바운드 규칙과 아웃바운드 규칙을 편집하고 그리고 마지막으로 Lab2에서 생성한 lab-subnet과 연결한다.

사전 준비물

AWS Free-Tier 계정

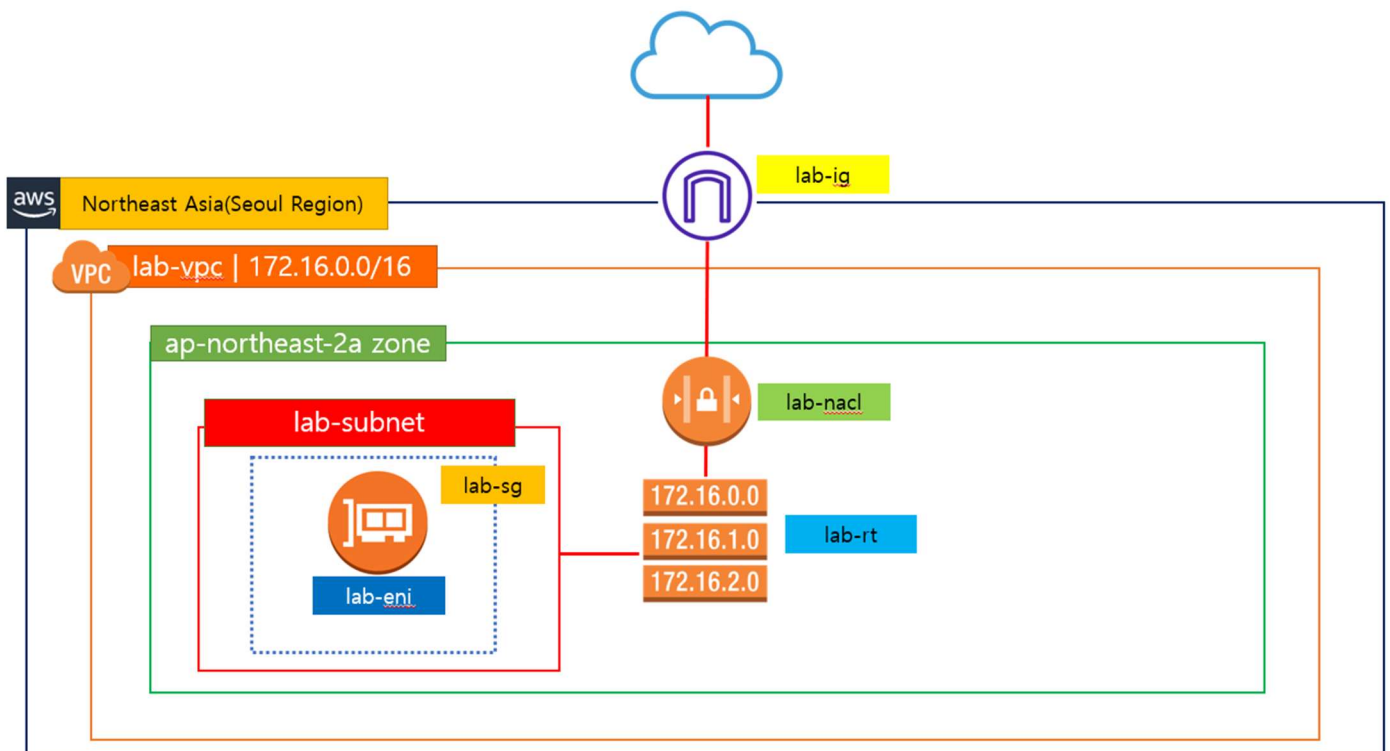
lab-vpc

lab-subnet

lab-eni

lab-ig

lab-rt



사용자 정의형 보안 그룹 생성하기

1. [서비스] > [VPC]의 좌측 메뉴 중 [보안] > [보안그룹]을 클릭하여 [보안 그룹] 페이지로 이동한다. 현재 기본 보안 그룹만 생성되어 있음을 확인할 수 있다.

