8253jang@daum.net
장희정

Domain 연동하기

준비하기

- gabia사이트에 회원 가입 후 550원(현금)짜리 계정 만든다.
  (https://www.gabia.com/)

또는

- "내도메인.한국" 에서 무료로 도메인 계정을 만든다.

gabia사이트를 이용하는 경우 참고

가비아 ACM(Authority Certification Management) 인증서가 늦게 떨어질 수 있기 때문에 실습하기 전에 개인 도매인 생성부터 먼저 해야 한다.– HTTPS 연결제공
교육장에서 하나의 ip를 타고 나가기 때문에 발급에 시간이 많이 소요될 수 있다.
KOSTA 강의장에서는 3일동안 한 ip당 3개만 가입 가능하므로 주의 – 각자 집에서 생성해오기)

1. 가비아 회원가입
2. 500원 짜리 개인 도메인 만들기(shop 이나 store로 끝나는 도메인을 준다.)
3. My가비아 클릭 - 도메인 생성시 1년 짜리로 해야 500원(부가세포함 550원)이 된다.
4. 네임 서버 신청은 가비아 네임 서버 사용으로 선택하기
5. 안전 잠금 서비스 신청하면 확인 이메일이나 메시지를 보내준다.
6. 동시 신청 가능 서비스에서 웹 호스팅 신청하면 비싸니까 신청하지 않기
7. 마이 가비아>> 서비스 관리에 가면 만든 도메인이 보인다.
8. 카드 결재가 최하가 1000원이므로 무통장 입금으로만 가능하다.

실습 – "내도메인한국" 으로 해본다.

- 회원가입을 진행한다.

- 아래화면처럼 원하는 도메인을 검색해서 등록하기를 한다.

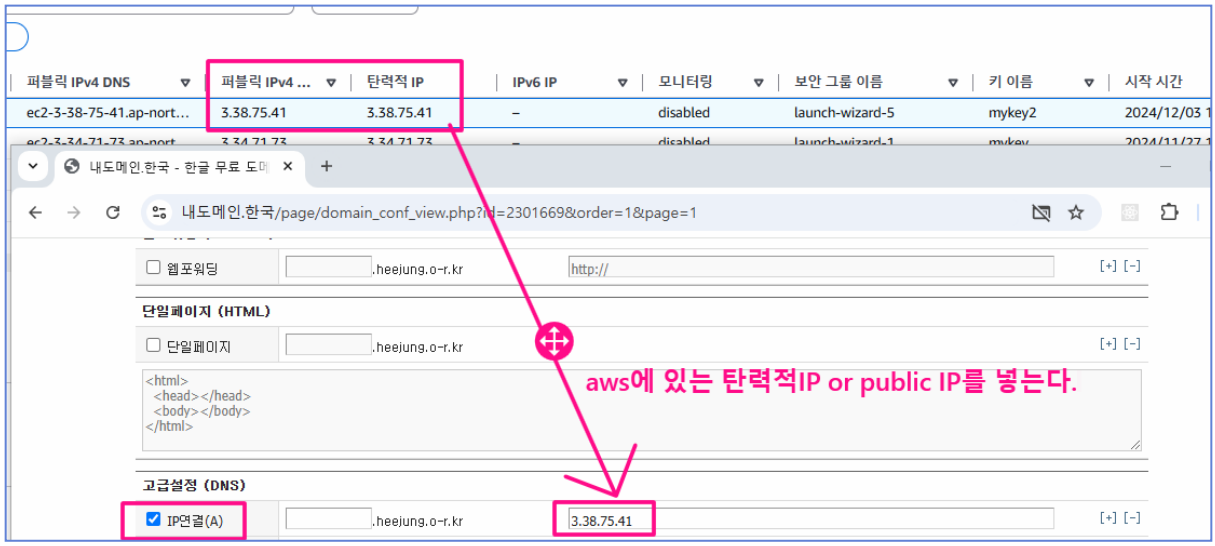
8253jang@daum.net
장희정

메뉴 > 도메인 관리 > 수정 클릭

8253jang@daum.net
장희정

AWS에 접속 해서 도메인으로 등록 하려는 인스턴스의 IP를 알아본다.

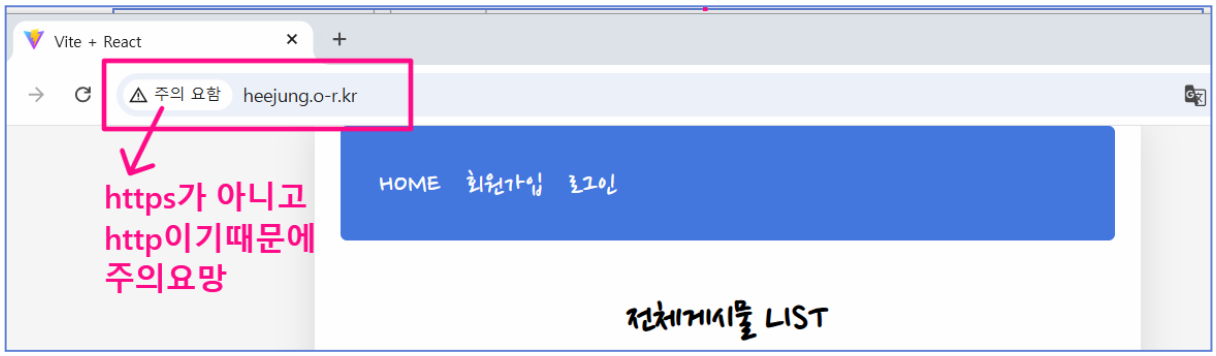
우리는 React를 start 해놓은 인스턴스의 IP를 도메인과 연결한다.



IP입력 후 보안코드 입력 한 후 수정하기를 클릭한다.

브라우저에서 도메인으로 요청해본다.

아래와 같이 도메인으로 잘 연결 된 것을 확인한다.



브라우저에서 "주의 요망" 또는 "보안 경고" 메시지가 나타나는 이유는 주로 **HTTP** 와 **HTTPS** 간의 차이 때문이다. HTTPS 는 보안이 강화된 HTTP 프로토콜로, 데이터를 암호화하여 전송한다. 반면 HTTP 는 암호화되지 않아서 보안이 취약하다. 따라서 HTTPS 를 사용하는 웹사이트는 데이터 전송 시 암호화와 인증을 제공하며, HTTPS 연결을 통해 웹사이트와의 통신을 보호할 수 있다.

보안 취약점 : HTTP 는 데이터를 암호화하지 않기 때문에, 네트워크 상에서 정보가 탈취될 수

있습니다. 예를 들어, 공용 Wi-Fi 에서 HTTP 를 통해 웹사이트에 접속하면, 악의적인 사용자가 중간에서 데이터를 가로챌 수 있다.

브라우저 경고 : 웹사이트가 HTTPS 를 사용하지 않고 HTTP 로 접속할 경우, **대부분의 최신 웹 브라우저(예: Chrome, Firefox)는 사용자의 보안을 위해 경고 메시지를 표시한다. "이 사이트는 안전하지 않음", "연결이 안전하지 않음" 등의 메시지가 나타나다.**

사이트 인증 부족 : **HTTPS 는 SSL/TLS 인증서를 사용하여 웹사이트의 신뢰성을 검증한다.** 인증서가 유효하고 신뢰할 수 있는 기관에서 발급되었음을 확인하는 절차가 포함된다. 반면 HTTP 는 인증서가 없기 때문에, 브라우저는 연결의 신뢰성을 보장할 수 없다.

검색 엔진 최적화(SEO) : 구글과 같은 검색 엔진은 HTTPS 웹사이트를 더 신뢰하며, HTTP 로만 접속할 수 있는 웹사이트는 SEO 순위에서 불이익을 받을 수 있다.

따라서 , HTTP 연결을 사용할 경우 보안이 약해지므로, 브라우저는 사용자에게 이를 경고하는 메시지를 표시하고, HTTPS 로의 전환을 권장한다.

https 프로토콜 적용하기

AWS에서 https를 사용하려면 SSL/TLS 인증서를 설정하고, 이를 통해 웹 서버에서 보안 연결을 지원해야 한다. 주요 단계는 AWS에서 인증서를 생성하고, 이를 웹 서버와 연결하여 HTTPS를 활성화한다.

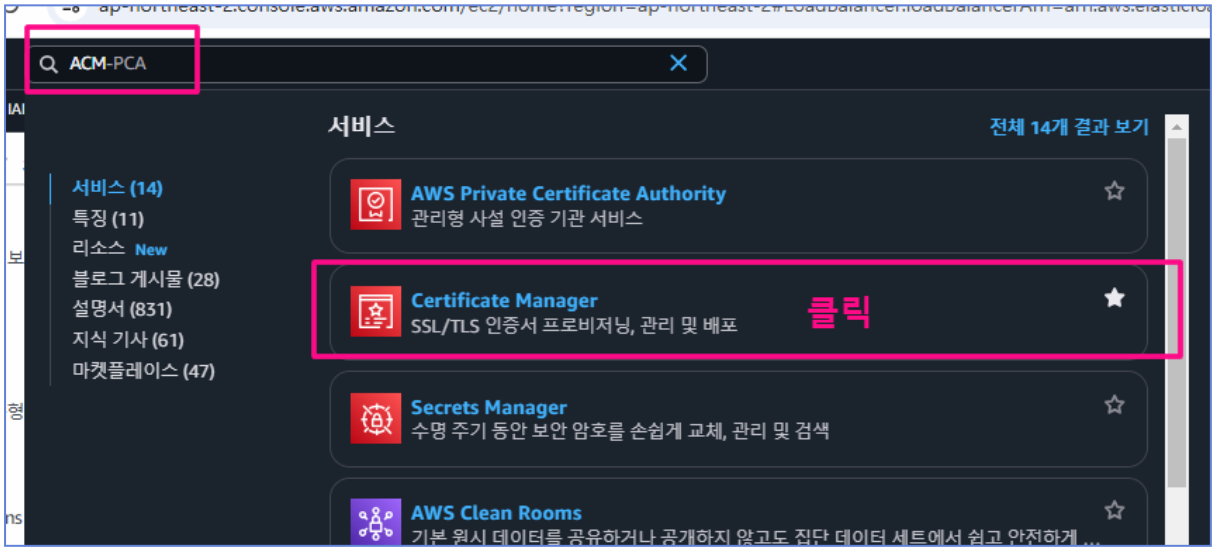
AWS에서 HTTPS를 설정하는 과정

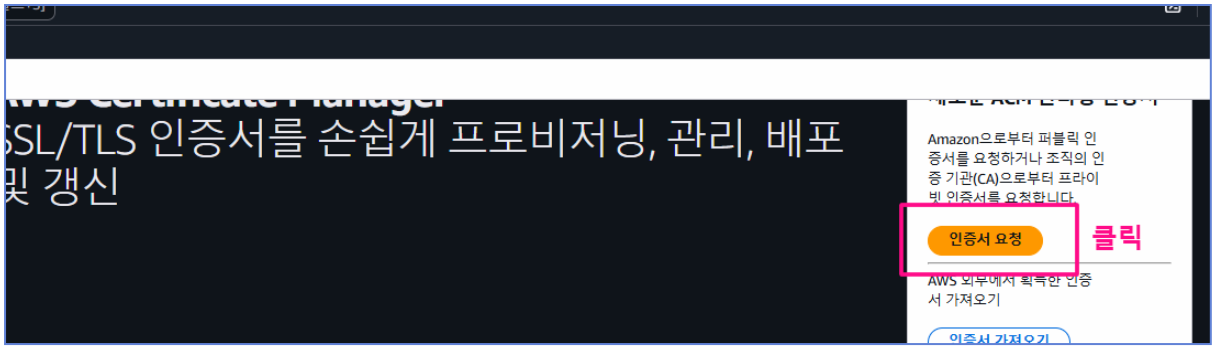
1. ACM(AWS Certificate Manager)에서 SSL/TLS 인증서 요청
2. 타켓그룹 생성
3. ELB(Elastic Load Balancer)생성
4. 보안그룹수정

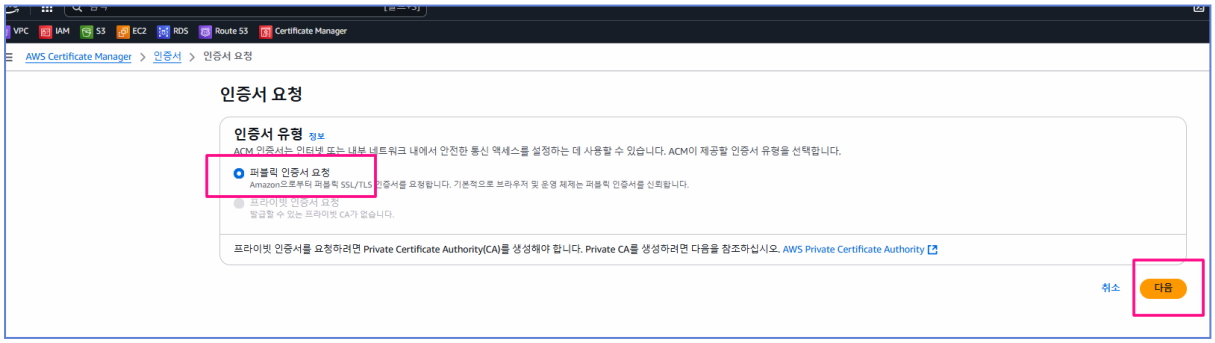
위 순서대로 진행 해보자.

Aws 에서 ACM검색

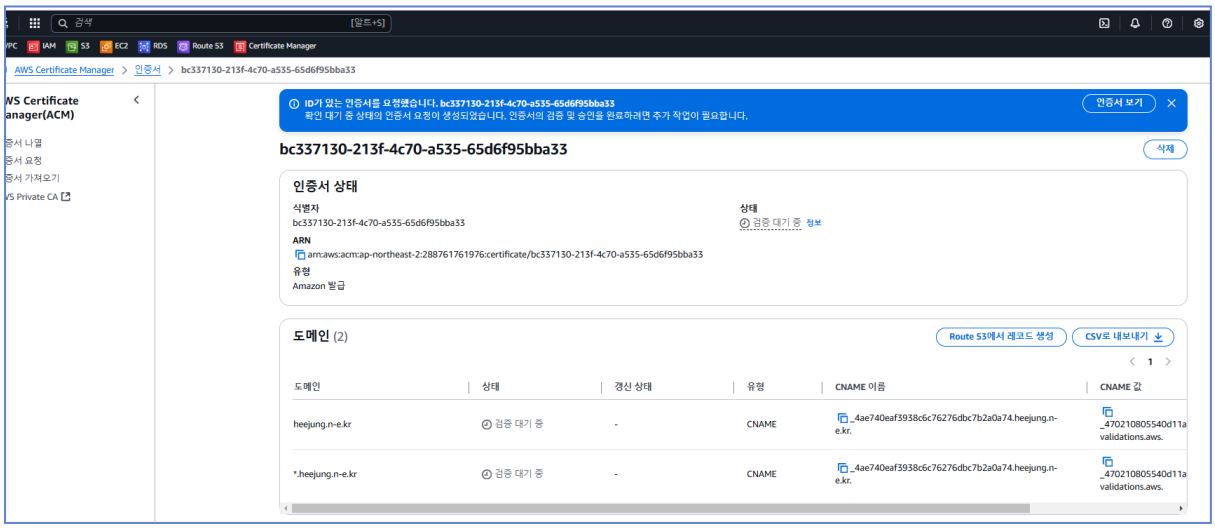
8253jang@daum.net
장희정

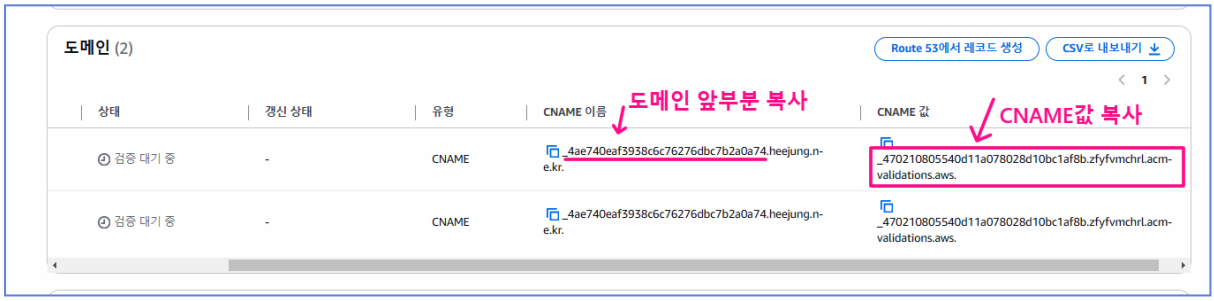




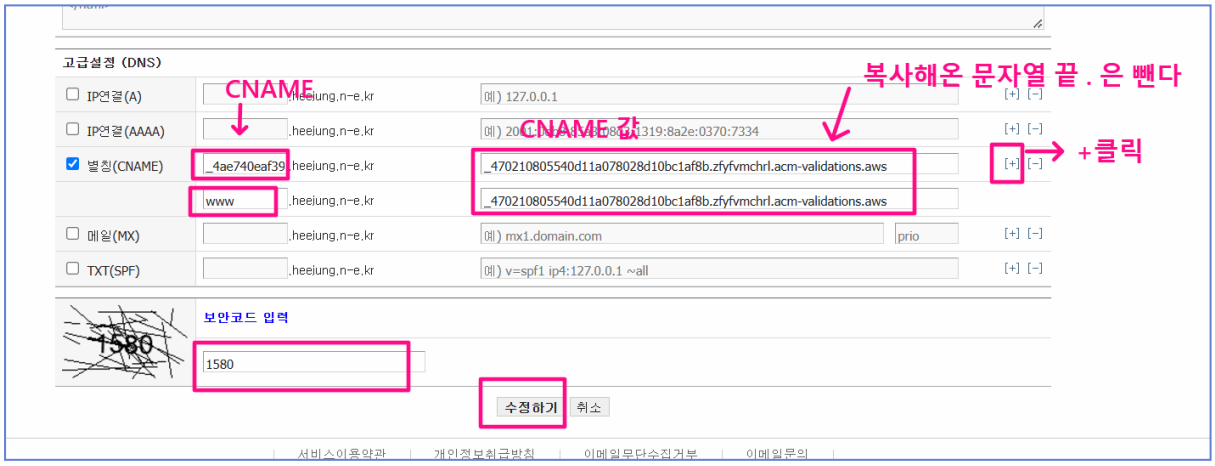


8253jang@daum.net
장희정

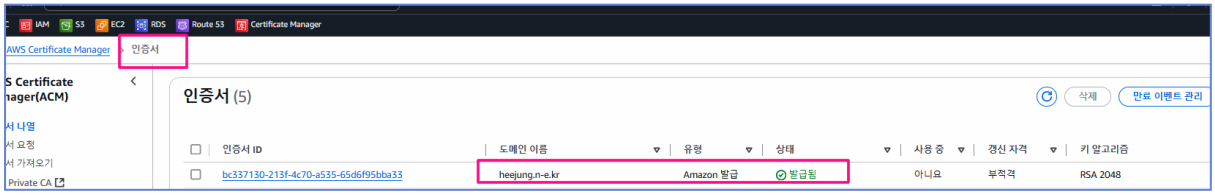




위 CNAME이름과 CNAME값을 "내도메인한국"의 나의 계정에 등록해야 인증서가 발급된다.
기존에 설정해 놓은 IP연결은 해지해도 된다.



다시 AWS로 돌아가서 잠시 기다리면(5분이내) 인증서가 발급 되었음을 확인한다.



이제 AWS에서 https를 사용할 때 매우 유용한 ELB를 생성해보자.

여러 서버에서 HTTPS를 처리하거나, 고가용성과 확장성이 중요한 웹 애플리케이션에서는 ELB를 사용하는 것이 권장되며 ELB는 HTTPS 요청을 처리하고 SSL/TLS 인증서를 관리하는 데 큰 도움이 된다.

☞ **ELB에 대해서**

AWS ELB(Elastic Load Balancer)는 Amazon Web Services(AWS)에서 제공하는 **로드 밸런싱 서비스**로 여러 서버(인스턴스)에 들어오는 트래픽을 분산하여 서버 간의 부하를 고르게 분배하고,

트래픽 처리 성능을 향상시키며, 애플리케이션의 고가용성 및 확장성을 보장한다.. ELB 는 특히 웹 애플리케이션에서 중요한 역할을 하며, **HTTPS** 와 같은 보안 트래픽을 처리하는 데 유용하다..

☞ **ELB 의 주요 특징:**

1. **트래픽 분산**:
   - ELB 는 여러 EC2 인스턴스(또는 다른 AWS 리소스)로 들어오는 트래픽을 분산시킨다. 이를 통해 서버 하나에 집중되는 과부하를 방지하고, 높은 가용성과 확장성을 유지할 수 있다.
2. **고가용성**:
   - 여러 가용 영역(Availability Zones)에서 자동으로 트래픽을 분배하여, 하나의 데이터 센터가 다운되더라도 다른 지역에서 트래픽을 처리할 수 있게 한다.
3. **자동 확장**:
   - 트래픽이 급증할 때 EC2 인스턴스를 자동으로 추가하거나 제거하여, 수요에 맞게 자동으로 확장하고 축소할 수 있다..
4. **다양한 프로토콜 지원**:
   - ELB 는 HTTP, HTTPS, TCP 등 여러 프로토콜을 지원한다. 따라서 다양한 유형의 트래픽을 처리할 수 있다.

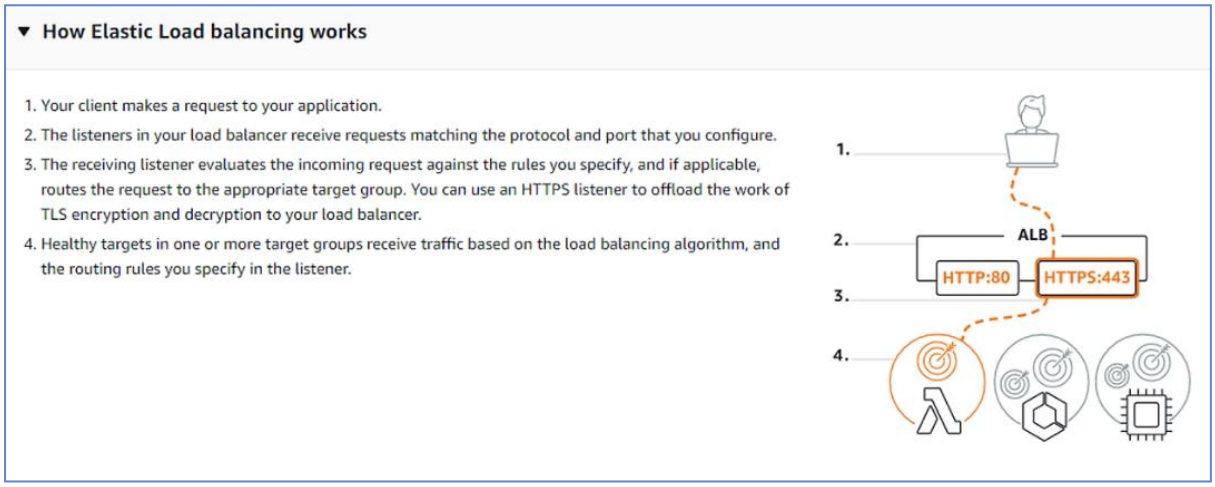
ELB를 사용하여 HTTPS를 설정하는 이유:

1. **SSL 종료 (SSL Termination)**:
   - ELB 는 **SSL 종료** 기능을 제공한다. 즉, 클라이언트에서 ELB 로 오는 HTTPS 요청을 먼저 받아 SSL 암호화를 해제(SSL Termination)하고, 그 후에 내부 트래픽은 **HTTP** 로 처리할 수 있다. 이는 내부 시스템에서 HTTPS 를 직접 처리할 필요 없이, 트래픽을 효율적으로 관리하는 데 유리하다.
2. **인증서 관리 간소화**:
   - SSL/TLS 인증서를 직접 웹 서버(예: Apache, Nginx)에 설치하는 대신, ELB 에 인증서를 연결해 관리할 수 있다. AWS Certificate Manager (ACM)을 통해 인증서를 ELB 에 쉽게 연결할 수 있다.
3. **고가용성 및 확장성**:
   - HTTPS 는 보안 연결을 위한 추가적인 처리 능력을 요구하는데, ELB 는 이를 자동으로 분산 처리한다. 또한 ELB 는 가용성 높은 구조로 여러 인스턴스에 트래픽을 분배하여 높은 트래픽에도 대응할 수 있다.
4. **보안**:
   - HTTPS 트래픽을 처리할 때, ELB 는 **웹 애플리케이션 방화벽(WAF)**, **DDoS 공격 보호**, **TLS 암호화** 등 추가적인 보안 기능을 통합할 수 있어 보안성을 강화할 수

있다.

다음과 같은 경우에는 ELB 를 사용하는 것이 권장한다.

1. **여러 EC2 인스턴스를 사용 중인 경우**:
   - 웹 애플리케이션을 여러 EC2 인스턴스에 배포하여 고가용성과 확장성을 요구하는 경우, ELB 는 트래픽을 균등하게 분배하여 서버의 부하를 고르게 나눈다.
2. **SSL/TLS 인증서 관리가 필요한 경우**:
   - ELB 를 사용하면 SSL 인증서를 중앙에서 관리할 수 있고, 인증서 갱신 및 배포가 간편해진다.
3. **트래픽 처리 성능이 중요한 경우**:
   - ELB 는 자동 확장 및 로드 밸런싱 기능을 통해 트래픽이 증가하더라도 안정적인 성능을 유지할 수 있다
4. **보안이 중요한 경우**:
   - ELB 는 HTTPS 트래픽을 안전하게 처리하고, Web Application Firewall(WAF)과 통합하여 보안 강화도 가능하게 해준다.



. 1. 클라이언트가 애플리케이션에 요청을 보낸다

2. 로드밸런서의 리스너가 설정했던 프로토콜 및 포트에 맞는 요청을 수신한다.

3. 수신 수신기는 사용자가 지정한 규칙과 비교하여 수신 요청이 유효한지 확인하고, 유효한 경우 해당 요청을 적절한 대상 그룹으로 라우팅한다. HTTPS 수신기를 사용하여 TLS 암호화 및 암호 해독 작업을 로드 밸런서로 오프로드할 수 있다.

4. 대상 그룹에 있는 하나 이상의 정상적인 서버는 로드 밸런싱 알고리즘 및 수신기에서 지정한 라우팅 규칙에 따라 트래픽을 수신한다.

ELB를 생성하기 전에 먼저 타켓그룹을 생성한다.

☞ **타켓그룹에 대해서**

AWS 에서 타겟 그룹(Target Group)은 Elastic Load Balancer(ELB)와 함께 사용되는 구성 요소로, 로드 밸런서가 트래픽을 분배할 대상 서버(인스턴스)들을 그룹화하여 관리하는 단위이다. 타겟 그룹은 트래픽을 분배할 대상 서버(타겟)들을 정의하며, 로드 밸런서가 특정 트래픽을 처리할 때 어떤 인스턴스에 요청을 전달할지 결정하는 데 중요한 역할을 한다..

타겟 그룹의 주요 개념:

1. **대상(Target)**:
   - 타겟 그룹은 여러 대상을 가질 수 있으며, 대상은 **EC2 인스턴스**, **Lambda 함수**, **IP 주소** 또는 **컨테이너** 등 다양한 형태로 존재할 수 있다. ELB 는 타겟 그룹을 기준으로 트래픽을 특정 대상에 전달한다.
2. **타겟 그룹의 역할**:
   - 타겟 그룹은 로드 밸런서가 요청을 분배할 때 어떤 서버(인스턴스)로 트래픽을 보내야 하는지 결정하는 단위이다.
   - 타겟 그룹에 속한 인스턴스들은 웹 서버 역할을 할 수 있으며, 애플리케이션을 처리하거나 API 요청을 받아 처리하는 등의 역할을 한다.
3. **헬스 체크(Health Check)**:
   - 타겟 그룹은 각 인스턴스의 상태를 모니터링한다. 로드 밸런서는 타겟 그룹의 **헬스 체크**를 통해 인스턴스가 정상적으로 작동하는지 확인한다. 헬스 체크에 실패한 인스턴스는 트래픽을 받지 않으며, 로드 밸런서는 다른 정상 인스턴스로 트래픽을 전달한다.
4. **로드 밸런서와의 연결**:
   - ELB(예: Application Load Balancer(ALB) 또는 Network Load Balancer(NLB)는 타겟 그룹과 연결된다. 트래픽을 분배할 때, 로드 밸런서는 요청을 받아 타겟 그룹에 설정된 인스턴스들로 분배한다.
   -

타겟 그룹의 종류:

1. **Application Load Balancer (ALB)**:

- **ALB** 는 주로 HTTP/HTTPS 트래픽을 처리한다. ALB 에서 타겟 그룹은 **EC2 인스턴스**, **Lambda 함수**, **IP 주소** 등을 대상으로 설정할 수 있다.
- 예를 들어, 여러 웹 애플리케이션 서버가 있을 때 ALB 는 요청을 각 타겟 그룹에 분배한다.

2. **Network Load Balancer (NLB)**:
   - **NLB** 는 주로 **TCP** 또는 **UDP** 트래픽을 처리한다.. NLB 도 타겟 그룹을 사용하지만, 기본적으로 **고속 네트워크 트래픽**을 처리하는 데 최적화되어 있다.
   - NLB 에서 타겟 그룹은 **EC2 인스턴스**와 **IP 주소**를 대상으로 설정할 수 있다.
3. **Gateway Load Balancer (GLB)**:
   - **GLB** 는 **네트워크 및 보안 장비**와 연동되는 로드 밸런서로, 보안 장비나 네트워크 장비를 대상으로 하는 타겟 그룹을 설정할 수 있다.
   -

타겟 그룹을 사용하는 이유:

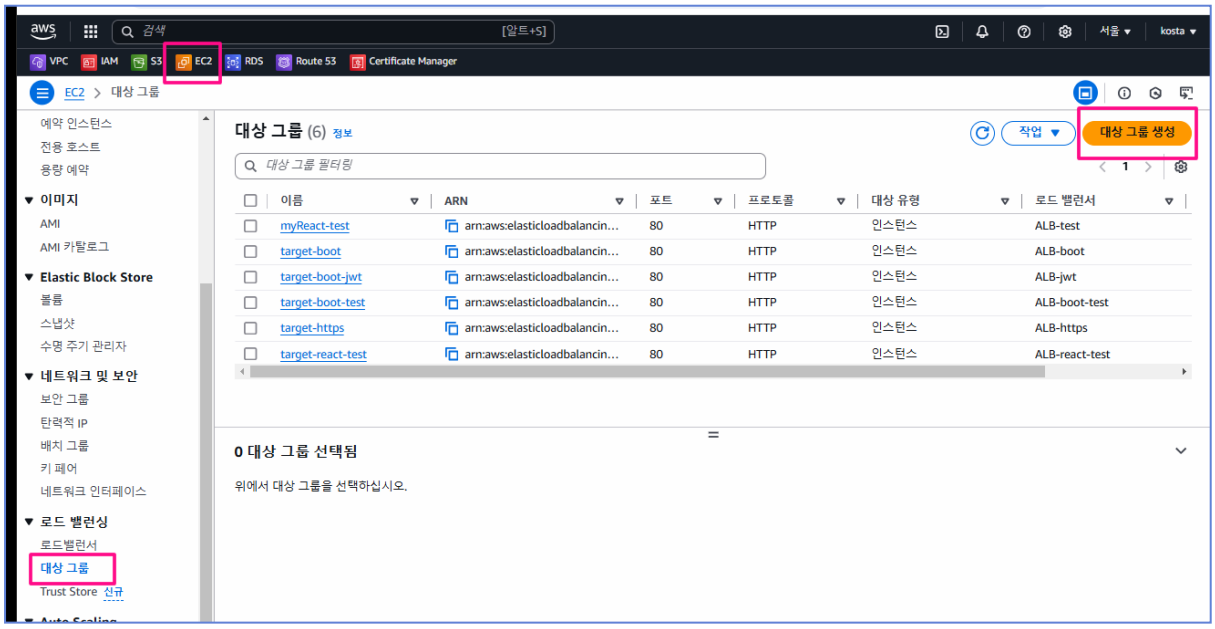
1. **로드 밸런싱**:
   - 타겟 그룹을 사용하면 로드 밸런서가 트래픽을 여러 인스턴스에 분배할 수 있게 되며 이를 통해 애플리케이션의 성능과 확장성을 향상시킬 수 있다.
2. **고가용성**:
   - 여러 인스턴스에 트래픽을 분배함으로써 **고가용성**을 확보할 수 있다. 한 인스턴스가 다운되더라도 다른 인스턴스가 트래픽을 처리할 수 있게 된다.
3. **헬스 체크**:
   - 로드 밸런서는 타겟 그룹의 인스턴스 상태를 지속적으로 모니터링한다. 헬스 체크에 실패한 인스턴스는 트래픽을 받지 않게 되어, 장애가 발생한 서버로 트래픽을 전달하지 않도록 할 수 있다.
4. **자동 확장**:
   - **Auto Scaling** 과 결합하여, 트래픽 부하가 커지면 새로운 인스턴스를 자동으로 타겟 그룹에 추가하고, 부하가 줄어들면 인스턴스를 자동으로 제거할 수 있다.
5. **다양한 리소스 관리**:
   - 타겟 그룹을 사용하면, EC2 인스턴스 외에도 Lambda 함수나 IP 주소 등을 타겟으로 설정하여 다양한 리소스를 관리할 수 있다.
   -

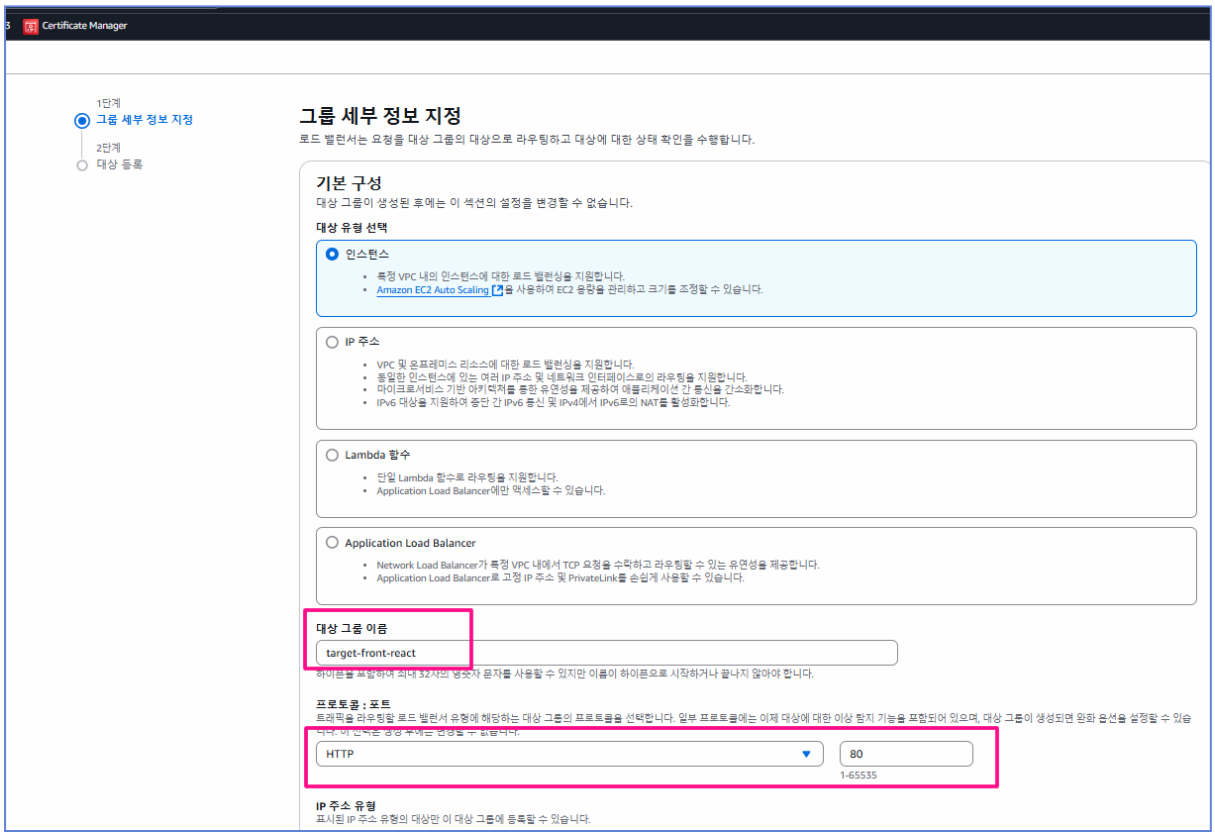
AWS 에서 **타겟 그룹**은 로드 밸런서가 트래픽을 분배할 대상 인스턴스를 그룹화하여 관리하는 단위로 타겟 그룹을 사용하면 트래픽 분배, 고가용성, 헬스 체크, 자동 확장 등의 기능을 효율적으로 설정하고 관리할 수 있다. ELB 는 이러한 타겟 그룹을 통해 여러 서버에 부하를 고르게 분배하며, 안정적이고 확장 가능한 서비스를 제공한다.