보안 그룹 (1/1) 정보

Name	보안 그룹 ID	보안 그룹 이름	VPC ID	설명	소유자
-	sg-036f791118604bff1	default	vpc-022fe4e78a6a726f6	default VPC security gr...	78953482

sg-036f791118604bff1 - default

세부 정보 | 인바운드 규칙 | 아웃바운드 규칙 | 태그

이제 Reachability Analyzer를 사용하여 네트워크 연결을 확인할 수 있습니다. [Reachability Analyzer 실행](#)

세부 정보

보안 그룹 이름	보안 그룹 ID	설명	VPC ID
default	sg-036f791118604bff1	default VPC security group	vpc-022fe4e78a6a726f6

소유자	인바운드 규칙 수	아웃바운드 규칙 수
789534828835	1 권한 항목	1 권한 항목

2. [인바운드 규칙] 탭을 클릭하여 기본 보안 그룹의 인바운드 규칙을 확인해 보면 모든 유형의 포트와 트래픽이 허용되어 있음을 확인할 수 있다.

sg-036f791118604bff1 - default

세부 정보 | **인바운드 규칙** | 아웃바운드 규칙 | 태그

이제 Reachability Analyzer를 사용하여 네트워크 연결을 확인할 수 있습니다. [Reachability Analyzer 실행](#)

인바운드 규칙 (1/1)

Name	보안 그룹 규칙 ID	IP 버전	유형	프로토콜	포트 범위	소스
-	sgr-007e6baf55397b0ba	-	모든 트래픽	전체	전체	sg-036f791118604bff1 / default

3. 새 보안 그룹 생성을 위해 페이지 우측 상단의 [보안 그룹 생성]을 클릭한다.

보안 그룹 (1/1) 정보

[보안 그룹 생성](#)

Name	보안 그룹 ID	보안 그룹 이름	VPC ID	설명	소유자
-	sg-036f791118604bff1	default	vpc-022fe4e78a6a726f6	default VPC security gr...	78953482

4. [보안 그룹 생성] 페이지에서 다음의 각 값을 설정한다.

- A. [보안 그룹 이름] : lab-sg
- B. [설명] : Security Group for Lab5
- C. [VPC] : lab-vpc

VPC > 보안 그룹 > 보안 그룹 생성

보안 그룹 생성 정보

보안 그룹은 인바운드 및 아웃바운드 트래픽을 관리하는 인스턴스의 가상 방화벽 역할을 합니다. 새 보안 그룹을 생성하려면 아래의 필드를 작성하십시오.

기본 세부 정보

보안 그룹 이름 정보

생성 후에는 이름을 편집할 수 없습니다.

설명 정보

VPC 정보

5. 페이지를 스크롤다운하여 [인바운드 규칙] 섹션으로 이동한다. [규칙 추가]를 클릭하여 다음과 같이 설정한다.

- A. [유형] : 모든 ICMP-IPv4, [소스] : Anywhere-IPv4
- B. [유형] : SSH, [소스] : Anywhere-IPv4

인바운드 규칙 정보

보안 그룹 규칙 ID	유형 정보	프로토콜 정보	포트 범위 정보	소스 정보	설명 - 선택 사항 정보
sgr-0d25fbce4688acedd	SSH	TCP	22	Anywh... 0.0.0.0/0	<input type="text"/> 삭제
-	모든 ICMP - IPv4	ICMP	전체	Anywh... 0.0.0.0/0	<input type="text"/> 삭제

규칙 추가

6. [아웃바운드 규칙]은 기본값 그대로 사용하기로 한다. [태그] 섹션에서 키와 값을 설정한 후 [보안 그룹 생성] 버튼을 클릭한다.

A. [키] : Name

B. [값] : lab-sg

아웃바운드 규칙 정보

유형 정보 프로토콜 정보 포트 범위 정보 대상 정보 설명 - 선택 사항 정보

모든 트래픽 전체 전체 사용자 ... 0.0.0.0 삭제

규칙 추가

태그 선택 사항

태그는 사용자가 AWS 리소스에 할당하는 레이블입니다. 각 태그는 키와 값(선택 사항)으로 구성됩니다. 태그를 사용하여 리소스를 검색 및 필터링하거나 AWS 비용을 추적할 수 있습니다.