8253jang@daum.net
장희정

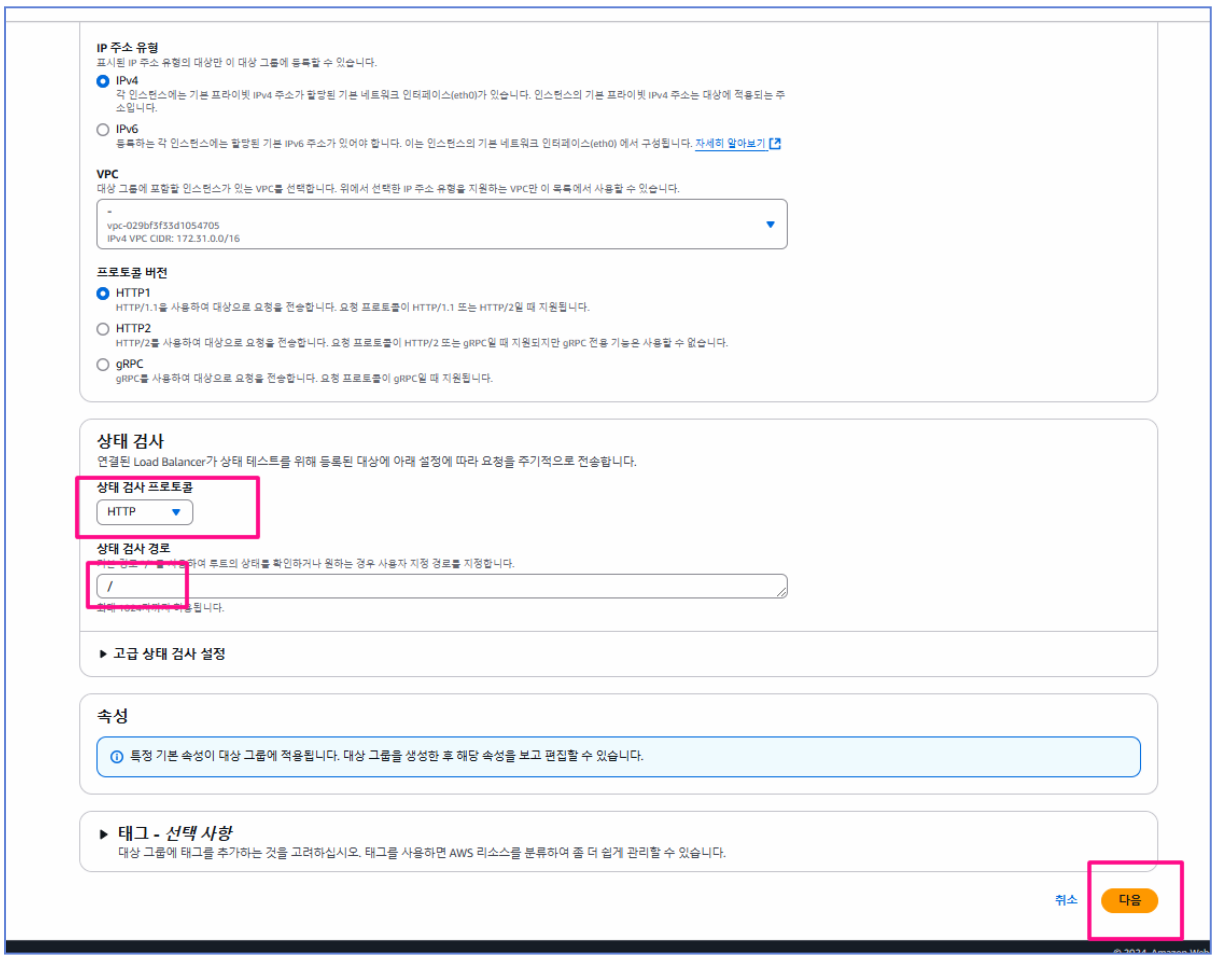
이제 실습해보자.

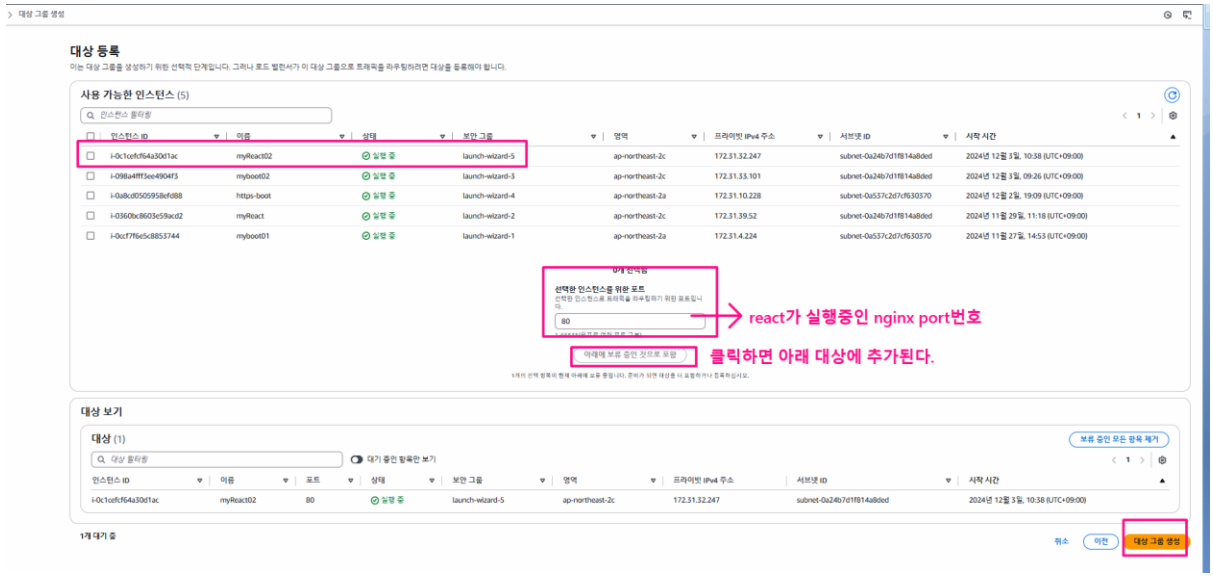
EC2를 클릭 > 로드밸런싱 > 대상그룹 선택 > 대상그룹 생성 선택



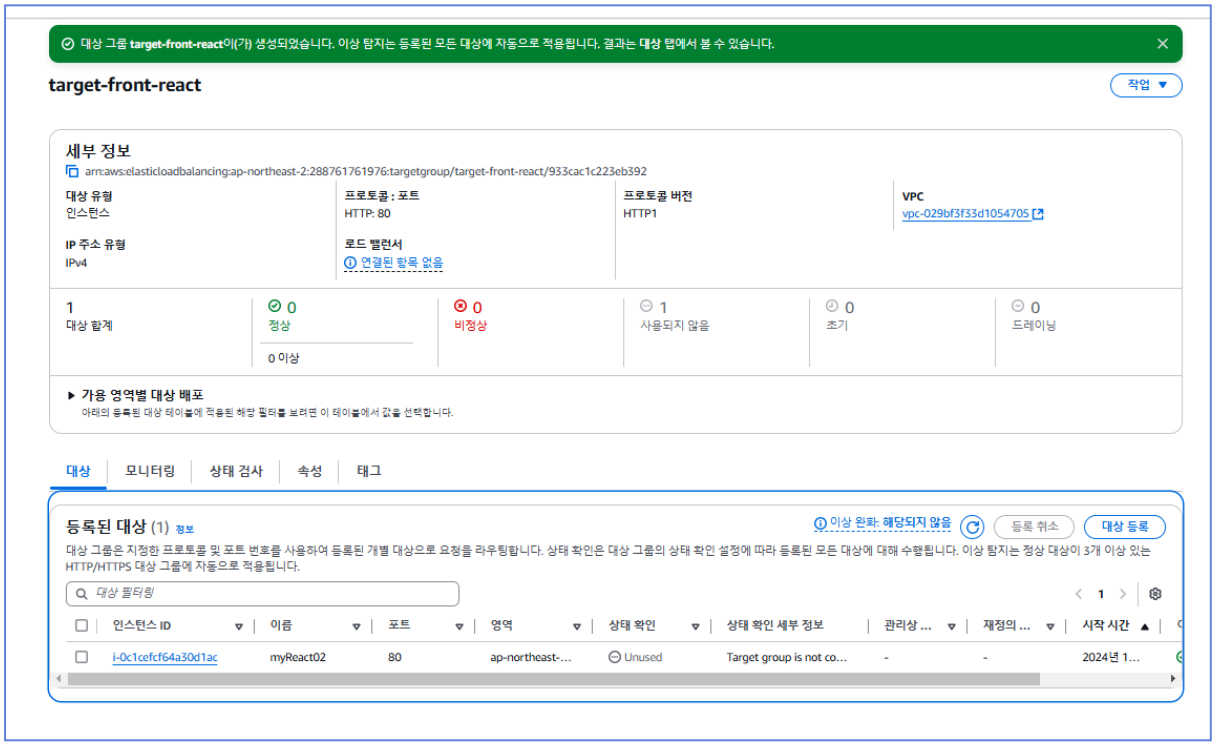


8253jang@daum.net
장희정

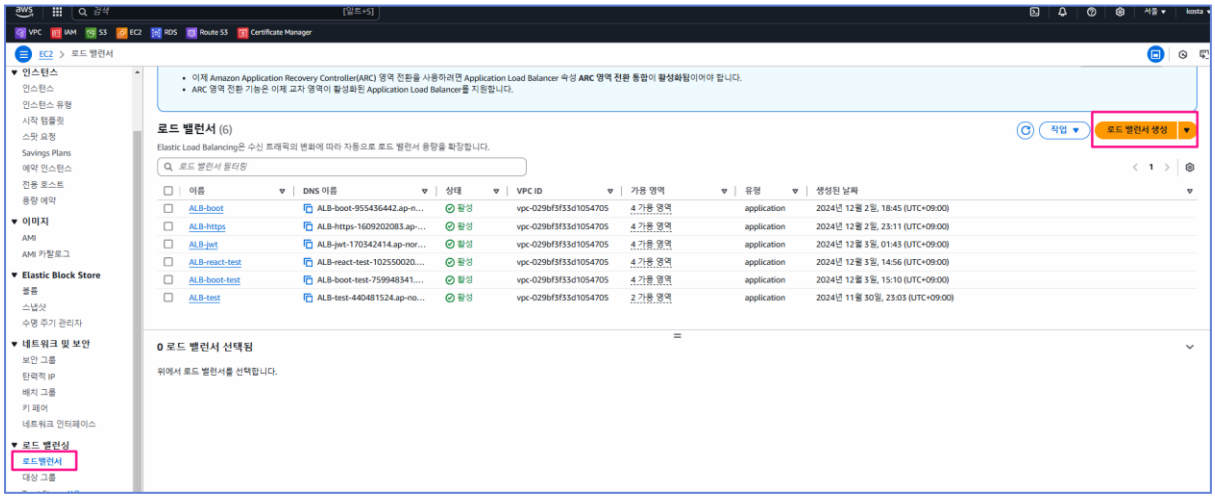




8253jang@daum.net
장희정



왼쪽 메뉴에서 로드밸런싱 > 로드밸런서 클릭 > 로드밸런서 생성



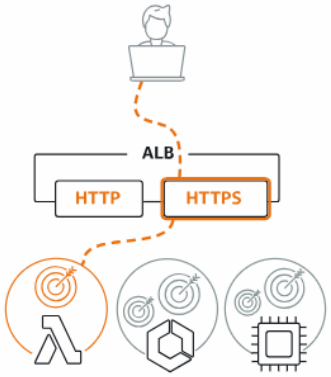
8253jang@daum.net
장희정

로드 밸런서 유형 비교 및 선택

자세한 하이라이트와 함께 전체 기능별 비교도 제공됩니다. 자세히 알아보기

로드 밸런서 유형

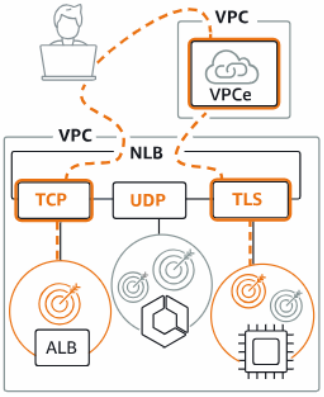
Application Load Balancer 정보



HTTP 및 HTTPS 트래픽을 사용하는 애플리케이션을 위한 유연한 기능이 필요한 경우 Application Load Balancer를 선택합니다. 요청 수준에 따라 작동하는 Application Load Balancer는 마이크로서비스 및 컨테이너를 비롯한 애플리케이션 아키텍처를 대상으로 하는 고급 라우팅 및 표시 기능을 제공합니다.

생성

Network Load Balancer 정보



애플리케이션에 초고성능, 대규모 TLS 오프로딩, 중앙 집중화된 인증서 배포, UDP에 대한 지원 및 고정 IP 주소가 필요한 경우 Network Load Balancer를 선택합니다. 연결 수준에서 작동하는 Network Load Balancer는 안전하게 초당 수백만 개의 요청을 처리하면서도 극히 낮은 지연 시간을 유지할 수 있습니다.

생성

Gateway Load Balancer 정보

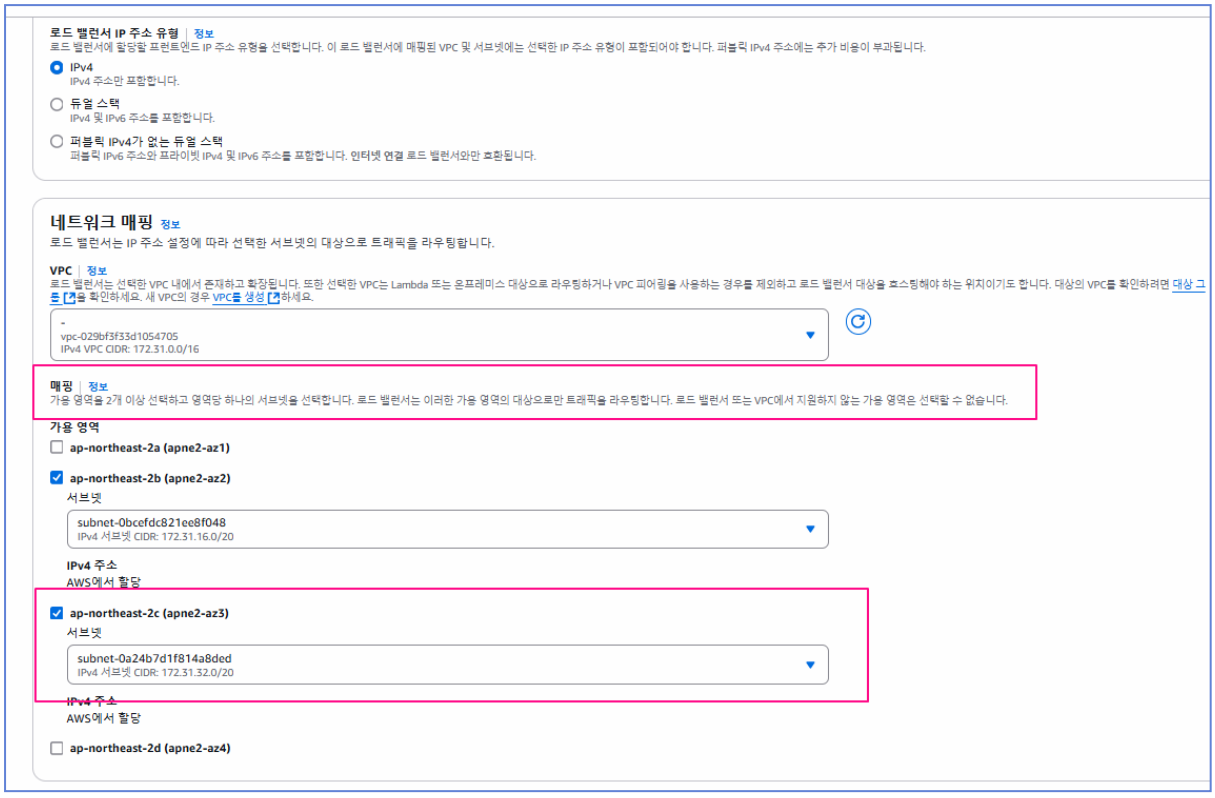
GENEVE를 지원하는 서드 파티 가상 어플라이언스 플릿을 배포 및 관리해야 할 경우 Gateway Load Balancer를 선택합니다. 이러한 어플라이언스를 사용하면 보안, 규정 준수 및 정책 제어를 개선할 수 있습니다.

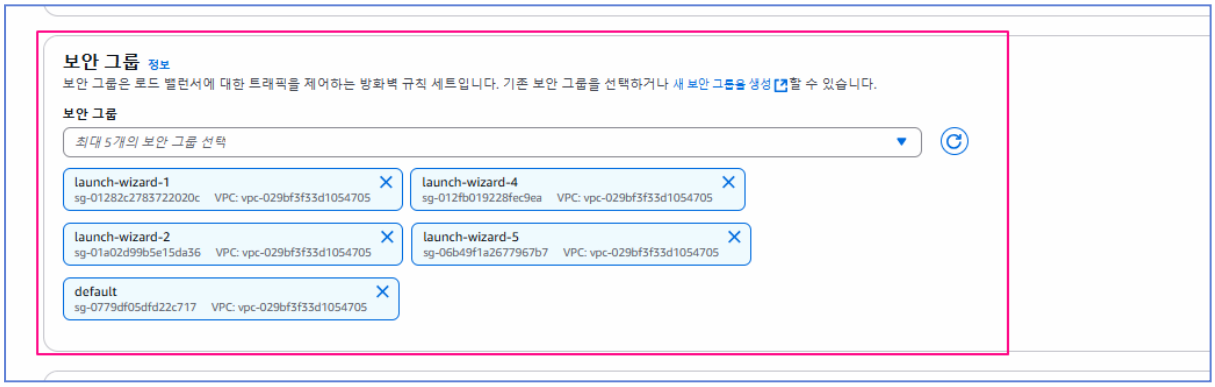
생성

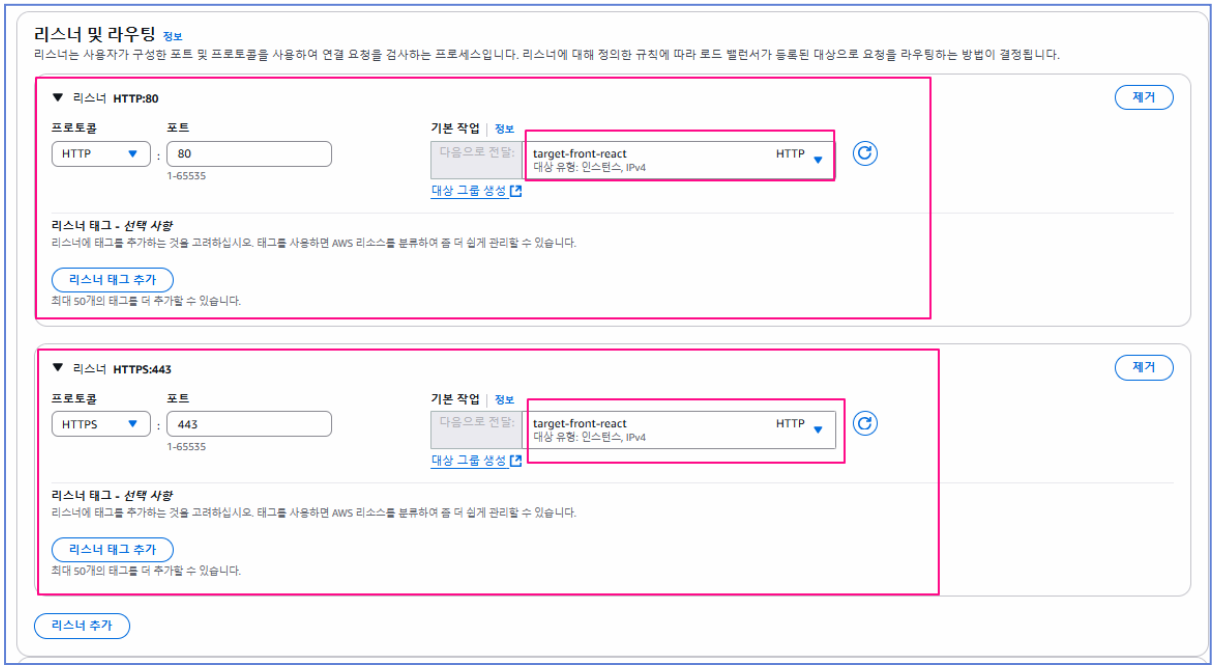
▶ Classic Load Balancer - *이전 세대*

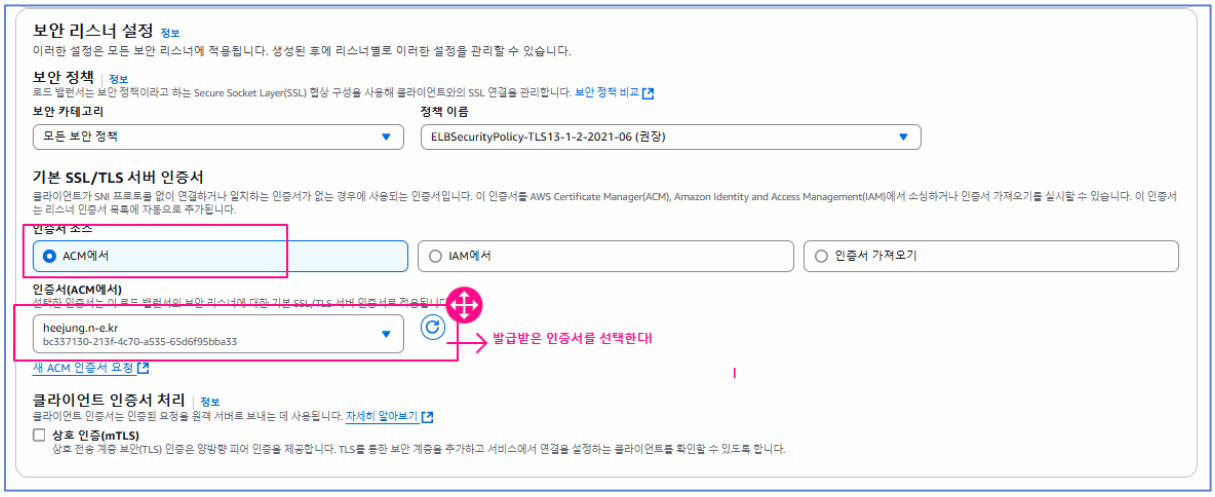
닫기


Application Load Balancer 생성 정보
Application Load Balancer는 수신 HTTP 및 HTTPS 트래픽을 요청 속성을 기반으로 Amazon EC2 인스턴스, 마이크로서비스 및 컨테이너와 같은 여러 대상에 배포합니다. 로드 밸런서는 연결 요청을 수신하면 우선 순위에 따라 리스너
Elastic Load Balancing의 작동 방식
기본 구성
로드 밸런서 이름
ALB-front-react
LB이름을 설정한다.
체계 | 정보
로드 밸런서 생성 후에는 스키마를 변경할 수 없습니다.
인터넷 경계
Serves internet-facing traffic.
Has public IP addresses.
DNS name is publicly resolvable.
Requires a public subnet.
내부
Serves internal traffic.
Has private IP addresses.
DNS name is not publicly resolvable.
IPv4 및 듀얼 스택 IP 주소 유형과 호환됩니다.
로드 밸런서 IP 주소 유형 | 정보
로드 밸런서에 할당할 프런트엔드 IP 주소 유형을 선택합니다. 이 로드 밸런서에 매핑된 VPC 및 서브넷에는 선택한 IP 주소 유형이 포함되어야 합니다. 퍼블릭 IPv4 주소에는 추가 비용이 부과됩니다.
IPv4
IPv4 주소만 포함합니다.
듀얼 스택
IPv4 및 IPv6 주소를 포함합니다.
퍼블릭 IPv4가 없는 듀얼 스택
퍼블릭 IPv6 주소와 프라이빗 IPv4 및 IPv6 주소를 포함합니다. 인터넷 연결 로드 밸런서와만 호환됩니다.
네트워크 매핑 정보
로드 밸런서는 IP 주소 설정에 따라 선택한 서브넷의 대상으로 트래픽을 라우팅합니다.
VPC | 정보
vpc-029bf3f33d1054705
IPv4 VPC CIDR: 172.31.0.0/16
매핑 | 정보
가용 영역을 2개 이상 선택하고 영역당 하나의 서브넷을 선택합니다. 로드 밸런서는 이러한 가용 영역의 대상으로만 트래픽을 라우팅합니다. 로드 밸런서 또는 VPC에서 지원하지 않는 가용 영역은 선택할 수 없습니다.
가용 영역

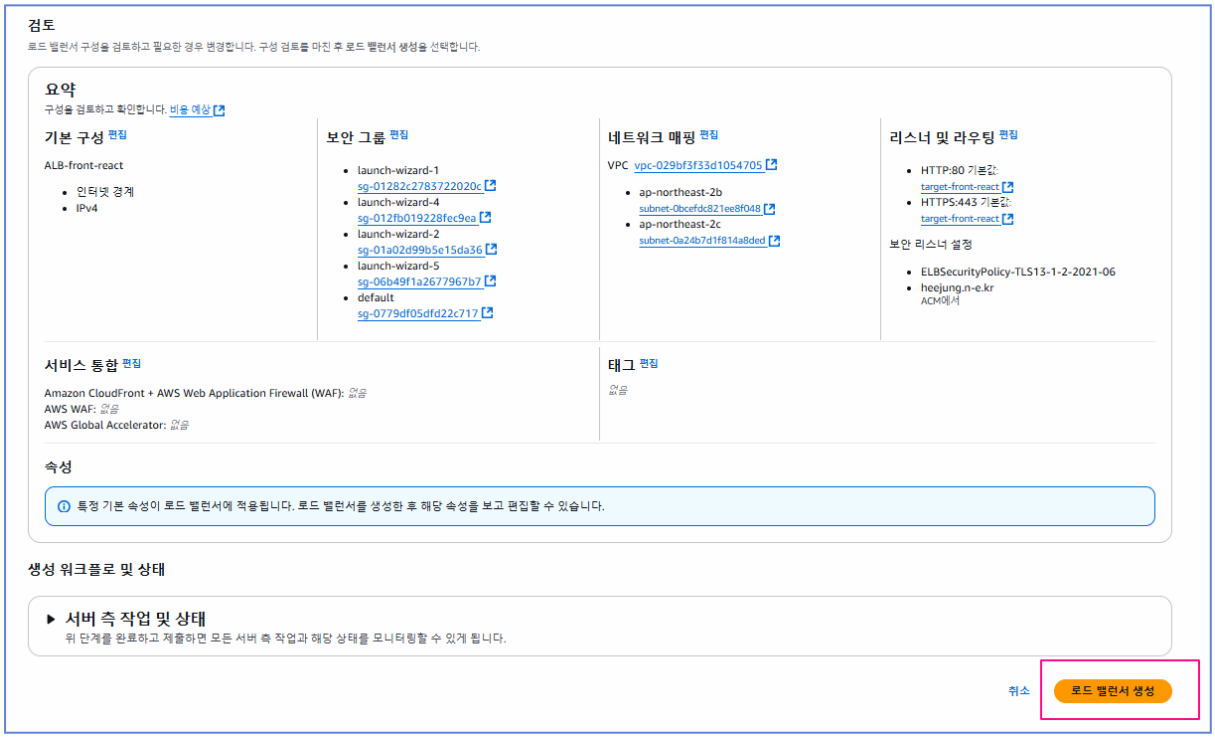

로드 밸런서 IP 주소 유형 | 정보
IPv4
IPv4 주소만 포함합니다.
듀얼 스택
IPv4 및 IPv6 주소를 포함합니다.
퍼블릭 IPv4가 없는 듀얼 스택
퍼블릭 IPv6 주소와 프라이빗 IPv4 및 IPv6 주소를 포함합니다. 인터넷 연결 로드 밸런서와만 호환됩니다.
네트워크 매핑 정보
로드 밸런서는 IP 주소 설정에 따라 선택한 서브넷의 대상으로 트래픽을 라우팅합니다.
VPC | 정보
vpc-029bf3f33d1054705
IPv4 VPC CIDR: 172.31.0.0/16
매핑 | 정보
가용 영역을 2개 이상 선택하고 영역당 하나의 서브넷을 선택합니다. 로드 밸런서는 이러한 가용 영역의 대상으로만 트래픽을 라우팅합니다. 로드 밸런서 또는 VPC에서 지원하지 않는 가용 영역은 선택할 수 없습니다.
가용 영역
ap-northeast-2a (apne2-az1)
ap-northeast-2b (apne2-az2)
서브넷
subnet-0bcefdc821ee8f048
IPv4 서브넷 CIDR: 172.31.16.0/20
IPv4 주소
AWS에서 할당
ap-northeast-2c (apne2-az3)
서브넷
subnet-0a24b7d1f814a8ded
IPv4 서브넷 CIDR: 172.31.32.0/20
IPv4 주소
AWS에서 할당
ap-northeast-2d (apne2-az4)

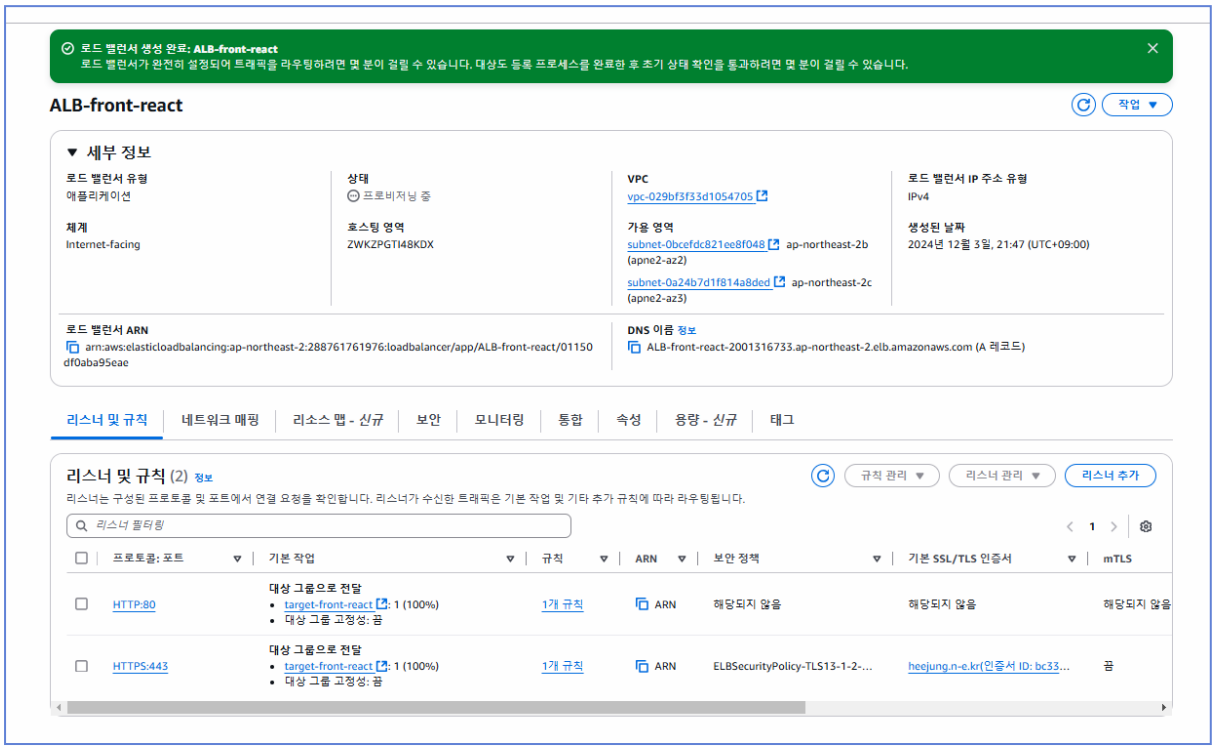

보안 그룹 정보
보안 그룹은 로드 밸런서에 대한 트래픽을 제어하는 방화벽 규칙 세트입니다. 기존 보안 그룹을 선택하거나 새 보안 그룹을 생성할 수 있습니다.
보안 그룹
최대 5개의 보안 그룹 선택
launch-wizard-1
sg-01282c2783722020c VPC: vpc-029bf3f33d1054705
launch-wizard-4
sg-012fb019228fec9ea VPC: vpc-029bf3f33d1054705
launch-wizard-2
sg-01a02d99b5e15da36 VPC: vpc-029bf3f33d1054705
launch-wizard-5
sg-06b49f1a2677967b7 VPC: vpc-029bf3f33d1054705
default
sg-0779df05dfd22c717 VPC: vpc-029bf3f33d1054705


리스너 및 라우팅 정보
리스너는 사용자가 구성한 포트 및 프로토콜을 사용하여 연결 요청을 검사하는 프로세스입니다. 리스너에 대해 정의한 규칙에 따라 로드 밸런서가 등록된 대상으로 요청을 라우팅하는 방법이 결정됩니다.
리스너 HTTP:80
제거
프로토콜
포트
HTTP
80
1-65535
기본 작업 정보
다음으로 전달:
target-front-react
대상 유형: 인스턴스, IPv4
HTTP
대상 그룹 생성
리스너 태그 - 선택 사항
리스너에 태그를 추가하는 것을 고려하십시오. 태그를 사용하면 AWS 리소스를 분류하여 좀 더 쉽게 관리할 수 있습니다.
리스너 태그 추가
최대 50개의 태그를 더 추가할 수 있습니다.
리스너 HTTPS:443
제거
프로토콜
포트
HTTPS
443
1-65535
기본 작업 정보
다음으로 전달:
target-front-react
대상 유형: 인스턴스, IPv4
HTTP
대상 그룹 생성
리스너 태그 - 선택 사항
리스너에 태그를 추가하는 것을 고려하십시오. 태그를 사용하면 AWS 리소스를 분류하여 좀 더 쉽게 관리할 수 있습니다.
리스너 태그 추가
최대 50개의 태그를 더 추가할 수 있습니다.
리스너 추가


보안 리스너 설정 정보
이러한 설정은 모든 보안 리스너에 적용됩니다. 생성된 후에 리스너별로 이러한 설정을 관리할 수 있습니다.
보안 정책 정보
로드 밸런서는 보안 정책이라고 하는 Secure Socket Layer(SSL) 협상 구성을 사용해 클라이언트와의 SSL 연결을 관리합니다. 보안 정책 비교
보안 카테고리
모든 보안 정책
정책 이름
ELBSecurityPolicy-TLS13-1-2-2021-06 (권장)
기본 SSL/TLS 서버 인증서
클라이언트가 SNI 프로토콜 없이 연결하거나 일치하는 인증서가 없는 경우에 사용되는 인증서입니다. 이 인증서를 AWS Certificate Manager(ACM), Amazon Identity and Access Management(IAM)에서 소싱하거나 인증서 가져오기를 실시할 수 있습니다. 이 인증서는 리스너 인증서 목록에 자동으로 추가됩니다.
인증서 소스
ACM에서
IAM에서
인증서 가져오기
인증서(ACM에서)
heejung.n-e.kr
bc337130-213f-4c70-a535-65d6f95bba33
발급받은 인증서를 선택한다
새 ACM 인증서 요청
클라이언트 인증서 처리 정보
클라이언트 인증서는 인증된 요청을 원격 서버로 보내는 데 사용됩니다. 자세히 알아보기
상호 인증(mTLS)
상호 전송 계층 보안(TLS) 인증은 양방향 피어 인증을 제공합니다. TLS를 통한 보안 계층을 추가하고 서비스에서 연결을 설정하는 클라이언트를 확인할 수 있도록 합니다.

8253jang@daum.net
장희정

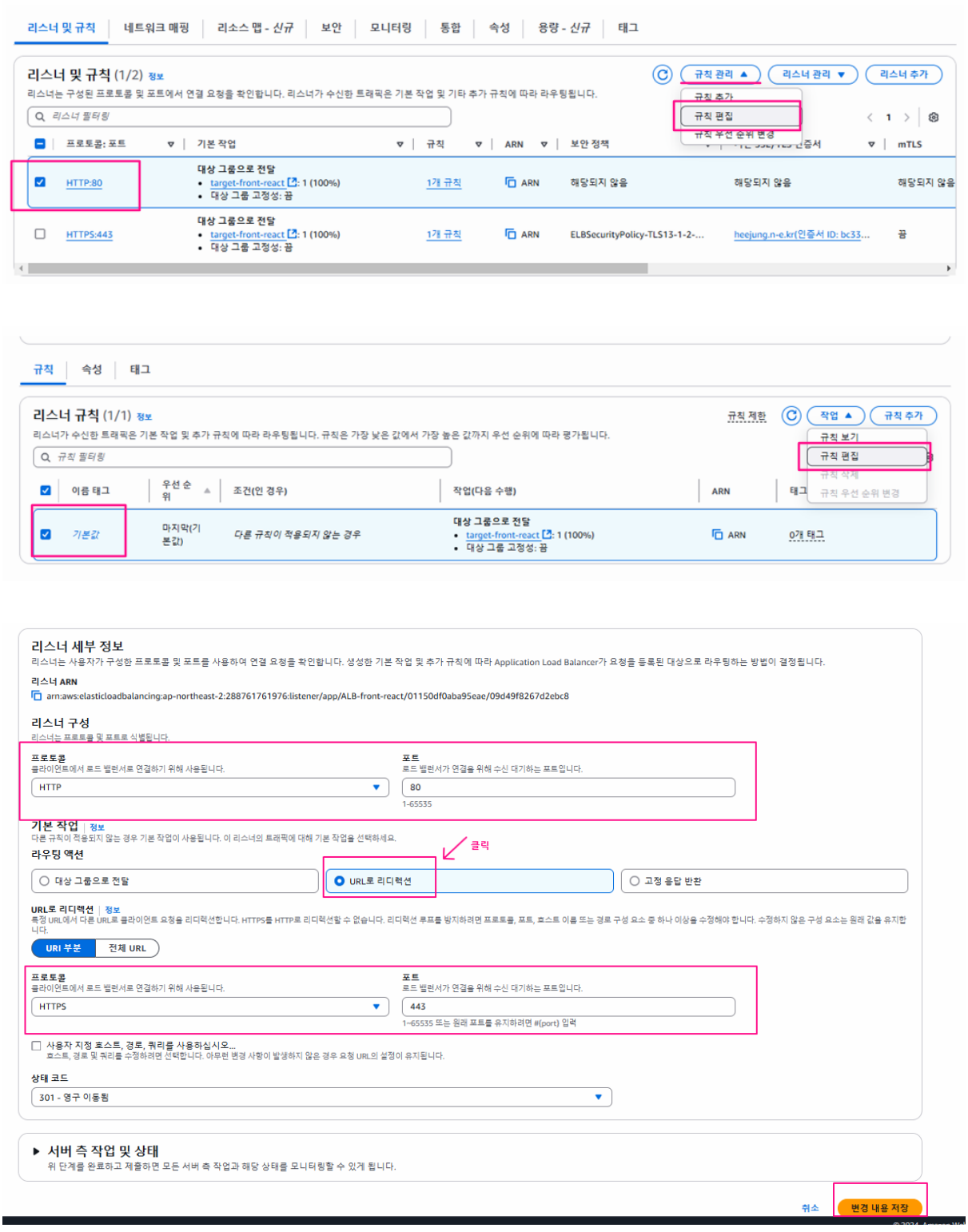




위 화면에서 http:80을 선택 하고 규칙관리 > 규칙편집을 클릭한다.