키 값 - 선택 사항

Q Name Q lab-sg 제거

새로운 태그 추가

최대 49개의 태그를 더 추가할 수 있습니다.

취소 **보안 그룹 생성**

7. 보안 그룹이 잘 생성되었다.

VPC > 보안 그룹 > sg-0eae8b8407d5da904 - lab-sg

sg-0eae8b8407d5da904 - lab-sg 작업 ▼

세부 정보

보안 그룹 이름 lab-sg	보안 그룹 ID sg-0eae8b8407d5da904	설명 Security Group for Lab5	VPC ID vpc-022fe4e78a6a726f6
소유자 789534828835	인바운드 규칙 수 2 권한 항목	아웃바운드 규칙 수 1 권한 항목	

인바운드 규칙 아웃바운드 규칙 태그

이제 Reachability Analyzer를 사용하여 네트워크 연결을 확인할 수 있습니다. Reachability Analyzer 실행 X

인바운드 규칙 (2) 태그 관리 인바운드 규칙 편집

Q 보안 그룹 규칙 필터

	Name	보안 그룹 규칙 ID	IP 버전	유형	프로토콜	포트
<input type="checkbox"/>	-	sgr-0ef764d5fa0309f6f	IPv4	모든 ICMP - IPv4	ICMP	전체
<input type="checkbox"/>	-	sgr-0d25fbce4688acedd	IPv4	SSH	TCP	22

8. [서비스] > [EC2] > [네트워크 및 보안] > [네트워크 인터페이스]를 클릭하여 Lab3에서 생성한 **lab-eni** 상세 페이지로 이동한다. 현재 [보안 그룹]은 기본 보안 그룹으로 설정되어 있음을 확인할 수 있다.

EC2 > Network interfaces > eni-0a121d58a2767aeba

eni-0a121d58a2767aeba(lab-eni)

네트워크 인터페이스 삭제 작업 ▼

이제 Reachability Analyzer를 사용하여 네트워크 연결을 확인할 수 있습니다. Reachability Analyzer 실행 ✕

세부 정보

▼ 네트워크 인터페이스 세부 정보

네트워크 인터페이스 ID eni-0a121d58a2767aeba	이름 lab-eni	설명 New ENI Creation
네트워크 인터페이스 상태 Available	인터페이스 유형 탄력적 네트워크 인터페이스	보안 그룹 sg-036f791118604bff1 (default)
VPC ID vpc-022fe4e78a6a726f6	서브넷 ID subnet-0402d4fa5c211af22	가용 영역 ap-northeast-2a
소유자 789534828835	요청자 ID -	요청자 관리형 아니요
소스/대상 확인 예		

9. 방금 생성한 **lab-sg** 보안 그룹과 연결하기 위해 [작업] > [보안 그룹 변경]을 클릭한다.

네트워크 인터페이스 삭제 작업 ▲

연결
분리
IP 주소 관리
주소 연결
주소 연결 해제
종료 동작 변경

보안 그룹 변경

소스/대상 확인 변경
태그 관리
접두사 관리
설명 변경

설명
New ENI Creation

보안 그룹
sg-036f791118604bff1

가용 영역
ap-northeast-2a

10. [보안 그룹 변경] 페이지에서 [연결된 보안 그룹]의 값을 **lab-sg**로 선택한다. 그리고 [보안 그룹 추가] 버튼을 클릭한다.

EC2 > 네트워크 인터페이스 > eni-0a121d58a2767aeba > 보안 그룹 변경

보안 그룹 변경 정보

Amazon EC2는 선택한 보안 그룹의 모든 규칙을 평가하여 인스턴스에서 송수신되는 인바운드 및 아웃바운드 트래픽을 제어합니다. 이 창을 사용하여 보안 그룹을 추가 및 제거할 수 있습니다.

네트워크 인터페이스 세부 정보

네트워크 인터페이스 ID
eni-0a121d58a2767aeba

연결된 보안 그룹

네트워크 인터페이스에 하나 이상의 보안 그룹을 추가합니다. 보안 그룹을 제거할 수도 있습니다.

네트워크 인터페이스와 연결된 보안 그룹(eni-0a121d58a2767aeba)

보안 그룹 이름	보안 그룹 ID	
default	sg-036f791118604bff1	<input type="button" value="제거"/>

11. 그리고 **default** 보안 그룹은 [제거] 버튼을 클릭하여 제거한다. 그리고 [저장]을 클릭한다.

EC2 > 네트워크 인터페이스 > eni-0a121d58a2767aeba > 보안 그룹 변경

보안 그룹 변경 정보

Amazon EC2는 선택한 보안 그룹의 모든 규칙을 평가하여 인스턴스에서 송수신되는 인바운드 및 아웃바운드 트래픽을 제어합니다. 이 창을 사용하여 보안 그룹을 추가 및 제거할 수 있습니다.

네트워크 인터페이스 세부 정보

네트워크 인터페이스 ID
eni-0a121d58a2767aeba

연결된 보안 그룹

네트워크 인터페이스에 하나 이상의 보안 그룹을 추가합니다. 보안 그룹을 제거할 수도 있습니다.

네트워크 인터페이스와 연결된 보안 그룹(eni-0a121d58a2767aeba)

보안 그룹 이름	보안 그룹 ID	
lab-sg	sg-0eaeeb8407d5da904	<input type="button" value="제거"/>

12. lab-eni의 보안 그룹이 변경됐음을 확인한다.

EC2 > Network interfaces > eni-0a121d58a2767aeba

eni-0a121d58a2767aeba(lab-eni)

네트워크 인터페이스 삭제작업 ▼

이제 Reachability Analyzer를 사용하여 네트워크 연결을 확인할 수 있습니다.

Reachability Analyzer 실행

세부 정보

▼ 네트워크 인터페이스 세부 정보

네트워크 인터페이스 ID eni-0a121d58a2767aeba	이름 lab-eni	설명 New ENI Creation
네트워크 인터페이스 상태 Available	인터페이스 유형 탄력적 네트워크 인터페이스	<div>보안 그룹 sg-0eaeeb8407d5da904 (lab-sg)</div>
VPC ID vpc-022fe4e78a6a726f6	서브넷 ID subnet-0402d4fa5c211af22	가용 영역 ap-northeast-2a
소유자 789534828835	요청자 ID -	요청자 관리형 아니요

사용자 정의형 NACL 생성하기

1. [보안] > [네트워크 ACL]을 클릭하여 네트워크 ACL 페이지로 이동한다. 현재 기본 NACL만 있다.

네트워크 ACL (1/1) 정보

Name	네트워크 ACL ID	연결 대상	기본값	VPC ID
-	acl-056fec0dcb376282d	subnet-0402d4fa5c211af22 / lab-subnet	예	vpc-022fe4e78a6a726f6 / lab-v

acl-056fec0dcb376282d

세부 정보

네트워크 ACL ID: acl-056fec0dcb376282d

연결 대상: subnet-0402d4fa5c211af22 / lab-subnet

기본값: 예

VPC ID: vpc-022fe4e78a6a726f6 / lab-vpc

소유자: 789534828835

2. [인바운드 규칙] 탭을 클릭한다. 모두 허용 규칙이 저장돼 있으므로 블랙 기반 경합 방식임을 알 수 있다. 아웃바운드 규칙도 이와 같다.

acl-056fec0dcb376282d

세부 정보 | **인바운드 규칙** | 아웃바운드 규칙 | 서브넷 연결 | 태그

이제 Reachability Analyzer를 사용하여 네트워크 연결을 확인할 수 있습니다. [Reachability Analyzer 실행](#)

인바운드 규칙 (2)

인바운드 규칙 편집

규칙 번호	유형	프로토콜	포트 범위	소스	허용/거부
100	모든 트래픽	모두	모두	0.0.0.0/0	Allow
*	모든 트래픽	모두	모두	0.0.0.0/0	Deny