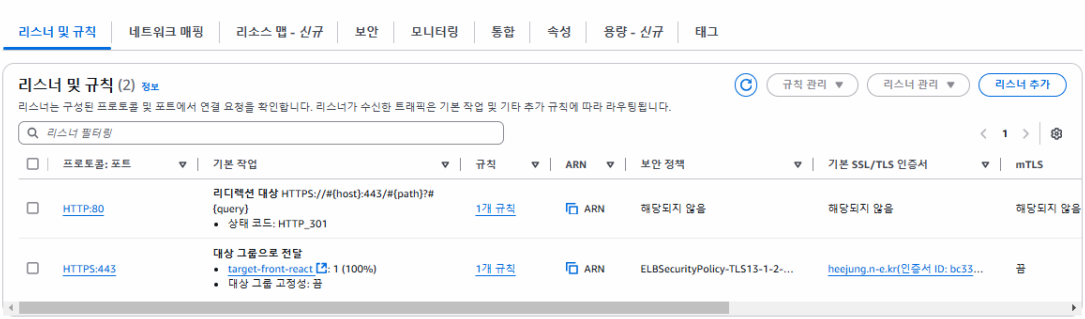
: http로 요청을 하더라도 https로 요청이 될 수 있도록 설정이 필요하다.

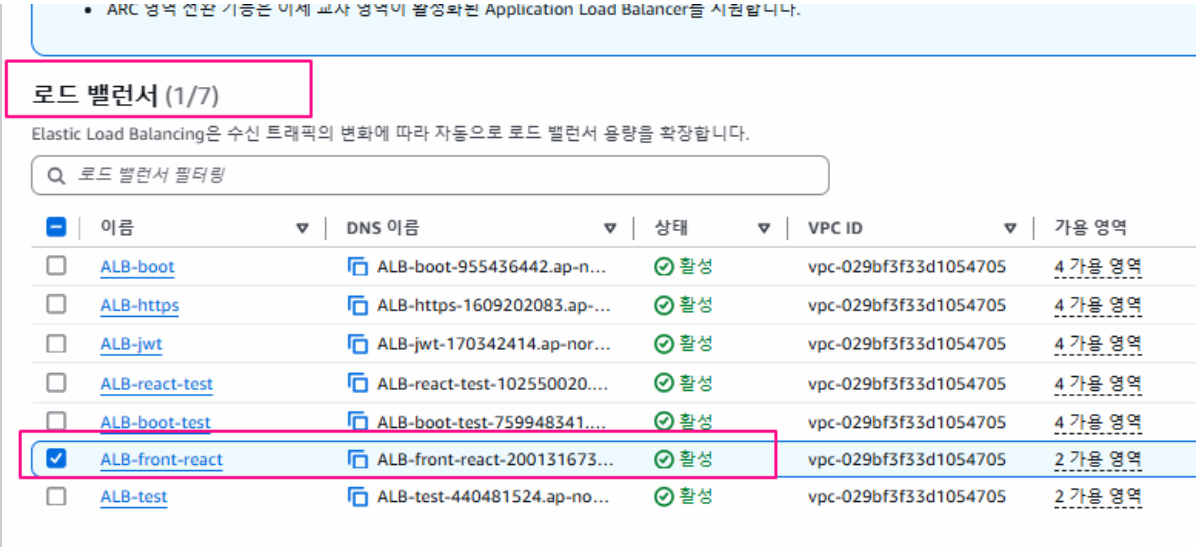
8253jang@daum.net
장희정



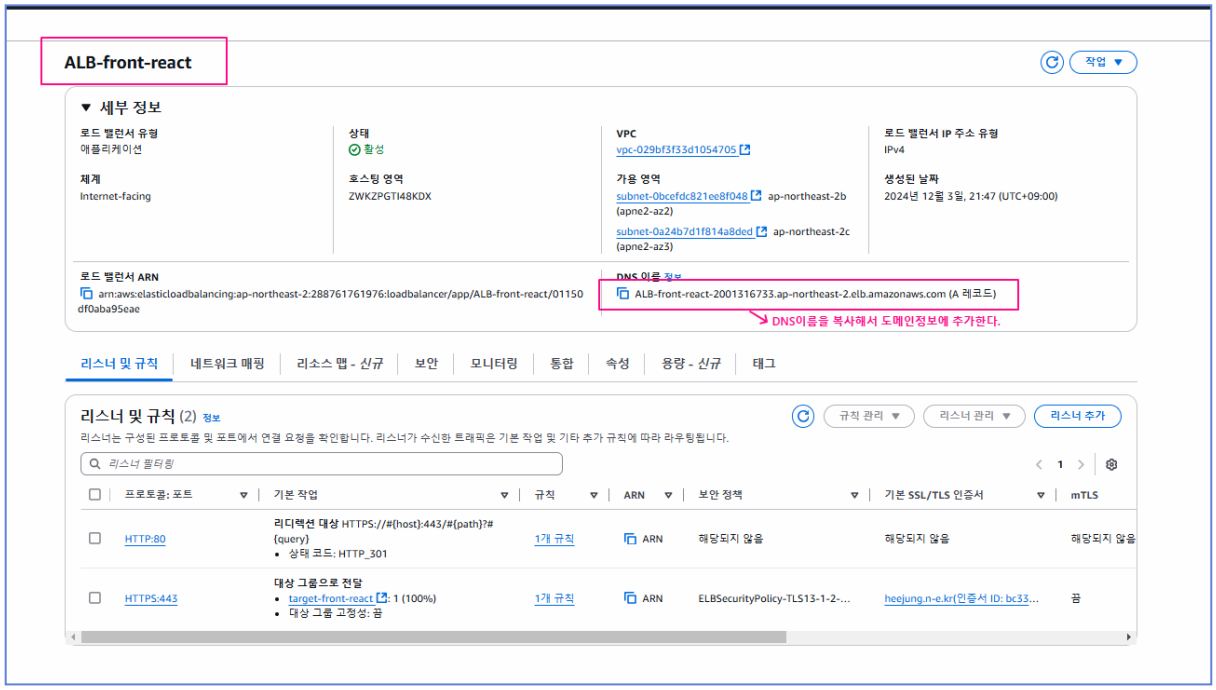
설정이 완료 된 후에 로드밸런서를 클릭해서 확인해본다.

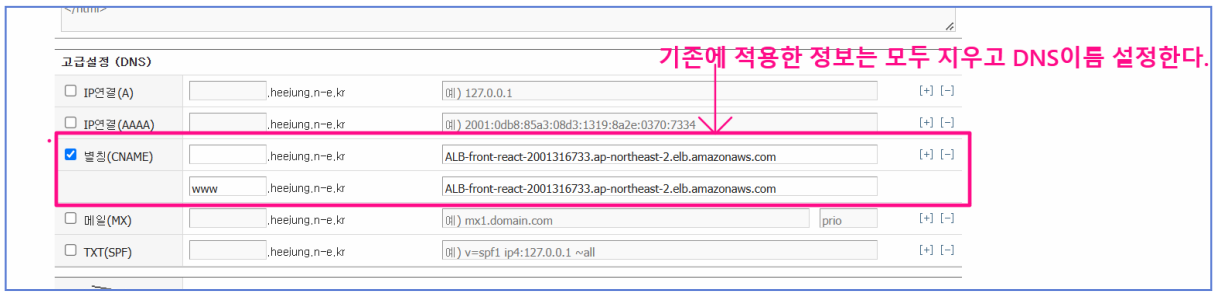
8253jang@daum.net
장희정

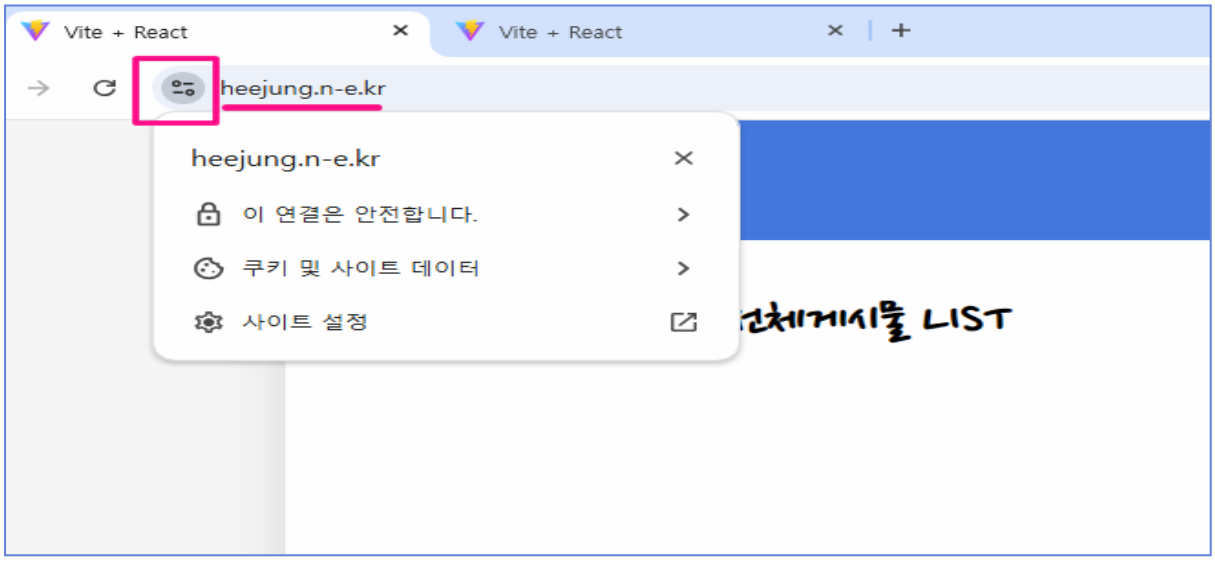




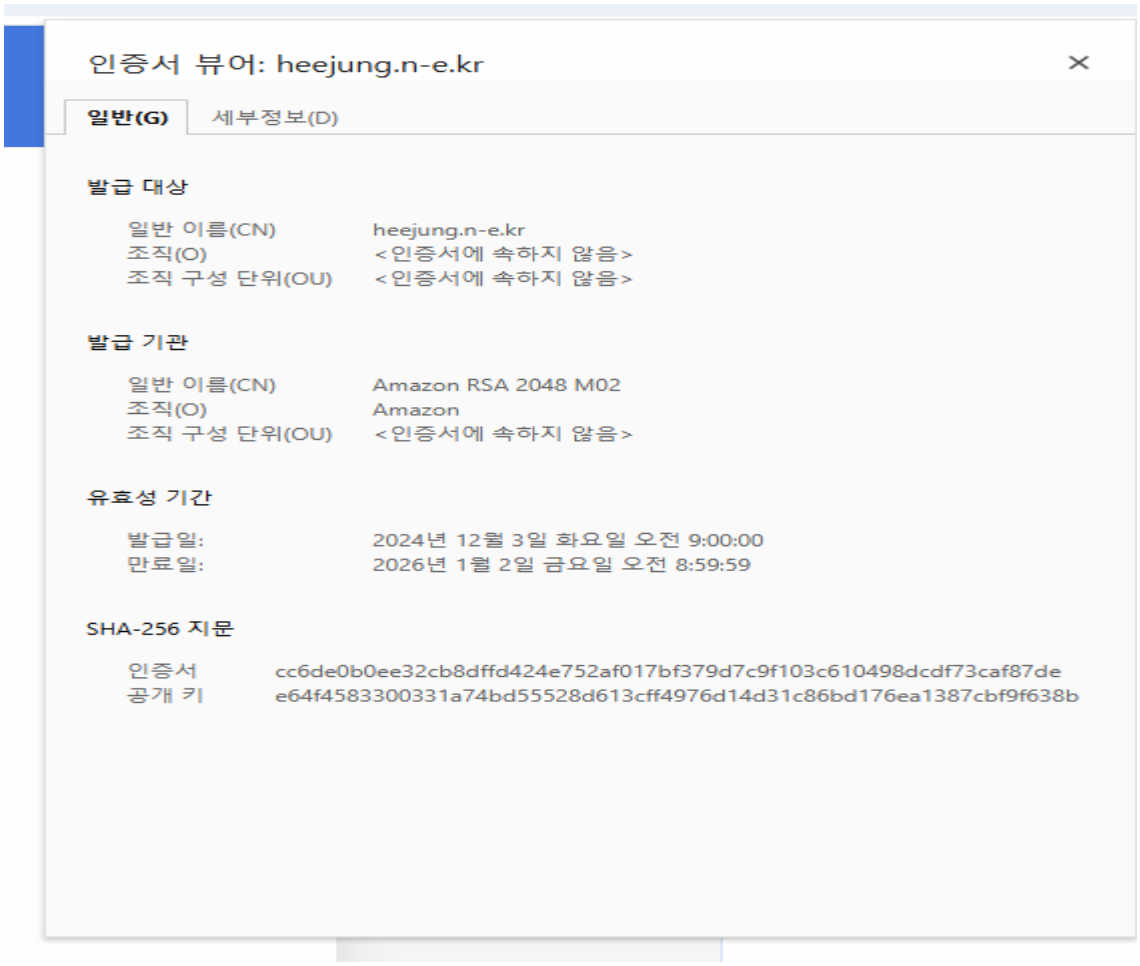
"내도메인한국" 접속해서 도메인정보를 수정한다.







"위의 이 연결은안전합니다." 클릭 > "인증서가 유효함" 클릭



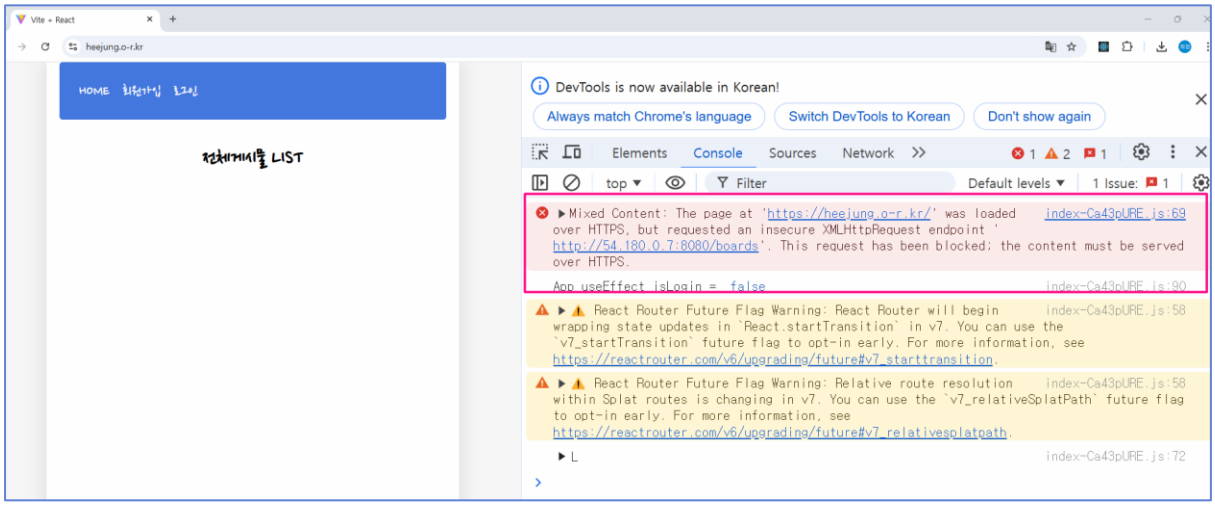
url주소를 복사해서 보면 아래처럼 https로 요청된 것을 볼 수 있다.

https://heejung.n-e.kr/

그러나,

backend Spring관련 데이터를 가져오지 못했다.!!!

개발자도구를 클릭하여 콘솔에 오류를 확인해보자.



이 에러는 **Mixed Content** 문제로, 웹 페이지가 **HTTPS** 프로토콜을 사용하여 로드되었지만, 페이지 내에서 **HTTP** 프로토콜을 사용하는 리소스를 요청했을 때 발생한다. **브라우저는 보안을 위해 HTTPS 페이지에서 HTTP 리소스를 불러오는 것을 차단한다.**

문제의 원인

URL 이 https:/heejung.n-e.kr/로 시작하는 웹 페이지는 HTTPS(보안 연결)를 사용해 로드되고 있지만 XMLHttpRequest 가 HTTP 로 요청되었다. 요청을 보내는 엔드포인트인 http://54.180.0.7:8080/boards 는 HTTP 로 시작한다. 이는 보안이 없는 연결로, HTTPS 페이지에서 이 리소스를 요청하면 보안상의 이유로 브라우저가 이를 차단한다.

.

왜 차단되는가?

- **HTTPS** 웹사이트는 데이터 전송을 암호화하고 보안성을 제공하기 위해 사용된다.
- 만약 HTTPS 페이지에서 HTTP 로 리소스를 요청하면, 그 요청은 암호화되지 않으며 중간에서 가로채어질 수 있는 위험이 존재한다.
- 브라우저는 이러한 보안상의 위험을 막기 위해 **Mixed Content** 를 차단한다.

해결 방법

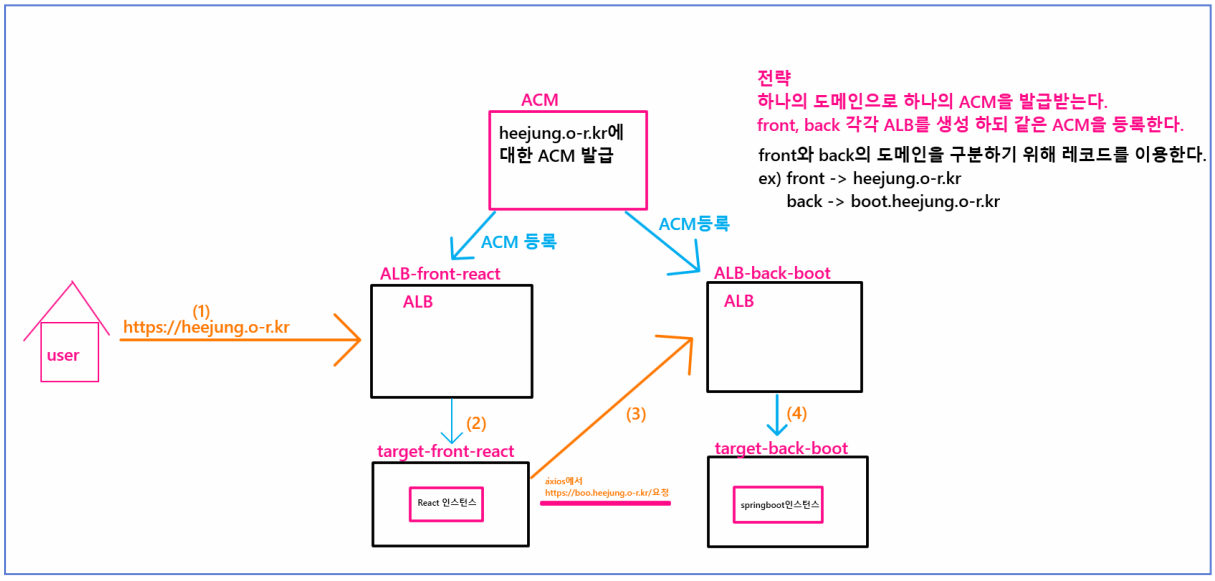
1. **HTTP 요청을 HTTPS 로 변경**:
    - 가능한 경우, http://54.180.0.7:8080/boards 엔드포인트를 HTTPS 로 변경하는 것이 가장 좋은 해결책이다.
    - 서버가 HTTPS 를 지원하도록 설정하고, 요청 URL 을 https://3.34.71.73:9000/boards 로 수정한다.

2. **서버에 SSL 인증서 적용**:
   - 엔드포인트인 http://54.180.0.7:8080/boards 가 SSL 을 지원하지 않는다면, 서버에 SSL 인증서를 설치하여 HTTPS 요청을 처리할 수 있도록 설정해야 한다.
3. **리디렉션 설정**:
   - HTTP 요청을 HTTPS 로 자동 리디렉션하는 방법도있다. 서버가 HTTP 로 들어오는 요청을 HTTPS 로 리디렉션할 수 있도록 설정하는 것이다.
   - 예를 들어, http://54.180.0.7:8080/boards 로 들어오는 모든 요청을 https://54.180.0.7:8080/boards 으로 리디렉션하도록 서버 설정을 변경한다.
4. **프론트엔드 수정**:
   - 클라이언트 측에서 요청을 보내는 URL 을 https://로 수정할 수도 있다. 즉, API 요청을 보내는 코드에서 HTTP 대신 HTTPS 를 사용하도록 한다.

결론

웹 페이지가 HTTPS 로 로드되었을 때, 모든 리소스와 API 요청 또한 HTTPS 로 이루어져야 한다. 이를 통해 **Mixed Content** 문제를 해결할 수 있으며, 페이지의 보안성을 유지할 수 있다.

우리의 해결 방법



이름규칙

	ALB이름	target그룹 이름	인스턴스
Front	ALB-front-react	target-front-react	React 인스턴스
back	ALB-back-boot	target-back-boot	Springboot 인스턴스

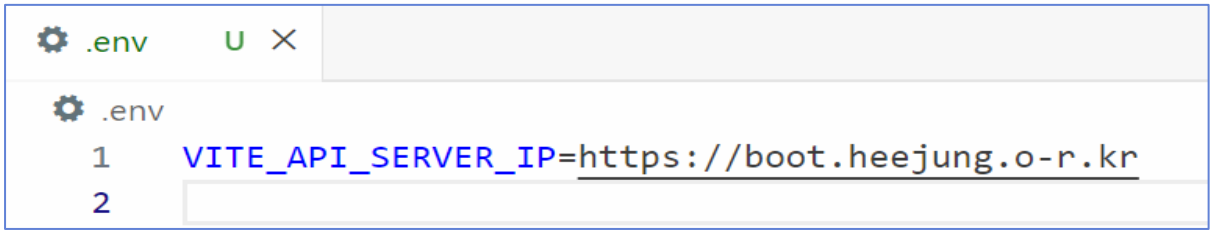
8253jang@daum.net
장희정

Front의 ALB세팅은 되었으니

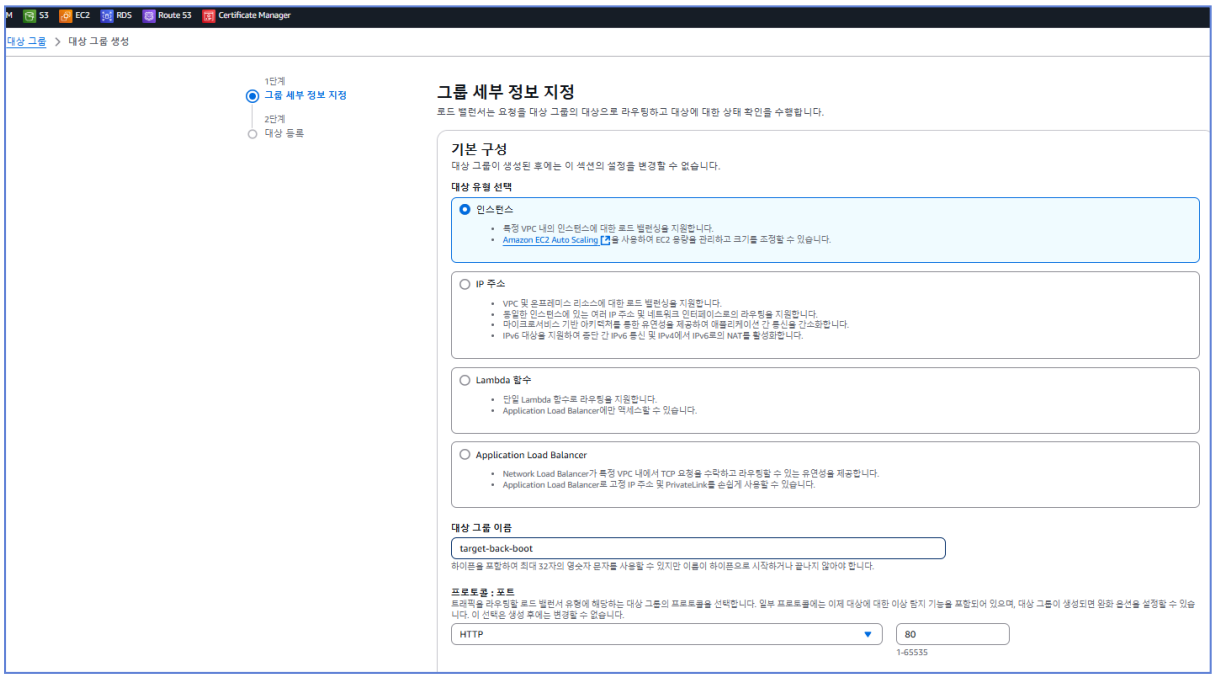
1)back에 해당하는 타켓그룹 생성 하고 ALB를 생성한다.

2) "내도메인한국"에 접속해서 도메인수정한다.

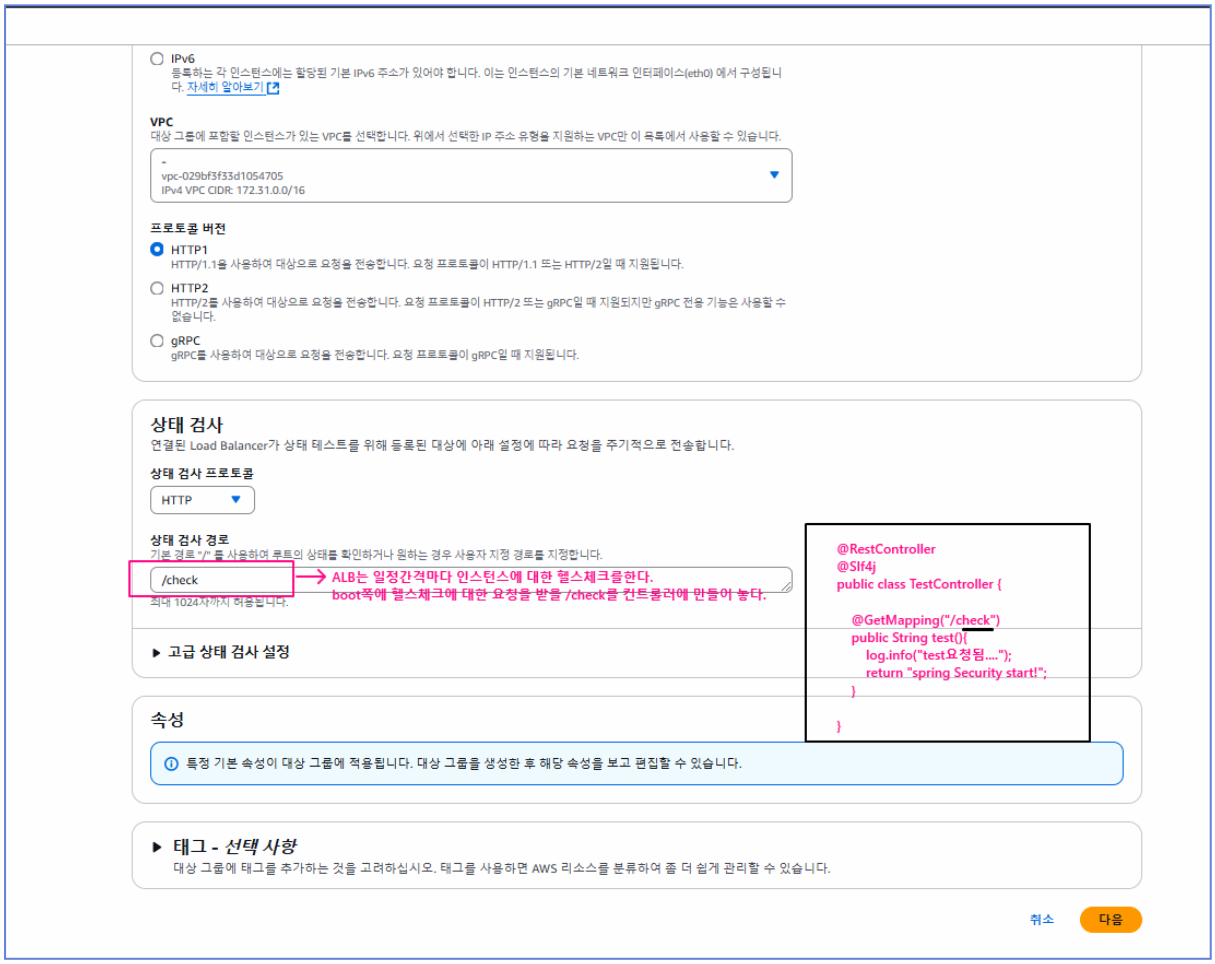
3)React 개발소스에서 .env의 파일을 아래와 같이 수정한다.

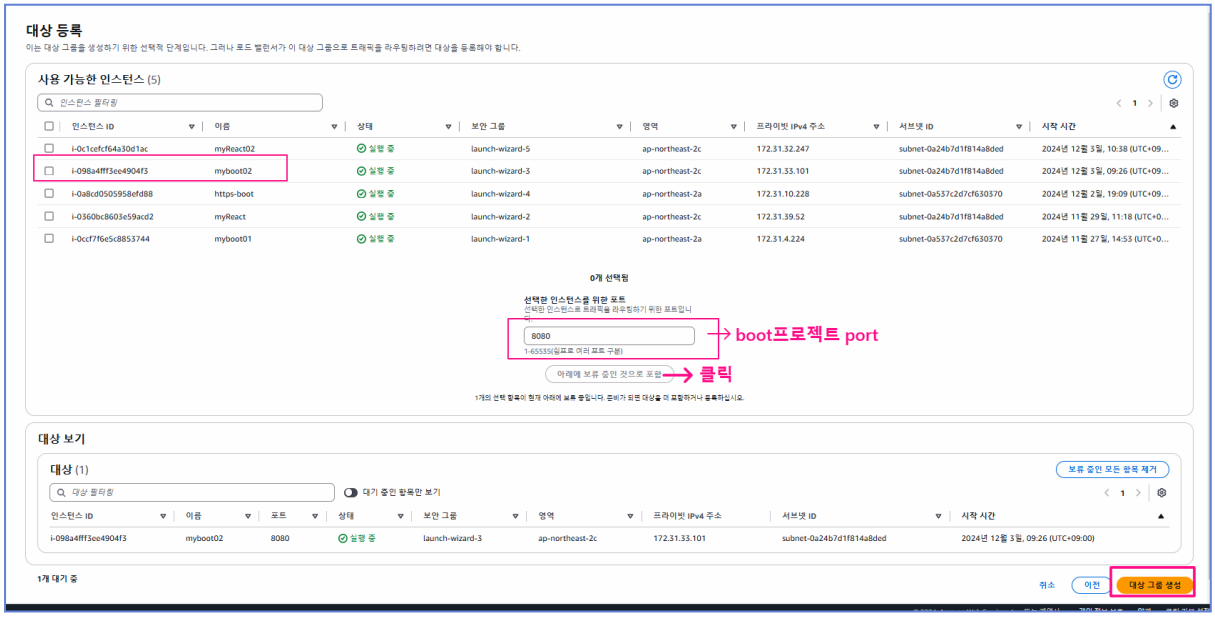


4)개발소스 build > git push > 인스턴스접속 > git clone > 파일이동 > nginx restart 한다.