3. [서브넷] 탭을 클릭해보면, 기본 NACL은 lab-subnet과 연결되어 있음을 확인할 수 있다.

acl-056fec0dcb376282d

세부 정보 | 인바운드 규칙 | 아웃바운드 규칙 | **서브넷 연결** | 태그

서브넷 연결 (1) 서브넷 연결 편집

Q 서브넷 연결 필터링 < 1 > ⚙

이름	서브넷 ID	연결 대상	가용 영역	IPv4 CIDR	IPv6 C
lab-subnet	subnet-0402d4fa5c211af22	acl-056fec0dcb376282d	ap-northeast-2a	172.16.100.0/24	-

4. 새 네트워크 ACL을 생성하기 위해 페이지 우측 상단의 [네트워크 ACL 생성]을 클릭한다.

네트워크 ACL (1/1) 정보 🔄 작업 ▼ **네트워크 ACL 생성**

Q 네트워크 ACL 필터링 < 1 > ⚙

<input checked="" type="checkbox"/>	Name	네트워크 ACL ID	연결 대상	기본값	VPC ID
<input checked="" type="checkbox"/>	-	acl-056fec0dcb376282d	subnet-0402d4fa5c211af22 / lab-subnet	예	vpc-022fe4e78a6a726f6 / lab-v

5. [네트워크 ACL 생성] 페이지에서 다음의 값을 설정한 후, [네트워크 ACL 생성] 버튼을 클릭한다.

- A. [이름] : lab-nacl
- B. [VPC] : lab-vpc
- C. [키] : Name
- D. [값] : lab-nacl

VPC > 네트워크 ACL > 네트워크 ACL 생성

네트워크 ACL 생성 정보

네트워크 ACL은 서브넷 내부와 외부의 트래픽을 제어하기 위한 방화벽 역할을 하는 선택적 보안 계층입니다.

네트워크 ACL 설정

이름 - 선택 사항

'Name' 키와 사용자가 지정하는 값을 포함하는 태그를 생성합니다.

lab-nacl

VPC

이 네트워크 ACL에 사용할 VPC입니다.

vpc-022fe4e78a6a726f6 (lab-vpc) ▼

태그

태그는 AWS 리소스에 할당하는 레이블입니다. 각 태그는 키와 선택적 값으로 구성됩니다. 태그를 사용하여 리소스를 검색 및 필터링하거나 AWS 비용을 추적할 수 있습니다.

키

lab-nacl

×

값 - 선택 사항

lab-nacl

×

제거

새 태그 추가

49을(를) 태그.개 더 추가할 수 있습니다.

취소

네트워크 ACL 생성

6. 네트워크 ACL이 잘 생성되었다. 방금 생성한 lab-nacl은 연결된 서브넷이 없고 기본 NACL이 아님을 알 수 있다.

네트워크 ACL (1/2) 정보

네트워크 ACL 필터링

Name	네트워크 ACL ID	연결 대상	기본값	VPC ID
lab-nacl	acl-07d66e330685b18ca	-	아니요	vpc-022fe4e78a6a726f6 / lab-
-	acl-056fec0dc376282d	subnet-0402d4fa5c211af22 / lab-subnet	예	vpc-022fe4e78a6a726f6 / lab-

acl-07d66e330685b18ca / lab-nacl

세부 정보 | 인바운드 규칙 | 아웃바운드 규칙 | 서브넷 연결 | 태그

세부 정보

네트워크 ACL ID	연결 대상	기본값	VPC ID
acl-07d66e330685b18ca	-	아니요	vpc-022fe4e78a6a726f6 / lab-vpc
소유자			
789534828835			

7. 먼저 [인바운드 규칙] 탭과 [아웃바운드 규칙] 탭을 클릭하면 모두 거부 규칙만 저장돼 있어 화이트기반 결합 방식임을 알 수 있다.

acl-07d66e330685b18ca / lab-nacl

세부 정보 | **인바운드 규칙** | 아웃바운드 규칙 | 서브넷 연결 | 태그

이제 Reachability Analyzer를 사용하여 네트워크 연결을 확인할 수 있습니다. Reachability Analyzer 실행

인바운드 규칙 (1)

인바운드 규칙 편집

인바운드 규칙 필터링

규칙 번호	유형	프로토콜	포트 범위	소스	허용/거부
*	모든 트래픽	모두	모두	0.0.0.0/0	Deny

8. **인바운드 규칙**과 **아웃바운드 규칙**을 편집해서 클라이언트 접속을 허용하기로 한다. [**인바운드 규칙**] 탭에서 [**인바운드 규칙 편집**]을 클릭한다.

acl-07d66e330685b18ca / lab-nacl

세부 정보 | **인바운드 규칙** | 아웃바운드 규칙 | 서브넷 연결 | 태그

이제 Reachability Analyzer를 사용하여 네트워크 연결을 확인할 수 있습니다. Reachability Analyzer 실행 X

인바운드 규칙 (1) 인바운드 규칙 편집

인바운드 규칙 필터링

규칙 번호	유형	프로토콜	포트 범위	소스	허용/거부
*	모든 트래픽	모두	모두	0.0.0.0/0	Deny

9. [**인바운드 규칙 편집**] 페이지에서 [**새 규칙 추가**] 버튼을 클릭하여 다음과 같이 설정하고 [**변경 사항 저장**] 버튼을 클릭한다.

A. [**규칙 번호**] : 100, [**유형**] : 모든 ICMP – IPv4, [**소스**] : 0.0.0.0/0, [**허용/거부**] : 허용

B. [**규칙 번호**] : 200, [**유형**] : SSH(22), [**소스**] : 0.0.0.0/0, [**허용/거부**] : 허용

VPC > 네트워크 ACL > acl-07d66e330685b18ca / lab-nacl > 인바운드 규칙 편집

인바운드 규칙 편집 정보

인바운드 규칙은 VPC에 도달할 수 있는 수신 트래픽을 제어합니다.

규칙 번호 정보	유형 정보	프로토콜 정보	포트 범위 정보	소스 정보	허용/거부 정보	
100	모든 ICMP - IPv4	ICMP(1)	모두	0.0.0.0/0	허용	제거
200	SSH(22)	TCP(6)	22	0.0.0.0/0	허용	제거
*	모든 트래픽	모두	모두	0.0.0.0/0	거부	

새 규칙 추가 규칙 번호별 정렬

취소 변경 사항 미리 보기 **변경 사항 저장**

10. [**아웃바운드 규칙**] 탭의 [**아웃바운드 규칙 편집**]을 클릭한다.

acl-07d66e330685b18ca / lab-nacl

세부 정보 | 인바운드 규칙 | **아웃바운드 규칙** | 서브넷 연결 | 태그

이제 Reachability Analyzer를 사용하여 네트워크 연결을 확인할 수 있습니다. Reachability Analyzer 실행 X

아웃바운드 규칙 (1) 아웃바운드 규칙 편집

아웃바운드 규칙 필터링

규칙 번호	유형	프로토콜	포트 범위	대상	허용/거부
*	모든 트래픽	모두	모두	0.0.0.0/0	Deny

11. [아웃바운드 규칙 편집] 페이지에서 다음과 같이 각각의 값을 설정한 후, [변경 사항 저장]을 클릭한다.

A. [규칙 번호] : 100, [유형] : 모든 ICMP - IPv4, [대상] : 0.0.0.0/0, [허용/거부] : 허용

B. [규칙 번호] : 200, [유형] : 모든 TCP, [대상] : 0.0.0.0/0, [허용/거부] : 허용

C. [규칙 번호] : 300, [유형] : 모든 UDP, [대상] : 0.0.0.0/0, [허용/거부] : 허용

VPC > 네트워크 ACL > acl-07d66e330685b18ca / lab-nacl > 아웃바운드 규칙 편집

아웃바운드 규칙 편집 정보

아웃바운드 규칙은 VPC에서 나갈 수 있는 발신 트래픽을 제어합니다.