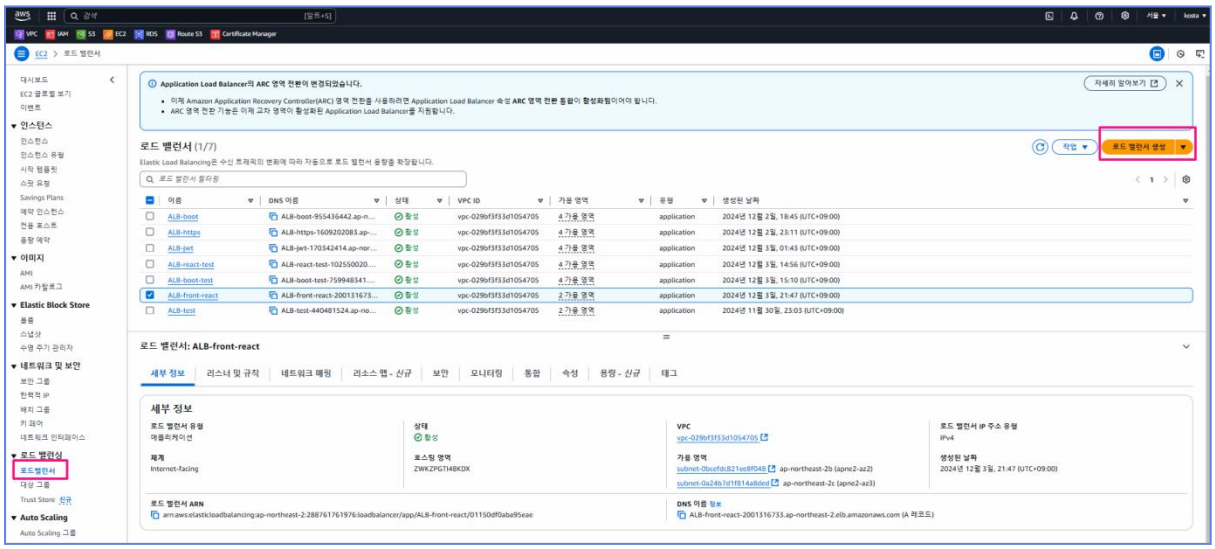
8253jang@daum.net
장희정

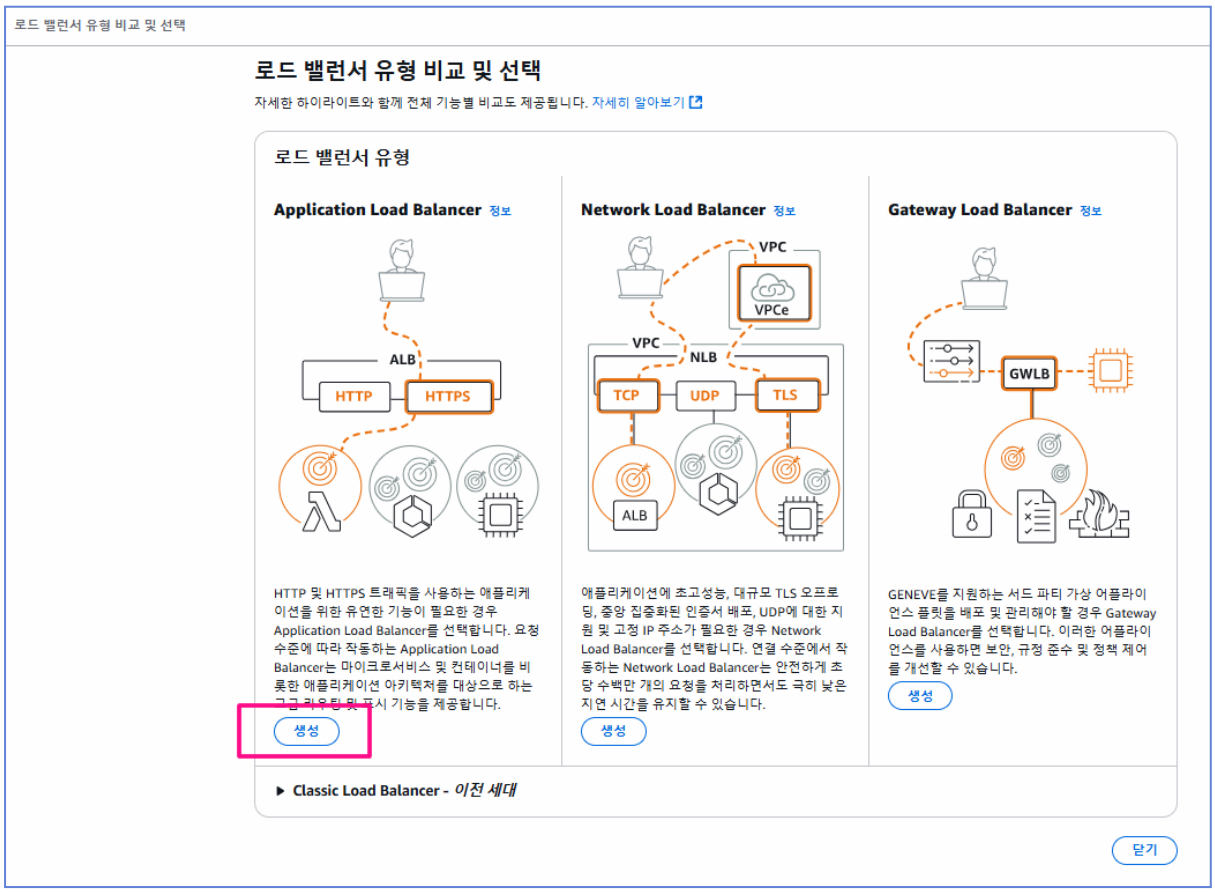


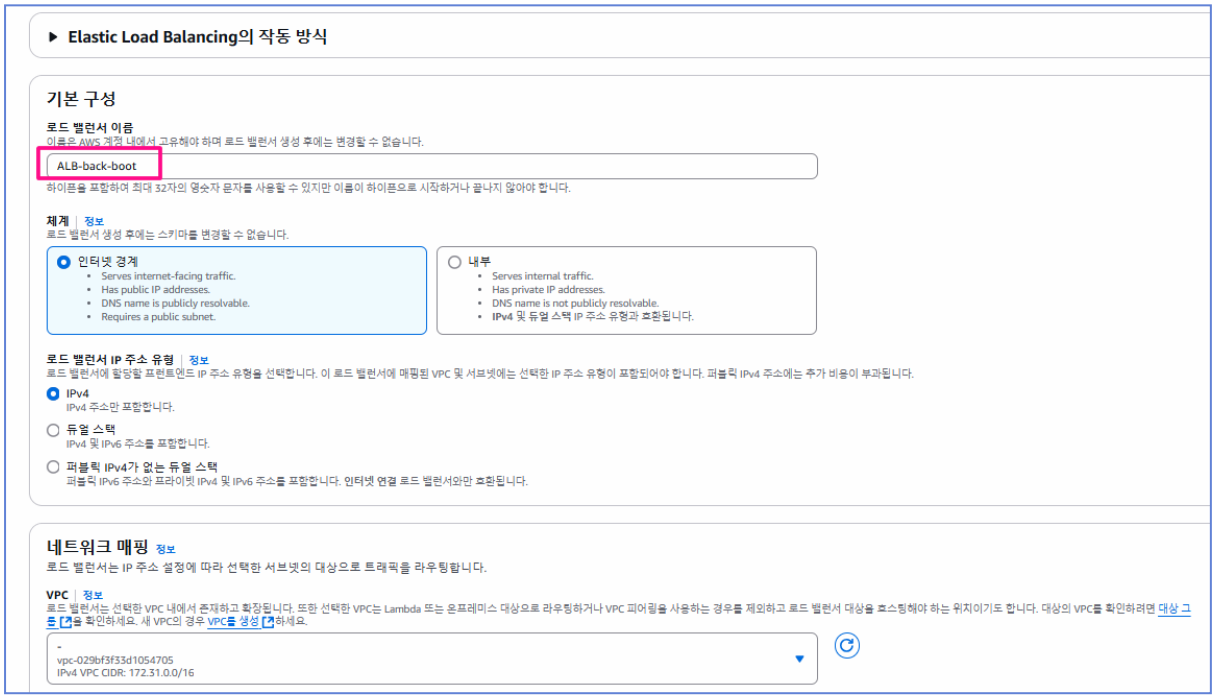


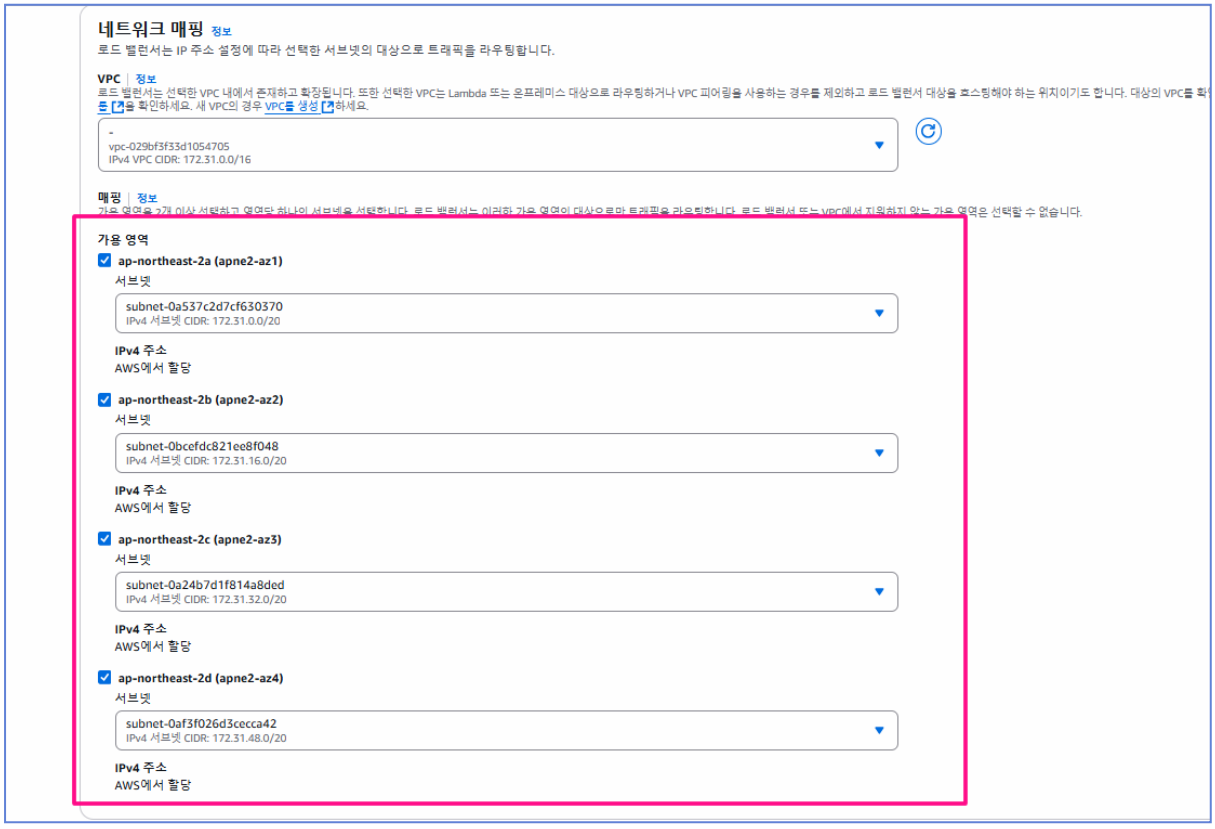
8253jang@daum.net
장희정

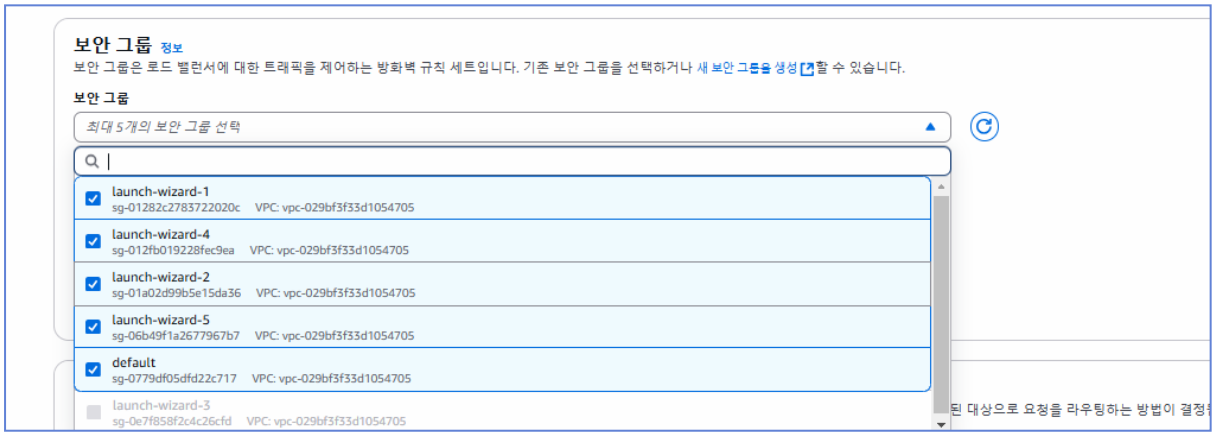
LB생성하기

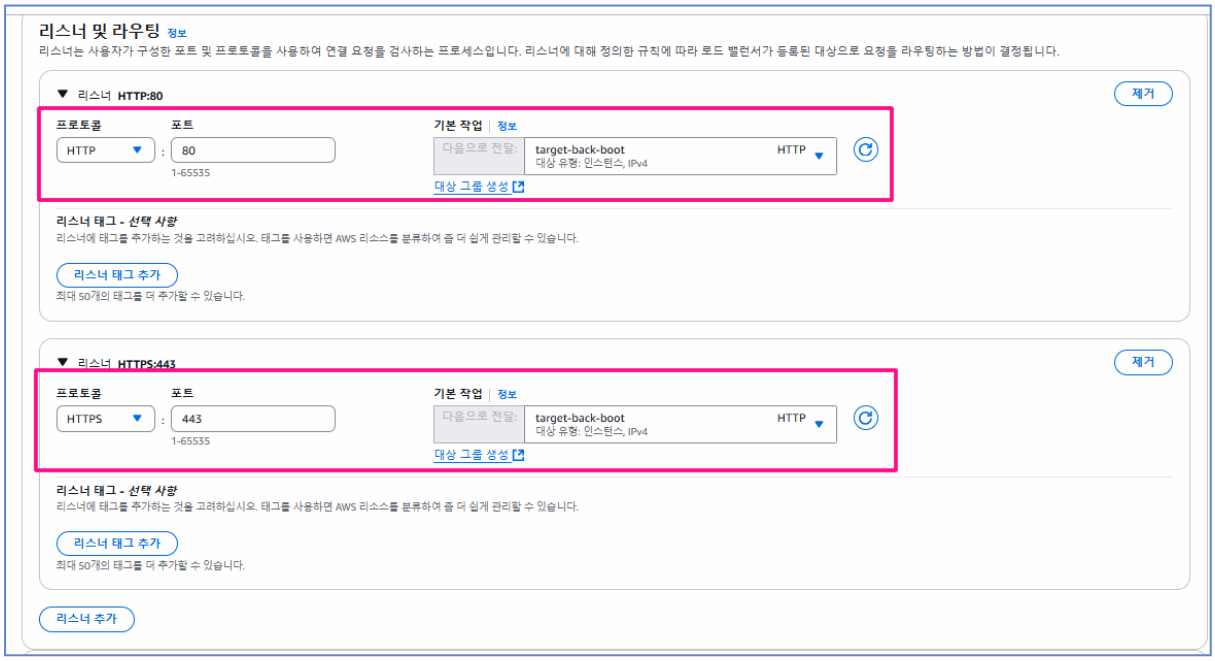


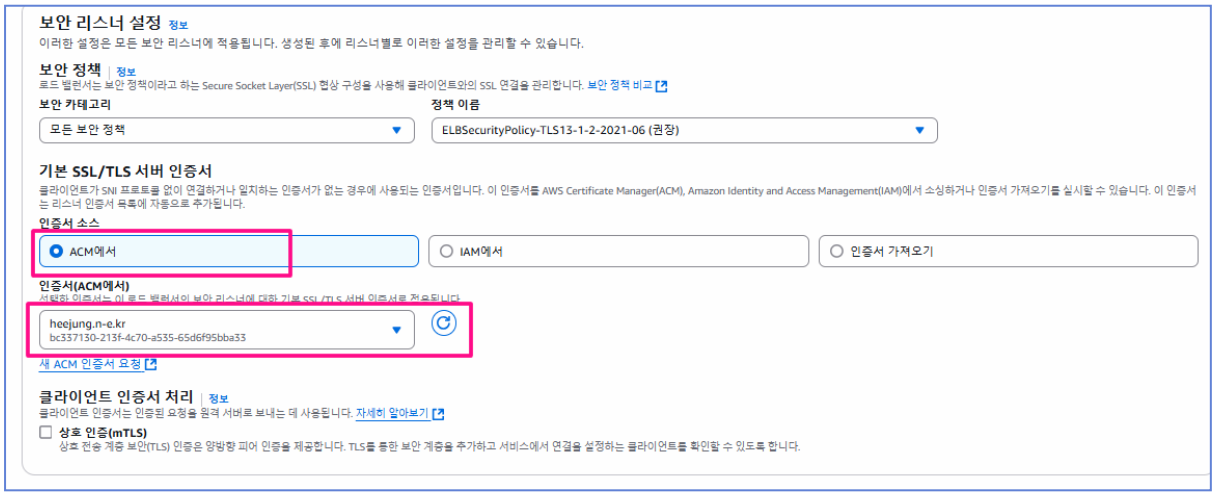


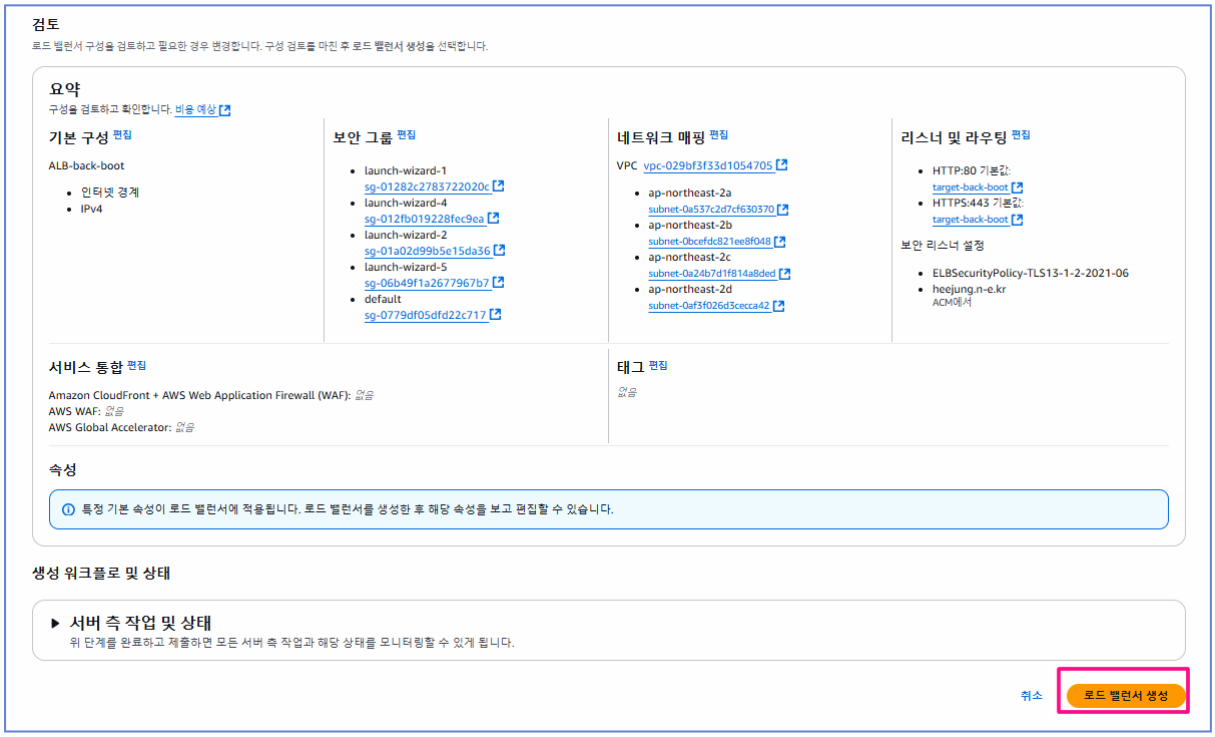

Elastic Load Balancing의 작동 방식
기본 구성
로드 밸런서 이름
이름은 AWS 계정 내에서 고유해야 하며 로드 밸런서 생성 후에는 변경할 수 없습니다.
ALB-back-boot
하이픈을 포함하여 최대 32자의 영숫자 문자를 사용할 수 있지만 이름이 하이픈으로 시작하거나 끝나지 않아야 합니다.
체계 | 정보
로드 밸런서 생성 후에는 스키마를 변경할 수 없습니다.
인터넷 경계
Serves internet-facing traffic.
Has public IP addresses.
DNS name is publicly resolvable.
Requires a public subnet.
내부
Serves internal traffic.
Has private IP addresses.
DNS name is not publicly resolvable.
IPv4 및 듀얼 스택 IP 주소 유형과 호환됩니다.
로드 밸런서 IP 주소 유형 | 정보
로드 밸런서에 할당할 프런트엔드 IP 주소 유형을 선택합니다. 이 로드 밸런서에 매핑된 VPC 및 서브넷에는 선택한 IP 주소 유형이 포함되어야 합니다. 퍼블릭 IPv4 주소에는 추가 비용이 부과됩니다.
IPv4
IPv4 주소만 포함합니다.
듀얼 스택
IPv4 및 IPv6 주소를 포함합니다.
퍼블릭 IPv4가 없는 듀얼 스택
퍼블릭 IPv6 주소와 프라이빗 IPv4 및 IPv6 주소를 포함합니다. 인터넷 연결 로드 밸런서와만 호환됩니다.
네트워크 매핑 정보
로드 밸런서는 IP 주소 설정에 따라 선택한 서브넷의 대상으로 트래픽을 라우팅합니다.
VPC | 정보
로드 밸런서는 선택한 VPC 내에서 존재하고 확장됩니다. 또한 선택한 VPC는 Lambda 또는 온프레미스 대상으로 라우팅하거나 VPC 피어링을 사용하는 경우를 제외하고 로드 밸런서 대상을 호스팅해야 하는 위치이기도 합니다. 대상의 VPC를 확인하려면 대상 그
룹을 확인하세요. 새 VPC의 경우 VPC를 생성하세요.
-
vpc-029bf3f33d1054705
IPv4 VPC CIDR: 172.31.0.0/16


네트워크 매핑 정보
로드 밸런서는 IP 주소 설정에 따라 선택한 서브넷의 대상으로 트래픽을 라우팅합니다.
VPC | 정보
-
vpc-029bf3f33d1054705
IPv4 VPC CIDR: 172.31.0.0/16
매핑 | 정보
가용 영역
ap-northeast-2a (apne2-az1)
서브넷
subnet-0a537c2d7cf630370
IPv4 서브넷 CIDR: 172.31.0.0/20
IPv4 주소
AWS에서 할당
ap-northeast-2b (apne2-az2)
서브넷
subnet-0bcefdc821ee8f048
IPv4 서브넷 CIDR: 172.31.16.0/20
IPv4 주소
AWS에서 할당
ap-northeast-2c (apne2-az3)
서브넷
subnet-0a24b7d1f814a8ded
IPv4 서브넷 CIDR: 172.31.32.0/20
IPv4 주소
AWS에서 할당
ap-northeast-2d (apne2-az4)
서브넷
subnet-0af3f026d3cecca42
IPv4 서브넷 CIDR: 172.31.48.0/20
IPv4 주소
AWS에서 할당