규칙 번호 정보	유형 정보	프로토콜 정보	포트 범위 정보	대상 정보	허용/거부 정보	
100	모든 ICMP - IPv4 ▼	ICMP(1) ▼	모두	0.0.0.0/0	허용 ▼	제거
200	모든 TCP ▼	TCP(6) ▼	모두	0.0.0.0/0	허용 ▼	제거
300	모든 UDP ▼	UDP(17) ▼	모두	0.0.0.0/0	허용 ▼	제거
*	모든 트래픽 ▼	모두 ▼	모두	0.0.0.0/0	거부 ▼	

새 규칙 추가 규칙 번호별 정렬

취소 변경 사항 미리 보기 **변경 사항 저장**

12. 방금 생성한 **lab-nacl**은 아직 **서브넷**에 연결되어 있지 않다. **서브넷**에 연결하기 위해 [서브넷 연결 편집]을 클릭한다.

네트워크 ACL (1/2) 정보

네트워크 ACL 생성

네트워크 ACL 필터링

	Name	네트워크 ACL ID	연결 대상	기본값	VPC ID
<input checked="" type="checkbox"/>	lab-nacl	acl-07d66e330685b18ca	-	아니요	vpc-022fe4e78a6a726f6 / lab-
<input type="checkbox"/>	-	acl-056fec0dcb376282d	subnet-0402d4fa5c211af22 / lab-subnet	예	vpc-022fe4e78a6a726f6 / lab-

acl-07d66e330685b18ca / lab-nacl

세부 정보 인바운드 규칙 아웃바운드 규칙 **서브넷 연결** 태그

서브넷 연결

서브넷 연결 필터링

이름	서브넷 ID	연결 대상	가용 영역	IPv4 CIDR	IPv6 CIDR
이 리전에 이 네트워크 ACL과 연결된 서브넷이 없습니다.					

서브넷 연결 편집

13. [서브넷 연결 편집] 페이지에서 [이용 가능한 서브넷] 목록에서 Lab2에서 생성한 lab-subnet을 체크하고, [변경 사항 저장]을 클릭한다.

VPC > 네트워크 ACL > acl-07d66e330685b18ca / lab-nacl > 서브넷 연결 편집

서브넷 연결 편집 정보

이 네트워크 ACL과 연결된 서브넷을 변경합니다.

이용 가능한 서브넷 (1/1)

Q 서브넷 연결 필터링

<input checked="" type="checkbox"/>	이름	서브넷 ID	연결 대상	가용 영역	IPv4 CIDR	IPv6 CIDR
<input checked="" type="checkbox"/>	lab-subnet	subnet-0402d4fa5c211af22	acl-056fec0dcb376282d	ap-northeast-2a	172.16.100.0/24	-

선택한 서브넷

subnet-0402d4fa5c211af22 / lab-subnet X

취소 **변경 사항 저장**

14. 이번 실습에서 생성한 lab-nacl의 인바운드 규칙과 아웃바운드 규칙 그리고 서브넷 연결까지 모두 마쳤다.

네트워크 ACL (1/2) 정보

Q 네트워크 ACL 필터링

<input checked="" type="checkbox"/>	Name	네트워크 ACL ID	연결 대상	기본값	VPC ID
<input checked="" type="checkbox"/>	lab-nacl	acl-07d66e330685b18ca	subnet-0402d4fa5c211af22 / lab-subnet	아니요	vpc-022fe4e78a6a726f6 / lab-vpc
<input type="checkbox"/>	-	acl-056fec0dcb376282d	-	예	vpc-022fe4e78a6a726f6 / lab-vpc

acl-07d66e330685b18ca / lab-nacl

세부 정보 | 인바운드 규칙 | 아웃바운드 규칙 | 서브넷 연결 | 태그

세부 정보

네트워크 ACL ID acl-07d66e330685b18ca	연결 대상 subnet-0402d4fa5c211af22 / lab-subnet	기본값 아니요	VPC ID vpc-022fe4e78a6a726f6 / lab-vpc
소유자 789534828835			