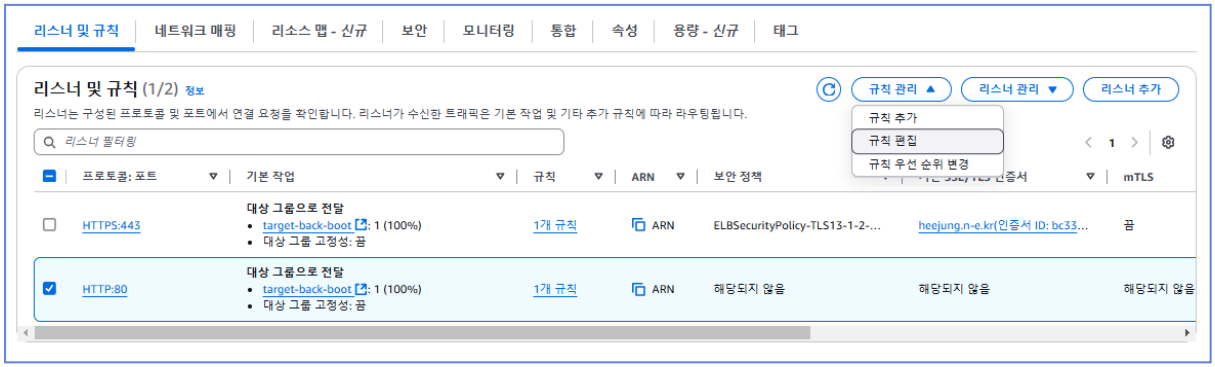

보안 그룹 정보
보안 그룹은 로드 밸런서에 대한 트래픽을 제어하는 방화벽 규칙 세트입니다. 기존 보안 그룹을 선택하거나 새 보안 그룹을 생성할 수 있습니다.
보안 그룹
최대 5개의 보안 그룹 선택
launch-wizard-1
sg-01282c2783722020c VPC: vpc-029bf3f33d1054705
launch-wizard-4
sg-012fb019228fec9ea VPC: vpc-029bf3f33d1054705
launch-wizard-2
sg-01a02d99b5e15da36 VPC: vpc-029bf3f33d1054705
launch-wizard-5
sg-06b49f1a2677967b7 VPC: vpc-029bf3f33d1054705
default
sg-0779df05dfd22c717 VPC: vpc-029bf3f33d1054705
launch-wizard-3
sg-0e7f858f2c4c26cfd VPC: vpc-029bf3f33d1054705

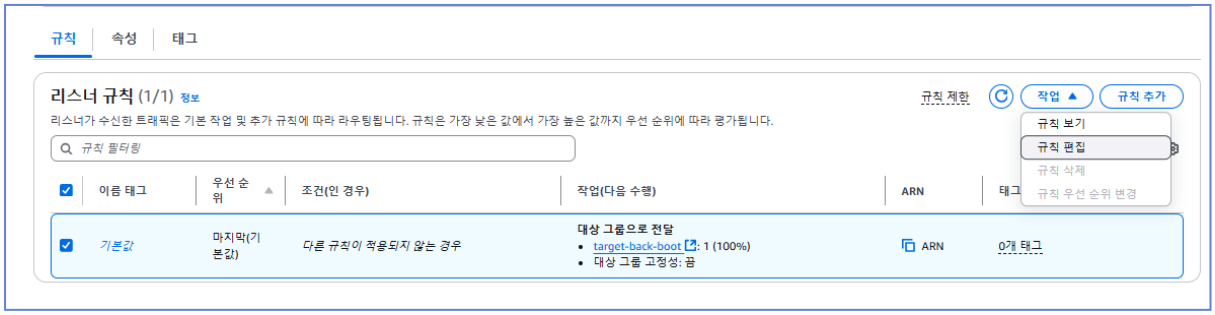

리스너 및 라우팅 정보
리스너는 사용자가 구성한 포트 및 프로토콜을 사용하여 연결 요청을 검사하는 프로세스입니다. 리스너에 대해 정의한 규칙에 따라 로드 밸런서가 등록된 대상으로 요청을 라우팅하는 방법이 결정됩니다.
리스너 HTTP:80
제거
프로토콜
포트
HTTP
80
1-65535
기본 작업 정보
다음으로 전달:
target-back-boot
HTTP
대상 유형: 인스턴스, IPv4
대상 그룹 생성
리스너 태그 - 선택 사항
리스너에 태그를 추가하는 것을 고려하십시오. 태그를 사용하면 AWS 리소스를 분류하여 좀 더 쉽게 관리할 수 있습니다.
리스너 태그 추가
최대 50개의 태그를 더 추가할 수 있습니다.
리스너 HTTPS:443
제거
프로토콜
포트
HTTPS
443
1-65535
기본 작업 정보
다음으로 전달:
target-back-boot
HTTP
대상 유형: 인스턴스, IPv4
대상 그룹 생성
리스너 태그 - 선택 사항
리스너에 태그를 추가하는 것을 고려하십시오. 태그를 사용하면 AWS 리소스를 분류하여 좀 더 쉽게 관리할 수 있습니다.
리스너 태그 추가
최대 50개의 태그를 더 추가할 수 있습니다.
리스너 추가


보안 리스너 설정 정보
이러한 설정은 모든 보안 리스너에 적용됩니다. 생성된 후에 리스너별로 이러한 설정을 관리할 수 있습니다.
보안 정책 정보
로드 밸런서는 보안 정책이라고 하는 Secure Socket Layer(SSL) 협상 구성을 사용해 클라이언트와의 SSL 연결을 관리합니다. 보안 정책 비교
보안 카테고리
모든 보안 정책
정책 이름
ELBSecurityPolicy-TLS13-1-2-2021-06 (권장)
기본 SSL/TLS 서버 인증서
클라이언트가 SNI 프로토콜 없이 연결하거나 일치하는 인증서가 없는 경우에 사용되는 인증서입니다. 이 인증서를 AWS Certificate Manager(ACM), Amazon Identity and Access Management(IAM)에서 소싱하거나 인증서 가져오기를 실시할 수 있습니다. 이 인증서는 리스너 인증서 목록에 자동으로 추가됩니다.
인증서 소스
ACM에서
IAM에서
인증서 가져오기
인증서(ACM에서)
선택한 인증서는 이 로드 밸런서의 보안 리스너에 대한 기본 SSL/TLS 서버 인증서로 배포됩니다.
heejung.n-e.kr
bc337130-213f-4c70-a535-65d6f95bba33
새 ACM 인증서 요청
클라이언트 인증서 처리 정보
클라이언트 인증서는 인증된 요청을 원격 서버로 보내는 데 사용됩니다. 자세히 알아보기
상호 인증(mTLS)
상호 전송 계층 보안(TLS) 인증은 양방향 피어 인증을 제공합니다. TLS를 통한 보안 계층을 추가하고 서비스에서 연결을 설정하는 클라이언트를 확인할 수 있도록 합니다.

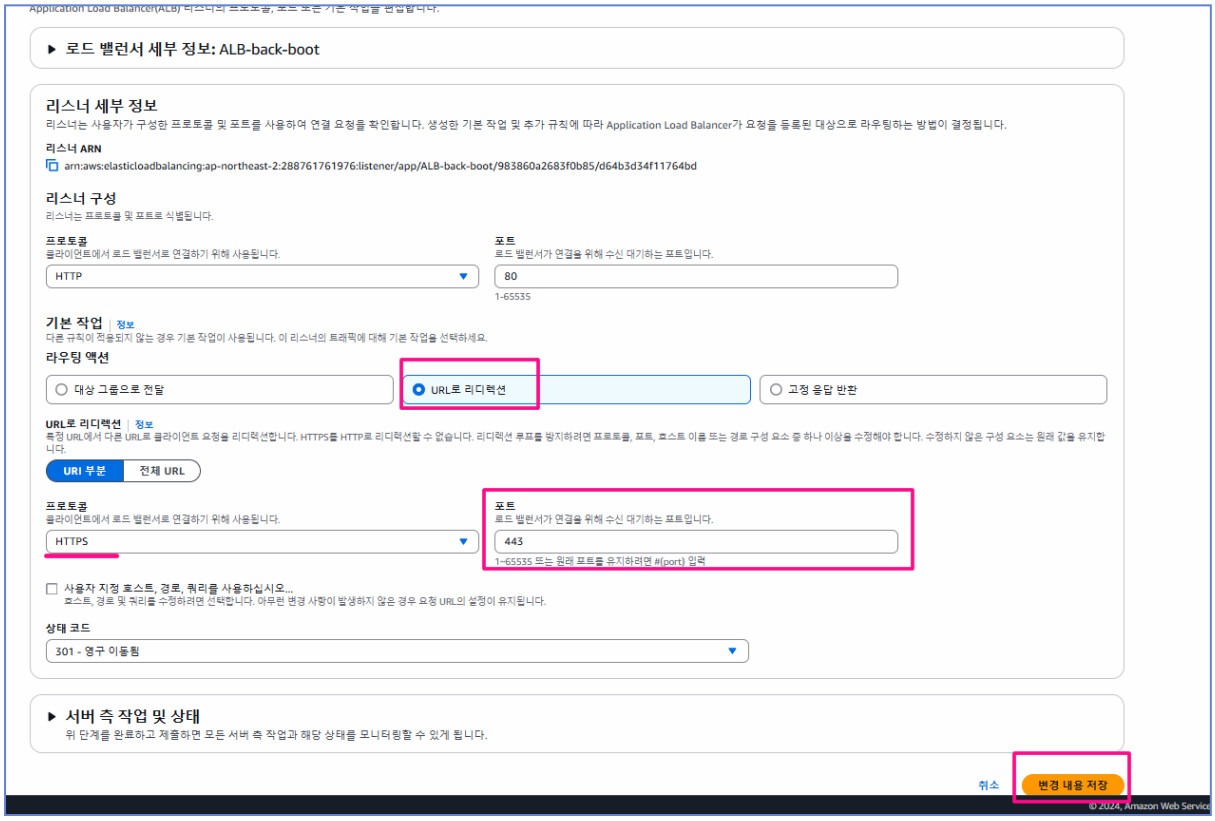


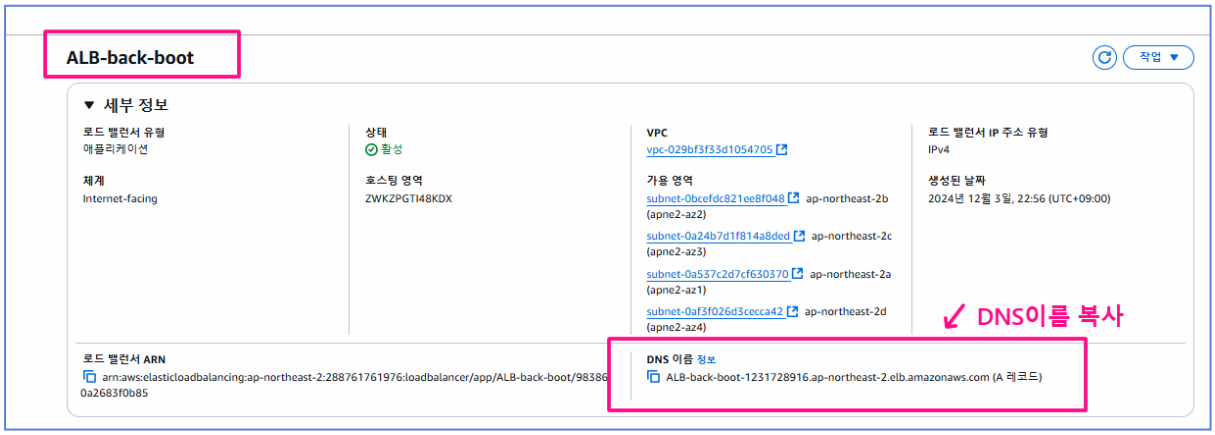
생성완료 후 리스너규칙에서 http:80의 규칙편집을 클릭해서 수정을 한다.

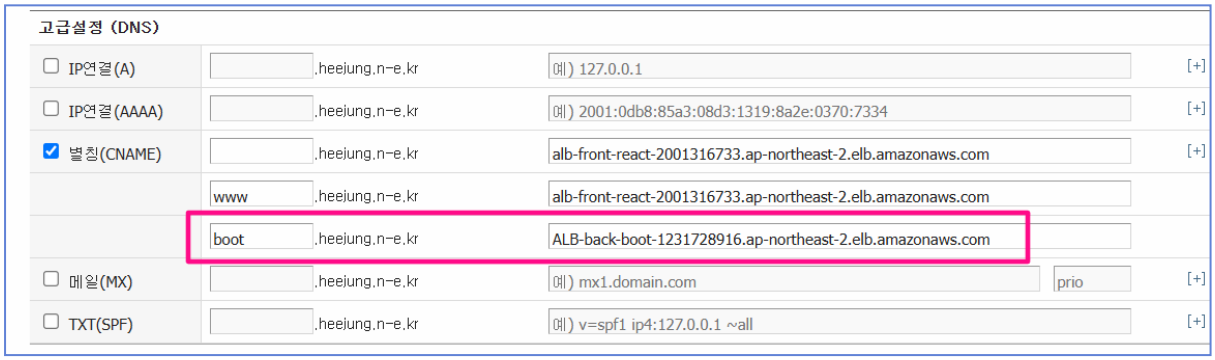




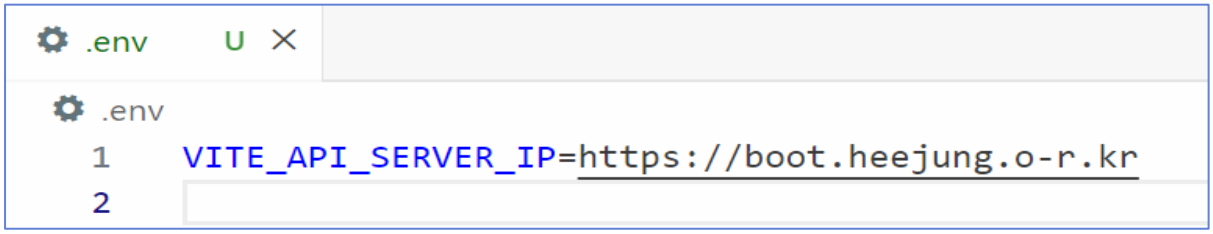
8253jang@daum.net
장희정







Front소스를 수정한다.



react프로젝트에 있는 dist폴더를 삭제한다.

npm run build

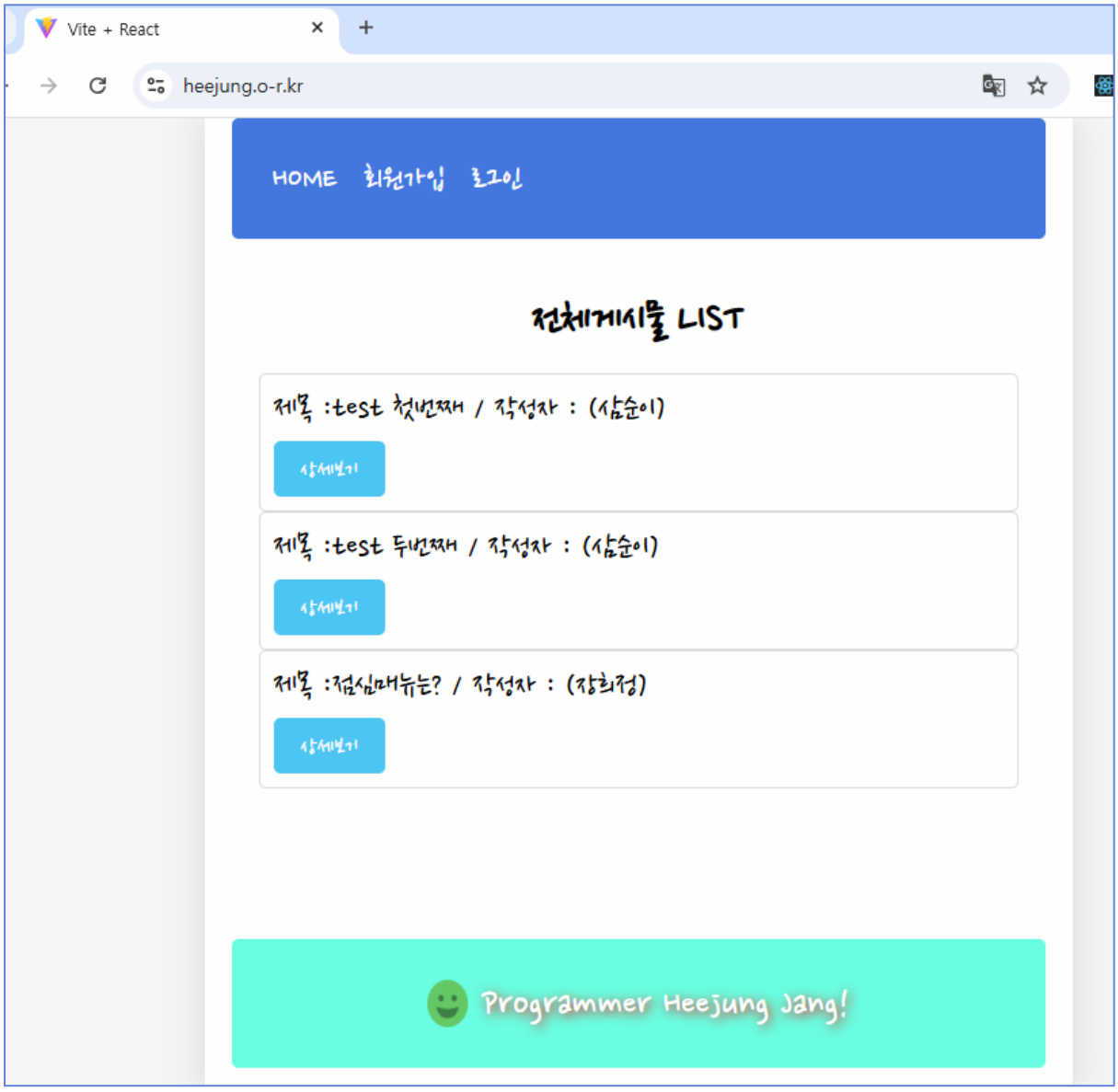
git add ./dist

git commit –m "메시지"

git push origin main

mobaXterm 접속해서 git을 내려 받고 파일을 nginx 폴더에 넣는다.

sudo systemctl restart nginx


Vite + React
heejung.o-r.kr
HOME 회원가입 로그인
전체게시물 LIST
제목 :test 첫번째 / 작성자 : (삼순이)
상세보기
제목 :test 두번째 / 작성자 : (삼순이)
상세보기
제목 :점심메뉴는? / 작성자 : (장희정)
상세보기
Programmer Heejung Jang!